Постоянный Комитет Союзного государства Беларуси и России
Аппарат Совета Безопасности РФ
Парламентское Собрание Союза Беларуси и России

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXI научно-практической конференции

17–19 мая 2016 года, г. Смоленск

Москва
Медиа Группа «Авангард»
2016

УДК 004(470+476)(061.3)
ББК 32.81

К63 **Комплексная защита информации:** материалы XXI научно-практической конференции, Смоленск, 17–19 мая 2016 г., — Москва, Медиа Группа «Авангард», 2016 год — 242 с.

ISBN 978-5-9906093-1-0

В сборнике представлены доклады ученых, специалистов, представителей государственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных направлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

УДК 004(470+476)(061.3)
ББК 32.81

ISBN 978-5-9906093-1-0

ОРГКОМИТЕТ КОНФЕРЕНЦИИ

СОПРЕДСЕДАТЕЛИ

БУРАВЛЕВ Сергей Михайлович,
Заместитель секретаря Совета безопасности РФ

ГАЙДУКЕВИЧ Валерий Владимирович,
Председатель Комиссии Парламентского Собрания Союза Беларуси и России по безопасности, обороне и борьбе с преступностью

ЧЛЕНЫ ОРГКОМИТЕТА

ГОРБАЧ Александр Николаевич,
директор Государственного предприятия «НИИ ТЗИ»

КАЧАЛИН Игорь Федорович,
заместитель начальника Центра ФСБ России

КУЗНЕЦОВ Николай Михайлович,
заместитель Губернатора Смоленской области

КУЗЬМИЦКИЙ Дмитрий Александрович,
начальник отдела Комитета государственной безопасности Республики Беларусь

КУЦ Анатолий Владимирович,
заместитель директора ФСТЭК России

ЛУНТОВСКИЙ Георгий Иванович,
Первый заместитель Председателя Банка России

НОСКОВ Алексей Васильевич,
начальник управления связи Государственного пограничного комитета Республики Беларусь

ОДЕРИХО Дмитрий Анатольевич,
заместитель начальника отдела Министерства внутренних дел Республики Беларусь

ПАВЛЮТЬ Александр Александрович,
заместитель начальника главного центра обеспечения безопасности информационных технологий Вооруженных Сил Министерства обороны Республики Беларусь

СИЛИЦКИЙ Андрей Геннадьевич,
начальник отдела Оперативно-аналитического центра при Президенте Республики Беларусь

СОКОЛОВ Алексей Валерьевич,
заместитель Министра связи и массовых коммуникаций РФ

ФИСЕНКО Владимир Карпович,
ведущий научный сотрудник ОИПИ Национальной академии наук Беларуси

ПРОГРАММНЫЙ КОМИТЕТ КОНФЕРЕНЦИИ

СОПРЕДСЕДАТЕЛИ

КОНЯВСКИЙ Валерий Аркадьевич,
научный руководитель ОАО «КБПМ» (Ростех)

ХАРИН Юрий Семёнович,
директор НИИ ППМИ БГУ

СЕКРЕТАРИ

ЗУБКОВ Артем Николаевич,
член Совета МОО «Ассоциация защиты информации», Генеральный директор Медиа Группы «Авангард» (РФ)

ЛАСИЦА Александр Михайлович,
начальник отдела Государственного предприятия «НИИ ТЗИ» (РБ)

ЧЛЕНЫ ПРОГРАММНОГО КОМИТЕТА

АБЛАМЕЙКО Сергей Владимирович,
ректор Белорусского государственного университета, академик НАН Беларуси (РБ)

АНИЩЕНКО Владимир Викторович,
заместитель генерального директора по науке и инновациям ЗАО «СОФТКЛУБ-Центр разработки», Председатель Совета Научно-технологической ассоциации «Инфопарк» (РБ)

БОБОВ Михаил Никитич,
заведующий отделом ОАО «АГАТ-системы управления» — управляющая компания холдинга «Геоинформационные системы» (РБ)

ЕМЕЛЬЯНОВ Геннадий Васильевич,
Президент МОО «Ассоциация защиты информации», кандидат физ.-мат. наук, член-корреспондент Академии криптографии РФ, действительный государственный советник РФ 3 класса (РФ)

ИВАНОВ Олег Вячеславович,
генеральный директор «Центр исследования безопасности информационных технологий» (РФ)

КУРБАЦКИЙ Александр Николаевич,
заведующий кафедрой БГУ (РБ)

КУЧИНСКИЙ Пётр Васильевич,
директор НИИ ПФП (РБ)

ПРИВЕТСТВИЕ ГОСУДАРСТВЕННОГО СЕКРЕТАРЯ СОЮЗНОГО ГОСУДАРСТВА БЕЛАРУСИ И РОССИИ Г. А. РАПОТЫ

Уважаемые участники конференции!

От имени Постоянного Комитета Союзного государства и от себя лично приветствую гостей и участников XXI научно-практической конференции «Комплексная защита информации»!

Вопросы совершенствования информационной безопасности Союзного государства и национальных систем защиты информации крайне важны для национальной безопасности России и Беларуси и Союзного государства в целом.

Достаточно отметить, что в целях решения этих вопросов выполнены три союзные программы и планируется проект новой программы «Паритет-2020».

Ежегодный статус этой конференции и широкий круг ее участников вот уже в течение 20 лет позволяет своевременно и на высоком техническом уровне отслеживать и реализовывать все передовые достижения в области информационной безопасности.

Повестка дня конференции охватывает весь перечень ключевых тем в области комплексной защиты информации, включая информационные системы и их стандартизацию. В ходе конференции вам предстоит обстоятельно проработать ряд практических, отраслевых вопросов, включая научные и образовательные, в том числе по формированию тематики будущих программ в этой области.

Выражаю уверенность, что данная конференция послужит дальнейшему динамичному развитию информационных технологий и средств их защиты в государствах-участниках Договора о создании Союзного государства, а ее поочередное проведение в различных регионах Беларуси и России — популяризации ее результатов на всем информационном пространстве Союзного государства.

Желаю участникам конференции успешной и результативной работы на благо государств-участников Союзного государства.

Государственный Секретарь
Союзного Государства Беларуси и России
Г. А. Рапота

ПРИВЕТСТВИЕ ЗАМЕСТИТЕЛЯ СЕКРЕТАРЯ СОВЕТА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ С. М. БУРАВЛЕВА

Приветствую организаторов, участников и гостей XXI научно-практической конференции «Комплексная защита информации»!

Стремительное развитие информационных и коммуникационных технологий и их активное внедрение во все сферы жизнедеятельности, а также формирование глобального информационного пространства ставят задачу по обеспечению информационной безопасности в разряд государственных приоритетов.

Уровень безопасности информационного пространства Союзного государства непосредственно влияет на возможность реализации прав и свобод граждан, на сохранение суверенитета и обеспечение стабильного развития экономики наших стран. При этом очевидно, что противодействие угрозам в информационной сфере возможно только на основе дальнейшего укрепления сотрудничества.

На протяжении длительного времени Конференция способствует консолидации усилий органов государственной власти, представителей научного, экспертного и бизнес-сообщества Республики Беларусь и Российской Федерации на данном стратегически важном направлении.

Итогом многолетней работы Конференции стало формирование эффективного механизма взаимодействия ведущих профильных экспертов в интересах выработки единого понимания основных вызовов и угроз в информационной сфере, а также согласованных подходов к решению широкого спектра актуальных задач в этой области.

Полагаю, что в ходе обсуждения вопросов повестки дня будут всесторонне проанализированы назревшие проблемы, касающиеся наиболее чувствительных аспектов обеспечения информационной безопасности, и определены оптимальные пути их решения.

Уверен, что практика ежегодного проведения Конференции будет способствовать эффективной реализации Соглашения между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности.

Желаю организаторам, участникам и гостям Конференции успешной и конструктивной работы.

Заместитель Секретаря Совета Безопасности Российской Федерации
С. М. Буравлев

ПРИВЕТСТВИЕ НАЧАЛЬНИКА ОАЦ ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ БЕЛАРУСЬ С. В. ШПЕГУНА

Уважаемые организаторы, участники и гости конференции!

От имени Оперативно-аналитического центра при Президенте Республики Беларусь и себя лично позвольте поприветствовать и поздравить вас с открытием XXI научно-практической конференции «Комплексная защита информации»!

В условиях интенсивного развития информационных технологий проблемы своевременного предупреждения и нейтрализации угроз информационной безопасности Республики Беларусь и Российской Федерации, как никогда, актуальны. Первостепенное значение приобретают вопросы эффективности применения технических и криптографических средств и методов защиты информации.

В 2015 году завершена программа Союзного государства «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на основе высоких технологий» на 2011–2015 годы. Исполнителями от Республики Беларусь реализовано 16 мероприятий, в рамках которых получено 57 результатов интеллектуальной деятельности.

Авторитетный состав участников конференции позволит обсудить перспективы использования полученных результатов и предложить новые направления исследований по совершенствованию системы защиты информационных ресурсов и систем.

Выражаю уверенность, что XXI научно-практическая конференция «Комплексная защита информации» станет площадкой для решения актуальных вопросов в сфере обеспечения защиты информации и безопасности объектов критически важной информационно-коммуникационной инфраструктуры Республики Беларусь и Российской Федерации, а также источником формируемой программы Союзного государства «Совершенствование системы защиты информационных ресурсов Союзного государства и государств — участников Договора о создании Союзного государства в условиях нарастания угроз в информационной сфере» на 2016–2020 годы.

Пользуясь случаем, позвольте выразить благодарность участникам конференции и отметить, что проведение данного мероприятия способствует решению широкого спектра задач в области защиты информации и вносит существенный вклад в укрепление национальной безопасности Республики Беларусь и Российской Федерации

Хочется пожелать всем участникам конференции конструктивного диалога, налаживания профессиональных взаимоотношений, а также принятия выверенных и перспективных решений!

Начальник Оперативно-аналитического центра
при Президенте Республики Беларусь
С. В. Шпегун

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

РЕЗУЛЬТАТЫ ДЕЯТЕЛЬНОСТИ В ОБЛАСТИ УКРЕПЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОЮЗНОГО ГОСУДАРСТВА

А. Н. ГОРБАЧ
директор государственного предприятия «НИИ ТЗИ»

Внедрение и совершенствование информационных технологий для автоматизации процессов взаимодействия между субъектами государств-участников Союзного государства в различных областях повышает эффективность их деятельности. Поэтому задача обеспечения безопасного использования непрерывно развивающихся информационных технологий в условиях изменяющегося спектра угроз всегда остается актуальной.

В условиях осложнения международной обстановки и активизации террористической деятельности усиливаются угрозы информационной безопасности Союзного государства, связанные с деятельностью иностранных государств, преступных сообществ и отдельных лиц в таких сферах, как государственное управление, банковская деятельность, эксплуатация автоматизированных систем управления технологическими процессами критически важных объектов, обработка персональных данных.

В этой связи одним из важных направлений деятельности Союзного государства является предупреждение и нейтрализация угроз информационной безопасности общих информационных ресурсов Республики Беларусь и Российской Федерации.

С целью единого научно-технического обеспечения защиты общих информационных ресурсов Беларуси и России Союзным государством непрерывно осуществляется деятельность, связанная с реализацией программ по укреплению информационной безопасности государств-участников Союзного государства.

В настоящее время завершена реализация программы Союзного государства «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на основе высоких технологий» на 2011–2015 годы (далее — Программа), утвержденной Постановлением Совета Министров Союзного государства от 20 апреля 2012 года № 6.

Целью Программы являлось решение задач обеспечения безопасности информации в критически важных системах информационной инфраструктуры и защиты информации ограниченного доступа в системах ее обработки, представленных ранее в рамках программ «Защита общих информационных ресурсов Беларуси и России» и «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на 2006–2010 годы». Выбранный подход позволяет целенаправленно формировать систему представлений, основных принципов, мер и средств предотвращения угроз безопасности информации, контроля эффективности применения разработанных мер и средств.

Реализация Программы позволила:

- осуществить разработку высокотехнологичных научно-технических решений для реализации мер по предупреждению и нейтрализации угроз общим информационным ресурсам Беларуси и России при внедрении новых технологий;
- обеспечить гармонизацию национальных нормативных правовых актов и методических документов в области защиты информации;

– создать условия для обеспечения устойчивого функционирования автоматизированных систем управления жизнеобеспечением городов и населенных пунктов, систем управления потенциально опасными объектами, предотвращения аварий и катастроф, заражения среды обитания;
– создать условия для обеспечения безопасности персональных данных в информационных системах персональных данных органов власти Союзного государства и государств-участников.

Государственным заказчиком Программы от Республики Беларусь выступал Оперативно-аналитический центр при Президенте Республики Беларусь.

Функции головного исполнителя Программы от Республики Беларусь выполняло Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации» (Государственное предприятие «НИИ ТЗИ). Головной исполнитель Программы в соответствии с заключенным контрактом с Государственным заказчиком осуществлял текущее управление реализацией Программы.

Исполнителями от Республики Беларусь выполнены 16 мероприятий Программы, в том числе 7 научно-исследовательских работ (НИР) и 9 опытно-конструкторских работ (ОКР).

В качестве исполнителей Программы с белорусской стороны участвовали государственное предприятие «НИИ ТЗИ», научно-исследовательское учреждение «Институт прикладных физических проблем им. А. Н. Севченко» Белорусского государственного университета, учреждение Белорусского государственного университета «Научно-исследовательский институт прикладных проблем математики и информатики», общество с ограниченной ответственностью «Лайт Вел Организейшн», закрытое акционерное общество «НТЦ Контакт», общество с ограниченной ответственностью «СЕНКОМ СИСТЕМС», закрытое акционерное общество «АВЕСТ».

В качестве соисполнителей Программы с белорусской стороны участвовали закрытое акционерное общество «БЕЛТИМ СБ», учреждение Белорусского государственного университета «Научно-исследовательский институт прикладных проблем математики и информатики», общество с ограниченной ответственностью «БАЙТИС», закрытое акционерное общество «АВЕСТ».

Необходимо отметить, что некоторые ОКР проведены совместно с российскими коллегами — представителями компании «Газинформсервис». В итоге результаты получены действительно совместными усилиями белорусских и российских ученых.

По результатам анализа проводимых исследований в Республике Беларусь в области защиты общих информационных ресурсов и систем информационно-телекоммуникационной инфраструктуры Союзного государства, хода их выполнения установлено, что все исследования проведены в соответствии с техническими заданиями по заключенным договорам. Сроки выполнения этапов НИОКР совпадают со сроками, указанными в ранее утвержденных планах-графиках выполнения НИОКР. Все работы по мероприятиям Программы, предусмотренные заключенными договорами, исполнителями выполнены полностью в установленные сроки.

Результаты реализации Программы соответствуют поставленным цели и задачам.

Оценка достижения результатов решения задач Программы проведена на основе показателей:

Показатели при решении первой задачи:

– количество проектов документов, разработанных исполнителями Республики Беларусь, регламентирующих деятельность по обеспечению безопасности информации

в критически важных системах информационной инфраструктуры — 11 (планируемое количество — 3);
- количество разработанных программно-технических средств обеспечения безопасности информации в критически важных системах информационной инфраструктуры — 1 (планируемое количество — 1);

Показатели при решении второй задачи:
- количество проектов документов, разработанных исполнителями Республики Беларусь, регламентирующих деятельность по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну (государственные секреты), при использовании высоких технологий её обработки — 15 (планируемое количество — 1);
- количество разработанных программно-технических средств защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну (государственные секреты), при использовании высоких технологий её обработки — 8 (планируемое количество — 8).

Экономический эффект от реализации Программы получен за счёт:
- предотвращения ущерба в результате нарушения функционирования информационно-телекоммуникационных систем органов власти и организаций Союзного государства или минимизации такого ущерба в случае реализации информационных угроз;
- экономии расходов Беларуси и России на защиту национальных информационных ресурсов и обеспечение безопасности информации в критически важных системах информационной инфраструктуры в результате применения средств защиты информации, единых нормативных правовых и методических документов, разработанных совместно в ходе выполнения Программы;
- развития производства конкурентоспособных технических, программно-аппаратных и программных средств защиты информации;
- ускорения темпов роста экономик государств-участников, развивающихся в условиях защищенного единого информационного пространства.

Экономический эффект от реализации программных мероприятий оценивается величиной финансовых средств, сэкономленных за счёт разработки единых для Союзного государства средств защиты информации, нормативных и методических документов, по отношению к суммарным затратам органов Российской Федерации и Республики Беларусь, уполномоченных в области защиты информации, если бы они такую разработку осуществляли самостоятельно.

Основными направлениями практического использования результатов реализации Программы являются:
- организация производства в Беларуси и России разработанных в ходе выполнения Программы высокотехнологичных средств защиты информации;
- обеспечение руководителей и специалистов, работающих в сфере обеспечения информационной безопасности Союзного государства и государств-участников, необходимыми нормативными и методическими документами, разработанными в ходе выполнения Программы;
- применение полученных результатов в интересах Беларуси и России при разработке и введении в действие национальных нормативных и методических документов в области защиты информации.

СЕКЦИОННОЕ ЗАСЕДАНИЕ «АКТУАЛЬНЫЕ ПРОБЛЕМЫ КАДРОВОГО ОБЕСПЕЧЕНИЯ ОТРАСЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

ОСОБЕННОСТИ ПРЕПОДАВАНИЯ ДИСЦИПЛИНЫ «СОЦИАЛЬНО-ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» В БГУИР

Л.М. ЛЫНЬКОВ, Т.В. БОРБОТЬКО, А.М. ТИМОФЕЕВ
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники»

В настоящее время информационно-психологическая безопасность является главным стратегическим объектом комплексного воздействия, осуществляемого в форме тайных операций информационно-психологической войны, которая определяет характер выбора целей, задач, формирования и использования сил и средств тайных операций на различных уровнях — оперативном, тактическом и стратегическом [1, 2].

В современных условиях информационное противоборство является эффективным, но еще не используемым в полной мере средством обеспечения геополитического баланса [3]. Решение практических задач геополитической конкурентной борьбы с использованием средств и методов информационного противоборства позволяет, в частности, даже слабым государствам и коалициям сохранять относительную независимость в виде выбора собственного внешнеполитического курса и возможности давать достойный (асимметричный) ответ на вызовы конкурирующих геополитических субъектов. С развитием сетевой информационно-телекоммуникационной инфраструктуры даже самые удаленные от линии непосредственного соприкосновения с вероятным противником районы и расположенные в них объекты оказываются в зоне досягаемости современных средств поражения. Таким образом, геополитическое пространство приобретает новые измерения, включая в себя пространство информационное и информационно-психологическое [3–6]. Обеспечение информационно-психологической безопасности является одним из приоритетных направлений национальной безопасности Республики Беларусь и других развитых стран.

Также следует отметить, что системы социальных отношений современного информационного общества оказывают достаточно сильное влияние на его формирование и развитие, что позволяет рассматривать эту систему в качестве среды организации и проведения информационно-психологических воздействий. Кроме того, использование социально-психологических средств и методов может являться одним из основных инструментов для осуществления несанкционированного доступа к информации. В этой связи при подготовке специалистов в области информационной безопасности представляется весьма важным изучение в учреждениях высшего образования социально-психологических аспектов информационной безопасности, что являлось целью данной работы.

Учебная дисциплина содержит следующие основные разделы:

- «Методология информационно-психологической безопасности», в котором предусмотрено изучение роли и места информационно-психологической безопасности в современном обществе, классификации угроз информационно-психологических воздействий на общество и методов противодействия их реализации, а также рассмотрение видов информационно-психологических воздействий в социальных системах;
- «Технологии информационно-психологических воздействий», содержащий такие подразделы, как «Объекты управления в социальной сфере», «Технологии информационно-психологического воздействия в массовых информационных процессах» и «Государственное регулирование в сфере обеспечения социально-психологической информационной безопасности»;
- «Скрытое управление личностью», предусматривающий изучение психологических основ и технологий скрытого управления личностью, а также средств защиты населения от такого воздействия;
- «Принципы социальной инженерии по противодействию утечке информации», в котором рассматриваются основные способы проникновения на охраняемый объект и способы несанкционированного доступа к конфиденциальной информации;
- «Личностные и социальные конфликты и методы их преодоления», в котором содержатся вопросы общей теории конфликта, в частности, его психологические и социальные составляющие, а также конфликты в сфере информационной безопасности;
- «Внутриличностные и межличностные конфликты и стратегия поведения», где предусмотрено изучение условий возникновения, типологии, последствия и механизмы разрешения внутриличностных и межличностных конфликтов;
- «Межгрупповые, межэтнические и межгосударственные конфликты», содержащий такие подразделы, как «Конфликты между социальными группами», «Межэтнические конфликты» и «Политические и межгосударственные конфликты»;
- «Обучение личности безопасному поведению с учетом психофизических характеристик», в котором рассматриваются методы исследования конфликтов (структурно-функциональный, процессуально-динамический, прогностический, разрешительный и др.), а также методы убеждений и воздействий (аутогенная тренировка, гипноз, подражание и пр.);
- «Информационное оружие», содержащий такие подразделы, как «Информационно-коммуникационное пространство войн», «Дискредитация руководства государства» и «Война компроматов»;
- «Системы массового оповещения», содержащий обзор акустических и телекоммуникационных систем оповещения, в том числе различных сетевых технологий, используемых средствами массовой информации;
- «Чрезвычайные ситуации и системы мультимедиа», содержащий такие подразделы, как «Методы защиты от негативных воздействий со стороны мультимедийных систем», «Контроль состояния человека» и «Стратегия защиты».

Изучаемые в рамках семинарских занятий методики тестирования и оценки различных аспектов социально-психологического поведения позволят специалистам в области информационной безопасности получить практические навыки и умения по оценке особенностей нервной системы, восприятия, памяти, внимания и мышления человека, достаточно важные при обеспечении информационной безопасности. Проведение диагностик по установлению различных особенностей нервной системы человека, а также его поведения, психического состояния, личностных качеств, логичности мышления,

темперамента и эмоциональной устойчивости позволяет развить механизмы информационно-психологической защиты личности. Разрабатываемые в рамках самостоятельной работы студентов программные комплексы могут быть использованы для диагностики силы, уравновешенности и подвижности нервной системы личности, а также для оценки уровня ригидности, конфликтности/тактичности и потребностей в саморазвитии.

Получение знаний о практических аспектах построения системы обеспечения национальной безопасности в результате изучения учебной дисциплины «Социально-психологические аспекты информационной безопасности» позволяет установить внутренние и внешние источники угроз национальной безопасности в социальной и информационной сферах, а также основные направления нейтрализации этих угроз.

Опыт преподавания учебной дисциплины «Социально-психологические аспекты информационной безопасности» у студентов специальности «Защита информации в телекоммуникациях» показал, что изучаемые в рамках лекционных и семинарских занятий вопросы вызвали повышенный интерес, что, безусловно, способствовало высокоэффективному формированию академических, социально-личностных и профессиональных компетенций у будущих специалистов по защите информации и инженеров по телекоммуникациям.

Исходя из особенностей развития современного информационного общества и возникающих новых угроз информационной безопасности в социально-психологической сфере, изучаемая дисциплина «Социально-психологические аспекты информационной безопасности» представляется весьма динамичной, что обуславливает необходимость внесения соответствующих корректив в ее содержание.

ЛИТЕРАТУРА

1. Операции информационно-психологической войны: краткий энциклопедический словарь-справочник / В. Б. Вепринцев [и др.]. — 2-е изд. — М.: Горячая линия-Телеком, 2015. — 495 с.
2. *Малюк А. А.* Защита информации в информационном обществе: учебное пособие для вузов / А. А. Малюк. — М.: Горячая линия-Телеком, 2015. — 230 с.
3. *Манойло А. В.* Технологии несилового разрешения современных конфликтов / А. В. Манойло; под ред. А. И. Петренко. — 2-е изд. — М.: Горячая линия-Телеком, 2015. — 392 с.
4. *Лыньков Л. М.* Особенности проведения практических занятий по дисциплине «Социально-психологические аспекты информационной безопасности» / Л. М. Лыньков, Т. В. Борботько, А. М. Тимофеев // Управление информационными ресурсами: материалы докладов XII Междунар. науч. — практ. конф., Минск, 11 декабря 2015 г. / Академия управления при Президенте Республики Беларусь; редкол.: И. И. Ганченок [и др.]. — Минск: Академия управления при Президенте Республики Беларусь, 2015. — С. 203–204.
5. *Новиков В. К.* Информационное оружие — оружие современных и будущих войн / В. К. Новиков. — М.: Горячая линия-Телеком, 2014. — 264 с.
6. *Душкина М.Р.* PR и продвижение в маркетинге: коммуникации и воздействие, технологии и психология: учебное пособие / М. Р. Душкина. — СПб.: Питер, 2010. — 560 с

ПРОБЛЕМЫ ПОВЫШЕНИЯ ГРАМОТНОСТИ В ОБЛАСТИ БЕЗОПАСНОСТИ ГРАЖДАН РФ

А.Е. БРАЖНИКОВ
НП «СЗИ»

Скорость, с которой современные информационные и телекоммуникационные технологии ворвались в нашу жизнь, позволила говорить о «цифровой революции», которая уже преобразует социальную и экономическую жизнь. В индустрии коммуникации и информации происходят коренные изменения. Чтобы охватить 50 миллионов человек, радио понадобилось 38 лет, а телевидению — 13 лет. Всего лишь за 4 года столько же людей стали использовать Интернет.

В 1993 году в «глобальной паутине» насчитывалось только 50 страниц; сегодня их более 1 миллиарда. В 1998 году к Интернету было подключено всего лишь 143 миллиона человек, к 2001 году количество пользователей достигло 700 миллионов человек, а в настоящее время — около 3 миллиардов. Интернет уже применяется в гораздо более широкой сфере, чем любое из когда-либо применявшихся ранее средств связи.

Громкий скандал вокруг Эдварда Сноудена и его разоблачения дали понять, что граждане любой страны уязвимы перед тотальной слежкой за ними через интернет и средства мобильной связи.

Оказалось, что не только государства, но и преступные сообщества используют новые технологии для преступной деятельности против граждан. Неграмотность населения в сфере высоких технологий приводит к кражи информации, денежных средств, шантажу граждан.

На текущий момент государство может защитить себя от угроз в сфере информационной безопасности, а обычные граждане нет! Это связано с тем, что люди мало имеют информации по методам защиты себя в области безопасности.

Исходя из этого был создан проект «Защитим себя вместе». Цель проекта направлена на помощь гражданам РФ в защите собственных интересов в различных сферах безопасности жизнедеятельности.

В 2013 г. под эгидой НП «Союз защитников информации» совместно с Министерством образования Московской области был проведен проект по защите информации в образовательных учреждениях Московской области.

Силами членов НП «СЗИ» на безвозмездной основе были защищены 7 образовательных учреждений Московской области.

По результату работ был разработан полный пакет документов по защите информации, который в себя включает: руководящие документы, учебные пособия и методические рекомендации, что позволяет сократить затраты по защите информации в образовательных учреждениях.

В 2014 году выпущена первая книга «О защите персональных данных» в которой рассказывалось в простой форме о данной проблеме.

Оказалось, что эта книга интересна и полезна, и необходима!

После этого вышел ряд книг: «Практические рекомендации по соблюдению законодательства Российской Федерации о персональных данных образовательными организациями», «Практические рекомендации как обезопасить себя от ненадежных партнеров», «Иностранные разведки.Сегодня».

Сейчас планируются «Теоретические основы технических разведок», «Основы защиты от технических разведок», «Иностранные разведки. Франция», «Иностранные разведки. Турция», «Практические рекомендации по безопасности в интернет пространстве», «Практические рекомендации по безопасности в финансовой сфере», «Практические рекомендации по безопасности в повседневной жизни гражданина».

Создан Клуб «Защитим себя вместе» — совместный проект общественных организаций специализирующихся в сфере безопасности жизнедеятельности граждан Российской Федерации и Торгового дома «Библио-Глобус».

Задача Клуба — оказание помощи гражданам РФ в защите собственных интересов в различных сферах безопасности жизнедеятельности. Реализация различных программ, проектов и мероприятий по безопасности жизнедеятельности граждан РФ. Обсуждение и презентация новых книг, практических рекомендаций, методик, которые будут полезны гражданам в защите своих прав в области безопасности жизнедеятельности.

Встречи, конференции, выставки, конкурсы и заседания в рамках клуба «Защитим себя вместе» охватывают актуальные вопросы безопасности жизнедеятельности граждан РФ: бизнес, банковский сектор, образование, здравоохранение, история, взаимоотношения с органами власти и многое другое, что может помочь человеку защитить себя от угроз, которые появляются в мире высоких технологий.

Созданы страницы в социальных сетях интернет, где размещены рекомендации по безопасности жизнедеятельности, освещаются новости в области безопасности.

Готовится ряд мероприятий по тематике «Безопасность в образовании», «Безопасность и общество». Все это направлено на повышение грамотности населения в сфере безопасности и возможности им самим противостоять угрозам новых технологий и возможностей преступных сообществ.

МЕДИЙНОЕ СОПРОВОЖДЕНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ СОРЕВНОВАНИЙ МОЛОДЕЖИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК ФОРМА ПРОФЕССИОНАЛЬНОЙ ОРИЕНТАЦИИ

А.Н. ЗУБКОВ
член Совета МОО «АЗИ»,
ООО «Медиа Группа «Авангард»
Е.Б. МЕЛЬНИКОВА
ООО «Медиа Группа «Авангард»

В 2013 году Правительством Российской Федерации утверждена Стратегия развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года. В документе определены масштабные задачи по обеспечению интенсивного роста отрасли. При этом отмечается нарастающий дефицит квалифицированных кадров в сфере информационных технологий и информационной безопасности. Общее число программистов в стране оценивается в 300 тыс. человек, а ежегодный выпуск специалистов в области АйТи составляет около 25 тыс.

В Стратегии отмечено, что «...сложившаяся ситуация уменьшает шансы России войти в число мировых лидеров сегмента заказной разработки программного обеспечения и аут-

сорсинга в сфере информационных технологий … Дальнейшее развитие большинства сегментов отрасли требует решения проблемы нехватки квалифицированных кадров».

Среди факторов, ограничивающих развитие отрасли информационной безопасности в России, отмечаются следующие:

– обострившийся в последние годы дефицит кадров;
– недостаточный уровень подготовки специалистов;
– и недостаточно высокая популярность профессий отрасли информационных технологий и защиты информации.

В связи с этим развитие человеческого капитала, в том числе за счет развития профильного образования и популяризации профессий отрасли отнесены Стратегией к числу основных задач развития отрасли информационной безопасности России.

Стоит акцентировать, что направление популяризации сформулировано в Стратегии достаточно конкретно, как «популяризация информационных технологий как сферы деятельности и смена имиджа отрасли от системного администрирования и разработки интернет-сайтов к созданию необходимых обществу комплексных технологий и решений».

При этом в документе отмечается, что высокая степень осведомленности о возможностях своего развития в области безопасности информационных технологий присутствует у молодежи в гг. Москве, Санкт-Петербурге, Казани, Екатеринбурге, Новосибирске и связанных с ними агломерациях. В связи с этим особенно важно обеспечить популяризацию соответствующих профессий среди молодежи и других экономически развитых регионов России.

В свете поставленных задач заслуживает внимания опыт работы в данном направлении отраслевых СМИ, созданных Медиа Группой «Авангард».

Медиа Группа с 2011 года ежеквартально выпускает журнал «BIS Journal. Информационная безопасность банков» и на постоянной основе сопровождает интернет-портал «Информационная безопасность банков», посвященные информационной безопасности банков, кредитно-финансовых организаций, платёжных систем. Издание осуществляется в партнерстве с отраслевыми сообществами — Ассоциация Российских Банков и Ассоциация защиты информации. Успех и стабильность этого пула СМИ обеспечило то, что он полностью отвечает потребностям сложившегося к тому времени весьма специфического сегмента IT-аудитории — специалистов в области информационной безопасности банков и кредитно-финансовых организаций.

К началу 2010-х годов данное направление деятельности сформировалось в самостоятельный рынок с собственными нормативно-правовой базой, заказчиками, поставщиками, специалистами и инфраструктурой. Прежде тематика информационной безопасности банков размывалась между банковским делом, вопросами корпоративной безопасности и IT-проблематикой. Специализированного периодического издания для обмена мнениями, обсуждения проблем и совместной выработки специалистами решений не существовало. Поэтому инициатива создания такого журнала и интернет-портала получила поддержку отраслевых регуляторов — Банка России, ФСБ России, ФСТЭК России и Роскомнадзора. Результаты медиа-исследований предпочтений экспертов показали, что такое специализированное издание, освещающее отраслевую проблематику, высоко востребовано.

Проблема кадров в сфере информационной безопасности банков в силу специфики этого сегмента стоит даже более остро, чем в целом по IT-отрасли, поэтому журнал BIS Journal и интернет-портал «Информационная безопасность банков» с самого начала уде-

ляют ей особое постоянное внимание. Популяризация информационной безопасности как сферы деятельности ведется в нескольких направлениях.

Во-первых, публикация популярных очерков по истории криптографии и информационной безопасности, очерков о людях, сыгравших в истории профессии заметную роль. Для этого в журнале созданы рубрики «История» и «Корифеи». Публикующиеся в них материалы являются увлекательным чтением как для специалистов, так и для широкого круга лиц. Безусловно, рассказы об истории отрасли и ее выдающихся представителях служат более глубокому пониманию сути профессии, своеобразным ориентиром, маяком при выборе школьниками и студентами жизненного пути. Всего по заказу редакции подготовлено и опубликованы десятки таких материалов.

Во-вторых, публикация материалов разных жанров (очерков и интервью) о наших современниках — людях, сыгравших заметную роль в становлении сферы информационной безопасности России на современном этапе, а также действующих ведущих практиках. Например, очерки — творческие портреты создателей современной банковской IT-системы России. Также публикации создателей FinCERT: Г. И. Лунтовского — первого заместителя председателя Банка России и А. М. Сычева — заместителя начальника Главного управления информационной безопасности и защиты информации Банка России. Большой резонанс в интервью с Натальей Касперской — генеральным директором российской компании InfoWatch.

Встречи на страницах журнала с такими незаурядными и в высшей степени компетентными людьми не только проясняет современную картину в сфере информационной безопасности страны, но и заряжает энергией, заставляет полюбить дело, которым занимаются герои публикаций, и, более того, расставляют правильные как профессиональные, так и нравственные акценты.

В-третьих, публикация материалов в специальной рубрике «Молодой специалист». Эта рубрика ориентирована именно на молодежь и проблемы молодежи, связанные с профессией. В ней используется все многообразие журналистских жанров и форм подачи материала: репортажи, интервью, статьи, мнения, авторские публикации. Такие материалы редакция старается разнообразно и качественно иллюстрировать.

Рубрика обладает широкой тематической амплитудой. Например, олимпиады школьников по математике, криптографии и информационной безопасности освещаются как в жанре классического репортажа, созданного репортерами издания, так и в жанре аналитической статьи, написанной авторитетными авторами.

В качестве примера можно привести статью вице-президента Академии криптографии РФ, доктора физико-математических наук В. Н. Сачкова «Спрос на таланты в математике и криптографии будет только расти». Такой же подход сохраняется и в освещении студенческой темы, а также в темах карьерного роста молодых специалистов, повышения квалификации на рабочем месте и др.

В-четвертых, самостоятельным направлением можно выделить освещение интеллектуальных соревнований для старшеклассников по профилю «информационная безопасность», в особенности их олимпиадный формат. С одной стороны, система проведения таких соревнований обеспечивает участие в них школьников из большого числа регионов, а не только из крупных городов. С другой стороны, их методическая база опирается на программы среднего общего образования и дополнительного образования детей, и именно такие специализированные олимпиады служат наиболее эффективным связующим звеном между школьниками и профессиями в сфере ИБ.

Подведение итогов каждой из таких олимпиад становится значимым информационным поводом и соответственно прекрасной возможностью привлечь внимание читателей к вопросам профориентации школьников, выбору ими жизненного пути. Медиа Группа «Авангард» с 2010 года непосредственно участвует в организации и поведении торжественных награждений победителей межрегиональных олимпиад по криптографии и по компьютерной безопасности.

Каждое такое мероприятие тщательно продумывается и проводится в общественно-значимых местах — так, чтобы стать важным, запоминающимся событием в жизни участников. Например, церемония награждения XXIII Межрегиональной олимпиады по математике и криптографии проходила в галерее народного художника СССР А. М. Шилова — члена Общественного совета при ФСБ России, и написать репортаж с нее редакция попросила Николая Конкина, председателя Совета директоров ЗАО «Холдинг Прогресс», который сделал это с вдохновением и на высоком аналитическом уровне.

Церемония награждения XXV Олимпиады проходила в Президентском зале РАН, где школьники имели возможность пообщаться с первыми лицами в сфере криптографии и информационной безопасности страны. В этом случае журнал опубликовал, помимо яркого фоторепортажа, мнения вице-президента Академии криптографии РФ В. Н. Сачкова и вице-президента РАН В. В. Козлова, а также серию мини-интервью с победителями Олимпиады. Значительность событий подтверждается и тем, что они освещаются в отраслевых и федеральных СМИ, в частности Российской газетой. Теле-киностудия Медиа Группы «Авангард» создает документальные фильмы, которые размещаются в открытом доступе на интернет-портале «Информационная безопасность банков» в разделе BIS TV.

Чтобы познакомиться с многообразием тем и ракурсов кадровой проблемы в сфере ИБ, находящих свое отражение в СМИ Медиа Группы, достаточно познакомиться с заголовками публикаций, увидевших свет в двадцати номерах журнала:

- «Девушка-разгадка. В банкиры — из «олимпийского резерва» [21].
- «Признания молодого специалиста. Чтобы защищать банковскую информацию, нужно научиться работать не только с «железом» и «софтом», но также с документами и персоналом» [23].
- «Сегодня подмастерья, а завтра мастера. Путь в первоклассные специалисты по защите информации начинается с младших классов обычной средней школы» [24].
- «Кадровая стратегия. Проведение олимпиад школьников по математике и криптографии помогает заблаговременно обеспечивать отрасль перспективными кадрами» [23].
- «Научить стратегическому опережению. Вузы должны выпускать не только квалифицированных пользователей систем и средств защиты информации, но и разработчиков решений» [29].
- «Новое пополнение формируется. Любовь к Родине — необходимый структурный элемент профессионального становления» [31].
- «Путь в повелители чисел. Школьные олимпиады по математике и информатике являются важным инструментом профессиональной ориентации и формирования кадрового резерва отрасли» [34].
- «Социальный лифт для профессионалов. Получить сертификацию ISACA непросто даже хорошему специалисту, но наградой служат высокий статус и карьерный рост» [35].

– «„Дорога, которую прокладываешь сам“. Дальновидные студенты упорно готовят себя к профессиональной карьере с вузовской скамьи» [36].
– «Ещё более страшно, чем ночью одной на тёмной улице». Угрозы и безопасность в интернете глазами старшеклассников» [23].

Большую роль в том, что рубрика уже несколько лет не перестает быть интересной и востребованной у читателей, является ее невидимая — журналистская и редакторская — составляющая. Именно журналисты и редакторы Медиа Группы «Авангард», находясь в постоянном поиске, формулируют новые темы для публикаций, откликаются на самые интересные, часто неожиданные, события, находят героев для очерков и репортажей, приглашают серьезных, вызывающих доверие, авторов аналитических статей и делают многое другое на благо своего издания.

Пятилетний опыт издания журнала и интернет-портала показал, что тема кадров в сфере информационной безопасности банков неисчерпаема, а ее актуальность со временем только нарастает. Были выявлены новые потребности аудитории, которые «бумажный» журнал в силу своего ограниченного объема не в состоянии полноценно удовлетворять. Поэтому Медиа группы «Авангард» работает над созданием самостоятельного образовательного интернет-портала «Дорога в будущее».

Концептуально портал охватывает и объединяет все многообразие кадровой тематики в сфере информационной безопасности. Он сопровождает своих читателей на всех ступенях профессиональной лестницы: от выбора жизненного пути на школьной скамье до поиска работы студентами и выпускниками вузов, и далее — на стадии «молодой специалист», где постоянное повышение квалификации является необходимым условием карьерного роста. В данный момент портал проходит апробацию в интернете, адрес http://theroadahead.ib-bank.ru/

Стратегия развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года в главе «Популяризация информационных технологий как сферы деятельности» дает конкретные рекомендации:

«Достичь поставленной цели возможно за счет репортажей в средствах массовой информации об историях, связанных с успехом в сфере информационных технологий, выпуска просветительских программ и публикаций, повествующих о преимуществах работы в отрасли, а также с помощью создания другой востребованной гражданами медиа-продукции.

Особое внимание следует уделить историям из жизни людей, успешных в области безопасности информационных технологий, основателей крупных, быстрорастущих или совершивших технологический прорыв компаний, достигших больших результатов в коммерциализации новых технологий».

Можно сделать вывод, что СМИ, выпускаемые Медиа Группой «Авангард», работают в русле этих рекомендаций, творчески развивают их и, безусловно, способствуют выполнению поставленной задачи. Все эти достижения были бы невозможны без постоянных тесных и доверительных контактов с отраслевым сообществом — экспертами, специалистами, представителями государственных, коммерческих и общественных организаций.

Выражаю коллегам благодарность за внимание и надежду на дальнейшее плодотворное сотрудничество!

СПИСОК ЛИТЕРАТУРЫ

1. Стратегия развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года, утверждена распоряжением Правительства Российской Федерации, 01.10.2013 г. № 2036-р.

2. Тайнопись древнерусских купцов. «BIS Journal» № 3(3)/2011
3. Борис Хагелин — отец коммерческой криптографии. К 120-летию рождения великого изобретателя и предпринимателя. «BIS Journal» № 3(6)/2012
4. На службе Родине, математике и криптографии. Жизнь и судьба В. Я. Козлова — одного из основоположников отечественной шифровальной науки. «BIS Journal» № 1(8)/2013
5. «Чтоб было в тех землях не знатно». К 380-летию первого документа, регламентирующего криптографическую деятельность в России. «BIS Journal» № 1(8)/2013
6. Гигант радиоинженерной мысли. К 105-летию со дня рождения В. А. Котельникова — основоположника отечественной науки секретной связи. «BIS Journal» № 2(9)/2013
7. Превращение криптологии в фундаментальную науку. Н. Н. Андреев: путь от инженера до президента Академии криптографии РФ. «BIS Journal» № 3(10)/2013
8. Пионеры отечественной машинной криптографии. К 70-летию присуждения Сталинской премии советским криптографам. «BIS Journal» № 4(11)/2013
9. Царь Алексей Михайлович — венценосный криптограф. Одним из важнейших нововведений времён его царствования стало учреждение и становление криптографической службы России. «BIS Journal» № 4(11)/2013
10. Важная веха истории отечественной криптографии. Исполняется 425 лет соглашению об организации шифрованной правительственной связи между Австрийской империей и Московским государством. «BIS Journal» № 1(12)/2014
11. Франц Эпинус: дольше всех во главе отечественной криптослужбы. К 290-летию со дня рождения выдающегося российского учёного-энциклопедиста. «BIS Journal» № 1(12)/2014
12. Защитники речи. О создателях отечественной техники шифрования голосовой связи. «BIS Journal» № 2(13)/2014
13. Колокольная стеганография. Увлекательная тайнопись утраченного символа Звенигорода. «BIS Journal» № 2(13)/2014
14. Рождение посольской тайнописи. Близится 425-летний юбилей начала российской шифрованной дипломатической переписки. «BIS Journal» № 3(14)/2014
15. Беспокойный гений. К 150-летию В. И. Кривоша, одного из лучших криптоаналитиков Российской империи, жизнь которого напоминает сюжет авантюрного романа. «BIS Journal» № 3(18)/2015
16. Криптограф Департамента полиции. Судьба И. А. Зыбина — самого талантливого специалиста царской охранки по «взлому» шифров «врагов внешних и внутренних». «BIS Journal» № 4(19)/2015
17. «СТО БР ИББС 20Соблюдение норм — основа доверия». «BIS Journal» № 4(15)/2014
18. «Внимание к безопасности — критерий зрелости. Стратегия снижения рисков в кредитно-финансовой сфере». «BIS Journal» № 2(21)/2016
19. Наталья Касперская: «Интернет — чудо, но в нём есть и…» Правилам информационной безопасности лучше всего начинать обучать в доступной форме с детского сада. «BIS Journal» № 3(10)/2013
20. «Спрос на таланты в математике и криптографии будет только расти». Победителей и призеров олимпиад школьников по математике и криптографии может ожидать большое будущее. «BIS Journal» № 3(14)/2014
21. Девушка-разгадка. В банкиры — из «олимпийского резерва». «BIS Journal» № 2(2)/2011
22. За семью паролями. Из студенток — в ангелы-хранители банковских тайн. «BIS Journal» № 2(5)/2012

23. Признания молодого специалиста. Чтобы защищать банковскую информацию, нужно научиться работать не только с «железом» и «софтом», но также с документами и персоналом. «BIS Journal» № 2(5)/2012
24. Сегодня подмастерья, а завтра мастера. Путь в первоклассные специалисты по защите информации начинается с младших классов обычной средней школы. «BIS Journal» № 4(7)/2012
25. Кадровая стратегия. Проведение олимпиад школьников по математике и криптографии помогает заблаговременно обеспечивать отрасль перспективными кадрами. «BIS Journal» № 2(9)/2013
26. «Учить информационной безопасности необходимо уже со школьной скамьи». Первый открытый онлайн-урок информационной безопасности для школьников киберполицейские провели в Москве. «BIS Journal» № 3(10)/2013
27. Да — безопасности, нет — беспечности! Участники автопробега Москва — Алтай преодолели 11 200 км, агитируя за безопасность электронных платежей. «BIS Journal» № 4(11)/2013
28. Готовить научную смену. В подготовке специалистов по информационной безопасности проявляется специфика университетского образования. «BIS Journal» № 1(12)/2014
29. Научить стратегическому опережению. Вузы должны выпускать не только квалифицированных пользователей систем и средств защиты информации, но и разработчиков решений. «BIS Journal» № 1(12)/2014
30. Школьники на стезе криптографии. Профессиональная ориентация специалистов информационной безопасности начинается в школе. «BIS Journal» № 2(13)/2014
31. Новое пополнение формируется. Любовь к Родине — необходимый структурный элемент профессионального становления. «BIS Journal» № 2(13)/2014
32. Гармония в алгебре. Характер подготовки специалистов по информационной безопасности в гуманитарных вузах определяется спецификой их будущей профессиональной деятельности. «BIS Journal» № 3(14)/2014
33. Школьные олимпиады по математике и информатике являются важным инструментом профессиональной ориентации и формирования кадрового резерва отрасли. «BIS Journal» № 4(15)/2014
34. Путь в повелители чисел. Школьные олимпиады по математике и информатике являются важным инструментом профессиональной ориентации и формирования кадрового резерва отрасли. «BIS Journal» № 4(15)/2014
35. Социальный лифт для профессионалов. Получить сертификацию ISACA непросто даже хорошему специалисту, но наградой служат высокий статус и карьерный рост. «BIS Journal» № 3(18)/2015
36. Александр Бердюгин: «Дорога, которую прокладываешь сам». Дальновидные студенты упорно готовят себя к профессиональной карьере с вузовской скамьи. «BIS Journal» № 4(19)/2015
37. «Ещё более страшно, чем ночью одной на тёмной улице». Угрозы и безопасность в интернете глазами старшеклассников. «BIS Journal» № 1(20)/2016
38. Призеры по призванию. Награждены школьники — победители XXV Олимпиады по математике и криптографии и X Олимпиады по компьютерной безопасности. «BIS Journal» № 2(210)/2016.

ПРОБЛЕМЫ ТРУДОУСТРОЙСТВА СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И СОВРЕМЕННЫЕ МЕТОДЫ РЕШЕНИЯ ЗАДАЧ КАДРОВОГО ОБЕСПЕЧЕНИЯ В СЛОЖИВШИХСЯ ЭКОНОМИЧЕСКИХ УСЛОВИЯХ

А.А. БОГАТЫРЕВА
Кадровое агентство ЦИБИТ
О.В. ИВАНОВ
ЦИБИТ

Если Вы в неформальной, дружеской обстановке зададите вопрос человеку, ищущему работу, почему он никак не может трудоустроиться, то с большей вероятностью он ответит, что работы на рынке практически нет, а те работодатели, которые есть предлагают рабский труд за миску чечевичной похлёбки. Если вы спросите работодателей, в чём причина столь долго поиска персонала, то скорее всего ответ будет такой: «На рынке только неучи и бездельники в высокими зарплатными ожиданиями». В кадровое агентство и соискатели и работодатели приходят как к врачу и откровенно говорят о своих проблемах, ожиданиях и опасениях. Непонимание рынка труда и нежелание принять во внимание текущую экономическую ситуацию не позволяет найти соискателям и работодателям друг друга.

Проблемы трудоустройства:

1. **Неправильный подход к поиску работу**

«Размещать резюме я не буду». «В эту компанию не пойду, они меня всё равно не возьмут». «Хорошо устроиться можно только по знакомству». Такие посылы нередки среди соискателей. И мы сталкиваемся с этим постоянно в нашем агентстве, проводя карьерные консультации. Если вы в поисках работы и цель её найти, то все средства хороши. Работодатель должен иметь возможность видеть ваше резюме. Оно должно быть, по крайней мере на 2–3 ведущих работных сайтах. Конечно, все знакомые должны быть оповещены, что вы в поисках. Разошлите резюме в кадровые агентства, пусть они проводят поиск за вас. Наше агентство активно ведёт работу с соискателями и уже для многих стало тем самым хороший знакомым, который может помочь с работой. Так что трудоустройство «по знакомству» применимо и к нам.

2. **Не хочется работать**

В общем-то, это может быть даже не явное нежелание, а подспудное. Есть люди, у которых после потери работы развивается депрессия, но есть и такие, кто вообще не желает работать, пусть даже это подсознательно. И если первым может помочь специалист-психолог, то вторым вряд ли что-то поможет, кроме проявления воли своего характера. Хотя иногда, особенно после долгого периода работы без отпуска, стоит дать себе время отдохнуть, набраться сил и соскучиться по трудовым будням.

3. **Я хочу мало работать и много получать.**

«У меня кредит», «Я женился», «Я снимаю квартиру, поэтому мне сейчас нужны деньги» — вот, по мнению соискателей, реальные причины, за которые им должны платить больше. Такой подход к оценке собственных профессиональных способностей раздражает работодателей. Чаще всего завышенные требования выдвигают молодые специалисты. Хотя долговые обязательства и семейные ситуации могут быть аргументом для повышения зарплаты. Работодатель хочет видеть, какая от сотрудника будет отдача. Важны опыт работы и профессионализм.

По мнению работодателей каждый третий кандидат предъявляет завышенные требования к заработной плате.

Есть категория заблуждающихся, кто не изучает рынок, а оценивает себя исходя из прошлого опыта работы. Обычно такие требования у бывших сотрудников банков или государственных структур, которых недавно сократили. Тут дело в том, что на прошлом месте им платили необоснованно высокую заработную плату, и теперь они считают, что на новой работе могут претендовать на те же суммы, а возможно и выше, учитывая их опыт работы. Особенно часто эту проблему мы видим у людей, которые проработали на одном месте больше 5 лет и не понимают реалий рынка труда. На сегодняшнем рынке этот вопрос стоит особенно остро, так как зарплаты упали на 20–30 %, и многие кандидаты, особенно те, кого сократили из крупных компаний, запрашивают суммы, бывшие актуальными 2–3 года назад.

Исходя из исследования на начало 2016 года.

Средняя заработная плата специалиста по информационной безопасности составляет в Москве –80 000 руб., в Санкт-Петербурге — 64 000 руб., в Волгограде — 38 000 руб., в Воронеже — 40 000 руб., в Екатеринбурге — 51 000 руб., в Казани — 40 000 руб., в Красноярске — 46 000 руб., в Нижнем Новгороде –44 000 руб., в Новосибирске — 50 000 руб., в Омске — 40 000 руб., в Перми — 46 000 руб., в Ростове-на-Дону — 45 000 руб., в Самаре — 46 000 руб., в Уфе — 40 000 руб., в Челябинске — 46 000 руб.

Кризис довольно неприятное слово. Хотя, для кого-то кризис, а для кого-то толчок к новым возможностям. Проблемы — двигают прогресс. На рынке труда не редки застои, но и они не повод для переживаний. В такие моменты, можно очень неплохо реализоваться и вашу работу ценят гораздо выше, нежели в благополучные времена.

А работодатель?

В 2015 году Центральным Банком России были отозваны лицензии у 93 кредитных организаций. В 2016 их пока 37. И достаточно большое количество персонала выплеснулось на рынок. При опросе работодателей многие говорят о том, что проблем с поиском не испытывают. У нас, в кадровом агентстве ЦИБИТ, учитывая нашу специализацию в отрасли, постоянно открыты вакансии специалистов по защите информации и информационной безопасности. Первичный отклик достаточно большой до 100 резюме на одну вакансию. Но при более детальном изучении выявляется, что соискатели, откликаясь не всегда понимают о чём речь. Или сложно опознаваемы в качестве специалистов по защите информации. Как мы в шутку говорим про них: «Кто Вы, доктор Зорге?» «В трудовой у меня записано: «программист». Согласно возлагаемым на меня задачам я больше похож на сисадмина, а информационной безопасностью занимаюсь вообще почти на общественных началах», — рассказывает системный администратор небольшой компании. Но и в более крупной компании штатное расписание может не предусматривать должность специалиста по информационной безопасности, хотя функционал востребован. Зная такую особенность мы просим соискателей приносить с собой на собеседование копию трудовой книжки и при возможности должностные инструкции, где был бы прописан функционал.

И всё же из 100 резюме только 5–6 соискателей можно показать работодателю исходя из компетенций. Но более профессионализма работодатели ценят честность и надежность. Специалист по информационной безопасности получает доступ к конфиденциальной информации компании. При необходимости, специалиста можно научить разбираться в новых системах. Если же человек профессионал в области информационной безопас-

ности, но к нему нет доверия — ни один руководитель отдела ИБ его не возьмет к себе в подразделение. Он опасен.

Настоящий специалист ИБ сочетает в себе множество талантов. Он одновременно:

- технарь, знающий софт и «железо»
- гуманитарий, умеющий использовать аналогии из привычной жизни
- педагог, обучающий пользователей
- экономист, доказывающий руководству необходимость инвестиций
- психолог, понимающий скрытые мотивы руководства и пользователей
- дипломат, разруливающий конфликты
- «сержант», умеющий «прикрикнуть»
- философ, не плачущий, когда начинается эпидемия или взломают сеть

СЕКЦИОННОЕ ЗАСЕДАНИЕ «АКТУАЛЬНЫЕ ВОПРОСЫ СОЗДАНИЯ ТРАНСГРАНИЧНОГО ПРОСТРАНСТВА ДОВЕРИЯ»

ТРЕБОВАНИЯ К СОЗДАНИЮ, РАЗВИТИЮ И ФУНКЦИОНИРОВАНИЮ ТРАНСГРАНИЧНОГО ПРОСТРАНСТВА ДОВЕРИЯ

С. А. КИРЮШКИН
Компания «Газинформсервис»

Для упрощения и стимулирования дальнейшего развития экономических связей в рамках Союзного Государства Беларуси и России путем построения эффективной системы трансграничной электронной торговли и широкого информационного взаимодействия необходима разработка и внедрение комплекса правовых, организационных и технических мероприятий, направленных на создание трансграничного пространства доверия (далее также «ТПД»).

Общепринятого единого концептуального подхода к построению систем трансграничного информационного взаимодействия на текущий момент не существует. Это обусловлено наличием в каждой отрасли и каждой стране своих особых требований по обеспечению юридической силы электронных документов и юридической значимости электронного взаимодействия. В результате в настоящее время отсутствуют слаженное взаимодействие инфраструктур и систем, влияющих на надежность, прослеживаемость и целостность электронной передачи данных при обмене электронными документами.

Таким образом, подготовка комплексных решений и предложение единой технологической, правовой и организационной базы для организации доверенного информационного взаимодействия между государствами позволит в результате сформировать ТПД для субъектов электронного взаимодействия.

Итогом этой работы должно стать создание проектов базовых нормативно-правовых и организационно-технических документов, создающих правовые, организационные и технические основы для организации юридически значимого трансграничного электронного обмена документами и данными при трансграничном информационном взаимодействии.

Доклад посвящен подходам, используемым при разработке системы технических требований к созданию, функционированию и развитию трансграничного пространства доверия.

АРХИТЕКТУРА БЕЗОПАСНОСТИ НАЦИОНАЛЬНОЙ СИСТЕМЫ БЕЗБУМАЖНОЙ ТОРГОВЛИ РЕСПУБЛИКИ БЕЛАРУСЬ

В. В. АНИЩЕНКО
Комитет по информационной безопасности Ассоциации «Инфопарк», ООО «СОФТКЛУБ»

Введение

Государство нуждается в инструменте, который позволит облегчить условия осуществления внешнеторговых сделок и упростит административные процедуры в Республике Беларусь, связанные с сопровождением внешнеторговой деятельности (ВТД), что позволит улучшить показатель страны «Международная торговля» в ежегодном отчёте Всемирного банка «Ведение бизнеса».

На сегодняшний день в Республике Беларусь, после заключения внешнеторговой сделки, участник ВТД должен пройти множество административных процедур различного характера для получения сопровождающих внешнеторговую сделку документов. Всё это требует обращений в огромное количество инстанций.

Компании, входящие в состав Научно-технологической ассоциации «Инфопарк», имеющие ряд компетенций в части реализации проектов, связанных с обеспечением электронной торговли внутри страны, автоматизации таможенных органов Республики Беларусь, при административной поддержке со стороны государства инициировали проект по разработке автоматизированной информационной системы, упрощающей административные процедуры сопровождения внешнеторговых сделок в Республике Беларусь и обеспечивающей электронное взаимодействие между субъектами внешнеторговой сделки и государственными органами, организациями, финансово-кредитными учреждениями. Данный проект включен в Государственную программу развития цифровой экономики и информационного общества на 2016–2020 годы под № 16 «Создание Национальной системы безбумажной торговли Республики Беларусь» (НСБТ).

Однако участие бизнеса возможно только при выполнении государством определённых условий. Сроки реализации проекта также зависят в первую очередь от оперативности действий государства в части адаптации национального законодательства и создания заинтересованности государственных органов, организаций, финансово-кредитных учреждений, регулирующих ВТД.

Предполагается, что создание НСБТ позволит обеспечивать проведение всех необходимых процедур, сопровождающих торговую сделку, посредством электронного взаимодействия всех участников через общенациональную систему электронной торговли, доступ к которой будет осуществляться через Единый портал при взаимодействии с защищенной платформой Общегосударственной автоматизированной информационной системы (ОАИС) и Государственной системой управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь (ГосСУОК). В НСБТ будет использован Единый стандарт электронного документа торговой сделки, разработанный на базе международных стандартов GOVCBR — GOVernment Cross Border Regulatory message (UN/EDIFACT, ЭДИФАКТ ООН).

Планируется, что разработчиком системы может выступить бизнес, а в рамках государственно-частного партнёрства будет сформирован владелец и оператор НСБТ.

Задачи НСБТ

Исходя из международного опыта построения общенациональных торговых систем, основными задачами НСБТ являются:

- автоматизация проведения бизнес процессов внешней и взаимной торговли;
- обеспечение однократного ввода информации о торговой сделке путём применения в системе Единого стандарта электронного документа торговой сделки;
- обеспечение информацией о торговой сделке всех заинтересованных органов государственного управления, участников торговых операций в рамках их компетенции;
- предоставление участнику торговых процессов в Республике Беларусь удобного инструментария для оперативного взаимодействия с регулирующими внешнюю и взаимную торговую деятельность государственными органами.

Логическая схема и архитектура НСБТ

В результате научно-технического сотрудничества представителей компаний Ассоциации «Инфопарк» с корейским партнёром KTNET (Korea Trade Network) предложено создать технологическую платформу (организационно-правовую и техническую среду) по охвату всей внешней и внутренней торговли Республики Беларусь.

Основными участниками НСБТ должны стать субъекты хозяйствования Республики Беларусь (производители и поставщики продукции (услуг), транспортно-логистические операторы, грузоперевозчики, торговые предприятия, экспортеры, импортеры, таможенные и экспедиционные агенты/брокеры и пр.), вовлеченные государственные органы и учреждения (посредством ОАИС), финансовые институты и организации.

Схематично НСБТ включает:

- подсистему поддержки портала безбумажной торговли, обеспечивающую сервисы маркетинга, лицензирования и сертификации, платежей и расчётов, таможенной и логистической поддержки;
- подсистему технологической инфраструктуры, обеспечивающую электронный коммерческий документооборот на базе стандартов EDI и взаимодействие с сервисами: Единого расчетного информационного пространства (ЕРИП), ГосСУОК и Доверенной третьей стороны (ДТС), Системы межведомственного документооборота (СМДО) и ОАИС;
- подсистему управления и мониторинга грузоперевозок, обеспечивающую сервисы консолидации грузов для перевозок, управления транспортной логистикой и контроля за перемещением товаров;
- подсистему поддержки информационного взаимодействия с международными транспортными системами: e-Freight, АС «Электронная перевозка» (БелЖД), TIR Carnet (БАМАП) и др.

Подсистема информационной безопасности НСБТ

Встроенные в программно-аппаратную инфраструктуру и автономные механизмы защиты информации обеспечат в НСБТ с заданным уровнем доверия доступность, целостность, конфиденциальность и юридическую значимость электронных документов при взаимодействии государственных и отраслевых информационных систем, а также позволят действовать в правовом поле, едином для всех участников информационного обмена во внутренней и внешней торговле.

Подсистема информационной безопасности НСБТ, с использованием: технических средств, включая средства передачи данных; общесистемного, прикладного и специ-

ального программного обеспечения; а также средств защиты информации — обеспечит решение задач защиты информации со следующим составом функций:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- управление идентификаторами и средствами аутентификации;
- управление криптографическими ключами и средствами криптографической защиты информации в соответствии с требованиями ГосСУОК, включая средства выдачи, отзыва и контроля сертификатов открытых ключей, а так же средства, выполняющие процессы шифрования, создания и проверки электронной цифровой подписи, создания и проверки ключей электронной цифровой подписи;
- антивирусная защита информации;
- регистрация и аудит событий безопасности;
- обнаружение и предотвращение вторжений;
- контроль и анализ защищенности информации;
- защита информации ограниченного распространения и средств защиты информации от несанкционированного доступа;
- обеспечение и контроль целостности интеграционной системы и информации;
- обеспечение доступности информации;
- защита сред виртуализации;
- защита технических средств;
- защита интегрированной системы и ее средств;
- защита систем связи и передачи данных.

Информационная безопасность НСБТ будет обеспечена путем реализации соответствующего комплекса мероприятий по управлению информационной безопасностью в соответствии с рекомендациями стандартов ISO/IEC 27001:2013 и ISO/IEC 27002:2013, а также других национальных и межгосударственных стандартов, перечень которых утверждается Оперативно-аналитическим центром при Президенте Республики Беларусь в рамках технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY), и в соответствии с которыми будут определены и реализованы политики, методы, процедуры, организационно-техническими структуры и функции программного обеспечения.

Информационная безопасность НСБТ будет реализована как в соответствии с национальными требованиями к обеспечению безопасности, так и с учетом межгосударственного взаимодействия с информационными системами государств — участников ЕАЭС и стран-членов ЕС в рамках инициативы по Гармонизации цифровых рынков Научно-технологической ассоциации «Инфопарк» и Европейской комиссии.

Применяемые сертифицированные решения по антивирусной защите обеспечат информационную безопасность НСБТ от угроз и последствий, исходящих от проникновения и воздействия вредоносных программ:

- нарушение конфиденциальности данных;
- нарушение целостности данных;
- нарушение доступности информационных систем.

Предусматривается реализация распространения средств антивирусной защиты на все информационные ресурсы НСБТ.

Защита конфиденциальной информации от несанкционированного доступа будет реализована с помощью сертифицированных средств защиты каналов (VPN), средств аутентификации пользователей и средств шифрования конфиденциальной информации.

СЕКЦИОННОЕ ЗАСЕДАНИЕ «ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»

ПОДХОД К ОЦЕНИВАНИЮ ПРОДОЛЖИТЕЛЬНОСТИ ЭТАПОВ ЖИЗНЕННОГО ЦИКЛА УЯЗВИМОСТЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Ю.К. ЯЗОВ, А.Л.СЕРДЕЧНЫЙ, И.А.ШАРОВ
ФАУ «ГНИИИ ПТЗИ ФСТЭК РОССИИ»

В настоящее время вопросу исследования уязвимостей программного обеспечения (ПО) уделяется достаточное внимание, о чём свидетельствует появление многочисленных информационных сообщений об уязвимостях на новостных и исследовательских ресурсах, освещающих события в области безопасности информации. И этот вопрос действительно важен, так как в основе большинства компьютерных атак лежит уязвимость ПО. Ежедневно публикуются сведения о более чем 15 таких уязвимостях разного уровня опасности, при этом несвоевременное устранение разработчиками даже одной критической уязвимости может стать причиной хищения конфиденциальной информации, нанесения репарационного ущерба, а также начала массового заражения компьютеров пользователей. Кроме того, даже с момента устранения разработчиком ПО уязвимости, обнаруженной в нём, может пройти немало времени, прежде чем данная уязвимость будет устранена администратором конкретной информационной системы. Чем больше проходит времени между обнаружением уязвимости и её устранением в информационной системе, тем больше возможностей для успешной реализации компьютерной атаки. Именно поэтому важным показателем для оценки защищённости информационных систем является продолжительность этапов жизненного цикла уязвимостей ПО. В настоящей статье предложен подход к оцениванию данного показателя при помощи модели жизненного цикла уязвимости и метода анализа косвенных сведений об уязвимостях, публикуемых в открытых источниках.

Для оценки уязвимостей в различных публикациях используется та или иная модель жизненного цикла уязвимости. Наиболее распространённой [1–7] является линейная диаграмма состояний, в которой стадии жизненного цикла уязвимости (такие как обнаружение, эксплуатация, устранение разработчиком и др.) последовательно сменяют друг друга. В [8] рассмотрена нелинейная диаграмма состояний, которая отражает более сложные зависимости этапов жизненного цикла (например, этап устранения уязвимости разработчиком может начинаться раньше этапа эксплуатации уязвимости). В [9] рассмотрена вероятностная модель, которая учитывает стохастический аспект смены этапов жизненного цикла.

Однако данные модели рассматривают лишь смену этапов жизненного цикла без учёта особенностей субъектов, которые определяют правила этих изменений. Например, уязвимость может стать опубликованной в нескольких случаях: разработчик ПО выпустил уведомление; исследователь опубликовал отчёт об обнаруженной уязвимости

в своём блоге; произошла утечка эксплойта в открытый доступ и др. При этом выпуск уведомления разработчиком и публикация эксплойта в открытом доступе могут происходить параллельно, а рассмотренные выше модели не позволяют учесть асинхронность изменений этапов жизненного цикла уязвимости и возможности нахождения уязвимости сразу в нескольких состояниях (одновременно быть «устранённой», «эксплуатируемой», но, при этом, «не опубликованной» как в случае с уязвимостями средств антивирусной защиты, разработчики которых стараются не афишировать недостатки безопасности в своих продуктах, но оперативно реагируют на результаты эксплуатации уязвимостей, а обновления рассылают без ведома пользователя в результате автоматическом режиме).

Для преодоления ограничений в моделях [1–9] в статье предложена модель жизненного цикла уязвимости, построенная на базе аппарата маркированных сетей Петри-Маркова [10]. Модель отражает процессы жизненного цикла уязвимости ПО с учётом субъектов, порождающих такие процессы (рисунок 1). Сама модель представлена на рисунке 2 (ввиду ограниченности объёма в статье приведена лишь сеть Петри без указания различий маркировки и вероятностей переходов).

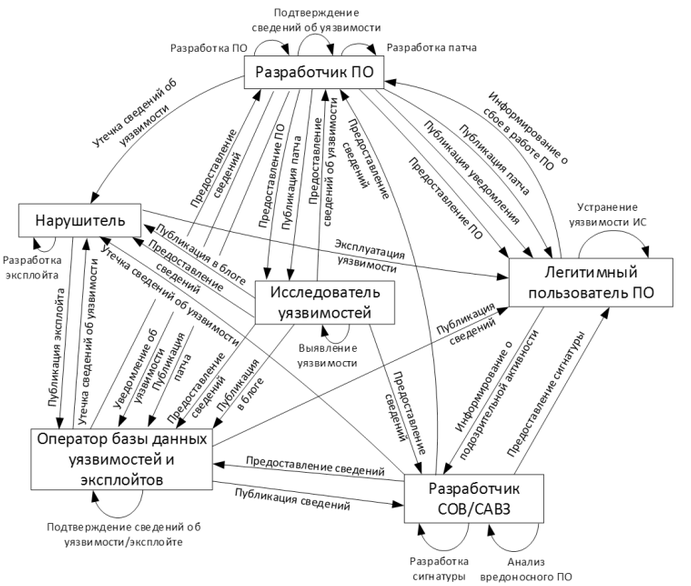


Рис. 1. Субъекты и процессы жизненного цикла уязвимости ПО

В качестве субъектов рассмотрены: исследователь уязвимостей ПО, разработчик ПО, легитимный пользователь ПО, разработчик СОВ/САВЗ, оператор базы данных уязвимостей и эксплойтов, а также нарушитель. Необходимо отметить, что в [1–9] разработчик СОВ/САВЗ в явном виде не рассматривался, однако, данный субъект имеет важное значение, так как он может обнаружить неизвестные экспойты и уязвимости на этапе функционирования ПО в результате выявления аномального поведения ПО. Также данный субъект занимается разработкой временного решения по устранению уязвимости до выхода официальных обновлений ПО.

Рассмотренные в [1–9] модели жизненного цикла уязвимостей ПО являются частными случаями предложенной модели. На рисунке 3 данное утверждение проиллюстрировано для моделей из [4] (рисунок 3.а) и [8] (рисунок 3.б).

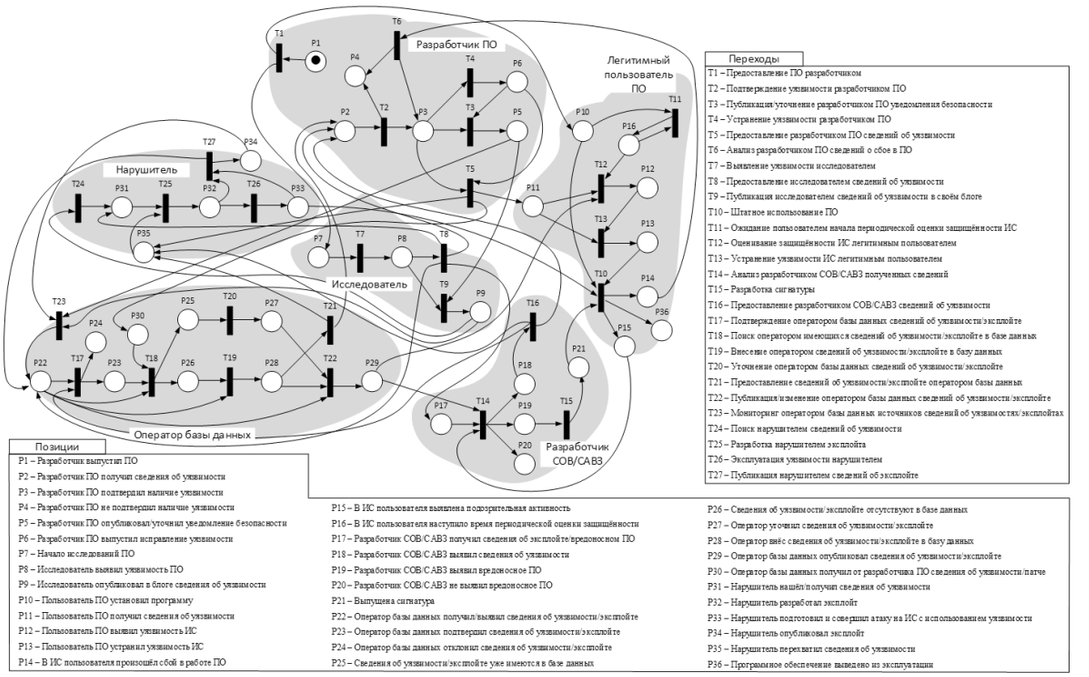


Рис. 2. Модель жизненного цикла уязвимостей ПО

Рис. 3. Сопоставление предложенной и существующих моделей жизненного цикла

Использование модели невозможно без предварительного задания её параметров: входных и выходных функций, функций задержек переходов, функций срабатывания переходов, вероятности выбора дуг и др. При этом значения параметров модели существенным образом зависят от цели исследований. Так, например, время устранения уязвимости для различных разработчиков может существенно отличается, соответственно, среднее время для разработчиков операционных систем будет отличаться от среднего времени для разработчиков браузеров.

Для определения параметров модели могут быть использованы открытые источники, публикующие сведения об уязвимостях программного обеспечения:

- базы данных уязвимостей/эксплойтов/сигнатур/инцидентов;
- уведомления/бюллетени безопасности разработчиков;

– новостные сайты и блоги исследователей безопасности информации.

В данных источниках содержатся как прямые, так и косвенные сведения, позволяющие воспроизвести хронологию событий, связанных с уязвимостями ПО.

Под прямыми сведениями будем понимать те сведения, которые точно указывают на какую-либо позицию или переход модели жизненного цикла уязвимости, а косвенными — параметры, которые характеризуют целый фрагмент модели, содержащий как минимум два элемента сети Петри. Для пояснения указанного принципа рассмотрим события жизненного цикла уязвимости CVE-2014–0983 в программе VirtualBox. Данная уязвимость была выявлена исследовательской группой Core Security, которая опубликовала отчёт о своих исследованиях [11]. В отчёте приведена хронология событий взаимодействия исследователя с разработчиком ПО, по которой можно определить параметры модели. Кроме того, в качестве дополнительных источников были рассмотрены:

– отчёт об изменении участка исходного кода VirtualBox [12] (данный отчёт позволил выявить дату подтверждения наличия уязвимости разработчиком ПО);
– уведомление безопасности разработчика Oracle Corporation [13], содержащий дату публикации разработчиком ПО сведений об уязвимости;
– сведения о дате публикации в базе данных эксплойтов Exploit Database [14].

На рисунке 4 показана модель жизненного цикла уязвимости CVE-2014–0983, построенная на основании предложенной модели и рассмотренных источников.

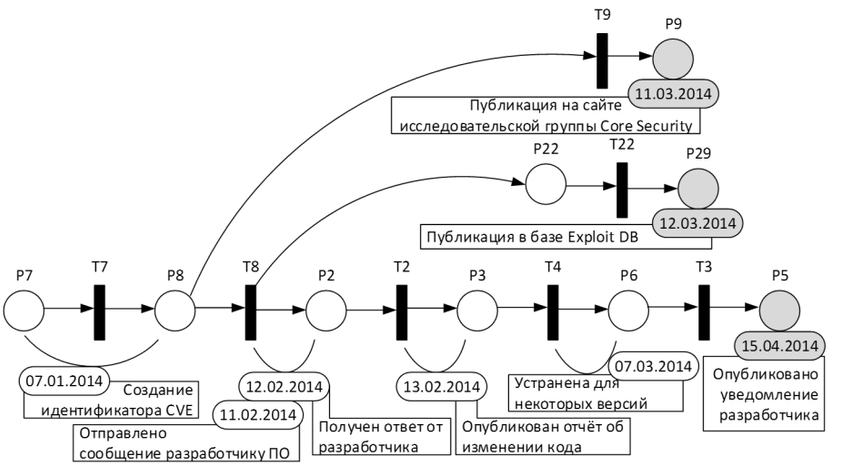


Рис. 4. Фрагмент модели жизненного цикла уязвимости CVE-2014–0983

На рисунке 4 отмечены прямые (даты публикации сведений об уязвимости исследователем, разработчиком ПО и оператором базы данных) и косвенные сведения (даты создания идентификатора CVE, отправления сведений об уязвимости разработчику ПО, получения подтверждения от разработчика, публикации разработчиком ПО отчёта об изменении уязвимого участка кода, устранения некоторых версий) о продолжительности этапов жизненного цикла уязвимости CVE-2014–0983, анализ которых позволяет сделать следующие выводы:

– прошло 98 дней с момента создания идентификатора CVE-2014–0983 до публикации сведений об уязвимости разработчиком ПО;
– прошло 35 дней с момента создания идентификатора CVE-2014–0983 до передачи сведений об уязвимости разработчику ПО;

– прошло более двух месяцев с момента получения разработчиком сведений об уязвимости до выпуска уведомления, содержащего рекомендаций по устранению;
– для некоторых версий VirtualBox уязвимость CVE-2014–0983 была опубликована, но не устранена 35 дней (являлась уязвимостью «нулевого дня»).

Анализ сведений, содержащихся в базах данных уязвимостей и эксплотов [15–22] показал, что наиболее распространёнными являются цепочки событий, показанные на рисунке 5.

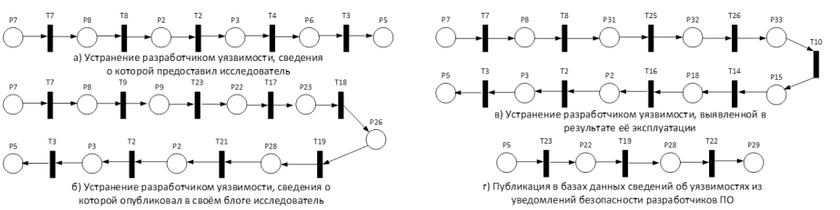


Рис. 5. Типовые цепочки событий, связанных с уязвимостями ПО

В интересах демонстрации возможности модели рассмотрим подход к оцениванию времени устранения уязвимости разработчиками основных типов программного обеспечения на основании косвенных сведений из базы NVD и CVE. Для анализа были выбраны сведения (опубликованные с 2008 по 2016 годы) об уязвимостях наиболее распространённых программных продуктов:

– операционные системы (Windows, ядро Linux, Red Hat, Ubuntu, openSuse, FreeBSD, Solaris, Android, MacOS/X);
– браузеры (Google Chrome, Safari, Firefox, Opera, Internet Explorer, Flash Player);
– системы управления базами данных (MS SQL Server, Oracle Database, MySQL, PostgreSQL, Firebird);
– офисное паромное обеспечение (Microsoft Word, Microsoft Excel, LibreOffice, OpenOffice, Microsoft PowerPoint, Acrobat Reader, WinRar, WinZip, Photoshop, Foxit Reader, Thunderbird, The Bat);
– серверное программное обеспечение (PHP, nginx, Lighttpd, Microsoft IIS, Tomcat, Apache HTTP Server, Bind, DHCP, NTP, OpenSSH, Samba);
– средства виртуализации (Java,.Net, ESX/ESXi, Xen Server, Virtualbox, Workstation).

Основная статистика по указанной выборки представлена на рисунке 6.

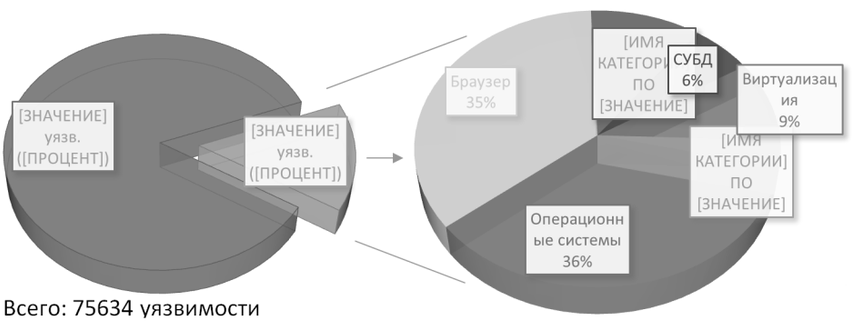


Рис. 6. Доля выбранных уязвимостей от общего числа уязвимостей базы данных NVD и их распределение по типам программного обеспечения

В базе данных NVD содержится дата публикации уязвимости, при этом, в соответствии с политикой NVD, сведения об уязвимости публикуются только после её устранения разработчиком ПО. Как было отмечено ранее при помощи базы CVE можно определить дату создания опубликованного идентификатора уязвимости. На первый взгляд, можно предположить, что идентификатор присваивается уязвимости тогда, когда сведения о ней поступили к сотрудникам, занимающимся ведением базы идентификаторов CVE, соответственно, разработчик узнает об уязвимости примерно в это же время. Если следовать данной логике, то можно посчитать время устранения уязвимости как разницу даты получения идентификатора CVE и даты публикации в базе NVD. Однако в реальности данные рассуждения оказываются ошибочными (если доверять информации из [11], идентификатор рассмотренной выше уязвимости был создан за месяц до предоставления сведений о ней разработчику). Это связано это с особенностями процедуры резервирования идентификаторов CVE.

Существует несколько способов получения идентификаторов, основной из которых — запрос идентификатора у одного из 18 (число актуально на февраль 2016 года) основных разработчиков программного обеспечения, которым MITRA делегировала полномочия назначать идентификаторы CVE. Для нашей выборки программных продуктов основными разработчиками являются компании Microsoft (2085 уязвимостей), Apple (1926 уязвимостей), Google (1334 уязвимостей), Adobe (1179 уязвимостей), Mozilla (1022 уязвимостей), Oracle (855 уязвимостей). На рисунке 4 показаны объём и порядок резервирования идентификаторов для уязвимостей, выявленных в выбранном ПО указанных разработчиков период с 2014 по 2016 годы.

Анализ показанных сведений позволяет выявить две важные особенности:

– большая часть идентификаторов CVE для ПО увязанных разработчиков резервируется большими порциями (по 50–150 идентификаторов в группе), для некоторых разработчиков можно выявить период резервирования (Oracle резервирует идентификаторы раз в три месяца);
– некоторые идентификаторы (например, рассмотренный ранее CVE-2014–0983) резервируются малыми группами (по 1–3 идентификатора в группе) в случайный момент времени.

В условиях отсутствия дополнительной информации о процедуре и количественных показателях ведения баз данных CVE и NVD можно сделать следующее предположение: в соответствии с внутренним распорядком и исходя из количества поступающих сведений об обнаруженных уязвимостях в своём ПО разработчик резервирует для подтверждённых уязвимостей идентификаторы CVE. При этом возможны ситуации, когда резервирование идентификаторов CVE осуществляется во внеочередном порядке как самими разработчиками, так сторонними исследователями. После выпуска обновлений разработчиком ПО сведения об уязвимостях публикуются в базе NVD. Данное предположение проиллюстрировано на рисунке 7 с использованием разработанной модели жизненного цикла уязвимости.

Исходя их данного предположения можно сделать вывод, о том, что время, прошедшее с момента получения идентификатора CVE до её публикации в NVD, находится в прямой зависимостью со временем устранения уязвимости разработчиком ПО.

На рисунке 8 отображена хронология резервирования идентификаторов CVE в период с 2014 по 2016 годы для выбранных разработчиков ПО, а на рисунке 9 показаны зависимости изменения времени, прошедшего с момента создания идентификатора CVE до

публикации сведений об уязвимости в базе NVD, для выбранных уязвимостей в соответствии с типом ПО.

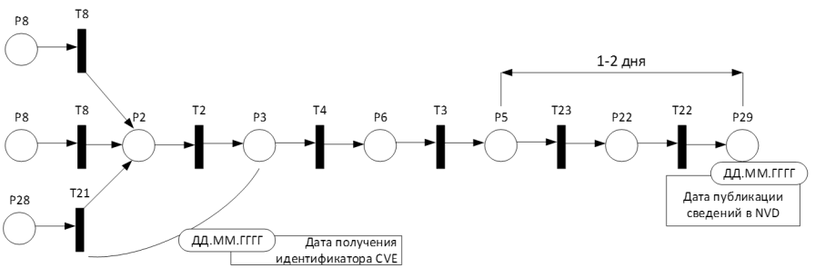


Рис. 7. Фрагмент модели жизненного цикла уязвимости, характеризующий события получения идентификатора CVE и публикации сведений в базе данных NVD

В результате анализа полученных данных выявлены следующие тенденции:

- снижение возраставшего до 2015 года времени, прошедшего с момента создания идентификатора CVE до её публикации в базе NVD, для серверного ПО, операционных систем, браузеров и офисного ПО;
- незначительный рост времени, прошедшего с момента создания идентификатора CVE до её публикации в базе NVD, для средств виртуализации;
- рост времени, прошедшего с момента создания идентификатора CVE до её публикации в базе NVD, для СУБД.

С учётом приведённого предположения о связи даты получения идентификатора CVE и дате выявления уязвимости аналогичные выводы можно сделать и в отношении времени устранения уязвимости разработчиками рассмотренных типов ПО.

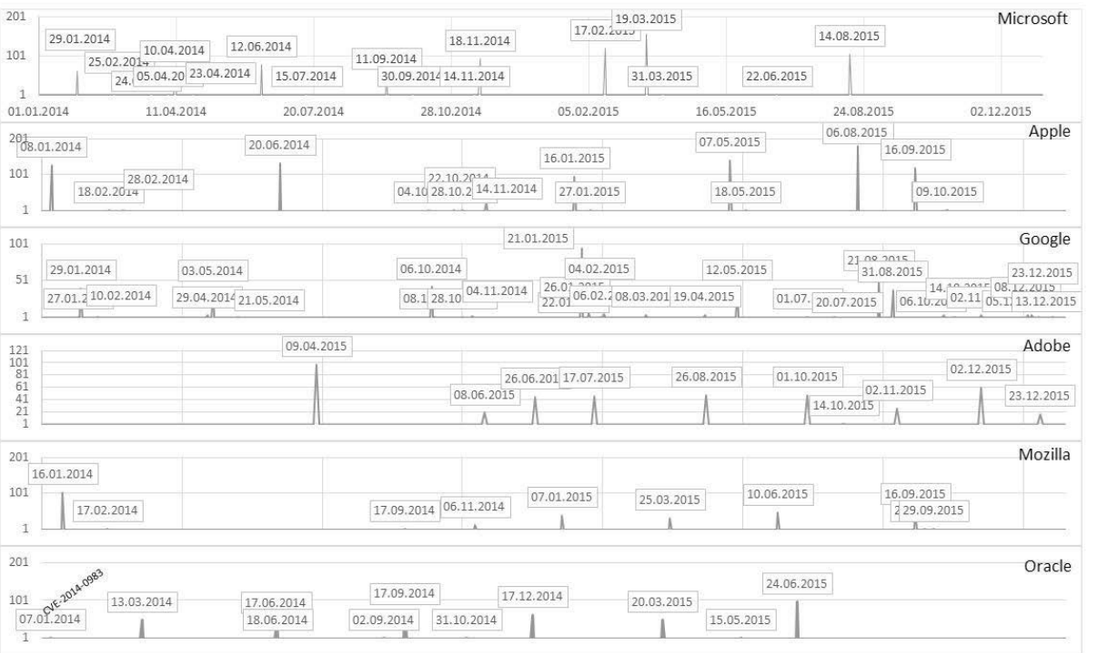


Рис. 8. Хронология резервирования идентификаторов CVE в период с 2014 по 2016 годы для выбранного ПО

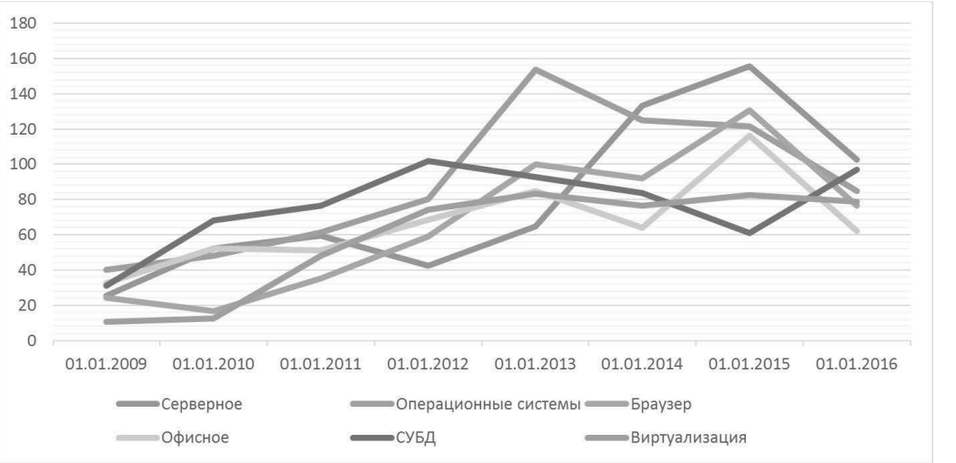


Рис. 9. Изменение времени, прошедшего с момента создания идентификатора CVE до публикации сведений об уязвимости в базе NVD, для выбранных уязвимостей

Таким образом, в статье рассмотрен подход к оцениванию продолжительности этапов жизненного цикла уязвимостей программного обеспечения на основе модели жизненного цикла уязвимостей программного обеспечения и предложена модель жизненного цикла уязвимостей программного обеспечения, основанная на использовании раскрашенных сетей Петри-Маркова и устраняющая ограничения существующих аналогичных моделей.

Также в статье определены понятия прямых и косвенных сведений об уязвимостях, которые можно использовать для расчёта параметров данной модели. Приведён пример расчёта продолжительности этапа устранения и публикации уязвимостей для таких типов ПО, как операционные системы, браузеры, офисное паромное обеспечение, серверное программное обеспечение и средства виртуализации. Расчёт проводился на основании косвенных сведений из баз данных CVE и NVD.

Предложенный подход позволит оценить вероятность реализации угроз, связанных с использованием уязвимостей ПО, и обосновать количественные требования к частоте обновления ПО, сканированию ИС на наличие уязвимостей и другим мерам защиты. Дальнейшим направлением исследований является проведение расчётов параметров модели жизненного цикла уязвимости для основных типов программного обеспечения, используемого в государственных информационных системах Российской Федерации.

ЛИТЕРАТУРА

1. *R. Wita, N. Jiamnapanon, Y. Teng-amnuay,* An Ontology for Vulnerability Lifecycle / Third International Symposium on Intelligent Information Technology and Security Informatics, 2010. p. 555–557.
2. *A. Jumratjaroenvanit, Y. Teng-amnuay,* Probability of Attack Based on System Vulnerability Life Cycle / International Symposium on Electronic Commerce and Security, 2008. p. 531–535.
3. *Browne H.K., W. A. Arbaugh, J. McHugh, and W. L. Fithen,* A trend analysis of exploitations / IEEE Symposium on Security and Privacy, 2001. p. 214–229.
4. *Al-Fedaghi S.,* System-based Approach to Software Vulnerability / IEEE International Conference on Social Computing / IEEE International Conference on Privacy, Security, Risk and Trust: p. 1072–1079.

5. *Frei, S., M. May, U. Fiedler, and B. Plattner,* Large-scale vulnerability analysis / SIGCOMM workshop on Large-scale attack defense, 2006, ACM: Pisa, Italy.
6. *Arbaugh, W.A., W. L. Fithen, and J. McHugh.,* Windows of vulnerability: a case study analysis / Computer, 2000. Volume 33(No. 12): p. 52–59.
7. *A. K. Shrivastava, R. Sharma, P. K. Kapur,* Vulnerability Discovery Model for a Software System Using Stochastic Differential Equation / International Conference on Futuristic trend in Computational Analysis and Knowledge Management, 2015. p. 199–205.
8. *Miles A. McQueen, Trevor A. McQueen, Wayne F. Boyer, May R. Chaffin.* Idaho National. Empirical Estimates and Observations of 0Day Vulnerabilities / Proceedings of the 42nd Hawaii International Conference on System Sciences — 2009, 12 p.
9. *HyunChul Joh, Y. K. Malaiya,* Defining and Assessing Quantitative Security Risk Measures Using Vulnerability Lifecycle and CVSS Metrics / Int'l Conf. Security and Management — 2009, p. 10–16.
10. *Язов Ю. К.* Основы методологии количественной оценки эффективности защиты информации в компьютерных системах. — Ростов-на-Дону, 2006. — 270 с.
11. Oracle VirtualBox 3D Acceleration Multiple Memory Corruption Vulnerabilities [Информационный ресурс]. Режим доступа: свободный — http://www.coresecurity.com/advisories/oracle-virtualbox-3d-acceleration-multiple-memory-corruption-vulnerabilities. Загл. с экрана. — Англ. яз.
12. Changeset 50441 in vbox [Информационный ресурс]. Режим доступа: свободный — https://www.virtualbox.org/changeset/50441/vbox. Загл. с экрана. — Англ. яз.
13. Уведомление безопасности разработчика Oracle Corp. [Информационный ресурс]. Режим доступа: свободный — http://www.oracle.com/technetwork/topics/security/cpuapr2014–1972952.html. Загл. с экрана. — Англ. яз.
14. База эксплойтов Exploit Database [Информационный ресурс]. Режим доступа — http://exploit-db.com свободный. Загл. с экрана. — Англ. яз.
15. Common Vulnerabilities and Exposures [Информационный ресурс] — Режим доступа: http://www.cvedetails.com/browse-by-date.php свободный. Загл. с экрана. — Яз.рус.
16. Национальная база данных уязвимостей США [Информационный ресурс]. Режим доступа — http://nvd.nist.gov свободный. Загл. с экрана. — Англ. яз.

СИСТЕМНЫЙ ПОДХОД: ЗАЩИТА ИНФОРМАЦИИ, ПОМЕХОЗАЩИЩЕННОСТЬ, ПОМЕХОУСТОЙЧИВОСТЬ

В. К. ЖЕЛЕЗНЯК
доктор техн. наук, проф., Полоцкий государственный университет
Д. С. РЯБЕНКО
канд. техн. наук, Полоцкий государственный университет
С. В. ЛАВРОВ
Полоцкий государственный университет

Объекты информатизации (ОИ) — автоматизированные системы формирования, обработки, преобразования, анализа, синтеза, моделирования сигналов различного назначения в аналоговой, цифровой форме. Системы многофункционального и многомерного назна-

чения представляются многоуровневыми моделями. Анализ таких моделей характеризуется при недостаточном объеме априорных сведений.

К априорным сведениям любого назначения информационных систем предъявляют требования высокой точности, чувствительности, помехозащищенности, высокого разрешения по частоте. Не менее сложной задачей является определение целевой функции и критериальных показателей. К таковым предъявляются показатели полноты, обобщенности, непротиворечивости, предпочтительности, эффективности.

Защищенность на ОИ устанавливается как приоритетное направление. Параметры, важнейшие характеристики определяют тесную связь с параметрами и характеристиками информационных систем ОИ. Информационные поля рассеивания формируют каналы утечки информации информационных систем. Параметры информационных сигналов, наведенные информационными полями рассеивания, являются случайными. Представление информационных полей рассеивания является векторным со случайными численными значениями и направлениями. Уровни излучений информационных полей рассеивания снижают их локализацией и схемно-конструктивными решениями. Нормированный показатель, устанавливающий защищенность каналов утечки информации от утечки, соответствует значению δ. В случае недостижимости значения δ, используют методы активного подавления маскирующими шумовыми сигналами, снижая помехозащищенность информационных систем объектов информатизации. Повышение помехозащищенности объектов информатизации обеспечивает их энергетическую и структурную скрытность [1]. Модель защиты информации представлена на рисунке 1.

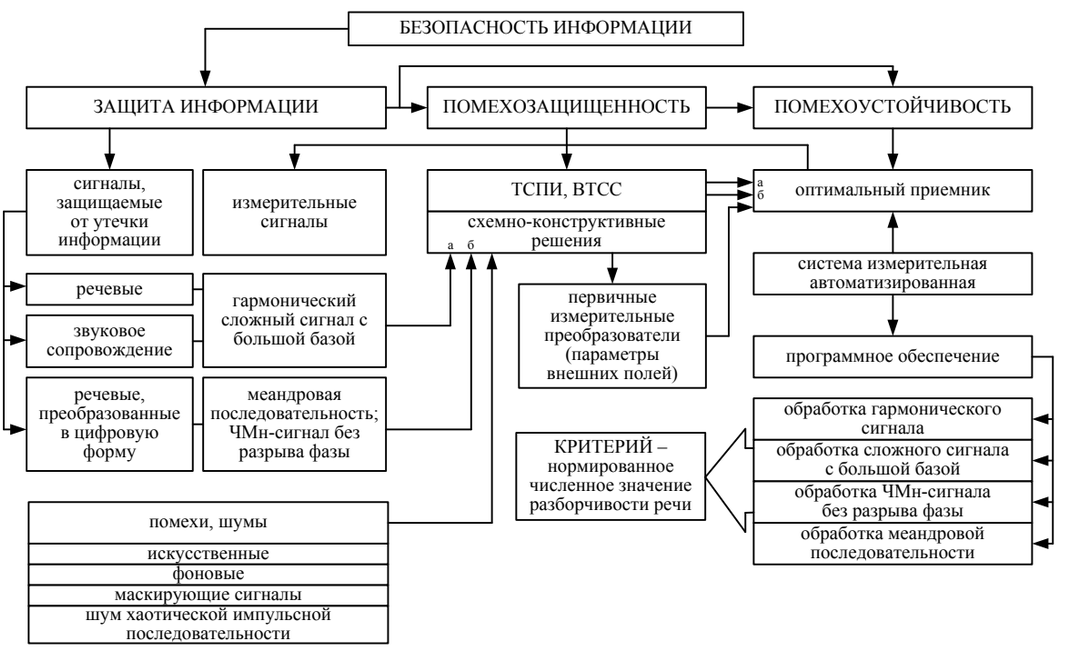


Рис. 1. Модель защиты информации.

На рисунке 1 представлены: ТСПИ — технические средства передачи информации, ВТСС — вспомогательные технические средства и системы, а, б — параметры сигналов на входе.

Система измерительная автоматизированная с программными компонентами генерирует измерительные сигналы и измерение их параметров, преобразовывает физические поля рассеивания в сигналы каналов утечки информации первичными измерительными преобразователями и обрабатывает оптимальным приемником. В зависимости от сигналов, защищаемых от утечки информации, измерительные сигналы различают:

- гармонический сложный сигнал с большой базой (ЛЧМ) — для речевых сигналов и сигналов звукового сопровождения видео;
- меандровая последовательность — для речевых сигналов, преобразованных в битовую последовательность;
- частотно-манипулированный сигнал без разрыва фазы — для речевых сигналов, преобразованных в цифровую форму.

Система измерительная автоматизированная осуществляет сбор первичной информации от всех видов каналов утечки речевой информации (акустический, виброакустический, электроакустический, магнитный, электрический, наводок сигналов рассеивания этих каналов на цепи управления, питания и заземления) путем преобразования физических информационных полей рассеивания в электрический сигнал. Система оценивает величину разборчивости речи в каналах утечки информации со слабыми сигналами в шумах высокого уровня в соответствии с требованиями нормативно-методических документов и обеспечивает полноту оценки защищенности ОИ.

Оценка и контроль защищенности речевой информации и принятых мер защиты основана на оценке физических параметров сигналов и фоновых шумов в каналах утечки информации с последующим автоматизированным расчетом обоснованного критерия — нормированного значения величины разборчивости речи.

Для оценки помехозащищенности в НЧ-диапазоне частот формируют стабильный в диапазоне частот шумовой сигнал. Такой сигнал формируется мерами напряженности магнитного поля в виде катушек (колец) Гельмгольца, по которым протекает электрический ток [2]. К таким катушкам предъявляются требования высокой точности, высокой стабильности по времени, обеспечение большого объема рабочего однородного поля. Кроме колец Гельмгольца используют системы контуров с током и соленоиды, обеспечивающие однородное поле и малые поля рассеивания за их пределами при наименьшем числе элементов системы [2].

Проблема повышения помехозащищенности и защищенности от утечки информации объектов информатизации является актуальной. Локализацию информационных магнитных полей рассеивания реализуют их экранированием с одновременной вынужденной деформацией полезного сигнала. Снижение весогабаритных характеристик аппаратуры весьма актуально. Экранам присуще изменять свои экранирующие свойства при воздействии на них ударов и вибраций. Актуальным является локализация полей рассеивания. Пассивные методы защиты информации повышают энергетическую и структурную скрытность [1], но не решают в полной мере поставленную проблему помехозащищенности и защиты информации, так как эти проблемы взаимоисключающие.

Для повышения защищенности информации практикуют активные методы защиты. Активные методы защиты, основанные на формировании маскирующих сигналов, которые повышают порог чувствительности при приеме информационных полей рассеивания. Таким образом, при определенных энергетических показателях (отношение сигнал/шум) обеспечивается защищенность объектов информатизации повышением порога чувствительности приема информационных полей рассеивания. Информационные поля

рассеивания характеризуются многовекторностью, формирующих информационное векторное поле.

Важным является разрушение каналов утечки информации активными способами — путем маскирования информационных и демаскирующих параметров сигналов маскирующими помехами. Активные методы защиты информации основаны на формировании преднамеренных шумов, обладающих необходимой эффективностью по заданному критерию эффективности, выбор которого обоснован в [3].

Маскирующие помехи, сформированные непосредственно из сигнала (видео-, речевой), наиболее адаптированы к его параметрам. В качестве источников генерации преднамеренных маскирующих шумов широко распространены шумовые диоды.

Основные параметры и характеристики помехи определяются источниками генерации преднамеренных маскирующих шумов, а усилительные каскады формируют частотный диапазон, при необходимости ограничивая его. Необходимые коррекции вводятся для регулировки напряжения, мощности выходных сигналов, согласования с нагрузкой, выполнения измерительных и контролирующих функций параметров и характеристик.

Маскирующий сигнал формируют для энергетического подавления маскируемого сигнала. Предложен вариант формирования маскирующей помехи [4], основной принцип которого в том, что формируют шумовой сигнал, из которого формируют маскирующий сигнал, шумовой и маскирующий сигналы суммируют. Для формирования маскирующего сигнала сформированный шумовой сигнал усиливают и разделяют на n параллельных полос от $f_н$ до $f_{вi}$, где $i=\overline{1,n}$, причем каждая последующая полоса от $f_н$ до $f_{вi+1}$ шире всех предыдущих полос $(f_н \div f_{в1}) < (f_н \div f_{в2}) < ... < (f_н \div f_{вi})$.

Усиливают сигнал каждой полосы. Затем сигнал каждой полосы преобразуют в ХИП с различными случайными длительностями τ и случайными периодами. Полученные ХИП каждой полосы регулируют по амплитуде, суммируют ХИП всех полос, и сигнал полученной ХИП нормируют. В результате получают маскирующий сигнал, который суммируют с шумовым сигналом. Суммарный сигнал возводят в квадрат по амплитуде, в результате получают шумовую помеху. Данную шумовую помеху суммируют с другой шумовой помехой, сформированной аналогичным образом, сумму сигналов усиливают, согласуют с нагрузкой, получая маскирующую помеху.

Системным подходом разработана модель защиты информации во взаимосвязи с помехозащищенностью и помехоустойчивостью. Помехозащищенность в НЧ-диапазоне частот оценивают сформированным стабильным шумовым сигналом с помощью колец Гельмгольца. На основании помехоустойчивости оптимальным приемником устанавливают меру защиты речевой информации научно-обоснованным численным значением показателя разборчивости речи. Требования научно-методических документов реализует полноту оценки защищенности ОИ.

ЛИТЕРАТУРА

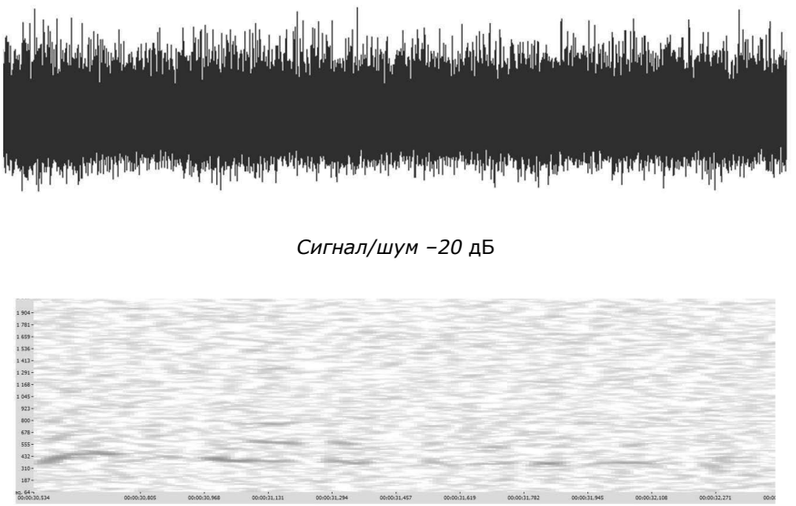
1. *Тузов Г. И.* Помехоустойчивость систем со сложными сигналами / Г. И. Тузов, В. А. Сивов, В. И. Прытков, Ю. Ф. Урядников, Ю. А. Дергачев, А. А. Сулиманов; под. ред. Г. И. Тузова. — М.: Радио и связь. 1985. — 264 с.
2. Магнитные измерения / Е. Т. Чернышев, Н. Т. Чернышева, Е. Н. Чечурина, Н. В. Студенцов, Н. В. Хорев и др. — М.: Изд-во стандартов, 1969. — 248 с.
3. *Железняк В. К.* Защита информации от утечки по техническим каналам: учебное пособие. ГУАП. — СПб., 2006. —188 с.

4. Способ формирования сигнала для маскирования речевых сигналов, видеосигналов и сигналов передачи данных: пат. 19227 Респ. Беларусь, МПК H 04K 1/00, H 04K 3/00 /В. К. Железняк, Д. С. Рябенко; заявитель Полоц. гос. ун-т. — № a 20121293; заявл. 10.09.2012; опубл. 30.06.2015// Официальный бюл. / Нац. центр интеллектуал. собственности. — 2015. —№ 3 (104). — С. 115–116.

КОМБИНИРОВАННЫЕ МАСКИРУЮЩИЕ СИГНАЛЫ ДЛЯ УСТРОЙСТВ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ

Г. В. ДАВЫДОВ
П. П. МАЗУР
А. В. ПОТОПОВИЧ

Защита речевой информации, циркулирующей в акустическом виде в защищаемом помещении, в первую очередь определяется правильным выбором средств защиты и режимами их работы. Обеспечить высокую степень звукоизоляции помещений не всегда возможно. Как правило, происходит переоборудование существующих помещений, и дополнительное нанесение звукоизоляционных материалов потребует больших финансовых затрат. Ввиду этого наиболее целесообразно использование активных устройств защиты речевой информации. Использование в таких устройствах маскирующих речь сигналов в виде «белого» шума для помещений с низкими звукоизолирующими свойствами приводит к дискомфорту в защищаемых помещениях. Кроме того, даже при соотношениях речевой сигнал/«белый» шум в –20 дБ для полосы частот от 125 до 8000 Гц по сонограмме записи можно определить участки с наличием речевого сигнала, хотя при прослушивании записи это сделать весьма трудно. На рисунке 1 приведена реализация записи для соотношения речевой сигнал/«белый» шум в –20 дБ и для полосы частот от 125 до 2000 Гц и ее сонограмма. На сонограмме четко прослеживаются участки с наличием речевого сигнала в записи (видны участки с первой второй и третьей формантами речевого сигнала).



Сигнал/шум –20 дБ

Рис. 1. Реализация записи речь/шум и ее сонограмма.

Для исключения указанного недостатка предлагается использовать комбинированные маскирующие сигналы включающие «белый» шум и речеподобные сигналы. Наиболее часто для защиты речевой информации используются маскирующие сигналы в виде «белого» или «розового» шумов, речеподобных сигналов (РПС), музыки или так называемых сигналов «речевой» коктейль. Весьма эффективным для защиты речевой информации являются комбинированные маскирующие сигналы, сформированные из «белого» шума и РПС. Речеподобные же сигналы рекомендуется формировать из базы аллофонов или дифонов диктора, речь которого требует наиболее высокой степени защиты.

В работе вопросы синтеза РПС рассматриваются для русского, белорусского и казахского языков с целью использования в системах защиты речи от несанкционированного прослушивания. Синтез таких сигналов для каждого языка требует учета его специфики. Компиляция участков естественной речи широко используется в системах синтеза речи и в системах тестирования линий связи. Однако, для русского, белорусского и казахского языков сведения о методах формирования РПС для защиты речевой информации и алгоритмах их реализации не разработаны.

При подготовке заданных текстов и создании речевых баз, учитывающих основные фонетические, лексические и грамматические особенности современных русского, белорусского и казахского языков может быть применена методика, основанная на создании РПС голосом диктора, речь которого необходимо защитить.

Помимо вышеуказанных этапов, весьма важным представляется выделение в языке так называемых «фонем» — таких звуковых единиц речи, которые имеют смыслоразличительное значение, так как в потоке речи в силу разных обстоятельств можно получать тот или иной оттенок (варианты фонем). При создании речевых баз русского, белорусского и казахского языков необходимо также понимание работы речевого аппарата, который принимает участие в создании звуков.

Для создания базы аллофонов необходимо было из слитной выделить необходимые аллофоны, путем сегментации речи. Анализ методов сегментации речевых сигналов на элементы речи (фразы, слова, аллофоны, периоды основного тона вокализованных участков речи) показывает, что наиболее часто для систем распознавания речи используются методы сегментации на базе скрытых марковских моделей и гибридные схемы, а для задач синтеза речи и формирования баз аллофонов — метод динамического программирования. Проведенный анализ точности сегментации речевого сигнала с использованием вектора признаков, состоящего из усредненного амплитудного спектра, оценки вокализованности речевого сигнала (меры тона) и их усредненных конечных разностей. Наиболее распространенными методами, использующими априорную информацию о сегментируемом сигнале, являются метод динамического программирования и метод сегментации, базирующийся на использовании скрытых марковских моделей. При сегментации речи на аллофоны основными этапами были определение кривой частоты основного тона, коррекция кривой частоты основного тона, сегментация речевого сигнала на периоды основного тона и далее выделение аллофонов.

Алгоритмы формирования маскирующих сигналов для систем защиты речевой информации включают алгоритмы формирования различных видов шумов и алгоритмы формирования сигналов похожих на речевые т.е. РПС.

РПС в виде диалога, имеющие вероятностный характер, могут применяться в качестве маскирующих сигналов в системах защиты информации от утечки по акустическим каналам и системах охранной и пожарной сигнализации для зашумления каналов связи с уровнями меньше пороговых, чтобы не нарушать режимы работы сигнализации.

Использование диалоговой формы РПС позволяет маскировать речевые сообщения дикторов, участвующих в диалоге. При этом в диалоге могут участвовать дикторы с речевыми сообщениями на разных языках, поэтому в работе будут использоваться базы аллофонов русского, белорусского и казахского языков, чтобы сформировать РПС сигналы на этих языках.

При любом способе синтеза РПС отправным пунктом является использование характеристик естественной речи на выбранном языке. РПС целесообразно придать сходство с каким-то образом препарированными акустическими сигналами речевого обмена. Для достижения таких качеств РПС следует формировать с учетом следующих признаков естественного диалога таких, как:

- чередование акустических сигналов речи участников диалога (одновременная их речь является нехарактерным кратковременным и редким режимом — например, при восклицаниях и репликах одного из участников диалога во время речи его партнера);
- определенная цельность, общая согласованность звукового рисунка совокупного речевого сигнала, соответствие этого рисунка распространенным ситуациям типа «вопрос — ответ», «обмен мнениями», «суждение — согласие (не согласие)» и т.п.;
- взаимосвязь темпа и громкости речи участников диалога;
- определенная согласованность интонационных и эмоциональных характеристик речи собеседников и др.

В этих условиях помимо синтезаторов речи участников диалога — программных или аппаратных — необходима головная программа или устройство, управляющие совместной работой этих синтезаторов. Управление с необходимостью распадется как на управление взаимодействием синтезаторов, так и на управление каждым из них в отдельности. Для синтеза РПС в диалоговой форме целесообразно использовать просодические параметры естественных речевых сигналов. Синтез РПС в диалоговой форме существенно более сложен, нежели формирование РПС одного абонента.

По количеству участников общения речь делится на монолог, диалог и полилог. Одной из форм полилога является деловая беседа, которой присущи следующие характерные особенности:

- дифференцированный подход с учетом коммуникативной цели;
- быстрота реагирования на высказывания;
- критическая оценка мнений, предложений и возражений;
- аналитический подход к учету и оценке всех факторов проблемы;

Переговоры по многим характеристикам сходны с деловой беседой.

Поэтому при разработке синтеза РПС диалоговой формы необходимо по возможности учитывать особенности естественного диалога в самых различных аспектах — лингвистическом, семантическом, синтаксическом и фонетическом.

В связи со сказанным, безусловно, целесообразным является использование общих характеристик диалоговой и монологовой речи, выявленных и устоявшихся, в частности, в лингвистических исследованиях.

Модель диалога может подразумевать использование различных голосов и различных групп слов. Библиотека моделей диалога, так же содержит сведения о том, как долго может продолжаться такой тип диалога и как долго в таком типе диалога может продолжаться речь одного человека. Например, тип диалога доклад может продолжаться до нескольких часов. Распространенные отчеты одного человека могут длиться до нескольких десятков минут, а вопросы, задаваемые докладчику, могут длиться до нескольких минут.

Все статистические данные, полученные из библиотек, объединяются в едином управляющем блоке. Который по заданным значениям задает синтезатору текста сгенерировать определенное число слов, с определенной орфографической нагрузкой, а синтезатору речи проговорить синтезированный текст определенным голосом.

После того, как текст, прочитан одним диктором, происходит вероятностная смена диктора, типа следующего предложения или вообще происходит смена вида диалога.

РПС предложено было использовать в виде диалога участников переговоров на трех языках русском, белорусском и казахском. Сценарии диалога могут быть следующие: говорит один из трех участников диалога в определенной последовательности, сменяя друг друга; говорит один из участников диалога и реплику вставляет другой участник диалога или одновременно говорят два участника диалога; одновременно говорят три участника диалога.

С учетом языка участника диалога число возможных сценариев диалога определится

$$C_3 = C_3^1 + C_3^2 + C_3^3 = 7,$$

где C_3 — число возможных сценариев диалога из трех человек; C_3^1 — число сочетаний один из трех; C_3^2 — число сочетаний два из трех; C_3^3 — число сочетаний три из трех.

В случае, когда участников диалога 6 человек, по 2 представителя (мужчина и женщина) для каждого из трех языков, число сценариев диалога определится

$$C_6 = C_6^1 + C_6^2 + C_6^3 = 41,$$

где C_6 — число возможных сценариев диалога из шести человек; C_6^1 — число сочетаний один из шести; C_6^2 — число сочетаний два из шести; C_6^3 — число сочетаний три из шести.

Распределения вероятностей сценариев по количеству одновременно говорящих, и длительностях такого сценария представлены в таблице 1.

Таблица 1.

Распределения вероятностей сценариев по количеству одновременно говорящих, и длительностях сценариев

Вид сценария	Распределение вероятностей % для сценариев	Распределение вероятностей % для длительностей диалога в мин.									
		5	4	3	2	1	0,5	0,4	0,3	0,2	0,1
C_n^1	89	23	17	15	12	8	6	5	4	3	2
C_n^2	8	-	-	-	-	6	14	20	30	20	10
C_n^3	3	-	-	-	-	-	6	19	35	25	15

Распределение вероятностей выбора дикторов для каждого из сценариев подчинено требованию равной вероятности. Например, для сценария C_6^1, когда в диалоге участвует один из шести, то вероятность того, что будет выбран именно этот участник диалога, равна 100/6 %.

Заключение

Защиту речевой информации от утечки по акустическим каналам можно обеспечить используя пассивные методы путем увеличения звукоизоляции ограждающих конструкций помещения и за счет использования активных методов защиты, основанных на

формировании маскирующих сигналов и возбуждении в акустических каналах утечки речевой информации акустических помех маскирующими сигналами.

Метод формирования маскирующих сигналов должен быть основан на следующих положениях. Маскирующие речь сигналы должны состоять из «белого» шума и РПС. РПС следует формировать с использованием вероятностных характеристик белорусской, русской и казахской речи. Это вероятности появления фонем в каждом из языков, длины слов, длины предложений, длины фоноабзацев и длины синтагм.

ПРИМЕНЕНИЕ ЗАЩИЩЕННЫХ КОМПЬЮТЕРОВ MKT-CARD LONG В СИСТЕМАХ УДАЛЕННОГО ДОСТУПА СМЕШАННОГО ТИПА

С. В. КОНЯВСКАЯ

В своих статьях и выступлениях мы неоднократно поднимали вопрос о защите систем удаленного доступа, в которых применяется «зоопарк» разнообразных клиентских устройств. Так, семинар, посвященный одному из аспектов этого вопроса — аттестации такой разнородной системы [1] — оказался самым востребованным на ТБ-Форуме-2016.

Однако жизнь все чаще сталкивает нас с обратной проблемой — необходимостью обеспечить работоспособность и защищенность системы, построенной на большом разнообразии не технических средств, а инфраструктурных решений. Системы все чаще совмещают в себе терминальный доступ, VDI и web, причем, рабочие места пользователей соседствуют с участками автоматической обработки данных, к одним и тем же файловым серверам обращаются компоненты разных (в том числе по уровню защищенности) систем, а клиентские СВТ применяются одновременно в двух и более контурах, которые должны, по-хорошему, быть строго изолированными один от другого.

Истоки такой ситуации нам всем хорошо понятны, поскольку мы работаем в одних и тех же реалиях. Обобщить их можно так: информационные системы складываются исторически.

Зачастую изначально они проектируются и какое-то время соответствуют современному уровню развития науки и техники. Затем осуществляется модернизация. Часто она вообще проходит незаметно — на уровне локальных улучшений системы управления, например. В той или иной специализированной подсистеме удобно осуществлять функции мониторинга через web-интерфейс — почему не ввести в нее такой модуль?

Потом наступает время более глобальной модернизации — технологии унеслись далеко вперед. Но имеющихся на модернизацию денег не достаточно на коренное **перепроектирование**, а достаточно (опять же, в хорошем случае) только на приобретение новых инфраструктурных элементов и технических средств. Например, на внедрение виртуальной инфраструктуры с целью централизации вычислений за счет виртуализации терминальных серверов и серверов обработки данных. Приобретенное (скорее всего, ПО и серверы, но, возможно, и средства защиты) встраиваются в систему настолько успешно, насколько хватает квалификации и энтузиазма у управляющего персонала системы и подрядчика. К счастью, человеческий фактор — это не всегда плохо, и системы продолжают работать и даже иногда начинают работать более эффективно.

И вот однажды необходимо включить в состав технологического процесса новую операцию, предположим, работу с электронной подписью (ЭП) в системе внутреннего электронного документооборота. Выбранное по тем или иным причинам средство электронной подписи (СЭП) принципиально удовлетворяет проектным характеристикам системы (поддерживает работу в терминальном режиме, имеет сертификат, поддерживает нужную систему управления ключами), для его применения необходимо только добавить в систему какой-то инфраструктурный элемент. Допустим, средство защиты канала. Мелочь. Но оно, в свою очередь, требует работы с другим протоколом обмена данными. Тоже не беда, протоколы-то стандартные. Вырастает нагрузка на канал — ну, в общем, тоже дело житейское — можно расширить каналы. Хуже, если начинает требоваться изменение версии ОС. Совсем незначительное — не замена на ОС другого семейства, а всего лишь другая версия. И вот с этой версией как раз перестает работать функциональное ПО, выполняющее целевую функцию системы. Не говоря уже о том, что система электронного документооборота (СЭДО) оказывается готова ко встраиванию СКЗИ, но не готова к выполнению требований к СЭП, и начинается выяснение границ ответственности — на чьей стороне, например, визуализация? СЭП или СЭДО? За счет свойств ключевого носителя или системы управления ключами лучше снижать нагрузку на персонал? И еще очень много аналогичных вопросов.

Как правило именно в этот момент эксплуатирующая организация задумывается о том, что что-то пошло не так, а подрядчик, выполняющий модернизацию, должен разрешить клубок проблем, возникших из-за исторически сложившейся цепочки логичных решений, часто совершенно не связанных между собою.

Абсолютно очевидно, что не имеет смысла рассказывать, как сделать, чтобы так не получалось — это всем хорошо известно: нужно все время проектировать. Но жизнь складывается тем не менее именно так, а не иначе.

Поэтому просто разберем возможное направление облегчения ситуации на примере условной системы удаленного доступа смешанного типа.

Пускай наша система совмещает в себе следующие инфраструктурные решения и технические средства:

1. физические серверы, часть из которых является ESXi-серверами, часть — терминальными серверами, часть — серверами приложений, часть — файловыми серверами, часть — серверами обработки данных, возможно еще есть какие-нибудь серверы безопасности и/или обновлений.
2. виртуальные серверы, среди которых те же терминальные серверы, серверы приложений, файловые серверы и серверы обработки данных (как правило так бывает тогда, когда систему начали «виртуализировать», но процесс растянулся по различным причинам на годы), и еще — серверы управления виртуальной инфраструктурой.
3. инфраструктура виртуализации — VMware.
4. отдельные функции управления системой реализованы в виде web-сервисов.
5. целевое функциональное ПО пользовательского сегмента информационной системы работает в терминальном режиме в среде Windows (на терминальных серверах — Windows).
6. терминальное ПО — Microsoft и Citrix.
7. два контура с разными уровнями защищенности (общедоступно и информация ограниченного доступа).

8. основным способом загрузки ОС терминальных клиентов является сетевой, но отдельные клиенты загружаются локально по причине плохих каналов в территориально удаленных подразделениях.
9. система ЭДО включает в себя механизмы ЭП, реализованные каким-то определенным СКЗИ.
10. в системе используются аппаратные идентификаторы пользователей и ключевые носители на базе USB-устройств и таблеток Touch Memory.
11. в системе контролируется применение флеш-носителей (есть определенные правила и ограничения, однако в целом они применяются).
12. и так далее, каждый интегратор и большинство эксплуатирующих организаций способны продолжить этот список новыми и новыми деталями без ущерба для правдоподобности общей картины.

Очевидно, что причин для тревог за работоспособность и защищенность такой системы — более чем достаточно, и утверждение, что снизить накал напряженности можно за счет использования определенного клиентского устройства в качестве основного — звучит малоубедительно.

Попробуем все же рискнуть.

Если обобщить до схематичности, то проблема такой «естественной» системы в том, что она развивается из специализированной в универсальную, а это процесс довольно противоестественный.

Изначально корректно спроектированная система «заточена» на оптимальное (то есть с максимальной эффективностью при минимальных затратах и сложностях управления) решение конкретных, ясно описанных в проекте задач.

Для решения ясно описанного круга задач во всех без исключения случаях лучше использовать специальные, а не универсальные средства. Этот тезис подробно раскрыт в [2–5].

Затем «жизнь вносит коррективы» **в систему, но не в проект**, и от специальных средств требуются все новые несвойственные им функции. Рассмотрим на примере средств защищенной сетевой загрузки ПО терминальных станций. Идея применения таких средств состоит в том, что от тонкого клиента не требуется ничего, кроме поддержки периферии, и/а пользователя, контролируемой целостности и аутентичности, журналирования и управляемости (то есть возможности контролируемой модификации в соответствии с изменениями ситуации со стороны удаленного аутентифицированного администратора). При этом защищенность становится, по сути, основной характеристикой технологии, так как с точки зрения состава, а тем более «удобства» такого загружаемого образа требования минимальны — пользователь с ним практически не имеет никаких дел, он работает с терминальным сервером уже после того, как средство защищенной сетевой загрузки закончило свою работу.

Однако увеличим постепенно число поддерживаемых чипсетов до нескольких десятков, расширим парк периферии (ведь каждый год начинает выпускаться много новых мониторов все лучшего качества), сделаем смешанной подсистему печати (введем и сетевые, и локальные принтеры, любой сотрудник скажет, что ему удобнее иметь принтер на своем столе, а не ходить к сетевому), добавим клиент VPN, поддержку разнообразных идентификаторов и ключевых носителей, а затем еще встроим клиента СЭП, чтобы выработка ЭП производилась корректно на стороне клиента, и загружаемый по сети образ станет полноценной операционной системой. Это неплохо, но он будет, скажем, довольно объемным — особенно для загрузки по каналам связи низкой пропускной способности.

То же касается всех технологий, нацеленных на специализацию системы, но развиваемых в сторону ее универсализации.

Протокол передачи данных, оптимизирующий передаваемые данные для минимизации нагрузки на канал, теряет все свои преимущества при попытке шифрования трафика. Также в этом случае теряют эффективность и специальные «компрессоры». Шифртекст не сжимается.

Примеры можно умножать.

Очевидно главное — чем более размывается контур круга задач системы, тем менее эффективными становятся специализированные технические средства и решения.

Казалось бы, выход очевиден — необходимо ставит универсальные ПЭВМ, защищать их универсальными ПАК СЗИ НСД (разумеется, семейства «Аккорд»), а также антивирусами, средствами межсетевого экранирования, шифрования трафика и всем остальным. Тем самым создадим среду функционирования криптографии (СФК) и решим все задачи. Кроме, разве что управляемости системы. И стоимости владения. И удобства обновления. И потери всех выгод от виртуализации и от терминального доступа. И… многого еще. В общем, необходимо признать, что это решение плохое, хотя нам, как производителям «Аккордов», довольно выгодное.

Видимо, необходимо найти ту грань универсальности и специализированности, которая позволит удовлетворить разросшимся требованиям системы, не вставая на экстенсивный путь бессмысленного наращивания ресурсов (использование техники все большей мощности со все более избыточной функциональностью, требующей обслуживания все большим штатом высококвалифицированного персонала).

Как ни удивительно, но именно подсистема защиты информации, которая, казалось бы, должна вносить в описанный хаос свою существенную лепту, может стать элементом, объединяющим все это в единое целое. И получится это как раз в том случае, если клиентские СВТ будут частью этой подсистемы, делая ее, тем самым фузионной, а не агглютинативной[1].

Защищенные терминалы, о которых пойдет речь, — это МКТ-card long, отечественные инновационные микрокомпьютеры с динамически изменяемой архитектурой, запатентованной под названием «Новая Гарвардская».

Архитектура описана в [8–13], а линейка микрокомпьютеров на ее основе в [14].

Для разрешения описанной ситуации мы предлагаем выбрать именно модель МКТ-card long потому, что ее форм-фактор (док-станция с отчуждаемым компьютером) оптимален для использования на стационарно расположенных рабочих местах.

В отличие от микрокомпьютеров в форм-факторе донглов, к которым необходимо каждый раз подключать всю периферию, в кабинетах на столах сотрудников будут оставаться док-станции с подключенными мониторами, клавиатурами, мышами, считывателями

---

[1] Агглютинация и фузия — это два способа построения слов в разных языках. Агглютинация — это механическое присоединения нового члена (форманта) с одним единственным значением (например, только множественность, или только мужской род, или только притяжательность) при каждом наращении смысла. Пример агглютинации в татарском: «в его письмах» хатларында (хат «письмо», -лар- формант множественного числа, -ын- притяжательный формант 3-го лица, -да формант местного падежа). Фузия же — это способ построения слов и форм, при котором один суффикс, например, может выражать сразу целую совокупность значений, а соединение частей слово происходит так, что не всегда легко провести точную границу. Например, слово «плачет»: корень «плак-» в месте присоединения суффикса (означающего *одновременно* и ед. ч., и 3 лицо, и настоящее время) — изменился: претерпел чередование к\ч (из-за влияния гласного переднего ряда на заднеязычный согласный).

Как правило, в языках наблюдаются оба способа, но один какой-нибудь преобладает. Интересно, что искусственные языки всегда агглютинативные. Среди естественных чисто агглютинативных языков: тюркские, некоторые финно-угорские, монгольские, тунгусо-маньчжурские, корейский, японский, грузинский, баскский, абхазо-адыгские, дравидийские, часть индейских и некоторые африканские.

ключевой информации и всем остальным, и на включение такого рабочего места будет уходить не больше времени, чем на запуск обыкновенного компьютера.

В образ операционной системы МКТ-card long интегрирована клиентская часть ПАК «Аккорд», общая для комплексов защиты физических и виртуальных инфраструктур (ПАК СЗИ НСД Аккорд-Win32 TSE / Аккорд-Win64 TSE, и ПАК СЗИ НСД Аккорд-В.), так что один и тот же терминал сможет работать с физическими и виртуальными терминальными серверами без внесения изменений в систему защиту или конфигурацию ОС. Таким образом исключаются сложности *по пунктам 1 и 2*.

Для корректной с виртуальными рабочими столами в образ ОС терминала встроен VMware View Client, тем самым сняты возможные конфликты *по пункту 3*.

Для защищенной работы с web-сервисами в ОС МКТ-card long встраивается браузер и межсетевой экран, который не позволит пользователю отвлечься на посторонние задачи, пользуясь наличием Интернет-соединения на рабочем месте. Таким образом, *пункт 4* также не вызовет проблем.

Наличие клиентов ICA и RDP исключают сложности, потенциально связанные *с пунктами 5 и 6*.

Задачу работы в двух контурах защиты (*пункт 7*) с использованием микрокомпьютеров семейства МКТ можно решить несколькими разными способами. Опишем те из них, которые не требуют использования никаких дополнительных инфраструктурных решений типа «брокеров» или аналогичных.

Очевидно, что основа у этих способов общая — работа в разных контурах будет изолирована в том случае, если соединение с серверной частью производится из разных ОС. Соответственно, мы можем:

1. использовать модификацию TrusT (компьютер в этом случае будет содержать физический переключатель и называться МКTrusT-card long). У этой модификации в разных физических банках памяти находятся две разные ОС. Запуск одной или второй ОС определяется положением физического переключателя. Этот механизм абсолютно надежен, поскольку перевести переключатель в другое положение может только пользователь, загружающий компьютер, а никак не вирус или хакер. Итак, **при одном положении переключателя запускается ОС, например, с ICA клиентом, который инициирует сессию с терминальным серверов в общедоступном контуре, а при втором положении переключателя — загружается ОС с, допустим, VMware View Client, соединяющимся с защищенным виртуальным рабочим столом**. Или как-угодно иначе. Главное, что из одной ОС можно попасть только в один контур, а из второй — только в другой.
2. при использовании стандартной комплектации МКТ-card long обеспечить две различные среды для доступа в разные контуры можно следующим образом. В общем случае, поскольку ОС в компьютерах МКТ неизменяемая (она находится в банке памяти, физически переведенном в режим Read Only), то параметры доступа хранятся на внутренней SD-карте. Однако помимо получения этих параметров с SD-карты, можно получать их (и какое-либо дополнительное ПО в случае необходимости) с сервера по сети.

В модификации «МКТ-card long для двойного применения» реализованы оба эти варианта одновременно, и **в процессе загрузки пользователь может выбрать, откуда получить конфигурационную информацию, и в зависимости от этого выбора попасть в один или в другой контур**.

В таком решении совмещены функции комплекса защищенной сетевой загрузки ПО терминальных станций «Центр-Т» и стандартные функции МКТ-card long. Такое совмещение удобно еще и тем, что микрокомпьютеры в этом случае можно использовать внутри уже имеющейся в организации инфраструктуры «Центра-Т», то есть используя Серверы хранения и сетевой загрузки этого комплекса, без разворачивания новых.

Наиболее логичным видится доступ в контур ограниченного доступа с помощью загружаемых по сети конфигураций, и доступ в общедоступный контур с конфигурациями на SD-карточке (потому что это позволит более гибко и оперативно управлять настройками доступа именно в более тщательно защищаемый контур). Хотя можно поступить и наоборот — зависит это скорее от желательного порядка администрирования этих конфигураций, чем от соображений безопасности.

Таким образом, помимо потенциально проблемного *пункта 7*, выполняется и условие *пункта 8*.

Ну и, конечно, неверно было бы списывать со счетов естественный способ, порождаемый самой архитектурой решения — док-станция и отчуждаемый ПК. Док-станции и ПК в общем случае инварианты один к другому, то есть любой ПК можно подключить к любой док-станции той же модели. А значит, доступ в разные контуры можно получать, просто подключая к своей док-станции разные компьютеры.

Пункт 9 — включение в технологию обработки электронных документов выработки и проверки ЭП — имеет огромное количество нюансов, связанных с особенностями деятельности организации, особенности документов, которые должны таким образом обрабатываться, и очень многого еще. Если нарисовать предельно обезличенную схему, то она, с учетом обрисованных условий, может выглядеть, например, примерно так: документы формируются на терминальных серверах и должны быть подписаны операторами терминалов, при этом работа должна производиться с учетом требований Федерального закона Российской Федерации от 06.04.2011 N 63-ФЗ «Об электронной подписи» (далее — 63-ФЗ) [15] и Требований к средствам электронной подписи (Приложение № 1 к приказу ФСБ России от 27 декабря 2011 г. № 796) (далее — Требования) [16].

С применением защищенного терминала МКТ-card long это может быть реализовано, например, так:

1. Документ формируется на терминальном сервере.
2. Когда его должен подписать оператор терминала, документ передается с терминального сервера на терминальный клиент.
3. В целях контроля целостности документа при передаче по каналу, перед отправкой на терминал он подписывается СКЗИ на ключе сервера в автоматическом режиме (статья 4 63-ФЗ[1]).
4. На терминале подпись проверяется резидентным СКЗИ терминала.
5. В случае подтверждения целостности, документ визуализируется (часть 2 статьи 12 63-ФЗ[2]).
6. Оператор должен сознательным действием подтвердить корректность отображенного документа (часть 2 статьи 12 63-ФЗ).
7. Подтверждение оператора является сигналом для вычисления хеш-функции от документа резидентным СКЗИ терминала. Далее тем же резидентным СКЗИ, или отчуждаемым персональным СКЗИ (токеном) вычисляется ЭП (п. 15 Требований[3]).
8. После подписания документ снова визуализируется на терминале (часть 2 статьи 12 63-ФЗ).

Подтверждение оператора является сигналом для отправки подписанного документа на сервер.

---

[1] Статья 4 ФЗ-63 «Принципами использования электронной подписи являются: недопустимость признания электронной подписи и (или) подписанного ею электронного документа не имеющими юридической силы только на основании того, что такая электронная подпись создана не собственноручно, а с использованием средств электронной подписи для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе».

[2] Часть 2 статьи 12 ФЗ-63: «При создании электронной подписи средства электронной подписи должны:

1) показывать лицу, подписывающему электронный документ, содержание информации, которую он подписывает;

2) создавать электронную подпись только после подтверждения лицом, подписывающим электронный документ, операции по созданию электронной подписи;

3) однозначно показывать, что электронная подпись создана».

[3] П. 15 Требований: «Средства ЭП класса КС3 противостоят атакам, при создании способов, подготовке и проведении которых используются возможности...: ... доступ к СВТ, на которых реализованы средство ЭП и СФ»

Идентификаторам и ключевым носителям в нашем описании условной системы посвящен отдельный пункт, однако именно в контексте ЭП имеет смысл заметить, что в случае актуальности угрозы использования подложного СВТ в качестве терминального клиента необходимо чтобы применяемый токен имел механизмы различения разрешенных и неразрешенных для работы с ключами СВТ (пункт 31 Требований[1]). Такое устройство — «Идеальный токен» [17–20] — поддерживается МКТ-card long.

Очевидно, что факторами, определяющими реализуемость данной схемы (как и любой другой разумной схемы встраивания в технологию ЭДО механизмов ЭП) на микрокомпьютерах семейства МКТ, являются с одной стороны, доверенная среда, обеспечиваемая технологически, и с другой, — их вычислительные характеристики, достаточные для вычисления и проверки ЭП резидентным СКЗИ и корректной визуализации документа[2].

На данный момент есть опыт встраивания всех наиболее распространенных отечественных СКЗИ.

В части идентификаторов и ключевых носителей (*пункт 10*) первоочередное значение имеет сложившаяся в системе практика применения, поскольку это как раз та мелочь, которой в системе настолько много, и замена которой настолько трудоемка, что необходимость такой замены, особенно единовременной, может стать решающим противопоказанием для приобретения новых СВТ или системы защиты. Если использование даже очень удачного во всех отношениях пользовательского терминала потребует перерегистрации всех пользователей во всех подсистемах, требующих предъявления идентификатора, или даже просто дополнительной регистрации еще N идентификаторов (особенно если N — трехзначное и выше число), то любой владелец системы взвесит трудозатраты на эту процедуру. Что уж говорить о ключевых носителях — во многих организациях выпуск ключей является абсолютно сакральной процедурой.

Имея в виду эту особенность, мы предусмотрели в МКТ-card long целый ряд возможностей.

Во-первых, сам отчуждаемый компьютер из состава МКТ-card long удовлетворяет всем признакам персонального аппаратного идентификатора и ключевого носителя. Он отчуждаемый, персональный, безусловно аппаратный и защищенный. Он может выполнять функции идентификатора пользователя в СЗИ НСД семейства «Аккорд» и защищенного ключевого носителя.

Такое хранение и аутентифицирующей, и ключевой информации является заметно более правильным с точки зрения защиты информации по следующим причинам. При идентификации с помощью компьютера, пользователь подтверждает не только то, что подключается к системе именно он, но и то, что он это делает именно со своего законного рабочего места, а не со специально подготовленного надлежащим образом ноутбука, например, просто используя свой легальный идентификатор. Это позволит блокировать значительное число уязвимостей, связанных с так называемым BYOD, что на самом деле зачастую является неконтролируемым размыванием защищенного контура.

---

[1] П. 31 Требований: «В состав средств ЭП классов КС3 должны входить компоненты, обеспечивающие: ... управление доступом субъектов к различным компонентам и (или) целевым функциям средства ЭП и СФ на основе параметров, заданных администратором или производителем средства ЭП ...».

[2] *Параметры компьютера:* Процессор 4-ядерный, 1,6 ГГц, Cortex A9; Графический процессор Mali400, 2D/ 3D OpenGL ES2.0/ OpenVG1.1; ОЗУ 2GB DRR3; WiFi IEEE 802.11 b/g/n; Bluetooth V4.2; Считыватель карт MICRO SD (TF card) до 32GB; Размер защищенного диска 8 ГБ.

Параметры док-станции: Порт HDMI: 2, Порт USB: 8 (host) + 1 (slave), Порт Ethernet, Порт питания: 1 DC 4.0mm, Питание: DC 5V, 2A.

В плане работы с ключами все еще более очевидно, ведь даже храня ключи на так называемом «токене», можно скомпрометировать их, подключив токен не к защищенному рабочему месту, а к какому-либо незащищенному компьютеру, на котором уже есть какой-нибудь ворующий ключи троян. Так же, как и в предыдущем случае, пользователь может действовать из лучших побуждений, например, желая поработать сверхурочно на домашнем компьютере, но при этом он сведет на нет усилия по защите информации в целой системе.

Заметим, что для укрепления метафорического смысла термина «ключ» — пропорции отчуждаемого компьютера таковы, что он помещается в стандартный пенал для ключей и может сдаваться под охрану в конце рабочего дня.

В случае если такое применение для эксплуатирующей организации привлекательно, перерегистрация идентификаторов и перезапись ключей можно производить постепенно, в плановом порядке, а в переходном периоде продолжать использовать уже введенные в эксплуатацию устройства — за эту возможность отвечает пункт «во-вторых» (ниже).

Во-вторых, в MKT-card long реализована поддержка наиболее распространенных типов идентификаторов (список расширяемый, поскольку образ ОС формируется для каждой конкретной системы отдельно) и ключевых носителей, работающих по стандартному протоколу CCID.

Особенностью политики работы с идентификаторами и ключевыми носителями в отдельных организациях бывает запрет на использование одного и того же устройства одновременно в обоих качествах. Даже если и в качестве носителя ключа, и в качестве идентификаторов используются, допустим, TM-идентификаторы, или USB-ключи, или смарт-карты — использовать *одно и то же* устройство для того, чтобы хранить данные для и/а и ключи с сертификатами — нельзя. В таких случаях, конечно, как бы ни было удобно идентифицироваться с помощью своего же рабочего места, и на нем же носить свои ключи, придется использовать отдельный ключевой носитель как минимум.

Учитывая описанные выше опасности, связанные с применениями ключевых носителей на несанкционированных компьютерах, мы рекомендуем — «Идеальный токен», который подключается только к заранее разрешенным администраторам рабочим местам.

Наконец, остался последний из выделенных в начале пунктов — *11-й пункт*: флешки.

До сих пор все средства защиты информации, нацеленные на контроль использования подключаемых устройств представляли собой некоторое ПО, устанавливаемое на сервер (или в ОС автономного ПК). Это были или модули в составе монитора разграничения доступа (такой модуль есть и в СПО «Аккорд»), или специальное ПО, предназначенное для контроля подключаемых устройств, типа Device Lock. Такие средства вполне

могут функционировать и в серверной части в описанной нами системы. Однако все, кто пытался решить задачу контролируемого использования флешек в организации знает, что этого не достаточно, и что необходимо не только применять флешки внутри защищенного контура по определенным правилам, но и исключить их применение за пределами контура, иначе все предпринятые усилия никак не помешают ни вынести информацию наружу, ни привнести вредоносное ПО извне.

Для комплексного решения этой задачи необходимо использовать флешки на базе защищенных служебных носителей. Работа с такими флешками — линейки «Секрет» [21] (а именно — «Секрет Особого Назначения») — в режиме терминальной сессии поддержана в МКТ-card long уже сегодня, а локальная работа с ними в собственной ОС терминала — дело ближайшего будущего: выход версии «Секрета Особого Назначения» для Linux запланирован на второе полугодие 2016 года.

Есть еще одна особенность нашей условной системы, которая не была вынесена в отдельный пункт, поскольку не является архитектурной, но явно заметна по сюжету. Это подверженность системы частым модернизациям по различным причинам.

Эта особенность важна для нас потому, что, казалось бы, находится в некотором противоречии с идеей зафиксированности и неизменности вычислительной среды, лежащей в основе линейки компьютеров МКТ. Противоречие это разрешено — для микрокомпьютеров реализована возможность обновления защищенной ОС. Если систему планируется модернизировать часто и радикально, — лучше заказывать МКТ-card long с поддержкой системы защищенных обновлений. В противном случае вносить изменения в его защищенную от перезаписи операционную систему будет все равно возможно, но только в сервисном центре.

Подведем итоги.

Мы рассмотрели систему, представляющую собой практически эталон предбарочной российской церковной архитектуры XVII века, когда за многочисленными пристроечками и новыми полезными элементами малореально рассмотреть изначальный замысел архитектора. Несомненно, так же, как и в архитектуре, в строительстве автоматизированных систем этот период тоже будет преодолен. Но преодолеть его хотелось бы минимально травматично и постараться при этом максимально сохранить инвестиции.

Защищенный терминал МКТ-card long представляется именно тем решением, которое будет одинаково эффективно и в «переходные периоды» модернизаций системы, и в периоды ее стабильных состояний.

СПИСОК ЛИТЕРАТУРЫ

1. *Конявская С. В., Рябов А. С., Лыдин С. С.* О том, почему не надо бояться «зоопарка» технических средств, или как самому себе аттестовать ИСПДн // Защита информации. Inside. СПб. 2015. № 5. С. 24–27.
2. *Конявский В. А.* Не надо оплачивать уязвимости // Аналитический банковский журнал. М., 2014. № 10 (222). С. 62–64.
3. *Конявский В. А.* Компьютер с вирусным иммунитетом // Информационные ресурсы России. 2015. № 6. С. 31–34.
4. *Конявская С. В.* Информатизация без нагрузки // Национальный банковский журнал. М., 2016. № 2 (февраль). С. 58–59.
5. *Конявский В. А.* Эпохе бурного развития — компьютер с динамической архитектурой // Национальный банковский журнал. М., 2016. № 3(март). С. 102–103.
6. *Реформатский А. А.* Лингвистика и поэтика. М., 1987. С. 52–76.

7. Компьютер типа «тонкий клиент» с аппаратной защитой данных: Патент на полезную модель № 118773. 27.07.12. Бюл. № 21.
8. Компьютер с аппаратной защитой данных от несанкционированного изменения: Патент на полезную модель № 137626. 20.02.2014. Бюл. № 5.
9. Мобильный компьютер с аппаратной защитой доверенной операционной системы: Патент на полезную модель № 138562. 20.03.2014. Бюл. № 8.
10. Мобильный компьютер с аппаратной защитой доверенной операционной системы от несанкционированных изменений: Патент на полезную модель № 139532. 20.04.2014. Бюл. № 11.
11. Мобильный компьютер с аппаратной защитой доверенной операционной системы: Патент на полезную модель № 147527. 10.11.2014. Бюл. № 31.
12. Мобильный компьютер с аппаратной защитой доверенной операционной системы от несанкционированных изменений: Патент на полезную модель № 151264. 27.03.2015. Бюл. № 9.
13. Рабочая станция с аппаратной защитой данных для компьютерных сетей с клиент-серверной или терминальной архитектурой: Патент на полезную модель № 153044. 27.06.2015. Бюл. № 18.
14. Trusted Cloud Computers [Электронный ресурс]. — URL: www.trustedcloudcomputers.ru.
15. Федеральный закон Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи».
16. Приказ ФСБ России от 27 декабря 2011 г. № 796. Приложение 1.
17. *Кравец В. В.* Идеальный токен // Комплексная защита информации. Материалы XX научно-практической конференции. Минск, 19–21 мая 2015 г. — Минск: РИВШ, 2015. С. 114–115.
18. *Ладынская Ю. П., Батраков А. Ю.* Хранение данных СКЗИ: выбор носителя // Информационная безопасность. Материалы XIII Международной конференции. Таганрог 2013. Часть. 1. С. 129–134.
19. *Бирюков К. А.* Средства безопасного хранения ключей // Безопасность информационных технологий. М., 2013. № 3. С. 50–53.
20. Съемный носитель ключевой и конфиденциальной информации. Патент на полезную модель № 147529. 10.11.2014, бюл. № 31.
21. Специальный съемный носитель информации. Патент на полезную модель № 94751. 27.05.2010, бюл. № 15.

ОЦЕНКА ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ, РАСПРОСТРАНЯЮЩЕЙСЯ ПО КАНАЛАМ С ЗАМИРАНИЯМИ НАКАГАМИ

В.А. ДМИТРИЕВ, А.Б. СТЕПАНЯН, Е.П. МАКСИМОВИЧ, В.К. ФИСЕНКО
ОИПИ НАН Беларуси

Передача информации в каналах связи, использующих свободное распространение сигнала, всегда сопровождается флуктуациями амплитуды сигнала. Случайные флуктуации амплитуды сигнала на входе приемника называются замираниями. В реальных условиях

при флуктуации амплитуд составляющих сигнала всегда наблюдаются и флуктуации фаз. Поэтому при наличии замираний фаза приходящего сигнала также является в той или иной степени неопределенной.

Каналом с замираниями будем называть такой канал, в котором амплитуды составляющих сигнала, приходящего к приемнику, подвержены флуктуациям. Физически в канале с замираниями обычно сигнал распространяется по нескольким путям. Если имеется большое число многократно отраженных лучей и отсутствует прямая видимость, огибающая полученного сигнала статистически описывается с помощью функции плотности вероятности Накагами

$$W_s\left(U_s\right)=\frac{2\cdot m^m\cdot U_s^{2m-1}}{\Gamma\left(m\right)\cdot\left(\sigma_s^2\right)^m}\cdot exp\left(-\frac{m\cdot U_s^2}{\sigma_s^2}\right), \tag{1}$$

где $m\geq\frac{1}{2}$ — глубина замирания, параметр, выражающий отношение средней мощности обнаруживаемого сигнала к дисперсии мгновенной мощности сигнала, σ_s^2 — дисперсия сигнала; $\Gamma\left(m\right)$ — гамма-функция.

Огибающая шума статистически описывается с помощью следующей функции плотности вероятности

$$W_n\left(U_n\right)=\frac{1}{\sqrt{2\cdot\pi\cdot\sigma_n^2}}\cdot exp\left(-\frac{U_n^2}{\sigma_n^2}\right), \tag{2}$$

где σ_n^2 — дисперсия шума.

Огибающая смеси сигнал + шум на входе приемника статистически описывается с помощью следующей функции плотности вероятности

$$W_{s+n}\left(U_{s+n}\right)=W_s\left(U_s\right)\cdot W_n\left(U_n\right). \tag{3}$$

При оптимальном приеме сигнала вероятность ошибочного приема (вероятность ложной тревоги) и вероятность правильного обнаружения определяются по формулам

$$P_{лт}=\int_h^{+\infty}W_n\left(U_n\right)dU_n, \tag{4}$$

$$P_o=\int_h^{+\infty}W_{s+n}\left(U_{s+n}\right)dU_{s+n}, \tag{5}$$

Систему обнаружения характеризуют средним риском, который определяет среднее значение ожидаемых потерь. Выбор оптимального решающего правила производится путем минимизации величины среднего риска.

Выбор порогового значения вероятности правильного обнаружения сигнала осуществляется с помощью минимизации вероятности полной ошибки, которая рассчитывается по формуле

$$P_{ош}=0,5\cdot\left(1-P_o+P_{лт}\right). \tag{6}$$

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Тихонов В. И.* Статистическая радиотехника / В. И. Тихонов. — М.: Радио и связь, 1982. — 624 с.
2. *Тихонов В. И.* Оптимальный прием сигналов / В. И. Тихонов. — М.: Радио и связь, 1983. — 320 с.

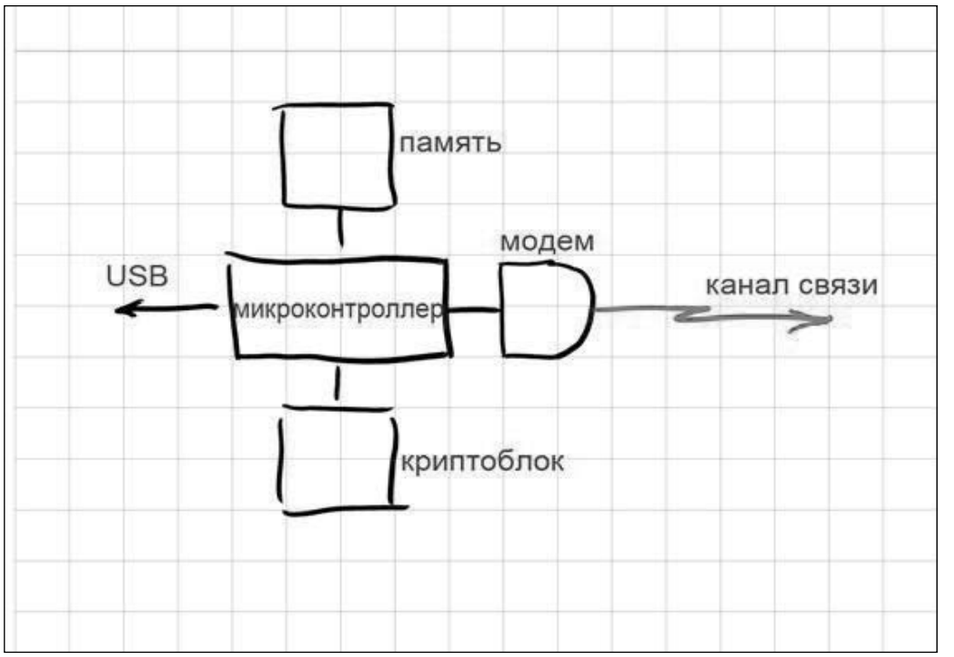
M&M!-ПЛАТФОРМА ДЛЯ ЗАЩИЩЕННЫХ МОБИЛЬНЫХ СИСТЕМ

Д. Ю. СЧАСТНЫЙ

В статье описываются варианты использования модема в устройстве M&M!(МАРШ! и модем) и приводятся примеры применения этого устройства в различных системах.

Ключевые слова: M&M!, МАРШ!, модем.

Идея устройства M&M! (МАРШ! и модем) была озвучена в середине 2012 года [1]. Кратко напомню суть: для обеспечения комфортной и в тоже время безопасной работы мобильных пользователей предлагалось в изделие МАРШ! добавить модем в качестве неотъемлемого аппаратного компонента. И схема устройства выглядела следующим образом:



Добавление модема позволило упростить использование СОДС МАРШ! (сетевые настройки резидентной ОС оставались постоянными и не требовали перенастройки при каждом сеансе работы) и обеспечить мобильность пользователей (так как устройство стало «независимо от провайдеров сети»). На тот момент обеспечение связи для СОДС МАРШ! казалось основным и единственным вариантом использования модема. Но

прошедшие четыре года показали, что мы ошибались. Добавление модема к микроконтроллеру, памяти, криптоблоку и usb-каналу привело к качественно новым возможностям использования устройства.

Во-первых, работа модема контролируется активным микроконтроллером и появляется возможность как управлять установлением сетевых соединений, так и осуществлять мониторинг всех данных, проходящих через устройство.

Во-вторых, наличие собственного криптоблока позволяет осуществлять различные криптографические преобразования проходящих через устройство данных, так и осуществлять взаимную криптографическую аутентификацию устройства и ответной стороны. Причем ключи могут храниться в устройстве и быть недоступными ни со стороны компьютера, ни со стороны сети.

В-третьих, микроконтроллер может самостоятельно устанавливать связь и осуществлять прием или передачу данных на заранее определенный сервер.

В-четвертых, наличие памяти, доступной как из компьютера, так и из устройства, позволяет обеспечивать передачу файлов данных в режиме почтового ящика: приложение в компьютере кладет файл данных в эту память как на обычный диск, а микроконтроллер передает этот файл на заранее определенный сервер.

Причем все вышеперечисленные функции осуществляются внутри устройства на собственном микроконтроллере без создания нагрузки на центральный процессор компьютера, к которому подключено устройство. Кроме того, код, исполняющийся внутри устройства, не подвержен несанкционированному изменению и не может быть заражен вирусами. Код пишется на Си, и для микроконтроллера разработаны высокоуровневые библиотеки для работы с модемом и прочей периферией.

Таким образом, устройство M&M! может быть использовано в качестве платформы для решения самых различных задач.

Например, сбор и передача параметров с различных датчиков в территориально-распределенных системах. Например, датчиков уровня паводковых вод. Или датчиков учета расхода тепла, газа или света. Подобные датчики установлены во множестве мест, в том числе труднодоступных, и тогда сбор параметров превращается в продолжительный процесс. Естественным выходом является модификация датчиков с тем, чтобы они могли самостоятельно передавать данные. Можно переразводить плату, добавлять туда модем, встраивать систему защиты, переписывать код. А можно использовать M&M! в режиме работы почтового ящика, подключив его к датчику по usb-каналу, и незначительно модифицировать код. Похожим образом можно использовать M&M! и в фискальных целях, соединив с кассовыми аппаратами и добавив функцию подписания данных перед отправкой на сервер микропроцессором устройства.

Еще одним вариантом применения M&M! может быть обеспечение гарантированной защищенной доставки данных именно на тот сервер, на который они должны быть доставлены после обработки на компьютере. В этом случае в момент установления соединения с сервером микропроцессор устройства проводит взаимную криптографическую аутентификацию с сервером и в случае положительного результата устанавливается соединение. Опять-таки важно отметить, что повлиять на результат этого процесса программное обеспечение, функционирующее в компьютере, никак не может.

И таких вариантов построения систем можно придумывать до бесконечности. Например, можно создать аппаратный файервол, который будет позволять пользователям посещать строго определенный набор сайтов из некоторого списка. И тем самым организации смогут с помощью таких служебных модемов экономить на трафике. Причем списки

с разрешенными сайтами M&M! сможет самостоятельно получать с сервера компании и актуализировать их после проверки под ними подписи.

Добавление модема в МАРШ! действительно качественно расширило возможности применения устройства для построения различных защищенных систем.

СПИСОК ЛИТЕРАТУРЫ:

1. *Конявский В. А.* ДБО — как сделать это безопасным. Часть II // Information Security/ Информационная безопасность. М., 2012. № 3 (июнь). С. 8–9.
2. Съемный носитель информации. Патент на полезную модель № 102139. 10.02.2011, бюл. № 4
3. Съемный носитель информации с безопасным управлением доступом. Патент на полезную модель № 123571. 27.12.2012, бюл. № 36.

ПОДХОД К СОЗДАНИЮ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ИНФОРМАЦИОННОЙ СИСТЕМЫ НА БАЗЕ ВЫСОКОПРОИЗВОДИТЕЛЬНЫХ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ ТЕХНОЛОГИЙ ОБРАБОТКИ ГЕОЛОГО-ГЕОФИЗИЧЕСКИХ ДАННЫХ

А.Б. СТЕПАНЯН, В.А. ДМИТРИЕВ, Е.П. МАКСИМОВИЧ, В.К. ФИСЕНКО
ОИПИ НАН Беларуси

Создание специализированных высокопроизводительных вычислительных систем и прикладного программного обеспечения, совместно обеспечивающих повышение эффективности поисков, разведки и разработки месторождений углеводородного сырья и других целевых полезных ископаемых, дает возможность в конечном итоге повысить экономический потенциал государств-участников Союзного государства, обеспечить их энергетическую и технологическую безопасность и снизить расходы государства на приращение разведанных запасов стратегического сырьевого ресурса и повышение качества его извлечения из недр.

Информационная система на базе высокопроизводительных информационно-вычислительных технологий обработки геолого-геофизических данных (далее — ИС СКИФ-НЕДРА) будет создаваться на основе UNICORE. Следовательно, основные функции системы защиты информации (СЗИ) ИС СКИФ-НЕДРА определяются функциями безопасности UNICORE.

UNICORE предоставляет такие сервисы безопасности, как аутентификация, управление доступом с помощью делегирования прав, конфиденциальность и целостность передачи информации.

Криптографические средства безопасности UNICORE основаны на OpenSSL и PKI (инфраструктуре открытых ключей). Все участники вычислительной среды (пользователи, вычислительные процессы и ресурсы) владеют сертификатами открытых ключей (далее — сертификат или СОК) в формате X.509, используемыми для аутентификации (выяснения «who is who»). В сертификате, подписанном ЭЦП удостоверяющего центра

(Certificate Authority), что гарантирует его подлинность, указаны идентификатор владельца (как правило, собственное имя — distinguished name) и соответствующий открытый ключ, срок действия и назначение сертификата.

Авторизация (предоставление участнику прав на доступ к ресурсам) выполняется в соответствии с результатами аутентификации и политики авторизации, принятой для данного ресурса.

Персональные сертификаты в формате X.509 выдаются на длительный срок в результате сложной и дорогостоящей процедуры установления личности субъекта.

Применение СОК для аутентификации предполагает использование личного ключа пользователя, который обычно хранится в зашифрованном виде на системе пользователя и защищен паролем, который надо предъявлять при каждом его использовании. Специфика выполнения заданий в UNICORE состоит в том, что задание, инициированное изначально пользователем (или другим заданием) требует подключения других ресурсов и входа в другие системы. Для устранения угрозы компрометации личного ключа пользователя необходимо обеспечить функцию единого входа (Single-Sign-On — однократного предъявления первичного личного ключа), исключающую передачу (пусть даже и безопасную) ключа на другие системы. Для реализации функции единого входа в UNICORE применяется безопасное делегирование прав (Delegation) на базе прокси-сертификата, действующего от имени владельца исходного сертификата.

Прокси-сертификат подписывается посредством первичного личного ключа или ключа другого прокси-сертификата. Прокси-сертификат имеет ограниченный срок действия (обычно не более 24 часа) и ограниченное (по сравнению с исходным СОК) назначение сертификата. Тем самым прокси-сертификат ограничивает права его владельца, снижая риск нарушения безопасности. Дополнительные расширения прокси-сертификата позволяют проследить всю цепочку сертификатов вплоть до исходного сертификата, что позволяет легко проверить его подлинность. Личный ключ прокси-сертификата хранится незашифрованным. Поэтому прокси-сертификат пригоден для непосредственного использования в вычислительной среде UNICORE.

Помимо указанных функций безопасности на основе UNICORE при создании СЗИ ИС СКИФ-НЕДРА необходимо обеспечить выполнение всего комплекса организационных и технических мер защиты информации, установленных в приказе Оперативно-аналитического центра при Президенте Республики Беларусь от 30 августа 2013 г. № 62 «О некоторых вопросах технической и криптографической защиты информации» [1]. Общая структура СЗИ ИС СКИФ-НЕДРА (с учетом требования приказа № 62) на основе UNICORE [2], приведена в рисунке 1.

Технические меры (функции) защиты информации, реализуемые в СЗИ ИС СКИФ-НЕДРА, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационной системы, должны обеспечивать:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- регистрацию событий безопасности;
- антивирусную защиту;
- обнаружение (предотвращение) вторжений;
- защиту среды виртуализации;
- защиту информационной системы, ее средств, систем связи и передачи данных с применением криптографические средства защиты информации.

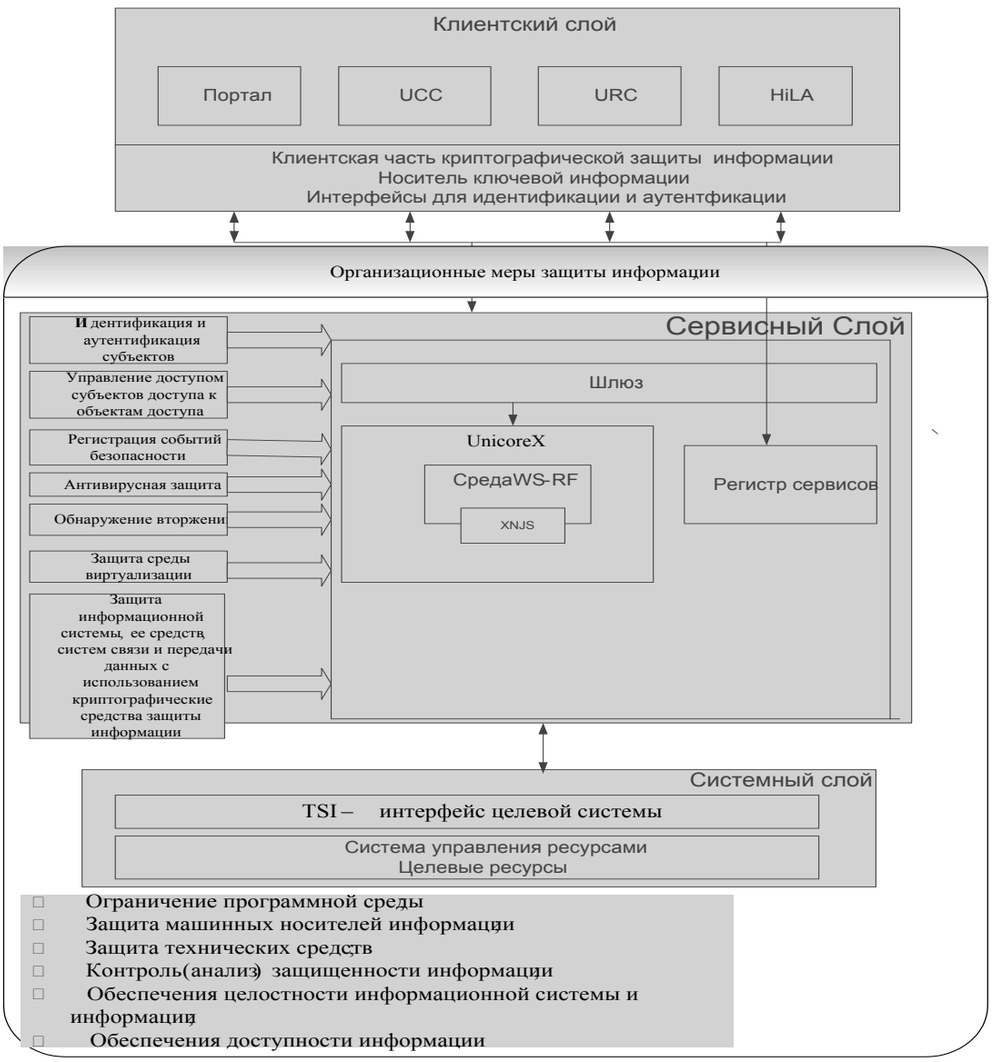


Рис. 1. Общая структура системы защиты информации ИС СКИФ-НЕДРА на основе UNICORE

Кроме этого должны быть реализованы организационные меры защиты информации, которые должны обеспечивать:

- ограничение программной среды;
- защиту машинных носителей информации;
- защиту технических средств;
- контроль (анализ) защищенности информации;
- целостность информационной системы и информации;
- доступность информации.

В соответствии с вышеприведенными техническими и организационными мерами, а также в соответствии с требованиями регулятора, для криптографической защиты информации можно использовать «Программный комплекс «Сервер TLS ABECT» (ПК AvTLSrv), реализующий защиту на транспортном уровне, или «Шлюз безопасности

Bel VPN Gate» и «Клиент безопасности Bel VPN Client 3.0.1», реализующий защиту на межсетевом уровне, которые имеют сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь.

ПК AvTLSrv предназначен для функционирования на стороне веб-сервера и обеспечивает:

- конфиденциальность передаваемых данных;
- целостность передаваемых данных;
- взаимную аутентификацию сторон с использованием СОК;
- одностороннюю аутентификацию сервера с использованием СОК.
- Bel VPN Gate обеспечивает:
- защиту транзитного трафика между различными узлами сети;
- защиту трафика самого шлюза безопасности;
- пакетную фильтрацию трафика.

Программно-аппаратное устройство Bel VPN Client обеспечивает защиту трафика между удаленным компьютером и шлюзом безопасности Bel VPN Gate. Клиент также обеспечивает пакетную фильтрацию трафика.

Таким образом, применение в UNICORE средства криптографической защиты информации имеющий сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь даст возможность аттестовать систему защиты информации ИС СКИФ-НЕДРА.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. О некоторых вопросах технической и криптографической защиты информации. Положение о порядке технической защиты информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам. Утвержден Приказом Оперативно-аналитического центра при Президенте Республики Беларусь 30 августа 2013 г. № 62 (в редакции приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 16 января 2015 г. № 3).
2. Архитектура UNICORE // Электронный документ [Электронный ресурс]. — Режим доступа: https://www.unicore.eu/documentation/architecture, свободный.

О СРЕДСТВАХ ДОВЕРЕННОЙ ЗАГРУЗКИ ДЛЯ АППАРАТНЫХ ПЛАТФОРМ С UEFI BIOS

С.С. ЛЫДИН

Закрытое акционерное общество «ОКБ САПР», Москва, Россия

UEFI BIOS представляет собой системное программное обеспечение нового поколения. Помимо функций, призванных повысить удобство эксплуатации компьютерных платформ, UEFI привносит ряд проблем безопасности, обусловленных архитектурными отличиями от «традиционного» BIOS. Настоящая статья содержит краткий анализ возможных угроз информационной безопасности архитектуры UEFI BIOS и определяет круг проблем, которые должны быть разрешены до начала использования этой архитектуры без ограничений.

Ключевые слова: UEFI, BIOS, средства доверенной загрузки, профиль защиты.

Процесс загрузки компьютера и состав компонентов, задействованных в этом процессе, определяется архитектурой системы. На высоком уровне абстракции применительно к большинству компьютеров загрузку можно представить в виде совокупности этапов, показанных на рисунке 1.

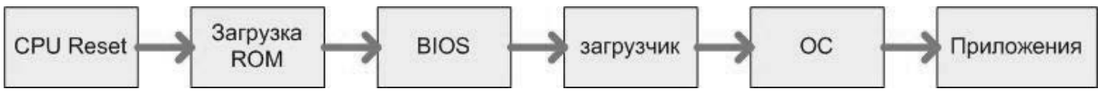


Рис. 1. Последовательность загрузки компьютера на высоком уровне абстракции

Из числа представленных на рисунке 1 элементов последовательности основное внимание в данной статье уделяется базовой системе ввода-вывода (basic input/output system, BIOS). BIOS представляет собой первую микропрограмму, которая исполняется после включения питания компьютера и хранится в энергонезависимой памяти, как правило, микросхеме флеш-памяти на материнской плате компьютера. Основное назначение BIOS состоит в:

- обеспечении инициализации и тестирования на низком уровне аппаратных компонентов компьютера, включая центральный процессор, динамическую оперативную память и др.;
- передаче управления загрузчику операционной системы (ОС).

BIOS могут разрабатываться как производителями комплектного оборудования (original equipment manufacturer, OEM), так и независимыми разработчиками, а поставляются конечным пользователям — производителями материнских плат и компьютеров. Нужно добавить, что производители часто, в том числе перед поставкой, обновляют системное программное обеспечение для того, чтобы исправить ошибки, поддержать новое аппаратное обеспечение и блокировать уязвимости.

Блокирование уязвимостей BIOS составляет актуальную задачу, поскольку, очевидно, для потенциального нарушителя всегда предпочтительнее скомпрометировать тот компонент, который загружается раньше прочих — получение контроля на более раннем этапе позволяет распространить влияние и на последующие элементы, такие как код режима управления системой (System Management Mode, SMM), загрузчик, гипервизор, ОС. Если успешные атаки на программы, исполняемые в пользовательском режиме, при современном положении вещей позволяют нарушителю добиться преимуществ хотя и очень существенных, но всё-таки ограниченных областью действия атакованной программы, то вредоносный код, записанный в BIOS, может позволить получить полный контроль над системой. Положение усугубляется тем, что, поскольку системный BIOS запускается с высоким уровнем привилегий на ранней стадии загрузки системы, вредоносный код, исполняемый на уровне BIOS, очень трудно обнаружить; кроме того, он может использоваться для повторного «инфицирования» системы даже после того, как была произведена переустановка ОС или даже замена жесткого диска компьютера. В этих условиях, очевидно, *BIOS и загрузчик должны восприниматься нарушителем как более привлекательные объекты атаки*. Действительно, в прошлые годы было опубликовано довольно большое количество сообщений о моделях возможных атак именно на эти цели. В рамках настоящей статьи не целесообразно останавливаться на них подробно, достаточно упомянуть только о двух типовых примерах [1]:

- атаки на BIOS, заключающиеся в подмене исходного кода BIOS вредоносным кодом BIOS, внедренным нарушителем;

– атаки на загрузчик, заключающиеся в установке подконтрольного нарушителю так называемого «буткита» (bootkit, разновидность «руткита» (rootkit), который исполняется в режиме ядра), «инфицирующего» загрузчик. При этом «буткит» может использоваться для организации утечки чувствительной информации, обрабатываемой в процессе загрузки, такой как пароли шифрования информации на жестком диске.

Подводя краткий промежуточный итог, можно констатировать, что *подмена микропрограммы BIOS вредоносным программным обеспечением в общем случае представляет опасную угрозу*, которая может быть частью сложной атаки на информационную систему организации, направленной на достижение длительного отказа в обслуживании (если BIOS в результате атаки подвергается разрушению) или обеспечение долгосрочного функционирования вредоносного кода в составе системы (если в результате атаки производится «инфицирование» BIOS) [2].

Однако что касается практической стороны вопроса, следует отметить, что атаки на так называемый «традиционный» BIOS (Legacy BIOS), который до сих пор выступал в настоящей статье в качестве предмета рассмотрения, как правило, связаны с низким уровнем мотивации нарушителя к их реализации — в силу слабого уровня стандартизации «традиционного» BIOS. Попытка разработать и внедрить вредоносный код, который мог бы использовать одновременно уязвимости, например, систем HP, Dell и IBM, обычно рассматривается нарушителем как неэффективная, потому что эти системы работают по-разному и реализовать универсальный механизм атаки весьма затруднительно. Иными словами, «эксплойты» для «традиционных» BIOS отличаются высоким уровнем зависимости от системы — как от версии BIOS, так и частного случая реализации аппаратных компонентов, таких как чипсет материнской платы. Подавляющая часть существующего вредоносного кода исполняется на уровне ядра ОС и более высоких уровнях, так, чтобы существовала возможность использовать его на максимально широком подмножестве систем. В силу указанного обстоятельства *известны лишь немногие практические реализации атак на уровне «традиционного» BIOS*. В качестве характерного примера можно привести лишь вирус «Чернобыль», обнаруженный в 1998 году. Для современных компьютеров этот вирус неактуален, поскольку они не содержат уязвимостей, которые им использовались [2].

Между тем, интенсивно осуществляемый в настоящее время переход от реализации «традиционного» BIOS к реализации, основанной на едином расширяемом микропрограммном интерфейсе (Unified Extensible Firmware Interface, UEFI), наряду с получением ряда функциональных преимуществ, в контексте обеспечения информационной безопасности характеризуется снижением для нарушителя сложности задачи внедрения вредоносного кода на уровне BIOS. Прежде чем привести подтверждения этому тезису, необходимо кратко ознакомиться с назначением и основными особенностями UEFI.

UEFI — это современный интерфейс между ОС и микропрограммами, управляющими низкоуровневыми функциями оборудования. Если последовательно придерживаться прежнего достаточно высокого уровня абстракции, процесс загрузки компьютера, использующего UEFI, формально представляется таким же, как и в случае с «традиционным» BIOS. Разница заключается в том, что код UEFI запускается, как правило, в современном 64-битном защищенном режиме работы процессора, тогда как код микропрограммы BIOS исполняется в 16-битном реальном режиме работы процессора. Однако в отличие от фактически неизменной по своему функциональному содержимому микропрограммы BIOS, система UEFI представляет собой программируемый интерфейс с довольно широ-

ким набором возможностей, совокупность которых придает ему черты самостоятельной операционной системы, пусть и облегченной. Основанием для подобной характеристики является то, что спецификация UEFI определяет, в частности, следующие элементы:

- *сервисы*. В UEFI допускается два типа сервисов: загрузочные (boot services) и среды выполнения (runtime services). Первые функционируют только до загрузки ОС компьютера и обеспечивают взаимодействие с графическими и текстовыми терминалами, шинами и т.д., а сервисы среды выполнения доступны даже из ОС компьютера;
- *драйверы устройств*. В UEFI реализуется платформонезависимая среда драйверов — EFI Byte Code (EBC). Взаимодействие ОС с драйверами устройств, как правило, осуществляется через EBC, что позволяет ОС компьютера использовать UEFI для базовой поддержки графических и коммуникационных функций до загрузки драйверов, установленных в ОС. Некоторые архитектурно-зависимые (non-EBC) драйверы имеют интерфейсы для использования ОС напрямую;
- *приложения*. Независимо от загружаемой ОС программа UEFI поддерживает возможность запуска отдельных приложений, которые могут разрабатываться и устанавливаться по усмотрению производителей компьютеров. К числу таких приложений относится, например, оболочка UEFI (UEFI shell). Оболочка может быть загружена еще до запуска ОС компьютера и использоваться для выполнения различных приложений: утилит по установке и настройке операционных систем, файловых менеджеров, утилит для просмотра файлов и др. Команды оболочки также позволяют копировать или перемещать файлы и каталоги в поддерживаемых файловых системах, загружать и выгружать драйверы. Оболочка поддерживает командную строку и командные файлы, аналогичные командам и пакетным файлам DOS.

Кроме того, спецификация UEFI определяет возможность *загрузки компьютера по сети* с помощью протокола удаленной загрузки (preboot execution Environment, PXE) и доступа к загрузочным образам, хранящимся в сетях хранения данных (storage area network, SAN).

Даже приведенного (далеко не полного) перечня функциональных возможностей UEFI BIOS достаточно, чтобы с очевидностью показать, что Я

Выше было показано, насколько важным для обеспечения информационной безопасности системы является сохранение целостности BIOS и компонентов, загружаемых после BIOS. Если рассматривать проблему безопасности информации несколько шире, следует постулировать, что важно обеспечить доверенную загрузку ОС, в рамках которой, помимо сохранения целостности ОС, выполняются, как правило, процедуры контроля устройств, с которых загружается ОС, а также процедуры идентификации и аутентификации пользователя.

В сложившейся практике перечисленные функции реализуются средствами доверенной загрузки (СДЗ), под которыми понимаются программно-технические средства, которые реализует функции по предотвращению несанкционированного доступа к программным и (или) техническим ресурсам компьютера на этапе его загрузки. СДЗ являются элементами подсистемы защиты информации от несанкционированного доступа и применяются на компьютерах совместно с другими средствами защиты информации.

На протяжении многих лет и до настоящего времени СДЗ разрабатывались и совершенствовались в условиях использования совместно с «традиционными» BIOS. Это обстоятельство определяло их архитектуру и принципы функционирования. В частности, при использовании «традиционного» BIOS обоснованной является реализация

принципа, согласно которому СДЗ начинает свою работу после выполнения системного BIOS и далее обеспечивает выполнение заданного набора требований доверия безопасности; при этом принимается, что код самого BIOS механизмами СДЗ проверять не нужно, поскольку, как было показано выше, атаки, связанные с подменой «традиционного» BIOS на практике по сути не реализуются. Но в том случае, если угроза подмены системного BIOS при использовании в информационной системе некоей организации все же признается актуальной, следует в установленном порядке проверить микропрограмму на наличие уязвимостей, позволяющих осуществить такую подмену. Данная проверка практически реализуема, поскольку общая архитектура и принципы функционирования «традиционного» BIOS хорошо известны, объем микропрограммного кода и набор функций весьма ограничен, а на выработку подходов к проведению различных исследований в распоряжении сообщества специалистов имелся не один десяток лет.

Ситуация выглядит совершенно иначе в случае использования UEFI BIOS:

1. все интерфейсы UEFI BIOS стандартизированы. Из этого следует то, что, в отличие от случая, когда используется «традиционный» BIOS, реализация атак на UEFI BIOS не состоит в сильной зависимости от архитектуры системы, и один и тот же «эксплойт» может использовать уязвимости на множестве компьютеров. В свою очередь, это означает, что сообщество больше не имеет права считать, что атаки на BIOS не реализуются на практике, что у нарушителя отсутствует для этого мотивация. Теоретические выводы подкрепляются и действительностью. Например, в [3] сообщается, что вследствие использования многими BIOS одного и того же кода обнаружены уязвимости, актуальные для 80 % исследованных компьютеров, включая модели Dell, Lenovo и HP; при этом уязвимости было настолько легко обнаружить, что удалось даже написать скрипт для автоматизации этого процесса, с помощью которого было выявлено множество уязвимостей. Далее, на конференции CanSecWest Vancouver 2015 исследователи из Legbacore продемонстрировали способ внедрения низкоуровневого троянского компонента LightEater [4]. Действуя на уровне UEFI, этот «буткит» остается невидимым для антивирусов. В проведенной демонстрации использовались материнские платы производства Acer, Asus, Gigabyte, Foxconn и MSI. В некоторых материнских платах удалось записать во флеш-память BIOS недопустимую инструкцию через модифицированный драйвер ядра, в результате которой успешную загрузку удалось выполнить только после физической замены чипа. В целом это напоминает новый виток развития вирусов типа «Чернобыль», но с гораздо более серьёзными последствиями. Эти выводы подтверждаются и многими другими свидетельствами (см., например, [5], [6], [7]).
2. UEFI BIOS имеет несоизмеримо более богатый набор функциональных возможностей (в качестве иллюстрации, дополнительной к тем многим, что уже были приведены ранее, можно отметить, например, что объем спецификации UEFI BIOS версии 2.6, последней на сегодняшней день, составляет более 2500 страниц), состав которого может существенно отличаться в различных системах в зависимости от предпочтений производителя. Это означает, во-первых, что проверить UEFI BIOS теми же методами, что использовались при проверке «традиционного» BIOS, не удастся, а во-вторых, усложнение и расширение его функциональности неизбежно влечет за собою увеличение «площади поверхности» для проведения разнообразных атак;
3. наличие широкого набора функций прикладного значения и наличие принципиальной возможности осуществления таких атак на UEFI BIOS, которые актуальны сразу для множества компьютеров, заставляет пересмотреть подход к процедурам

обновления системного BIOS. Следует признать, что на практике в информационных системах организаций процедура обновления «традиционного» BIOS представляла собой весьма редкое явление или же вообще не производилась. Очевидно, в случае с UEFI BIOS ее придется производить (локально и (или) через сеть) значительно чаще, что, в свою очередь, открывает новый класс уязвимостей для системного BIOS. В пользу значимости данной проблемы свидетельствует хотя бы то, что NIST выпустил специальные рекомендации по снижению вероятности угроз UEFI BIOS, большая часть содержания которых посвящена обеспечению защиты именно процедур обновления [2].

Таким образом, можно констатировать, что принципы обеспечения доверенной загрузки систем с UEFI BIOS должны принципиально отличаться от тех, что на протяжении многих лет применялись для систем на основе «традиционного» BIOS. Эти различия, по-видимому, обусловливают необходимость выработки нового подхода как для установления требований безопасности, которым должно удовлетворять соответствующее СДЗ, так и нового подхода к формированию со стороны регуляторов заключения о соответствии продукта предъявленным к нему требованиям безопасности информации.

В качестве реакции на данный тезис может последовать возражение, что, как известно, в соответствии с информационным письмом ФСТЭК России от 06.02.2014 N 240/24/405 «Об утверждении Требований к средствам доверенной загрузки» с 1 января 2014 года сертификация средств защиты информации, реализующих функции доверенной загрузки, в системе сертификации ФСТЭК России проводится на соответствие утвержденным Требованиям к средствам доверенной загрузки. И поскольку данные требования разрабатывались и утверждались в условиях, когда UEFI BIOS уже получил достаточно широкое распространение, от разработчика, может быть, не требуется ничего иного, как выполнить указанные требования, а от оценщика — в ходе сертификационных испытаний проверить соответствие СДЗ требованиям, изложенным в профилях защиты СДЗ.

Нужно, конечно, согласиться, что требования существуют, и, тем не менее, следует признать, что их недостаточно для решения описанной проблемы безопасности. Дело в том, что одно из основополагающих свойств любого профиля защиты заключается в том, что он предоставляет независимое от реализации описание требований безопасности, но не регламентирует, каким образом будут выполняться изложенные в нем требования. Выше было показано, что на самом высоком уровне абстракции процессы загрузки при использовании двух типов BIOS сходны, и, значит, попытка формирования независимых от реализации требований безопасности имеет право на жизнь. Однако дальше было показано, что при ближайшем рассмотрении имеющиеся между двумя типами BIOS различия носят настолько принципиальный характер, что принципы обеспечения доверенной загрузки систем с «традиционным» BIOS оказываются недействительными для систем с UEFI BIOS. Таким образом, именно разница в реализации становится очень значимым препятствием на пути выполнения требований, обнажая их недостаточность.

Можно привести множество примеров для подтверждения справедливости этого утверждения. Так, в профилях защиты СДЗ устанавливается, что СДЗ должно реализовывать функцию управления доступом к ресурсам компьютера в части обеспечения недоступности штатными средствами его ресурсов в случае загрузки нештатной ОС. Данное условие представляется в целом совершенно справедливым, но с учетом того, что UEFI BIOS, как было показано выше, как раз является штатным средством и реализует многие функции, свойственные операционной системе, включая функции доступа к ресурсам компьютера *еще прежде, чем производится загрузка* как штатной, так и нештатной ОС,

нужно признать, что выполнения указанного в профилях защиты условия недостаточно для достижения соответствующих целей безопасности.

Кроме того, профили защиты СДЗ основываются на предположении, что среда функционирования СДЗ должна обеспечивать невозможность отключения (обхода) компонентов СДЗ. Фактически это означает, что та или иная организация должна каким-то образом обеспечить, чтобы с помощью механизмов UEFI BIOS используемых в ней компьютеров нельзя было отключить компоненты СДЗ. Ответ на вопрос о том, каким образом это можно обеспечить в условиях, когда UEFI BIOS в сущности представляет собой обновляемую операционную систему с переменным составом элементов и большим числом функциональных возможностей, неочевиден, хотя попытки его отыскать предпринимаются [8]. Открытыми остаются и другие вопросы: в частности, должно ли СДЗ каким-то образом обеспечивать безопасное обновление BIOS, и если нет, то какой компонент подсистемы информационной безопасности должен контролировать процедуру обновления; или каким образом СДЗ должно расценивать попытку загрузки компьютера по сети и т.д.

Разумеется, все изложенное не означает, что проблема безопасности, связанная с использованием UEFI BIOS, не решаема в принципе. На все вопросы, конечно, существуют ответы, и могут быть разработаны как соответствующие технические решения, так и методы проверки соответствия этих решений требованиям безопасности информации. Но для этого сейчас требуется еще приложить существенные усилия со стороны сообщества специалистов по информационной безопасности, направленные в том числе, если не на разработку отдельных профилей защиты для систем с UEFI BIOS (хотя этот шаг выглядит логически обоснованным, поскольку среда функционирования СДЗ, содержащая в своем составе «традиционный» BIOS, принципиально отличается от среды функционирования СДЗ, содержащей UEFI BIOS, и, следовательно, состав даже высокоуровневых требований безопасности как к СДЗ, так и к его среде функционирования может отличаться), то, по крайней мере, на разработку методических материалов по реализации и оценке требований к таким системам на основе результатов накопления научно-технического опыта. В противном случае выполнение требований может превратиться в пустую формальность и привести к ситуации, когда будут разрабатываться СДЗ, которые полностью удовлетворяют положениям нормативных документов и используются при оснащении компьютеров в коммерческих и государственных организациях, а нейтрализация актуальных угроз и реализация целей информационной безопасности при этом обеспечиваться не будет. При этом внешне ситуация может выглядеть абсолютно естественно, существующие недостатки окажутся только отретушированы, а не искоренены.

Попытки решения описанной технической проблемы в частном случае, которые предпринимаются в настоящее время, выглядят несколько более оправданными, но, разумеется, в самом лучшем случае могут привести к достижению лишь локальных успехов. К числу таких попыток, по-видимому, следует отнести создание собственного UEFI BIOS с интегрированным сертифицированным СДЗ, которое предназначено для выполнения требований безопасности. В рамках подобных решений остаются нерешенными все те же вопросы обновления UEFI BIOS; нейтрализации угроз, реализуемых с помощью штатных средств UEFI BIOS; обеспечения защиты обширного уже эксплуатирующегося в организациях парка компьютеров, условия гарантийного обслуживания которых не предусматривают возможность замены одной микросхемы UEFI BIOS микросхемой стороннего производителя, и др.

Очевидно, для разработки универсальных СДЗ, адекватных существующим проблемам безопасности, требуется время. При этом компьютеры на основе UEFI BIOS со всеми известными и еще не до конца осознанными уязвимостями используются уже сейчас. В существующих условиях представляется целесообразным временный отказ от использования компьютеров с UEFI BIOS, по меньшей мере, в государственных информационных системах, в которых обрабатывается информация ограниченного доступа.

СПИСОК ЛИТЕРАТУРЫ

1. Xiaoyu Ruan. Platform Embedded Security Technology Revealed // Apress, 2014.
2. David Cooper, William Polk, Andrew Regenscheid, MurugiahSouppaya. BIOS Protection Guidelines. // NIST Special Publication 800–147, April 2011.
3. Kim Zetter. Hacking BIOS Chips Isn't Just the NSA's Domain Anymore. // URL: http://www.wired.com/2015/03/researchers-uncover-way-hack-bios-undermine-secure-operating-systems (дата обращения: 19.04.2016).
4. Corey Kallenberg and Xeno Kovah, LegbaCore. How many million BIOSes would you like to infect? // URL: https://reverse.put.as/wp-content/uploads/2016/01/HowManyMillionBIOSesWouldYouLikeToInfect_Whitepaper_v1.pdf (дата обращения: 19.04.2016).
5. Michael Mimoso. NEW BIOS IMPLANT, VULNERABILITY DISCOVERY TOOL TO DEBUT AT CANSECWEST. // URL: https://threatpost.com/new-bios-implant-vulnerability-discovery-tool-to-debut-at-cansecwest/111710/ (дата обращения: 19.04.2016).
6. Darren Pauli. Noobs can pwn world's most popular BIOSes in two minutes. // URL: http://www.theregister.co.uk/2015/03/19/cansecwest_talk_bioses_hack/ (дата обращения: 19.04.2016).
7. Thomas Fox-Brewster. 'Voodoo' Hackers: Stealing Secrets From Snowden's Favorite OS Is Easier Than You'd Think. // URL: http://www.forbes.com/sites/thomasbrewster/2015/03/18/hacking-tails-with-rootkits/#6537d0596143 (дата обращения: 19.04.2016).
8. *Алтухов А. А.* Неатомарный взгляд на РКБ как на композицию перехвата управления и контроля целостности. // Комплексная защита информации: материалы XX науч. — практ. конф., Минск, 19–21 мая 2015 г. — Минск: РИВШ, 2015, с 53–55.

АППАРАТНО-ПРОГРАММНОЕ УСТРОЙСТВО ГЕНЕРАЦИИ СЛУЧАЙНЫХ ЧИСЛОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С USB-ИНТЕРФЕЙСОМ

П. В. КУЧИНСКИЙ, М. И. НОВИК, Н. А. РАЩЕНЯ

Введение

Надежность и безопасность средств криптографической защиты информации определяется безопасностью и качеством используемых в них ключей. Для формирования криптографических ключей гарантированного качества применяют генераторы случайных числовых последовательностей (ГСЧП). При этом генерируемые случайные числа должны быть равномерно распределены на всем диапазоне и независимы. Обеспечение равновероятности и независимости на заданном уровне достигается применением ГСЧП,

использующих для генерации случайных чисел недетерминированные физические процессы.

Разработано аппаратно-программное устройство генерации случайных числовых последовательностей на физическом источнике шума с USB-интерфейсом (ГСЧП «Ключ-ВС»).

1. Структурная схема устройства

ГСЧП «Ключ-ВС» выполнен в виде аппаратно-программного устройства, в состав которого входят следующие основные модули:

- схема обработки шумового сигнала;
- программируемая логическая интегральная схема (ПЛИС);
- USB-мост;
- блоки стабилизации и преобразования напряжения;
- датчик температуры;
- блок индикации.

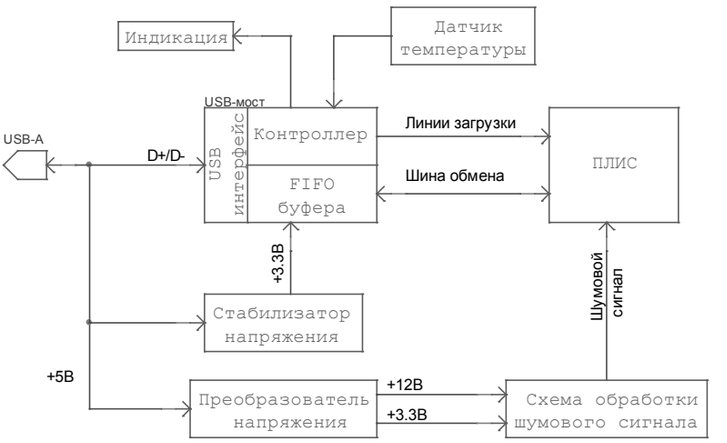


Рис. 1. Структурная схема ГСЧП «Ключ-ВС»

Схема обработки шумового сигнала обеспечивает получение аналогового шумового сигнала с физического источника шума (полупроводникового шумового диода) и его преобразование в цифровую форму. В качестве физического источника шума в ГСЧП «Ключ-ВС» используется шумовой диод ND 103L.

ПЛИС выполняет обработку оцифрованного аналогового шумового сигнала, обеспечивая получение первичной СЧП. Она также обеспечивает функции интерфейса обмена с USB-мостом. В ГСЧП «Ключ-ВС» применена ПЛИС XC 6SLX4.

USB-мост обеспечивает реализацию внешнего интерфейса изделия с целевой ПЭВМ. Для обмена данными между ПЛИС и ПЭВМ используются FIFO-буфера моста USB. Кроме того, USB-мост включает контроллер, который обеспечивает выполнение функций управления режимами работы моста USB, а также загрузку в ПЛИС конфигурационных данных. В качестве USB-моста в ГСЧП «Ключ-ВС» применена микросхема CY 7C 68013A.

Модули стабилизации и преобразования напряжения обеспечивают электропитание ГСЧП «Ключ-ВС» от USB-порта целевой ПЭВМ, включая организацию всех режимов

электропитания (плюс 3,3 В, плюс 5 В, плюс 12 В), необходимых для функционирования аппаратных и аппаратно-программных компонент устройства.

Датчик температуры обеспечивает измерение температуры и во взаимодействии с контроллером моста USB позволяет обеспечить контроль температурного режима эксплуатации ГСЧП «Ключ-ВС».

Блок индикации предназначен для визуального отображения основных режимов функционирования устройства в целях обеспечения удобства его эксплуатации. Его наличие позволяет оператору визуально определять состояние устройства (работоспособно, не функционирует, находится в состоянии ошибки или обмена данными и т.д.). На аппаратном уровне индикация обеспечивается применением светодиода.

2. Назначение и основные технические характеристики устройства

ГСЧП «Ключ-ВС» предназначен для генерации и вывода в персональную электронную вычислительную машину (ПЭВМ) случайной числовой последовательности (СЧП) на физическом источнике шума.

Область применения ГСЧП «Ключ-ВС» — системы и аппаратно-программные комплексы криптографической защиты информации, изготовления ключевой документации, сертификационные и доверительные центры инфраструктуры на публичных ключах, лабораторные и научные исследования.

ГСЧП «Ключ-ВС» обеспечивает:

- генерацию СЧП с использованием физического источника шума на полупроводниковом диоде и ее вывод в ПЭВМ;
- самотестирование работоспособности;
- тестирование работоспособности по команде оператора;
- контроль качества СЧП по команде оператора;
- контроль температуры на поверхности платы (внутри корпуса) устройства (при включенном электропитании ПЭВМ);
- функционирование под управлением операционной системы (ОС) Windows XP/7;
- визуальную индикацию режимов функционирования.

ГСЧП «Ключ-ВС» выполнен в виде аппаратно-программного устройства, помещенного в защитную оболочку (металлический корпус), не имеет самостоятельного применения и должен использоваться в составе ПЭВМ.

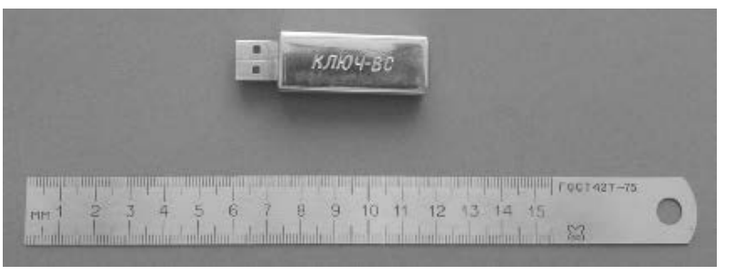


Рис. 2. Внешний вид ГСЧП «Ключ-ВС»

Основные технические характеристики ГСЧП «Ключ-ВС»:

- скорость генерации СЧП не менее 5 Мбит/с;
- взаимодействие с ПЭВМ через интерфейс USB 2.0;
- электропитание от USB порта ПЭВМ +5 В;

– формирование и выгрузка в ПЭВМ СЧП в виде двоичной последовательности по статистическим свойствам близкой (не хуже 10–5) к последовательности независимых равновероятных испытаний;
– встроенный датчик температуры;
– блокировка выгрузки СЧП при выходе температуры на поверхности платы (внутри корпуса) устройства за заданный диапазон (от плюс 5 до плюс 60 °С);
– встроенный светодиод для визуальной индикации режимов функционирования;
– статистическое тестирование качества выгруженной в ПЭВМ СЧП в соответствии с тестами, определенными в FIPS 140–1 [1].

Полученные с ГСЧП «Ключ-ВС» выборки СЧП (1000 подвыборок по 106 бит) успешно проходят тестирование с использованием пакета тестов NIST [2].

3. Программное обеспечение устройства

Программное обеспечение (ПО) ГСЧП «Ключ-ВС» включает специальное ПО (СПО) и прикладное ПО (ППО).

СПО ГСЧП «Ключ-ВС» состоит из:
– программы контроллера моста USB (LuNG02.iic) — обеспечивает функционирование устройства на шине USB, а также загрузку в ПЛИС конфигурационных данных;
– программы-файла конфигурации ПЛИС (LuNG02.bin) — обеспечивает функции интерфейса обмена с мостом USB и цифровой обработки шумовых сигналов.

ППО ГСЧП «Ключ-ВС» состоит из:
– драйвера (LospUSB.sys) — обеспечивает функционирование устройства под управлением ОС Windows XP/7;
– библиотеки функций (LuNG02.dll) — предоставляет разработчику пользовательских программ интерфейс работы с устройством под управлением ОС Windows XP/7;
– пользовательского ПО — предоставляет интерфейс пользователя для работы с устройством под управлением ОС Windows XP/7.

Пользовательское ПО обеспечивает следующие основные функциональные возможности:
– просмотр характеристик ГСЧП «Ключ-ВС»;
– тестирование ГСЧП «Ключ-ВС»;
– получение и сохранение в файл СЧП с ГСЧП «Ключ-ВС»;
– проверку качества СЧП;
– ведение журнала событий.

Контроль качества сгенерированной (выгруженной) СЧП осуществляется путем выполнения статистических тестов. При этом оператор имеет возможность выбрать режим тестирования: выполнить все доступные или только выбранные статистические тесты.

Во время работы пользовательского ПО обеспечиваются:
– визуальная индикация режимов и результатов выполнения команд оператора;
– выдача сообщений об ошибках, возникающих при работе оператора с ГСЧП «Ключ-ВС», включая ошибки при тестировании работоспособности устройства.

В ППО изделия реализована возможность переключения на английский язык интерфейса оператора.

Заключение

Для генерации СЧП на физическом источнике шума разработано аппаратно-программное устройство ГСЧП «Ключ-ВС» с USB-интерфейсом, обеспечивающее формирование

и выгрузку в ПЭВМ со скоростью не менее 5 Мбит/с СЧП в виде двоичной последовательности по статистическим свойствам близкую (не хуже 10–5) к последовательности независимых равновероятных испытаний.

ССЫЛКИ

1. Security requirements for Cryptographic Modules. FIPS 140–1. — U. S. Department of Commerse. 1994.
2. NIST SP 800–22. A Statistical Test Suite for Random and Pseudorandom Numbers, revision 1a.

СЕКЦИОННОЕ ЗАСЕДАНИЕ «ВОПРОСЫ СТАНДАРТИЗАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

КРИПТОГРАФИЧЕСКИЕ СТАНДАРТЫ РЕСПУБЛИКИ БЕЛАРУСЬ И ИХ РАЗВИТИЕ

С.В. АГИЕВИЧ, Д.В. ЕРМОЛИЦКИЙ, С.В. КУТУЗОВ, Д.В. НЕСТЕРОВ, О.В. СОЛОВЕЙ, Ю.С. ХАРИН
Белорусский государственный университет
НИИ прикладных проблем математики и информатики
Оперативно-аналитический центр при Президенте Республики Беларусь

Существующая система криптографических стандартов

В Республике Беларусь с 1999 года ведутся работы по разработке технических нормативных правовых актов (ныне государственных стандартов и предварительных стандартов, ранее руководящих документов Национального банка), устанавливающих требования к компонентам криптографической «инфраструктуры» (см. [1]). В настоящее время в республике действует более 20 государственных стандартов в данной области (+ 2 предварительных стандарта и проект руководящего документа). Данные стандарты определяют требования к алгоритмам криптографических преобразований и протоколам (алгоритмам шифрования и режимам его использования — ГОСТ 28147–89, СТБ 34.101.31–2011, процедурам выработки и проверки электронной цифровой подписи — СТБ 1176.2–99, СТБ 34.101.45–2013, функции хэширования — СТБ 1176.1–99, СТБ 34.101.31–2011, протоколу TLS — СТБ 34.101.65–2014), управления криптографическими ключами (алгоритмы генерации псевдослучайных чисел — СТБ 34.101.47–2012, формат запроса на издания сертификата открытого ключа — СТБ 34.101.17–2012, формат сертификата открытого ключа и списка отозванных сертификатов — СТБ 34.101.19–2012, алгоритм разделения секрета — СТБ 34.101.60–2014, протоколы формирования общего ключа на основе эллиптических кривых — СТБ 34.101.66–2014). Также определены требования безопасности к программным, программно-аппаратным и техническим средствам криптографической защиты информации — СТБ 34.101.27–2011 и СТБ П 34.101.43–2009. Установлены требования к формату карточки открытого ключа и политике применения сертификатов удостоверяющего центра.

Развитие системы криптографических стандартов

В 2016 году в Республике Беларусь планируется расширить действующую систему стандартов в области криптографической защиты информации: ввести в действие СТБ 34.101.77 «Информационная технология и безопасность. Алгоритмы хэширования» и дополнить СТБ 34.101.47 «Информационная технология и безопасность. Алгоритмы генерации псевдослучайных чисел». В первом стандарте будет определено семейство алгоритмов хэширования, во втором будут дополнительно введены алгоритмы генерации одноразовых паролей. Опишем стандартизируемые алгоритмы.

Алгоритмы хэширования

В информационных системах республики для управления электронными цифровыми подписями (ЭЦП) используется СТБ 34.101.45 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи на основе эллиптических кривых». Этот стандарт определяет три уровня стойкости: $l = 128$, $l = 192$ и $l = 256$. Для того чтобы поддержать уровень l, требуется использовать функцию хэширования с 2l-битовыми значениями. СТБ 34.101.31 определяет 256-битовую хэш-функцию belt-hash, но 384- и 512-битовые функции хэширования пока в нашей стране не стандартизованы. Отметим, что ЭЦП на высоких уровнях стойкости востребованы уже сейчас. Например, сверхнадежные подписи нужны для построения долговременных архивных хранилищ.

Для поддержки ЭЦП на уровнях $l = 192$ и $l = 256$ было решено разработать семейство алгоритмов хэширования. Это семейство получило название Bash (Hash с заменой H на B).

Алгоритмы Bash строятся по схеме sponge (губка), предложенной Г. Бертони, Дж. Дэменом, М. Питерсом и Ж. Ван Ашем в [2]. Базовым композиционным элементом Bash является шаговая функция Bash-f. Эта функция обновляет хэш-состояние по очередному блоку обрабатываемых данных. Функция строится с помощью логических операций ($\neg$, $\wedge$, $\vee$) над 64 разрядными словами, циклических сдвигов этих слов и поразрядных и исключающих сложений ($\oplus$). Таким образом, функция относится к классу LRX (Logical+Rotation+Xor).

Выбранная платформа sponge + LRX была с успехом применена в алгоритмах хэширования Keccak (SHA-3), которые были стандартизированы в США в 2015 году в FIPS 202. Считая семейство Keccak творческой удачей и с уважением относясь к многочисленным криптографическим находкам его разработчиков, мы, тем не менее, решили продолжить традицию национальной криптографии и разработать собственное семейство. По нашим оценкам, производительность Bash близка к производительности Keccak. Текущие гарантии стойкости, выраженные в оценках снизу для числа активных S-блоков, для Bash и Keccak также сопоставимы.

Алгоритмы Bash работают не только на уровнях $l = 192$ и $l = 256$, но и на других уровнях из множества $\{16, 32, 48, \ldots, 256\}$. Алгоритм уровня l обрабатывает данные блоками из 1536–4l битов и возвращает хэш-значение длины $2l$. Принципы построения алгоритмов описаны в [3].

Алгоритмы генерации одноразовых паролей

В массовых информационных системах для проверки подлинности клиентов перед серверами чаще всего используется парольная аутентификация. Пароль — это классический секрет, с обработкой которого может справиться обычный человек. Пароль достаточно легко запомнить, для его хранения не нужны дополнительные устройства, пароль легко ввести практически в любой программно-аппаратной среде. Но парольная аутентификация обладает и существенными недостатками. Во-первых, пользователь не способен запомнить сильный высокоэнтропийный секрет. Пароль — это всегда слабый секрет, и у противника появляется возможности угадать его. Во-вторых, парольная аутентификация теряет надежность в агрессивной среде, т.е. там, где противник может перехватывать вводимые пользователем данные.

Аутентификация может быть усилена, если пользователь применяет специальные устройства, которые способны хранить сильные секреты и проводить с ними криптографические вычисления. С помощью этих устройств можно организовать надежный криптографический протокол аутентификации. Но такой протокол, как правило, будет иметь высокую вычислительную сложность. Поэтому устройство должно обладать доста-

точно серьезными вычислительными ресурсами, что повышает его стоимость и во многих случаях делает его применение экономически неоправданным. Кроме этого, для выполнения сложного протокола устройство должно быть плотно сопряжено с информационной системой, в которой пользователь работает, а это оказывается не всегда возможным.

Выходом является упрощение криптографических вычислений и выдача их результата в виде короткого пароля с малым сроком действия. Такой пароль принято называть одноразовым (one-time password, OTP). Даже если одноразовый пароль будет скомпрометирован, компрометация затронет только конкретный сеанс пользователя или даже определенный промежуток этого сеанса.

Средства формирования одноразовых паролей получили широкое распространение в связи с массовой аутентификацией в сети Интернет. Эти средства могут быть аппаратными (пример — токен SecureID компании RSA) или программными (приложение Authenticator компании Google). Унификация средств требует стандартизации алгоритмов формирования одноразовых паролей, правил формирования их входных данных, правил кодирования паролей, правил аутентификации.

Основные шаги по стандартизации сделаны международным комитетом OATH (Open AuTHentication). Под эгидой этого комитета разработаны 3 основных стандарта: RFC 4226, RFC 6238 и RFC 6287. В стандартах определены алгоритмы HOTP, TOTP и OCRA. Алгоритмы строят пароль по общему для клиента и сервера ключу и дополнительным уникальным данным: монотонному счетчику, отметке времени, случайному запросу. Алгоритмы по сути определяют 3 типа систем аутентификации: на основе событий, на основе времени и на основе запросов.

В системах первого типа пароль меняется при возникновении определенных событий. Как правило, таким событием для клиента является любая попытка аутентификации, а для сервера — успешная попытка.

В системах на основе событий противник может предъявлять серверу пароли до тех пор, пока целевое событие не произошло и, таким образом, возникают предпосылки для перебора паролей. Для защиты от перебора сервер должен предусмотреть блокировку ввода пароля на некоторое время или до возникновения определенного события, например, разблокировки.

События для клиента и сервера могут различаться, их пароли могут разойтись, и поэтому система аутентификации нуждается в дополнительных механизмах синхронизации. В системах на основе алгоритма HOTP клиент и сервер хранят счетчики попыток аутентификации. Синхронизация состоит в том, что сервер проверяет пароль не только на текущем значении счетчика, но и на d будущих значениях. Фактически сервер проверяет будущие пароли, которые могут оказаться текущими относительно клиента. Если i-й будущий пароль оказался подходящим, то сервер восстанавливает синхронизацию, увеличивая счетчик не на 1, а на $i + 1$. Синхронизация будет полностью потеряна, если клиент выполнил более d попыток аутентификации, о которых не известно серверу.

В системах на основе времени одноразовый пароль обновляется каждые t секунд (на практике $t = 30$ или 60). Устройство должно быть снаряжено достаточно точным таймером, что может привести к значительному его удорожанию. С другой стороны, системы на основе времени имеют ряд преимуществ относительно систем на основе событий. Во-первых, возможности противника по перебору паролей ограничены — он должен успеть подобрать пароль в течение t секунд. Во-вторых, опасность рассинхронизации не столь велика, как в предыдущем случае. Для синхронизации клиенту и серверу достаточно согласовать показания времени.

В системах на основе запросов одноразовый пароль строится на основании случайного запроса сервера. Фактически одноразовый пароль превращается в ответ протокола «запрос — ответ». Таймер не нужен, но дополнительно к интерфейсу вывода пароля должен быть предусмотрен интерфейс ввода запроса. Проблемы с синхронизацией отсутствуют, но противник может перебирать пароли относительно текущего запроса сколь угодно долго. Серверу следует ограничивать число попыток ввода пароля, иначе система перестанет быть стойкой.

Итоги представленного сравнительного анализа обобщены в таблице 1.

Таблица 1

Схема генерации OTP	Аппаратные требования	Синхронизация	Надежность
на основе событий	интерфейс вывода (дисплей)	динамически по правильным паролям, возможна потеря	средняя
на основе времени	интерфейс вывода, таймер	согласования времени	высокая
на основе запросов	интерфейс вывода, интерфейс ввода (миниклавиатура)	не нужна	высокая

В СТБ 34.101.47 стандартизируются все три схемы. Сохранена максимальная совместимость с базовыми RFC. В качестве базового алгоритма генерации псевдослучайных чисел предлагается использовать hmac[belt-hash] (он определен в этом же стандарте).

ЛИТЕРАТУРА

1. Криптографические стандарты Республики Беларусь. Электронный ресурс по адресу: http://apmi.bsu.by/resources/std. Последнее обращение: 2016.04.21.
2. *Bertoni G., Daemen J., Peeters M., Van Assche G.* Cryptographic sponge functions. Version 0.1, 2011. Avail. at: http://sponge.noekeon.org/CSF-0.1.pdf.
3. *Agievich S., Marchuk V., Maslau A., Semenov V.* Bash-f: another LRX sponge function. Submitted to the 5th Workshop on Current Trends in Cryptology, 2016.

ПЕРСПЕКТИВЫ РАЗВИТИЯ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Ю.К. ЯЗОВ, С.В. СОЛОВЬЕВ, Е.В. КОЛЕСНИКОВА
ФАУ «ГНИИИ ПТЗИ ФСТЭК РОССИИ»

В настоящее время общие информационные ресурсы Республики Беларусь и Российской Федерации включают в себя более 20 крупных информационных систем, обеспечивающих деятельность Союзного государства и государств-участников Договора о создании Союзного государства в таких сферах, как военно-техническое сотрудничество и оборона, таможенный, пограничный и экспортный контроль, взаимодействие правоохранительных органов и органов юстиции, а также других сферах деятельности. В сфере совместной

деятельности Республики Беларусь и Российской Федерации может быть задействовано более 20 автоматизированных систем управления технологическими процессами, включая системы управления движением железнодорожного транспорта, топливно-энергетическим комплексом, географические и навигационные системы, финансово-кредитные и другие системы информационной инфраструктуры.

В этой связи одним из важных направлений деятельности Союзного государства является обеспечение защиты общих информационных ресурсов Республики Беларусь и Российской Федерации.

Деятельность по защите информации (ЗИ) включает правовые, организационные, технологические, технические, информационные и другие составляющие. Наряду с ее многоаспектностью характерным является:

- большое количество и разнообразие используемой информации;
- применение разнообразных, зачастую не связанных между собой отечественных и зарубежных нормативных документов по ЗИ;
- большое количество и разнообразие мер и средств ЗИ, которые могут применяться для нейтрализации угроз безопасности информации;
- неоднозначность в принятии решений о составе и характеристиках конкретных мер и средств защиты;
- сложность охвата всех аспектов организации и ведения ЗИ;
- значительные затраты времени и сил на организацию и ведение защиты информации.

Широкий спектр, сложность и разноплановость задач по ЗИ определяют потребность в создании специальных информационных систем обеспечения такой деятельности, систем поддержки принятия решений (СППР), которые востребованы на различных уровнях принятия решений по защите информации — в органах государственной власти на федеральном, региональном и местном уровнях, в организациях и предприятиях, на объектах защиты, где решаются вопросы ЗИ от несанкционированного доступа и от утечки по техническим каналам.

С помощью СППР осуществляется сбор, обработка и накопление большого объема разноплановой информации, решение комплекса информационных и расчетных задач, подготовка необходимой информации для принятия решений, разработка и доведение документов до должностных лиц и др.

Например, СППР могут быть использованы при:

- оценке возможностей нарушителей безопасности информации;
- анализе возможных уязвимостей программного обеспечения (ПО);
- анализе возможностей реализации угроз безопасности информации;
- оценке последствий от реализации угроз безопасности информации;
- определении требований к системе защиты информации (СЗИ) на объекте защиты, структуры СЗИ и выборе средств защиты;
- определении характеристик ПО СЗИ.

Существующие в настоящее время СППР в основном ориентированы на анализ и управление рисками. Например, СППР иностранного производства: программные продукты COBRA, GRAMM, MARION, RiskWatch, RickPac, RA2 art of risk, vsRisk, Callio Secura 17799, Buddy System, MethodWare, Proteus, а так же СППР отечественного производства: АванГард, РискМенеджер, Digital Security Office 2006 (включающий систему анализа и управления информационными рисками ГРИФ и систему разработки и управления политикой безопасности информационной системы КОНДОР).

Следует отметить, что применение СППР иностранного производства затруднено, потому что они:

– не учитывают современную нормативную базу России и Беларуси в области ЗИ и не позволяют отслеживать изменения в ее составе;
– не ориентированы на построение СЗИ;
– не содержат необходимого информационного обеспечения деятельности по ЗИ.

Кроме того, важным фактором является высокая стоимость указанных систем, например стоимость лицензии за одно рабочее место некоторых программных продуктов СППР иностранного производства составляет от 10 000 долларов.

Разработка отечественных СППР в интересах решения задач в области ЗИ должна учитывать:

– регулярные изменения (совершенствование) аппаратного и программного обеспечения объектов защиты;
– непрерывно расширяющийся спектр подлежащих учету и анализу угроз безопасности информации и, как следствие, необходимость их прогнозирования;
– интенсивно меняющийся состав нормативного обеспечения (отечественного и международного) в области ЗИ;
– отсутствие по многим аспектам планирования и выполнения мероприятий по ЗИ необходимого методического обеспечения, в том числе касающегося формальных критериев принятия решений;
– быстрое устаревание системных решений по построению СППР и составу реализуемых функций, необходимость регулярного реинжиниринга СППР.

Проведенный анализ существующих СППР, выполняемых ими функций, состава задач в области ЗИ, решение которых может поддерживаться с применением СППР, показал, что СППР в области ЗИ имеют следующую типовую структуру (рисунок 1).

Рис.1. Обобщенная структура СППР в области ЗИ

Состав подлежащих разработке СППР в различных отраслях приведен на рисунке 2.

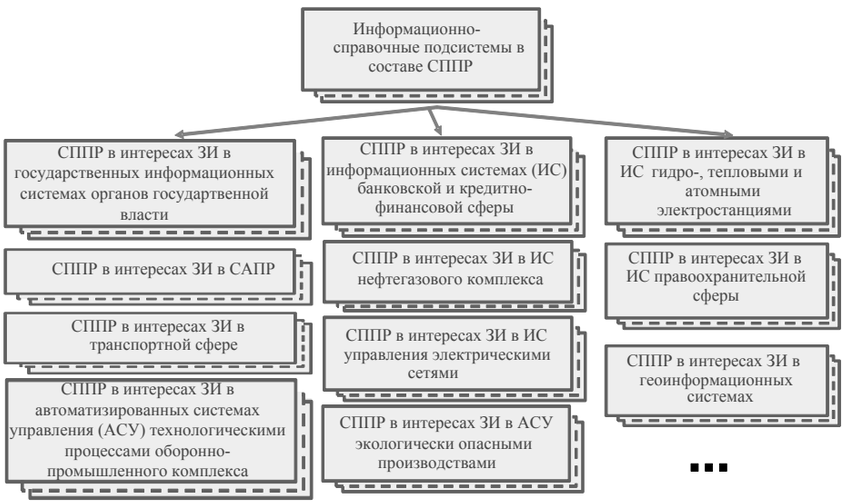


Рис. 2. Состав подлежащих разработке СППР в интересах ЗИ

Также следует отметить, что при создании СППР в области ЗИ перспективными направлениями являются:

– использование web-технологий при построении СППР;
– создание распределенных многопользовательских информационных систем;
– создание СППР с элементами искусственного интеллекта и др.

На настоящий момент подлежат исследованию следующие вопросы:

– определение степени централизации информационных ресурсов распределенных СППР;
– прогноз развития и разработка методологии реинжиниринга СППР в области ЗИ;
– исследование возможности и способов интеграции готовых решений в СППР.

Таким образом, СППР в области защиты совместных информационных ресурсов Союзного государства имеют практическую востребованность, а вопросы их разработки и реинжиниринга требуют серьезной научной проработки.

НЕКОТОРЫЕ АСПЕКТЫ ФОРМИРОВАНИЯ И РЕАЛИЗАЦИИ ТРЕБОВАНИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ

В.К. ФИСЕНКО, В.А. ДМИТРИЕВ, А.Б. СТЕПАНЯН, Е.П. МАКСИМОВИЧ
ОИПИ НАН Беларуси
П.А. ДЕРУЖКО
Белорусский государственный университет

Со второй половины девятнадцатого и в начале двадцатого века остается актуальной проблема формирования и реализации требований по защите информации информационных систем. В мае 1998 г. специалистами организаций ряда стран (США, Канады, Великобритании, Германии, Нидерландов и Франции) завершена разработка, а в 1998 г. принят

международный стандарт ИСО/МЭК 15408 «Информационная технология. Методы и средства безопасности. Критерии оценки безопасности информационных технологий» [1], на основе которого разработан и модернизирован СТБ 34.101. 1, 2, 3–2004, получивший наименование «Общие критерии» и применимы как для продуктов, так и для систем информационных технологий. Данные стандарты представляли собой наиболее полный на то время набор функциональных и гарантийных требований безопасности, которые удовлетворяли потребности заказчиков, разработчиков, испытателей и пользователей. Каждое требование безопасности представлено классом, семейством и компонентом. Компонент содержит наименование требования и формулировку правила реализации требования. Вторая версия международного стандарта была разработана в 2008 г. специалистами подкомитета SC 27 Объединенного технического комитета JTC 1 «Информационные технологии» ISO/IEC, который применим лишь для продуктов информационных технологий.

Достоинством указанных международных стандартов является то, что в них представлены как наименования требований безопасности, так и правила по реализации требований для каждого компонента соответствующего класса функциональных и гарантийных требований. В процессе разработки и практического применения информационных систем реализация функциональных и гарантийных требований безопасности, определенных в соответствии с указанными выше стандартами, не всегда обеспечивает требуемую защищенность информационных систем. Дополнительно требуется формирование и реализация требований организационно — распорядительного характера.

Ученые и специалисты России разработали документы, содержащие меры защиты информации в государственных информационных системах, а также правила их формирования. и реализации. Так в 2014 г. разработан методический документ «Меры защиты информации в государственных информационных системах» [2] и утвержден в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

В методическом документе представлены 13 групп мер по защите информации:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- обеспечение целостности информационной системы и информации;
- обеспечение доступности информации;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств и систем связи и передачи данных.

Каждая группа разбита на определенную совокупность конкретных мер по защите информации. Каждая конкретная мера любой из 13 групп представляет собой совокупность средств по защите информации.. Для каждой меры защиты приведена совокупность минимальных требований по реализации каждой меры защиты.

Правила и процедуры по реализации требований о защите информации и мер защиты информации в конкретной информационной системе определяются в эксплуатацион-

ной документации на каждую систему защиты и организационно-распорядительных документах. Выбор требований по защите информации определяется приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [3].

Выбор мер защиты информации осуществляется с учетом класса защищенности информационной системы, определяющего требуемый уровень защищенности содержащейся в ней информации, угроз безопасности информации, включенных в модель угроз безопасности информационной системы и структурно-функциональных характеристик информационной системы (структуры и состава информационной системы; физических, логических, функциональных и технологических взаимосвязей между сегментами информационной системы; взаимосвязей с иными информационными системами и информационно-телекоммуникационными сетями, режимов обработки информации в информационной системе и в ее отдельных сегментах), а также иных характеристик информационной системы, применяемых информационных технологий и особенностей функционирования систем.

К сожалению, в документе [2] не отражена связь процедур и правил формирования и реализации мер и требований по защите информации с международными критериями [1], в том числе с заданием по безопасности или с техническим заданием на разработку системы защиты информации.

Издан приказ Оперативно-аналитического центра при Президенте Республики Беларусь № 62 от 30.08.2013 (в редакции приказа Оперативно-аналитического центра при Президенте Республики Беларусь № 3 от 16 января 2015 г.), который содержит перечень требований к системе защиты информации, подлежащих включению в задание по безопасности на информационную систему или в техническое задание на информационную систему» [4].. В нем приведено 74 требования для классов объектов информатизации А2, Б2, В2., в том числе требование по криптографической защите информации.

Фактически данный перечень требований к системе защиты информации однозначно соответствует по наименованию перечню конкретных мер по защите информации[2].

К сожалению, в новой версии приказ № 62 [4] не представлены процедуры и правила по реализации требований, что затрудняет его практическое использование. Сотрудники ОИПИ НАН Беларуси использовали методический документ России, утвержденный ФСТЭК России 11.02.2014, и после некоторых редакционных правок сгруппировали весь комплекс в 13 групп мер защиты информации, отдельно выделив группу мер по криптографической защиты информации.

Для каждого требования определены процедуры и правила по реализации, которые могут быть представлены в организационно-распорядительных документах, в СТБ 34.101.1.2.3. —2014, а также непосредственно в дополненной авторами таблице с перечнем требований и правил по их реализации. Перечень организационно-распорядительных документов пока не определен. Такие документы надо разрабатывать в качестве методических нормативных документов и утверждать или в ОАЦ, или же в Госстандарте Республики Беларусь. Для демонстрации предложений по реорганизации таблицы требований, представленных в [4], ниже приводится в табличной форме одно из требований по защите информации с указанием меры защиты, правил реализации требований для объектов информатизации.

Для реализации приведенных в [4] требований можно воспользоваться правилами, изложенными в СТБ 34.101.2–2014. Ниже представлены два варианта такого представления правил реализации.

Требование 13 из [4]: Определение, при необходимости, действий субъектов, которые могут совершаться такими субъектами до их идентификации и аутентификации

Ниже приведены правила по реализации указанного выше требования на основе двух документов.

1. По СТБ 34.101.2–2014

Требование: Компонент FIA _UAU.1 Выбор момента времени аутентификации.

FIA _UAU.1.1 ФВБО должны от имени пользователя допускать выполнение (назначение: управление данными аутентификации; управление данными аутентификации пользователем, осуществляющим аутентификацию; управление списком действий, которые могут выполняться перед аутентификацией пользователя), чем пользователь аутентифицирован.

Требование (мера защиты)	Правила реализация требований	Класс объекта информатизации		
		А2	Б2	В2
2 Управление доступом субъектов доступа к объектам доступа				
12 Блокирование доступа к информационной системе после истечения установленного времени бездействия (неактивности) субъекта или по его запросу	Владелец информационной системы должен создать организационно — распорядительный документ по правилам и процедурам блокирования сеансов доступа после истечения установленного времени бездействия (неактивности) субъекта или по его запросу, который должен содержать следующие требования и правила по их реализации. а) в информационной системе должно обеспечиваться блокирование сеанса доступа пользователя после установленного оператором времени его бездействия (неактивности) в информационной системе или по запросу пользователя. Блокирование сеанса доступа пользователя в информационную систему обеспечивает временное приостановление работы пользователя со средством вычислительной техники, с которого осуществляется доступ к информационной системе (без выхода из информационной системы); б) для заблокированного сеанса должно осуществляться блокирование любых действий по доступу к информации и устройствам отображения (кроме необходимых для разблокирования сеанса); в) блокирование сеанса доступа пользователя в информационную систему должно сохраняться до прохождения им повторной идентификации и аутентификации в соответствии с мерами по защите класса «Идентификация и аутентификация субъектов доступа и объектов доступа». Для повышения качества и своевременности блокирования доступа к информационной системе после истечения установленного времени бездействия (неактивности) субъекта или по его запросу необходимо реализовать следующие требования: 1) в информационной системе должно обеспечиваться блокирование сеанса доступа пользователя после времени бездействия (неактивности) пользователя: а) до 15 минут; б) до 5 минут; 2) в информационной системе на устройстве отображения (мониторе) после блокировки сеанса не должна отображаться информация о сеансе пользователя (в том числе использование «хранителя экрана», гашение экрана или иные способы); 3) в информационной системе должно обеспечиваться завершение сеанса пользователя (выхода из системы) после превышения установленного оператором времени бездействия (неактивности) пользователя.	+	+	+

FIA_UAU.1.2 ФВБО должны требовать, чтобы каждый пользователь был успешно аутентифицирован перед тем, как ему будет разрешено осуществление любых других действий, выполняемых при посредничестве ФВБО от имени этого пользователя.

Требование: Компонент FIA_UID.1 выбор момента времени идентификации.

FIA_UID.1.1 ФВБО должны от имени пользователя допускать выполнение (назначение: управление идентификаторами пользователя; управление списком действий, которые допускается выполнять перед идентификацией, если авторизованный администратор имеет право изменять эти действия) прежде, чем пользователь идентифицирован.

FIA_UID.1.2 ФВБО должны требовать, чтобы каждый пользователь был успешно идентифицирован перед тем, как ему будет разрешено осуществление любых других действий, выполняемых при посредничестве ФВБО от имени этого пользователя.

2. По организационно-распорядительному документу

Владелец информационной системы должен создать организационно распорядительный документ по правилам и процедурам определения действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации, который должен содержать следующие требования:

а) должны быть установлены действия пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации, и запрет на действия пользователей, не включенных в перечень разрешенных действий, до прохождения ими процедур идентификации и аутентификации;

б) разрешение действий пользователей до прохождения ими процедур идентификации и аутентификации должно осуществляться при предоставлении пользователям доступа к общедоступной информации (веб — сайтам, порталам, иным общедоступным ресурсам);

в) администратору безопасности разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования информационной системы в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

Разработчик задания по безопасности или технического задания на информационную систему вправе самостоятельно определять в конкретном случае какой вариант реализации требований использовать. Однако надо учитывать, что значительная часть требований документа [3] регламентируются организационно-распорядительными документами. Это означает, что в задании по безопасности в разделе «Требования безопасности» должен быть подраздел «Организационно — технические требования», а также в разделе «Обоснование требований безопасности» ввести подраздел «Обоснование организационно-технических требований». Для реализации указанных предложений необходимо разрабатывать организационно-распорядительные документы, для чего предлагаем в рамках программы «Защита информации 3» поставить работу по созданию программного комплекса автоматизации процесса формированию требований безопасности и правил их реализации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ИСО/МЭК 15408 Информационная технология. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Часть 1 Введение и общая модель, часть 2 Функциональные требования безопасности, часть 3 Гарантийные требования безопасности.

2. Методический документ. Меры защиты информации в государственных информационных системах. Утвержден ФСТЭК России 11.02.2014.
3. Об утверждении требований по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утвержден приказом ФСТЭК России от 11 февраля 2013 г. № 17
4. О некоторых вопросах технической и криптографической защиты информации. Положение о порядке технической защиты информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам. Утвержден Приказом Оперативно-аналитического центра при Президенте Республики Беларусь 30 августа 2013 г. № 62 (в редакции приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 16 января 2015 г. № 3).

СЕКЦИОННОЕ ЗАСЕДАНИЕ «ЗАЩИТА АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ»

ФОРМИРОВАНИЕ ТРЕБОВАНИЙ ДЛЯ ОЦЕНКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЛОЖНЫХ ПРОМЫШЛЕННЫХ ОБЪЕКТОВ

И. И. ЛИВШИЦ
ООО «Газинформсервис»
В. В. МАЛИКОВ
Департамент охраны МВД Республики Беларусь

Методологическая основа обеспечения ИБ

В настоящее время проблема формирования требований для обеспечения безопасности сложных промышленных объектов (СлПО), и прежде всего для объектов топливно-энергетического комплекса (ТЭК) является актуальной для специалистов в области обеспечения информационной безопасности (ИБ). Для лиц, принимающих решения (ЛПР) важно унифицировать совокупность требований, принятых в Российской Федерации (РФ) на законодательном уровне, например: Федеральные законы, Постановления Правительства, Приказ ФСТЭК России № 31. Также представляется целесообразным для формирования современной методологической основы дополнительно применять современные риск-ориентированные стандарты ISO, прежде всего:

- ISO/IEC 27001 — системы менеджмента информационной безопасности;
- ISO/IEC 20000 — системы управления ИТ-сервисами;
- ISO/IEC 22301 — системы менеджмента непрерывностью бизнеса;
- ISO 50001 — системы энергоменеджмента;
- ISO 9001 — системы менеджмента качества.

Указанные нормативные документы совместно формируют современную методологическую основу обеспечения ИБ для СлПО ТЭК.

Актуальная статистика сертификации ISO

На основании доступной статистики сертификации стандартов ISO определим численные показатели статистики по двум основным стандартам — ISO серии 9001 (отчасти как дань традициям) и «целевого» стандарта ISO серии 27001 для обеспечения ИБ. Результаты представлены в таблице 1.

Статистика роста интереса к стандарту ISO 27001

На основании доступной статистики сертификации стандартов ISO, показанной выше, рассмотрим динамику только «целевого» стандарта ISO серии 27001 для обеспечения ИБ. Результаты представлены на рис. 1.

Таблица 1

Статистика сертификации ISO серии 9001 и 27001

Показатель	2010	2011	2012	2013	2014
Стандарт ISO 9001					
Кол-во сертификатов в мире	1118510	1079228	1096987	1129446	1138155
Динамика,%	—	−3,51%	1,65%	2,96%	0,77%
Кол-во сертификатов в Европе	530039	459367	469739	485554	483710
Динамика,%	—	13,33%	2,26%	3,37%	−0,38%
Кол-во сертификатов в РФ	62265	13308	12488	11764	11301
Динамика,%	—	−78,63%	−6,16%	−5,80%	−3,94%
Стандарт ISO 27001					
Кол-во сертификатов в мире	15626	17355	19620	22293	23972
Динамика,%	—	11,06%	13,05%	13,62%	7,53%
Кол-во сертификатов в Европе	4800	5289	6379	7950	8710
Динамика,%	—	10,19%	20,61%	24,63%	9,56%
Кол-во сертификатов в РФ	72	31	27	48	50
Динамика,%	—	−56,94%	−12,90%	77,78%	4,17%

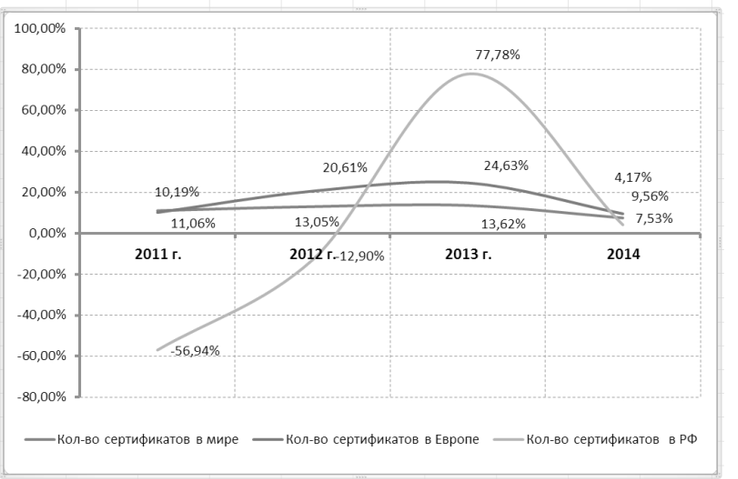


Рис. 1. Динамика сертификации по стандарту ISO 27001

Необходимо отметить существенное отставание в РФ по сертификации СМИБ на соответствие требованиям ISO 27001 в период 2011–2012 гг., однако в 2013 г. наблюдался значительный положительный рост, сохранившийся до 2014 г. Тем не менее, столь значительные колебания графика динамики сертификации по ISO 27001 по сравнению с более спокойными трендами в мире и Европе за аналогичный интервал, не позволяют принимать данный стандарт как единственный отраслевой норматив в области ИБ. Отча-

сти данная динамика характерна для нестабильного рынка углеводородного сырья, когда основное внимание ЛПР приковано к иным приоритетам основной деятельности.

Защита ценных для бизнеса активов

В любой системе менеджмента одним из важнейших вопросов является вопрос корректного выявления перечня активов, для которых требуется обеспечить защиту от актов незаконного вмешательства. Для ТЭК проблему защиты СлПО целесообразно сопоставить с общей проблемой выявления и защиты ценных для бизнеса активов в составе СМИБ. В стандартах ISO изложена четкая логика данного процесса — выделенная совокупность ценных (критичных) активов, намеченных ЛПР к защите в составе СМИБ объектов ТЭК, требует определенных ресурсов (временных, технических, персонал) для оценки уязвимостей, анализа соответствующих угроз, формирования перечня рисков и плана обработки рисков. Справочно можно рекомендовать Приказ ФСТЭК России № 31 (приложение 1) и дополнительно — Постановление Правительства № 304.

Оценка стоимости системы защиты для ценных активов

Для оценки стоимости системы защиты могут быть предложены различные варианты, в частности — простое суммирование всех реализованных мер (средств) обеспечения ИБ, организационных и иных мероприятий, реализованных на конкретном СлПО ТЭК. Однако данный подход не позволяет решить более важную проблему — предоставить ЛПР не просто оценку стоимости некоторой системы защиты (или сопоставления различных вариантов), а дать оценку относительно стоимости защищаемых активов СлПО.

Предлагаемый подход позволит ЛПР оперировать в режиме, близком к режиму реального времени (РРВ) как различными вариантами системы защиты — например, разным перечнем мер (средств) обеспечения ИБ в составе СМИБ, так и перечнем ценных активов, для защиты которых и создается СМИБ. Представляется удобным данный показатель численно определять как отношение двух стоимостей — стоимости мер (средств) обеспечения ИБ в составе СМИБ и стоимости ценных активов в составе СлПО, определенных ЛПР для защиты. Формула для определения такого показателя представлена ниже:

$$К_{СМИБ} = \frac{\frac{И\ тек.}{И\ баз.} \cdot \sum_{i=1}^{m} \sum_{k=1}^{3} M_{ИБ\,ik} \cdot \alpha_{ik}}{\sum_{j=1}^{n} A_j \cdot V_j}$$

Где:

$И_{тек}$ — кол-во выявленных инцидентов ИБ за текущий период;

$И_{баз}$ — кол-во инцидентов ИБ за предыдущий период;

i (1, m) — перечень мер и средств контроля и управления ИБ;

k (1, 3) — виды аудитов (первой, второй и третьей стороной);

$M_{ИБ\,ik}$ — стоимость i-меры и средств контроля и управления ИБ;

α_{ik} — оценка результативности i-меры (средства) контроля и управления ИБ по итогам k-аудита;

j (1, n)– перечень защищаемых активов;

A_j — стоимость защищаемого актива;

V_j– оценка значимости защищаемого актива для бизнеса.

Учет угроз и анализ уязвимостей на объектах ТЭК

Представляется полезным в практике обеспечения ИБ для СлПО ТЭК применять совместно требования Постановления Правительства РФ № 861 (Приложение 1) с переч-

нем типовых угроз стандарта ISO 27005 (Приложение «С»). Также важно, что все упомянутые выше стандарты ISO (в частности, 27001) реализуют замкнутый цикл PDCA, который обеспечивает многовариантные обратные связи в режиме, близком к РРВ для обеспечения ЛПР в необходимой мере достаточным объемом количественных данных (например — метрик ИБ). Дополнительно важно отметить техническую задачу, реализация которой, как правило, отражена только в стандартах ISO (например, п. 7.5.3 в ISO 27001 и п. 4.6.5 в ISO 50001 соответственно) — управление записями в СлПО ТЭК. В частности, должны выполняться требования для обеспечения защиты важных записей при предоставлении информации об угрозе, в зависимости от способа (средств): телефонной связи, радиосвязи, электронной или факсимильной связи (соответственно, п.п. 9 и 10 Постановления Правительства РФ № 861).

Анализ уязвимостей в соответствии с Приказом ФСТЭК России № 31 включает анализ уязвимостей средств защиты информации, технических средств и ПО. Среди методов оценки технических уязвимостей отметим методы тестирования ИС для выявления уязвимостей:

- Тестирование и оценка безопасности;
- Тестирование на проникновение;
- Проверка кодов.

В частности, в ст. 9 Приказа ФСТЭК России № 31 определено, что паспорт, признанный по результатам актуализации подлежащим замене и утратившим силу, хранится в порядке, установленном субъектом ТЭК, в течение 25 лет. Это положение также соответствует требованиям, соответственно, п. 9.3 в ISO 27001 и п. 4.7 в ISO 50001 по анализу со стороны руководства («Management Review»).

Требования по выполнению проверок (аудитов) СлПО ТЭК

Отметим, что в Приказе ФСТЭК России № 31 многократно отмечается важная роль ISO 27001 (даны прямые ссылки, соответственно, на п.п. 13.4 и 15.2). Кроме того, в стандартах ISO установлены требования по выполнению проверок (аудитов) активов СлПО ТЭК (соответственно, в п. 9.2 в ISO 27001 и п. 4.6.3 ISO 50001). Наиболее важные проверки на объектах ТЭК установлены Приказом ФСТЭК России № 31 и, дополнительно ISO 27001.

Таким образом, для оценки ИБ для СлПО ТЭК представляется целесообразным выполнение совместно требований ФСТЭК России и, дополнительно, современных риск-ориентированных стандартов ISO, прежде всего серии 27001.

ОЦЕНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ ЭНЕРГЕТИЧЕСКИХ СИСТЕМ

М.Н. БОБОВ, Д.Г. ГОРЯЧКО, А.А. ОБУХОВИЧ

ОАО «АГАТ-системы управления» — управляющая компания холдинга «Геоинформационные системы управления»

В энергетических системах наиболее тяжелыми и требующими длительного времени восстановления событиями являются системные аварии, вызванные возникновением многочастотного асинхронного режима, лавинообразным снижением частоты и напряжения, и в конечном итоге, прекращением энергоснабжения всех потребителей.

Оценка информационной безопасности событий, приводящим к системным авариям, включает два этапа:

– определение перечня возможных системных аварий;
– оценка рисков нарушения информационной безопасности объектов, приводящих к системным авариям.

Перечень возможных системных аварий определяется путем формирования математической модели и проведением расчетов исследуемой энергетической системы с применением соответствующего специализированного программного обеспечения.

Исходными данными для моделирования являются:

– структура энергетической системы или ее части;
– режимы работы системы;
– характеристики объектов системы;
– характеристики используемых в системе средств противоаварийной автоматики и средств частотной разгрузки системы;
– сценарии несанкционированных воздействий на оборудование объектов системы;
– характеристика системной аварии (полное или частичное погашение системы, погашение отдельного объекта).

Моделирование системных аварий, вызванных несанкционированными воздействиями, осуществляется путем расчета установившихся и переходных процессов в системе.

В результате моделирования по каждой системной аварии определяется перечень объектов генерации и/или распределения системы с указанием перечня присоединений, несанкционированное отключение которых приводит к рассматриваемым последствиям.

На втором этапе производится оценка рисков, связанных с нарушениями функционирования объектов энергосистемы и приводящих к системным авариям.

Для получения оценки риска каждой из приведенных выше системных аварий применяется метод, основанный на выявлении и дедуктивном анализе критических событий.

Согласно этому методу каждое критическое событие представляется как совокупность опасных (причинных) событий, обуславливающих его наступление.

Для оценки вероятности реализации критических событий проводится их иерархическая декомпозиция, как по месту возникновения составляющих опасных событий, так и по факторам, обуславливающим их возникновение.

В частности, декомпозиция по месту возникновения опасных событий может предусматривать последовательную детализацию системной аварии по следующим уровням:

первый — по объектам системы;

второй — по оборудованию объектов системы;

третий — по элементам оборудования объектов системы.

Причем, при переходе к более низкому уровню иерархии угрозы верхнего уровня рассматриваются как опасные события для низкого уровня.

Декомпозиция по причинам возникновения производится одновременно с декомпозицией по месту возникновения.

На каждом из приведенных уровней могут быть выявлены полные группы причин, вызывающих системную аварию. К таким причинам относятся:

– отказы элементов оборудования;
– алгоритмические ошибки;
– нарушения информационной безопасности;
– прочие причины.

Опасные события информационной безопасности по каждой из причин определяются дедуктивным образом и представляются в виде древовидной схемы, которая отображает их логическую взаимосвязь с конечным событием.

На втором уровне декомпозиции угрозы первого уровня рассматриваются в качестве опасных событий второго уровня. В качестве их причин определены угрозы нарушения информационной безопасности, обусловленные воздействиями на оборудование на объектах системы.

Расчетные формулы для определения вероятностей реализации угроз определяются перечнем составляющих их угроз следующего (более низкого) уровня и их отношениями (зависимые или независимые события) друг с другом.

Итерационная процедура анализа выполняется для каждого уровня декомпозиции с учетом следующих условий:

- совокупность составляющих событий более низкого уровня должна обеспечивать наступление события более высокого уровня;
- составляющие события на каждом уровне представляют собой конечное множество событий, которое является полной группой событий.

Низший уровень декомпозиции определяется исходя из следующих правил:

- каждая из угроз низшего уровня самостоятельно не приводит к ущербу, а лишь создает необходимые для этого условия;
- каждая из угроз низшего уровня не нуждается в дальнейшей декомпозиции для ее оценки;
- вероятность реализации каждой из угроз низшего уровня может быть оценена;
- расчет вероятности угроз низшего уровня производится за заданный (равный для всех событий) интервал времени.

Оценка вероятности критического события осуществляется на основе комбинированного метода, заключающегося в обязательном проведении качественной и количественной (детальной) оценки риска для угроз низшего уровня, последующего расчета вероятностей причинных событий и на их основе вероятности критического события. При этом, определение расчетных формул для вычисления вероятностей конечного и причинных событий производится на каждом уровне декомпозиции.

Проведение по предлагаемой процедуре анализа системных аварий и оценки риска информационной безопасности в энергетической системе позволяет определить:

- оценку риска системной аварии как в энергосистеме, так и по каждому задействованному в ней объекту энергосистемы;
- условия и причины возникновения системных аварий;
- сценарии нарушений информационной безопасности на объектах, приводящие к системным авариям;
- наиболее опасные уязвимости в автоматизированных системах управления объектов энергетики, способствующие реализации угроз, приводящих к системным авариям;
- вклад рассматриваемых на каждом уровне декомпозиции факторов в итоговую оценку риска системной аварии, что особенно важно при его обработке;
- актуальные требования по предотвращению (снижению вероятности реализации) угроз и снижению риска информационной безопасности до приемлемого уровня на объектах энергетической системы.

Рассмотренный метод оценки информационной безопасности энергетических систем имеет следующие достоинства:

– предоставление строгого, систематизированного и в то же время гибкого подхода, позволяющего анализировать результаты воздействия разнообразных факторов, включая случайные и преднамеренные воздействия персонала объекта системы и отказы оборудования (программные сбои);
– применение подхода «сверху вниз» позволяет рассматривать и учитывать в оценке только те воздействия, которые связаны с конечным событием — причинением ущерба.

К ВОПРОСУ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ОТРАСЛЕВЫХ ИНФРАСТРУКТУР

Э. П. КРЮКОВА
Государственное предприятие НИИ ТЗИ

Критически важные объекты (далее — КВО) входят в состав социальных, производственных, инженерных, транспортных, энергетических, информационно-коммуникационных и иных инфраструктур, нарушение функционирования которых может оказать существенное влияние на принятие органами власти политических и управляющих решений, устрашить население, дестабилизировать общественный порядок, причинить вред здоровью населения или окружающей среде, значительный материальный ущерб, создать угрозу национальной безопасности.

Широкое внедрение вычислительной техники в системах управления технологическими и производственными процессами, системах контроля и управления безопасностью, в автоматизированных информационных системах организационного управления, системах физической защиты, их взаимодействие в критических инфраструктурах через локальные, корпоративные и иные сети расширило возможности и эффективность оперативного управления КВО и критически важными инфраструктурами, одновременно повысив их уязвимость к угрозам различного рода.

Характер угроз, инициируемых различными факторами, базируется главным образом на злоумышленных действиях человека или группы людей, имеющих конкретную целевую направленность. Несанкционированный доступ, хищение, искажение, перехват, другие противоправные действия в отношении охраняемой информации на КВО способствуют ее успешному использованию для организации компьютерных атак на критически важные системы контроля и управления, саботажа в отношении его критических активов, террористических актов в отношении персонала, диверсионных актов другим правонарушениям.

Большая часть критической информации, хранящейся на различных носителях, обрабатываемой в автоматизированных информационных системах, передаваемой по сетям не всегда правильно идентифицируется по уровню критичности, а информация высокой критичности не всегда получает адекватную защиту.

К охраняемой информации на КВО следует отнести:
– информацию о системе организационного управления, в том числе бизнес-информацию (о персонале, локальные нормативные акты, контракты и т. д.);

- техническую информацию, описывающую все аспекты проекта КВО, испытаний, эксплуатации, технического обслуживания его систем и оборудования, расположения критически важных активов и др.;
- технологическую информацию, генерируемую в ходе управления технологическими процессами (нормальная эксплуатация);
- оперативную информацию, получаемую от систем контроля и управления, важных для безопасности КВО, систем физической защиты и др.;
- информацию о КВО, представляемую в средствах массовой информации.

При организации защиты информации на КВО должны рассматриваться следующие основные группы взаимосвязанных целей обеспечения безопасности КВО:

- информационная безопасность КВО — защита конфиденциальности информации;
- компьютерная безопасность КВО — защита ресурсов компьютерных систем, обеспечение целостности, доступности информации, которая является результатом функционирования компьютерных систем, преобразующих сигналы датчиков процессов в команды для управления системами и оборудованием и в информацию для принятия решений операторами (защита критической информации);
- физическая безопасность — предотвращение несанкционированного доступа в зоны, где генерируется критическая информация и/или находятся автоматизированные системы и технические средства ее обработки и хранения.

В настоящее время в связи с участившимися сетевыми атаками на системы контроля и управления критически важными инфраструктурами выделяется новое направление в проблеме обеспечения компьютерной безопасности КВО — кибернетическая безопасность.

Обеспечение кибернетической безопасности КВО требует новых подходов:

- повышения готовности персонала КВО к компьютерным атакам, разработки правил поведения в кибернетическом пространстве, повышения ситуационной осведомленности субъектов, в ведении которых находятся сегменты трансграничных критических инфраструктур;
- создания надежных механизмов защиты от сбоев и отказов в системах управления безопасностью КВО ключевых трансграничных инфраструктур, снижения времени реагирования механизмов безопасности на инциденты, предупреждения или смягчения последствий инцидентов и аварий;
- организации непрерывно функционирующей и надлежащим образом управляемой системы мониторинга угрожающих факторов, начиная от раннего обнаружения, распознавания источника и характера атаки, возможного ее предупреждения, предотвращения, оповещения соответствующего персонала КВО.

При этом особо актуальной является упреждающая или проактивная защита архитектуры контроля и управления безопасностью КВО от компьютерных атак.

Анализа статистики нарушений безопасности КВО в пределах некоторой отраслевой инфраструктуры или их аналогов в смежных отраслях недостаточно, чтобы принимать решения при обосновании безопасности конкретного КВО. Одним из важнейших условий обеспечения готовности КВО к упреждающему реагированию на угрозы безопасности должна стать интеграция возможностей структур государственного и коммерческого секторов по сбору информации об угрозах безопасности КВО трансграничных отраслевых инфраструктур, возможных направлениях, целях, мощности предполагаемых атак, возможных последствиях, способах противодействия и др.

Возможные направления обмена информацией между государственным и коммерческим секторами (примеры)

Государственный сектор	Коммерческий сектор
Знания о возможностях кибернетических атак ключевых террористических организаций	Информация о крупных категориях активов в энергетическом секторе (например, данные по газу, нефти, электроэнергии, возобновляемым источникам энергии; показатели надежности; информация о торговых операциях с энергией)
Информация о связях между разными террористическими и не террористическими группами	Информация о технических уязвимостях определенных продуктов программного и аппаратного обеспечения, используемого операторами критической инфраструктуры
Знания о векторах прошлых атак	Анонимная информация о виде и последствиях прошлых атак
Знания о возможных векторах будущих атак, полученные из анализа подпольных веб-сайтов кибернетических преступных групп	Данные о потребностях восстановления КВО и инфраструктуры, возникающих в результате разных видов и форм атак. Данные о схемах атак в других важнейших секторах инфраструктуры, которые могут служить признаками раннего предупреждения для энергетического сектора

Самым надежным источником информации об угрозах критическим инфраструктурам являются разведывательные органы. Они собирают и анализируют данные с целью предоставления новейшей и самой достоверной информации, необходимой для реалистической оценки угроз национальной безопасности.

Совместное использование такой информации и координация мероприятий по обеспечению безопасности КВО трансграничных критических инфраструктур требует создания на уровне Союзного государства Компетентного независимого органа (Центра), который обладал бы, в частности, полномочиями для сбора, обобщения, предоставления такой информации, оповещения об актуальных угрозах, координации совместных мероприятий по реагированию на них, организации взаимопомощи в восстановлении функционирования КВО, участия в исследовании инцидентов, в поиске и преследовании нарушителя.

При разработке и эксплуатации систем контроля и управления, важных для безопасности КВО, следует переходить на стандарты Международной электротехнической комиссии, которые содержат четкие, проверенные практикой требования, ориентированные на обеспечение надежности функционирования и безопасности КВО при использовании компьютерных систем и в настоящее время вводятся и в Республике Беларусь, и в Российской Федерации.. Эти стандарты устанавливают единый подход к проектированию архитектуры безопасности КВО — проектирование «сверху вниз», при котором эта архитектура создается как «система систем», требования к качеству и надежности функционирования которой устанавливаются и контролируются уполномоченными государственными органами..

Критически важные системы контроля и управления, составляющие архитектуру безопасности КВО, должны иметь встроенную защиту, направленную на реализацию заданных в обосновании безопасности КВО функций. Качество их разработки и реализации должно контролироваться на всех этапах жизненного цикла каждой системы.

В зарубежной практике коммерческие продукты информационных технологий категорически запрещены для использования в критически важных приложениях на КВО. Продукты информационных технологий, в частности, компьютерные системы и их компоненты, сертифицированные на основе стандартов серии «Общие критерии», проекти-

руются «снизу вверх», т.е. с ориентацией на потребности и возможности заказчика, аттестуются по его техническим условиям. При необходимости их использования они должны быть в обязательном порядке проанализированы и протестированы уполномоченными государственными органами на соответствие требованиям компьютерной безопасности и обеспечивать соответствующий уровень надежности функционирования КВО.

Непременным условием выдачи лицензии на право ввода КВО в эксплуатацию должно стать предоставление обоснования его информационной и компьютерной безопасности, разрабатываемое совместно специалистами эксплуатирующей организации с привлечением внешних экспертов по безопасности и представителей уполномоченных государственных органов, и включение в декларацию промышленной безопасности КВО раздела, посвященного его информационной и компьютерной безопасности.

РАЗРАБОТКА СИСТЕМ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ЭНЕРГЕТИЧЕСКОЙ ОТРАСЛИ

М.Н. БОБОВ, Д.Г. ГОРЯЧКО, А.А. ОБУХОВИЧ
ОАО «АГАТ-системы управления» — управляющая компания холдинга «Геоинформационные системы управления»

Система менеджмента информационной безопасности (СМИБ) является частью общей системы управления организации (предприятия), основана на оценке рисков и предназначена для организации, эксплуатации, мониторинга и совершенствования системы обеспечения информационной безопасности (СОИБ) и представляет собой модель для создания, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения защиты информационных активов, включающую в себя организационную структуру и комплект документов.

Необходимость разработки СМИБ критически важных объектов информатизации (КВОИ) определена ТКП 483–2013 «Информационные технологии и безопасность. Безопасная эксплуатация и надежное функционирование критически важных объектов информатизации. Общие требования».

Структура СМИБ и требования к ее реализации определены СТБ ISO/IEC 27001–2011 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» и СТБ ISO/IEC 27002–2012 «Информационные технологии. Методы обеспечения безопасности. Кодекс практики для менеджмента информационной безопасности».

Создание организационной структуры СМИБ является итерационным процессом, начинающимся с поручения конкретным исполнителям подготовить «План мероприятий по созданию и внедрению СМИБ» и завершающийся (если не учитывать последующие улучшения) при утверждении комплекта документов, регулирующих процессы обеспечения информационной безопасности в организации.

Верхний уровень организационной структуры СМИБ составляют руководство областной организации энергетической отрасли (Облэнерго) и руководители предприятий– владельцев КВОИ, входящих в ее структуру.

Руководство Облэнерго берет на себя ответственность за:

– принятие стратегических решений по вопросам обеспечения защиты информации в организации;
– координации действий предприятий– владельцев КВОИ, входящих в структуру организации, при планировании и выполнении мероприятий по разработке и внедрению документов СМИБ;
– утверждения основополагающих документов СМИБ;
– выделения соответствующих материальных и кадровых ресурсов для обеспечения функционирования систем защиты информации КВОИ;
– организации обучения и повышения квалификации специалистов КВОИв сфере информационной безопасности.

Руководители предприятий — владельцев КВОИ организуют работы и несут ответственность за разработку и внедрение документов СМИБ.

Второй уровень организационной структуры СМИБ составляет подразделение технической защиты информацииорганизации, которое организует методическое руководство, координацию разработки и внедрения документов СМИБ на предприятиях — владельцах КВОИ.

Нижний уровень организационной структуры составляют администраторы защиты информации КВОИ.

Комплект документов СМИБ организации условно разделяется на следующие категории:

– организующие документы;
– документы, регламентирующие процессы;
– документы для персонала.

Организующие документы, утверждаемые руководством Облэнерго:

– политика информационной безопасности организации;
– регламент функционирования СМИБ КВОИорганизации;
– положение по разделению информационных ресурсов КВОИ по категориям доступа;
– правила разграничения доступа в КВОИ;
– модель угроз информационной безопасности в КВОИ;
– основные положения системы управления информационными рисками в КВОИ;
– методика оценки рисков информационной безопасности в КВОИ.

Документы, регламентирующие процессы на конкретных КВОИ:

– инструкция по обеспечению защиты информации;
– инструкция о порядке применения средств защиты информации
– программа и методики проверок СОИБ КВОИ в процессе эксплуатации;
– положение об антивирусном контроле;
– положение об использовании носителей информации;
– положение о резервном копировании информации;
– положение о гарантированном уничтожении информации с носителей;
– правила реагирования на инциденты информационной безопасности;
– порядок расследования инцидентов информационной безопасности;
– методика мониторинга среды функционирования и анализа уязвимостей.

Документы для персонала КВОИ:

– порядок оповещения ответственных за функционирование КВОИ лиц в случае обнаружения нарушений информационной безопасности;
– инструкция по использованию информационных активов КВОИ.

Отличительной особенностью автоматизированных систем управления технологическими процессами, отнесенных впоследствии к КВОИ, разработка и внедрение которых проводилась зарубежными фирмами или собственными силами предприятий — владельцев КВОИ, является практическое отсутствие эксплуатационной документации, позволяющей однозначно идентифицировать состав технических средств, программного обеспечения и обрабатываемую информацию КВОИ. Поэтому в состав документации целесообразно включить группу документов, идентифицирующих КВОИ.

Документы, идентифицирующие КВОИ:

- формуляр КВОИ;
- схема электрическая функциональная КВОИ;
- описание информационных процессов КВОИ;
- реестр информационных активов КВОИ.

СЕКЦИОННОЕ ЗАСЕДАНИЕ «ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ»

АКТУАЛЬНЫЕ ПРОБЛЕМЫ БЕЗОПАСНОСТИ ВЕДОМСТВЕННЫХ РАДИОСЕТЕЙ

А. В. НОСКОВ

Радиосвязь является основным видом связи с подвижными объектами, обеспечивающим управление органами и подразделениями правоохранительных и силовых ведомств, а в ряде случаев единственным видом связи, обеспечивающим оперативное управление подразделениями при осложнении оперативной обстановки, при ликвидации последствий стихийных бедствий. Важным преимуществом радиосвязи является ее высокая мобильность, то есть возможность изменения состава сети радиосвязи или полное ее перемещение без нарушения работоспособности. Применение радиосвязи позволяет сконцентрировать в минимальные сроки и в нужном месте необходимое количество сил и средств для проведения мероприятий, согласовать по времени их действия и осуществлять единое руководство. Требования к качеству функционирования сетей радиосвязи как составной части систем управления растут постоянно, адаптируясь к быстро меняющимся условиям эксплуатации.

Обеспечение безопасности при ведении переговоров в радиосистеме встает на первое место, когда передаваемая информация имеет конфиденциальный характер или является информацией ограниченного доступа, что особенно актуально, в первую очередь, для государственных ведомств. Поэтому при проектировании и внедрении ведомственных сетей радиосвязи немаловажным аспектом являются вопросы безопасности. Для организации ведомственных радиосетей специализированного пользования можно использовать сухопутную подвижную радиосвязь на основе конвенциональных радиосетей, транкинговых систем связи. Значительные преимущества транкинговых систем (высокая пропускная способность, степень защищенности от несанкционированного доступа) ставили бы их вне конкуренции, однако экономическая составляющая внедрения таких систем сводит на нет все технические преимущества.

Грамотно спроектированная и аккуратно реализованная радиосистема стандарта DMR сможет существенным образом расширить функциональные возможности как самой радиосистемы, так и ее безопасность. IP Site Connect, Capasity Plus и Linked Capacity Plus являются специализированным вариантом построения конвенциональной цифровой сети радиосвязи с использованием ретрансляторов и абонентского оборудования MOTOTRBO и предоставляют пользователям выбор для создания радиосетей в которых невысокие затраты на создание базовой инфраструктуры сочетаются с возможностью использовать преимущества стандарта DMR на большой территории. Для передачи голоса и данных в сети IP Site Connect используется технологии пакетной коммутации IP, что упрощает подключение базового оборудования к каналам TCP/IP, и позволяет быстро интегрировать радиосеть в существующие системы локальной передачи информации.

Для исключения доступа к базовой инфраструктуре посторонних радиоабонентов в Capasity Plus и Linked Capacity Plus возможно использование функций «Ограничение доступа к системе» и «Проверка ID радиостанции».

«Ограничение доступа к системе» базируется на использовании специального кода длиной до 24 знаков, который программируется в ретрансляторы и абонентские радиостанции. Только в случае идентичности этого кода, радиостанция получает возможность работать с ретрансляторами. Дополнительным ограничением на использование базовой инфраструктуры системы является «Проверка ID радиостанции» на принадлежность к заранее определенному диапазону ID, который также программируется в ретрансляторах. Более гибкую возможность блокировки работы радиоабонентов по принципу «белый список» или «черный список» предоставляет диспетчерское ПО SmartPTT. Список формируется на радиосервере SmartPTT независимо от настроек «Ограничение доступа к системе» и «Проверка ID радиостанции». Таким образом, возможно одновременное использование трех указанных выше функций, что позволяет надежно защитить радиосеть от несанкционированного использования.

Для исключения доступа к базовой инфраструктуре посторонних радиоабонентов в Connect Plus используется несколько механизмов проверки абонентской радиостанции:

- Первый уровень базируется на проверке идентификационного кода системы ID_SYS — данный код должен совпадать в радиостанциях и сайтовых контроллерах системы.
- Вторым механизмом является проверка идентификационного кода радиостанции ID_RADIO на принадлежность к заранее определенному диапазону ID, который также программируется в сайтовых контроллерах.
- Третий уровень ограничения использует проверку электронного серийного номера радиостанции ESN, который является уникальным, программируется на заводе и не может быть изменен пользователем. В памяти сайтового контроллера создается таблица соответствия ESN и ID_RADIO, по которой проводится проверка радиостанции.
- Четвертый механизм — проверка принадлежности радиостанции к определенной группе TalkGroup_ID, которая может быть обслужена системой на определенном сайте.

Сочетание всех четырех способов проверки гарантирует, что только авторизованные радиостанции получат доступ к базовой инфраструктуре и сервисам системы Connect+.

Для защиты радиопереговоров от несанкционированного прослушивания абонентские радиостанции MOTOTURBO имеют встроенный маскиратор речи (шифрование радиоканала): базовый и расширенный режим. Базовый режим шифрования обеспечивает возможность скремблирования голоса, а также выбор из 255-ти ключей одного 16-бит ключа шифрования. Расширенный режим шифрования позволяет осуществить выбор из 16-ти уникальных ключей одного 40-бит ключа шифрования. Ключи «привязываются» к псевдониму абонента, что позволяет в одной радиосети создать несколько ключевых групп работающих на разных ключах;

Системы связи между ретрансляторами по протоколу IP обеспечивают опционную аутентификацию всех пакетов, передаваемых между устройствами системы связи. Функция «закрытый VPN-туннель» позволяет сконфигурировать систему с использованием VPN маршрутизаторов для подключения узловых устройств сети. Пакетная аутентификация защищает от несанкционированного доступа других устройств из IP-сети,

каждый пакет содержит криптографическую подпись (алгоритм Keyed-Hash Message Authentication Code (HMAC)).

Таким образом, в подобных радиосистемах реализованы следующие меры защиты информации:

1. На уровне физической безопасности:
   Все оборудование размещено в контролируемой зоне с исключением возможности бесконтрольного доступа посторонних лиц к техническим и программным средствам.
2. На уровне сетевой безопасности:
   2.1. Шифрование беспроводной сети передачи данных.
   2.2. Применение списков контроля доступа.
   2.3. Использование защищенного канала передачи между ретранслятором и сервером — VPN-туннель.

Для организации дополнительной защиты информации предполагается применение и средств организации VPN-туннелей с использованием белорусских криптографических алгоритмов. Данные возможности предоставляют программно-аппаратные продукты разрабатываемые белорусскими компаниями («С-Терра Бел», НИИ ТЗИ).

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ПРОТОКОЛОВ SSL/TLS

Д.А. КУЗЬМИЦКИЙ, А.Ю. ЖМАКОВ

Введение

После смерти в 2014 году SSLv3 лозунг «Откажись от SSLv3» стал для системных администраторов одним из основных. Однако несмотря на это значительное число систем остаются уязвимыми к различным атакам на протоколы SSL/TLS в то время как администраторы полагают, что системы защищены. В данной статье приводится краткий обзор проблем безопасности, которые значительно ослабляют информационные системы. При этом основная причина возникновения данных проблем — ошибки администрирования. Многие все еще пытаются оживлять SSLv3 и даже SSLv2 полагая, что они повышают удобство работы для клиентов.

Взлом TLS при помощи SSLv2 (атака DROWN)

DROWN — это новая межпротокольная атака, которая позволяет расшифровать пассивно записанные сессии между клиентами, использующими новейшую версию протокола TLS, и сервером, поддерживающим устаревшую версию SSLv2, при этом сервер выступает в качестве оракула заполнителя (padding) для алгоритма RSA. Типичный сценарий предполагает, что атакующий наблюдает 1 000 установлений соединений по протоколу TLS, затем сам устанавливает 40 000 соединений по протоколу SSLv2 и производит 250 вычислительных операций для дешифрования шифртекста RSA длиной 2048 бит. При этом жертва атаки никогда не устанавливает соединения по протоколу SSLv2. Согласно исследованиям авторов атаки [1], по состоянию на 1 марта 2016 года около 33 % всех HTTPS-серверов и около 22 % имеющих сертификаты, которым доверяют браузеры, были уязвимы к атаке DROWN ввиду повсеместного повторного использования закрытых ключей и сертификатов.

Сервер уязвим к атаке DROWN, если он допускает подключение к нему с использованием протокола SSLv2. Это на удивление распространенное явление вследствие неправильной настройки или некорректных значений по умолчанию для выбора используемых протоколов.

Также сервер уязвим к атаке DROWN, если его личный ключ используется каким-либо другим сервером (или этим же сервером, но для другого сервиса), допускающим подключение к нему с использованием протокола SSLv2. Эта ситуация становится возможной ввиду такого явления, как использование одного и того же сертификата для разных сервисов (например, для HTTPS и SMTP). Зачастую компании излишне экономят на сертификатах, а администраторы не придают должного внимания необходимости использования различных сертификатов для различных сервисов или серверов.

Несовершенная секретность

Анализ безопасности использования протокола согласования ключа на основе алгоритма Диффи-Хеллмана показал, что этот протокол менее безопасен, чем многие полагают. Так, Logjam — это атака на протокол TLS, которая позволяет с использованием метода «человек посередине» заставить атакуемого снизить требования к параметрам до использования «экспортного» варианта алгоритма Диффи-Хеллмана. Экспортный вариант алгоритмов — это устаревшее понятие, так как ограничения на экспорт криптографии были существенно снижены США в 2000-м году. Несмотря на снятие ограничений, многие библиотеки и программы по-прежнему поддерживают «экспортные» варианты алгоритмов. Для алгоритма Диффи-Хеллмана длина ключа в «экспортном» варианте составляет 512 бит. Усугубляет ситуацию то, что практически во всех реализациях протокола используются одни и те же группы. Данный факт позволяет провести предварительные вычисления для обеспечения последующего дискретного логарифмирования за приемлемое время. Более того, в статье [4] утверждается, что предварительное вычисление логарифмов от 768- и даже 1024-битовых ключей под силу, например, многим государствам. При этом малое количество фиксированных или стандартизованных групп используется миллионами серверов. Например, предварительное вычисление для одной 1024-битной группы позволит пассивно прослушивать порядка 18 % популярных HTTPS-сайтов.

Вред устаревшей криптографии

За последние годы наблюдалось значительное количество серьезных атак, которые использовали устаревшую или отжившую криптографию. Многие из скомпрометированных протоколов или криптографических примитивов на удивление широко распространены в развернутых системах даже спустя десятилетия после того, как была продемонстрирована их слабость. Например, атака DROWN фактически является модификацией атаки 18-летней давности, в которой использовалась слабость некоторых комбинаций алгоритмов и протоколов, к тому времени уже имевших более стойкую замену. Это также касается таких знаменитых криптографических функций как MD 5, SHA-1 и RC 4. Многие полагают, что известность и распространенность какой-либо функции — это залог ее стойкости. Разработчики систем, использующих SSL/TLS зачастую выбирают легковесность реализации вместо безопасности. Например, некоторые почтовые сервера даже сейчас по умолчанию используют MD 5 в качестве хэш-функции для TLS. Результаты, опубликованные еще в 2012 году в работе [5], привели к осознанию необходимости запрета использования функции MD 5 в сертификатах X.509, при этом использование MD 5 в самих протоколах установления соединения все еще допускается. Лучшие атаки

на MD 5 по поиску коллизии с использованием заданного префикса имеют трудоемкость 239 выполнений MD 5, а с использованием общего префикса — всего 216 выполнений MD 5 [5].

Хотелось бы обратить особое внимание на необходимость ухода от устаревших и запрещенных технологий до того, как они превратятся в источник уязвимостей для систем. В качестве реакции на многие из упомянутых уязвимостей разработчики браузеров начали активно предупреждать конечных пользователей о том, что при установлении соединения TLS согласовываются нестойкие параметры, включая сертификаты с хеш-суммами по алгоритмам MD 5 или SHA-1, короткие длины ключей для алгоритмов RSA и Диффи-Хеллмана, соединения с использованием SSLv3. Разработчики ставят превыше всего удобство использования и обратную совместимость, поступаясь ими только при наличии практических атак. Данная ситуация разительно отличается от процесса обнаружения криптографических уязвимостей, когда малейшие подозрения на возможное уменьшение стойкости, будучи при этом далекими от практического воплощения, служат сигналом возможных проблем в будущем.

Одним из возможных долгосрочных решений служит упреждающее удаление всех устаревших и запрещенных технологий. Одним из положительных движений в этом направлении может служить процесс разработки TLS 1.3, в котором полностью удалено согласование ключа по алгоритму RSA, а согласование ключа по алгоритму Диффи-Хеллмана ограничено несколькими большими группами, позволяющими противостоять криптоанализу как в ближайшем, так и в отдаленном будущем. В своих требованиях форум CA/Browser предписывает [2] отказаться от использования SHA-1 к концу 2016 года, а также запретить выдачу сертификатов более чем на 39 месяцев вне зависимости от цели использования. Появились ресурсы [3], которые помогают администраторам лучше понять принципы настройки систем безопасности (таких как TLS), собирая лучшие практики настройки в одном месте. Это избавляет администраторов от необходимости долгих поисков устаревших или слабых настроек в их системах, концентрируя их внимание на текущих актуальных наборах параметров и настроек.

Заключение

Из сказанного выше можно сделать простой вывод: попытка компромисса между безопасностью и совместимостью часто приводит к проблемам в безопасности. Невозможно защититься от всего, но защищаться от уже выявленных угроз нужно. Невозможно учесть все, но учитывать в настройках по умолчанию явные атаки или слабости нужно. Невозможно быстро избавиться от наследия устаревших технологий, но при переходе на новые технологии нужно максимально дистанцироваться от них.

Описанные в данной статье проблемы в основном становятся возможными при недостаточном понимании администраторами систем грани дозволенного при обеспечении поддержки устаревших технологий. К сожалению, можно констатировать факт, что не всегда руководства пользователей для соответствующих сервисов (например, почтовых серверов) содержат внятное и актуальное объяснение порядка настройки систем безопасности, включая TLS. Значительное число неофициальных кратких руководств, содержащих описание порядка настройки до работоспособного состояния, почти никогда не уделяют внимания безопасности, но наоборот, указывают как быстро сделать самоподписанный сертификат для TLS, отключить «ненужную» проверку соответствия сертификата или списка отозванных сертификатов. Лозунги в стиле «лучше дать пользователю плохую криптографию, чем передавать данные в открытом виде» вообще выбивают почву из-под

ног безопасности, ведь подобные настройки в конечном итоге приводят к ложному ощущению безопасности, которая может вообще не обеспечиваться.

ЛИТЕРАТУРА

1. DROWN: Breaking TLS using SSLv2. URL: https://drownattack.com.
2. Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates. / CA/Browser Forum. URL: https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.3.4.pdf.
3. Applied Crypto Hardening / Breyha, W., Durvaux, D., Dussa, T., Kaplan, L. A. et al . — 2016. — April. URL: https://bettercrypto.org/static/applied-crypto-hardening.pdf.
4. Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice / Adrian, D., Bhargavan, K., Durumeric, Z., Gaudry, P. et al // In Proceedings of 22nd ACM Conference on Computer and Communications Security / Oct. 2015. URL: https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf.
5. Stevens, M., Lenstra, A. K. Chosen-prefix collisions for MD 5 and applications // IJACT, 2(4):322–359, 2012.

ПРОБЛЕМА АТТЕСТАЦИИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НАЦИОНАЛЬНОЙ ГРИД-СИСТЕМЫ РЕСПУБЛИКИ БЕЛАРУСЬ

А.Б. СТЕПАНЯН, В.А. ДМИТРИЕВ, Е.П. МАКСИМОВИЧ, В.К. ФИСЕНКО
ОИПИ НАН Беларуси

Доклад посвящен анализу существующей системы защиты информации национальной Грид-сети «СКИФ» Республики Беларусь и выявлению основных направлений ее дальнейшего развития и совершенствования с целью удовлетворения всех необходимых требований действующего законодательства РБ в области защиты информации и последующей аттестации системы в установленном порядке [1–2].

Национальная Грид-сеть РБ предназначена для решения сложных задач, которые связаны с выполнением ресурсоемких расчетов или обработкой больших объемов данных и не допускают эффективного решения в рамках традиционных информационных технологий. К таким задачам относятся, например, задачи моделирования промышленных изделий и процессов, управления сложными технологическими процессами в авиа- и автомобилестроении, атомной промышленности, ракетно-космической отрасли, задачи криптографии, медицинской диагностики, разработки новых лекарственных средств, имитационного моделирования биологических процессов, управления чрезвычайными ситуациями и многие другие.

В качестве основной платформы для построения национальной Грид-сети РБ разработчики выбрали программное обеспечение UNICORE, представляющее собой набор веб-сервисов и технологий для организации высокопроизводительной вычислительной сети. В качестве криптографических средств защиты используется OpenSSL — криптографический пакет с открытым исходным кодом для работы с SSL/TLS.

Выбор программного обеспечения UNICORE был обусловлен следующими его преимуществами:

- обеспечивает поддержку большого числа операционных и пакетных систем (написано на языке Java, что гарантирует его выполнение в любой операционной системе, для которой существует интерпретатор этого языка (Windows, Linux, Mac OS и т.д.));
- распространяется бесплатно, исходные тексты доступны под свободной лицензией GPL, что позволяет их свободное копирование, модификацию и удешевляет процесс разработки;
- характеризуется гибкостью, что предоставляет благоприятные возможности для дальнейшего развития пока недостаточно обширной функциональности UNICORE;
- базируется на общепринятом открытом стандарте OGSA (Open Grid Services Architecture), описывающем сервис-ориентированную архитектуру построения Грид-систем;
- обладает достаточно развитой системой обеспечения информационной безопасности;
- предоставляет широкие возможности для обеспечения легкой инсталляции, конфигурирования, администрирования и мониторинга системы, позволяет объединить множество разнородных вычислительных ресурсов (кластеров организаций).

UNICORE просто в использовании для широкого круга пользователей. Имеет несколько различных законченных клиентов с удобными консольными и графическими интерфейсами, обеспечивающими однородный доступ к различным системам и эффективное взаимодействие пользователя с ресурсами вычислительной сети.

Система защиты информации UNICORE реализует следующие основные функции безопасности:

- идентификация и аутентификация субъектов доступа и объектов доступа
- управление доступом субъектов доступа к объектам доступа, реализующее такие возможности, как ограничение доступа (ограниченный срок действия или ограниченные права), передача клиентом части прав, необходимых для выполнения действий на другой вычислительной установке (на основе использования механизм делегирования прав, подразумевающего, что пользователю нужно лишь один раз пройти процедуру аутентификации, а далее система сама обеспечивает аутентификацию пользователя на всех ресурсах, которыми он собирается воспользоваться);
- защита информации от несанкционированного доступа (конфиденциальность);
- защита информации от несанкционированной модификации (целостность);
- обеспечение невозможности отказа пользователя от совершенного действия (неотказуемость).

При реализации указанных функций используются следующие основные технологии защиты:

- идентификация и аутентификация на основе сертификатов открытых ключей серверов и пользователей;
- криптографическая защита информации ограниченного распространения при передаче по каналам связи Грид-сети;
- управление доступом к вычислительным ресурсам и ресурсам хранения данных.

Данные технологии базируются на использовании инфраструктура открытых ключей X.509 и протокола TLS/SSL с поддержкой стандарта обмена данными об аутентификации и авторизации SAML для обеспечения технологии единого входа, а также стандарта XACML, который определяет язык для описания политик управления доступом.

SAML (англ. security assertion markup language) — язык разметки, основанный на языке XML. Представляет открытый стандарт обмена данными аутентификации и авторизации

между участниками, в частности, между поставщиком учетных записей и поставщиком сервиса. Одной из важных проблем, которую пытается решить SAML, является обеспечение сквозной аутентификации при работе через Web-браузер. Язык SAML не зависит от платформы и может обеспечить стандартный способ обмена аутентификационными и авторизационными данными между приложениями разных производителей.

XACML (eXtensible Access Control Markup Language) — основанный на языке XML стандарт, определяющий язык описания политик управления доступом, модель и способы их обработки. Управление доступом базируется на использовании правил предоставления доступа, отвечающих за возможность совершения какого-либо действия или доступа к какому-либо объекту и дающих ответ («Да» либо «Нет») на вопрос «Есть ли доступ?». Условие любого правила сводится к набору логических выражений, вычисление которых дает один из двух указанных вариантов ответа. Соответственно политика управления доступом базируется на использовании логических выражений, оперирующих атрибутами и константными значениями.

OpenSSL, используемый в UNICORE, поддерживает разные алгоритмы шифрования и хеширования, в том числе:

- Симметричное шифрование — Blowfish, Camellia, DES, RC 2, RC 4, RC 5, IDEA, AES, ГОСТ 28147–89;
- Хеш-функции — MD 5, MD 2, SHA, MDC-2, ГОСТ Р 34.11–94;
- Асимметричное шифрование и электронная цифровая подпись — RSA, DSA, Diffie-Hellman key exchange, ГОСТ Р 34.10–2001 (34.10–94).

При этом поддержка алгоритмов ГОСТ появилась в версии 1.0.0, выпущенной 29 марта 2010 года, и была реализована сотрудниками фирмы «Криптоком».

Необходимо отметить, что ни один из перечисленных алгоритмов не сертифицирован в Республике Беларусь. В то же время в статье 28 закона Республики Беларусь «Об информации, информатизации и защите информации» [1], определено, что информация, распространение и (или) предоставление которой ограничено, не отнесенная к государственным секретам, должна обрабатываться в информационных системах с применением системы защиты информации, аттестованной в порядке, установленном Оперативно-аналитическим центром при Президенте Республики Беларусь. В данной статье, также отмечается, что для создания системы защиты информации используются средства технической и криптографической защиты информации, имеющие сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь, или положительное экспертное заключение по результатам государственной экспертизы, порядок проведения которой определяется Оперативно-аналитическим центром при Президенте Республики Беларусь. Перечень всех сертифицированных в РБ криптографических алгоритмов приведен в приказе Оперативно-аналитического центра при Президенте Республики Беларусь от 30 августа 2013 г. № 62 «О некоторых вопросах технической и криптографической защиты информации» [2].

Порядок криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам в Республики Беларусь установлен приказом [2].

В данном приказе отмечается, что при принятии собственником (владельцем) информационной системы решения о применении средств криптографической защиты информации (СКЗИ) для защиты служебной информации ограниченного распространения, определенной в соответствии с законодательством, должно обеспечиваться выполнение

определенных технических мер. В частности, криптографическая защита служебной информации ограниченного распространения должна осуществляться на отдельно выделенном средстве вычислительной техники, не подключенном к информационным сетям, сетям электросвязи общего пользования, в том числе к глобальной компьютерной сети Интернет. В случае, когда такое подключение требуется для обеспечения технологических процессов функционирования информационных систем, оно должно осуществляться с применением средств защиты информации, имеющих сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь и обеспечивающих исключение возможности несанкционированного доступа к служебной информации ограниченного распространения, а также к самой информационной системе.

В приказе приведен перечень технических нормативных правовых актов и документов, в которых определены требования к криптографическим механизмам. В частности, для криптографического механизма «шифрование» в этот перечень включены: ГОСТ 28147–89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования» и СТБ 34.101.31–2011 «Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности»; имитозащита — ГОСТ 28147–89 и СТБ 34.101.31–2011; электронная цифровая подпись — СТБ 1176.1–99 и СТБ 34.101.47–2012.

Таким образом, в настоящем состоянии национальная Грид-сеть, основанная на применении OpenSSL, не соответствует действующим законам РБ, и ее невозможно аттестовать в РБ. Для аттестации Грид-сети необходимо применение средств защиты информации (подобно OpenSSL), имеющих сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации».
2. Приказ оперативно-аналитического центра при президенте Республики Беларусь от 30 августа 2013 г. № 62 «О некоторых вопросах технической и криптографической защиты информации».

КИБЕРПРЕСТУПНОСТЬ: СОВРЕМЕННЫЕ ТЕНДЕНЦИИ

Т. В. РАДЫНО
Открытое акционерное общество
«МИНСКИЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ ЗАВОД ИМЕНИ В.И.КОЗЛОВА»

В связи с с переходом индустриального общества к обществу информационному, изменяется и структура преступности. Новые преступления, связанные с посягательствами на информацию, передачу данных, информационные технологии, совершаемые в компьютерных сетях и системах, а также во всемирной сети Интернет, распространяются с геометрической прогрессией. Уголовная юстиция должна быть вооружена современным инструментарием поисково-познавательной деятельности, который разрабатывается криминалистической и уголовно-правовой наукой.

В развитии человеческого общества внедрение компьютеров, современных средств переработки и передачи информации в различные сферы деятельности послужило началом нового эволюционного процесса, называемого информатизацией. Информатизация общества сегодня представляет собой организационный, социально-экономический и научно-технический процесс, обеспечивающий условия для формирования и использования информационных ресурсов и реализации информационных отношений [5].

Человеческое общество пережило как минимум четыре информационные революции. Последняя из них связана с изобретением микропроцессорных технологий и появлением персонального компьютера, и, как следствие — информационной коммуникации. Произошел переход от механических, электрических средств преобразования информации к электронным. Миниатюризация аппаратуры, машин, приборов, создание программно-управляемых устройств и процессов сделали использование информационно-компьютерных средств коммуникации необходимой и неотъемлемой частью жизни человека и общества. Появилась новая отрасль — информационная индустрия (переработка информации на базе компьютерных и телекоммуникационных информационных технологий), связанная с производством технических средств, методов, технологий для производства новых знаний формируется комплексная инфраструктура для оказания электронных услуг населению [1].

Информационная технология — это совокупность процессов, методов осуществления поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также пользования информацией и защиты информации [5].

В информационном обществе традиционно выделяют следующие особенности общественного развития: процесс компьютеризации обеспечивает высокий уровень автоматизации обработки информации во всех сферах жизни общества, движущей силой развития общества становится производство информационного, а не материального продукта, изменятся не только производство, но и весь уклад жизни, система ценностей.

Так, по сравнению с индустриальным обществом, где все направлено на производство и потребление товаров, в информационном обществе производятся и потребляются интеллект, знания, что приводит к увеличению доли умственного труда. Ценится новизна информации, ее удобоваримость и понятность, оперативность подачи. От человека требуется способность к нестандартному мышлению, решению разноплановых задач. Возрастает спрос на знания, их быструю оборачиваемость. Материальной и технологической базой информационного общества становятся различного рода системы на базе компьютерной техники и компьютерных сетей, информационной технологии, телекоммуникационной связи.

Все эти процессы пронизывают не только общественно-полезные сферы жизни общества — общие тенденции информационного общества характерны также и для преступной среды, преступного сообщества. Большая часть преступлений уже совершается в информационном пространстве, и удельный вес этих преступлений в общей массе неуклонно растет. Это так называемая «киберпреступность».

Под киберпреступностью принято понимать совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей и против компьютерной системы или сети [2].

Это определение соответствует рекомендациям экспертов ООН. Такой позиции придерживается и Организация экономического сотрудничества и развития, определяющая

компьютерные и связанные с ними преступления как любое незаконное, неэтичное или неуполномоченное поведение, связанное с процессами автоматической обработки и/или передачи данных.

В связи с динамичным и масштабным ростом киберугроз и киберпреступлений, причиняемым ими ущербом государственным структурам, юридическим и физическим лицам, в том числе поставщикам услуг, такие угрозы и преступления представляют серьезнейшую проблему для общества, а борьба с ними является актуальной и стратегически важной задачей для правоохранительных органов, особенно в части, касающейся реализации мер, направленных на эффективное противодействие росту киберпреступности, своевременное установление лиц, совершивших преступные деяния и, конечно, получение доказательств, подтверждающих совершение правонарушения [3].

Представители государств — членов Совета Европы, США, Канады, Японии в ноябре 2001 г. подписали международную Конвенцию по киберпреступности. В этом документе преступления, совершенные в информационной среде против информационных ресурсов или с помощью информационных средств, фактически определены как киберпреступления, к числу которых относятся, в частности: противозаконный доступ в информационную среду; неправомерный перехват информационных ресурсов; вмешательство в информацию, содержащуюся на магнитных носителях; вмешательство в компьютерную систему; противозаконное использование устройств; подлог с использованием компьютерных технологий; мошенничество с использованием компьютерных технологий; преступления, относящиеся к «детской» порнографии; преступления, относящиеся к нарушениям авторских и смежных прав [4].

Таким образом, в качестве объективной стороны преступных посягательств можно определить преступную деятельность, осуществляемую посредством или связанную с компьютерами, компьютерными системами или сетями. Общим объектом таких преступлений является компьютерная безопасность, предметом — компьютерные системы и сети, информация на электронных носителях. Однако, с нашей точки зрения, в современных реалиях необходимо пересмотреть подходы к определению личной информации, поскольку максимально актуальной становится дискуссия о природе информации, хранящейся в личных аккаунтах пользователей социальных сетей, информация, хранящаяся в почтовых ящиках (e-mail), переписке в системах типа skype и viber и проч. С этой точки зрения законодателю следует особое внимание обратить на официальное толкование практики применения таких составов преступлений, как статья 179 Уголовного кодекса Республики Беларусь (далее — УК)»Незаконное собирание либо распространение информации о частной жизни», ст. 203 «Нарушение тайны переписки, телефонных переговоров телеграфных или иных сообщений», ст. 250. «Распространение ложной информации о товарах и услугах», ст. 254. «Коммерческий шпионаж», ст. 356 «Измена государству», ст. 358 «Шпионаж», ст. 358–1 «Агентурная деятельность», ст. 373. «Умышленное разглашение государственной тайны» [6].

Безусловно, основными составами преступлений, из которых складывается так называемая киберпреступность, по-прежнему являются деяния, ответственность за которые предусмотрена главой 31 УК — преступления против информационной безопасности.

Предметом уголовно-правового и криминалистического изучения являются те черты, признаки, явления, процессы, закономерности преступной деятельности, ее отражения в окружающей среде, непосредственное изучение которых позволит сформировать криминалистическую характеристику соответствующих преступлений: преступлений против конфиденциальности, целостности и доступности компьютерных данных и систем;

методика расследования преступлений, непосредственно связанных с использованием компьютерных, телекоммуникационных средств; преступлений, связанных с контентом (содержанием) данных; преступлений с нарушением авторских прав и смежных прав.

Совершенное в киберпространстве преступление должно расследоваться соответствующими методами с использованием современных технологий. На смену классических методов уголовного процесса и розыскной деятельности должен прийти специалист, легко идущей по цифровому следу: преступник в большинстве случаев является высококвалифицированным специалистом в области IT-технологий со сформированными профессиональными навыками «заметания следов», преступления им совершаются скрытно, относятся к неочевидным преступным деяниям, носят длящийся характер.. В последнее время наблюдается тенденция к приобретению киберпреступлениями группового характера либо киберпреступник использует большое количество компьютеров. Правильное определение источника, носителя доказательственной информации, оптимальный способ ее собирания и закрепления затрудняется тем, что доказательства преступной деятельности сохраняются и передаются по электронным сетям.

Сохраняя традиционные поисково-познавательные методы деятельности и процедуры научного познания, применяемые следователем, дознавателем, экспертом, гособвинителем, судьей, тем не менее сегодня приходится активно работать над созданием если не новой, то параллельной научной системы криминалистического поиска. Эта система должна быть направлена на использование кибернетических методов, широкое применение специальных познаний в сфере IT-технологий.

Кадровое, материально-техническое обеспечение расследования киберпреступлений, повышение качества и эффективности поисково-познавательной деятельности лиц, ведущих расследование, — задачи, требующие незамедлительного разрешения. В настоящее время экспертные учреждения испытывают острейшую нехватку специалистов в области анализа алгоритмов работы программ для ЭВМ, изучения исходного кода в различных языках программирования, в сфере сетевого взаимодействия. Нельзя игнорировать тот факт, что за последние десятилетия появилось огромное количество новых профессий в сфере программирования, системного администрирования, криптографии. В правоохранительной сфере такое разделение труда также должно стать приоритетным направлением в формировании кадрового резерва профессионалов, поскольку такого рода специалистов следственным органам катастрофически не хватает.

Тенденция научного разделения труда в сфере высоких технологий, специализация отдельных коммерческих организаций в информационной отрасли помогает решать вопросы оптимизации труда и оперативного решения конкретных задач в IT-сфере. Полагаем, что подобная специализация следственных подразделений дала бы серьезный толчок развитию как уголовно-процессуальной, так и криминалистической науки и практики. Возможно, стоит рассмотреть вопрос о выделении информационных направлений в работе сотрудников правоохранительных органов и подготовки специалистов-криминалистов в конкретных областях знаний. Система специализированных учебных учреждений, включая ведомственные учреждения Министерства внутренних дел, позволяет уже сегодня обеспечить территориальное разделение по отраслям с трансляцией необходимой информации по каналам связи без необходимости физического перемещения носителей информации. При должном системном подходе и организационной проработке на высоком уровне юридического закрепления, внедрение серьезной специализации среди представителей следственных органов — это единственный способ не отстать в информационном развитии от криминального мира.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ:

1. «Адаптивная модификация» криминалистики в информационном обществе как закономерная реакция на распространение киберпреступности (Степаненко Д. А.) («Российский следователь», 2015, N 15)
2. *Тропина Т. Л.* Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: автореф. дис. … канд. юрид. наук. Владивосток, 2005. С. 9.
3. *Чекунов И. Г.* Современные киберугрозы. Уголовно-правовая и криминологическая классификации и квалификации киберпреступлений // Право и кибербезопасность. 2012. N 1. С. 12.
4. Конвенция о преступности в сфере компьютерной информации (ETS N 185) [рус., англ.] (Заключена в г. Будапеште 23 ноября 2001 г.) // СПС «КонсультантПлюс» (дата обращения: 12.03.2015).
5. Закон Республики Беларусь от 10.11.2008 N 455-З (ред. от 04.01.2014)»Об информации, информатизации и защите информации»
6. Кодекс Республики Беларусь от 09.07.1999 N 275-З (ред. от 20.04.2016)»Уголовный кодекс Республики Беларусь»

СТАТИСТИЧЕСКИЕ МЕТОДЫ ОЦЕНКИ РАСПРЕДЕЛЕНИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А. И. ТРУБЕЙ

Учреждение БГУ НИИ прикладных проблем математики и информатики

Для оценки рисков ИБ по формуле $ALE = AV \cdot EF \cdot ARO$ необходимо определить ожидаемую среднегодовую частоту реализации угроз — ARO (AV — стоимость активов, EF — степень уязвимости актива к угрозе). Прогнозируемые частоты реализации угроз (инцидентов ИБ) определяются с применением теории вероятностей и математической статистики, аналитических методов, а также экспертных оценок. Для прогнозирования частот реализации угроз на текущий или будущий годы необходимо проводить анализ угроз на основе накопленных данных об инцидентах ИБ за предыдущие годы. Анализ уязвимостей и угроз, характерных для государственных ИС, может проводиться с использованием банка данных угроз безопасности информации ФСТЭК России. Предлагается метод оценки инцидентов, связанных с реализацией возможных угроз, воздействующих на ИС, с использованием критерия χ^2.

Предположим, что частоты реализации угроз (каналов утечки) $E_1,\ldots,E_i,\ldots,E_N$ за отрезки времени $t_1,\ldots,t_k,\ldots,t_M$ (например, за квартал, год) составляют $\nu_{k,1},\ldots,\nu_{k,i},\ldots,\nu_{k,N}$ ($\nu_{k,i}$ — частота реализации угрозы E_i за отрезок времени t_k). Получим M независимых выборок, каждая из которых есть реализация некоторой полиномиальной схемы с исходами $1,\ldots,N$. Объемы выборок равны $z_1,\ldots,z_M$; $z = \sum_{k=1}^{M} z_k$, $t_0 = min\{z_1,\ldots,z_M\}$.

Выясним, происходили ли изменения в распределении вероятностей реализации угроз во временных промежутках $t_1,\ldots,t_k,\ldots,t_M$, т.е. проверим однородность выборок. Для проверки однородности полиномиальных выборок обычно используют статистику χ^2.

$$\chi^2 = \sum_{k=1}^{M}\sum_{i=1}^{N}\frac{\left(\nu_{k,i} - z_k m_i / z\right)^2}{z_k m_i / z} = z\sum_{k=1}^{M}\sum_{i=1}^{N}\frac{1}{z_k m_i}\left(\nu_{k,i} - m_i\frac{z_k}{z}\right)^2, \quad (1)$$

где $m_i = \sum_{k=1}^{M}\nu_{k,i}$.

При $z_0 \to \infty$ данная статистика сходится по распределению к случайной величине $\chi_{(M-1)(N-1)}$, имеющей распределение хи-квадрат с $(M-1)(N-1)$ степенями свободы. Проверяемая гипотеза принимается, когда значение статистики χ^2 не превышает критического значения χ_p^2, или достигнутый уровень значимости больше заданного уровня значимости p. Для всех ожидаемых частот должно соблюдаться условие: $t_k p_{k,i} \geq 5$.

Представляют интерес частные случаи формулы (1). При $M = 2$ мы будем иметь 2 независимые выборки, $N-1$ степеней свободы и формула примет вид:

$$\chi_{k,l}^2 = z_k z_l \sum_{i=1}^{N}\frac{1}{\nu_{k,i} + \nu_{l,i}}\left(\frac{\nu_{k,i}}{z_k} - \frac{\nu_{l,i}}{z_l}\right)^2, \quad (2)$$

где $\nu_{k,1},\ldots,\nu_{k,N}$; $\nu_{l,1},\ldots,\nu_{l,N}$ — наборы частот соответственно k-й и l-й выборок; $z_k = \sum_{i=1}^{N}\nu_{k,i}$; $z_l = \sum_{i=1}^{N}\nu_{l,i}$.

При $N = 2$ мы будем иметь M последовательных наблюдений, в каждом из которых угроза l осуществляется соответственно $\nu_1,\nu_2,\ldots,\nu_j,\ldots,\nu_M$ раз. Проверяется гипотеза о том, что угроза l во всех наблюдениях имеет одну и ту же, постоянную вероятность p. и Формула для статистики хи-квадрат (с $M-1$ степенями свободы) примет вид:

$$\chi^2 = \sum_{j=1}^{M}\frac{\left(\nu_j - z_j p^*\right)^2}{z_j p^* q^*} = \frac{1}{p^* q^*}\sum_{j=1}^{M}\frac{\nu_j^2}{z_j} - z\frac{p^*}{q^*}, \quad (3)$$

где $p^* = 1 - q^* = \frac{1}{t}\sum_{j=1}^{M}\nu_j$.

Если выборки «близки» к однородным, то статистика χ^2 будет иметь нецентральное распределение хи-квадрат с тем же числом степеней свободы и ее значение будет пропорционально объему выборки. Использование больших выборок может привести к решению об отклонении гипотезы H_0, хотя неоднородность выборок может быть несущественной и иногда ею можно пренебречь. В статистических приложениях широко используют различные приближения с помощью «центрального» хи-квадрат распределения и нормального распределения.

Проиллюстрируем применение предложенного метода на примере отчетов JSOC Security flash report, которые основаны на данных, полученных в коммерческом центре мониторинга и реагирования на инциденты информационной безопасности — Solar JSOC. По информации руководства компании в настоящее время к Solar JSOC подключено более 20 клиентов: предприятия энергетики, финансовые организации, транспортные компании. При формировании выборок будем рассматривать не суммарные частоты инцидентов, зафиксированные компанией Solar JSOC, а средние частоты реализации угроз на каждого клиента компании. Для определенности количество клиентов будем считать равным 20.

1. Распределение инцидентов по внешним и внутренним

Проверим, совместимы ли приведенные в таблице 1 данные с гипотезой о том, что, реализация внутренних, а, следовательно, и внешних угроз в указанные промежутки времени имеют одни и те же вероятности.

Таблица 1

Частоты внешних и внутренних инцидентов

Инциденты	3 кв. 2014	4 кв. 2014	1 кв. 2015	2 кв. 2015	3 кв. 2015	4 кв. 2015	χ^2_5
Внешние	358	480	623	866	950	869	10,5
Внутренние	585	984	1115	1528	1779	1703	10,5
Всего	943	1464	1738	2394	2729	2572	

Вычислим значение статистики χ^2 по формуле (3) для $N = 2$. Получим χ^2, что лежит ниже уровня значимости $p = 0,05$ с четырьмя степенями свободы, равного 11,1, и можно считать, что указанная гипотеза справедлива.

2. Внешние инциденты

Инициаторами и причиной внешних инцидентов являются действия лиц, не являющихся внутренними пользователями. Частоты инцидентов приведены в таблице 2.

Таблица 2

Направления атак внешних инцидентов

Суммарные частоты внешних инцидентов		Частоты внешних инцидентов по направлениям атак					
		E_1	E_2	E_3	E_4	E_5	E_6
		Атаки на web-прилож.	Brute-force и компр. уч. данных внеш. серв.	Компр. админ. учетных записей	Атаки на управл. протоколы систем	DDoS-атаки	Прочие внешние атаки
4 кв. 2015	869	358	156	25	45	39	246
3 кв. 2015	950	371	209	20	60	31	259
2 кв. 2015	866	380	217	28	60	19	162
1 кв. 2015	623	263	169	16	45	10	120
4 кв. 2014	480	188	106	10	30	16	130
3 кв. 2014	358	136	92	5	19	10	96
χ^2_{25} = 90,4		χ^2_5 =6,9	χ^2_5 =22,9	χ^2_5 =5,1	χ^2_5 =3,9	χ^2_5 =13,1	χ^2_5 =38,5

Оценим однородность полученных выборок. В таблице 2 приведены значения статистик χ^2, вычисленных по формуле (1) (для суммарных выборок при M =6, N =6) и по формуле (3) (для частот конкретных инцидентов при M =6, N =2). Значения статистик свидетельствуют о том, что происходили определенные (однако не существенные) изменения в распределении вероятностей реализации внешних угроз в указанные промежутки времени. При этом вероятности реализации угроз E_1, E_3, E_4, практически не изменялись. При сравнении выборок инцидентов за последний (четвертый) квартал 2015 года с третьим кварталом по формуле (2) получим χ^2_5=8,3 (для пяти степеней свободы), которое означает, что в течение данных кварталов не произошло существенных изменений в распределении внешних инцидентов.

3. Внутренние инциденты

Инициаторами и причиной внутренних инцидентов являются действия внутренних сотрудников: халатность в соблюдении политик ИБ или их прямое нарушение, компрометация или передача учетных данных сотрудников, злонамеренные и незлонамеренные воздействия на бизнес-процессы и функционирование систем. К внутренним пользователям-инициаторам инцидента относятся все пользователи с возможностью доступа в локальную сеть без преодоления периметра. Частоты данных инцидентов по направлениям атак приведены в таблице 3.

Таблица 3

Направления атак внутренних инцидентов

Суммарные частоты внутренних инцидентов		**Частоты внутренних инцидентов по направлениям атак**					
		E_1	E_2	E_3	E_4	E_5	E_6
		Утечки конф. данных	**Вирусные атаки**	**Компр. учетных записей**	**Нарушение политик доступа в Интернет**	**Нелегит. работы под привилегир. учетными записями**	**Нелегит. изменения в IT-системах, несанкц. активн, удал. доступа, прочее**
4 кв. 2015	1703	685	245	225	198	105	245
3 кв. 2015	1779	630	231	209	278	132	299
2 кв. 2015	1528	433	294	236	170	93	302
1 кв. 2015	1115	337	190	180	138	60	210
4 кв. 2014	984	349	128	115	154	73	165
3 кв. 2014	585	151	69	82	72	64	117
χ^2_{25} = 206,2		χ^2_5 =78,2	χ^2_5 =39,0	χ^2_5 =19,1	χ^2_5 =24,9	χ^2_5 =23,2	χ^2_5 =21,8

Значения статистик χ^2, приведенных в таблице 3 свидетельствуют о том, что происходили существенные изменения в распределении вероятностей внутренних угроз в указанные промежутки времени.

В таблице 4 приведено распределение частот внутренних инцидентов по каналам утечек, а также соответствующие значения статистик χ^2 для суммарных выборок и для конкретных каналов утечек.

Таблица 4

Распределение внутренних инцидентов по каналам утечек

Суммарные частоты внутренних инцидентов		**Частоты внутренних инцидентов по каналам утечек**				
		E_1	E_2	E_3	E_4	E_5
		Устройства доступа в Интернет	**Электронная почта**	**Веб-ресурсы**	**Съемные носители**	**Печать**
4 кв. 2015	1703	291	550	364	334	164
3 кв. 2015	1779	279	555	420	307	218
2 кв. 2015	1528	219	449	417	284	159
1 кв. 2015	1115	144	294	353	225	99
χ^2_{20} = 81,9		χ^2_4 =10,4	χ^2_4 =12,6	χ^2_4 =45,5	χ^2_4 =4,9	χ^2_4 =10,4

Значения статистик χ^2 свидетельствуют о том, что происходили определенные (однако не существенные) изменения в распределении вероятностей каналов утечек в указанные промежутки времени.

Метод может использоваться для выявления тенденций в динамике угроз. Если при сравнении частот инцидентов ИБ за текущий квартал, полугодие, год с частотами инцидентов за прошлый квартал, полугодие, год не выявлено существенного изменения в распределении вероятностей инцидентов (значение статистики χ^2 не превышает заданного уровня), то с определенной вероятностью можно предположить, что эти показатели будут стабильны в среднесрочной перспективе. Это позволит спрогнозировать потенциальные частоты инцидентов на будущий год, которые, в свою очередь, могут быть использованы при оценке рисков ИБ. Если же значение статистики χ^2 однородности значительно превышает заданный уровень, то необходимо выявлять причины сложившейся ситуации с изменением распределения инцидентов и проводить углубленный анализ угроз, воздействующих на ИС.

СЕКЦИОННОЕ ЗАСЕДАНИЕ «НОВЫЕ ИДЕИ И ПОДХОДЫ К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»

ТЕХНОЛОГИЯ БИОМЕТРИЧЕСКОЙ ПОДДЕРЖКИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ОБЕЗЛИЧИВАНИЕМ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ В МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

А.И. ИВАНОВ, Ю.К. ЯЗОВ, О.В. КОРНЕЕВ

Показано, что перспективным является защита персональных данных пациентов в медицинских информационных системах с использованием технологии биометрического обезличивания информации. Все медицинские электронные документы в этом случае хранятся в обезличенной форме. Снять свою защиту обезличиванием может только сам пациент и второе лицо — «гарант обезличивания». При этом медицинский персонал технически не имеет возможности получить персональные данные пациентов, а пациент не может послать вместо себя другого человека (исключена подмена пациента другим человеком). Каждое значимое действие пациента выполняется после биометрической аутентификации, формируются данные аудита информационной безопасности. Результаты биометрической аутентификации заносятся в электронный документ, который подписывается цифровой подписью сервера биометрической аутентификации и лечащего врача. Биометрические вычисления и криптографические преобразования по формированию цифровой подписи выполняются в доверенной вычислительной среде «БиоТокен», которая включается между сканером биометрической информации и ПЭВМ медицинской информационной системы.

Ключевые слова: биометрическая аутентификация, обезличивание персональных данных, нейросетевое преобразование биометрических данных в код.

Одной из важнейших проблем информатизации современного общества является проблема хищения персональных данных. Ранее при использовании документов на бумаге личные медицинские карты с историями болезни хранились в регистратуре медицинских учреждений. Массовое хищение персональной информации, содержащейся в медицинских картах, ранее было технически затруднено из-за большого веса и объема документов. Ситуация изменилась с появлением медицинских информационных систем, у медицинского и технического персонала появилась возможность хищения базы электронных документов, содержащей значительные объемы персональных данных.

Парольная защита доступа к персональным данным, к сожалению, оказывается не состоятельной, так как пользователи не могут запоминать длинные пароли. Использование комбинации пароль и токен при доступе к базам медицинских документов также не решает проблемы, так как эти аутентификационные атрибуты могут оказаться у другого лица по сговору или по халатности. Определить того, кто осуществил хищение персональных данных, не удается.

Техническим решением задачи защиты персональных данных является обезличивание базы электронных медицинских документов. В том случае, если из медицинских документов изъяты открытые персональные данные, хищение их базы теряет смысл. Похитивший базу электронных документов злоумышленник не имеет технической возможности определить кому принадлежит тот или иной документ. Появляется возможность открыто хранить обезличенные электронные медицинские документы не только в информационной системе медицинского учреждения, но и привлекать для хранения «облачные» сервисы (рис. 1).

Рис. 1. Защита персональных данных в медицинских информационных системах через обезличивание с биометрической аутентификацией пользователей

Защита обезличиванием персональных данных строится на технологиях биометрико-нейросетевой аутентификации личности. Пользователь при доступе к его личной информации объявляет свой «цифровой псевдоним» и далее предъявляет свои биометрические данные. Если биометрические данные пользователя подтверждаются как «свои», доступ к электронной медицинской карте предоставляется врачу, пациенту, иному медицинскому работнику без разглашения персональных данных пациента. При этом «узнает» пользователя вычислительная машина, которая умеет работать с защищенными контейнерами биометрических данных. Воспользоваться своим защищенным контейнером может только его хозяин. На рис. 1 база с защищенными биометрико-нейросетевыми контейнерами отображена пунктиром (пунктирным кругом).

Гарантией безопасности хранения биометрических данных каждого пациента в защищенных нейросетевых контейнерах является соответствие этих контейнеров требованиям пакета стандартов ГОСТ Р 52633.xx-20xx, что в России должно быть подтверждено сертификатом ФСТЭК России.

Технология биометрической поддержки обезличивания электронных документов имеет программные компоненты и средства аппаратно-программной поддержки. Приходится пользоваться «программным интерфейсом поддержки биометрического обезличивания», компоненты которого отображены в верхней части рис. 2. В нижней части этого рисунка отображены новые компоненты медицинской информационной системы, которые должны появиться при использовании новой технологии. В медицинской информационной системе появляется «модуль реализации процедур обезличивания», который создает и использует защищенные биометрические контейнеры и связанные с ними обезличенные персональные данные (цифровые псевдонимы в форме сертификатов открытых ключей пользователей, не раскрывающие подлинных персональных данных пациентов). Связка цифровых псевдонимов с подлинными персональными данными хранится в сейфе вне медицинской информационной системы (смотри правый нижний угол рис. 2).

Снять защиту обезличиванием можно только в ручном режиме, открыв сейф с бумажными документами или накопителем с электронными копиями договоров, а также иных документов (отсканированных паспортов, отсканированных полисов медицинского страхования, и т.д.).

Рис. 2. Биометрическая поддержка системы обезличивания

При реализации новой технологии коренным образом меняется процедура регистрации пациента. В обычных медицинских информационных системах регистрация пациента сводится к вводу паспортных данных человека и номера его страхового полиса. При организации биометрической поддержки приходится дополнительно осуществлять регистрацию биометрических данных человека. Регистрируемый пациент должен «обучить» нейронную сеть преобразователя «биометрия-код» в соответствии с алгоритмом ГОСТ Р 52633.5–2011. Для этого пациенту нужно предъявить несколько примеров своего биометрического образа. Если используется анализ рисунка отпечатка пальца, то нужно от 8 до 16 раз приложить к сканеру свой палец. Если используется анализ динамики воспроизведения рукописного пароля, то регистрируемый должен воспроизвести от 8 до 16 раз свой рукописный пароль на графическом планшете. В конечном итоге «подсистема под-

держки биометрического обезличивания» должна сформировать открытые и защищенные биометрические контейнеры пользователей и уничтожить биометрические примеры, на которых обучалась нейронная сеть преобразователя биометрия-код. На рис. 3 отражены основные этапы биометрической регистрации пациентов.

Следует подчеркнуть, что именно на этапе биометрической регистрации происходит разделение персональных данных на опасные (хранимые далее в сейфе вне информационной системы) и на обезличенные (хранимые далее в медицинской информационной системе).

Далее при эксплуатации медицинской информационной системы сейф с действительными персональными данными пациентов уже не нужен. Процедуры биометрической аутентификации личности людей выполняются при всех значимых действиях врачей и пациентов.

И медицинские работники, и пациенты вместо набора на клавиатуре паролей доступа предъявляют свою биометрию. При необходимости могут также использоваться идентификационные карты и обычные таблетки-токены. Доступ к процедурам обработки обезличенных данных пациентов (медицинским картам, историям истории болезни, справкам, направлениям) всегда происходит после биометрической аутентификации и врача, и пациента, как это показано на рис. 4.

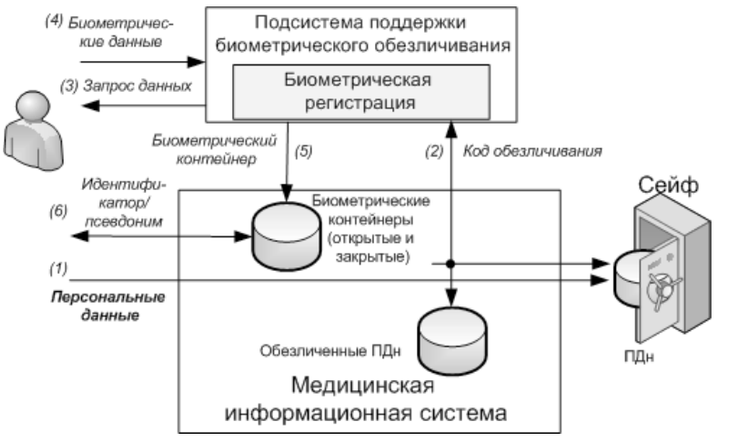


Рис. 3. Биометрическая регистрация пациента

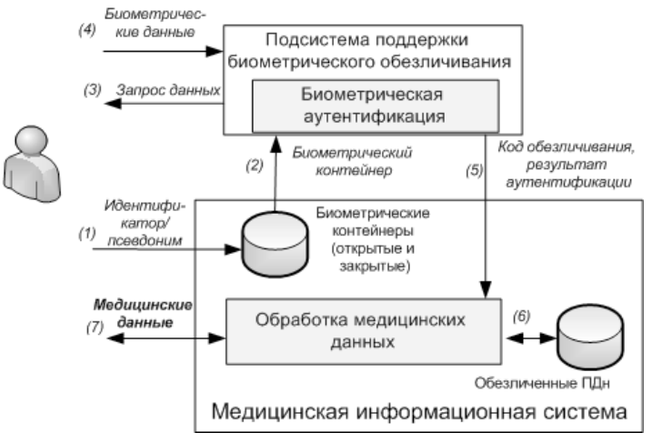


Рис. 4. Доступ к обработке обезличенных данных пациента

Принципиально важным преимуществом такой организации информационных систем является то, что исключается ситуация обмена полномочиями между медицинским персоналом (нельзя соседу передать идентификационную карту и пароль доступа). Пациенты также не могут злоупотребить своей обезличенностью, послав вместо себя другого человека сдавать анализы. Биометрическая аутентификация делает цифровую подпись под электронным документом более значимой. Врач или пациент уже не могут отказаться от цифровой подписи, сославшись на хищение пароля доступа и утерю идентификационной карты.

Новая технология биометрической поддержки обезличенности уже сегодня может быть реализована на практике в двух вариантах: с анализом рукописных паролей и с анализом рисунка отпечатка пальцев. При этом могут использоваться обычные идентификационные карты, обычные токены, сертифицированное программное обеспечение ПЭВМ медицинской информационной системы и должен быть исключен запуск неизвестных программных компонент в медицинской информационной системе.

Снизить требования к безопасности ПЭВМ информационной системы возможно в случае, если осуществлять криптографические преобразования данных аутентификации (формирование и проверку цифровых подписей) и биометрико-нейросетевой аутентификации внутри доверенной вычислительной среды «БиоТокен». Габаритные размеры и внешний вид доверенной вычислительной среды «БиоТокен» приведены на рис. 5.

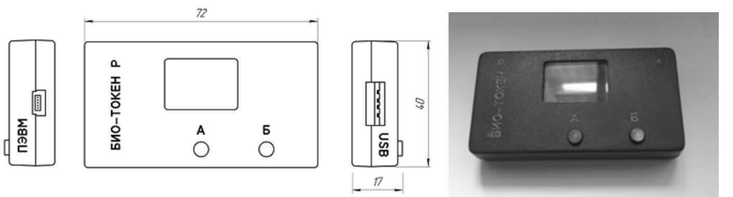


Рис. 5. Габаритные размеры и внешний вид доверенной вычислительной среды «БиоТокен», включаемой между ПЭВМ и сканером биометрической информации

Доверенная вычислительная среда «БиоТокен» предназначена для включения между сканером биометрической информации и ПЭВМ, которая может быть подключена через Интернет к облачному сервису хранения обезличенных медицинских электронных документов, то есть ПЭВМ с потенциально недоверенной операционной средой (правая часть рис. 1). В рамках ОКР «Лекарь», выполненной в соответствии программой защиты информационных ресурсов Союзного государства, созданы опытные образцы доверенной вычислительной среды «БиоТокен» в двух вариантах исполнения, как это показано на рис. 6.

Рис. 6. Два исполнения доверенной вычислительной среды «БиоТокен-Р" для анализа рукописных паролей и «БиоТокен-П» для анализа рисунка отпечатка пальца

Со стороны ПЭВМ медицинской информационной системы «БиоТокен» воспринимается как USB накопитель, куда можно разместить электронный документ и далее сформировать под ним цифровую подпись врача или пациента после соответствующей биометрической аутентификации. Структура аппаратно-программного комплекса «БиоГарант», обеспечивающего биометрическое обезличивание электронных документов медицинской информационной системы, приведена на рис. 7.

Рис. 7. Структура аппаратно-программного комплекса «БиоГарант», обеспечивающего биометрическое обезличивание МИС

Как видно из рис. 7, наряду с традиционными компонентами программного обеспечения медицинских информационных систем, появляются новые компоненты доверия, такие как: «Сервер биометрической аутентификации» и «Сервер биометрического удостоверяющего центра». По сути дела, они и являются принципиально новыми элементами, позволяющими развернуть биометрическую поддержку обезличивания электронных документов медицинских информационных систем следующего поколения.

Следует подчеркнуть, что создание любых новых приложений биометрии должно быть безопасным, то есть при проектировании обязательно должны выполняться все требования пакета стандартов ГОСТ Р 52633.xx-20xx. Рассмотренная в данном докладе биометрическая поддержка обезличивания медицинских электронных документов является одним из вариантов применения универсальных механизмов биометрической нейросетевой аутентификации.

СОЗДАНИЕ МНОГОКАНАЛЬНЫХ КВАНТОВЫХ СИСТЕМ ПЕРЕДАЧИ ДАННЫХ С ФУНКЦИЕЙ ОБНАРУЖЕНИЯ ЗЛОУМЫШЛЕННИКА

О. К. БАРАНОВСКИЙ
Учреждение образования «Белорусская государственная академия связи»
Е. В. ВАСИЛИУ
Одесская национальная академия связи им. А. С. Попова
А. О. ЗЕНЕВИЧ
Учреждение образования «Белорусская государственная академия связи»

Развитие инфокоммуникационных технологий предъявляет все более повышенные требования к пропускной способности каналов связи. В условиях современной электромагнитной обстановки до настоящего времени вне конкуренции системы волоконно-оптической связи, обеспечивающие скорость передачи информации (СПИ) до 10 Тбит/с. Вместе с тем для решения задач обеспечения конфиденциальности информации, передаваемой по волоконно-оптическим линиям связи, проходящим через неконтролируемые зоны, все чаще рассматривается целесообразность применения квантово-криптографических систем связи, которые соответствуют высоким требованиям безопасности информации [1,2].

Важнейшим режимом работы систем защищенной связи является согласование ключевых параметров криптографических алгоритмов, которые будут применяться для передачи защищаемой информации. Сегодня квантово-криптографические системы в режиме распределения ключей характеризуются низкой СПИ из-за несовершенства используемого оборудования и сложностей реализации процедур обмена данными. Для защиты передаваемой информации используется квантово-механический ресурс: каждый бит информации кодируется состоянием фотона. При попытке несанкционированного считывания информации происходит изменение состояния фотона, что обнаруживается авторизованными в системе пользователями. В связи с этим решается задача повышения СПИ в таких системах.

Одним из подходов к повышению СПИ является расширение числа каналов квантовой системы. Принцип функционирования многоканальной квантовой системы заключается в следующем. Поступающая на вход системы битовая последовательность разделяется на слова, содержащие i бит. Каждый бит кодируется посредством отдельного источника оптического излучения с длиной волны λ_k. С помощью оптического смесителя и нейтрального светофильтра оптическое излучение ослабляется до интенсивности, при которой каждый бит представляет собой однофотонный импульс с длиной волны λ_k. На приемной стороне однофотонные импульсы с применением диспергирующего элемента разделяются по длине волны и регистрируются счетчиками фотонов [3].

Передача данных маломощными оптическим сигналами, содержащими в среднем один фотон на каждый передаваемый бит является характерной отличительной особенностью многоканальных квантовых систем по сравнению с системами связи со спектральным уплотнением. В отдельных случаях такой режим позволяет обнаруживать наличие подслушивающего злоумышленника путем введения автоматического контроля за вероятностью ошибки регистрации.

Перехват оптического излучения злоумышленником реализовывается пассивным или активным методом съема данных, что приводит к потере частичной или полной мощно-

сти оптического излучения, несущего информацию о каждом отдельном бите сообщения, в результате увеличивается число ошибок регистрации. Рост числа ошибочных регистраций будет свидетельствовать о наличии подключения злоумышленника к оптическому волокну. В случае, когда злоумышленник использует компенсационный метод съема данных, то число ошибочных регистраций может не измениться [4].

В связи с вышеизложенным предлагается использовать дополнительную меру защиты, связанную с возможностью реализации злоумышленником компенсационного метода съема данных с оптоволоконной линии связи.

Для обнаружения подключения злоумышленника выполняется измерение временной задержки между моментами времени регистрации отдельных битов, передаваемых на некоторых длинах волн λ_1 и λ_2. Так как оптическое волокно обладает дисперсией, то фотоны с длинами волн λ_1 и λ_2 распространяются в нем с различными скоростями. Следовательно, при одновременном входе двух фотонов с длинами волн λ_1 и λ_2 в оптическое волокно они будут регистрироваться на его выходе с некоторой временной задержкой τ_0, зависящей от длины волокна. Временная задержка τ_0 для оптического волокна измеряется до его подключения в систему связи. После подключения оптического волокна в систему связи выполняется измерение времени задержки τ на выходе оптического волокна между двумя одновременно испущенными фотонами с длинами волн λ_1 и λ_2, используемыми для передачи отдельных битов. Затем сравнивают между собой величины τ и τ_0 и, если эти величины не совпадают, то делают вывод о наличии подключения злоумышленника к оптическому волокну. При обнаружении подключения злоумышленника к оптическому волокну передачу данных прекращают.

Для определения длин волн, которые необходимо использовать при передаче данных, выполнены исследования зависимости отношения $\Delta P_{pot}/\Delta D$ от длины волны оптического излучения (ΔP_{pot} — изменения вероятности потери оптического сигнала в оптическом волокне, ΔD — изменение диаметра макроизгиба). Измерения проводились для серийно выпускаемого оптического волокна G.652.

Установлено, что для обеспечения приемлемой скорости передачи данных по оптоволоконной линии связи в режиме формирования ключа целесообразно использовать длины волн 850 и 1625 нм. При этом обеспечивается наилучшая защищенность передаваемой информации, поскольку для вывода оптического излучения с длиной волны 850 нм из волокна злоумышленнику необходимо сформировать макроизгиб диаметром более 20 мм, что хорошо диагностируется на длине волны 1625 нм. Диагностирование макроизгиба на длине волны 1625 нм осуществляется по увеличению P_{pot} не менее, чем на 50 %. При этом одновременно испущенные фотоны с этим длинами волн после распространения по оптическому волокну имеют наибольшую временную задержку τ между собой. Временная задержка между этими фотонами при длине оптического волокна 1 км составляет 45±0,5 нс.

Предложенный способ обнаружения злоумышленника, реализующего компенсационный способ съема информации в канале связи, работающем в режиме передачи данных по оптическому волокну с использованием однофотонных импульсов, позволяет сделать практически невозможным скрытие факта перехвата данных ввиду малых времен передачи данных в канале связи.

СПИСОК ЛИТЕРАТУРЫ

1. *Килин С. Я.* Квантовая криптография: идеи и практика / С. Я. Килин; под ред. С. Я. Килин, Д. Б. Хорошко, А. П. Низовцев. — Минск: Белорус. наука, 2007. — С. 31, 157–176.

2. *Румянцев К. Е.* Квантовая связь и криптография: учебное пособие / К. Е. Румянцев, Д. М. Голубчиков. — Таганрог: Изд-во ТТИ ЮФУ, 2009. — С. 90–92.
3. *Зеневич А. О.* Многоканальная квантовая система связи для передачи конфиденциальной информации / А. О. Зеневич, А. М. Тимофеев, А. Г. Косари, А. А. Липай, Е. В. Мороз, В. С. Толкачева // // Межд. научн. — техн. конф., приуроченная к 50-летию МРТИ-БГУИР (Минск, 18–19 марта 2014 года): материалы конф. в 2 ч. Ч. 1. — Минск, 2014. — С. 426–427.
4. *Манько А.* Защита информации на волоконно-оптических линиях связи от несанкционированного доступа / А. Манько, В. Каток, М. Задорожний // Правове, нормативне та метрологичне забезпечення системи захисту інформації в Україні. — 2001. — № 2. С. 249–255.

ОЦЕНКА ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ АЛГОРИТМОВ РАЗДЕЛЕНИЯ ИНФОРМАЦИИ В КАЧЕСТВЕ ОСНОВНОГО СПОСОБА ЗАЩИТЫ ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ В СЕТЯХ ХРАНЕНИЯ ДАННЫХ

С.В. СОЛОВЬЕВ, В.Н. СИГИТОВ, И.А. ШАРОВ
ФАУ «ГНИИИ ПТЗИ ФСТЭК РОССИИ»

Сети хранения данных на основе протокола iSCSI — архитектурное решение для удаленного подключения внешних устройств хранения данных (т.н. блочных устройств) к рабочим станциям на основе существующих сетевых каналов передачи данных, при котором блочное устройство распознается и управляется рабочей станцией как локальное.

Подобная организация удаленного доступа к информации предназначена для снятия ограничений на обработку информации, возникающих при использовании технологий сетевого доступа с использованием протоколов, основанных на пакетной передаче данных, и позволяет получить управление файловой системой блочных устройств хранения данных, в том числе и находящихся на значительном территориальном удалении от рабочей станции, что обусловлено возможностью использования в качестве основного канала передачи данных сети Интернет. Это достигается комбинированием работы:

- пакетного стандарта передачи данных, являющегося основой функционирования современных сетей передачи данных;
- блочного стандарта передачи данных, применяемого при локальном подключении устройств хранения данных к рабочей станции.

Однако сети хранения данных на основе протокола iSCSI стали рассматриваться в качестве серьезной альтернативы уже существующим сетевым технологиям только в последнем десятилетии, вследствие чего до сих пор серьезно не рассматривались вопросы обеспечения безопасности данных, обрабатываемых в подобных информационных системах, в части:

- описания специфических угроз, возникающих исключительно в сетях хранения данных и связанных с использованием дополнительных программных и/или программно-аппаратных средств;

– оценки применимости и достаточности требований существующих нормативно-методических документов по защите информации при ее обработке в сетях хранения данных;
– использования уникальных только для сетей хранения данных способов и мер защиты информации.

В ходе формирования модели угроз безопасности информации, обрабатываемой в сетях хранения данных на основе протокола iSCSI, был выявлен ряд специфических угроз, свойственных только информационным системам, построенным на основе данной технологии, таких как:

– случайное или преднамеренное одновременное подключение нескольких клиентов к одному блочному устройству, приводящее к нарушению целостности хранимых на устройстве данных;
– нарушение процесса коммутации соединений путем проведения сетевых атак на коммутационное оборудование (реализованное на программном или аппаратном уровне), приводящее к рассинхронизации процессов блочной передачи данных и др.

Практическая реализация в сетях хранения данных известных на сегодня мер защиты информации вызывает сложности, обусловленные специфической архитектурой подобных информационных систем, например, более 30 % требований по защите информации являются частично или полностью невыполнимыми в условиях применения сетей хранения данных на основе протокола iSCSI, что создает целый ряд проблем с точки зрения защиты информации:

– отсутствие ограничений по вводу/выводу информации на блочные устройства;
– невозможность подтверждения источника информации и т. п.

Возможным выходом из сложившейся ситуации может стать разработка новых способов защиты информации, обрабатываемой в сетях хранения данных, построенных на основе протокола iSCSI. В качестве одного из таких способов может рассматриваться применение алгоритмов разделения информации, предложенных Михаэлем Рабиным в 1989 г. [1] как основного механизма хранения и передачи данных в распределенных системах, включающих в себя большое количество независимых друг от друга элементов, централизованный контроль за которыми не представляется возможным.

Применение в сетях хранения данных, построенных с использованием протокола iSCSI, алгоритмов разделения информации может решить проблему, связанную с невозможностью контроля за блочными устройствами, и обеспечить целостность, доступность и конфиденциальность информации, хранимой на таких устройствах.

Алгоритмы разделения информации представляют собой метод, основанный на преобразовании файла F длиной $L = |F|$ в последовательность из n частей $F_1, F_2, \ldots F_n$ размером L/m $(m < n)$ таким образом, что оригинальный файл F может быть восстановлен из любых доступных m частей. С теоретической точки зрения алгоритмы разделения информации представляют из себя m-из-n коды с заданной избыточностью [2], обладающие свойством «несистематичности», заключающимся в «неузнаваемости» отдельных частей файла, подвергшегося кодированию.

При этом несистематические m-из-n коды с заданной избыточностью используются для кодирования m частей $S_1, S_2, \ldots S_m$ в n «неузнаваемых» частей $F_1, F_2, \ldots F_n$ так, что

$$(S_1, S_2, \ldots S_m) * G_{m*n} = (F_1, F_2, \ldots F_n)$$

где G_{m*n} — это порождающая матрица, отвечающая следующим двум условиям:

– любой столбец матрицы G_{m*n} не равен любому столбцу единичной матрицы $m*m$;
– любые m столбцов матрицы G_{m*n} образуют невырожденную $m*m$ матрицу.

Первое условие гарантирует, что отдельные части F_1, F_2, ... F_n будут неузнаваемыми, а второе — что исходный файл F может быть восстановлен из любых доступных m частей.

С точки зрения обеспечения целостности и доступности информации данный алгоритм, в случае его применения в сетях хранения данных, не вызывает вопросов — потеря не более чем $n - m$ элементов из последовательности F_1, F_2, ... F_n все равно позволит восстановить исходные данные, как показано на рисунке 1 [3].

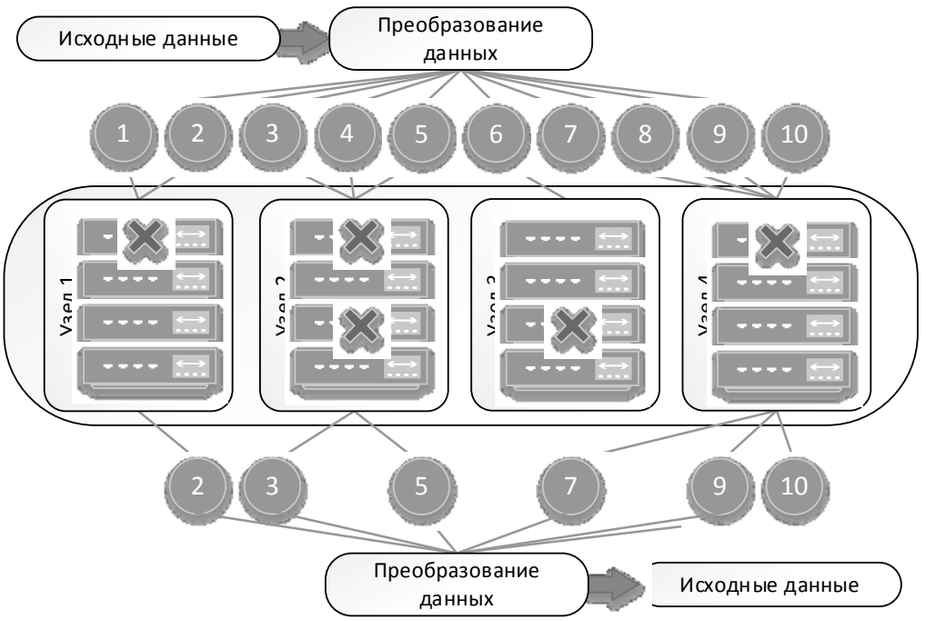


Рис. 1. Схема работы алгоритмов разделения информации

Но с точки зрения конфиденциальности данных алгоритмы разделения информации обеспечивают относительно низкий уровень безопасности информации, так как в отличие от традиционных способов защиты они изначально не были ориентированы на защиту информации от несанкционированного доступа.

В ходе последних международных исследований были получены доказательства возможности применения алгоритмов разделения информации в целях обеспечения ее конфиденциальности. Основываясь на результатах исследований, проведенных в 2012 году [4], можно сделать вывод о том, что алгоритмы разделения информации способны создать препятствия нарушителю при его попытках получить исходный файл F путем анализа данных, подвергшихся преобразованиям. Для этого все алгоритмы разделения информации как минимум должны проходить строгую проверку на выполнение следующих условий:

- алгоритмы разделения информации не обеспечивают достаточный уровень конфиденциальности тогда и только тогда, когда используемый код с заданной избыточностью соответствует следующему условию: в порождающей матрице G_{m*n} есть подматрица $A_{m'+n'}$ с рангом системы столбцов r, где m', $n' < m$ и $n' - r = m - m' > 0$;
- алгоритмы разделения информации способны обеспечить достаточный уровень конфиденциальности информации, если используемый в них код с заданной избыточностью удовлетворяет следующему условию: любая квадратная матрица из порождающей матрицы G_{m*n} является невырожденной.

Однако данные условия являются слишком общими и не учитывают множество частных вопросов, связанных с обеспечением безопасности информации, обрабатываемой в сетях хранения данных, построенных с использованием протокола iSCSI. Также на данный момент отсутствуют рекомендации, связанные с выбором порождающей матрицы G_{m*n} в целях уменьшения трудозатрат на разработку алгоритма разделения информации и его оптимизации в зависимости от текущих параметров конкретной защищаемой информационной системы. Например, в ходе исследования матриц Вандермонда на предмет их применимости в качестве порождающих матриц G_{m*n}, было установлено, что они определены над конечным полем и могут содержать вырожденные квадратные подматрицы, что нарушает одно из условий обеспечения достаточного уровня конфиденциальности информации, обрабатываемой в распределенных информационных системах.

Также, на сегодняшний день, не проводились исследования, включающие в себя оценку:

- применимости алгоритмов разделения информации в целях нейтрализации выявленных специфических угроз безопасности информации, возникающих при ее обработке в сетях хранения данных, построенных с использованием протокола iSCSI;
- эффективности алгоритмов разделения информации как возможной компенсирующей меры защиты информации в условиях применения специфической архитектуры сетей хранения данных;
- влияния алгоритмов разделения информации на параметры защищаемой информационной системы, такие как скорость передачи данных, нагрузка на вычислительные ресурсы, максимальное (минимальное) количество узлов сети и т.д.

Исходя из вышесказанного можно сделать однозначный вывод о том, что алгоритмы разделения информации на основе произвольного несистематического кода на данный момент не гарантируют конфиденциальности информации, обрабатываемой в сетях хранения данных, построенных с использованием протокола iSCSI, и требуют дополнительных исследований, как минимум включающих:

- разработку методического обеспечения оценки эффективности применения алгоритмов разделения информации в целях обеспечения безопасности информации;
- экспериментальное подтверждение правильности выбора математического аппарата, используемого в процессе в процессе оценки эффективности защиты информации от несанкционированного доступа в сетях хранения данных.

ЛИТЕРАТУРА

1. M. O. Rabin, Efficient dispersal of information for security, load balancing, and fault tolerance, Journal of the ACM, vol. 36, no. 2, pp. 335–348, Apr. 1989.
2. F.J.MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes. New York: North-Holland, 1977.
3. Cleversafe to Have Strong Presence Addressing Cloud Storage, SNIA Storage Developers Conference and Cloud Burst Summit, Sep. 2011.
4. Mingqiang Li, On the Confidentiality of Information Dispersal Algorithms and Their Erasure Codes, arXiv:1206.4123v2 [cs.IT], 2013.

СОВЕРШЕНСТВОВАНИЕ МЕТОДОВ ОБНАРУЖЕНИЯ УСТРОЙСТВ НЕСАНКЦИОНИРОВАННОГО СЪЕМА ИНФОРМАЦИИ

П. П. МАЗУР

1. Информационная сфера играет все возрастающую роль в обеспечении безопасности государства и общества.

Основными источниками угроз информационной безопасности являются противозаконная деятельность отдельных лиц, направленная на сбор, хищение и распространение (продажу) информации, закрытой для доступа посторонних.

Не секрет, что основной объем охраняемой информации в настоящее время добывается с помощью так называемых «закладных устройств». Наибольшее распространение получили радиомикрофоны, звукозаписывающие устройства и видеорегистраторы передающие информацию по радиоэфиру. Выявление и нейтрализация таких устройств представляет собой важнейшую и достаточно сложную задачу в системе мероприятий по защите информации.

Среди тенденций развития закладных устройств можно выделить увеличение времени накопления информации и повышение скорости передачи информации. Это направлено на сокращение времени нахождения закладного устройства «в эфире», что существенно затрудняет поиск таких устройств детекторами поля. Кроме того, комплексы для обнаружения закладных устройств, основанные на детектировании радиоизлучения от них, не позволяют обнаружить выключенные радиозакладки.

Основными техническими средствами поиска таких устройств на сегодняшний день являются нелинейные локаторы. В то же время рабочие частоты всех локаторов, представленных на рынке известны, и во многих профессиональных средствах разведки предусмотрены технические решения (режекторные фильтры, экранировка и т. п.), направленные на снижение вероятности их обнаружения. Кроме того, нелинейные локаторы малоэффективны при досмотре помещений, ограждающие конструкции которых выполнены из гипсокартона. Это связано с большим числом ложных сработок.

В связи с этим специалистами Учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» был предложен новый метод обнаружения закладных устройств, имеющих в своем составе приемо-передающие тракты, основанный на частотно-селективном возбуждении антенной системы и связанных с ней фильтрующих компонентов зондирующими радиоимпульсами. Обнаружение осуществляется путем приема и фиксации возникающих при облучении откликов собственных резонансных колебаний. Кроме того, данный метод позволяет обнаруживать эндовибраторы, не имеющие в своем составе нелинейные элементы. В то же время, в отличии от комплексов, предназначенных для обнаружения эндовибраторов, которые регистрируют модуляцию вторичного излучения при совместном облучении зондирующим электромагнитным и провоцирующим акустическим сигналами, для работы локатора, основанного на предложенном методе не требуется дополнительно воздействовать акустическим сигналом. Тем самым решается вопрос обеспечения скрытности проведения поисковых работ.

В период с 2012 по 2015 годы в рамках государственной научно-технической программы «Защита информации-2» в Республике Беларусь была проведена опытно-конструкторская работа, по результатам которой создан локатор для обнаружения устройств

несанкционированного съема информации «ЛВР-2Р», принцип работы которого основан на предложенном методе.

Конструктивное исполнение локатора ЛВР-2Р аналогично некоторым из представленных на рынке нелинейных локаторов «Катран», «NR-μ» и т.п. Он состоит из автономного генераторно-приемного блока, приемно-передающей антенны и соединительного кабеля.

Рис.1. Внешний вид автономного генераторно-приемного блока

Локатор работает в частотном диапазоне от 30 до 3000 МГц, что позволяет охватить подавляющее большинство типов радиозакладных устройств. Время сканирования всего диапазона частот составляет не более 3-х секунд. Дальность обнаружения составляет около 1 метра, однако практика применения показала возможность обнаружения и на больших расстояниях.

Основными недостатками, выявленными в ходе испытаний и применения, явились низкая селективность и наличие сработок от «легальных» устройств, расположенных в досматриваемом помещении. Для проведения работ целесообразно выносить из помещения все радиоэлектронные средства, не вызывающие подозрения.

При наличии исходной информации о предполагаемом диапазоне частот, на которых предположительно работают радиозакладки в проверяемом помещении, предусмотрена возможность выбора диапазона частот работы локатора, что существенно сокращает время досмотра помещения и практически исключает ложные сработки.

2. С развитием и миниатюризацией современной техники связана еще одна тенденция развития закладных устройств. Она заключается во встраивании закладного устройства в технические устройства, ставшими обычными практически в любом офисе (кабинете, квартире), такими как: телевизор, компьютер, телефон и т.п., на этапе его изготовления. Аппаратная закладка может быть активна постоянно, а может быть активирована в нужный момент путем передачи определенной команды. Команда может быть передана по радиоэфиру, через проводные линии связи, а может быть выражена и в определенном слове (фразе и т.п.).

Обнаружение таких аппаратных закладок сильно затруднено. Однако принцип их работы связан с рядом демаскирующих признаков:

– наличие приемных/передающих антенн;
– наличие «микрофона».

В то же время, в качестве указанных компонентов закладного устройства могут быть задействованы штатные компоненты технического средства.

Однако исследования показали, что самым главным демаскирующим признаком является выделение тепла при работе электронных компонентов, задействованных для реализации закладного устройства.

Так была выдвинута гипотеза о возможности обнаружения встроенных закладных устройств путем регистрации изменений температурных режимов работы радиоэлектронных компонентов при воздействии провоцирующих акустических и электромагнитных сигналов.

В период с 2011 по 2015 годы также в рамках государственной научно-технической программы «Защита информации-2» в Республике Беларусь была проведена опытно-конструкторская работа, по результатам которой создан комплекс проверки техники на наличие аппаратных средств недекларированных возможностей (шифр «Детектор»).

Обнаружение аппаратных средств съема информации осуществляется путем сравнении термограмм при штатной работе средства и фиксации изменений при воздействии на устройство провоцирующих акустических и электромагнитных сигналов.

В основе комплекса используется тепловизор с высоким разрешением (менее 0,05 С°). Такое разрешение обусловлено незначительными температурными изменениями, происходящими в радиоэлектронных компонентах при их работе.

В состав комплекса также входят:

– генератор провоцирующих электромагнитных сигналов;
– комплект антенн;
– акустическая колонка
– компьютер переносной.

Управление комплексом осуществляется от ПЭВМ.

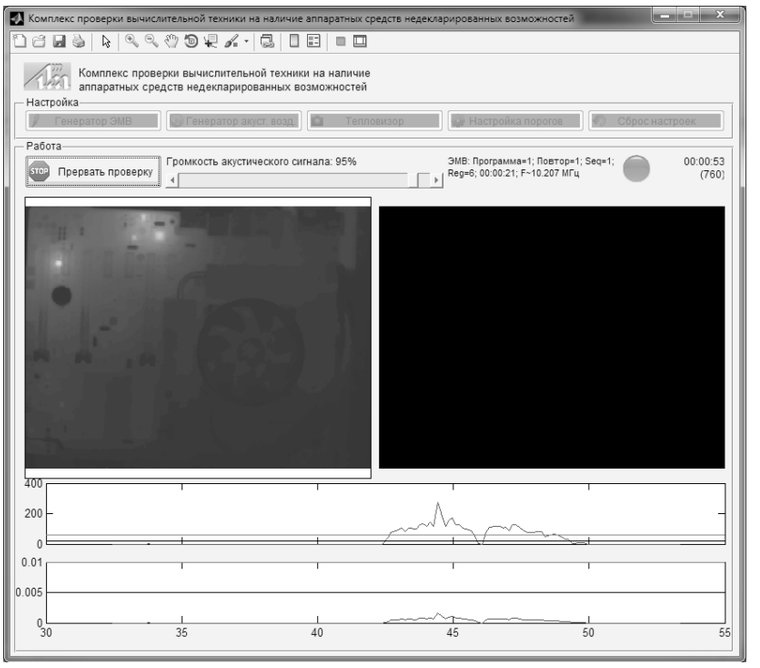


Рисунок 2. Вид рабочего окна на компьютере переносном при выполнении проверки

Последовательность проведения исследования определяется оператором. Температурные изменения фиксируются автоматически. Условия, при которых возникли изменения ото-

бражаются и могут быть повторно воспроизведены при просмотре оператором результатов исследований. О наличии недекларированной функции оператор принимает решение самостоятельно.

Среди недостатков комплекса необходимо отметить повышенные требования по оборудованию помещения (желательно отсутствие окон, неизменный температурный режим и т. п.), продолжительность исследования одного технического средства, а также высокая стоимость, обусловленная дороговизной комплектующих.

ПОДХОД В КОНКРЕТИЗАЦИИ ЧАСТОТ НЕКОТОРЫХ РАДИОЗАКЛАДНЫХ УСТРОЙСТВ

В. И. ВОРОШЕНЬ, П. П. МАЗУР

Использование межсетевых экранов, детекторов вторжений, средств антивирусной защиты и криптографии не обеспечивает гарантированной защиты от утечки информации и передачи команд деструктивного воздействия на компьютерные системы критически важных объектов в условиях применения продуктов информационных технологий и средств защиты информации импортного производства [1]. В связи с этим сохраняется актуальной задача по выявлению недекларированных функций и аппаратных закладных устройств, работающих по радиоканалу.

В настоящей работе на основании анализа «заплаток» в частотных диапазонах сканирующих приемников ведущего производителя даются рекомендации по конкретизации частот некоторых радиозакладных устройств.

Публикация материалов под условным названием «48 страниц каталога жучков АНБ США» вызвала в сети Интернет большой резонанс. По этому поводу в Википедии появилась отдельная страница «Каталог ANT (АНБ)», на которой изложены не только история развития прецедента и некоторые мнения экспертов, но также приведены сами рекламные листки с названиями, аннотациями и ценами изделий.

Номенклатура Каталога кроме программных продуктов содержит 28 изделий, обносящихся к аппаратным закладным устройствам. В свою очередь, эту группу можно условно разделить следующим образом. Три позиции представляют просто процессоры (микроконтроллеры), для работы которых необходима внешняя периферия, печатные платы и др. Десять устройств предназначены для работы в сетях сотовой связи: начиная от эмуляторов базовых станций и заканчивая специализированными (модернизированными) мобильными телефонами. Одиннадцать аппаратных закладных устройств работают (передают информацию) по радиоканалу. Характерно то, что функционально нет ни одного радиопередатчика. Используются приемопередатчики (transceivers) с возможностью дистанционного управления, либо организации сетевой передачи, а также транспондеры для модуляции отражения радиосигнала. О рабочих частотах радиозакладных устройств в Каталоге ничего не сообщается.

Одним из методов решения задачи по уточнению диапазонов частот радиозакладных устройств, может стать анализ запретов Федеральной Комиссии Связи США (FCC) на прослушивание эфира. Наиболее просто такую информацию можно извлечь из технических описаний сканирующих приемников, разрешенных к продаже в США.

В таблице 1 приведены частотные диапазоны сканирующего приемника IC-PCR 2500 в том виде, как это изложено в соответствующем руководстве японской фирмы ICOM Incorporated (на сайте www.icom.co.jp).

В таблице 1 номера частотным диапазонам даны условно. Первые 4 столбца в неком обобщенном виде иллюстрируют отношение FCC к возможности прослушивания информации в частотном диапазоне от 0.01 до 3300 МГц. Как видно из таблицы, фирма ICOM выполнила рекомендации соответствующих комиссий США и Франции и поставила программные ограничения в своем всеволновом приемнике. Немаловажно то, что приемник IC-PCR 2500 можно позиционировать как средство радиоконтроля; он даже не имеет общепринятых органов управления, и полностью управляется от персонального компьютера.

Выпуск приемника IC-PCR 2500 и публикация руководства пользователя к нему относятся к периоду 2005–2007 г. Для дальнейшего развития основной идеи настоящей работы полезно проследить, как трансформировались со временем описания ограничений на диапазоны сканирования приемников фирмы ICOM Inc. Так, в мануале на современную дорогостоящую модель 2007–2014 годов IC-R 9500 с расширенным до 3335 МГц диапазоном сканирования для Франции приводятся прежние данные — столбец 5 из таблицы.

Таблица 1

Частотные диапазоны сканирующего приемника IC-PCR 2500

№	Частотные диапазоны для США, МГц	Пропущенный диапазон, МГц	Пропущено МГц	Частотные диапазоны для Франции, МГц	Частотный диапазон для остальных стран, МГц
1	2	3	4	5	6
1	*0.01–810	810–851	41	0.01–30	0.01–3300
2	851–867	867–896	29	50.2–51.2	
3	896–1300	–	–	87.5–108	
4	1300–1811	1811–1852	41	144–146	
5	1852–1868	1868–1897	29	430–440	
6	1897–2306	2306–2357	51	1240–1300	
7	2357–2812	2812–2853	41		
8	2853–2867	2867–2898	31		
9	2898–3110	3110–3136	26		
10	3136–3155	3155–3181	26		
11	3181–3300				

*оригинальные значения типа 0.010000–809.999999 округлены до ближайшего целого

1. Для версии приемника, продаваемой в США, пишется просто — диапазоны сотовой связи блокированы (Cellular bands are blocked in the U.S.A. version). Эта же фраза записана в спецификации приемника IC-R 1500. Оценим эффективность такого блокирования на примере таблицы 1. Для упрощения изложения последующего материала введем термин «Заплатки FCC» вместо одного из заголовков таблицы 1 «Пропущенный диапазон».

В таблице 2 приведены частоты американского стандарта сотовой связи GSM-850 и заплаток FCC. Визуальная ширина столбцов выбрана произвольно.

Таблица 2

Сопоставление с американским стандартом GSM-850

**Заплатки FCC, МГц	810–851				867–896		
Частоты GSM-850, МГц		MS ↑ 824–849			2	BTS ↓ 869–894	2
Ширина опасных диапазонов, МГц	14		2				

** два первых «пропущенных» диапазона — столбец 3 из таблицы 1

Здесь и далее обозначение MS ↑ символизирует частоты передачи (восходящий трафик) мобильной станции — сотового телефона, BTS ↓ — частоты передачи базовой станции. Как видно, ширина заплаток FCC выбрана с большим запасом — обозначено заливкой серым цветом. Можно сформулировать промежуточный вывод. Пользователь такого сканирующего приемника не только не услышит, как работает мобильная связь GSM-850, но также не услышит и не увидит на спектральной диаграмме любое другое радиопередающее средство в нескольких полосах частот, равных в сумме 20 МГц.

Еще один интересный вывод можно сделать, проанализировав таким же образом, стандарт GSM-1900 (см. таблицу 3).

Таблица 3

Сопоставление с американским стандартом GSM-1900

Заплатки FCC, МГц	1811–1852	?	1868–1897	?	
Частоты GSM-1900, МГц		MS ↑ 1850–1910			BTS ↓ 1930–1990
Ширина опасного диапазона, МГц	39				

«Блокирование» этого диапазона оказалось на деле не столь эффективным, как в предыдущем случае. Пользователь приемника полностью видит и слышит работу базовых станций во всем выделенном диапазоне 1930–1990 МГц и сотовые телефоны — в двух окнах с суммарной полосой 16+13 МГц (в таблице 3 отмечены знаком?). Но самое главное остается заблокированным довольно широкий диапазон от 1811 до 1850 МГц, свободный от средств сотовой связи (также отмечено заливкой серым цветом).

Теперь можно перейти к решению поставленной задачи, предварительно задавшись вопросом: зачем понадобилось ставить ограничения на прослушивание эфира приемниками с простыми аналоговыми демодуляторами для аудио сигналов? С большой долей вероятности можно сделать вывод, что определенные выше (таким эмпирическим путем) частотные диапазоны предназначены для работы устройств негласного получения информации, в том числе и из Каталога ANT. Это не категоричный вывод. Без сомнения, что в этих же диапазонах могут также работать и другие федеральные службы, использующие средства связи с простыми незащищенными видами модуляции. Но последний фактор в настоящее время уже практически неактуален. Армейские и другие силовые ведомства повсеместно используют цифровые радиостанции, работающие в гораздо более широких

диапазонах частот, в том числе с программной перестройкой частоты или с шумоподобными сигналами. Перехватить информацию, передаваемую такими системами практически невозможно, по крайней мере, с помощью простого сканирующего приемника.

Другая ситуация складывается в области радиозакладных устройств. Судя по Каталогу ANT, остаются «на вооружении» методы снятия информации с высокочастотным подсветом (навязыванием), с использованием активных и полуактивных транспондеров (эндовибраторов). Именно для этих целей рекламируется комплект аппаратуры CTX4000, который в терминологии Википедии называется «приспособление для радаров постоянной частоты». В комплект входят: генератор на диапазон от 1 до 2 ГГц с выходной мощностью 2 Вт, усилитель мощности до 1 кВт, специализированный приемник и две направленные антенны. На основании изложенного материала можно предположить, что, по крайней мере, в США этот комплект будет работать в более узком частотном диапазоне, а именно от 1811 до 1850 МГц (см. таблицу 3). В этом случае обладатель сканирующего приемника (по всей видимости, не только фирмы ICOM Inc.) не будет шокирован огромным сигналом, наблюдаемым на спектрограмме, так как уже известно, что приемник уже настроен при изготовлении так, чтобы пропустить некоторые избранные частоты.

Можно дополнительно сформулировать еще один менее строгий тезис о том, что сами транспондеры, предназначенные для съема информации, являются специализированными устройствами, работающими, как правило, на одной частоте. Будучи спроектированными, на определенные частоты для внутреннего применения, они могут быть применены и в других странах.

Таким образом, подводя итоги, можно уточнить несколько частотных диапазонов, на которых с большей вероятностью можно ожидать угрозы со стороны радиочастотных закладных устройств из Каталога ANT/АНБ. Это опасные диапазоны: 810–824 МГц, 849–851 МГц, 867–869 МГц и 894–896 МГц (таблица 2), а также 1811–1850 МГц (таблица 3). Представленный список можно расширить, проанализировав аналогичным образом, оставшиеся пять «заплаток FCC».

ЛИТЕРАТУРА

1. *Барановский О. К.* Техническая защита информации в условиях применения импортных продуктов и систем информационных технологий // Материалы 16-й межд. НТК «Комплексная защита информации», 17–20 мая 2011 года, Гродно, РБ

ОСНОВНЫЕ ПОДХОДЫ ПРИ ОРГАНИЗАЦИИ ГОЛОСОВОГО СПАМА И СПОСОБЫ ПРОТИВОДЕЙСТВИЯ

А. С. ШЕЛКОВ, Н. В. НАСОНОВА, Л. М. ЛЫНЬКОВ
Белорусский государственный университет информатики и радиоэлектроники

Введение

С развитием VoIP-платформ организация голосового спама упростилась технически, а организация защитных мер от такого спама наоборот стала сложнее. Использование

голосового спама позволило злоумышленникам выполнять ряд задач: начиная от рекламных сообщений, заканчивая DOS-атакой на абонентов. Данная проблема затрагивает не только абонентов телефонных сетей и сетей операторов сотовой связи, но актуальна и для пользователей программ IP-телефонии, таких как Skype, Viber.

Предугадать, когда и как будет осуществляться поток вызовов голосового спама практически невозможно. Из-за особенностей организации сетей сотовой связи абоненты практически не защищены от такого вида спама. Из-за того, что большинство реализаций голосового спама основано на использовании VoIP-платформ, тодинамика интенсивности подобного спамабудет связана с динамикой развития VoIP.Динамика количества пользователей VoIP и уровня проникновения на рынок телекоммуникаций на рисунке 1 (прогноз 2012 года) [1].

Рис. 1. Динамика количества пользователей VoIP и уровня проникновения на рынок телекоммуникаций (прогноз 2012 года)

На данный момент в месяц блокируется в среднем только 10–20 обнаруженных рассылок голосового спама [2].

Основные угрозыголосового спама для конечных пользователей:

1. причинение неудобств пользователям сетей связи;
2. значительные денежные затраты абонентов сетей связи;
3. полная недоступность абонентов сетей связи для входящих и исходящих вызовов (ущерб зависит от сферы применения телефонного номера абонента);
4. принуждение абонентов сетей связи к отказу от телефонных номеров.

Анализ жалоб от абонентов РБ на различных информационных сайтах и порталах подтверждает актуальность данного вопроса.

Классификация голосового спама

Голосовой спам — выборочный либо массовыйпоток голосовых вызовов коммерческого либо другого характера, организованный с использованием технологий голосовой передачи данных.

Голосовой спам по назначению подразделяется на:

1. рекламные сообщения — используются рекламными организациями, торговыми предприятиями, а также любыми другими организациями, поскольку целевой диапазон использования таких рассылок достаточно широк;
2. лавина вызовов (CallFlood) — используются злоумышленниками в основном для создания полной недоступности абонентов сетей связи для входящих и исходящих вызовов.
3. мошеннические вызовы — используются злоумышленниками для получения денежных средств.

Самый «безобидный» тип голосового спама — это рекламные сообщения. Для организации массовой рассылки голосовых сообщений, содержащих рекламу, используются аппаратные, программные, аппаратно-программные VoIP-платформы, которые имеют подключение к SIP-провайдеру. SIP-провайдер — телекоммуникационная компания, которая обеспечивает своим клиентам (в основном юридическим лицам) доступ к телефонным сетям через протокол сигнализации SIP. Для передачи голосового трафика обычно используется протокол RTP [3].

Алгоритм подобной рассылки:

ШАГ 1 — VoIP-платформа совершает вызов абоненту из своей адресной книги (список рассылки).ШАГ 2 –если абонент поднял трубку, то VoIP-платформа проигрывает рекламное сообщение. ШАГ 3 –абонент завершает вызов либо VoIP-платформа проигрывает сообщение до конца и сама завершает вызов.

Лавина вызовов (CallFlood) — тип голосового спама, когда на определённый номер(а) совершается большое количество вызовов с большого пула номеров. На рисунке 2 и 3 изображены трейсы подобной рассылки для протокола SIP и ISUP соответственно.

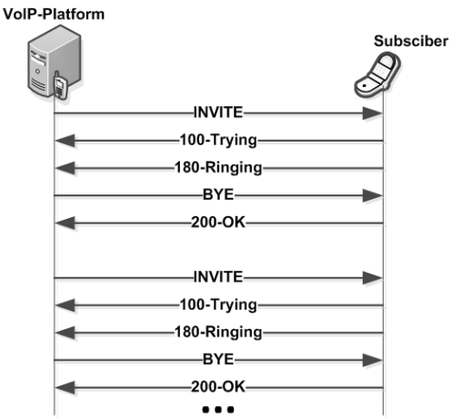


Рис. 2. Трейс CallFlood через SIP

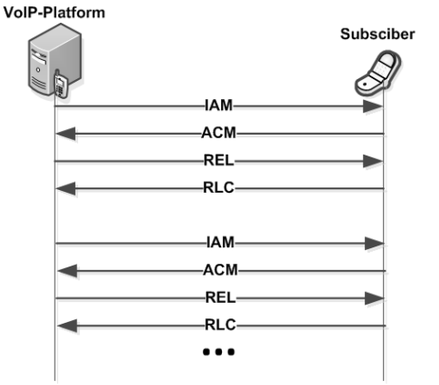


Рис. 3. Трейс CallFlood через ISUP

Таким образом, на ТА абонента постоянно совершаются вызовы, делая его недоступным для исходящих и входящих вызовов. Пример схемы технической реализации голосового спама для рекламных сообщений и лавины вызовов изображён на рисунке 4.

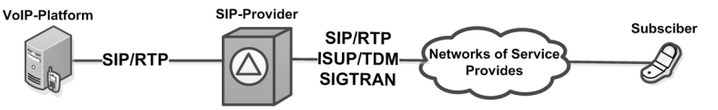


Рис. 4. Схема технической реализации голосового спама

Мошеннический способ организации голосового спама заключается в том, что злоумышленник покупает/арендует номер в стране с высокой стоимостью терминации вызова. Далее с этого номера совершается массовый обзвон абонентов из адресной книги спамера. Трейс единичного вызова для протокола ISUP изображён на рисунке 5. В данном случае злоумышленник совершает короткий вызов и бросает трубку. Злоумышленник совершает

массовый обзвон с расчётом на то, что кто-нибудь ему перезвонит, за счёт чего звонящий абонент потеряет денежные средства.

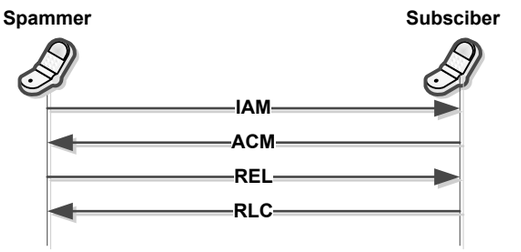


Рис. 5. Трейс вызова при мошенническом способе голосового спама через ISUP

Анализ возможных способов защиты

Рассылка рекламных сообщенийосуществляется с небольшого пула номеров и обычно не блокируется. Абонент-получатель обычно отказывается от рассылки у компании, которая рассылку осуществляет. Однако, если сервис-провайдер получает большое число жалоб от абонентов, то он может и заблокировать пул рекламных номеров в своей сети.

Сложность блокирования лавины вызовов зависит от величины пула номеров, с которого осуществляются вызовы. Грамотно организованную лавину вызовов через SIP-провайдера, находящегося в другой стране, блокировать невозможно без ущерба для абонентов.

Как правило, стандартный способ блокировки мошеннических вызовах — блокировка исходящих вызовов с номера мошенника. Возможность такой блокировки зависит от гибкости настроек коммутационного оборудования сервис-провайдера. В этом случае лучшая защита — информированность абонентов.

Остальные способы блокировки без влияния на абонентов технически не реализуемы.

Более эффективное договорное взаимодействие между сервис-провайдерами и SIP-провайдерами позволит избежать самого попадания спам-вызовов в сети первых. Данные подходы ещё только в процессе разработки и существенного влияния на текущую ситуацию не оказывают.

Заключение

Как показывает анализ, противодействие голосовому спаму возможно только при следующих условиях:

1. злоумышленники используют малый пул номеров, например, 05789xxxxxxx (наиболее актуально для лавины вызовов);
2. гибкость настроек коммутационного оборудования, что позволит блокировать спам-вызовы без серьёзной нагрузки на оборудование, либо специальное устройство, функционирующее как брандмауэр для спама, например, специальный STP-шлюз;
3. сознательность абонентов, то есть абоненты информированы о возможности подобного спама и способны оперативно проинформировать своего провайдера о факте спама.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Статья «Российский и мировой рынок IP-телефонии в корпоративном и частном сегментах». Режим доступа: http://www.json.ru/poleznye_materialy/free_market_watches/analytics/rossijskij_i_mirovoj_rynok_ip-telefonii_v_korporativnom_i_chastnom_segmentah.

2. Статистический отчёт ИП «Велком» с 2012 по 2015 год.
3. Официальный сайт провайдер «Телфин». Режим доступа: http://www.telphin.ru.
4. ETS 300 343 «Integrated Services Digital Network (ISDN); Signalling interworking specification for ISDN User Part (ISUP) version 1».
5. 3GPP TS 24.229 «IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3».

ПАНЕЛИ ЭЛЕКТРОМАГНИТНОЙ ЗАЩИТЫ ПОМЕЩЕНИЙ НА ОСНОВЕ ТЕХНИЧЕСКОГО УГЛЕРОДА И ДРЕВЕСНОГО УГЛЯ НА ЦЕЛЛЮЛОЗЕ ПИРАМИДАЛЬНОЙ ФОРМЫ

Х.А.Э. АЙАД, А.М.А. МОХАМЕД, Т.А. ПУЛКО, Л.М. ЛЫНЬКОВ
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники»

Предложены комбинированные панели пирамидальной формы, с покрытиями на основе углеродсодержащих порошкообразных наполнителей в водно-дисперсионном составе «Агнитерм».

Для защиты жилых, промышленных и выделенных помещений от электромагнитного загрязнения, необходимо создание универсальных композиционных покрытий для конструкций экранов ЭМИ, ослабляющих электромагнитное излучение СВЧ диапазона, экологически совместимых с человеческим организмом, обладающих пониженными стоимостью и массогабаритными характеристиками, что являлось целью проведенных исследований. Помимо высоких поглощающих свойств растворного и порошкообразного наполнителей в диапазоне СВЧ снижение коэффициента отражения достигается также за счет формирования геометрических неоднородной поверхности экрана, что приводит к возникновению многочисленных переотражений в объеме экрана и затуханию энергии ЭМИ.

На настоящий момент перспективным является создание экранов электромагнитного излучения на основе композиционных материалов, содержащих порошкообразные углеродосодержащие и растворные наполнители. Для этих целей используются различные модификации углерода: аморфный углерод, графит, углеродные нанотрубоки и др. Учитывая широкополосность характеристик поглощения ЭМИ СВЧ водой и водными растворами, на основе компонентов с магнитными и диэлектрическими потерями, предложено разработать композиционный экран ЭМИ в виде панелей пирамидальной формы на основе целлюлозы с комбинированным покрытием на основе технического углерода и древесного угля.

Использование в качестве материала основы целлюлозы обусловлено высокой впитывающей способностью, воздухопроницаемостью, гигроскопичностью, что обуславливается капиллярно-пористым коллоидным характером ее структуры [1]. В качестве порошкообразных наполнителей для синтеза экранирующего композиционного покрытия были предложены — древесный уголь и технический углерод. Древесный уголь является экологически чистым природным сорбентом, микропористым высокоуглеродистым продуктом. Технический углерод — высокодисперсное углеродистое вещество, отличающееся турбостратным (разориентированным) строением частиц, органофильностью их

поверхности, широким интервалом размеров первичных частиц и их агрегатов, разнообразием форм распределения частиц, способностью формировать вторичную пространственную структуру [2]. Для увеличения эффективности поглощения электромагнитного излучения при синтезе покрытия использовался нетоксичный, гигроскопичный раствор хлористого кальция $CaCl_2$.

Для реализации поставленной цели были сформированы образцы панелей электромагнитной защиты пирамидальной формы с площадью основания 0,4 × 0,4 м^2 и высотой пирамидальных элементов (полых внутри) порядка 0,45 м, что коррелирует с рабочими длинами волн разработанной конструкции. В качестве связующего компонента покрытия использовался водно-дисперсионный состав «АгниТерм М». Огнестойкое покрытие «АгниТерм М» обеспечивает пассивную противопожарную защиту путем образования под воздействием высокой температуры трудногорючего пенообразного термоизолирующего слоя (кокса).

Измерение экранирующих характеристик проводилось на автоматизированном измерителе модуля коэффициентов передачи и отражения SNA 0.01–18 в диапазоне частот 0,7…3,0 ГГц. Ослабление, вносимое исследуемым образцом, определяется отношением напряженностей волн, падающей и прошедшей через образец. Коэффициент отражения R характеризует долю падающей энергии ЭМИ, отраженную от образца.

Коэффициент передачи для образца № 1 (массов ая доля технического углерода 10 %) имеет минимальные значения (–3,1…–8,2 дБ), при увеличении концентрации углерода в составе краски коэффициент передачи увеличивается, для образца № 2 (массовая доля технического углерода 30 %) –0,3…–3,4 дБ, для образца № 3 (массовая доля технического углерода 50 %)–0,4…–4,2 дБ. Коэффициент отражения для всех образцов одинаковый и составляет–0,5…м19,5 дБ (рисунок 1).

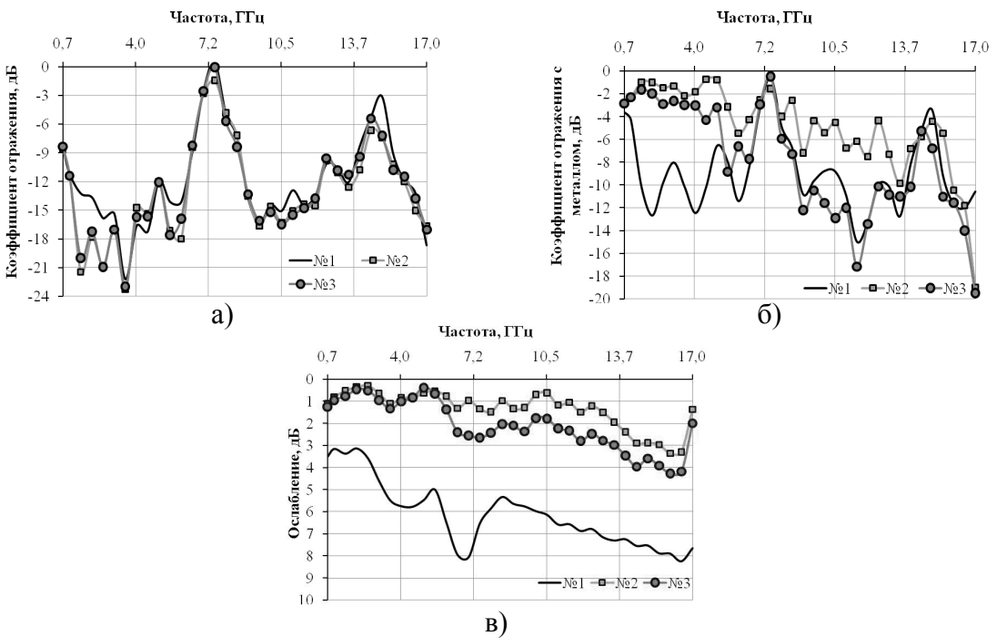


Рис. 1. Частотная зависимость экранирующих характеристик образцов панелей электромагнитной защиты на основе технического углерода на целлюлозе пирамидальной формы в частотном диапазоне 0,7…17,0 ГГц: а) коэффициент отражения; б) коэффициент отражения с металлом; в) ослабление

При увеличении концентрации углерода в составе огнестойкой краски коэффициент отражения, измеренный с металлическим отражателем за образцом, увеличивается. Для образца № 1 (массовая доля технического углерода 10 %) коэффициент отражения имеет значения порядка –0,6…–22,1дБ, для образца № 2 (массовая доля технического углерода 30 %) –0,7…–11,8 дБ, для образца № 3 (массовая доля технического углерода 50 %) значения коэффициента отражения изменяются от –0,5 дБ до –19,5 дБ с резонансом на частотах 5…7 ГГц.

На основании полученных зависимостей ослабления ЭМИ от частоты было установлено, что образцы с покрытиями на основе древесного угля (образец 4) в диапазоне 0,7…3,0 ГГц характеризуются значениями ослабления ЭМИ в пределах 2,0…17,0 дБ (рисунок 2). Причем разница в значениях ослабления ЭМИ в зависимости от состава наполнителя находится в пределах 2,0 дБ. Установлено, что значение коэффициента отражения ЭМИ находится в пределах –4,0…–22 дБ на частотах 0,7…3,0 ГГц независимо от состава покрытий, что определяется пирамидальной поверхностью образцов. В режиме короткого замыкания в диапазоне частот 0,7…1,5 ГГц наблюдается значительный разрыв в значениях коэффициентов отражения ЭМИ. Так, для покрытий с использованием древесного угля в составе покрытия значение коэффициента отражения ЭМИ находится в пределах –8,0…–26,0 дБ, тогда как для образцов с комбинированным покрытием (древесный уголь, TiO_2) значения коэффициента отражения находятся в пределах –2,0…–10,0 дБ.

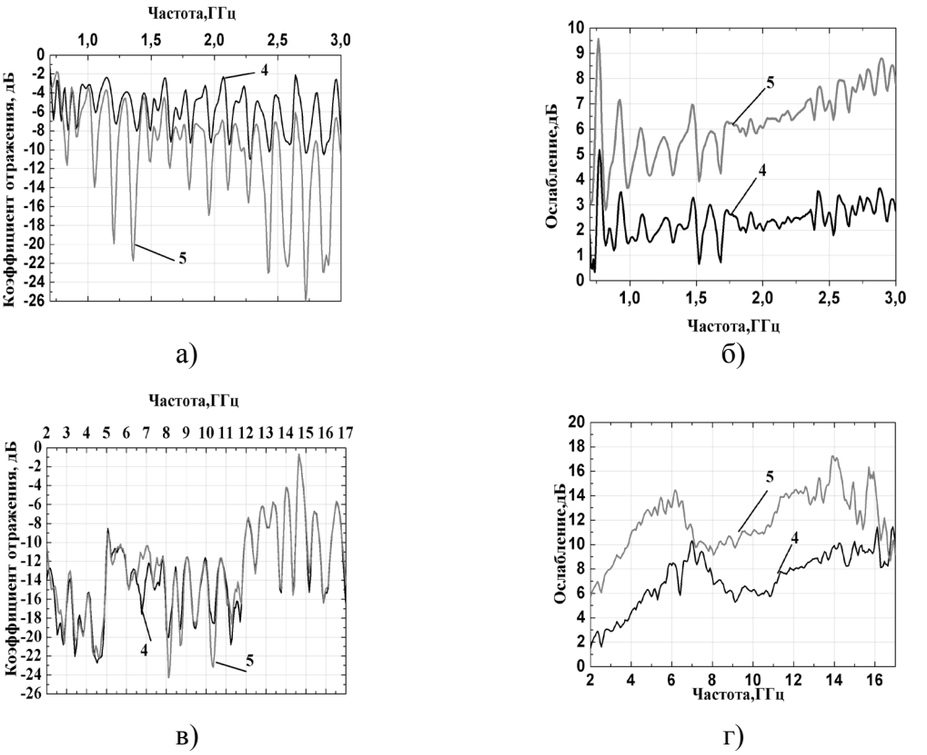


Рис. 2. Частотная зависимость экранирующих характеристик образцов панелей электромагнитной защиты на основе древесного угля на целлюлозе пирамидальной формы в частотном диапазоне 0,7…3,0 ГГц: а) коэффициент отражения; б) ослабление и в диапазоне 2,0…17,0 ГГц: а) коэффициент отражения; б) ослабление

С увеличением частоты в диапазоне частот 2,0…17,0 ГГц наблюдается значительное увеличение значений ослабления ЭМИ в пределах 2,0…10,0 дБ для группы образцов с покрытием из комбинированного порошкообразного наполнителя (древесный уголь, TiO_2) (рисунок 2). Для группы образцов покрытия с использованием порошкообразного наполнителя (древесный уголь) значения ослабления ЭМИ находятся в пределах 6,0…14 дБ во всем исследуемом диапазоне частот 2,0…17,0 ГГц.

Таким образом, пирамидальная конструкция влагосодержащих экранов с разработанными комбинированными покрытиями на основе древесного угля позволяет повысить эффективность экранирования ЭМИ в частотном диапазоне 2,0…8,0 ГГц в среднем на 10,0 дБ по сравнению с экраном с плоской, что можно учесть при создании высокоэффективных экранов и поглотителей ЭМИ диапазона СВЧ.

ЛИТЕРАТУРА

1. Новые материалы для экранов электромагнитного излучения / Л. М. Лыньков [и др.] // Доклады БГУИР. — 2004. — Т. 2, № 5. — С. 152–167.
2. *Ruddick W.* Tech Service: Carbon black dispersion measurement / W. Ruddick // Rubber World. — 2006. — Vol. 233, № 4. — P. 15.

ШИРОКОПОЛОСНЫЕ ЭКРАНЫ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ НА ОСНОВЕ ВЛАГОСОДЕРЖАЩИХ КОМПОЗИТОВ

Н. В. НАСОНОВА, И. А. ГРАБАРЬ, Л. М. ЛЫНЬКОВ
Белорусский государственный университет информатики и радиоэлектроники

Отдельным направлением, связанным с побочными электромагнитными излучениями (ЭМИ) средств вычислительной техники, является необходимость создания мобильных средств для обеспечения защиты информации от утечки через каналы ПЭМИ. При этом широко применяются радиопоглощающие материалы, локально перераспределяющие энергию ЭМИ. Возможность программно управлять генерацией электромагнитного излучения компьютера без внедрения аппаратных закладных устройств [1] создает угрозу возникновения дополнительного канала утечки конфиденциальной информации, который сложно поддается контролю.

Исходя из отклика воды на электромагнитное излучение в широкой области частот миллиметрового диапазона, экраны и радиопоглотители, эффективно поглощающие электромагнитную энергию в диапазоне СВЧ, охватывающим частотную область информативных побочных излучений технических средств обработки информации. Вода представляет собой полярный диэлектрик с максимумом потерь в диапазоне СВЧ и поглощение ЭМИ водой обусловливается работой электромагнитной энергии на ориентацию диполей молекул воды в соответствии с линиями внешнего электрического поля.

Целью работы являлось разработка широкополосных экранов электромагнитного излучения на основе влагосодержащих композитов.

Для размещения воды и водных растворов предложено применять высокопористые сорбенты на основе волокнистых, порошковых материалов, химических соединений.

В научно-исследовательской лаборатории БГУИР разрабатываются и изучаются экраны и поглотители ЭМИ на основе воды и водных растворов, закрепленных в различных пористых порошковых и волокнистых матрицах [2–4]. Эффективность экранирования ЭМИ такими материалами достигает свыше 40 дБ, возможно получение коэффициента отражения ЭМИ до –15,0… –5,0 дБ в диапазоне частот 0,7…117 ГГц. Разработан ряд приемов стабилизации экранирующих характеристик формируемых композиционных влагосодержащих материалов в широком диапазоне температур и условий эксплуатации. Предложены элементы конструкций экранов и радиопоглотителей ЭМИ, обладающих гибкостью, оптической прозрачностью, вид которых зависит от особенностей их применения.

Взаимодействие влагосодержащих материалов с ЭМИ определяется их влагосодержанием и структурой, которые определяют диэлектрические свойства композитов. Моделирование диэлектрической проницаемости и диэлектрических потерь исследуемых материалов позволяет разрабатывать различные конструкции экранов и радиопоглотителей, а также задавать технологические параметры изготовления влагосодержащих сред для получения определенных диэлектрических характеристик.

В ходе исследования были получены частотные зависимости комплексных параметров диэлектрической проницаемости для исследованных волокнистых матриц с различным влагосодержанием, а также была построена математическая модель исследуемых материалов. Толщина образцов составляла 1,3 мм и 1,2 мм соответственно. Влагосодержание матриц изменялось в пределах 10…55 % мас. с шагом 5 %.

Результаты расчетов показали, что диэлектрическая проницаемость влагосодержащих волокнистых матриц из синтетических волокон возрастает пропорционально увеличению влагосодержания от 2,5 до 10 при изменении влагосодержания с 10 до 40 %. Это связано с тем, что вода распределена в межнитевых и межволоконных пространствах волокнистой матрицы, которая обладает большой площадью поверхности пор и, как следствие, большой поверхностью контакта твердого тела с водой. В результате, на молекулы воды, распределенные в поровых промежутках, воздействуют силы притяжения поверхности твердого тела, ограничивая их диэлектрическую восприимчивость и снижая величину диэлектрической проницаемости.

Для влагосодержащих материалов из натуральных волокон в диапазоне влагосодержаний 15…50 % мас. диэлектрическая проницаемость увеличивается с 15 до 30, а при 55 % мас. влагосодержании составляет уже 58. Особенностью исследуемой влагосодержащей матрицы является способность натурального волокна к набуханию и взаимодействие ее макромолекул с молекулами воды, что влияет на подвижность молекул воды и способность диполей взаимодействовать с внешним электрическим полем. Это приводит к тому, что большая часть молекул воды в целлюлозной матрице оказывается в «связанном» состоянии, вследствие чего появление объемной формы воды и область повышения наклона кривой ε' наблюдается при величине влагосодержания 50 %. Диэлектрические потери при изменении влагосодержания изменяются незначительно и составляют 4,7…6. Полученное небольшое изменение диэлектрических потерь с увеличением водосодержания матриц может быть связано с высокой пористостью и большой удельной поверхностью пор исследуемых волокнистых материалов, что обусловливает наличие большого количества воды, находящейся вблизи поверхности твердого тела и попадающей под влияния поверхностных сил.

При построении модели диэлектрической проницаемости исследуемого материала, состоящего из нескольких фаз: твердого тела образующей матрицы, жидкости (свобод-

ной и связанной воды) и воздуха, была использовала формула рефракционной модели [5] закона смешения для определения диэлектрической проницаемости смесей:

$$\sqrt{\varepsilon_м} = v_1 \cdot \sqrt{\varepsilon_1} + v_2 \cdot \sqrt{\varepsilon_2} + v_3 \cdot \sqrt{\varepsilon_3}\ , \tag{1}$$

где v — парциальный объем каждого компонента смеси, ε — диэлектрическая проницаемость каждого компонента смеси.

В применении к исследуемым волокнистым водосодержащим матрицам это выражение может быть записано следующим образом:

$$\sqrt{\varepsilon_м} = v_{вол} \cdot \sqrt{\varepsilon_{вол}} + v_{вод} \cdot \sqrt{\varepsilon_{вод}} + v_{возд} \cdot \sqrt{\varepsilon_{возд}} \tag{2}$$

где $v_{вол}$, $v_{вод}$, $v_{возд}$ — объемная доля волокнистого материала, воды и воздуха соответственно в рассматриваемом композиционном материале; $\varepsilon_{вол}$, $\varepsilon_{вод}$, $\varepsilon_{возд}$ — диэлектрическая проницаемость компонентов композиционного материала: волокнистого материала, воды и воздуха соответственно.

Высокая пористость исследуемых матриц и рассмотрение воды в порах в виде многослойной структуры свидетельствуют о необходимости учета диэлектрических свойств связанной и свободной воды в качестве компонентов. Для этого применялась теорией смесей:

$$\sqrt{\varepsilon_{вод}} = v_{связ.вод} \cdot \sqrt{\varepsilon_{связ.вод}} + v_{своб.вод} \cdot \sqrt{\varepsilon_{своб.вод}} \tag{3}$$

где $v_{связ.вод}$, $v_{своб.вод}$ — доля связанной и свободной воды в общем объеме воды; $\varepsilon_{связ\ вод.}$, $\varepsilon_{своб.\ вод}$ — диэлектрическая проницаемость связанной и свободной воды соответственно.

Применительно к влагосодержащим пористым матрицам можно составить систему из трех уравнений:

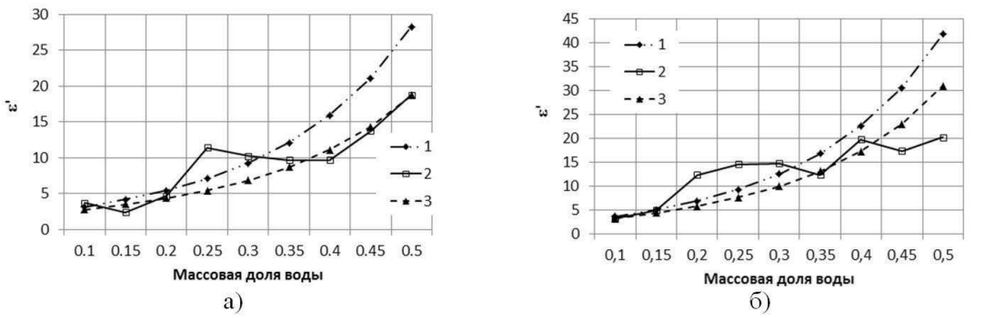
$$\begin{aligned} v_{связ.вод} \cdot \sqrt{\varepsilon_{связ.вод}} + v_{своб.вод} \cdot \sqrt{\varepsilon_{своб.вод}} + v_{возд} \cdot \sqrt{\varepsilon_{возд}} = \\ = \sqrt{\varepsilon_м} - v_{вол} \cdot \sqrt{\varepsilon_{вол}} \end{aligned} \tag{4}$$

$$\rho_{связ.вод} \cdot v_{связ.вод} + \rho_{своб.вод} \cdot v_{своб.вод} + \rho_{возд} \cdot v_{возд} == \rho_м - \rho_{вол} \cdot v_{вол} \tag{5}$$

$$v_{связ.вод} + v_{своб.вод} + v_{возд} = 1 - v_{вол} \tag{6}$$

где $v_{вол}$, $v_{вод}$, $v_{возд}$ — объемная доля волокнистого материала, воды и воздуха соответственно в рассматриваемом композиционном материале; $\varepsilon_{вол}$, $\varepsilon_{вод}$, $\varepsilon_{возд}$ — диэлектрическая проницаемость компонентов композиционного материала: волокнистого материала, воды и воздуха соответственно.

По результатам моделирования построены зависимости диэлектрической проницаемости волокнистых материалов от их влагосодержания. Результаты представлены на рисунке.



1 — Результаты моделирования без учета связанной воды; 2 — Экспериментальные данные; 3 — Результаты моделирования с учетом связанной воды

Зависимость диэлектрической проницаемости волокнистой матрицы от влагосодержания: а) синтетическое волокно, б) натуральное волокно

Графики показывают, что диэлектрическая проницаемость модели влагосодержащего материала, заполненного свободной водой, выше, чем полученные экспериментальные данные. Это свидетельствует о существовании большого количества связанной воды, диэлектрическая проницаемость которой ниже, чем у свободной, а поскольку площадь поверхности пор большая, то и вклад связанной воды в общую диэлектрическую проницаемость материала существенный. В полученной модели можно подбором параметра k парциальной доли связанной воды привести кривую диэлектрической проницаемости к экспериментальной характеристике, и таким образом оценить количество связанной воды. Для исследованных волокнистых матриц из синтетических и натуральных волокон величина k составила 0,4 и 0,3 соответственно.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Представлен метод извлечения данных с изолированных от внешнего мира компьютеров: [Электронный ресурс] — Код доступа: http://www.securitylab.ru/news/479880.php, дата доступа: 28.03.2016.
2. *Колбун Н. В.* Технология изготовления экранов электромагнитного излучения на основе влагосодержащих капиллярно-пористых материалов // Дисс. … канд. техн. наук: 05.27.06 — Мн., 2005. — 175 с.
3. *Борботько Т. В.* Технология создания гибких конструкций широкополосных экранов ЭМИ // Дисс. … канд. техн. наук: 05.27.06 — Мн., 2003. — 158 с.
4. Стабильность водосодержащих конструкций экранов электромагнитного излучения для защиты информации от утечки по техническим каналам: диссертация на соискание ученой степени кандидата технических наук: 05.13.19; 05.27.06: защищена 21.04.11: утверждена 28.09.11 / Пулко Татьяна Александровна; научный руководитель Насонова Наталья; Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники»
5. *Кобляков А. И.* Структура и механические свойства трикотажа, М., 1973.
6. Fang Lu, Seichi Okamura // Proc. of SPIE. — 2000. — Vol. 4129. — Pp. 82–87.

ШКОЛА МОЛОДЫХ УЧЕНЫХ

ДОВЕРЕННАЯ ЗАГРУЗКА И КОНТРОЛЬ ЦЕЛОСТНОСТИ АРХИВИРОВАННЫХ ДАННЫХ. ЧАСТЬ И ЦЕЛОЕ

А.А. АЛТУХОВ

Национальный исследовательский ядерный университет «МИФИ», Москва Россия,
Закрытое акционерное общество «ОКБ САПР», Москва, Россия

В статье показывается необходимость контролировать отдельные элементы, входящие в состав архивов. Приводятся конкретные примеры, показывающие актуальность проблемы.

Ключевые слова: доверенная загрузка, модуль доверенной загрузки, средство доверенной загрузки, резидентный компонент безопасности, доверенная вычислительная среда, доверенные вычисления, контроль целостности

Модель доверенной вычислительной среды (ДВС) [1. С. 204] остаётся на настоящий момент одной из актуальных и практически применимых субъектно-объектных моделей защиты технологи электронного обмена информации. Хотя нельзя отрицать, что развитие парадигм доверенных вычислений и субъектно-объектных моделей не стоит на месте [2]. Целый класс задач электронного обмена информации решается в рамках подхода доверенного сеанса связи (ДСС) [3–8]. Однако развитие происходит не только за счёт разработки новых парадигм, но и за счёт улучшения и совершенствования уже существующих. В частности идёт развитие в рамках субъектно-объектной модели ДВС. Появляются предложения по новым реализациям и функциональному составу резидентного компонента безопасности (РКБ) [9; 10], наличие которого предполагается в ДВС [1. С. 1]. Не следует забывать и о средствах доверенной загрузки, как наиболее распространённых реализациях РКБ. Процесс обеспечения доверенной загрузки по-прежнему является одним из основных способов решения проблемы защиты информации от несанкционированного доступа и организации доверенной вычислительной среды. Одной из наиболее популярных и проверенных временем реализаций РКБ является средство доверенной загрузки (СДЗ), в частности аппаратные (программные) модули доверенной загрузки А(П)МДЗ или в терминологии отечественных регуляторов средство доверенной загрузки уровня платы расширения. Средство доверенной загрузки — программно-техническое средство, которое осуществляет блокирование попыток несанкционированной загрузки нештатной операционной системы, контроль целостности своего программного обеспечения и среды функционирования (программной среды и аппаратных компонентов средств вычислительной техники), а также не препятствует доступу к информационным ресурсам в случае успешных контроля целостности своего программного обеспечения и среды функционирования, проверки подлинности пользователя и загружаемой операционной системы [11–14].

Большинство современных и проверенных временем систем защиты информации от несанкционированного доступа включают в себя компонент, обеспечивающий доверенную загрузку. Он является фундаментальной составляющей многих систем защиты [15], которые выполняют самые различные функции безопасности: аудита, аутентификации,

разграничения доступа и прочие функции безопасности, — в операционных системах (ОС) [16; 17], средствах виртуализации [18, 19], системах управление базами данных, электронном документообороте и т.д.

Контроль целостности элементов среды является одной из основ создания ДВС [1, С. 219]. Следовательно, одна из основных групп функций, которые должны быть реализованы РКБ — это функции контроля целостности: контроль целостности технического состава ЭВМ и локально вычислительной сети (ЛВС), контроль целостности ОС, контроль целостности прикладного программного обеспечения (ППО) и данных [Там же, С 266]. Необходимость выше описанных функций не противоречит нормативным документам отечественных регуляторов. В список основных угроз безопасности информации, нейтрализация которых должна быть обеспечена, входят: нарушение целостности программной среды средств вычислительной техники и (или) состава компонентов аппаратного обеспечения средств вычислительной техники в информационной системе, нарушение целостности программного обеспечения средства доверенной загрузки [11, С. 5].

Все множество функций контроля можно сгруппировать в три класса.

- контроля целостности технических средств ЭВМ,
- контроль целостности системных областей жёстких дисков,
- контроль целостности отдельных файлов и программных средств.

Последняя в списке группа и отвечает за осуществление контроля целостности ОС и необходимых программных компонентов, в том числе и иных средств защиты и элементов комплексов защиты, работающих после СДЗ в ДВС.

Данная функция реализуется как пошаговый контроль целостности объектов файловых систем для различных файловых систем: *FAT12, FAT16, FAT32, NTFS, HPFS, Ext2, Ext3, Ext4, FreeBSD UFS/UFS 2, Solaris UFS, QNX4, MINIX, ReiserFS* [1, С. 266; 15]. Иными словами для возможности контроля целостности загружаемой операционной системы, необходимо осуществлять контроль целостности исполняемых файлов и файлов конфигурации, необходимых и влияющих на загрузку ОС. Следует отметить, что на практике конкретные типы файловой системе соответствуют конкретной операционной системе.

Для осуществления контроля данных: файлов, каталогов и прочих объектов файловых систем — необходимо получить доступ к этим данным. Данные могут находиться как на различных аппаратных носителях (например, не только на обычных жёстких дисках, но и на накопителях на магнитной ленте и RAID массивах), так и на различных файловых системах. В силу того факта, что СДЗ работает до загрузки ОС и должно быть самодостаточным, для успешного контроля целостности, необходимо обеспечить разбор файловых систем.

В соответствии с парадигмой ДВС и требованиями к функции СДЗ нет необходимости контролировать абсолютно все. Под целостностью вычислительной среды понимают стабильность в течение рассматриваемого периода в требуемом диапазоне состава объектов и процессов, их взаимосвязей и параметров функционирования [1, с. 207]. Какой состав, какие параметры и взаимосвязи и в течение какого периода времени — все это определяется для каждого конкретного случая. . На практике на состав контролируемых параметров (в частности список контролируемых файлов) могут влиять такие конкретные вещи, как тип операционной системы [20 С. 17; 21 С. 52], функции, выполняемые автоматизированной системой и прочие. Тонкая настройка достигается за счёт возможности контроля отдельных файлов и их атрибутов [21 С. 34].

Есть особые типы файлов, которые являются структурами данных, каждый элемент которых может использоваться различными программами и процессами. Иными сло-

вами, несмотря на то, что данная структура в файловой системе представлена одним или несколькими элементами, на самом деле она является коллекцией логических элементов. Одни логические элементы в конкретном случае влияют на загрузку ОС, а другие нет.

Под коллекцией данных будем разуметь некоторый набор логических элементов, которые представлены одним или несколькими объектами файловой системы. Примерами могут служить различные файлы конфигураций, базы данных, образы дисков, архивы и прочие различные структуры данных.

Одним из примеров подобной коллекции данных является реестр *Windows* [23]. Поскольку на процесс загрузки операционных систем семейства *Windows* влияют не только системные файлы, но и реестр, контроля файловой системы не достаточно для того, чтобы убедиться в корректности загрузки этих ОС, необходимо также проконтролировать неизменность отдельных ветвей реестра.

Штатная работа многих программ в течение одной сессии пользователя предполагает модификацию некоторых веток реестра, которые не влияют на доверенную загрузку. Работа ОС вполне может предполагать изменения реестра в рамках сеанса работы. Таким образом, после завершения работы файлы, в которых содержится реестр, меняются. Попытка контролировать реестр на уровне файловой системе становится несостоятельной, что проявляется в практической невозможности создать рабочую доверенную среду. В этом случае для обеспечения доверенной загрузки ОС семейства *Windows* необходимо обеспечить возможность контроля отдельных элементов системного реестра [15; 21 С. 10].

Обобщая выше сказанное, можно выйти на более глобальную идею. Возможность контролировать логические элементы коллекции данных позволит обеспечить возможность более тонкой настройки контролируемых параметров ДВС. В частности контроль отдельных настроек, занесённых в файл конфигурации (пусть даже не сложной структуры, например обычные текстовых *INI*) позволяет расширить возможности эксперта, определяющего условия функционирования системы доверенной обработки информации. Важно понять, что конкретный объект файловый системы не является «логически атомарным». Он может содержать различные логические элементы, часть из которых влияет на процесс обеспечения доверенной загрузки, а другая часть нет. Таким образом, с практической точки зрения встаёт вопрос определения коллекций данных, влияющих на загрузку ОС и реализацию функциональности СДЗ контроля отдельных логических элементов коллекций данных.

Выше был приведён пример и показана необходимость контролировать состава коллекции данных, влияющих на загрузку ОС. Коллекция данных является широким понятием и существует потенциально бесконечное количество конкретных примеров. В данной работе предлагается ограничиться рассмотрением некоторых коллекций данных, логическими элементами которых являются файлы.

Под «виртуальными дисками» будем подразумевать такие коллекции данных, логические элементы которых являются объектами файловых систем: файлы и каталоги. Примерами виртуальных дисков могут служить различные форматы архивов и различные образы дисков.

Говоря об архивах, следует отметить, что традиционно они используются для удобства хранения и переноса информации (например, передачи по каналам связи), а также экономии места, занимаемого на накопителях.

Однако во многих ОС в процессе загрузки используются определённые типы архивов. Рассмотрим некоторые наиболее важные и актуальные примеры.

vSphere Hypervisor или *ESXi* — это аппаратный гипервизор, который устанавливается непосредственно на физический сервер и разделяет его на несколько виртуальных машин [22]. Формально *ESXi* является такой же операционной системой как *Windows* или *GNU\Linux*, не считая того, что он создан для выполнения строго конкретной задачи — виртуализации. Не приводя подробной структуры разбиения диска на разделы и перечня файлов, замечу, что в состав файлов *ESXi* входит файл с именем *state.tgz*, который является, образом файловой системы гипервизора. Данный файл является сжатым *tar* архивом корневой файловой системы *ESXi* и является, необходим для загрузки ОС *ESXi*.

Ещё одним важным примером «виртуальных дисков» является файл *initrd*. Загрузка ОС на базе ядра Linux обычно предполагает загрузку двух элементов. Файла ядра операционной системы и файла, содержащего временную файловую систему (следует отметить, что два выше перечисленных элемента физически могут представлять один файл). *Initrd* (*Initial RAM Disk*, диск в оперативной памяти для начальной инициализации) — временная файловая система, используемая ядром Linux при начальной загрузке. *Initrd* обычно используется для начальной инициализации перед монтированием корневых («настоящих») файловых систем, которые обычно расположены в ПЗУ, например на жёстком диске ПЭВМ. Данный подход решает проблему функциональной достаточности модульного ядра ОС во время загрузки: для монтирования файловой системы необходим модули для работы с диском и файловой системой, а для чтения модулей необходима файловая система, с которой этот модуль читается [24]. Файл *initrd* является сжатым архивом *cpio*.

Ещё одним примером является архив типа *squashfs (.sfs)* — сжимающая файловая система, предоставляющая доступ к данным в режиме «только для чтения». Данная файловая система используется преимущественно в ОС GNU/Linux. Данная файловая система широко используется в файловых системах предназначенных «только для чтения» (Live CD), а также в ограниченных по размеру блочных устройствах или системах хранения (во встраиваемых системах и тонких клиентах) [22]. Обычно данный виртуальный диск представлен в виде целого файла-архива, в котором находиться образ корневой файловой системы.

Три выше приведённых типа архива обладают несколькими общими свойствами:

- являются образами файловой системы, которые необходимы для загрузки и/или работы ОС,
- являются одним объектом файловой системы (файл),
- содержат в себе несколько файлов (являются виртуальными дисками).

Из выше приведённых свойств следует, что изменение любого логического элемента, входящего в состав архива, сопровождается изменением всего файла. В случае если нет возможности контролировать состав элементов архива по отдельности, то возможно только фиксировать изменение файла архива целиком. Изменения в данные файлы могут вноситься как в процессе обновления, так и в процессы работы ОС. Таким образом, штатная работа или обновление ОС, не влияющие на доверенную загрузку и вносящие изменения в вышеперечисленные архивы, будут фиксироваться СДЗ как нарушения контроля целостности, в результате чего будут возникать дополнительные издержки, связанные с фиксацией инцидента и реагированием на него. Вышеописанная проблема возникает из-за отсутствия технической возможности реализовать выбор диапазона состава объектов и процессов, их взаимосвязей и параметров функционирования вычислительной среды в соответствии с конкретной задачей.

Решать вышеуказанную проблему возможно подстроив задачи под функциональные возможности СДЗ, тем самым ограничивая функциональные возможности автоматизи-

рованных систем и фактически сузив возможные варианты реализации ДВС. Однако не следует забывать, что СДЗ является лишь средством, которое должно работать в соответствии с постулатами ДВС.

Для организации тонкой настройки контроля целостности параметров вычислительной среды и повышения эффективности работы процессов, реализующих меры защиты, необходимо обеспечить возможность контроля отдельных элементов: файлов и каталогов, входящих в состав архива и влияющих на загрузку ОС.

Возможность контролировать файлы, входящие в составе архивов добавлена в АМДЗ Аккорд. В интерфейс администрирования была добавлена функциональность работы с виртуальными дисками. Просматривая содержимое файловой системы, пользователь имеет возможность выбрать файлы, которые поддерживаются в АМДЗ в качестве виртуальных дисков. После подключения, выбранного виртуального диска, он появляется в списке виртуальных дисков и с ним можно работать таким же образом, как и с физическими дисками, просматривать содержание и ставить конкретные файлы и каталоги на контроль.

Кроме трёх выше перечисленных архивов (*Squashfs*, *tar.gz* и *cpio*) также поддерживаются архивы *zip* и образы *CD/DVD* дисков *ISO9660*.

СПИСОК ЛИТЕРАТУРЫ

1. *Конявский В. А., Гадасин В. А.* Основы понимания феномена электронного обмена информацией (Библиотека журнала «УЗИ»; Кн. 2). Мн.: «Беллитфонд», 2004. — 282 с.
2. «Доверенная гарвардская» архитектура — компьютер с динамически изменяемой архитектурой.// Комплексная защита информации: материалы XX науч. — практ. конф., Минск, 19–21 мая 2015 г. — Минск: РИВШ, 2015, с 32–37.
3. *Конявский В. А.* Доверенный сеанс связи. Развитие парадигмы доверенных вычислительных систем — на старт, внимание, МАРШ! // Комплексная защита информации. Материалы XV международной научно-практической конференции (Иркутск (Россия), 1–4 июня 2010 г.). М., 2010.
4. *Каннер А. М.* Средство организации доверенного сеанса как альтернатива доверенной вычислительной среде // Информационные технологии управления в социально-экономических системах. Вып. 4. М., 2010. С. 140–143.
5. *Счастный Д. Ю.* Ноутбук руководителя// Комплексная защита информации: материалы XX науч. — практ. конф., Минск, 19–21 мая 2015 г. — Минск: РИВШ, 2015, с 112–113.
6. Съёмный носитель информации. Патент на полезную модель № 102139. 10.02.2011, бюл. № 4.
7. Съёмный носитель информации с безопасным управлением доступом. Патент на полезную модель № 123571. 27.12.2012, бюл. № 36.
8. Съёмный носитель информации на основе энергонезависимой памяти с расширенным набором функций информационной безопасности. Патент на полезную модель № 130441. 20.07.2013, бюл. № 20.
9. *Алтухов А. А.* Неатомарный взгляд на РКБ как на композицию перехвата управления и контроля целостности// Комплексная защита информации: материалы XX науч. — практ. конф., Минск, 19–21 мая 2015 г. — Минск: РИВШ, 2015, с 53–55.
10. *Алтухов А. А.* Контроль доступа на основе атрибутов и оптимизация управления множеством АПМДЗ// Комплексная защита информации: материалы XX науч. — практ. конф., Минск, 19–21 мая 2015 г. — Минск: РИВШ, 2015, с 55–60.

11. МЕТОДИЧЕСКИЙ ДОКУМЕНТ ПРОФИЛЬ ЗАЩИТЫ СРЕДСТВА ДОВЕРЕННОЙ ЗАГРУЗКИ УРОВНЯ ПЛАТЫ РАСШИРЕНИЯ ЧЕТВЕРТОГО КЛАССА ЗАЩИТЫ ИТ.СДЗ.ПР4.ПЗ [Электронный ресурс]. URLhttp://fstec.ru/component/attachments/download/661 (дата обращения: 10.04.2016).
12. МЕТОДИЧЕСКИЙ ДОКУМЕНТ ПРОФИЛЬ ЗАЩИТЫ СРЕДСТВА ДОВЕРЕННОЙ ЗАГРУЗКИ УРОВНЯ ЗАГРУЗОЧНОЙ ЗАПИСИ ПЯТОГО КЛАССА ЗАЩИТЫ ИТ.СДЗ.З35.ПЗ [Электронный ресурс]. URL: http://fstec.ru/component/attachments/download/659 (дата обращения: 10.04.2016).
13. МЕТОДИЧЕСКИЙ ДОКУМЕНТ ПРОФИЛЬ ЗАЩИТЫ СРЕДСТВА ДОВЕРЕННОЙ ЗАГРУЗКИ УРОВНЯ ЗАГРУЗОЧНОЙ ЗАПИСИ ШЕСТОГО КЛАССА ЗАЩИТЫ ИТ.СДЗ.336.ПЗ [Электронный ресурс]. URL: http://fstec.ru/component/attachments/download/660 (дата обращения: 10.04.2016).
14. МЕТОДИЧЕСКИЙ ДОКУМЕНТ ПРОФИЛЬ ЗАЩИТЫ СРЕДСТВА ДОВЕРЕННОЙ ЗАГРУЗКИ УРОВНЯ БАЗОВОЙ СИСТЕМЫ ВВОДА-ВЫВОДА ЧЕТВЕРТОГО КЛАССА ЗАЩИТЫ ИТ.СДЗ.УБ4.ПЗ [Электронный ресурс]. URL: http://fstec.ru/component/attachments/download/662 (дата обращения: 10.04.2016).
15. СЗИ НСД «Аккорд-АМДЗ» [Электронный ресурс]. URL: http://accord.ru/accord.html (дата обращения: 10.04.2016).
16. ПАК Аккорд-Win32(TSE) и ПАК Аккорд-Win64(TSE) [Электронный ресурс]. URL: http://www.accord.ru/acwin32.html (дата обращения: 10.04.2016).
17. ПАК СЗИ НСД Аккорд-X [Электронный ресурс]. URL: http://accord.ru/acx.html (дата обращения: 10.04.2016).
18. ПАК Аккорд-В. [Электронный ресурс]. URL: http://accord.ru/accord-v.html (дата обращения: 10.04.2016).
19. ГиперАккорд [Электронный ресурс]. http://accord.ru/hyper-accord.html (дата обращения: 10.04.2016).
20. Программно-аппаратный комплекс «Аккорд-В.» (версия 1.3) Руководство по установке [Электронный ресурс]. http://www.accord-v.ru/docs/Accord-V_Installation_Guide.pdf(дата обращения: 10.04.2016).
21. Программно-аппаратный комплекс средств защиты информации от НСД для ПЭВМ (PC) «Аккорд-АМДЗ» (Аппаратный модуль доверенной загрузки) Руководство администратора. [Электронный ресурс]. http://www.accord.ru/docs/amdz/AMDZ_L_Admin_manual.pdf (дата обращения: 10.04.2016).
22. vSphere и vSphere with Operations Management. [Электронный ресурс]. http://www.vmware.com/ru/products/vsphere/features/esxi-hypervisor (дата обращения: 10.04.2016).
23. Regestry. [Электронный ресурс]. https://msdn.microsoft.com/en-us/library/ms724871.aspx (дата обращения: 10.04.2016).
24. Using the initial RAM disk (initrd) [Электронный ресурс]. https://www.kernel.org/doc/Documentation/initrd.txt (дата обращения: 10.04.2016).
25. Li, X.R. A novel over writable and restoring solution of filesystem for NAND flash// 3rd International Conference on Information Technology and Management Innovation, ICITMI 2014; Shenzhen; China; 19 July 2014 through 20 July 2014; Volume 631–632, 2014, Pages 1057–1060

СТАТИСТИЧЕСКИЕ ОЦЕНКИ ЭНТРОПИЙНЫХ ФУНКЦИОНАЛОВ И ИХ ИСПОЛЬЗОВАНИЕ В ЗАДАЧАХ СТАТИСТИЧЕСКОГО ТЕСТИРОВАНИЯ КРИПТОГРАФИЧЕСКИХ ГЕНЕРАТОРОВ

В.Ю. ПАЛУХА, Ю.С. ХАРИН
ФПМИ БГУ, НИИ ППМИ БГУ

Введение

Важным структурным элементом средств криптографической защиты информации (криптосистем) являются генераторы случайных и псевдослучайных последовательностей [1]. Стойкость криптосистем зависит от того, насколько близка генерируемая последовательность по своим свойствам к равномерно распределённой случайной последовательности (РРСП). Одним из подходов к оценке качества генератора является статистическое оценивание энтропии и сравнение полученной оценки с ожидаемым значением для РРСП. Существуют различные функционалы энтропии, например, в [2] приводятся формулы 23 функционалов. Наиболее распространены функционалы энтропии Шеннона, Реньи и Тсаллиса, которые рассматриваются в данной статье.

Функционалы информационной энтропии

Пусть на вероятностном пространстве (Ω, F, P) с множеством состояний $\Omega = \{\omega_1, \ldots, \omega_N\}$ и вероятностями $p_i = P\{x = \omega_i\}$, $p_i \geq 0$, $\sum_{i=1}^{N} p_i = 1$ наблюдается последовательность $\{x_t\}$.

Определим функционал энтропии согласно [1]:

$$H_{h,w}^{\varphi_1,\varphi_2}(P) = h\left(\frac{\sum_{i=1}^{N} w_i \varphi_1(p_i)}{\sum_{i=1}^{N} w_i \varphi_2(p_i)}\right), \qquad (1)$$

где $w_i > 0$, $i = 1, \ldots, N$ — веса состояний ω_i, и заданы функции $h: \mathbb{R} \to \mathbb{R}$, $\varphi_1: [0,1) \to \mathbb{R}$, $\varphi_2: [0,1) \to \mathbb{R}$.

В таблице 1 приведены наиболее часто используемые в теории информации функционалы энтропии в соответствии с общим видом (1).

Таблица 1

Основные функционалы энтропии

Тип	Формула	h(x)	$\varphi_1(x)$	$\varphi_2(x)$	w_i
Шеннон	$H(P) = -\sum_{i=1}^{N} p_i \ln p_i$	x	$-x\log x$	x	w
Реньи	$H_r(P) = \frac{1}{1-r} \ln\left(\sum_{i=1}^{N} p_i^r\right),\ r \in \mathbb{N}, r > 1.$	$(1-r)^{-1}\log x$	x^r	x	w
Тсаллис	$S_r(P) = \frac{1}{r-1}\left(1 - \sum_{i=1}^{N} p_i^r\right),\ r \in \mathbb{N}, r > 1.$	$(1-r)^{-1}(x-1)$	x^r	x	w

Статистические оценки энтропии

Будем рассматривать стационарные в узком смысле двоичные последовательности $\{x_t\} \in V = \{0,1\}$ на некотором вероятностном пространстве (Ω, F, P). Пусть $p_{i_1,\dots,i_s} = P\{x_{t+1} = i_1, \dots, x_{t+s} = i_s\}$ — распределение вероятностей s-граммы $(x_{t+1},\dots,x_{t+s}) \in V_s$, которое не зависит от $t \in \mathrm{N}_0 = \mathrm{N} \cup \{0\}$. В предыдущих обозначениях имеем $N = 2^s$.

Обозначим: $x^{\underline{r}} = x(x-1)\dots(x-r+1)$ — нисходящая факториальная степень (при $x < r$ полагают $x^{\underline{r}} ::= 0$) [3]; $H_* = \{\{x_t\}$ есть РРСП$\}$ — гипотеза о том, что наблюдаемая последовательность является «чисто случайной», т.е. РРСП.

Пусть наблюдается n фрагментов длины s: $X^{(k)} = (x_1^{(k)}, \dots, x_s^{(k)}) \in V_s, \quad k = 1, \dots, n$, сформированных из элементов последовательности $\{x_t\}$. Для построения статистических оценок функционалов энтропии необходимо построить оценки распределения вероятностей $p_J(s) = P\{X^{(k)} = J_1^s\}$, где $J_1^s = (j_1, \dots, j_s) \in V_s$ — мультииндекс, по n фрагментам длины $s \geq 1$. Построим оценки вероятностей $\{\hat{p}_J(s)\}$ и r-ых степеней вероятностей $\{\widehat{p_J^r}(s)\}$, используя частотные статистики:

$$\hat{p}_J(s) = \frac{\nu_J}{n}, \quad \widehat{p_J^r}(s) = \frac{\nu_J^{\underline{r}}}{n^r}, \quad \nu_J = \sum_{k=1}^{n} \delta_{X^{(k)},J}, \quad \delta_{X^{(k)},J} = \begin{cases} 1, X^{(k)} = J; \\ 0, X^{(k)} \neq J. \end{cases} \tag{2}$$

На основе частотных статистик (2) построим оценку s-мерной энтропии Шеннона:

$$\hat{H}(n,s) = -\sum_{J \in V_s} \hat{p}_J(s) \ln \hat{p}_J(s), \tag{3}$$

а также оценки s-мерной энтропии Реньи и Тсаллиса

$$\widehat{H_r}(n,s) = \frac{1}{1-r} \ln\left(\sum_{J \in V_s} \widehat{p_J^r}(s) \right), \tag{4}$$

$$\widehat{S_r}(n,s) = \frac{1}{r-1}\left(1 - \sum_{J \in V_s} \widehat{p_J^r}(s) \right). \tag{5}$$

Рассмотрим асимптотику, означающую, что с увеличением количества наблюдений n увеличивается число N возможных исходов полиномиальной схемы:

$$n, N = 2^s \to \infty, n/N \to \lambda, 0 < \lambda < \infty. \tag{6}$$

Распределение вероятностей статистических оценок функционалов энтропии описывается следующей теоремой, доказательство которой базируется на результатах из [4].

Теорема. При истинной гипотезе H_* в асимптотике (6) статистические оценки функционалов энтропии (3)–(5) имеют асимптотически нормальное распределение, причём для асимптотических математических ожиданий и дисперсий справедливы равенства

$$E\{\hat{H}(n,s)\} = \ln n - e^{-\lambda} \sum_{k=1}^{+\infty} \frac{\ln(k+1)\lambda^k}{k!},$$

$$D\{\hat{H}(n,s)\} = \frac{e^{-\lambda}}{n} \sum_{k=1}^{+\infty} \frac{(k+1)\lambda^k}{k!} \ln^2(k+1) - \frac{e^{-2\lambda}}{2^s}\left(\sum_{k=1}^{+\infty} \frac{\ln(k+1)\lambda^k}{k!} \right)^2 - \frac{e^{-2\lambda}}{n}\left(\sum_{k=1}^{+\infty} \ln(k+1) \frac{\lambda^k}{k!}(k+1-\lambda) \right)^2,$$

$$E\{\widehat{H_r}(n,s)\} = s\ln 2, \tag{7}$$

$$D\{\widehat{H_r}(n,s)\} = \frac{\sum_{i=1}^{r} s(r,i)\sum_{j=0}^{i-1} C_i^j r^{i-j}\sum_{k=1}^{j} S(j,k)\lambda^k - r^2\lambda^{r-1} + r!}{(r-1)^2 n\lambda^{r-1}},$$

$$E\{\widehat{S_r}(n,s)\} = \frac{1}{r-1}\left(1 - \frac{1}{2^{s(r-1)}}\right),$$

$$D\{\widehat{S_r}(n,s)\} = \frac{\lambda^{r-1}}{(r-1)^2 n^{2r-1}}\left(\sum_{i=1}^{r} s(r,i)\sum_{j=0}^{i-1} C_i^j r^{i-j}\sum_{k=1}^{j} S(j,k)\lambda^k - r^2\lambda^{r-1} + r!\right),$$

где $s(r, i)$ и $S(r, i)$ — числа Стирлинга первого и второго рода соответственно [3].

Интервальные оценки энтропии и проверка гипотез

Поскольку нам известно асимптотическое распределение точечных оценок энтропии, мы можем построить интервальные оценки. Зададим уровень значимости $\varepsilon \in (0,1)$. Введём обозначения: $\hat{h}(n,s)$ — статистическая оценка энтропии Шеннона, Реньи или Тсаллиса, построенная по n фрагментам длины s; μ и σ^2 — асимптотические математическое ожидание и дисперсия статистической оценки используемого функционала энтропии при истинной гипотезе H_*, вычисленные по формулам (7) из теоремы 1. Тогда в асимптотике (6) с вероятностью $1 - \varepsilon$ $\hat{h}(n,s) \in (t_-, t_+)$, $t_\pm = \mu \pm \sigma\Phi^{-1}(1 - \frac{\varepsilon}{2})$, где $\Phi^{-1}(p)$ — квантиль уровня p стандартного нормального закона [5].

На основе интервальной оценки построим решающее правило для статистического тестирования генераторов, т.е. проверки гипотез о том, является ли наблюдаемая последовательность генератора «чисто случайной»: H_* и $\overline{H_*}$. Вычислим для наблюдаемой последовательности статистику $\hat{h}(n,s)$ и доверительный интервал для заданного уровня значимости. Решающее правило имеет вид:

$$\begin{cases} H_*, & \text{если } t_- < \widehat{h_r}(n,N) < t_+; \\ \overline{H_*}, & \text{в противном случае,} \end{cases} \qquad t_\pm = \mu \pm \sigma\Phi^{-1}\left(1 - \frac{\varepsilon}{2}\right),$$

В случае принятия решения о справедливости гипотезы H_* можно сделать вывод о том, что генератор пригоден для использования в криптосистемах, поскольку по своим свойствам он неотличим от равномерно распределённой случайной последовательности на основе выборки объёма n.

Заключение

Для проверки пригодности генераторов случайных и псевдослучайных последовательностей в криптосистемах предложено использовать статистические оценки функционалов энтропии Шеннона, Реньи и Тсаллиса, построенные по выходным последовательностям генераторов. Найдены асимптотические распределения вероятностей точечных стати-

стических оценок, на основе которых построены интервальные оценки и разработано решающее правило для статистического тестирования генераторов.

СПИСОК ЛИТЕРАТУРЫ

1. Криптология / Ю. С. Харин [и др.]. — Минск: БГУ, 2013. — 512 с.
2. Esteban, M.D. A summary on entropy statistics / M. D. Esteban, D. Morales // Kybernetika. — 1995. — Vol. 31, № 4. — P. 337–346.
3. Энвин, А. Ю. Дискретная математика: Конспект лекций / А. Ю. Энвин. — Челябинск: Издательство ЮУрГУ, 1998. — 176 с.
4. Holst, L. Asymptotic normality and efficiency for certain goodness-of-fit tests / L. Holst // Biometrika. — 1972. — № 59. — P. 137–145.
5. Харин, Ю. С. Теория вероятностей, математическая и прикладная статистика / Ю. С. Харин, Н. М. Зуев, Е. Е. Жук. — Минск: БГУ, 2011. — 463 с.

ОСОБЕННОСТИ ТЕСТИРОВАНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЕ

Н. В. МОЗОЛИНА, К. А. ЛУГОВЦОВА
МФТИ, Москва, Россия

В статье рассматриваются особенности и проблемы функционального тестирования средств защиты информации от несанкционированного доступа в виртуальной инфраструктуре, а также предлагается способ их решения при помощи средств автоматизации тестирования и разделения процесса тестирования на два независимых этапа.

Ключевые слова: функциональное тестирование, автоматизация процессов тестирования, виртуальная инфраструктура.

Неотъемлемым этапом разработки программного обеспечения, в том числе и средств защиты информации, является тестирование всех его компонентов на соответствие заданным требованиям. Существует множество видов тестирования, в данной статье ограничимся рассмотрением функционального тестирования, направленного на проверку того, какие функции программного обеспечения реализованы, и что они работают верным образом [1].

Процесс функционального тестирования состоит из четырёх стадий: выбор действия, определение ожидаемого результата этого действия, определение фактического результата и сравнение результатов.

Одним из самых простых способов тестирования является выполнение всех этих операций человеком вручную. Такой подход хоть и не требует большого объема подготовительных действий от тестировщика, но вместе с тем имеет ряд существенных минусов: человек может случайно или осознанно пропустить часть тестов, неверно интерпретировать результаты испытания, сделать ложные выводы, а также такое тестирование может растянуться на недели и даже месяцы. Для решения таких проблем используют автоматизацию: IBM Rational Functional Tester (RFT), TestComplete и другие продукты позволяют воспроизводить действия пользователя программного обеспечения, обраба-

тывать результаты тестовых испытаний и сравнивать их с ожидаемыми. Это исключает ошибки, которые человек мог сделать в силу усталости или невнимательности, а также значительно сокращает время выполнения тестов.

Чем сложнее устроен создаваемый продукт, тем более объемными и затратными становятся тестовые испытания не только с точки зрения времени, но и с точки зрения ресурсов, необходимых для работы тестируемого программного обеспечения. Особенно остро эта проблема стоит при испытании средств защиты информации для виртуальных инфраструктур.

Рассмотрим проблемы и особенности проведения тестовых испытаний при разработке программно-аппаратного комплекса «Сегмент-В.» и способ их решения.

Данный продукт предназначен для защиты инфраструктур виртуализации, построенных на базе платформы VMware vSphere. «Сегмент-В.» представляет собой совокупность технических и программных средств, предназначенных для обеспечения защиты от несанкционированного доступа [2].

Одна из основных функций программно-аппаратного комплекса — управление доступом субъектов к объектам в виртуальной инфраструктуре. Она осуществляется за счёт перехвата всех команд управления прокси-сервером «Segment-V. Module" и их обработки на основе заранее созданных правил (метки и уровни доступа для объектов и субъектов, списки разрешённых действий пользователей, политики прокси-сервера). Эта функция осуществляется модулем контроля доступа, входящим в прокси-сервер «Segment-V. Module».

Для тестирования модуля контроля доступа необходимо провести тестовые испытания, охватывающие весь спектр возможных действий администратора виртуальной инфраструктуры. Результатом исполнения теста должны быть данные об исполняемой команде управления, субъекте и объектах, участвующих в данном действии.

Использование автоматизированных тестов, моделирующих операции пользователя, избавляет тестировщика от необходимости вручную исполнять каждое действие и следить за их результатами [3], но, как и прежде, требуют наличия тестовой виртуальной инфраструктуры, предусматривающей всевозможные отношения между объектами и субъектами доступа.

Например, виртуальная машина может находиться на локальном хранилище хоста или на хранилище, подключённом по iSCSI, гипервизоры могут образовывать кластер или не быть объединёнными в общий ресурс. Кроме того, «Сегмент-В.» позволяет назначать метки и уровни доступа субъектов и объектов, что рождает новые отношения между элементами инфраструктуры. Для полной проверки работы функции управления доступом «Сегмента-В.» тестовая инфраструктура должна предоставлять возможность работать с каждым типом объектов и всеми возможными отношениями между ними и субъектами. Виртуальная инфраструктура, удовлетворяющая этим условиям, требует значительных вычислительных ресурсов и места на хранилище.

Для решения этой проблемы был использован следующий подход: четыре стадии процесса тестирования выполняются в два этапа:

1. выбор действия, определение ожидаемого результата этого действия с помощью записи команд в log-файл и создания файлов с эталонными результатами теста;
2. определение фактического результата проведения тестов модуля контроля доступа и сравнение его с эталонным.

Исполнение первого этапа начинается с написания автоматизированных тестов (test_name.java), которые исполняются с помощью RFT на рабочем месте тестировщика и вос-

производят действия администратора виртуальной инфраструктуры в vClient. Команда управления, реализуемая в каждом отдельном тесте, перехватывается на прокси-сервере, который пишет в log-файл (message.log) все принятые HTTP-пакеты, содержащие данные об этом действии. Формат log-файла соответствует входным данным модуля контроля доступа. message.log автоматически передаётся на рабочее место тестировщика, где переименовывается в test_name.log. В процессе исполнения теста в RFT также создаётся файл с ожидаемыми результатами выполнения тестового испытания test_name.etalon.

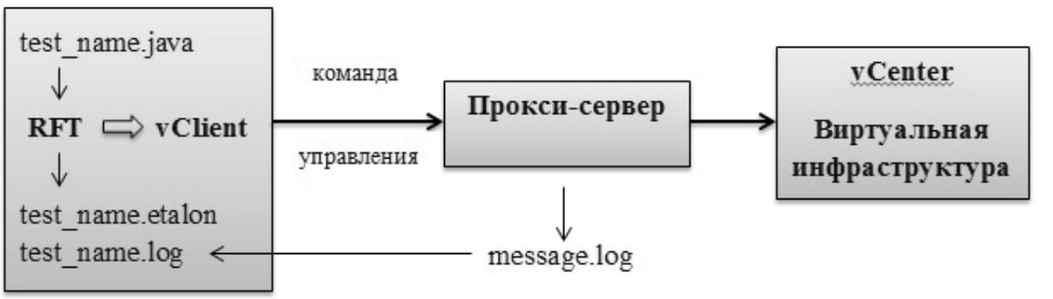


Рис. 1. Этап 1. Схема получения ожидаемого результата выполнения теста (test_name.etalon) и log-файла (test_name.log)

На втором этапе тестирования test_name.log обрабатывается модулем контроля доступа, работающим на отдельной машине для тестовых испытаний. В результате работы модуля создаётся file.log, который с помощью скрипта проверки сравнивается с ожидаемым test_name.etalon.

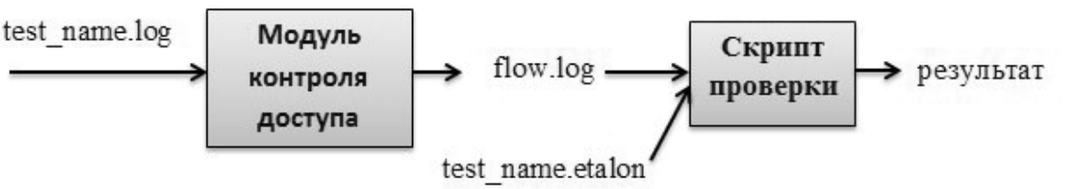


Рис. 2. Этап 2. Схема получения результата выполнения теста и его сравнение с ожидаемым результатом.

В результате такого разделения тестирования первый этап зависит только от виртуальной инфраструктуры, а второй — только от модуля контроля доступа.

Благодаря этому исполнение автоматизированных тестов на виртуальной инфраструктуре — наиболее объемная операция с точки зрения времени и ресурсов — становится редким действием, которое требуется проводить лишь при изменениях в платформе виртуализации. Это избавляет нас от постоянной необходимости содержать тестовую виртуальную инфраструктуру.

Непосредственное проведение тестов модуля контроля доступа на втором этапе требует незначительных вычислительных ресурсов, а также происходит значительно быстрее, чем при тестировании с использованием тестовой инфраструктуры, как не зависит от

времени получении данных об объектах — все необходимые сведения уже содержатся в test_name.log.

Таким образом, данный подход к функциональному тестированию решает проблемы, связанные с человеческим фактором, длительным временем проведения тестовых испытаний и большими вычислительными ресурсами, необходимыми для выполнения тестов. Автоматизация тестовых испытаний позволяет снять с человека ответственность за корректную интерпретацию результатов и выполнение всех тестов и позволяет сократить время тестирования, а разделение процесса тестирования на два независимых этапа позволяет сократить требуемые вычислительные ресурсы.

СПИСОК ЛИТЕРАТУРЫ

1. *Куликов С. С.* Тестирование программного обеспечения. Базовый курс: практ. пособие. Минск: Четыре четверти, 2015. С. 63–110
2. *Постоев Д. А.* Управление доступом в виртуальных системах на основе контроля информационных потоков // Безопасность информационных технологий. М., 2014. № 4. С. 86–91.
3. *Каннер (Борисова) Т. М., Кузнецов А. В., Обломова А. И.* Тестирование средств защиты информации // Информационная безопасность. Материалы XIII Международной конференции. Таганрог 2013. Часть. 1. С. 121–129.

О ПРОГНОЗИРОВАНИИ ДВОИЧНЫХ ВРЕМЕННЫХ РЯДОВ С ИСПОЛЬЗОВАНИЕМ NVIDIA CUDA

В.В. ПЬЯНОВ, Ю.С. ХАРИН,
НИИ ППМИ БГУ

Введение

Случайные последовательности и их генераторы являются неотъемлемыми элементами современных криптосистем [1]. Случайные последовательности используются для построения гаммы в поточных криптосистемах, сеансовых и других ключей в блочных криптосистемах. Отметим, что для криптографических приложений требуются равномерно распределенные случайные последовательности значительной длины. Поэтому возникает важная задача статистического тестирования таких последовательностей. Одним из направлений статистического тестирования является проверка свойства невозможности прогнозирования выходных последовательностей криптографических генераторов статистическими методами. В данной статье представляется эффективный вычислительный алгоритм статистического прогнозирования, основанный на нахождении оптимального шаблона прогнозирования в классе малопараметрических цепей Маркова высокого порядка.

Математическая модель временного ряда

Пусть на вероятностном пространстве (Ω, F, P) наблюдается двоичный временной ряд $x = (x_1,..,x_T) \in V^T = \{0,1\}^T, x_t \in V = \{0,1\}, t = 1,\ldots,T$, длины T, являющийся цепью Маркова порядка s, $s \gg 1$, обладающий следующим гипотетическим свойством:

$$\frac{1}{2}-\varepsilon \le \left| P\{x_t = j_0 | x_{t-1} = j_1, \ldots, x_{t-s} = j_s\} - \frac{1}{2} \right| \le \frac{1}{2},\ j_0, j_1, \ldots, j_s \in V, \qquad (1)$$

где $\varepsilon \in \left[0, \frac{1}{2}\right)$ — некоторое достаточно малое число. Это свойство означает, что при некотором достаточно большом s в выходной последовательности $\{x_t\}$ криптографического генератора существует статистически значимая зависимость глубины s. Прогнозированию подлежит последующий бит $x_{T+1} \in V$.

Так как распределение вероятностей, входящее в (1), на практике неизвестно, а его статистическое оценивание имеет вычислительную сложность порядка $O\left(2^{s+1}\right)$, то необходимы другие подходы к прогнозированию, использующие малопараметрические модели цепи Маркова высокого порядка[1–4]. Выберем в качестве такой модели цепь Маркова порядка s с r частичными связями[2].

Пусть $r \in \mathbb{N}, 1 \le r \le s$ — число связей, $M = \{m_1, m_2, \ldots, m_r\}$ — целочисленный -вектор с упорядоченными компонентами $1 \le m_1 \le m_2 \le \ldots \le m_r \le s$, который будем называть шаблоном, $P = (p_{j_0,\ldots,j_{s-1},j_s}), j_0, \ldots, j_s \in V$ — $(s+1)\times(s+1)$ матрица вероятностей одношаговых переходов цепи Маркова x_t:

$$p_{j_0,\ldots,j_{s-1},j_s} = P\{x_t = j_0 | x_{t-1} = j_1, \ldots, x_{t-s} = j_s\},$$

$Q = (q_{j_0,\ldots,j_{r-1},j_r}), j_0, \ldots, j_r \in V$ — некоторая $(r+1)\times(r+1)$ стохастическая матрица.

Цепь Маркова $x_t \in V$ принято называть цепью Маркова *s*-го порядка с r частичными связями и обозначать ЦМ(s,r), если ее вероятности одношаговых переходов допускают следующее малопараметрическое представление:

$$p_{j_0,\ldots,j_{s-1},j_s} = q_{j_0,j_{m_1},\ldots,j_{m_r}},\ j_0, \ldots, j_s \in V.$$

В дальнейшем будем считать, что двоичный временной ряд

$$x = (x_1, .., x_T) \in V^T = \{0,1\}^T, x_t \in V = \{0,1\}, t = 1, \ldots, T$$

является цепью Маркова *s*-го порядка с r частичными связями.

Алгоритм прогнозирования на основе ЦМ(s,r) и его реализация на NVIDIA CUDA

Выберем $r \in \mathbb{N}, 1 \le r \le s$ и зафиксируем произвольный упорядоченный набор r номеров координат шаблона $M = \{m_1, m_2, \ldots, m_r\}$, где $1 \le m_1 \le m_2 \le \ldots \le m_r \le s$. Введем в рассмотрение условную вероятность события:

$$p(r, j_0, M) ::= P\{x_{T+1} = j_0 | x_{T-m_1} = j_1, \ldots, x_{T-m_r} = j_r\},$$

где $j_1, \ldots, j_r \in V$ — фиксированные наблюдаемые значения $x_{t-m_1}, \ldots, x_{t-m_r}$. В силу (1) будем строить прогноз для x_t на основе $x_{T-m_1}, \ldots, x_{T-m_r}$. Согласно [3], оптимальная прогнозирующая статистика для модели ЦМ(s,r) примет вид:

$$\hat{x}_{T+1} = \arg\max_{j_0} p(r, j_0, M). \qquad (2)$$

Сложность вычисления прогнозирующей статистики (2) имеет порядок $O\left(T+2^{r+1}\right)$. Точность прогноза оценивается величиной[3]

$$\mathrm{p}_{+}\left(r,M\right):=\max_{j_0\in V}\mathrm{p}\left(r,j_0,M\right).$$

Точность прогнозирования можно увеличить, максимизируя по $r\in\left[r_{min},r_{max}\right]$ и шаблону[4]:

$$p_{+}\left(r;M\right)\to\max_{r,M}, \tag{3}$$

где $r_{min}\left(r_{max}\right)$ — минимальное (максимальное) возможное число связей.

Решением экстремальной задачи (3) будет являться набор r^{*},M^{*} наиболее информативных компонент шаблона. Если решать данную максимизации (3) перебором, то вычислительная сложность будет иметь порядок $O\left(C_s^r T+2^{r+1}\right)$. Для уменьшения вычислительной сложности будем использовать алгоритм последовательной максимизации, позволяющий приближенно решать задачу максимизации по M. Пусть r изменяется в пределах $1\le r_{min}\le r\le r_{max}\le s$. Решим задачу максимизации по M для $r=r_{min}$ перебором всех возможных шаблонов длины r_{min} и получим $M^{r_{min}}$. Затем будем последовательно увеличивать r, добавляя к $M^{r_{min}}$ ещё одну не задействованную компоненту:

$$M^{r_{min}}=\arg\max_{M}p_{+}\left(r,\mathrm{M}\right),$$

$$M^{r}=\arg\max_{m\in\{1,..,s\}\setminus M^{r-1}}p_{+}\left(r,(M^{r-1},m)\right).$$

И так далее увеличиваем r пока не достигнем $r=r_{max}$.

В качестве оценки M^{*} принимаем $M^{r_{max}}$. Подставляя M^{*} в (2), получаем оценку для будущего значения x_{T+1}.

Для эффективной реализации алгоритма использовалась технология NVIDIA CUDA [5], которая благодаря архитектуре SIMT позволяет эффективно производить перебор при решении экстремальных задач (3), (4).

Численные результаты

Параметр s, означающий порядок цепи Маркова (глубину стохастической зависимости), в представленном алгоритме предполагался известным. Отметим, что в [4] предложен метод статистического оценивания параметров s,r на основе байесовского информационного критерия и информационного критерия Акаике.

Для тестирования разработанного алгоритма по точности, характеризуемой вероятностью ошибки:

$$p_{\text{ош.}}=P\left\{\hat{x}_{T+1}\ne x_{T+1}\right\},$$

и вычислительной сложностью, характеризуемой затратами машинного времени $t_{маш.}=1$ для вычисления прогноза $\hat{x}_{T+1}$, проведены две серии компьютерных экспериментов.

В первой серии обрабатывалось 10 реализаций двоичного дискретного временного ряда длины $T=2^{15}$, порождаемого линейной рекуррентой:

$$x_t=x_{t-16}\oplus x_{t-14}\oplus x_{t-13}\oplus x_{t-11},$$

соответствующего модели ЦМ(s,r) при $s=16, r=4, M^*=\{11,13,14,16\}$ и удовлетворяющего свойству (1) при $\varepsilon=0$. При $r_{min}=3, r_{max}=6$ прогнозирование всех 10 реализаций произошло безошибочно: $\hat{p}_{ош.}=0$; время обработки одной реализации составило $t_{маш.}=1$ сек. Результаты обработки всех 10 реализаций представлены в таблице 1 (истинные компоненты шаблона в оценке $\hat{M}^{r_{max}}$ выделены жирным шрифтом).

Во второй серии обрабатывалось 10 реализаций двоичного дискретного временного ряда длины $T=2^{15}$, порождаемого нелинейной рекуррентой:

$$x_t = x_{t-1} \oplus x_{t-2} \oplus x_{t-8}x_{t-11} \oplus x_{t-10}x_{t-16},$$

соответствующего модели ЦМ(s,r) при $s=17, r=6, M^*=\{1,2,8,10,11,16\}$ и удовлетворяющего свойству (1) при $\varepsilon=0$. При $r_{min}=4, r_{max}=6$ прогнозирование всех 10 реализаций произошло безошибочно: $\hat{p}_{ош.}=0$; время обработки одной реализации составило $t_{маш.}=1.8$ сек. Результаты обработки всех 10 реализаций представлены в таблице 2.

Таблица 1

Результаты прогнозирования для первой серии

Номер эксперимента	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
x_{T+1}	0	1	1	0	1	0	1	1	0	1
$\hat{x}_{T+1}$	0	1	1	0	1	0	1	1	0	1
$\hat{M}^{r_{max}}$	**16,14, 13,11**, 10, 4	**16**,15, **14,13, 11**, 5	**16,14, 13,11**, 7, 4	**16,14, 13,11**, 10, 8	**16,14**, **13**,12, **11**, 9	**16,14, 13,11**, 9, 6	**16,14**, **13**,12, **11**, 4	**16**,15, **14,13, 11**, 8	**16,14, 13,11**, 9, 6	**16,14, 13,11**, 10, 7

Таблица 2

Результаты прогнозирования для второй серии

Номер эксперимента	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
x_{T+1}	1	0	1	0	0	1	0	0	1	1
$\hat{x}_{T+1}$	1	0	1	0	0	1	0	0	1	1
$\hat{M}^{r_{max}}$	**1, 2, 10,11**, 14, **16**	**1, 2**, 4, 9, **11, 16**	**1, 2**, **10,11**, 13, **16**	**1, 2**, 3, 5, **8, 10**	**1, 2**, 6, **8, 10,16**	**1, 2, 8,10**, 11,17	**1, 2, 11**,14, **16**, 17	**1, 2**, 5, **8**, **10,16**	**1, 2, 11**,12, 15, **16**	**1, 2**, 7, **8**, **10**, **11**

Таким образом, компьютерные эксперименты показали эффективность разработанного алгоритма прогнозирования.

ЛИТЕРАТУРА

1. Криптология / Ю. С. Харин [и др.]. — Минск: БГУ, 2014. — 512 с.
2. *Харин Ю. С.* Цепи Маркова с r-частичными связями и их статистическое оценивание / Ю. С. Харин // Доклады НАН Беларуси. — 2004. Т. 48, № 1. — С. 40–44.

3. *Харин Ю. С.* Оптимальность и робастность в статистическом прогнозировании: монография / Ю. С. Харин. — Минск: БГУ, 2008. — 263 с.
4. *Харин Ю. С., Петлицкий А. И.,* «Идентификация двоичной цепи Маркова s-го порядка с r частичными связями при наличии аддитивных искажений», Дискрет. матем., 22:4 (2010), 138–155
5. CUDA Toolkit documentation. http://docs.nvidia.com/
6. *Dubrova E.* A List of Maximum Period NLFSRs //IACR Cryptology ePrint Archive. — 2012. — Т. 2012. — С. 166.
7. *Ward R. W., Molteno T. C. A.* Table of linear feedback shift registers. — Electronics Group, University of Otago, 2012.

ДОВЕРЕННАЯ ЗАГРУЗКА И МЕНЕДЖМЕНТ ЛОГИЧЕСКИХ ДИСКОВ. РОСКОШЬ ИЛИ НЕОБХОДИМОСТЬ

Д. И. ДЕВЯТИЛОВ
МФТИ

В тезисах описывается система LVM и объясняется необходимость контроля целостности файлов на данных системах.

Парадигма доверенных вычислений начала развиваться с конца прошлого столетия. Наблюдая за эволюцией парадигмы (от функционально-замкнутой среды (ФЗС) до доверенного сеанса связи (ДСС)) [14], можно с уверенностью сказать, что основа — это концепция (доверенной вычислительной среды) ДВС, для создания которой одним из условий является наличие резидентного компонента безопасности (РКБ)[1]. РКБ осуществляет проверку целостности технических и программных средств ПК и может быть реализован в виде аппаратного модуля доверенной загрузки (АМДЗ). Доверенная загрузка — загрузка операционных систем (ОС) только с заранее определенных носителей и после успешного прохождения специальных процедур контроля целостности (КЦ) программных и аппаратных средств ПК [2]. Конечно же, уместно говорить не о доверенной загрузке ОС, а о доверенной загрузке загрузчика ОС, т. к. после прохождения процедур КЦ управление передается не коду ОС, а коду загрузчика [3]. Доверенная загрузка будет считаться выполненной только после успешного прохождения всех процедур КЦ.

В силу того, что информационные технологии постоянно развиваются, усовершенствуются старые и создаются новые программные и аппаратные компоненты, в частности, операционные и файловые системы, необходимо для обеспечения функций безопасности доверенной загрузки поддерживать появляющиеся удобства цивилизации, уметь с ними работать. Ответом на такой вызов становится как усовершенствование самих фундаментальных парадигм доверенных вычислений [8, 9] и новых взглядов на реализацию РКБ [6, 13], так и поддержка новых технологий в существующих и уже зарекомендовавших себя подходах [7].

Необходимость более гибкого управления памятью запоминающих устройств ПК подталкивает на создание новых систем управления дисковым пространством [10]. Часто возникает необходимость в разбиении или, наоборот, соединении отдельных блоков памяти жесткого диска, сохраняя при этом все установленные ОС, данные и программы. Плюс, не хочется прибегать к резервному копированию имеющихся фай-

лов. В настоящий момент с этой задачей отлично справляется LVM (Logical Volume Manager) — система управления дисковым пространством, абстрагирующаяся от физических устройств [4].

Другими словами, LVM — это дополнительный слой абстракции от аппаратной части ПК, с помощью которого можно эффективно и легко управлять дисковым пространством, объединяя множество разнородных жестких дисков в один, или, наоборот, отделяя их друг от друга. При этом все операции можно выполнить, не прибегая к перезагрузке компьютера. В современном администрировании рабочих станций это очень важно, так как излишние простои могут привести к финансовым потерям.

Несомненными плюсами использования LVM являются:

- использование любого количества жестких дисков или их разделов как один большой раздел;
- логические диски могут быть распределены на несколько жестких дисков;
- можно производить создание, изменение и удаление логических томов в любом виде, независимо от физического расположения тома; так же это можно делать в режиме реального времени;
- возможность создавать резервную копию файловой системы практически на лету;
- использование прозрачного шифрования файловой системы и кэширование часто используемых данных;
- динамическое увеличение размеров томов по мере их заполнения.

Бесспорным недостатком LVM считается то, что данный менеджер дисков реализован только для Unix-подобных операционных систем. Также к недостаткам можно отнести и сложность настройки.

В ОС семейства Windows аналогом LVM является технология динамических дисков, что еще раз говорит о востребованности таких типов систем гибкого менеджмента жестких дисков.

Но, несмотря на существующие недостатки, LVM является мощным инструментом для управления дисковым пространством СВТ. И для создания ДВС необходимо, чтобы РКБ «умел» работать с LVM. Например, в таких СЗИ, как ПАК «Соболь», не поддерживается контроль целостности файлов, расположенных на дисках с виртуальными файловыми системами и дисках, являющихся наборами томов LVM [15].

А в средствах защиты информации (СЗИ) от несанкционированного доступа (НСД) семейства Аккорд [5, 12] поддержка LVM и динамических дисков реализована в полном объеме. Если смотреть с практической точки зрения, то в Аккорде есть список, в котором отображаются группы и тома LVM. Пользователь может работать с томами так же, как и с разделами: выбирать нужный файл и ставить его на контроль. Пользователи могут быть спокойны за свои данные, которые обрабатываются в файловой системе, поддерживающей менеджер логических томов. Процедуры контроля целостности здесь осуществляются так же, как и на системах без LVM, и только после успешного их прохождения выполняется доверенная загрузка операционной системы.

LVM — мощный инструмент, создающий удобство и массу возможностей для работы с дисковыми накопителями. Поэтому для того чтобы идти в ногу со временем, необходимо уметь осуществлять контроль целостности, файлов и программ, обрабатываемых в данной системе.

СПИСОК ЛИТЕРАТУРЫ.

1. *Конявский В. А.* Доверенный сеанс связи. Развитие парадигмы доверенных вычислительных систем — на старт, внимание, МАРШ! // Комплексная защита информации. Сборник материалов XV Международной научно-практической конференции (1–4 июня 2010 г., Иркутск (Россия)). М., 2010. С. 166–169.
2. *Алтухов А. А.* Концепция персонального устройства контроля целостности вычислительной среды. // Вопросы защиты информации. 2014. № 4. С. 64–68.
3. *Каннер А. М.* Linux: о доверенной загрузке загрузчика ОС. // Безопасность информационных технологий. М., 2013. N 2. С. 41–46.
4. *AJ Lewis.* LVM HOWTO. [Электронный ресурс] URL: http://www.tldp.org/HOWTO/LVM-HOWTO/ (дата обращения: 13.04.2016).
5. СЗИ НСД Аккорд-АМДЗ. [Электронный ресурс] URL: http://www.accord.ru/amdz.html (дата обращения: 14.04.2016).
6. *Алтухов А. А.* Неатомарный взгляд на РКБ, как на композицию перехвата управления и контроля целостности. // Международная конференция «Комплексная защита информации». 2015 г., Беларусь. С. 53–55.
7. *Борисова Т. М., Романенко Н. В.* Аккорд-АМДЗ: Next Generation. // Международная конференция. 2012 г. Суздаль. Россия. С. 57–58.
8. *Конявский В. А.* Организация безопасного ДБО на основе СОДС «МАРШ!». // Национальный банковский журнал. № 9. 2011 г. С. 88–89.
9. *Кравец В. В.* Доверенная вычислительная среда на планшетах Dell. «МАРШ!». // Вопросы защиты информации: Научно-практический журнал/ФГУП «ВИМИ», 2014. № 4 (107). С. 32–33.
10. *Chang-Soo Kim, Gyoung Bae Kim, Bum Joo Shin*. Method for managing logical volume in order to support dynamic online resizing and software raid and to minimize metadata and computer readable medium storing the same. заявитель и патентообладатель. Electronics And Telecommunications Research Institute. № US 6718436 B 2. Заявлен 07.12.2001. Опубликован 06.04.2004.
11. *Конявский В. А.* Эпохе бурного развития — компьютер с динамической архитектурой. // Национальный банковский журнал. М., 2016. № 3 (март). С. 102–103.
12. Способ защиты от несанкционированного доступа к информации, хранимой на персональной ЭВМ. Патент на изобретение № 2475823. 20.02.2013, бюл. № 5.
13. *Алтухов А. А.* Контроль доступа на основе атрибутов и оптимизация управления множеством АПМДЗ. // Материалы XX научно-практической конференции. Минск, 19–21 мая 2015 г. — Минск: РИВШ, 2015. С. 55–60.
14. *Конявский В. А., Гадасин В. А.* Основы понимания феномена электронного обмена информацией (Библиотека журнала «УЗИ»; Кн. 2). Мн.: «Беллитфонд», 2004. — С. 282.
15. ПАК «Соболь». Версия 3.0. Комментарии к версиям 2.0.88 ПО Windows, 3.0.41/40 ПО Linux и 1.0.180 BIOS. [Электронный ресурс] URL: http://www.securitycode.ru/_upload/editor_files/documentation/sobol_2/Sobol_FSB_ReleaseNotes.pdf (дата обращения: 18.04.2016).

ОЦЕНКА СТЕГАНОГРАФИЧЕСКИХ КОНТЕЙНЕРОВ НА ОСНОВЕ МАРКОВСКИХ МОДЕЛЕЙ

А.С. ПРОЦКЕВИЧ, Ю.С. ХАРИН
Белорусский государственный университет

Введение

Стеганография скрывает сам факт передачи информации. В настоящее время эта научная область стремительно развивается. Основным свойством, которое характеризует качество стегосистемы, является необнаруживаемость, т.е. невозможность доказательства существования скрытой информации. Свойство необнаруживаемости связано с понятием «качества» контейнера, т.е. оценкой его пригодности для встраивания сообщения. В качестве модели сообщения обычно используется равномерно распределенная случайная последовательность (сжатое зашифрованное сообщение). Одной из оценок «качества» контейнера является стеганографическая ёмкость. Стеганографическая ёмкость — это максимальное число бит, которые могут быть встроены без появления статистически обнаруживаемых модификаций [1]. Актуальными являются задачи оценки свойств контейнера, определения областей контейнера, безопасных для встраивания, а также построения математических моделей, на основании которых производится оценка стеганографической ёмкости контейнера.

В данной работе для решения указанных задач в случае LSB встраивания сообщения в контейнер применяются математические модели цепи Маркова порядка si Марковского случайного поля, строятся статистические оценки стеганографической ёмкости контейнера, определяются фрагменты контейнера, пригодные для встраивания.

Исследование свойств контейнера на основе двоичных цепей Маркова заданного порядка

Пусть наблюдается контейнер, представляющий собой последовательность n двоичных N-векторов:

$$X_1 = \left(x_{11},\ldots,x_{1N}\right)^T,\ldots,X_n = \left(x_{n1},\ldots,x_{nN}\right)^T \in V_N = \left\{0,1\right\}^N.$$

Пусть $1 \le N_0 \le N$ — число «наименее значимых бит». В методе LSB встраивания сообщения в контейнер используется последовательность двоичных N_0 — векторов:

$$x_1 = \left(x_{11},\ldots,x_{1N_0}\right)^T,\ldots,x_n = \left(x_{n1},\ldots,x_{nN_0}\right)^T \in V_{N_0}.$$

Для простоты обозначений в данной работе рассмотрим случай $N_0 = 1$; результаты получены и для $N_0 > 1$. Таким образом, исходные данные представляют собой дискретный временной ряд с пространством состояний $V = \left\{0,1\right\}$:

$$y_t = x_{t1}, t = 1,\ldots,n.$$

Зададим число m для $\left(2m+1\right)$-окна скользящего просмотра данных. Если предположить, что y_t есть ОЦМ некоторого заданного порядка с матрицей вероятностей одношаговых переходов [2]

$$P = \left(p_{i_1,\ldots,i_s,j} \right), p_{i_1,\ldots,i_{s+1}} = P\left(y_t = j | y_{t-1} = i_1, \ldots, y_{t-s} = i_s \right),$$

то находим частоты

$$\nu_{i_1,\ldots,i_s,j} = \sum_{i=t-m+s}^{t+m} I\left\{ y_{t+1} = j, y_t = i_1, \ldots, y_{t-s+1} = i_s \right\}, \left(i_1, \ldots, i_s, j = 0,1 \right),$$

$$\nu_{i_1,\ldots,i_s} = \sum_{j=0}^{1} \nu_{i_1,\ldots,i_s,j},$$

где $I\{\bullet\}$ — индикатор события, указанного в скобках. Используя критерий согласия Пирсонас параметрами $\left(2^S, \alpha\right)$, где 2^S – число степеней свободы, α — уровень значимости, построим статистический тест проверки гипотезы о виде матрицы вероятностей одношаговых переходов, означающую «чистую случайность» $\{y_t\}$:

$$H_0 = \left\{ p_{i_1,\ldots,i_s,j} = 0.5, i_1, \ldots, i_s, j = 0,1 \right\}, H_1 = \overline{H_0}.$$

Этот критерий имеет вид [3]:

$$H_0 \text{ отвергается} \leftrightarrow \{\chi_n^2 > \chi_{1-\alpha,2^S}^2\},$$

где

$$\chi_n^2 = \sum_{i_1,\ldots,i_s,j \in \{0,1\}} \frac{\left(\nu_{i_1,\ldots,i_s,j} - \frac{1}{2}\nu_{i_1,\ldots,i_s} \right)^2}{\frac{1}{2}\nu_{i_1,\ldots,i_s}},$$

$\chi_{1-\alpha,2^S}^2$ – квантиль уровня $1-\alpha$ стандартного хи-квадрат распределения с 2^S степенями свободы.

В случае принятия гипотезы H_0 область контейнера, которая находится в окне скользящего просмотра данных $\{t-m, t-m+1, \ldots, t+m\}$, считается «неопасной» и пригодной для встраивания сообщения.

Исследование свойств контейнера на основе марковских случайных полей

Пусть теперь контейнер представляет собой изображение в градациях серого, представляющее собой $(n_1 \times n_2)$ матрицу $A = \left(a_{ij} \right), a_{ij} \in V_{256}$. Рассмотрим LSB-матрицу изображения $X = \left(x_{ij} \right)$, состоящую из наименее значимых бит каждого пикселя, и выберем *шаблон соседства* для элемента x_{ij} этой матрицы следующим образом: $\left\{ x_{i-1,j}, x_{i,j-1} \right\}$.

Предполагается, что:

$$\mathbb{P}\left\{ x_{ij} | \left\{ x_{kl} : k \le i, l \le j \right\} \right\} = \mathbb{P}\left\{ x_{ij} | x_{i,j-1}, x_{i-1,j} \right\},$$

и что X — *марковское случайное поле* с вероятностями одношаговых переходов:

$$p_{i_1,i_2,i_3} = \left\{ x_{ij} = i_3 \mid x_{i,j-1} = i_1, x_{i-1,j} = i_2 \right\}, \quad \left(i_1, i_2, i_3 = 0,1 \right).$$

Определим гипотезы:

$$H_0 = \left\{ \mathbb{P}\left(x_{ij} | x_{i,j-1}, x_{i-1,j}\right) \equiv \frac{1}{2}, i = 2,\ldots,n_1, j = 2,\ldots,n_2 \right\}; H_1 = \overline{H_0}.$$

Зададим $m_1 \times m_2$ окно просмотра данных и найдём частоты:

$$\nu_{i_1,i_2,i_3} = \sum_{j=2}^{m_2} I\left\{x_{ij} = i_3, x_{i,j-1} = i_1, x_{i-1,j} = i_2\right\}, \left(i_1, i_2, i_3 = 0,1\right),$$

$$\nu_{i_1,i_2} = \sum_{j=2}^{m_2} I\left\{x_{i,j-1} = i_1, x_{i-1,j} = i_2\right\}, \left(i_1, i_2 = 0,1\right).$$

Для проверки H_0, H_1 используем критерий согласия Пирсона:

$$H_0 \text{ отвергается } \leftrightarrow \{\chi_n^2 > \chi_{1-\alpha,4}^2\},$$

где

$$\chi_n^2 = \sum_{i_1,i_2,i_3 \in \{0,1\}} \frac{\left(\nu_{i_1,i_2,i_3} - \frac{1}{2}\nu_{i_1,i_2}\right)^2}{\frac{1}{2}\nu_{i_1,i_2}},$$

$\chi_{1-\alpha,4}^2$ – квантиль уровня $1-\alpha$ стандартного хи-квадрат распределения с 4 степенями свободы.

Если принимается гипотеза H_0, то фрагмент контейнера {t, …, t+m_2 } с индексом j считается «безопасным» и пригодным для встраивания.

Численные результаты экспериментов

Произведены оценки свойств пяти контейнеров, представляющих собой bmp-изображения размером 512×512 в градациях серого. Получены оценки их относительной стеганографической ёмкости в зависимости от выбранной модели наблюдения, произведена визуализация пригодных и непригодных для встраивания областей контейнера. Относительной стеганографической ёмкостью назовём отношение числа бит, пригодных для встраивания, к числу бит в LSB-матрице изображения. В моделях на основе цепи Маркова заданного порядка, изображение преобразуется в двоичную последовательность построчной развёрткой.

Типы используемых в экспериментах моделей.

1. Модель наблюдения: двоичная цепь Маркова 0-го порядка (т.е. схема независимых испытаний), размер скользящего окна просмотра данных $2m+1=33$ бита.
2. Модель наблюдения: двоичная цепь Маркова 1-го порядка, размер скользящего окна просмотра данных $2m+1=33$ бита.
3. Модель наблюдения: двоичная цепь Маркова 2-го порядка, размер скользящего окна просмотра данных $2m+1=33$ бита.
4. Модель наблюдения: марковское случайное поле с заданным шаблоном, размер окна просмотра данных 2×32 бита ($n_1=2, n_2=32$).

В таблице 1 представлены оценки относительной стеганографической ёмкости в процентах для пяти контейнеров при использовании четырёх указанных выше моделей LSB-контейнеров.

Рис. 1. Контейнеры 1–5

Таблица 1

Оценка относительной стеганографической ёмкости контейнера в зависимости от параметров испытания

Контейнер	Модель 1	Модель 2	Модель 3	Модель 4
1	84,03	60,77	22,00	20,46
2	76,65	55,25	20,98	16,61
3	74,44	54,62	20,44	17,03
4	83,73	59,82	22,45	23,11
5	71,57	52,37	19,73	19,07

ЛИТЕРАТУРА

1. *Fridrich, J.* Steganography in digital media / J. Fridrich //Cambridge University Press, Cambridge, 2010.
2. Криптология / Ю. С. Харин [и др.]. — Минск: БГУ, 2013.
3. *Медведев, Ивченко*. Введение в математическую статистику. Москва, 2010.

КОНТРОЛЬ ЦЕЛОСТНОСТИ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ И ЕЁ КОНФИГУРАЦИИ

Н. В. МОЗОЛИНА
МФТИ

В тезисах предлагается определение предмета контроля целостности виртуальной инфраструктуры и её конфигурации и способ контроля с помощью представления конфигурации виртуальной инфраструктуры графом специального вида.

Ключевые слова: контроль целостности, виртуальная инфраструктура, конфигурация виртуальной инфраструктуры.

Для защиты среды виртуализации требуется выполнение множества мер [1], в том числе должен выполняться контроль целостности виртуальной инфраструктуры и ее конфигураций. Для обеспечения контроля в первую очередь следует определить, что является предметом контроля и каким способом можно его осуществить.

Целостность — одно из трёх основных свойств информации с точки зрения безопасности [2], обеспечение которых является общепринятой практикой защиты информации.

Целостность информации определяется как свойство безопасности информации, при котором отсутствует любое ее изменение либо изменение субъектами доступа, имеющими на него право [1].

При таком определении целостности информация рассматривается исключительно как неделимый объект в том смысле, что нельзя разбить его на контролируемые и неконтролируемые части.

Например, есть некоторый текст, целостность которого контролируется. Безусловно, в нём можно выделить отдельные абзацы, предложения, слова, но при этом изменения в любой части текста могут повлечь за собой искажение смысла информации в целом, а потому нельзя пренебрегать контролем целостности любой из частей.

На практике данный подход не может быть применим, так как реальные объекты имеют сложную структуру и чаще всего являются динамическими, то есть содержат в себе части, изменяющиеся в процессе работы. Например, файловая система хранит на диске в составе директории атрибуты файлов, в том числе меняющиеся данные о дате последнего открытия файла [3], а работа операционной системы и компьютера в целом невозможна без изменений в оперативной памяти. В таких случаях принято выделять критически важные части сложного объекта и контролировать их целостность [4].

Для защиты виртуальных инфраструктур подход, при котором контролируется целостность абсолютно всех частей инфраструктуры, также не подходит. Виртуальная инфраструктура должна рассматриваться как система, состоящая из различных объектов: виртуальных машин, хостов, хранилищ и других объектов в зависимости от конкретной реализации. При этом каждый объект также не является неделимым, и потому вопрос о контроле целостности виртуальной инфраструктуры сводится к контролю целостности только критически важных объектов виртуальной инфраструктуры и их частей.

Вместе с тем, такой подход имеет и недостаток: он не учитывает связи между объектами виртуальной инфраструктуры и различные параметры настройки, то есть конфигурацию.

Для различных виртуальных сред общими будут связи, характеризующие принадлежности одних объектов другим (например, виртуальная машина принадлежит хосту в том смысле, что запущена на нём), связи, характеризующие управление (например, в рамках решения vSphere кампании VMware возможно управление множеством хостов-гипервизоров ESXi с помощью vCenter Server), связи, отражающие передачу данных (например, подключение виртуальных машин к сети).

Игнорирование связей между объектами может повлечь за собой возникновение угроз безопасности. Пусть в виртуальной инфраструктуре существуют 2 сегмента, предназначенные для работы с информацией различного уровня доступа. Первый сегмент для работы с информацией ограниченного доступа включает в себя хост-гипервизор № 1 с работающими на нём виртуальными машинами, второй сегмент предназначен только для работы с общедоступной информацией и состоит из хоста-гипервизора № 2, на котором запущены некоторые виртуальные машины. Если через некоторое время виртуальные машины, работающие на гипервизоре № 1, окажутся включенными на гипервизоре № 2, то возникнет угроза безопасности, связанная со смешением двух различных сегментов, что может повлечь за собой и смешение информации различного уровня доступа. Несмотря на возникновение угрозы и нарушение целостности системы в целом, целостность каждого хоста-гипервизора и каждой виртуальной машины может быть сохранена.

Помимо связей контроль целостности виртуальной инфраструктуры должен учитывать также параметры настройки виртуальной среды. Они значительно разнятся в зависимости от конкретного программного обеспечения, используемого для виртуализации. Примером параметра настройки для среды виртуализации, построенной на платформе vSphere, может служить разрешение или запрет на управление гипервизором ESXi напрямую, в обход vCenter Server (lockdown mode).

Таким образом, необходимо контролировать не только целостность выделенных (критически важных) объектов (частей объектов) виртуальной инфраструктуры, но и целостность её конфигурации, связей между объектами, а также параметры настройки среды виртуализации. Как и в случае с объектами, следует рассматривать лишь критически важные связи и настройки. Минимальный набор наиболее значимых для контроля объектов, связей и настроек должен быть основан на требованиях государственных регуляторов [5, 6] и рекомендациях производителей сред виртуализации [7, 8].

Вопрос обеспечения целостности виртуальных инфраструктур на платформах vSphere и Hyper-V решён с помощью ПАК «Аккорд-В.» и ПАК СЗИ НСД «ГиперАккорд», которые обеспечивают доверенную загрузку виртуальных машин, контролируя целостность оборудования, операционной системы, BIOS и MBR виртуальных машин [9, 10]. Входящий в их состав аппаратный модуль доверенной загрузки, Аккорд-АМДЗ, контролирует целостность технических и программных средств физических серверов (гипервизоров, хранилищ). [11] Эти средства защиты позволяют обеспечить целостность всех объектов виртуальной инфраструктуры.

Вопрос контроля конфигурации требует выбора способа представления связей между объектами. Если каждый объект виртуальной инфраструктуры представить в виде вершины графа, то связи между объектами будут представляться рёбрами. Такой способ представления конфигурации инфраструктуры не является новым, привычен для пользователей сред виртуализации [12] и вместе с тем удобен как для визуального восприятия, так и для хранения в памяти компьютера [13].

В отличие от привычного определения графа, когда рёбра отличаются друг от друга только вершинами, которые они связывают (и, возможно, порядком вершин в случае ориентированного графа), для представления конфигурации виртуальной инфраструктуры стоит назначить каждому ребру некоторое свойство, тип связи, которую данное ребро отражает.

Учитывать различие между связями следует по той причине, что изменение типа связи влечёт за собой изменения в работе инфраструктуры. Например, на хосте-гипервизоре ESXi работает виртуальная машина, целостность которой контролируется. После установки на эту машину vCenter Server целостность как виртуальной машины, так и хоста может быть сохранена, связь между объектами, если не учитывать её тип, также останется прежней, но вместе с тем произойдёт существенное изменение в работе системы: появится возможность управлять хостом-гипервизором ESXi с этой виртуальной машины. Если учитывать тип связи между объектами, то такое преобразование повлечёт за собой нарушение целостности конфигурации, что отражает реальные изменения в системе.

Каждый контролируемый параметр настройки можно соотнести с одним или несколькими объектами виртуальной инфраструктуры и хранить свойство соответствующих вершин графа.

Представление конфигурации виртуальной инфраструктуры в виде графа изложенным способом возможно в любой момент жизни виртуальной инфраструктуры и такой граф определён однозначно критически важными объектами, связями и параметрами.

Это позволяет сравнивать текущую конфигурацию системы с некоторой эталонной (фиксированной) через сравнение двух графов и тем самым контролировать целостность конфигурации системы.

Таким образом, при применении предложенного подхода предметом контроля целостности виртуальной инфраструктуры и её конфигурации являются критически важные объекты инфраструктуры, связи между ними и параметры настройки. Обеспечение контроля целостности объектов осуществляется с помощью соответствующих средств защиты информации, а для контроля связей и настроек может использоваться представление виртуальной инфраструктуры с помощью графа специального вида и последующее сравнение текущего графа с эталонным.

СПИСОК ЛИТЕРАТУРЫ

1. Методический документ ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах».
2. *Девянин П. Н.* Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений. М.: Академия, 2005. С. 5.
3. *Карпов В. Е., Коньков К. А.* Основы операционных систем. Курс лекций. Учебное пособие. М.: Интернет-университет информационных технологий, 2005. С. 173.
4. *Конявский В. А., Гадасин В. А.*. Основы понимания феномена электронного обмена информацией. 3.1.4. Свойства документа — доступность, целостность, легитимность [Электронный ресурс] URL: http://www.okbsapr.ru/docs/books/opf/37_opf.htm (дата обращения: 12.04.2016)
5. Приказ № 17 ФСТЭК России от 11 февраля 2013 г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
6. Приказ № 21 ФСТЭК России от 18 февраля 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
7. VMware Security Hardening Guides [Электронный ресурс] URL: http://www.vmware.com/ru/security/hardening-guides (дата обращения: 12.04.2016)
8. Security guide for Hyper-V in Windows Server 2012 [Электронный ресурс] URL: https://technet.microsoft.com/en-us/library/dn741280.aspx (дата обращения: 12.04.2016)
9. ПАК СЗИ НСД «ГиперАккорд» [Электронный ресурс] URL: http://www.accord.ru/hyper-accord.html (дата обращения: 12.04.2016)
10. ПАК АККОРД-В. [Электронный ресурс] URL: http://www.accord.ru/accord-v.html (дата обращения: 12.04.2016)
11. *Конявская С. В., Мищенко М. Г., Синякин С. А.*. Аппаратные СЗИ НСД. Повторение пройденного. [Электронный ресурс] URL: http://www.okbsapr.ru/konyavskaya_2007_3.html#_ftn2 (дата обращения: 12.04.2016)
12. Using VirtualCenter maps to display VMware Infrastructure relationships [Электронный ресурс] URL: http://searchvmware.techtarget.com/tip/Using-VirtualCenter-maps-to-display-VMware-Infrastructure-relationships (дата обращения: 12.04.2016)
13. *Томас Х. Кормен, Чарльз И. Лейзерсон, Рональд Л. Ривест, Клиффорд Штайн.* Алгоритмы: построение и анализ, 3-е издание.: Пер. с англ. — М.: Вильямс, 2013. С. 626

СТЕНД ДЛЯ ОЦЕНКИ ПО ТЕПЛОВЫМ ПОЛЯМ СКРЫТЫХ ЭЛЕМЕНТОВ В РАДИОЭЛЕКТРОННОЙ АППАРАТУРЕ

А. И. КУХАРЕНКО

Учреждение образования«Белорусский государственный университет информатики и радиоэлектроники»

Измерение тепловых полей радиоэлектронных компонентов, размещенных на печатной плате устройства, может быть использовано для диагностики радиоэлектронной аппаратуры, поиска неисправностей, выявления некорректной работы компонентов или обнаружения потенциальных точек отказа и утечек информации в аппаратуре. Регистрация тепловых полей компонентов осуществляется с помощью тепловизора, имеющего чувствительность не хуже 50мК в диапазоне 7,5–14мкм и передающего в реальном времени термографическое изображение на ПК для дальнейшей обработки программным обеспечением.

Инерционность изменения температуры поверхности проверяемых объектов из-за изменений температуры кристаллов определяется теплопроводностью и теплоемкостью примененных материалов. Высокая теплопроводность кристаллического кремния внутри микросхемы, теплоотвод через припой, медные дорожки и слои заземления и питания на многослойных печатных платах существенно влияют на распределение температур на корпусах компонентов и вокруг их. Хороший теплоотвод на печатную плату сглаживает изменения температур исследуемых радиоэлектронных компонентов и вносит инерционность в получаемые радиометрические изображения, что обуславливает применение тепловизора с высокой чувствительностью.

Изменение температур компонентов и печатной платы может составлять десятки градусов разницы между отключенным устройством и включенным, но эти изменения температуры долговременные и инерционные, и занимают от нескольких минут до нескольких часов, в зависимости от массы и теплоемкости устройства. Значительный же интерес представляют не статические, инерционные изменения температур, а быстрые, динамические изменения температуры электронных компонентов. Такие изменения происходят за секунды, и могут составлять от менее чем 0,1°С до нескольких градусов. Так, с помощью стенда были проведены исследования PCI-Express карточки с микросхемой, обеспечивающей связь по протоколу IEEE 802.11g (WiFi). Тепловизор передавал термографические изображения на компьютер для обработки и анализа. Результаты измерений показали, что температура правой нижней части кремниевого кристалла (точка Sp1), предположительно отвечающая за прием и передачу сигналов, поднималась при переключении от стационарного режима работы в режим поиска свободного от помех канала. На рисунке 1, первым кадром показана термограмма микросхемы на которой видны границы кристалла, корпус и элементы обвязки компонента.

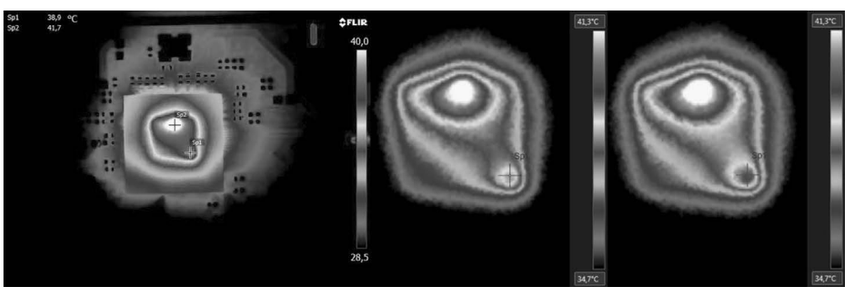


Рис. 1. Термографические изображения микросхемы

На втором и третьем кадре рисунка показано сравнение увеличенной области в центре микросхемы в стационарном режиме и режиме поиска соответственно. Температура точки Sp1 в первом случае составила 39,0°C, во втором 39,3°C, зафиксировано увеличение температуры на 0,3°C. Измерения были проведены с малого расстояния, с разрешением 640×480 пикселей и с использованием макролинзы. При измерениях с большим полем зрения или с меньшим разрешением тепловизора, изменения температуры, из-за усреднений по пикселям, в том же случае составит не 0,3°C, а еще меньше.

Таким образом, важной задачей при разработке стенда оценки по тепловым полям элементов в радиоэлектронной аппаратуре является измерение малых колебаний температуры, отделение их от шумов и визуализация этих малых изменений тепловых полей.

Влияние на термографическое изображение рассеивающих свойств поверхностей проверяемых объектов, дрейф температуры окружающей среды, высокие шумы изображения, а также различная инерционность процессов в каждом конкретном случае вынуждает отказаться от измерения абсолютных значений температуры в каждой точке и перейти к статистической оценке термографических изображений. Статистический анализ изображения применяется для определения характеристик шума термографического изображения и детектирования выхода значений температур за диапазон допустимых значений. Перед проверкой выполняется накопление и усреднение распределения теплового поля по проверяемому объекту, формируется базовое радиометрическое изображение путем нахождения среднего значения для каждого пикселя изображений. Далее ведется сравнения базового радиометрического изображения с текущим путем нахождения разности этих изображений для каждого пикселя. Эта разность сравнивается с пороговым значением. Пример результатов работы алгоритма обработки термографических изображений показан на изображении ниже.

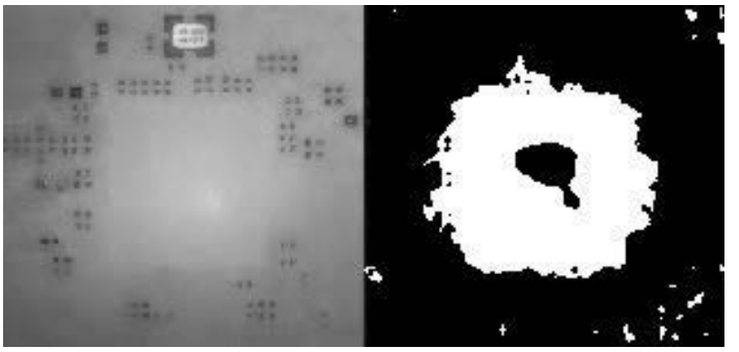


Рис. 2. Термографическое изображение слева и результат работы алгоритма справа

Высокая чувствительность статистического алгоритма накладывает определенные требования на условия проведения измерений. Так, печатная плата исследуемого устройства не должна подвергаться воздействию внешних тепловых полей от световых лучей, тела человека и нагревательных приборов. Вибрации тепловизора и исследуемого устройства должны быть сведены к минимуму.

НОВЫЙ ЗАЩИЩЕННЫЙ СПОСОБ РАСПРОСТРАНЕНИЯ ЛИЦЕНЗИЙ НА ПО

А.Ю. ЧАДОВ
МФТИ

В тезисах описывается реализация нового способа распространения лицензий на ПО, его функциональность и актуальность.

Анализ существующих способов распространения лицензий

На данный момент распространение лицензий[1] на ПО является основным способом распространения программной продукции. Существуют различные способы распространения лицензий: регистрационные коды, активация через интернет или при помощи сотрудников фирмы-производителя, ключевые диски, электронные ключи. Но все они обладают своими недостатками. Регистрационный ключи можно использовать повторно на другой рабочей станции; регистрация через интернет требует обязательного наличия соединения с сетью Интернет на рабочей станции пользователя, что не всегда возможно; регистрация при помощи сотрудников фирмы-производителя отнимает у них время, да и может затянуться; привязка к ключевым дискам вынуждает пользователя постоянно использовать диск, что не очень удобно, а порча или утеря носителя приводят к невозможности пользоваться продуктом; электронные ключи довольно хороший вариант, но и у него есть свои недостатки: самые простые варианты ключей, такие как ключи с памятью, достаточно легко эмулировать, а более сложные, такие, как ключи с программируемым алгоритмом, для пользователя — стоят достаточно дорого (несколько тысяч рублей за штуку), а от продавца — требуется время и затраты на встраивание в продукт.

В данной статье описывается новый способ распространения лицензий, который обеспечивает достаточно высокий уровень защищённости и помогает избежать описанных выше недостатков других продуктов. Суммируем их:

- невозможность защиты от многократного использования одной лицензии;
- необходимость наличия соединения с сетью Интернет у конечного пользователя;
- необходимость дополнительного взаимодействия с сотрудниками фирмы-производителя;
- необходимость серии дополнительных действий со стороны фирмы-производителя, таких как наладка сервера или перенос части кода программы на отчуждаемое устройство;
- высокая цена.

Функциональность решения

Решение называется программно-аппаратный комплекс «Мобильный Генератор Лицензий» (ПАК МГЛ). Он состоит из аппаратных модулей МГЛ (АМ МГЛ), представляющих из себя переносное USB-устройство, одного мастер-устройства (АМ МГЛ «Мастер»), хранящегося у фирмы-производителя, и сопутствующего программного обеспечения: ПО настройки, использующееся в фирме-производителе и ПО, предназначенное для работы с устройством сотрудников фирмы-покупателя: консоль администратора и консоль пользователя. Консоли распространяются на самом устройстве и хранятся на его внешнем диске.

---

[1] Лицензия на объект интеллектуальной собственности — разрешение на использование объекта интеллектуальной собственности (изобретения, промышленного образца, полезной модели, товарного знака, ноу-хау (know how)) на определенных условиях, как правило — за определенное вознаграждение

Лицензии распространяются при помощи АМ МГЛ. Фирма-производитель заносит в устройство данные, необходимые для генерации лицензий, и указывает, какое число лицензий и на какие продукты оно может активировать. Затем устройство — напрямую или через интегратора — передаётся фирме-покупателю. Там назначаются администратор устройства и оператор устройства, они устанавливают свои пароли при помощи соответствующего ПО. Подключив АМ МГЛ к рабочей станции, на которой установлено лицензируемое ПО, пользователь активирует лицензию. Активация может быть произведена как во время установки ПО, так и после, при помощи консоли пользователя. После активации лицензии для дальнейшей работы с лицензируемым ПО подключение устройства к рабочей станции не требуется.

Может возникнуть необходимость разделить лицензии, которые может выдать устройство (передать между отделениями фирмы, или интегратор хочет отдать часть лицензий в одну компанию, а часть в другую). Для этого в АМ МГЛ предусмотрена функция обмена лицензиями между устройствами (здесь и далее передачей лицензий и обменом лицензиями между устройствами будет называться увеличение числа лицензий, которое может выдать одно устройство, за счёт уменьшения числа лицензий, которое может выдать другое, на то же число). Администратор устройства может передать необходимое число лицензий на другое устройство. Процедура может проводиться как между подключёнными к одной рабочей станции устройствами, так и удалённо.

Защищённость решения

Устройство не выдаёт заранее заложенный в него файл лицензии, а само его генерирует из хранящихся внутри данных. Таким образом, лицензию можно выдать с привязкой к конкретной рабочей станции, это позволяется защититься от несанкционированного копирования.

Обмен данными между устройствами при обмене лицензиями защищён криптографическими протоколами, что не позволяет злоумышленнику использовать полученные от устройства данные для несанкционированного увеличения числа имеющихся лицензий.

Аналогичным образом защищён обмен информацией с рабочей станцией.

Итог

Данный метод распространения лицензий лишён всех недостатков, описанных в первой части: лицензии могут генерироваться для конкретной рабочей станции, устройство само генерирует лицензии и не требует соединения с сетью Интернет или контакта с сотрудниками фирмы-производителя, цена устройства относительно невысока, т.к. на одном устройстве можно передать множество лицензий.

Также этот метод достаточно удобен как для продавца, так и для покупателя, и характеризуется высокой защищенностью от атак.

СТЕНД ДЛЯ ИССЛЕДОВАНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕПЛОВЫМ КАНАЛАМ

В.В ЛОБУНОВ, Т.В. БОРБОТЬКО, Е.И. ХИЖНЯК

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники»

С развитием современных средств технической разведки (СТР) возникла потребность в создании технологий противодействия. Одним из примеров развития СТР является

развитие тепловизионной техники, позволяющей обнаруживать и идентифицировать объекты на больших расстояниях, а также в условиях плохой видимости.

Основной задачей при тепловом скрытии объектов от тепловизионных средств обнаружения является минимизация температурного различия объекта наблюдения и фона. Увеличение теплового контраста происходит за счет процессов теплового обмена между объектом наблюдения и средой, в которой он находится, что приводит к увеличению вероятности его обнаружения.

Технический контроль эффективности теплового скрытия объектов наблюдения, реализуемый с помощью тепловизионной техники, обычно проводится в условиях ограниченной освещенности объекта в видимом диапазоне длин волн, то есть ночью. Однако задача теплового скрытия усложняется, если необходимо скрыть не только собственное инфракрасное излучение, но также рассеять излучение мощного стороннего источника, отраженного от поверхности скрываемого объекта. Подобным излучением может являться солнечное излучение, которое повышает тепловой контраст поверхности объекта по отношению к фону.

При разработке и исследовании защитных материалов требуется обеспечить условия проведения эксперимента, схожие с условиями их эксплуатации, что обуславливает актуальность разработки лабораторного стенда для проведения исследований подобных материалов. Таким образом, для исследования средств защиты информации от утечки по тепловым каналам, был разработан и изготовлен стенд, позволяющий имитировать распространение солнечного излучения на исследуемую поверхность и оценивать изменение температуры поверхности при различных углах визирования путем регистрации инфракрасного излучения (ИК).

На рисунке 1 представлена схема разработанного стенда.

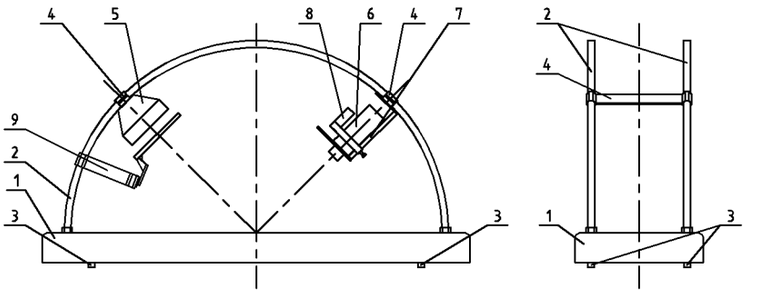


Рис. 1. Схема измерительного стенда: 1 — предметный столик; 2 — металлические дуги; 3 — ножки; 4 — подвижные крепления; 5 — источник излучения; 6 — устройство регистрации ИК излучения; 7 — держатель; 8 — блок управления; 9 — подвижный алюминиевый экран

Конструкция стенда представляет собой две параллельные металлические дуги 2, закрепленные на предметном столике 1. Указанные элементы конструкции являются направляющими для подвижных креплений 4, к которым в свою очередь крепятся источник излучения 5 и держатель 7, предназначенный для неподвижной фиксации устройства регистрации ИК излучения 6. Таким образом, источник излучения и приемник независимо перемещаются по дугам на углы в пределах 180° относительно поверхности предметного столика, в центре которого размещается исследуемый образец.

Стенд является разборным, и, в процессе его транспортировки, для размещения подвижных креплений 4, держателя 7, а также остальных крепежных изделий, необходимых

для его сборки, в предметном столике 1 с нижней стороны присутствует полость. Также в конструкции предусмотрены регулируемые по высоте ножки 3 для позиционирования стенда в горизонтальной плоскости.

Источник излучения оптического диапазона длин волн, имитирующий солнечное изучение, представляет собой алюминиевое основание, на котором в гексагональном порядке закрепляется 7 галогенных ламп типа MR 16 электрической мощностью 50 Вт каждая. Выбранная галогенная лампа имеет параболический отражатель, который направляет излучение в пределах угла 38°, и таким образом, за счет конструкции излучателя, обеспечивается нормальное распределение излучения по поверхности исследуемого образца.

В качестве устройства регистрации ИК излучения была выбрана тепловизионная камера MobIR M4. Устройство работает в инфракрасном диапазоне длин волн 8–12 мкм и имеет неохлаждаемую болометрическую матрицу с разрешением 160×120 пикселей, размер пикселя — 35 мкм. Данная тепловизионная камера позволяет производить измерение температуры поверхности объектов в диапазоне от –25 °С до 250 °С с точностью ±2 °С.

Для дистанционного управления устройством регистрации ИК излучения 6 и автоматизации процесса получения термографических изображений, используется блок управления 8. Устройство представляет собой механический привод с микроконтроллерным управлением, который устанавливается на устройство регистрации излучения и взаимодействует с его панелью управления путем подачи на блок управляющего сигнала.

При исследовании процесса остывания образцов, используется подвижный алюминиевый экран 9, который препятствует распространению излучения нагретого источника. Экран управляется путем подачи ШИМ сигнала на механический привод.

На рисунке 2 представлена зависимость температуры от времени нагрева поверхности маскировочной сети, размещенной на грунте. Показано, что в зависимости от углов визирования, температура поверхности повышается до 95 °С при угле 30° от нормали за время нагрева 30 минут, а при угле 75° от нормали, за аналогичное время нагрева, температура поверхности повышается до 72 °С. Установленные закономерности были получены при апробации стенда.

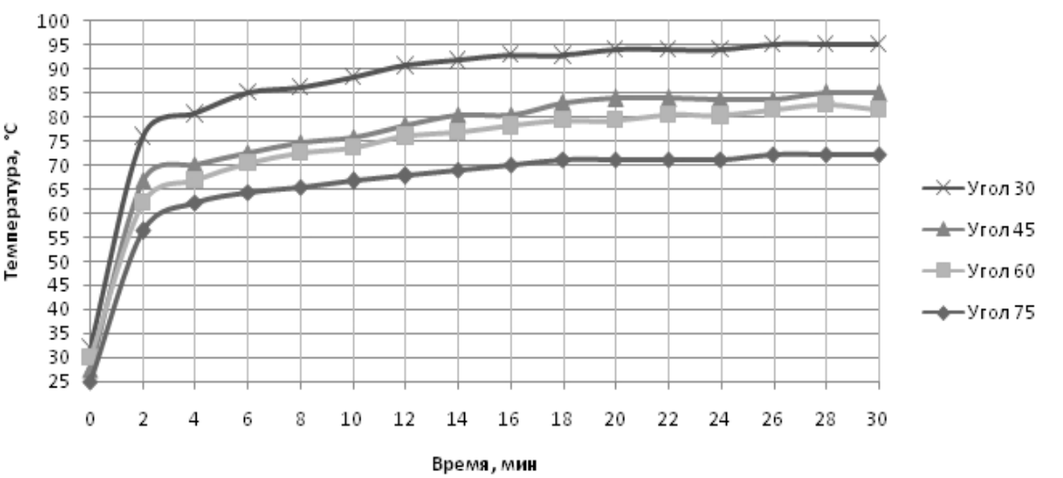


Рис. 2. Температура поверхности маскировочной сети, располагаемой на поверхности грунта, при различных углах визирования

ЗАОЧНЫЕ ДОКЛАДЫ

ОЦЕНКА БЕЗОПАСНОСТИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ НА ОСНОВЕ «ОБЩИХ КРИТЕРИЕВ»

В.А. АРТАМОНОВ

Возрастающее применение мобильных информационных технологий вывело вопрос безопасности данных в мобильных устройствах на новый уровень. А так как приложения в смартфонах и других подобных им гаджетах используются не только на потребительском уровне, но и на корпоративном, то безопасность мобильных приложений обращает к себе все более пристальные взгляды и новые решения. Проблемы реализации хранилищ данных и их передачи можно считать самыми важными среди проблем безопасности приложений на смартфонах, потому что две эти проблемы представляют максимальный риск как для индивидуальных пользователей, так и для корпораций. Несмотря на то, что есть множество атак инъекционного типа, которые проводятся с прицелом на *API* и недостатки при организации памяти, глубина такой атаки опирается на скомпрометированный сервер или не до конца безопасный обмен данными, дающий злоумышленнику возможность манипулирования обменом данными со смартфоном. Средства безопасности, предустановленные в операционной системе создают все больше и больше препятствий, необходимых для преодоления того чтобы атака завершилась успехом, и нарушитель политики безопасности получил доступ к использованию недостатков в организации памяти в устройстве. На практике эти недостатки в сторонних приложениях не несут в себе огромного риска для платформы в целом, до тех пор, пока они не будут скомбинированы с уязвимостями самой ОС.

Множество компонентов информационных систем, взаимодействующих с критичными ресурсами, включает программные решения для мобильных платформ. Актуальность таких решений определяется значительным развитием мобильных систем и, в совокупности с востребованностью аудита информационной безопасности как этапа разработки защищенных систем обработки данных, обуславливает насущность исследования мобильных приложений в контексте информационной безопасности.

В работе [1] приведена систематизация типовых уязвимостей мобильных приложений, работающих под управлением наиболее распространённых мобильных ОС *Android, iOS* и *Windows Phone*:

- Использование незащищенных протоколов передачи информации.
- Небезопасная конфигурация защищенного соединения.
- Небезопасная аутентификация веб-сервера.
- Использование небезопасных криптографических методов.
- Небезопасное хранение конфиденциальных данных.
- Непреднамеренная компрометация данных.
- Вывод конфиденциальной информации в системный журнал событий.
- Небезопасное использование возможностей межпроцессного взаимодействия.
- Небезопасная обработка входных данных.
- Небезопасное использование возможностей сети GSM.
- Отсутствие проверок наличия несанкционированного привилегированного доступа к мобильному устройству.

- Недостаточная защита пакета приложения и его компонентов.
- Небезопасная конфигурация и использование потенциально уязвимых методов в контексте обработки управляемых ресурсов.

В контексте разработки информационных систем, к которым предъявляются повышенные требования безопасности, такие уязвимости следует рассматривать как уязвимости критичной степени важности. В связи с этим актуальным становится вопрос оценки безопасности мобильных приложений, в том числе соответствия их определённым, заранее установленным критериям (сертификация). Для этого обратимся к международному опыту, в частности к стандарту ИСО/МЭК 15408 «Критерии оценки безопасности информационных технологий» более известному под брэндом — *Общие критерии (ОК)* [2,3]. ОК в применении к оценке безопасности изделий информационных технологий (ИТ) являются по сути *метасредствами*, задающими систему понятий, в терминах которых должна производиться оценка, и содержащими относительно полный каталог требований безопасности (функциональных и доверия), но не предоставляющих конкретных наборов требований и критериев для тех или иных типов продуктов и систем ИТ, выполнение которых необходимо проверять. Эти требования и критерии фигурируют в профилях защиты (ПЗ) и заданиях по безопасности (ЗБ)[4]. Предполагается, что профили защиты, в отличие от заданий по безопасности, носят относительно универсальный характер: они характеризуют определенный класс изделий ИТ вне зависимости от специфики условий применения.

Общие положения политик безопасности, относящиеся к защитным сервисам мобильных приложений могут состоять в следующем:

- Описания правил идентификации и аутентификации всех субъектов доступа (порядок аутентификации, разделение функций пользователя и администратора, условия, накладываемые на порядок аутентификации в зависимости от статуса и условий работы пользователя в информационной системе).
- Описания управления доступом к информационным ресурсам сервиса безопасности (модель доступа, критерии предоставления доступа, наборы привилегий субъектов доступа, порядок изменения правил доступа).
- Описание подотчетности пользователей, реализуемой посредством сервиса безопасности (какие действия пользователей при работе с какими сервисами могут быть подотчетны при применении объекта оценки, описанного в профиле).
- Описания правил протоколирования и аудита для анализа функционирования сервиса безопасности.
- Обеспечение доступности коммуникационных каналов.
- Описания правил обеспечения конфиденциальности и целостности управляющей информации (в частности, при удаленном администрировании).
- Описания порядка обеспечения целостности аппаратно-программной и информационной частей сервиса безопасности (список контролируемых компонент, порядок контроля и т.д.).
- Обеспечение невозможности обхода защитных средств (набор управленческих решений, обеспечивающих соответствующие предположения безопасности).

Мобильные приложения могут быть развернуты с использованием архитектуры *толстый клиент* (приложение, обеспечивающее расширенную функциональность независимо от центрального сервера), или тонкий клиент (программа-клиент в сетях с клиент-серверной или терминальной архитектурой, который переносит все или большую часть задач по обработке информации на сервер). Выбор типа приложения («толстого»

или «тонкого»), зависит от его сложности, используемого устройства, сферы применения, а также наличия или отсутствия сетевого подключения.

Управление мобильными устройствами и приложениями (MDM) позволяет применять разнообразные политики безопасности для мобильных устройств, таких как смартфоны и планшеты. Цель этих политик заключается в установлении уровней безопасности адекватных для обеспечения безопасной обработки корпоративных и персональных данных при подключении к сетевым ресурсам предприятий, корпораций и банков. Пример такого подхода предложен в ПЗ, опубликованном в документе [5].

Этот документ предоставляет базовый набор функциональных требований безопасности (SFR) для системы MDM, которая является объектом оценки (ОО). **MDM-система** является лишь одним из компонентов развертывания корпоративных мобильных устройств. Другие компоненты, такие как платформы мобильных устройств, которые обеспечивают соблюдение политик безопасности, а также сервера управления доступом к сети, находятся вне области данного документа.

MDM-агент, который находится в центре внимания этого ПЗ, установлен на мобильном устройстве, как приложение или является частью его ОС. MDM-агент устанавливает защищенное соединение с **MDM-сервером** и управляется администратором безопасности. Магазин приложений (MAS) сервера для загрузки и установки приложения всего предприятия организуется централизованно. MDM-агент должен тесно взаимодействовать или быть частью платформы мобильного устройства для установления политики безопасности и выполнения запросов о состоянии устройства. Мобильное устройство, в свою очередь, имеет свои собственные требования безопасности, указанные в мобильном и базовом ПЗ [6,7] на предмет которых мобильное устройство должно быть оценено либо одновременно или до оценки MDM-агента. Если MDM-агент является частью ОС мобильного устройства, агент может представлять несколько интерфейсов для настройки мобильного устройства, таких как локальный интерфейс и интерфейс удаленного доступа. Агенты, соответствующие этому профилю должны по крайней мере предложить интерфейс с доверенным каналом, который является частью MDM-системы. Совместимые агенты могут также предложить другие интерфейсы, а также новые аспекты конфигурации этих приложений.

Требования доверия безопасности ОК определяют оценочные уровни доверия (ОУД), которые определяют область сертификации соответствия. Для большинства областей применения достаточно третьего уровня доверия; с другой стороны, этот уровень достижим при разумных затратах на разработку, так что его можно считать типовым. В число требований доверия третьего оценочного уровня входят:

- анализ функциональной спецификации, спецификации интерфейсов, эксплуатационной документации;
- независимое тестирование;
- наличие проекта верхнего уровня;
- анализ стойкости функций безопасности;
- поиск разработчиком явных уязвимостей;
- контроль среды разработки;
- управление конфигурацией.

В принципе достижим и четвертый оценочный уровень, который можно рекомендовать для конфигураций повышенной защищенности. Вероятно это самый высокий уровень, который можно достичь при существующей технологии программирования и разумных затратах материальных и временных ресурсов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Сафин Л. К.* Исследование информационной защищённости мобильных приложений / Л. К. Сафин, А. В. Чернов, Я. А. Александров, К. Н. Трошина // Вопросы кибербезопасности. — 2015. — № 4 (12). — С. 28–36.
2. Common Criteria for Information Technology Security Evaluation, Part (1,2,3): Introduction and General Model, CCMB-2012–09-(001,002, 003) Version 3.1 Revision 4, September 2012.
3. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012–09–004, Version 3.1, Revision 4, September 2012.
4. *Бетелин В. Б.* Профили защиты на основе «Общих критериев». Аналитический обзор/ В. Б. Бетелин, В. А. Галатенко, М. Т. Кобзарь, А. А. Сидак, И. А. Трифаленков// Бюллетень JET INFO — 2003.
5. Extended Package for Mobile Device Management Agents Version 2.0 /3.1, PP_MDM_AGENT_v 2.0//NSA, 2014–12–31.
6. Protection Profile for Mobile Device Fundamentals Version 2.0 /3.1, PP_MD_v2.0//NSA, 2014–09–17.
7. Protection Profile for Mobile Device Management Version 2.0 /3.1, PP_MDM_v2.0//NSA, 2014–12–31.

МЕХАНИЗМ ОБНОВЛЕНИЯ ЗАЩИЩЕННЫХ МИКРОКОМПЬЮТЕРОВ МКТ

А. Ю. БАТРАКОВ
ЗАО «ОКБ САПР», Москва, Россия

Статья посвящена описанию двух методов обновления защищенных микрокомпьютеров: с изменением и без изменения состояния ПЗУ.

Ключевые слова: защищенный компьютер, микрокомпьютер, обновление.

Защищенные микрокомпьютеры МКТ обладают простым, но надежным механизмом обеспечения целостности операционной системы. Вся внутренняя память данных микрокомпьютеров физически переводится в режим «только чтение» [1–7]. Это гарантирует, что никакие зловреды не могут быть записаны в МКТ, а никакие предустановленные средства разграничения доступа не могут быть удалены или выключены [8].

Но может ли быть удобным и безопасным средство, которое нельзя изменить? Полагаем, нет.

Во-первых, огромное количество обнаруженных за последнее время уязвимостей показывает, что бывают необходимы обновления системных библиотек и программного обеспечения. Чего стоит один только печально знаменитый Heartbleed. Во-вторых, мир не стоит на месте и появляются новые модели принтеров, сканеров и другой техники. Для них могут понадобиться новые драйвера. В-третьих, не стоит забывать, что может обновляться и пользовательское программное обеспечение, например, с целью расширения функционала.

Таким образом, становится очевидно: удобное и безопасное средство должно иметь возможность обновления. Но память физически находится в режиме «только чтение».

Как быть? Один из способов обновления очевиден: передать устройство в сервисный центр, где будут произведены все технологические операции для перезаписи памяти. Этот способ требует доставки всех обновляемых устройств в сервисные центры, а также ненулевое время на проведение обновления. Неудобно!

Для проведения быстрого и удобного обновления была разработана специальная технология. В микрокомпьютерах МК имеется посадочное место для MicroSD карты. На эту карту может быть записан образ обновления. Образ содержит в себе информацию обо всех изменениях: какой файл заменить, какой удалить, какой добавить.

Почему образ обновления не может принести с собой зловреда? Все очень просто. Образ обновления распространяется только совместно с электронной подписью. Неизменная операционная система содержит в себе сертификат, на котором подпись может быть проверена. При каждой загрузке неизменная операционная система проверяет подпись под образом обновления. Если подпись верна, обновление применяется к файловой системе прямо в оперативной памяти. Если же проверка подписи закончилась ошибкой, загрузка будет прервана.

Таким образом, с одной стороны, операционная система осталась неизменной, а с другой стороны, она обновлена.

Разумеется, у этой технологии есть и свои минусы. Так как при каждом старте операционной системы (даже после перезагрузки!) необходимо проверить подпись под образом, загрузка несколько замедляется. По нашим тестам — не сильно. Примерно на 10 секунд при размере образа обновления в 100 мегабайт. 100 мегабайт — довольно много. В них одновременно могут содержаться сразу нескольких новых библиотек, несколько дополнительных драйверов. Но обновления со временем накапливаются, а образ разрастается. Особенно быстро образ растет при обновлении версии операционной системы. Тут образ может легко увеличиться до гигабайта и более. Понятно, что с таким образом обновления работать неудобно.

В этом случае предлагается все же передать устройства в сервисный центр, где после проведения необходимых технологических процедур все обновления будут применены к основной операционной системе. Это позволит резко сократить время загрузки и начать собирать новые обновления.

Как подписанный образ обновления должен попасть на MicroSD-карту? Есть несколько вариантов. Самый незамысловатый — администратор извлекает карту из МКТ, записывает на нее образ, после чего возвращает карту на место. Этот способ подходит если количество используемых МКТ невелико.

Более удобный способ — централизованная передача обновлений по сети. Для этого устанавливается простейший сервер. Микрокомпьютеры по регламенту или по команде запрашивают обновления у сервера. Если обновление есть, оно закачивается на карту памяти. И уже при следующей перезагрузке обновление будет применено.

Может возникнуть вопрос, а зачем закачивать обновление на карту памяти, если можно при каждом включении забирать образ обновления с сервера по сети? Можно и так! Об этой технологии читайте в статье «Центр-Т на защищенных микрокомпьютерах МКТ».

СПИСОК ЛИТЕРАТУРЫ:

1. Компьютер типа «тонкий клиент» с аппаратной защитой данных: Патент на полезную модель № 118773. 27.07.12. Бюл. № 21.
2. Компьютер с аппаратной защитой данных от несанкционированного изменения: Патент на полезную модель № 137626. 20.02.2014. Бюл. № 5.

3. Мобильный компьютер с аппаратной защитой доверенной операционной системы: Патент на полезную модель № 138562. 20.03.2014. Бюл. № 8.
4. Мобильный компьютер с аппаратной защитой доверенной операционной системы от несанкционированных изменений: Патент на полезную модель № 139532. 20.04.2014. Бюл. № 11.
5. Мобильный компьютер с аппаратной защитой доверенной операционной системы: Патент на полезную модель № 147527. 10.11.2014. Бюл. № 31.
6. Мобильный компьютер с аппаратной защитой доверенной операционной системы от несанкционированных изменений: Патент на полезную модель № 151264. 27.03.2015. Бюл. № 9.
7. Рабочая станция с аппаратной защитой данных для компьютерных сетей с клиент-серверной или терминальной архитектурой: Патент на полезную модель № 153044. 27.06.2015. Бюл. № 18.
8. *Конявский В. А.* Компьютер с вирусным иммунитетом // Информационные ресурсы России. 2015. № 6. С. 31–34.

ИСПОЛЬЗОВАНИЕ ВИРТУАЛЬНОЙ МАШИНЫ DOSBOX ПРИ ИЗУЧЕНИИ КРИПТОГРАФИЧЕСКОГО ПАКЕТА PGP

В. А. ГАНЖА, О. И. ЧИЧКО

Рассматривается проблема обучения студентов практическим навыкам работы по схеме криптографии с открытым ключом.

Несмотря на то, что к 2016 году накоплено огромное количество литературы и наработок по теме защиты информации, в настоящее время всё равно наблюдается неослабевающий интерес к методам защиты информации в различных информационных системах. Это обусловлено тем, что, в информационные технологии продолжают вовлекаться массы людей, представляющие широкий социальный срез населения, куда могут попасть не вполне благополучные и не вполне благонадёжные категории пользователей, ищущих свой интерес в нарушениях штатной работы информационных систем, во взломе компьютерных сетей организаций [1].

Учебной программой дисциплины «Методы защиты информации» предусмотрено практическое освоение криптографических пакетов с открытым ключом. Таким программным обеспечением является единственный пакет — PGP (*Pretty-Good-Privacy*), основанный на алгоритме асимметричного шифрования RSA.

С середины 90-годов пакет PGP распространял сам его «отец-основатель» Филипп Циммерманн (Philip Zimmermann) [2], основавший PGP корпорацию. Но в 2010 году PGP-корпорация была приобретена фирмой Symantec [3]. Теперь пакет PGP доступен только от фирмы Symantec, лицензия на который стоит более $ 150. Дороговизна — одна из причин, по которой этот пакет мы не скоро увидим в компьютерном классе вуза.

Вторая причина в особенностях самого пакета PGP последней версии. Фирма Symantec продаёт сейчас пакет PGP 10-й версии. PGP-10, являясь проприетарным программным продуктом, как и большинство программ, разработанных под Windows, имеет хронические «болячки», заключающиеся: в разбрасывании файлов по разным каталогам; создании

не вполне очевидных записей в системном реестре и в сокрытии многих деталей работы криптографического алгоритма с открытым ключом.

Авторам не удалось в учебных целях вычленить из рабочих файлов программы PGP 10 открытый и закрытый ключи; не удалось также «обмануть» программу и зашифровать файл не имея электронной почты. Программа при инсталляции настойчиво ищет на машине почтового клиента Thunderbird, Outlook и ему подобные и шифрует файлы с целью непременной отсылки по электронной почте, через интернет некому адресату.

В описании PGP 10.2 присутствуют следующие строки «PGP Corporation представила персональный пакет защиты и шифрования данных, где реализованы средства автоматического исполнения для организации корпоративной защиты. Полностью автоматическая работа пакета PGP Desktop скрывает от пользователя все действия по кодированию или декодированию данных».

Быть может это и хорошо для рядового пользователя, но совершенно недопустимо при обучении будущего программиста, будущего специалиста по информационным технологиям. Для этой категории обучаемых необходимо полностью показать и продемонстрировать всю «кухню», всю анатомию работы пакета PGP и криптоалгоритма RSA.

Оптимальным вариантом оказалась одна из первых 16-разрядных версий пакета PGP-5, который бесплатно распространялся ещё Филиппом Циммерманном и который без проблем запускается в консоли любой 32-разрядной машины Windows XP/7. Однако в большинстве минских вузов произошло поголовное обновление компьютерных классов на 64-разрядные машины, а в 64-разрядной консоли пакет PGP-5 работать не может.

Выход только в использовании виртуальной машины. Опять таки, для компьютерного класса вуза выбор оказался предопределён: замечательная виртуальная машина Vmware не подходит, поскольку достаточно тяжеловесна, капризна и далеко не бесплатна. Виртуальная машина DOSBox версии 0.74 [4] оказалась самым подходящим вариантом, она в качестве гостевой операционной системы может быть инсталлирована и запущена в любой 64-разрядной среде. DOSBox — вполне простая программа и к тому же с открытым исходным кодом, то есть бесплатная в отличие от других виртуальных машин.

На рисунке 1 показано окно запущенной виртуальной среды DOSBox, где в качестве виртуального диска C: смонтирована ветка реальной файловой системы хостовой машины d:\anti.win\PGP5.

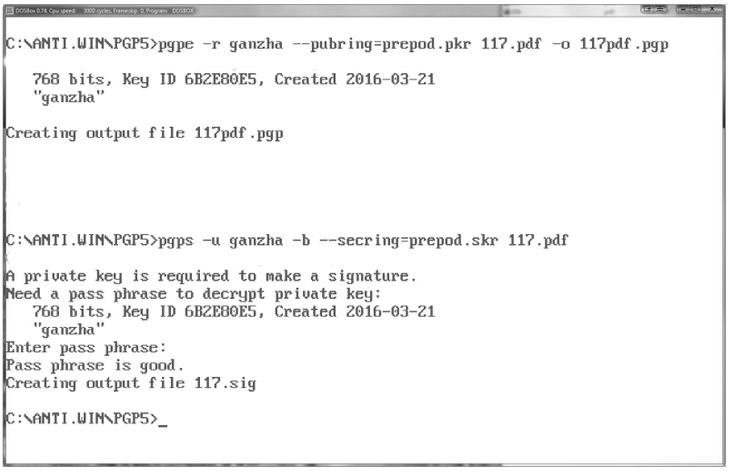


Рис. 1. Окно запущенной виртуальной среды DOSBox

На копии экрана (рисунок 1) представлена работа двух команд со всеми ключами. Первая — pgpe шифрует файл 117.pdf в закодированный файл 117pdf.pgp; вторая команда pgps — создаёт электронную подпись 117.sig для этого же файла 117.pdf.

Простота использования и небольшой набор команд способствует быстрому обучению и освоению студентами пакета DOSBox. Эта программа была установлена на компьютерах в нашем учебном классе.

С помощью этого пакета в компьютерном классе удалось выполнить лабораторные работы по всем стандартным вопросам [5] освоения пакета PGP предусмотренные учебной программой:

- использование функции симметричного шифрования по алгоритму IDEA;
- создание пары ключей для работы по алгоритму RSA;
- обмен ключом шифрования по алгоритму Диффи-Хеллмана;
- рассылка открытого ключа студентами группы друг другу и организация локального обмена зашифрованными сообщениями;
- расшифровывание полученных сообщений личным ключом;
- создание цифровой подписи личным ключом;
- верификация цифровой подписи списка предложенных файлов.

ЛИТЕРАТУРА

1. *Ганжа В. А., Сидорик В. В., Чичко О. И.* Компьютерные сети. Информационная безопасность и сохранение информации. Учебно-методическое пособие. Минск БГУИР, 2014. — С. 128.
2. http://philzimmermann.com/RU/background/index.html
3. https://www.symantec.com/products/information-protection/encryption
4. http://www.dosbox.com/
5. *Левин М.* PGP. Кодирование и шифрование информации с открытым ключом. — М. Бук-пресс, 2006, — С. 166.

КРИПТОГРАФИЮ — НА СЛУЖБУ ЕГЭ!

М. М. ГРУНТОВИЧ

Закрытое акционерное общество «ОКБ САПР», Москва, Россия

В статье предлагается метод обеспечения конфиденциальности, целостности и неотказуемости при рассылке информации из центра с использованием типовых ключевых USB-токенов, при котором получить доступ к ее содержанию могут не менее двух из трех ее получателей.

Ключевые слова: шифрование, целостность, неотказуемость, разделение секрета.

Введение

Как-то перед нами была поставлена задача разработать безопасную систему рассылки контрольно-измерительных материалов КИМ ЕГЭ. Задача, на первый взгляд, типовая, однако у заказчика была еще одна вводная: для вскрытия контрольно-измерительных материалов необходимо присутствие не менее двух человек из трех представителей регионального центра тестирования.

В инвариантной форме это звучит так: необходимо обеспечить безопасную доставку файла из центра к получателям с обеспечением следующих свойств информационной безопасности:

- конфиденциальности,
- целостности,
- неотказуемости (центр не может отказаться, что именно он разослал этот файл),
- невозможности получения монопольного доступа к содержанию только одним лицом из трех.

При этом предпочтительно максимально использовать существующие средства криптографической защиты информации, например, персональные USB-токены.

Налицо СКЗИ с пороговой схемой разделения секрета. Сразу же на ум приходит линейная схема разделения секрета Шамира, но проблема в том, что штатное СКЗИ, каковым является USB-токен, не умеет делать необходимые вычисления, а изменять прошивку устройства не желательно. Нам все же удалось ридумать, как можно реализовать разделение секрета с использованием типовых персональных USB-токенов.

Архитектура системы

Система защиты состоит из следующих элементов:

- центр управления ключами (ЦУК), организующий криптографическую защиту сети,
- центр рассылки, обладающий ключевой информацией для связи со всеми остальными участниками, использующий HSM с неизвлекаемой персональной ключевой информацией на борту,
- региональные пункты получения информации, организующие работу на местах,
- получатели информации в количестве трех человек в каждом региональном пункте, каждый из которых обладает ключевым носителем (USB-токеном) с неизвлекаемой персональной ключевой информацией.

Принцип работы

Идея:

- ключевая система с архитектурой «звезда»: центр рассылки имеет ключи парной связи со всеми получателями,
- центр рассылки подписывает содержимое файла для каждого регионального пункта,
- выполняет шифрование файла на случайно сгенерированном разовом ключе,
- этот ключ шифруется в адрес каждой из трех пар получателей (три получателя — три пары),
- три экземпляра зашифрованного разового ключа вместе с зашифрованным файлом и подписью образуют защищенный контейнер,
- контейнер отсылается в региональный пункт,
- любые двое получателей в региональном пункте предоставляют свои ключевые носители,
- из файла контейнера извлекается и расшифровывается разовый ключ,
- извлекается и расшифровывается целевой файл,
- проверяется электронная подпись центра рассылки.

Ключевая система

ЦУК представляет собой Удостоверяющий центр с соответствующей ключевой информацией:

- ключ подписи сертификатов,
- сертификат ключа проверки электронной подписи центра рассылки,

– сертификаты открытых ключей Диффи-Хеллмана (Д-Х) центра рассылки и получателей.

У центра рассылки имеется следующая ключевая информация:
– ключ электронной подписи (ЭП) центра рассылки,
– закрытый ключ Д-Х центра рассылки,
– сертификат ключа проверки ЭП ЦУК,
– сертификаты открытых ключей Д-Х получателей,
– собственные сертификаты ключа ЭП и открытого ключа Д-Х.

Каждый получатель владеет минимальной ключевой информацией:
– свой закрытый ключ Д-Х,
– сертификат ключа проверки ЭП ЦУК.

Помимо этого в вычислениях система использует:
– ключи парной связи центра рассылки и получателя,
– разовый ключ шифрования контейнера,
– которые вычисляются/генерируются непосредственно перед использованием и уничтожается сразу же после этого.

Подготовительный этап

ЦУК:
– генерирует ключевую информацию всех участников системы и готовит соответствующие ключевые носители,
– безопасным образом доставляет в центр рассылки ключевой носитель, сертификат ключа проверки ЭП ЦУК и базу сертификатов открытых ключей получателей,
– безопасным образом доставляет в региональные пункты по три ключевых носителя (токена) с ключевой информацией получателей.

Формирование контейнера

Для защиты файла в адрес регионального пункта, представленного тройкой получателей, центр рассылки выполняет следующую последовательность действий:
1. проверяет сертификаты трех получателей,
2. вычисляет ЭП содержимого файла,
3. генерирует случайный разовый ключ,
4. шифрует содержимое файла на разовом ключе,
5. шифрует разовый ключ на каждой из трех пар ключей получателей,
6. вкладывает в контейнер зашифрованное содержимое файла, значение ЭП, три экземпляра зашифрованного разового ключа, сертификаты открытых ключей центра рассылки,
7. вычисляет контрольную сумму контейнера, как код аутентификации на разовом ключе и добавляет ее в контейнер.

Шифрование данных выполняется в режиме гаммирования с обратной связью, ключей — в режиме простой замены.

Шифрование разового ключа K в адрес пары получателей i и j (i<j) на шаге 5) в HSM центра рассылки предлагается выполнить следующим образом:
1. экспортировать разовый ключ K на открытом ключе получателя i (результат: K*i — зашифрованный K на ключе парной связи центра рассылки и получателя i),
2. вычислить ключ парной связи с получателем j,
3. зашифровать на нем данные K*i (результат: ключ K*, последовательно зашифрованный на ключах связи Центра рассылки с получателями i и j).

Расшифрование контейнера

Получив контейнер с файлом, любая пара представителей регионального пункта выполняет следующую последовательность действий:

1. извлекает и проверяет сертификаты открытых ключей центра рассылки,
2. считывает экземпляр разового ключа, зашифрованный для данной пары получателей,
3. расшифровывает разовый ключ,
4. проверяет контрольную сумму контейнера,
5. расшифровывает содержимое файла на разовом ключе,
6. проверяет ЭП центра рассылки.

Расшифрование разового ключа K* на шаге 3) с использованием персональных USB-токенов пользователей i и j (i<j) предлагается выполнить следующим образом:

1. в токене j расшифровать данные K* на ключе парной связи с центром рассылки, результат K*i,
2. импортировать ключ K*i в токен i на открытом ключе центра рассылки.

Далее токен j должен выполнить операции проверки кода аутентификации и расшифрования содержимого файла, и при этом разовый ключ не появляется в открытом виде в ОЗУ компьютера.

В описании алгоритмов формирования/разбора контейнера мы опустили служебную часть: идентификация, отметка времени. Это конечно тоже необходимо, но не является целью данной заметки.

Таким образом, с помощью типовых персональных USB-токенов может быть построена пороговая схема разделения секрета. При этом изменение штатной прошивки токенов не требуется, во время работы долговременная персональная ключевая информация не появляется в ОЗУ компьютеров, а также обеспечиваются необходимые свойства безопасности информации при передаче по открытому каналу связи.

DOS/DDOS-АТАКА

Д.И. ДЕВЯТИЛОВ

Московский физико-технический институт (ГУ)

В статье приводится общая классификация DoS-атак, рассматриваются проблемы борьбы с DoS/DDoS-атаками, и предлагаются методы их решения.

Ключевые слова: флуд, DNS-сервер, хакер, провайдер, эксплойт, сетевое оборудование, отказ в обслуживании.

Введение

Интернет стремительно превращается в рынок услуг с очень большим оборотом денежных средств. Сбой или недоступность информационного сервера влечет огромные финансовые потери. В последнее время стала особенно актуальной проблема DoS/DDoS-атак. Их мощность увеличилась почти в 3.5 раза [1] только за четвертый квартал 2014 года. Для обеспечения информационной безопасности в организациях необходимо уметь отражать или предотвращать DoS/DDoS-атаки, но на сегодняшний день нет эффективного решения.

DoS (*Denial of Service* — отказ в обслуживании) — хакерская атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых

легальные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднён. DDoS (*Distributed Denial of Service* — распределённая атака типа «отказ в обслуживании») — это атака, выполняющаяся одновременно с большого числа компьютеров. Цель атакующих — сделать в Интернете недоступным тот или иной ресурс. В настоящее время DoS и DDoS-атаки наиболее популярны, так как позволяют довести до отказа практически любую систему, не оставляя юридически значимых улик [2].

На данный момент существует множество частных методов борьбы с DoS-атаками, но отдельно друг от друга их применение неэффективно, так как при возникновении DoS-атаки непонятно, к какому типу она относится. Универсальных рецептов противодействия DoS/DDoS атакам нет. Но уже сейчас можно предпринять ряд мер по снижению вероятности реализации таких атак, основываясь на их классификации. Именно она помогает быстро обнаружить начало DoS-атаки и использовать известные методы борьбы для ее предотвращения.

Классификация DoS-атак [3]

На данный момент выделяют 4 типа DoS-атак:

- атака на насыщение полосы пропускания;
- атака, приводящая к недостатку системных ресурсов;
- атака, использующая ошибки программирования;
- атака на DNS-серверы.

Каждый из этих типов имеет свои особенности.

Атака на насыщение полосы пропускания

Обычно злоумышленники для атаки на целевую систему используют флуд (*flood* — «наводнение», «переполнение») — атака, связанная с большим количеством обычно бессмысленных запросов к компьютерной системе или сетевому оборудованию, имеющая своей целью или приводящая к отказу в работе системы из-за насыщения полосы пропускания канала связи. Есть несколько разновидностей флуда: *HTTP-флуд, ICMP-флуд, UDP-флуд, SYN-флуд* и др.

Методы борьбы

По умолчанию все серверы должны быть обновлены до последней версии патча защиты, если таковая имеется. Также должны быть отключены все сервисы, которые не используются в сети.

Один из методов борьбы с DDoS-атаками, рассчитанными на насыщение полосы пропускания канала связи, является постоянная смена IP-адреса компьютера-жертвы. Данный вид защиты носит название «движущейся оборонительной цели». После изменение IP-адреса маршрутизаторы сбросят вредоносные пакеты, которые поступали на конкретный IP-адрес.

Отключение широковещательной передачи сообщений помогает в борьбе против ICMP-флуда. В этом случае хосты больше не будут использоваться в качестве усилителей DDoS-атаки.

Так же создается специальная база маршрутов, по которым обычно идут пакеты в штатном режиме работы системы. Это позволяет защититься от UDP, TCP и ICMP-флудов.

Атака, приводящая к недостатку системных ресурсов

В данном случае DoS-атака направлена на захват системных ресурсов компьютера, не затрагивая канал связи. Процессор сервера может не справиться со сложными вычислениями. Произойдет сбой из-за того, что центральный процессор или оперативная память

окажутся недоступны. Примерами таких атак являются: отправка «тяжелых пакетов», переполнение сервера лог-файлами, атака на плохо организованную систему квотирования или на отсутствие проверки данных пользователя.

Методы борьбы
Существуют различные системы обнаружения вторжений, которые позволяют обнаруживать DoS-атаки по известным сигнатурам, распознавая аномальное поведение системы.

Атака, использующая ошибки программирования
Еще данный вид атаки называют атаками на приложения. Этот вид атак наиболее опасен и влечет за собой тяжелые последствия для сервера, так как плечо атаки (отношение ресурсов необходимых на стороне приложения к ресурсам на атакующей стороне) в этом случае максимально. Более продвинутые хакеры, полностью разобравшись в структуре системы или приложения, пишут специальные программы — эксплойты, которые помогают атаковать коммерческие предприятия. Примером таких атак является простое переполнение буфера. Часто хакеры используют недостатки в программном коде.

Методы борьбы
Создается база шаблонов известных эксплойтов и производится мониторинг вхождений данных шаблонов в саму систему.

Анализ журнала событий после и во время DoS-атаки помогает выявить новые типы атак, либо модификации старых.

Атака на DNS-серверы
Данный вид атаки самый дорогостоящий и ресурсозатратный. Хакеры, используя крупные ботнеты, атакуют правительственные организации, очень крупные компании, либо известные интернет-магазины. Сервер-жертва может находиться в простое достаточно длительное время. Из-за этого компания несет огромные убытки [4]. В 2012 году хакеры группы Anonymous хотели вывести из строя глобальную сеть, путем атаки на 13 корневых серверов DNS [5]. В этом же году крупнейший в мире хост — провайдер Go Daddy и вместе с ним более 33 миллионов доменов по всему миру пострадали от DDoS-атаки [6]. Одной из самых мощных атак в истории считается атака на компанию Spamhaus в 2012 году. Она продлилась несколько дней и достигла своей пиковой мощности в 300 Гб/с [7].

Методы борьбы
Одним из эффективных методов борьбы является перенаправление трафика на площадку более мощного провайдера. За счет этого увеличивается полоса пропускания канала связи, трафик фильтруется и уже легитимный трафик идет к пользователю.

Защита от DoS/DDoS-атак
От любой атаки можно защититься, но в настоящее время нет универсального способа защиты. Полной обобщенной классификации нет, в том числе и в той, что представлена, смешаны разные уровни абстракции. Одни компании используют статические средства защиты до начала самой атаки, выстраивая специальные фильтры. Они в свою очередь обучаются на маршрутах сайта, по которым ходят обычные пользователи. Происходит мониторинг Интернет-трафика в реальном времени. Другие — хранят базу данных сигнатур уже известных DoS-атак. Производя при этом мониторинг всей системы по сигнатурам, можно зафиксировать начало DoS-атаки. Но, как и в случае с вирусами, данный способ не так эффективен, потому что при появлении какой-либо

новой DoS-атаки данная база сигнатур бесполезна. Еще один способ обнаружения начала DoS-атаки предоставляет собой выявление аномального поведения в системе. Текущее состояние системы в реальном времени сравнивается с ее нормальным состоянием, т. е. тем, когда наблюдается обычная динамика трафика и производительности самого сервера [8]. Все эти способы помогают защититься лишь от некоторых видов DoS-атак. Хакеры, нацеленные «уронить» тот или иной сервер, анализируют защиту и придумывают другие способы воздействия на нее, усиливая атаку, либо вовсе прибегая к иному методу. Стоит так же отметить тот факт, что противодействия различным видам DoS/DDoS-атак являются частью средств и методов информационной безопасности в общем смысле. Поэтому стоит актуальная задача интеграции приведенных выше решений борьбы с DoS-атаками в уже известные методы защиты информации, к DoS-атакам не относящиеся.

Таким образом, хочется получить серебряную пулю, которая сможет поразить не только все компьютеры-зомби, но ликвидировать эксплойты, флуд и прочую нечисть.

Частные подходы слишком ресурсозатратны и в силу огромного разнообразия DoS-атак, не обеспечивают систему полноценной защитой. Но правильная классификация — это первый шаг к созданию комплексного расширяемого аппарата, способного детектировать, принимать необходимые меры в начале атак и, в некоторых случаях, полностью защищать систему от них. Также стоит учитывать тот факт, что за последнее время увеличилась мощность DoS-атак, а вместе с этим увеличились и затраты на ее реализацию. Поэтому, не имея 100 % защиты от них, но основываясь на существующей классификации DoS-атак можно выстроить защиту своей системы так, что данные атаки стали бы просто экономически невыгодными. Для этого, по мере возможности, на вооружении надо иметь все известные способы защиты системы от атак.

СПИСОК ЛИТЕРАТУРЫ:

1. Qrator Labs отмечает массовое распространение инструментов для DDoS. //БИТ [Электронный ресурс]. URL: http://bit.samag.ru/news/more/917(дата обращения: 15.04.2015).
2. *J. Yuan, K. Mills.* Monitoring the Macroscopic Effect of DDoS Flooding Attacks. IEEE Transactions on dependable and secure computing., Senior Member, IEEE. M., 2005–12 p.
3. *C. Douligeris, A. Mitrokotsa.* DDoS Attacks and defense mechanisms: a classification. P., 2003–24 p.
4. KasperskyLab. «Лаборатория Касперского» отразила одну из мощнейших в истории Рунета DDoS-атак. [Электронный ресурс].http://www.kaspersky.ru/news?id=207733980 (датаобращения: 16.04.2015).
5. *N. Quinn.* In Flawed, Epic Anonymous Book, the Abyss Gazes Back. N. Y. Wired. 2012–3 p.
6. *N. Perlroth.* GoDaddy Goes Down, and a Hacker Takes Credit. // Bits. 2012.
7. *M. Prince.* The DDoS That Knocked Spamhaus Offline (And How We Mitigated It). // CloudFlare blog.
8. *M. J. Hashmi, M. Saxena, Dr. R. Saini.* Classification of DDoS Attacks and their Defense Techniques using Intrusion Prevention System. Research Scholar, Singhania University, Pacheri Bari, Jhujhunu, R. 2013. — 8 p.

ИСПОЛЬЗОВАНИЕ МИКРОКОМПЬЮТЕРОВ В ЗАЩИЩЁННЫХ СИСТЕМАХ

А.В. ИВАНОВ
Московский физико-технический институт (ГУ)

В статье приводятся общие требования к работе с удалённой инфраструктурой, особенностях микрокомпьютеров, и практическая программно-аппаратная реализация требований в виде готовых устройств.

Ключевые слова: дистанционное банковское обслуживание, ДБО, облачная инфраструктура, удалённая инфраструктура, микрокомпьютер, доверенная среда, доверенная загрузка, МКTrusT, MeeGoPad.

Введение

Тема данного доклада — защищённые компьютеры и их применение в областях деятельности, требующих высоких уровней защищённости, таких как дистанционное банковское обслуживание (ДБО) или предоставление услуг удалённых (облачных) сервисов.

Работа с удалённым ресурсом предполагает три составляющие: клиент, канал связи и сервер. Сервер находится на стороне банка или компании, и в столь серьёзном деле, как, например, работа с деньгами, сервер качественно защищён. Чего нельзя сказать о канале и клиенте. В качестве каналов связи выступают открытые сетевые каналы (например сеть интернет), которые совершенно не защищёны, если для этого не предпринято каких-нибудь специальных мер. А пользователь, не являясь специалистом в области защиты информации не умеет, и даже не знает, что и от чего защищать. Как правило, пользователи пользуются антивирусами и более ничем.

Для того чтобы обеспечить защиту клиента и канала, чтобы получить уверенность в гарантированной безопасности, необходимо обеспечить доверенную среду, то есть изолированную среду, в которой обеспечено доверие ко всем компонентам. Фактически доверенная среда обеспечивается доверенной загрузкой и средствами разграничения доступа с динамическим контролем целостности.

Для этого можно обеспечивать полноценную защиту. То есть компьютер с аппаратным модулем доверенной загрузки[1] (например ПАК СЗИ НСД «Аккорд-АМДЗ») [1]. В операционную систему устанавливается антивирус и межсетевой экран. Канал защищается благодаря установленному в операционной системе VPN. Благодаря такой защите пользователь получает доверенную среду.

Второй вариант защиты состоит в использовании пользователями токенов с ключами ЭЦП и сертификатами. При работе клиента с удалённым сервисом идёт сравнение сертификатов на токене и на сайтах, к которым пользователь обращается. Дополнительными уровнями защиты являются электронная цифровая подпись запросов пользователя и введение пин-кода устройства. Предполагается, что если злоумышленник не подменил токен, а программно изменить данные он там не может, то пользователь защищён. Канал связи в этом случае не защищается.

Проблема такова: полноценная защита дорога, усечённая — неэффективна [3–4].

Усечённая защита не спасает от попадания на фишинговые сайты, от атак типа «человек посередине». Даже если сообщается, что сайт подозрительный, пользователь может

[1] Доверенная загрузка — это загрузка операционных систем только с заранее определенных постоянных носителей (например, только с жесткого диска) после успешного завершения специальных процедур: проверки целостности технических и программных средств ПК (с использованием механизма пошагового контроля целостности) и аппаратной идентификации/аутентификации пользователя [2].

этого не понять и продолжить работу. Один из возможных примеров — игнорирование пользователем сообщений браузера «сертификат не действителен» и продолжение работы с подозрительным сайтом.

Усечённая защита не обеспечивает доверенную среду. А если её нет, то сообщение о неверном сертификате даже не будет показываться — троян скроет окошко с сообщением и сам нажмёт кнопку «Ок». Или даже подменит браузер.

Таким образом усечённая защита даёт лишь видимость защиты, что ещё более пагубно для пользователей, давая ложную уверенность и снижая бдительность.

Задача — сделать информационное взаимодействие клиента и инфраструктуры безопасным, удобным и при этом недорогим [5–6].

Решением могут стать микрокомпьютеры (МК). Если неизменность операционной системы обеспечивается аппаратным, физическим способом, то никакие программные действия хакеров не смогут изменить целостность, а, следовательно, доверенность программной среды. При первоначальной подготовке такого МК к работе, операционную систему необходимо записать в банк памяти, после чего аппаратно запретить запись, перевести эту область памяти в режим Read Only с физического переключателя. Однако доступ к переключателю должен быть только у специалистов на аттестованном производстве, и пользователю переключение должно быть недоступно.

Межсетевой экран встраивается в ОС. Канал будет защищаться с помощью встроенного VPN. При наличии неизменяемого образа ОС антивирус фактически не нужен. В худшем случае, система будет поражена на один сеанс, до перезагрузки.

С использованием такого устройства можно защитить и клиентскую часть клиент-серверной структуры, и канал связи.

На рынке представлен целый ряд устройств, в той или иной мере подходящих для решения поставленной задачи. Рассмотрим их основные особенности.

Архитектура

Многие МК построены на альтернативной «гарвардской» архитектуре, получившей название ARM, а не на распространённой «фон-неймановской» x86. ARM — это архитектура, на основании которой построено множество разных процессоров. У них может быть совершенно разная периферия, разные методы взаимодействия с периферией, разная частота и энергопотребление, но объединяет их одно — процессорное ядро ARM.

ARM, с одной стороны, проще по сравнению с x86, и имеет большую производительность и меньшее энергопотребление. С другой стороны — меньший набор команд и тот факт, что длина команды фиксирована, приводит к увеличению объема программ. Достоинством архитектуры является расширение безопасности TrustZone Technology, находящееся в ARMv6KZ и других, более поздних архитектурах, обеспечивающее низкозатратную альтернативу добавлению специального ядра безопасности, создавая 2 виртуальных процессора, поддерживаемых аппаратным контролем доступа. Это позволяет ядру приложения переключаться между двумя состояниями, называемыми «миры», чтобы не допустить утечку информации из более важного мира в менее важный.

Типичные приложения TrustZone Technology должны запускать полноценную операционную систему в менее важном мире, и компактный, специализированный на безопасности, код в более важном мире, тем самым усиливая защищённость устройства.

Кроме того, под архитектуру ARM написано на порядок меньше вирусов.

Драйвера и ПО

На данный момент существует серьёзный недостаток ARM. Программного обеспечения, в том числе и операционных систем, быстро и стабильно работающего на ARM крайне мало. В перечень операционных систем, поддерживающих архитектуру ARM, входит крайне ограниченный набор Linux (и сами системы урезанные) под конкретные линейки процессоров, Windows Runtime и, возможно, Windows 10 (когда Microsoft выполнит своё обещание и выпустит специальную версию системы).

Проблемы возникают, например, при подключении периферии, при попытке использовать веб-камеру и передавать звук по скайпу, сложности возникают при любом запросе, выходящем за рамки ПО, находящегося в системе «по умолчанию».

Так, на добавление чего-то нового в операционной системе Windows разработчиком затрачивается 5 минут, в случае Linux — день, а в случае специализированного Linux под малораспространённую архитектуру ARM — нет гарантии, что заработает.

Кроме того, в Linux под ARM база драйверов для мультимедиа пока что мала.

Защищённые операционные системы

Удобно иметь на борту МК две операционных системы — защищённую для работы с важной информацией и незащищённую для всего остального. Хорошо бы заставить пользователя переключаться между ними, разрешив в защищённой системе только минимально необходимый функционал. Потому что работа с важной информацией и открытые вкладки с развлекательными порталами — вещь несовместимая. Имея возможность зайти на развлекательный сайт с подозрительным контентом, рано или поздно пользователь заглянет туда отдохнуть и отвлечься. И, скорее всего, нахватает вирусов. Нужно иметь возможность отключать периферию, сеть (как беспроводную, так и проводную), прописывать сайты, на которые разрешён доступ. В случае, если требуется более тонкая настройка политики безопасности, нужно предусмотреть возможность изменения настроек «на лету», потому что образ системы неизменяемы. Например, хранить их на SD-карте и подгружать подписанный файл с ними как часть системы.

А переключение между ОС сделать аналоговым переключателем и вывести индикацию, к примеру, выбрать тревожный красный цвет светодиода для информирования о том, что работа идёт в защищённой системе.

Надёжный способ сделать образ ОС неизменяемым — записать систему и после этого сделать эту область диска Read Only, получив операционную систему, гарантированно защищённую от несанкционированных воздействий. Чтобы не произошло, МК можно перезагрузить и вновь работать в неповреждённой системе. Запрет записи можно реализовать как программно, так и аппаратно, но аналоговая безопасность лучше цифровой. Если осуществляется программная защита, например, политики разграничения доступа (администратор/обычный пользователь) в системах Windows, то вирус, сломавший подконтрольное ПО, также сможет обойти систему слежения за последним. Переключение аппаратного рычажка вирусам неподвластно.

В случае Flash-памяти это делается относительно тривиально. Для этого одна из ножек микроконтроллера замыкается с землёй и делается аппаратный переключатель внутри устройства.В случае более сложной памяти, например EMMC, задача сразу же усложняется. Можно попробовать расшифровывать и блокировать команды на запись. Или сообщить ридеру, что запись не разрешена. Последний вариант основан на том, что на карточках памяти есть «шторка», в одном из положений запись разрешена, в другом

запрещена и ридер это понимает. Для более громоздких накопителей типа HDD/SSD существуют отдельные устройства-блокираторы. Но что касается именно микрокомпьютеров, наиболее адекватно и надёжно защищается только Flash.

Что имеем

На рынке представлены HDMI-стики, которые идеально подходят к поставленным требованиям по размеру и функционалу. Действительно, их можно подключить к телевизору или монитору, получив в результате полноценный компьютер, а их мобильность позволяет пользоваться ими в поездках.

Хотелось бы выбрать из всего ассортимента HDMI-стиков такое устройство, которое обладало бы максимумом достоинств и имело бы минимум недостатков. Это нетривиальная задача, универсального решения для которой не существует. Крайне важны защищённость устройства и его функциональные возможности. В свою очередь, защищенность напрямую зависит от типа памяти, и наилучшим решением является Flash-модуль. Также хотелось бы обеспечить доверенную среду. Операционная система, в свою очередь, должна поддерживать предпочитаемое программное обеспечение, желательно, в наиболее широком ассортименте. На данном этапе ОС Windows обладает много более широкой базой драйверов и ПО. Получается, что несмотря на лучшие показатели архитектуры ARM, на данный момент большими возможностями обладает x86, следовательно охватывает больше задач и большую аудиторию пользователей. Необходимо предоставить администраторам и специалистам ИБ возможность тонкой настройки устройства, включая его политику безопасности. Также должен быть защищен канал связи. Нельзя забывать и о цене.

Таким образом обозначены следующие характеристики:

1. Архитектура
2. Тип памяти
3. Доверенная среда
4. Операционные системы
5. Настройка политики безопасности
6. Цена

Посмотрим, какие из представленных на рынке устройств на рынке наиболее подходит под такое описание.

Первое из них — МКTrusT. Микрокомпьютер «гарвардской» архитектуры, позволяющий работать в двух режимах — защищенном (Linux в режиме ReadOnly) или незащищенном (Android в режиме ReadWrite) без ограничения возможностей. Влияние операционных систем друг на друга исключается технологически благодаря независимым банкам памяти, один из которых аппаратно защищён от записи. Это обеспечивает сохранение доверенности защищённой ОС — у систем нет общего информационного ресурса. Переключение между операционными системами аппаратное с помощью внешнего переключателя. Неизменяемый образ операционной системы обеспечивает доверенную загрузку. Производится индикация режимов красным и зелёным свечением светодиода. В записываемом образе ОС Linux заранее определяются такие параметры, как разрешённые сайты, возможность пользоваться проводной/беспроводной связью, разрешённая периферия, права пользователя и др. Впрочем, есть возможность обновления «на лету» — подгрузить как часть системы подписанный файл с настройками с SD-карты. Канал связи защищён встроенным VPN [7].

Микрокомпьютер снабжён программным обеспечением клиента системы разграничения доступа «Аккорд-ТК», что обеспечивает ещё большую гибкость настройки политик безопасности пользователей при работе с удалённой инфраструктурой.

MKTrusT соответствует 11 из 15 требований, описанных в 21м приказе ФСТЭК [8]. Решение защищено аппаратными способами, описанными в патентах [9–10]. Цена — 15 тысяч рублей.

Однако, MKTrusT ограничен архитектурой процессора. Устройство обладает как всеми достоинствами, так и недостатками ARM, например, возникают проблемы с ПО, в частности, с работой виртуальных машин. В Horizon View не работает Real-Time Audio-Video (RTAV) — веб-камеры и микрофоны. Заявлено, что в системах виртуализации Citrix таких проблем нет, но как показывает практика — микрофон или звук от виртуальной машины не работают, весь лог завален ошибками. Во всём остальном — идеальный выбор.

Второе — микрокомпьютер MeeGoPad T01. Основное преимущество — архитектура x86 и операционная система Windows 8.1 with Bing (производитель не платит за лицензию Microsoft — это даёт возможность делать устройство дешевле). Компьютер тоже поддерживает режим dual-boot, дополнительно можно поставить Android или Linux. При тестировании этого устройства было проверено, что клиенты Citrix Receiver и VMware Horizon View для удаленных рабочих столов прекрасно работают «из коробки» конкретно под Windows. Был проведён эксперимент, показавший, что в виртуальной машине прекрасно работает веб-камера и звук по скайпу. MeeGoPad поддерживает всё необходимое ПО сразу «из коробки». Поддерживается VPN. Доверенная среда не обеспечивается, а политики безопасности определяются исключительно возможностями установленной ОС. MeeGoPad соответствует 8 из 15 требований, описанных в 21м приказе ФСТЭК [7]. Цена — чуть больше 7 тысяч.

Главная проблема MeeGoPad заключается в типе памяти. Если не обеспечить аппаратный запрет на запись или не обеспечить другой способ обеспечения доверенной среды — гарантировать безопасность невозможно. Существуют пути решения данной проблемы. Например установить в МК программно-аппаратный модуль доверенной загрузки. Или заказать линейку устройств, где вместо памяти EMMC будет стоять Flash, которая будет защищаться по проверенной схеме. Смена типа памяти видится наиболее простым и дешёвым решением.

Заменив память, получим мощный защищённый компьютер на архитектуре x86 с Windows на борту, готовым пакетом драйверов и ПО. Таким образом, он совместит в себе большинство вышеописанных достоинств, тем самым приблизившись к идеальному защищённому устройству для работы с удалёнными инфраструктурами и ДБО.

Сводная таблица

	Архитектура	Тип памяти	Доверенная среда	ОС	Настройка политики безопасности	Цена
MKTrusT	Гарвардская ARM	Flash. Защищена.	Обеспечивается физической неизменностью образа ОС и независимыми банками памяти.	Защищённый Linux и незащищённый Android.	Средствами ОС + ПО системы разграничения доступа Аккорд-ТК.	15000
MeeGo-Pad T01	Фон Неймана x86	EMMC. Не защищена. Можно выпустить устройства с другим типом памяти.	Не обеспечивается. К примеру, можно поставить Flash или аппаратный модуль доверенной загрузки.	Незащищённый Windows 8.1, незащищённый Android или Linux.	Средствами ОС.	7000

Итого

Получается, что устройства, целиком подходящего под все описанные требования, не существует. Однако имеются очень близкие по характеристикам.

При работе с удалённой инфраструктурой зачастую предлагаются ненадёжные, урезанные решения для имитации защиты и успокоения клиента. Микрокомпьютеры являются наиболее приемлемым способом защитить клиента и канал передачи данных «по-честному».

Несмотря на муки выбора между достоинствами и недостатками тех или иных устройств, краеугольным камнем является возможность аппаратной защиты памяти от записи. И вопрос защиты типов памяти помимо Flash остаётся открытым.

Перспективность ARM устройств возрастает, но их взлёт произойдет не раньше, чем через пару лет, когда будет создана необходимая программная база драйверов и программного обеспечения, а также библиотек для их создания. Тем не менее, достоинства этих устройств неоспоримы, их выгодно использовать, а в случаях, требующих RTAV — пользоваться архитектурой x86.

Возможно, грандиозный прорыв случиться раньше, когда выйдет Windows 10 под ARM-архитектуру, выход которой намечен на конец этого года.

СПИСОК ЛИТЕРАТУРЫ

1. Каннер (Борисова) Т. М., Романенко Н. В. Аккорд-АМДЗ: Next Generation.// Комплексная защита информации. Безопасность информационных технологий. Материалы XVII Международной конференции 15–18 мая 2012 года, Суздаль (Россия). 2012. С. 57–58.
2. *Бажитов И. А.* Обеспечение доверенной среды в ОС Linux с использованием ПАК СЗИ НСД «Аккорд-X» // Комплексная защита информации. Материалы XV международной научно-практической конфереции (Иркутск (Россия), 1–4 июня 2010 г.). М., 2010. С. 32.
3. *Конявский В. А.* Прогноз развития Российского сегмента сети Интернет до 2010 года // Управление защитой информации. 2003. Т. 7. № 3.
4. *Конявский В. А., Поспелов А. Л.* Национальный оператор идентификации, или как повысить доверие клиентов к ДБО и понизить риски // Национальный банковский журнал. М., 2013. № 2 (105). С. 86–87.
5. *Конявский В. А., Ухлинов Л. М.* Практика обеспечения безопасности дистанционного банковского обслуживания // Вопросы защиты информации. 2012. № 3. С. 58–61.
6. *Конявский В. А.* Минимизация рисков участников дистанционного банковского обслуживания // Вопросы защиты информации. 2014. № 4 (107). С. 3–4.
7. *Конявский В. А.* Защищённый микрокомпьютер МКTrusT — новое решение для ДБО // Национальный банковский журнал. М., 2014. № 3 (март). С. 105.
8. Приказ № 21 ФСТЭК России от 18 февраля 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
9. Компьютер типа «тонкий клиент» с аппаратной защитой данных. Патент на полезную модель № 118773. 27.07.12, бюл. № 21.
10. Мобильный компьютер с аппаратной защитой доверенной операционной системы. Патент на полезную модель № 138562. 20.03.2014, бюл. № 8.

ОПРЕДЕЛЕНИЕ ВЕРОЯТНОСТИ РЕАЛИЗАЦИИ УГРОЗЫ ЗА СЧЕТ ИСПОЛЬЗОВАНИЯ ДАННЫХ ОБ ИНЦИДЕНТАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

М.А. ИОФФЕ, Р.А. НУРДИНОВ

Краткое вступление, постановка проблемы

На сегодняшний день количественная оценка вероятности реализации угрозы весьма затруднена ввиду отсутствия четких требований к составу исходных данных, правил оценки (математической модели), достаточного количества и правил обработки статистических данных [1].

Научная задача исследования заключается в разработке научно-обоснованной формализованной модели количественной оценки вероятности реализации угроз безопасности информационной системы.

Базовые положения исследования

Оценка вероятности реализации угрозы за определенный период времени является задачей прогнозирования. Как известно из литературы, всё многообразие методов прогнозирования можно разделить на экспертные (интуитивные) и формализованные [2].

На практике, чаще всего, вероятность реализации угрозы определяется экспертными методами, что вызывает скептическое отношение к таким оценкам ряда специалистов, ориентированных на практические задачи [1]. Это обусловлено существенными недостатками экспертных методов оценки, такими как субъективность, высокая степень неопределенности, невозможность динамической переоценки.

Формализованные методы прогнозирования, в свою очередь, подразделяются на:

- статистические методы (корреляционный, регрессионный, факторный анализ и т.д.);
- структурные методы (нейронные сети, сети Петри, цепи Маркова и т.д.);
- методы моделирования (имитационное, сетевое, матричное и т.д.).

Для компенсирования недостатков одних методов при помощи других в работе предлагается использовать комбинированный подход к оценке вероятности реализации угрозы, включающий две последовательные взаимосвязанные процедуры:

- определение метрик оценки вероятности реализации угроз и начальных значений их весовых коэффициентов;
- разработка методики обучения модели на основе данных об инцидентах информационной безопасности.

Результаты

Функция вероятности реализации угрозы задана в работе как произведение степени опасности нарушителя и степени реализации защитных мер, направленных на предотвращение данной угрозы, вычтенной из единицы. Степень опасности нарушителя принимает значение в интервале от 0 до 1, определяемое средневзвешенным геометрическим значений следующих метрик нарушителя: мотивация, затрачиваемое время, компетентность, информированность, права доступа, техническая оснащенность [2]. Степень реализации защитных мер также принимает значения в интервале от 0 до 1, и определяется средневзвешенным геометрическим значений метрик защитных мер, сформированных на основании Приказа ФСТЭК России № 17 [3].

Начальная оценка весовых коэффициентов метрик произведена с использованием метода парных сравнений группой экспертов из 12 человек по шкале, предложенной

Т. Саати [4]. Полученные в результате обработки матриц парных сравнений векторы весовых коэффициентов метрик были усреднены, и нормированы к 1.

Также в работе предложена методика динамического обучения предложенной модели. Процесс обучения заключается в корректировке весовых коэффициентов метрик на основании данных о реализованных или предотвращенных угрозах с применением метода обратного распространения ошибки в последовательном режиме.

Применение метода обратного распространения ошибки для аппроксимации функции вероятности реализации угрозы обусловлено рядом преимуществ, среди которых стоит выделить нетребовательность к входным данным и возможность исключения из модели незначимых и добавления новых метрик в процессе обучения

Проведен ряд экспериментов, подтверждающих достоверность и результативность предлагаемых модели и методики её обучения.

Эксперимент

Целью обучения стало выполнение аппроксимации функции вероятности взлома удаленным нарушителем со степенью опасности d=0.5. Целевые значения весовых коэффициентов определены в результате анализа открытых баз инцидентов ИБ (OWASP, HACKMAGEDDON) и аналитических отчетов компаний Positive Technologies, Лаборатория Касперского и других. Объекты обучающей выборки сгенерированы на основании целевых значений весов и пороговой функции вывода. Эксперименты проводились на обучающей выборке из 1000 инцидентов. Результаты усреднялись по 1000 циклам. По результатам проведённого анализа для корректировки весовых коэффициентов в режиме последовательного обучения в ходе экспериментов целесообразно рассмотреть использование следующих методов, применение которых возможно в методе обратного распространения ошибки:

- метод градиентного спуска с адаптивным темпом обучения;
- с фиксированным
- с моментом

Проведение экспериментального исследования по обучению модели проводилось для решения следующих задач:

- сравнение нескольких методов обучения и выбор наиболее подходящего из них;
- определение результативности обучения модели (изменение величины ошибки в зависимости от объема обучающей выборки);
- определение наиболее подходящих значений параметров обучения модели и правил их изменения;

На первом этапе аппроксимация функции защищенности на основе статистики инцидентов осуществлялась методом градиентного спуска, лежащим в основе классического метода обратного распространения ошибки.

Чем больше темп обучения, тем стремительнее меняются весовые коэффициенты. Так, при темпе обучения равным 0,07 на 100-м шаге обучения удалось снизить ошибку до 0,0483. На 1000-м шаге обучения лучший результат, полученный при темпе обучения равным 0,02, составил 0,0136 (рисунок 1).

При использовании метода градиентного спуска с адаптивным темпом обучения и с моментом равным 0,5 удается снизить среднюю ошибку до 0.027 за 100 обучающих примеров и до 0.005 за 1000 обучающих примеров.

Таким образом, наилучший результат аппроксимации функции защищенности был достигнут при использовании метода градиентного спуска с адаптивным темпом обучения t и с моментом равным 0,5.

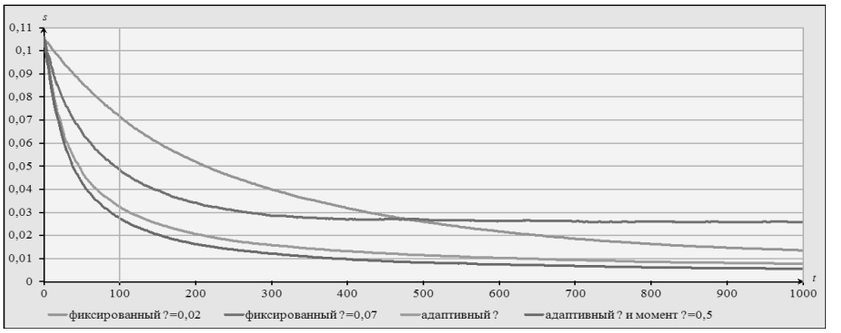


Рис. 1. Результаты обучения модели

Практические результаты

Основные выводы:

- количественная оценка затруднена из-за отсутствия четких требований к составу исходных данных, правил оценки и правил обработки статистических данных;
- существующие методы обладают рядом существенных недостатков, ограничивающих их практическую применимость, точность результатов и возможность оперативного реагирования на изменения области оценки.

Преимущества предложенного метода:

- высокая точность результатов оценки (при выборке из 100 инцидентов средняя ошибка менее 3 %, при выборке из 1000 инцидентов — менее 1 %);
- высокая гибкость (возможность обучения не неполных данных);
- возможность реагирования на изменения области оценки за счет динамического обучения в последовательном режиме;
- значительное сокращение роли и объема работы экспертов.

Полученные в ходе исследования результаты использованы при создании программного модуля оценки рисков на платформе RSA Archer eGRC.

Из преимуществ разработанного модуля следует выделить то, что его использование позволяет существенно сократить роль и объём работы экспертов при оценке рисков и, прежде всего, вероятности реализации угроз, а также возможность осуществлять динамическую переоценку и обучение при изменении входных данных и, таким образом, оперативно реагировать на изменения окружающей среды.

ЛИТЕРАТУРА

1. *Вихров Н. М., Ныркov А. П., Каторин Ю. Ф., Шнуренко А. А., Башмаков А. В., Соколов С. С., Нурдинов Р. А.*. Анализ информационных рисков // Морской вестник. 2015. № 3. С. 81–85.
2. ГОСТ Р ИСО/МЭК 18045–2013 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий.
3. Приказ ФСТЭК от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
4. *Саати Т. Л.* Принятие решений: Метод анализа иерархий: пер. с англ. / Т. Л. Саати; Переводчик Р. Г. Вачнадзе. — М.: Радио и связь, 1993 . — 314 с.

КОММУТАТОР USB-КАНАЛА КАК ТЕХНИЧЕСКОЕ СРЕДСТВО ДЛЯ ТЕСТИРОВАНИЯ ПРОГРАММНО-АППАРАТНЫХ СЗИ

Т.М. КАННЕР
ЗАО «ОКБ САПР»

В статье рассматривается назначение, состав и принцип функционирования коммутатора USB-канала, применяемого для автоматизированного тестирования «мобильных» программно-аппаратных средств защиты информации, функционирующих в операционной системе средств вычислительной техники и имеющих USB-интерфейс подключения. Обоснована необходимость эмуляции автоматизированного физического отключения и подключения СЗИ к определенному интерфейсу СВТ с помощью технического (программно-аппаратного), а не программного средства.

Ключевые слова: автоматизированное тестирование, «мобильные» программно-аппаратные СЗИ, коммутатор USB-канала.

В настоящее время информационные системы создаются и развиваются очень быстро за счет использования эффективных инструментальных средств, в связи с этим необходимо максимально сократить время, затрачиваемое на разработку СЗИ, выделив этапы, которые можно полностью автоматизировать или автоматизировать при определенных условиях. К таким этапам относятся тестирование, верификация и исправление найденных ошибок. Эти этапы неоднократно повторяются в процессе разработки СЗИ. Сокращения временных затрат на разработку СЗИ можно достичь за счет автоматизации процесса тестирования.

Для программных СЗИ существует большое количество разнообразных средств автоматизации тестирования [1], применение которых может быть затруднено для программно-аппаратных СЗИ из-за наличия аппаратного компонента и особенностей его функционирования [2–4].

Аппаратный компонент может быть «мобильным» — отчуждаемым от средства вычислительной техники (СВТ) в течение эксплуатации программно-аппаратного СЗИ. В этом случае при проведении тестирования СЗИ его иногда необходимо переподключать к СВТ, то есть физически отключать, затем подключать к соответствующему интерфейсу. Автоматизировать процесс тестирования таких СЗИ затруднительно без использования дополнительного технического средства, учитывающего особенности функционирования аппаратной компоненты СЗИ [5]. Такое техническое средство должно эмулировать физическое отключение и подключение СЗИ к определенному интерфейсу СВТ автоматизированным способом.

Сэмулировать подключение/переподключение СЗИ к СВТ также можно с помощью программных средств (с использованием BIOS, настройкой конкретной операционной системы (ОС)). Однако при этом такое подключение/переподключение может не полностью эмулировать физическое отключение (например, может не происходить отключение питания), что делает невозможным использование таких программных средств для тестирования «мобильных» программно-аппаратных СЗИ, функционирующих в среде ОС СВТ. Кроме того, такие программные средства могут быть неуниверсальными для различных версий ОС, BIOS и так далее. В связи с этим для подключения/переподключения к СВТ «мобильных» программно-аппаратных СЗИ, функционирующих в среде

ОС, целесообразно применять именно технические, а не программные средства. Проведенный анализ открытых источников показал, что технических средств тестирования, реализующих возможность эмуляции физического подключения/отключения СЗИ к СВТ на рынке не представлено, поэтому такое средство требуется разработать.

При разработке технического средства тестирования необходимо учитывать тип интерфейса подключения «мобильного» СЗИ к СВТ, при этом принцип работы для различных интерфейсов должен быть единообразен. Также техническое средство тестирования, реализованное для одного из типов интерфейса, должно быть применимо для различных СЗИ, использующих этот интерфейс для подключения к СВТ.

В соответствии с изложенными принципами в ОКБ САПР был разработан так называемый коммутатор USB-канала (внешний вид изображен на Рис. 1), предназначенный для автоматизации тестирования «мобильных» СЗИ, подключаемых к USB-интерфейсу СВТ.

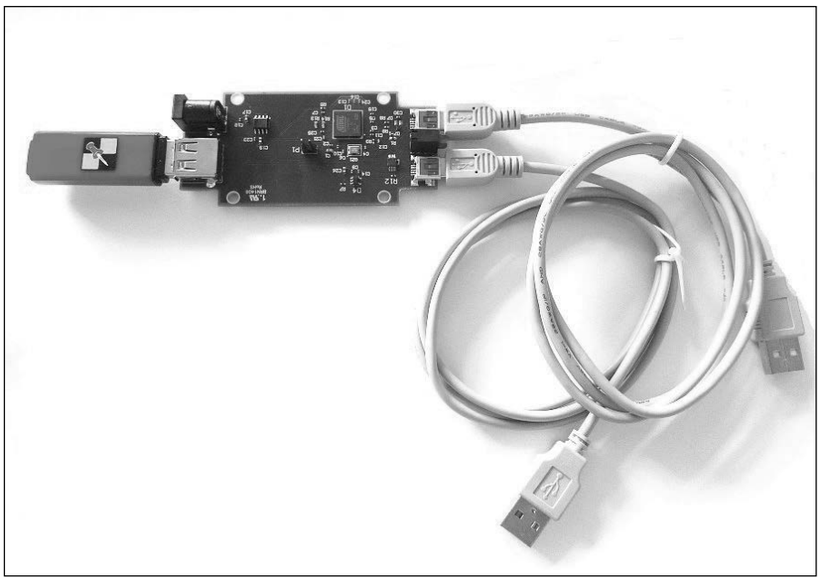


Рис. 1. Коммутатор USB-канала с подключенным коммутируемым СЗИ — ПСКЗИ ШИПКА

Данный программно-аппаратный комплекс представляет собой:

- техническое средство, устанавливаемое между USB-интерфейсом СВТ и СЗИ «в разрыв» USB-канала, и осуществляющее его коммутацию в соответствии с командами, поступающими по каналу управления;
- программное обеспечение, позволяющее программно из ОС СВТ подать соответствующую команду по каналу управления (включить или отключить передачу данных и питание для коммутируемого USB-устройства).

Такое техническое средство способно физически прерывать питание различных подключаемых к нему USB-устройств (например, ПСКЗИ ШИПКА и СН «Секрет» производства ОКБ САПР [6, 7]) без их физического отключения/переподключения.

Коммутатор USB-канала предназначен для выполнения следующих функций:

1. управляемое переподключение USB-устройств в процессе их автоматизированного тестирования (то есть коммутатор USB-канала используется как техническое средство тестирования);

2. управляемая блокировка доступа к USB-каналу (коммутатор USB-канала — как компонент СЗИ, реализующий блокировку запрещенных USB-устройств и позволяющий осуществлять доступ к разрешенным USB-устройствам).

Функционально коммутатор USB-канала состоит из следующих компонентов:

– аппаратный компонент с внутренним ПО (firmware), запускающимся при поступлении питания и выполняющим основной функционал программно-аппаратного комплекса;
– программный компонент (внешнее ПО), состоящий из:
  библиотеки для встраивания и использования комплекса в стороннем ПО;
  утилиты командной строки для выполнения коммутации USB-устройств (с использованием библиотеки).

Коммутация USB-канала обеспечивается синхронным включением и выключением мультиплексора линий данных и питания. Команды между внешним и внутренним ПО передаются путем обмена сообщениями специального формата по управляющему каналу данных.

С использованием библиотеки для встраивания комплекса в стороннее ПО или работающей на ее основе утилиты командной строки можно подать следующие команды аппаратному компоненту:

– включить передачу данных и питание;
– отключить передачу данных и питание;
– запросить состояние коммутации.

Программный интерфейс коммутатора USB-канала предоставляет следующий набор функций:

– *std:: list<std:: string> US_Enumerate();*
– *std:: string US_ON(std:: string usbSwitcher);*
– *std:: string US_OFF(std:: string usbSwitcher).*

Где:

– usbSwitcher — строка (из списка, возвращаемого US_Enumerate()), идентифицирующая коммутатор USB-канала, которому передается команда (вида «OKB SAPR USB Switcher X», где X — номер подключенного к СВТ коммутатора, начиная с «0»);
– US_Enumerate — функция, осуществляющая поиск и вывод списка найденных и доступных в данный момент коммутаторов USB-канала (либо пустой список — в случае отсутствия подключенных к СВТ коммутаторов);
– US_ON — функция, передающая команду на включение передачи данных и питания устройств, подключенных к коммутатору USB-канала (в случае корректного завершения работы возвращает «SUCCESS», иначе — генерируется исключение типа std: string с подробным описанием ошибки);
– US_OFF — функция, передающая команду на отключение передачи данных и питания устройств, подключенных к коммутатору USB-канала (в случае корректного завершения работы возвращает «SUCCESS», иначе — генерируется исключение типа std: string с подробным описанием ошибки).

При использовании коммутатора USB-канала с помощью утилиты командной строки (USBSwitcherConsole.exe) необходимо передавать на вход следующие параметры:

– list — для вывода списка доступных коммутаторов USB-канала (то есть реализуется выполнение функции US_Enumerate из библиотеки встраивания и использования комплекса в стороннем ПО);
– on <switcherName> — для включения передачи данных и питания устройств, подключенных к соответствующему коммутатору (то есть реализуется выполнение

функции US_ON из библиотеки встраивания и использования комплекса в сторонем ПО). Без указания <switcherName> команда отправляется на первый доступный коммутатор;

– off <switcherName> — для отключения передачи данных и питания устройств, подключенных к соответствующему коммутатору (то есть реализуется выполнение функции US_OFF из библиотеки встраивания и использования комплекса в сторонем ПО). Без указания <switcherName> команда отправляется на первый доступный коммутатор.

Пример работы утилиты командной строки (USBSwitcherConsole.exe), а именно — вывод списка доступных коммутаторов, включение и отключение передачи данных и питания, изображен на рис. 2.

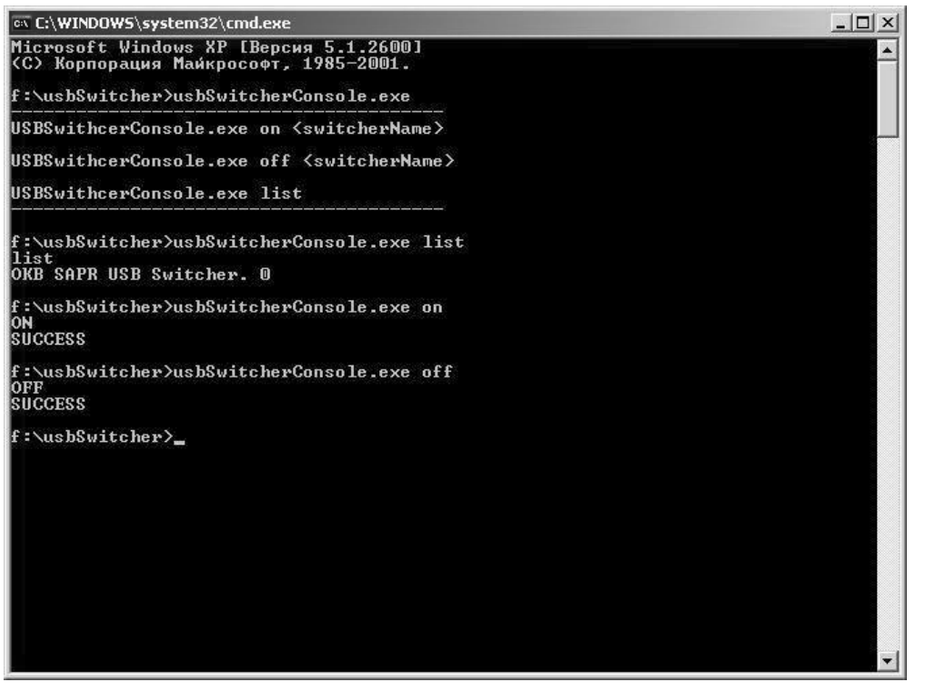


Рис. 2. Пример работы утилиты командной строки коммутатора USB-канала

Таким образом, разработанный программно-аппаратный комплекс при вызове описанных команд по управляемой коммутации СЗИ полностью эмулирует его физическое отключение и подключение к СВТ как на уровне питания, так и на уровне канала передачи данных. Коммутатор USB-канала можно использовать для автоматизации тестирования «мобильных» программно-аппаратных СЗИ, функционирующих в среде ОС СВТ, и имеющих USB-интерфейс подключения, например, таких, как ПСКЗИ ШИПКА и ПАК «Секрет».

СПИСОК ЛИТЕРАТУРЫ

1. *Каннер Т. М., Обломова А. И.* О выборе инструмента автоматизации тестирования для программно-аппаратных СЗИ // Вопросы защиты информации. Научно-практический журнал, М., 2014. № 4. С. 34–36

2. *Каннер (Борисова) Т. М., Кузнецов А. В.* Проблемы тестирования СЗИ, функционирующих до старта ОС // Комплексная защита информации. Электроника инфо. Материалы XVIII Международной конференции 21–24 мая 2013 года, Брест (Республика Беларусь). 2013. С. 114–115
3. *Каннер (Борисова) Т. М., Обломова А. И.* Способы автоматизации тестирования СЗИ, функционирующих в ОС, на примере ПСКЗИ ШИПКА // Комплексная защита информации. Электроника инфо. Материалы Электроника инфо. Материалы XVIII Международной конференции 21–24 мая 2013 года, Брест (Республика Беларусь). 2013. С. 117–118
4. *Каннер Т. М., Куваева К. А.* Формирование подхода к автоматизации тестирования СЗИ, в конструктив которых входит флеш-память, функционирующих в ОС // Вопросы защиты информации. Научно-практический журнал. М., 2014. № 4. С. 52–54
5. *Каннер Т. М.* Применимость методов тестирования ПО к программно-аппаратным СЗИ // Вопросы защиты информации. М., 2015. № 1. С. 30–39
6. Специальный съемный носитель информации. Патент на полезную модель № 94751. 27.05.2010, бюл. № 15.
7. Мобильное устройство защиты информации. Патент на полезную модель № 83862. 20.06.2009, бюл. № 17.

ПРИМЕНЕНИЕ КРИПТОГРАФИЧЕСКОЙ ОБФУСКАЦИИ ДЛЯ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

А.В. КОЗАЧОК
Академия ФСО России

Обфускацией программы называется всякое ее преобразование, которое сохраняет вычисляемую программой функцию, но при этом придает программе такую форму, что извлечение из текста программного кода ключевой информации об алгоритмах и структурах данных, реализованных в этой программе, становится трудоемкой задачей [1].

В настоящее время исследования в области обфускации программного кода проводятся по двум направлениям: системное программирование; математическая криптография. Наибольший интерес представляет второе направление, в рамках которого была предложена концепция неразличимой обфускации.

С позиции математической криптографии разработка эффективных алгоритмов позволит решить целый ряд серьезных вопросов, например, с ее помощью можно преобразовать криптосистему с секретным ключом к криптосистеме с открытым ключом, проводить вычисления над зашифрованными данными, реализовывать системы функционального шифрования, доверенные схемы перешифрования и электронно-цифровой подписи, создавать верифицируемые системы тайного голосования и схемы двойственного шифрования.

Исследования в области неразличимой обфускации, проводимые в настоящее время, как российскими учеными (Варнавский Н. П., Захаров В. А., Кузюрин Н. Н.), так и зарубежными (S. Garg, C. Gentry, S. Halevi, B. Barak, J. S. Coron, T. Lepoint, M. Tibouchi) базируются на возможности обфускации булевых функций (булевых схем).

Согласно работам [2, 3, 4] процедура неразличимой обфускации включает в себя пять основных этапов.

1. Преобразование булевой функций в вид ветвящейся программы.
2. Преобразование ветвящейся программы в вид матричной ветвящейся программы.
3. Рандомизация матричной ветвящейся программы.
4. Кодирование рандомизированной матричной ветвящейся программы с помощью схемы дифференциального кодирования (Graded Encoding Scheme).
5. Вычисление обфусцированной функции.

В 2001 году впервые строгое математическое определение стойкости обфускации программного кода была предложено Бараком [5]: обфускация считается стойкой, если всякий противник может извлечь из текста обфусцированной программы за разумное (полиномиальное относительно размера входных данных) время не больше информации, чем можно было бы получить, проводя тестовые испытания этой программы как «черного ящика».

Определение. (Обфускация в модели виртуального «черного ящика»). Пусть $\{C_\ell\}_{\ell\in N}$ — класс булевых схем, тогда обфускатором в модели виртуального «черного ящика» для класса схем $\{C_\ell\}_{\ell\in N}$ называется такая (полиномиальная вероятностная машина Тьюринга) PPT O, которая удовлетворяет следующим требованиям:

– функциональная эквивалентность. Для любой схемы $C\in\{C_\ell\}_{\ell\in N}$ и любого входа x существует пренебрежимо малая функция μ, такая что:

$$\Pr[(O(C))(x)\neq C(x)]\le\mu(|C|);$$

– полиномиальные издержки. Существуют полином $poly(\cdot)$ такой, что для любой схемы $C\in\{C_\ell\}_{\ell\in N}$:

$$|O(C)|\le poly(|C|);$$

– свойство виртуального «черного ящика»: для любой PPT A (противника) существуют такая PPT Sim (симулятор) и пренебрежимо малая функция μ такая, что для любой схемы $C\in\{C_\ell\}_{\ell\in N}$:

$$|\Pr[A(O(C))=1]-\Pr[Sim^C(1^{|C|})=1]|\le\mu(|C|).$$

Это означает, что не существует алгоритма распознавания обфускации более эффективного, чем обычное предположение, сделанное на основе анализа входов и выходов обфусцированной программы (функции или обфусцированного набора инструкций).

Неразличимость обфусцированных программ означает, что если две эквивалентные программы (одинакового размера) P_1,P_2, такие, что $\forall x: P_1(x)=P_2(x)$, а $O-$ это обфускатор неразличимости, который принимает на вход программу $P(x)$ и на выходе генерирует новую программу $O(P(x))$, то $iO(P_1(x))$ и $iO(P_2(x))$ будут вычислительно неразличимы:

$$\exists P_1(x),P_2(x).\forall x: P_1(x)=P_2(x)\to iO(P_1(x))\approx iO(P_2(x)).$$

На основе данной конструкции предлагается доказательство о том, что возможно построение неразличимого обфускатора, стойкого в модели виртуального «черного ящика». Обфускатор O принимает в качестве входных данных программу f, представленную в виде булевой функции, и на выходе генерирует обфусцированную программу $O(f)$. Формально, обфускатор неразличимости O можно считать компилятором, принимающим на вход булеву функцию $f(x)$ и генерирующим на выходе обфусцированную программу $f'(x)=O(f(x))$. При этом должно выполняться следующее условие: $\forall x: f'(x)=f(x)$.

Определение стойкости обфускации в модели виртуального «черного ящика» требует, чтобы для любой PPT A (противника) существовал полиномиальный симулятор *Sim*, такой, что для каждой схемы *C*, за полиномиальное время распознаватель *Dist* не может различить результат, вычисленный противником A (A принимает обфусцированную программу *O*(*C*) в качестве входа), от результата, вычисленного симулятором *Sim*, имеющим лишь оракульный доступ к *C*, при этом *Sim* может сделать полиномиальное количество запросов к *C*.

Данная работа посвящена модификации существующих подходов к осуществлению неразличимой обфускации с целью устранения ряда ограничений, обусловленных применяемыми механизмами, моделями и алгоритмами, а также доказательству стойкости предложенного подхода в модели со случайным оракулом.

СПИСОК ЛИТЕРАТУРЫ

1. *Варновский Н. П., Захаров В. А., Кузюрин Н. Н., Шокуров А. А.* Современное состояние исследований в области обфускации программ: определения стойкости обфускации // Труды Института Системного программирования: М.: ИСП РАН, 2014. Т. 26, № 3. С. 167–198.
2. *S. Garg, C. Gentry, S. Halevi.* Candidate multilinear maps from ideal lattices. In Advances in Cryptology — EUROCRYPT, 2013, pp. 1–17.
3. *Pass R., Seth K., Telang S.* Indistinguishability obfuscation from semantically-secure multilinear encodings // In Advances in Cryptology — CRYPTO, 2014. pp. 500–517.
4. *Козачок А. В.* Аналитическая модель защиты файлов документальных форматов от несанкционированного доступа / А. В. Козачок, М. В. Бочков, Р. Р. Фаткиева, Л. М. Туан. // Труды СПИИРАН (Санкт-Петербург), 2015. — Вып. 43. — С. 228–252.

МИФЫ О БИТКОИНАХ

В. В. КРАВЕЦ
ОКБ САПР, МФТИ (ГУ)

Аннотация
В предложенной статье рассматриваются некоторые известные мифы о системе Bitcoin. Для полного понимания необходимо наличие общих знаний о Bitcoin и биткоинах.

Ключевые слова: биткоин, bitcoin

Даже в 2008 году, когда Сатоси Накамото разработал протокол и принцип работы системы Bitcoin, она уже тогда вызывала огромное количество вопросов. Когда ответ на вопрос не удается получить быстро, будь то в силу нежелания глубоко копать или прочих причин, то ответ на такой вопрос может быть додуман и превращен в миф. Не думаю, что стоит останавливаться на политических, идеологических и финансовых вопросах. В данной статье я бы хотел осветить ряд мифов, которые относятся к самой системеBitcoin, ее математическому устройству или к схеме протокола. Предполагаю, что базовые прин-

ципы ее устройства знакомы читателю. В противном случае, он с легкостью может получить общее представление из популяризаторских статей в интернете (например, [1–3]). В основном мифы будут связаны друг с другом, поэтому имеет смысл читать их именно последовательно.

1. Все транзакции — это перевод биткоинов с одного кошелька на другой

Чтобы разобраться в этом вопросе нужно сначала ответить на ряд более сложных. Раз криптовалюта так похожа на обычные деньги, то кажется, что и работа с ними должна быть похожа на работу с деньгами. Кошелек биткоинов в этом смысле для человека представляется чем-то вроде счета, и он волен переводить деньги свободно с одного счета на другой. Но это вовсе не так! Все транзакции в системе можно условно поделить на две части — входные и выходные. Входные транзакции — это такие переводы, которые ассоциированы с тем или иным кошельком, и владелец данного кошелька может ими распоряжаться. Выходная транзакция — это то, во что превращаются входные транзакции, когда владелец решает распорядиться своими средствами. Главное отличие транзакции в системе биткоин от транзакций, например, банковских, состоит в том, что транзакция не всегда указывает явно, куда будут переданы средства. Внутри транзакции передается скрипт на специальном языке программирования [4], результат исполнения которого и определяет принадлежность средств.

Напомню, что в основе протокола лежат, в том числе и следующие криптографические преобразования: пользователь генерирует закрытый ключ, из закрытого ключа выводится открытый ключ, из открытого ключа, путем хэширования выводится адрес кошелька в системе[5].

Одним из самых частых скриптов в транзакции является проверка обладания закрытым ключом. Для этого скрипт составлен так, что доказательством владения будет подпись данных. Но существуют и многие другие варианты скриптов. Сам скриптовый язык не прост, но он вполне позволяет переводить биткоины, например, на те кошельки, открытый ключ которых соответствует каким-то определенным требованиям, как-то: байтовое представление ключа является симметричным, или содержит байт *0xff* ровно два раза. Использовать такую выходную транзакцию сможет любой человек, чей открытый ключ удовлетворяет данным требованиям. Более того, нельзя точно указать, кому принадлежит такая входная транзакция до тех пор, пока владелец явно не решит ей распорядиться. Именно в этот момент он укажет доказательство владения, опубликовав открытый ключ и подпись данных транзакции [6].

2. Все существующие (добытые) биткоины кому-то принадлежат

Этот миф легко развенчать, основываясь на том, что рассказано в предыдущем пункте. Дело в том, что раз транзакция имеет внутри себя некоторый скрипт, то есть вероятность, что скрипт будет написан неверно — это может быть как некорректный скрипт (имеющий ошибку в синтаксисе), так и корректный скрипт, для которого не существует возможности доказательства владения (например, одновременная проверка, что открытый ключ должен иметь все байты равные *0xff* и сразу же, что эти же все байты равны *0xaa*). Для таких скриптов уже никто не докажет владение, а соответственно никто не получит эти биткоины.

3. Одному закрытому ключу соответствует ровно один адрес кошелька в системе

Сразу ответим — одному закрытому ключу соответствует ровно два адреса в системе биткоин. Для того, чтобы разобраться почему так вышло, нужно немного рассказать о неко-

торых сущностях, лежащих в основе всей системы и протоколов. Закрытый ключ — это большое случайное число, а открытый ключ, который ему соответствует — это точка на эллиптической кривой. Из байтового представления открытого ключа и выводятся оба адреса кошелька. Дело в том, что один и тот же открытый ключ может иметь два различных байтовых представления, и для каждого из них адрес будет выведен свой.

Что же за представления это могут быть? Первое представление — это 65 байт. Первый байт содержит константу *0x04* (признак полной записи), затем следуют два набора по 32 байта, которые описывают координаты точки. Второе представление — короткая запись. Поскольку координаты x и уравнения кривой достаточно для восстановления координаты y. Единственно уточнение состоит в том, что при восстановлении возникает неопределенность в четности восстанавливаемой координаты. Поэтому в байтовом виде открытый ключ содержит 33 байта, первый из которых представляет собой одну из двух констант *0x02* или *0x03* (признак короткой записи и указание на четность), за которым следуют 32 байта координаты x точки.

Одним из следствий данной особенности является тот факт, что типовая транзакция проверяет не только обладание закрытым ключом, но и точное соответствие адресу. Не очень понятна, правда, необходимость такой проверки: минимальными затратами каждый владелец закрытого ключа может добавить и второй адрес в свой клиент, а значит и распоряжаться обоими кошельками.

Все кошельки имеют «файловую проекцию» и поэтому их легко украсть

Нередко можно встретить утверждение, что биткоины имеют проблему в безопасности следующего рода — основные клиенты для работы с биткоинами хранят данные владельца в файлах. Таким образом указывается, что потенциальный хакер может украсть такой файл и, узнав пароль от него, фактически похитить и все биткоины, ассоциированные с данным кошельком. Если провести аналогию с деньгами в банке, где потенциальный хакер может завладеть паролем от интернет-банкинга, то у пользователя такого интернет-банка есть хотя бы возможность обратиться в сам банк. Успешность такого обращения я оставлю за рамками статьи. А в случае с биткоинами обращаться куда-либо бесполезно — нет единого центра, который бы отменил транзакцию или оспорил ее.

Тем не менее, если у кого-то «достаточный» уровень паранойи, то он может сделать следующее: сам сгенерировать закрытый ключ, получить из него открытый и из него вывести нужный адрес, после чего с помощью типовой транзакции отправить на него средства. Таким образом, получатся биткоины ассоциированные с адресом, который не защищен каким бы то ни было файлом, а закрытый ключ может находится где угодно, от токенов, до памяти самого владельца. При необходимости воспользоваться средствами данного кошелька можно легко добавить данный кошелек в программу-клиент и вести типовую работу.

Выше я перечислил не все, но довольно-таки часто встречаемые мифы о биткоинах. Не буду даже пытаться утверждать, что большая их часть была охвачена: если рассматривать их все, то можно написать не один цикл книг. Чего только стоят вопросы об анонимности использования биткоинов, рассмотрение работы биткоин-миксеров, вопросы от том, что будет, когда Bitcoin исчерпает заранее установленный лимит создания новых биткоинов.

Обычно статьи о биткоинах принято заканчивать словами о том, что в будущем все деньги исчезнут и останутся системы, основанные на той же идеологии, что и биткоины. Или, наоборот, тем, что через полгода о биткоинах никто и не вспомнит. Я не могу делать такой прогноз, поскольку не обладаю нужной компетентностью. Но одно я могу сказать точно — Bitcoin — это отличная математическая и криптографическая система, анализировать которую можно долго и каждый раз найти что-то новое для себя. В этом

качестве она точно займет свое место в книгах по криптографии. Например, программисты оценят открытый исходный код клиента, который прозрачно показывает реализацию всех используемых алгоритмов, а преподаватели могут приводить Bitcoin как хороший пример реализации криптографических протоколов, указывая какие уязвимости в системе электронных денег существуют и как они могут быть закрыты. Я разбираю протоколы, лежащие в основе системы Bitcoin, в рамках лекций «Криптографические протоколы» для 5 курса студентов МФТИ.

СПИСОК ЛИТЕРАТУРЫ

1. Биткойн. [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Биткоин (дата обращения 11.05.2015).
2. Bitcoin. Как это работает. [Электронный ресурс]. URL: http://habrahabr.ru/post/114642/ (дата обращения 11.05.2015).
3. Как работает Биткойн? [Электронный ресурс]. URL: https://bitcoin.org/ru/how-it-works (дата обращения 11.05.2015).
4. Script — Bitcoin Wiki. [Электронный ресурс]. URL: https://en.bitcoin.it/wiki/Script (дата обращения 11.05.2015).
5. Technical background of version 1 Bitcoin addresses — Bitcoin Wiki. [Электронный ресурс]. URL: https://en.bitcoin.it/wiki/Technical_background_of_Bitcoin_addresses (дата обращения 11.05.2015).
6. Transaction — Bitcoin Wiki. [Электронный ресурс]. URL: https://en.bitcoin.it/wiki/Transaction (дата обращения 11.05.2015).

МАНДАТНЫЙ МЕХАНИЗМ РАЗГРАНИЧЕНИЯ ДОСТУПА — ЭТО ПРОСТО

Е.А. МАРЕННИКОВА

Закрытое акционерное общество «ОКБ САПР», Москва, Россия

В статье рассматривается разграничение доступа пользователей на примере типовой современной компьютерной системы. Обозначены основные угрозы информационной безопасности компьютерной системы, определен способ блокирования угроз. Рассмотрены основные принципы управления потоками информации в рамках мандатного механизма разграничения доступа в СЗИ от НСД «Аккорд».

Ключевые слова: мандатный механизм разграничения доступа, управление потоками информации, метки доступа.

В большинстве КС для разграничения доступа используется дискреционный механизм разграничения доступа [1]. Существует мнение, что применение мандатного механизма неизбежно приведет к возникновению проблем, таких как, например, отсутствие возможности работы с файлами, доступ к которым закрыт мандатными метками. Однако в большинстве случаев некорректная работа мандатного механизма разграничения доступа связана с некорректным выполнением процедуры установки меток мандатного доступа. Зная основные принципы работы мандатного механизма разграничения доступа, выполнить процедуру установки меток мандатного доступа просто.

Рассмотрим на примере типовой современной компьютерной системы (КС) [2], [3], как корректно выполнить разграничение доступа пользователей к объектам КС.

Пусть имеется КС такая, что вся информация (персональные данные пользователей и т.д.), с которой работают пользователи, находится на терминальном сервере (или ферме терминальных серверов).

На рабочем месте сотрудника организована лишь трансляция производимых им действий в графическом виде на монитор. Пусть в состав данной КС входит следующий набор составных частей:

- серверная часть;
- клиентская часть.

Серверная часть предназначена для выполнения пользовательских приложений и организации доступа пользователей к этим приложениям в режиме терминального доступа, а также построения среды хранения данных пользователей и служебных данных, необходимых для выполнения КС своих функций.

Структурными единицами серверной части КС являются терминальные серверы, предназначенные для выполнения приложений в терминальном режиме и файловый сервер, предназначенный для хранения личных папок и профилей пользователей КС.

При работе с информацией ограниченного доступа, часть терминальных серверов, участвующих в данном процессе, объединяются в отдельную ферму, доступ к которой предусматривается для пользователей, работающих с информацией ограниченного доступа.

Клиентская часть включает в себя рабочие станции пользователей КС.

Основные угрозы информационной безопасности КС [4], [5]:

- нарушение доступности информации
- нарушение целостности информации (данных) и программного обеспечения
- нарушение конфиденциальности (неправомерное использование) информации, в том числе за счет хищения отчуждаемых машинных носителей с несанкционированно копированной информацией.

К числу угроз, связанных с недостатками действующих правил разграничения доступа (ПРД), относятся:

- передача или копирование информации из конфиденциальных каталогов в открытые, в том числе сохранение информации конфиденциального характера в открытые каталоги;
- возможность превышения должностных полномочий персонала КС.

Задача управления потоками информации и обеспечения невозможности передачи информации конфиденциального характера в открытые каталоги, являющаяся актуальной в рамках устранения (блокирования) выявленных угроз информационной безопасности КС, может быть реализована только посредством использования соответствующих функций СЗИ от НСД.

В большинстве распространенных СЗИ от НСД реализация данной задачи обеспечивается с использованием возможностей мандатного управления доступом.

Управление потоками информации в рамках мандатного механизма разграничения доступа, на первый взгляд, представляется достаточно громоздкой и сложной задачей. Для корректной настройки мандатного механизма необходимо проанализировать, к каким объектам обращался процесс с запросом на создание, чтение, запись, а после выполнения анализа необходимо корректно установить соответствующие метки доступа процессу и соответствующим объектам (файлам, каталогам, сетевым ресурсам и т.д.) [6].

Процедуры анализа и установки меток доступа занимают достаточно большое количество времени. Возможно, именно поэтому многие организации испытывают затруднения при использовании мандатного механизма разграничения доступа.

Однако процедуры установки меток доступа и анализа, к каким объектам обращался процесс с запросом на создание, чтение, запись в рамках мандатного механизма разграничения доступа можно упростить, используя СЗИ от НСД, в которых предоставляются соответствующие механизмы автоматизации [7].

Так, в СЗИ от НСД «Аккорд» [8] управление потоками информации в рамках мандатного механизма разграничения доступа осуществляется по следующему алгоритму:

1. необходимо присвоить определенную метку доступа процессу;
2. необходимо присвоить соответствующую метку доступа объектам (файлам, каталогам, сетевым ресурсам и т.д.), к которым обращается процесс с запросом на создание, чтение, запись;
3. необходимо присвоить соответствующий уровень доступа пользователю, который работает с процессом в рамках выполнения должностных обязанностей;
4. необходимо разрешить в рамках одного сеанса пользователя выполнение процедуры редактирования документов с разными метками доступа.

После выполнения описанных действий запустить процесс может только пользователь с соответствующим уровнем доступа. После запуска процесс с установленным уровнем доступа может получить доступ к объектам (данным, другим процессам) только с соответствующей меткой доступа.

Для решения проблемы редактирования документов с разными метками доступа в рамках одного сеанса пользователя в ПО ПАК «Аккорд» имеется механизм автоматизации, в рамках которого администратор информационной безопасности может:

5. определить перечень задач (включая системные процессы), использование которых необходимо для выполнения должностных обязанностей пользователя КС;
6. определить объекты, к которым выполняются запросы на открытие файлов для чтения/записи (эти запросы зачастую не зависят от переменных среды, а определяются разработчиками программных пакетов).
7. назначить метку «ОБЩИЙ_РЕСУРС» информации, которую необходимо обрабатывать в рамках сеансов работы пользователей с разными уровнями доступа. Если администратор безопасности присваивает эту метку какой-либо папке, то далее создается несколько копий этого объекта, и каждой копии присваивается одна из меток доступа прописанных в конфигурационном файле системы защиты. Имена копий различаются на один символ, а в процессе работы монитор безопасности динамически перенаправляет ввод-вывод с объекта-оригинала на копию с нужной меткой доступа;
8. предоставить пользователю выбор уровня доступа запускаемой задачи или выбор уровня конфиденциальности сеанса пользователя.

Процедура определения перечня задач и объектов доступа основана на анализе журналов регистрации событий СЗИ от НСД «Аккорд». При этом требуется высокая детальность журнала, чтобы определить, какая программа к каким объектам обращается с запросами на чтение/запись.

ПО ПАК «Аккорд» позволяет выбрать из журнала список исполняемых файлов, отследить операции чтения/записи для отдельных процессов, и сохранить в файл процессы и объекты, которым нужно присвоить метку «ОБЩИЙ_РЕСУРС», а также сформировать списки «общих» ресурсов для конкретных процессов: «общих» ресурсов, необходимых для работы всех пользователей, «общих» ресурсов, необходимых для работы отдельного

пользователя, процессов, которые требуется запускать как в конфиденциальном, так и в общедоступном режиме.

Итак, зная основные принципы работы мандатного механизма разграничения доступа, можно достаточно просто выполнить процедуру установки меток мандатного доступа, тем самым позволяя:

1. осуществлять корректную работу программ с реальным выполнением дисциплины контроля потоков информации;
2. выполнять обработку документов разного уровня конфиденциальности одним набором прикладного ПО без ухудшения надежности защитных механизмов.
3. выполнять обработку информации разных уровней конфиденциальности в рамках сеансов работы пользователя с выбором уровня доступа.

СПИСОК ЛИТЕРАТУРЫ

1. *Киреенко А.Е.* Разработка метода и алгоритма контроля информационных потоков в операционных системах с дискреционным разграничением доступа. – Режим доступа: www.pvti.ru/data/file/bit/2013/2013_2/part_11.pdf;
2. Терминальный доступ: понятие, преимущества, недостатки и особенности работы данной системы [Электронный ресурс]. – Режим доступа: http://www.shindler.ru/content/terminalnyi-dostup-ponyatie-preimushchestva-nedostatki-i-osobennosti-raboty-dannoi-sistemy. – Заглавие с экрана;
3. Защита информации в системах терминального доступа [Электронный ресурс]. – Режим доступа: http://www.okbsapr.ru/sol2.html. – Заглавие с экрана;
4. Угрозы безопасности информации [Электронный ресурс]. – Режим доступа: http://data-sec.ru/public/information-threats/. – Заглавие с экрана;
5. *Конявский В.А.* Компьютерная преступность. – М., 2008;
6. *Конявский В.А.* Управление защитой информации на базе СЗИ НСД «Аккорд». – М., 1999;
7. *Конявский В.А.* Методы и аппаратные средства защиты информационных технологий электронного документооборота. – М., 2005;
8. Способ защиты от несанкционированного доступа к информации, хранимой на персональной ЭВМ/ Патент на изобретение № 2475823. 20.02.2013, бюл. № 5.

О СЛУЧАЙНЫХ БЛУЖДАНИЯХ НА ОБОБЩЕННЫХ В СМЫСЛЕ IMASE И ITO ГРАФАХ ДЕ БРЕЙНА

С.Ю. МЕЛЬНИКОВ

Обобщенным в смысле Imase и Ito графом де Брейна $G(n,d)$, $n,d=1,2,...$, называется ориентированный граф на n вершинах, с дугами, ведущими из вершины i в вершину $di+r \pmod n$, $0 \le i \le n-1$, $0 \le r \le d-1$. Такой граф ([1, 2]) имеет nd дуг и является регулярным степени d. Граф $G(d^t,d)$, $t=1,2,...$ является классическим d-ичным графом де Брейна степени t.

Рассмотрим случайное блуждание на графе $G(n,d)$, при котором начальная вершина выбирается случайно из множества вершин графа, а шаг блуждания проходит по исходящим из нее дугам. Предположим, что переходы из вершины в вершину незави-

симы и вероятность шага блуждания из вершины i в вершину $di+r\left(\mathrm{mod}\, n\right)$ равна p_r, $\sum_{r=0}^{d-1} p_r = 1$, $0 < p_r < 1$.

Задачи, связанные с изучением случайных блужданий на классических графах де Брейна, рассматривались в литературе как в случае $p_r = 1/d$ ([3, 4]), так и в общем случае ([5, 6]).

Утверждение. Пусть $n = sd^t$, $t \geq 0$, s и d — взаимно-простые числа. Для $0 \leq q \leq n-1$ обозначим $b_r\left(q\right)$ — количество символов r в d-ичной записи числа $q \bmod \left(d^t\right)$. Стационарное распределение описанного случайного блуждания на вершинах графа $G\left(n,d\right)$ имеет вид:

$$P\left(q\right) = \frac{1}{s}\prod_{r=0}^{d-1} p_r^{b_r(q)},\ 0 \leq q \leq n-1.$$

Следствие. Если n и d — взаимно-простые числа, то стационарное распределение на вершинах графа является равномерным и не зависит от значений $\left\{p_r, 0 \leq r < d\right\}$:

$$P\left(q\right) = \frac{1}{n},\ 0 \leq q \leq n-1.$$

СПИСОК ЛИТЕРАТУРЫ

1. *Imase M., Itoh M.* A design for directed graphs with minimum diameter, IEEE Trans. Comput. 32 (1983) 782–784.
2. *Максимовский А. Ю., Мельников С. Ю.* О числе обобщенных в смысле Imase и Itoh регистров сдвига, устанавливаемых постоянным входом в фиксированное состояние. // ОПиПМ, т. 22, вып. 5, 2015. http://tvp.ru/conferen/vsppm16/chelso144.pdf
3. *Мори Т.* Случайные блуждания на графах де Брейна // ТВП, 37:1 (1992), 194–197.
4. *Колодзей А. В.* Контрольные множества ориентированных графов // ОППМ, т. 22, вып.1, 2015. http://tvp.ru/conferen/vsppm16/chelso005.pdf
5. *Alhakim A.* On the eigenvalues and eigenvectors of an overlapping Markov chain // Probab. Theory Related Fields, 128(4): 589–605, 2004.
6. *Ayyer A., Strehl V.* Stationary distribution and eigenvalues for a de Bruijn process // In: Kotsireas, I.S., Zima, E.V. (eds.) Advances in Combinatorics, pp. 101–120. Springer, Berlin (2013).

АРХИТЕКТУРА КРИПТОГРАФИЧЕСКОГО СОПРОЦЕССОРА НА ПЛИС

А. Ю. РОДИОНОВ

Закрытое акционерное общество «ОКБ САПР», Москва, Россия

В статье дается подробное описание архитектуры криптографического сопроцессора на основе ПЛИС, как наиболее подходящей аппаратной платформе для его реализации. Приведен перечень минимально необходимых элементов системы, их взаимосвязи между собой. Освещены особенности аппаратной реализации в аспекте обеспечения высокой производительности системы. Большое внимание уделяется вопросу безопасности архитектуры с описанием возможных атак и соответствующих мер противодействия.

Ключевые слова: ПЛИС, СКЗИ, HSM, параллельные вычисления, ключевая информация.

Непрерывное увеличение количества пользователей и устройств, подключенных к телекоммуникационным сетям, увеличение пропускной способности каналов связи и вместе с этим объемов передаваемых данных повышают требования к вычислительных мощностям поставщиков дистанционных информационных услуг. Независимо от рода предоставляемых услуг некоторое количество ресурсов выполняют функции по обеспечению информационной безопасности, в частности криптографические функции. Высокие требования к производительности серверов для работы с криптографией вынуждают использовать отдельные аппаратные модули для этой задачи. В данной статье описана архитектура криптографического сопроцессора, проектировавшегося с учетом современного состояния аппаратных и программных решений, отечественных криптографических алгоритмов, обеспечивающая потенциально высокое быстродействие и высокий класс защиты.

Исходя из области применения криптографического сопроцессора, можно сформулировать ряд требований, которым он должен соответствовать.

1. Гибкая настройка и возможность обновления аппаратной реализации криптографических алгоритмов. Реализация данного требования значительно упрощает поддержку произведенных сопроцессоров, позволяя исправлять ошибки, оптимизировать и добавлять новые реализации криптоалгоритмов. Пользователи смогут динамически менять конфигурацию сопроцессора под текущие нужды системы. Например, при необходимости зашифровать большое количество файлов можно переконфигурировать сопроцессор, уменьшив количество блоков вычисления хэш-функции и увеличив количество блоков шифрования.
2. Преобладание значимости количества одновременных операций над скоростью их выполнения. Отказ в обслуживании из-за недостатка свободных ресурсов более критичен, чем более продолжительное ожидание ответа.
3. Безопасное хранение ключевой информации.

Современные аппаратные решения предлагают несколько альтернатив в качестве платформы для реализации сопроцессора.

1. Интегральные схемы специального назначения (ASIC). Разрабатываются для выполнения строго определенных функций, например криптоалгоритмов. Из-за своей узкой специализации имеют высокое быстродействие, но при этом отсутствует возможность динамического аппаратного конфигурирования, что приводит к замене устройства при необходимости использования других криптоалгоритмов. Дороги в разработке и мелкосерийном и единичном производстве.
2. Микроконтроллеры и процессоры. Возможна лишь программная реализация алгоритмов, позволяющая легко и быстро разрабатывать, переконфигурировать устройство, но обладающая меньшим быстродействием по сравнению с аппаратной реализацией.
3. Программируемая логическая интегральная схема (FPGA). В отличие от цифровых микросхем логика работы задается не на производстве, а при помощи заранее подготовленной прошивки при подаче электропитания, что позволяет динамически переконфигурировать схему. Сочетание этого свойства с быстродействием аппаратной реализации делает ПЛИС наилучшим выбором в соответствии с приведенными требованиями, поэтому дальнейшее описание архитектуры будет основано на ее применении.

Помимо высокого быстродействия аппаратная реализация криптографических алгоритмов в виде отдельных функциональных блоков позволяет воспользоваться таким преимуществом как распараллеливание вычислений. Таким образом, на одном сопро-

цессоре в один момент времени независимо друг от друг могут выполняться вычисления в соответствии с действующими ГОСТ: ГОСТ 28147–89, ГОСТ 34.12–2015, ГОСТ Р 34.11–94, ГОСТ Р 34.11–2012, ГОСТ Р 34.10–2001, ГОСТ Р 34.10–2012. Естественно для эффективной работы параллельных вычислений необходима соответствующая поддержка на высоком абстрактном уровне, например организация программных процессов/потоков в ОС хоста и виртуальных каналов передачи данных.

В целом сопроцессор можно представить в виде взаимодействующих между собой и хостом функциональных блоков. Реализация сложных взаимосвязей между ними и распределение нагрузки возлагается на центральный управляющий элемент. В отличие от функциональных блоков, реализующих ресурсоемкие криптоалгоритмы с неизменной структурой, управляющий элемент большую часть времени находится в режиме ожидания результатов их работы. Кроме того, логика его работы сложна в отладке и может претерпевать изменения. По этим причинам целесообразно реализовать его в виде soft-процессора (процессор, созданный с помощью логического синтеза), выполняющего программный код под управлением многозадачной операционной системы необходимой для поддержки абстракции параллельных вычислений. Исходя из типичного сценария работы управляющего программного потока, состоящего из ожидания запроса на обработку данных, инициализации соответствующего функционального блока и перехода в режим ожидания результатов обработки или нового запроса, оптимальным вариантом является кооперативная ОС. При данном подходе текущий поток исполняется до тех пор, пока явно не передаст управление следующему потоку, что гарантирует постановку задачи функциональному блоку без накладных расходов на переключение контекста, которые могли бы проявляться при использовании ОС с вытесняющей многозадачностью. Кроме того, отсутствует необходимость защиты разделяемых ресурсов критическими секциями, мьютексами, что значительно упрощает программирование.

Кроме уже рассмотренных составляющих элементов сопроцессора для его функционирования необходимы:

1. ПЗУ для хранения ключевой информации, прошивки ПЛИС, кода программ и другой служебной информации;
2. ОЗУ;
3. физический датчик случайных чисел для выработки ключевого материала и случайных последовательностей.

Наиболее безопасным решением было бы размещение всех вышеописанных компонентов внутри одного кристалла. К сожалению, внутренних ресурсов ПЛИС может быть недостаточно для решения задач высоконагруженных серверов. Универсальное решение состоит в задействовании внешних по отношению к ПЛИС аппаратных компонентов для расширения функциональных возможностей сопроцессора. Однако с увеличением количества элементов системы возрастает ее сложность и количество уязвимостей. Рассмотрим возможные атаки на информационную систему с использованием СКЗИ, в контексте их направленности на проектируемый сопроцессор, а также архитектурные решения, противодействующие им.

1. Атака, направленная на изменение прошивки ПЛИС или кода программ в ПЗУ на этапе производства или обновления СКЗИ. Хранение данной информации в открытом виде позволяет нарушителю успешно провести эту атаку, будучи не обнаруженной. Защититься можно добавлением к хранящейся информации имитовставки, вычисленной на секретном ключе производителя, зашиваемым в сопроцессор на этапе производства. Поскольку ПЛИС не может проверить свою собственную прошивку, необходимо добавить элемент, который бы вычислял имитовставку и инициализировал ПЛИС. В качестве такого элемента может выступать микроконтроллер, в котором

хранится ключ производителя. Это решение позволяет выявить несанкционированные модификации при старте устройства микроконтроллером, так и в любой момент времени специальным ПО в ОС хоста.

2. Компрометация ключевой информации, хранящейся в открытом виде в ПЗУ, нарушителем, имеющем физический доступ к СКЗИ. Ее конфиденциальность может быть обеспечена шифрованием на мастер-ключе, не покидающем кристалл ПЛИС, и расшифрованием в ПЛИС непосредственно перед использованием в функциональном блоке.
3. Компрометация ключевой информации, передаваемой между ПЗУ и ПЛИС в открытом виде по каналам побочных излучений и наводок. Вышеописанный метод по ее зашифрованию обеспечивает защиту от данной атаки.
4. Компрометация ключевой информации, хранящейся в открытом виде в ОЗУ, нарушителем, имеющем физический доступ к СКЗИ. ОЗУ используется для размещения кода программ, кучи и стэка центрального управляющего элемента. Из этого следует, что управляющий элемент не должен иметь доступ к ключевой информации в открытом виде, чтобы избежать возможности ее попадания в ОЗУ. Таким образом, функция шифрования, расшифрования и передачи ключевой информации в открытом виде в функциональные блоки по шине данных, не соединяющейся с управляющим элементом и ОЗУ, возлагается на отдельный элемент в ПЛИС. Из-за высокой частоты использования секретных ключей сопроцессором, работу по зашифрованию/расшифрованию целесообразно оптимизировать, объединив ее с функцией кэширования в том же блоке.
5. Несанкционированный доступ к СКЗИ. В случае кражи СКЗИ нарушитель может, пользуясь штатными функциями СКЗИ, выполнять криптографические преобразования данных с использованием секретных ключей. Для исключения этой возможности достаточно разделить мастер-ключ, на котором зашифрованы секретные ключи, на две части, одна из которых зашита в микроконтроллере сопроцессора, а другая записана на отчуждаемом ключевом носителе, необходимая к предъявлению перед началом работы.

Итоговая схема криптографического сопроцессора представлена на рисунке 1.

Рис. 1. Архитектура криптографического сопроцессора

БЕЗОПАСНОСТЬ ВИРТУАЛЬНЫХ ИНФРАСТРУКТУР. СЛОЖНОСТИ И НЮАНСЫ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ РЕГУЛЯТОРА

А.С. РЯБОВ, Д.В. УГАРОВ, Д.А. ПОСТОЕВ
Закрытое акционерное общество «ОКБ САПР»

Статья посвящена вопросам безопасности виртуальных инфраструктур. Рассмотрены проблемы, связанные с выполнением требований нормативно правовых актов и методических документов ФСТЭК России в части защиты виртуальных инфраструктур. Предложены решения задачи обеспечения безопасности виртуальных инфраструктур, учитывая сложности и нюансы требований регулятора.

Ключевые слова: виртуальная инфраструктура, ФСТЭК России, виртуальная машина, доверенная загрузка, сегментация виртуальных инфраструктур.

Виртуализация уже прочно вошла в нашу жизнь и требования по ее защите были сформулированы нормативными и методическими документами ФСТЭК России [1–4]. Но и сегодня у специалистов по информационной безопасности выполнение требований регулятора в части защиты виртуальных инфраструктур вызывает затруднения и ряд вопросов. Это обусловлено «расплывчатостью» требований регулятора, слабым пониманием данных требований со стороны потребителей и недобросовестностью некоторых вендоров, сложностью выполнения определенных мер. Теперь обо всем поподробнее:

Анализируя требования в части защиты виртуальной инфраструктуры, можно сразу же столкнуться с первым «узким местом» — дефицитом необходимых определений некоторых терминов, которые встречаются в тексте документов. В качестве примера можно отметить такие термины как «виртуальное программное обеспечение», «виртуальное аппаратное обеспечение», «файл-образ» и т. д. Отсутствие глоссария является первым «препятствием» на пути к однозначному пониманию и правильному выполнению требований регулятора. Ситуация также усугубляется отсутствием реальных примеров по соотнесению этих терминов с элементами виртуальных инфраструктур различных вендоров (VMware vSphere, Microsoft Hyper-V и прочих). Для решения данной проблемы необходим стандарт (ГОСТ) в области защиты виртуальных инфраструктур, в котором были бы приведены все необходимые термины и определения.

Вторым «препятствием» на пути к выполнению требований регулятора является то, что некоторые недобросовестные вендоры вводят в заблуждение потребителей средств защиты информации, заявляя о том, что можно выполнить практически все меры в части защиты виртуальной инфраструктуры всего лишь одним средством защиты информации. Однако анализ требований показывает, что реализовать меры такими продуктами можно лишь частично, и для полноценной реализации всех мер в части защиты виртуальных инфраструктур требуется применение множества продуктов:

- для реализации мер ЗСВ.1, ЗСВ.2, ЗСВ.3, ЗСВ.5, ЗСВ.6, ЗСВ.7 необходимо применять специализированные сертифицированные средства защиты виртуальных инфраструктур. В частности, для защиты платформы VMware vSphere может применяться ПАК СЗИ от НСД «Аккорд-В.»;
- мера ЗСВ.4 и ЗСВ.10 реализуются совокупностью классических сетевых средств защиты (FW/VPN), в том числе и виртуальных (virtual appliance), функциями платформы виртуализации, а также наложенными средствами защиты информации;

- мера ЗСВ.8 реализуется средствами резервного копирования и восстановления данных, адаптированных для виртуальных инфраструктур, механизмами резервирования, встроенными в платформу виртуализации, а также другими организационно-техническими мерами, например, дублированием серверов, каналов связи и т.д;
- мера ЗСВ.9 реализуется путем применения антивирусного программного обеспечения, адаптированного для платформ виртуализации.

Отдельно отметим, что мера ЗСВ.10 стоит особняком, и сегментирование виртуальной инфраструктуры является комплексной задачей и должно быть реализовано с нескольких различных сторон:

- организационными мерами;
- функциями платформы виртуализации,
- функциями сетевого оборудования и сетевых средств защиты, в том числе и виртуальных (virtual appliance);
- наложенными средствами защиты информации.

Рис. 1. Комплексный подход к реализации меры ЗСВ.10

Рассмотрим комплексный подход к реализации меры ЗСВ.10, который необходимо выполнять при проектировании системы защиты информационной системы, построенной с использованием технологии виртуализации.

В первую очередь необходимо провести категоризацию обрабатываемой в информационной системе информации, определить каким группам пользователей она должна быть доступна с точки зрения бизнес-процессов в организации. Полученные сведения необходимы для формирования политики доступа пользователей к информации. Также необходима информация об архитектуре информационной системы. Полученные данные используются для настройки виртуальных инфраструктур с учетом требований безопасности. Однако функционала средств виртуализации для этого недостаточно, потому что настройками виртуальной инфраструктуры обеспечивается правильность работы в штатном режиме, и для защиты их от несанкционированных изменений со стороны администраторов виртуальной инфраструктуры необходимо использовать наложенные СЗИ.

Рассмотрим более детально реализацию меры ЗСВ.10 с этой точки зрения на примере виртуальной инфраструктуры VMware vSphere и ПАК СЗИ от НСД «Аккорд-В.». Для сегментирования виртуальных инфраструктур ФСТЭК России предлагает выполнить несколько требований [3]:

1. Сегментирование информационной системы проводится с целью построения многоуровневой (эшелонированной) системы, разделения информационной системы на разные классы защищенности.
Для VMware vSphere предполагается выделение логически независимых объектов (кластеров хостов и хранилищ, а так же распределенных коммутаторов). Граница сегмента проходит по границе данных объектов, а изоляция информационных потоков обеспечивается средствами виртуальной инфраструктуры с помощью задания правил миграции и разделения сетей виртуальными коммутаторами.

Для разграничения доступа пользователей к ресурсам сегментов разных уровней необходимо использовать иерархические метки безопасности. Данный функционал реализует модуль контроля потоков «Аккорд-В.» путем задания уровней доступа администраторам виртуальной инфраструктуры, а также меток конфиденциальным ресурсам: виртуальным машинам, шаблонам, хостам, хранилищам и виртуальным группам портов (в том числе распределенным). Таким образом можно ограничить доступ администраторов одного сегмента к другому и тем самым обеспечить правильность и неизменность настроек виртуальной инфраструктуры. Помимо проверки соответствия уровней пользователя и запрашиваемых ресурсов, «Аккорд-В.» позволяет запретить перемещение и подключение объектов одного уровня иерархии в сегмент другого уровня, что позволяет обеспечить логическую изолированность сегментов.

2. Сегментирование информационной системы, предусматривающее выделение группы виртуальных машин, хранилищ информации и информационных потоков, предназначенных для решения выделенных (обособленных) задач.
В виртуальной инфраструктуре подобная категоризация пользователей и доступных им ресурсов реализуема несколькими способами:

- выделение ресурсов в отдельные логические группы — папки (применимо для виртуальных машин и шаблонов);
- использование ролевой модели доступа;
- применение технологии VLAN для разделения сетевого трафика, для передачи информации разной категории.

С помощью модуля контроля потоков «Аккорд-В.» можно организовать полноценное разграничение доступа пользователей к сегментам на основе неиерархических меток безопасности (категорий). Назначая метки конфиденциальным ресурсам и группам пользователей, которым необходим доступ к ним, обеспечивается изоляция сегментов, предназначенных для решения выделенных задач. Также «Аккорд-В.» обеспечивает невозможность перемещение ресурсов из одного сегмента в другой на основании контроля назначенных категорий.

3. Выделение в отдельный сегмент (отдельные сегменты) серверов управления виртуализацией (автоматизированного рабочего места администратора управления средствами виртуализации).
Данная мера реализуется «по умолчанию» благодаря использованию сетевых устройств и не требует дополнительных уточнений.

4.Физическое сегментирование виртуальной инфраструктуры для решения выделенных (обособленных) задач.
Для реализации данного требования помимо логического сегментирования и организации полномочного (мандатного) разграничения доступа предполагается физическое

разделение серверов, хранилищ и сетевых устройств, обрабатывающих и передающих информацию, предназначенную для решения выделенных (обособленных) задач.

В заключение можно отметить, что появление в 2013 году нормативно-правовых актов и методических документов ФСТЭК России, содержащих требования по защите виртуальных инфраструктур является большим плюсом. Но выполнение требований и по сей день вызывает у специалистов затруднения и ряд вопросов.

Сообществу необходим стандарт (ГОСТ) по безопасности виртуальных инфраструктур, для четкого и однозначного понимания всех требований регулятора.

Потребителям средств защиты необходимо взять на заметку, что невозможно выполнить все требования регулятора по защите виртуальных инфраструктур только одним средством защиты. Для полноценной реализации всех мер требуется применение множества продуктов.

Также не стоит забывать о том, что и реализация отдельных мер требует комплексного подхода. Например, сегментирование виртуальных инфраструктур (ЗСВ.10) должно быть реализовано с нескольких различных сторон: организационными мерами, функциями платформы виртуализации, функциями сетевого оборудования и сетевых средств защиты, в том числе и в виде виртуальных аплаенсов, наложенными средствами защиты информации.

СПИСОК ЛИТЕРАТУРЫ

1. Приказ № 17 ФСТЭК России от 11 февраля 2013 г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
2. Приказ № 21 ФСТЭК России от 18 февраля 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
3. Методический документ ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах».
4. Приказ № 31 ФСТЭК России от 14 марта 2014 г. «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ВИРТУАЛЬНЫХ ИНФРАСТРУКТУР В БАНКОВСКОМ СЕКТОРЕ

А.С. РЯБОВ
Закрытое акционерное общество «ОКБ САПР»

Статья посвящена вопросам безопасности виртуальных инфраструктур в банках и других финансовых организациях. Рассмотрены основные принципы защиты виртуальной инфраструктуры в разрезе Рекомендаций Банка России РС БР ИББС-2.8–2015, а также предложены решения по обеспечению безопасности.

Ключевые слова: информационная безопасность, технологии виртуализации, банковский сектор, РС БР ИББС-2.8–2015, виртуальная машина.

В последнее время развитие нормативной базы по информационной безопасности (ИБ) для банковского сектора идет очень активно. В 2014 году обновился Стандарт Банка России СТО БР ИББС-1.0–2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» [1]. Без внимания не остались и вопросы, связанные с безопасностью технологий виртуализации. В положениях стандарта появились базовые требования по защите виртуальных инфраструктур. Для уточнения базовых требований [1] в 2015 году Банком России выпущены рекомендации РС БР ИББС-2.8–2015 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности при использовании технологий виртуализации» [2].

Обеспечение ИБ технологий виртуализации в разрезе документа [2] подразумевают эшелонированный подход к защите. В документе даются рекомендации по:

- разделению потоков информации и изоляции виртуальных машин (ВМ);
- обеспечению информационной безопасности образов ВМ;
- обеспечению информационной безопасности серверных компонентов виртуализации;
- обеспечению информационной безопасности ВМ;
- обеспечению информационной безопасности автоматизированных рабочих мест пользователей, используемых при реализации технологии виртуализации рабочих мест пользователей;
- мониторингу информационной безопасности;
- составу ролей и разграничению полномочий эксплуатационного персонала;
- обеспечению информационной безопасности системы хранения данных.

Рассмотрим наиболее важные положения документа [2] и предложим способы реализации защитных мер:

В банковских организациях существуют различные банковские технологические процессы — платежный, информационный, а также банковские технологические процессы, в рамках которых обрабатываются персональные данные [1]. Банковские технологические процессы имеют разные уровни критичности с точки зрения информационной безопасности. Для каждого вида банковского технологического процесса необходимо создать отдельный контур безопасности путем применения отдельного хост-сервера для каждого контура. Информационное взаимодействие между контурами необходимо обеспечивать с помощью сертифицированного сетевого оборудования, обеспечивающего контроль не выше сетевого уровня семиуровневой модели OSI [2].

Необходимо также обеспечить и запрет нерегламентированного информационного обмена между ВМ и другими компонентами виртуализации [2]. Например, в VMware vSphere информационный обмен между ВМ и ESXi обеспечивается помощью настройки VMCI (Virtual Machine Communication Interface). Настройки VMCI хранятся в фалах оборудования ВМ и без надлежащего контроля могут быть подвержены модификации. Для защиты настроек от модификации необходимо применять механизмы (средства защиты), которые позволяют контролировать конфигурацию оборудования ВМ (например, это может быть программно-аппаратный комплекс «Аккорд-В.»).

В рекомендациях по обеспечению ИБ базовых образов ВМ большое внимание уделяется вопросам контроля настроек ВМ, антивирусного контроля, обновления программных средств, а также целостности ОС, прикладного ПО и СЗИ ВМ [2].

При обеспечении безопасности текущих образов ВМ необходимо также позаботится о вопросах запрета несанкционированного копирования этих образов [2]. С данной задачей может справиться программно-аппаратный комплекс «Сегмент-В.», путем запрета клонирования и экспорта ВМ, а также запрета доступа к хранилищу пользователям.

При обеспечении безопасности серверных компонентов виртуализации, автоматизированные рабочие места, предназначенные для администрирования, рекомендуется располагать в специально выделенном сегменте вычислительных сетей [2]. При этом для контроля использования иных АРМ для выполнения задач управления и администрирования серверных компонентов виртуализации рекомендуется использование сертифицированных сетевых технических средств [2], например, комплекс «Сегмент-В.».

Средства управления и администрирования виртуализации являются сердцем инфраструктуры и подлежат тщательной защите. Для управления доступом к указанным элементам необходимо применять надежные сертифицированные СЗИ от НСД (например, СЗИ от НСД «Аккорд-Win64» (TSE)).

В соответствии с положениями [2] для антивирусной защиты виртуальной инфраструктуры рекомендуется применять средства, функционирующие на уровне гипервизора без установки агентского ПО на ВМ.

Для доступа пользователей к ВМ, включенным в контур безопасности платежного технологического процесса и контур безопасности ИСПДн посредством АРМ пользователя, рекомендуется применять двухфакторную аутентификацию с использованием аппаратных средств [2] (например, персональные идентификаторы «ШИПКА»).

Немаловажным аспектом безопасности виртуальной инфраструктуры является мониторинг. Для осуществления такого мониторинга должны обеспечиваться сбор, архивирование и хранение в течение определённого периода времени журналов, в которых регистрируются действия пользователей, нештатные ситуации и события ИБ виртуальной инфраструктуры. Как правило, сертифицированные СЗИ от НСД для виртуальных инфраструктур осуществляют регистрацию событий безопасности и имеют средства для их просмотра и анализа. Для архивации и надежного хранения журналов безопасности рекомендуется использовать мобильное USB-устройство с управляемым доступом «Программно-аппаратный журнал» (ПАЖ), которое позволяет осуществлять сбор, архивацию и безопасное хранение журналов безопасности. При необходимости (например, при обнаружении инцидента ИБ) архивы журналов можно экспортировать для исследования в аналитические системы, например, в системы SIEM.

Необходимо также определиться с составом ролей и разграничением полномочий эксплуатационного персонала. Для виртуальной инфраструктуры необходимо выделить следующие роли эксплуатационного персонала [2]:

- Администратор ВМ и администратор информационной безопасности ВМ;
- Администратор ИБ по управлению серверными компонентами виртуализации;
- Администратор по управлению серверными компонентами виртуализации;
- Администратор СХД.

Заключительным этапом является обеспечение безопасности систем хранения данных (СХД). В соответствии с [2] в СХД рекомендуется выделять отдельные логические разделы для каждого контура безопасности. При этом доступ к СХД рекомендуется осуществлять только с использованием гипервизора, АРМ, используемых для выполнения задач управления и администрирования СХД, и технических средств, используемых

для резервного копирования информации. Для контроля доступа к логическим разделам СХД рекомендуется применение сертифицированных сетевых технических средств, а для доступа к средствам управления и администрирования СХД рекомендуется использовать двухфакторную идентификацию, реализуемую сертифицированными СЗИ от НСД (например, СЗИ от НСД «Аккорд-Win64»).

В рекомендациях [2] также большое внимание уделяется регламентированию (документированию) различных процессов, связанных с обеспечением ИБ технологий виртуализации. Например, документирование процессов жизненного цикла базовых образов, документирование состава ПО базовых образов, регламентация обновления программного обеспечения и т.д. Таким образом, необходима разработка новых или корректировка существующих в банке внутренних документов.

Таким образом, можно сделать следующие выводы: построение системы защиты виртуальной инфраструктуры в соответствии с рекомендациями Банка России РС БР ИББС-2.8–2015 является комплексной задачей, и обеспечивается организационными и техническими мерами.

При этом в качестве организационных мер можно выделить разработку новых и корректировку действующих внутренних организационных документов банка, как верхнеуровневых (частных политик ИБ), так и низкоуровневых — процессных (регламенты, инструкции, списки, перечни).

К техническим мерам можно отнести:

- настройка и конфигурация платформы виртуализации;
- сегментирование инфраструктуры;
- установка адаптированных для виртуальной инфраструктуры средств защиты.

Также можно выделить следующий набор необходимых средств защиты для реализации безопасности виртуальной инфраструктуры:

- межсетевые экраны и сетевое оборудование;
- средства защиты информации, адаптированные для виртуальных инфраструктур (например, для популярной в России платформы виртуализации VMware vSphere — программно-аппаратные комплексы «Аккорд-В.» и «Сегмент-В.», а для платформы Microsoft Hyper-V — комплекс «ГиперАккорд»);
- средства двухфакторной аутентификации (например, персональные идентификаторы «ШИПКА»);
- средства антивирусной защиты, адаптированные для виртуальных инфраструктур;
- средства сбора, архивации и надежного хранения журналов безопасности.

Средства защиты должны быть сертифицированы по требованиям безопасности ФСТЭК.

В заключение можно отметить, что методическая база по информационной безопасности банковского сектора серьезно изменилась за последнее время. Банк России не оставил без внимания и вопросы обеспечения информационной безопасности популярного направления — виртуализации. При этом Рекомендации Банка России РС БР ИББС-2.8-2015 являются универсальными для популярных на российском рынке платформ: VMware vSphere, Microsoft Hyper-V. Несмотря на рекомендательный статус, документ РС БР ИББС-2.8-2015 учитывает специфические особенности организации банковской системы. Поэтому специалистам по информационной безопасности банков, использующих виртуализацию в качестве среды обработки данных, рекомендуется применять положения документа РС БР ИББС-2.8-2015 при реализации системы защиты как «руководство к действию».

СПИСОК ЛИТЕРАТУРЫ

1. Стандарт Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».
2. Рекомендации Банка России РС БР ИББС-2.8-2015 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности при использовании технологий виртуализации».

ЗАЩИТА ИНФОРМАЦИИ НА ОСНОВЕ ХАОТИЧЕСКОЙ ДИНАМИКИ

А. В. СИДОРЕНКО

Быстрое развитие информационных технологий, глобальной сети Интернет и социальных сетей привело к формированию информационной среды, оказывающей влияние практически на все сферы человеческой деятельности. В связи с этим возникла необходимость развития методологических основ передачи информации, поиска системных решений с применением эффективных алгоритмов и методов построения средств защиты информации для обеспечения ее целостности и достоверности.

Высокий уровень информационных методов анализа нелинейных сложных систем и определения закономерностей в области самоорганизации и хаотической динамики позволяет решить проблемы передачи, шифрования и приема информации.

Интерес к использованию систем хаотической динамики в телекоммуникационных сетях обусловлен такими свойствами как естественная широкополосность, обеспечение синхронизации передатчика и приемника, возможность передачи информации в средах при наличии шумов. Необходимая для передачи данных энергетика обеспечивается наличием указанной полосы частот, а качество передачи — использованием когерентного приема и возможностью функционирования систем в средах с многолучевым распространением.

Для защиты информации от несанкционированного доступа, как правило, используется ее шифрование. Одним из перспективных направлений в современной криптографии является разработка алгоритмов шифрования с использованием хаотической динамики. Применение таких систем для защиты информации обусловлено способностью хаотических отображений обеспечивать скрытость передачи зашифрованной информации. Наличие таких важных свойств как чувствительность к начальным условиям и системным параметрам, свойства псевдослучайности и топологической транзистивности являются позитивными для шифрования информации.

Существующие в настоящее время традиционные алгоритмы шифрования, среди которых наиболее известными являются AES, DES, ГОСТ 28147–89, СТБ 34 10131–2007, характеризуются быстротой, стойкостью, универсальностью. Однако для шифрования изображений они не могут быть применены в силу ряда причин. В частности, размер изображения при шифровании, как правило, значительно превосходит размер текстового или бинарного сообщения, что приводит к значительному возрастанию временных затрат на шифрование. Это приводит к необходимости разработки новых алгоритмов шифрования, а приведенная информация свидетельствует в пользу систем с хаотической динамикой.

В предлагаемой работе рассматриваются вопросы применения систем хаотической динамики для шифрования изображений, создания алгоритмов шифрования и определения стойкости созданных алгоритмов.

Общая архитектура основанных на хаотической динамике криптографических систем типа перестановки — рассеяния используемых для шифрования изображений приведена на рисунке 1.

Криптографические системы такого типа включают два взаимно независимых этапа. На первом этапе (этапе перестановки) согласно некоторым преобразованиям, все пиксели изображения меняются местами без изменения своих значений. Для обеспечения снижения корреляции смежных пикселей изображения перестановка производится n раз, где $n \geq 1$. В результате каждый пиксель заменен другим из этого же изображения. Таким образом, добиваются перемешивания пикселей изображения. Однако, поскольку значения пикселей не изменялись, гистограмма распределения по яркости элементов изображения совпадает с диаграммой исходного изображения. На втором этапе (этапе диффузии) значения пикселей последовательно изменяются таким образом, чтобы небольшое изменение одного пикселя распространялось по всему изображению. Чтобы достигнуть удовлетворительного уровня перемешивания и диффузии цикл перестановки-рассеяния повторяется m раз ($m \geq 1$).

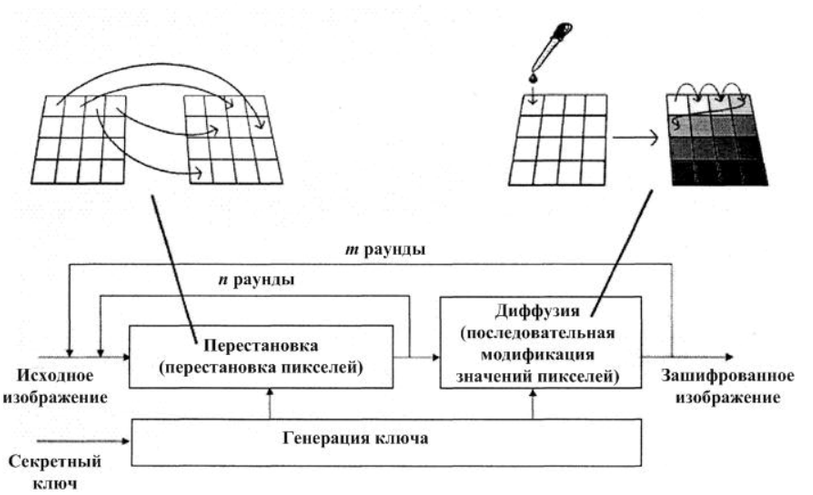


Рис. 1. Схема алгоритмов шифрования типа перестановки — рассеяния

Для улучшения защиты информации, параметры, управляющие перемешиванием и диффузией, должны быть различными в разных раундах. Это достигается использованием циклического генератора ключей с изначальным секретным ключом. В таких криптографических системах этап перемешивания, этап диффузии и генерация ключей могут быть реализованы с помощью хаотических отображений.

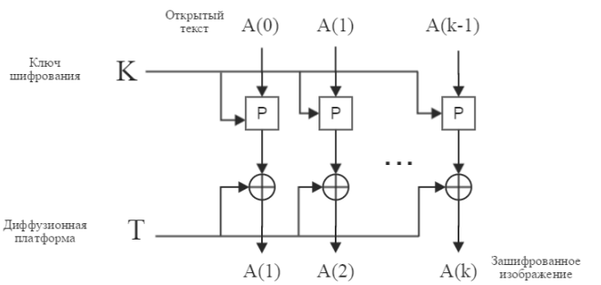
В исходном изображении между соседними пикселями наблюдается высокое значение корреляции. Для ее снижения пиксели необходимо переместить в различные места изображения детерминированным образом, чтобы их можно было инвертировать в процессе расшифрования. Хаотическим отображениям свойственны перемешивающие и эргодические свойства, чувствительность к параметрам управления, что подтверждает возможность их использования в качестве ключа шифрования.

Процедура расшифрования подобна процедуре шифрования, но выполняется в обратном порядке. Это означает, что изображение преобразуется обратной функцией диффузии, затем происходит перемешивание пикселей в обратном порядке. Это происходит в силу обратимости хаотических отображений. Число раундов расшифрования должно быть равно числу раундов при шифровании. Восстановленное с помощью верного ключа изображение является точной копией исходного изображения.

Структурная схема одного из алгоритмов шифрования-расшифрования приведена на рис. 2.

В этом алгоритме хаотическое отображение используется и для перестановки пикселей, и для рассеяния. В качестве ключа применяются начальные условия, параметр хаотического отображения, количество циклов перестановки-рассеяния. Шифр является симметричным, так как для шифрования и расшифрования используется один и тот же ключ. Построение алгоритма шифрования с использованием хаотической динамики включает: 1) инициализацию ключа; 2) создание рассеивающей платформы; 3) смещение цветовых компонент; 4) перемешивание RGB — плоскостей (красный, зеленый, синий цвета); 5) перемешивание пикселей изображения; 6) рассеяние (XOR, операция «исключающее или») изображения с помощью рассеивающей платформы.

Этапы 4, 5, 6 для лучшего шифрования могут повторяться несколько раз.



Перестановка (P) и рассеяние (XOR)

Рис. 2. Схема алгоритма

Применение криптографических средств защиты информации в практически реализуемых системах неразрывно связано со стойкостью алгоритмов шифрования. В вероятностных терминах стойким считается алгоритм, для которого перехват зашифрованных сообщений не приводит к появлению точки единственного принятия решения об используемом или переданном открытом сообщении.

При традиционном подходе стойкость алгоритма шифрования определяется стойкостью к известным видам криптографических атак, применяемых с целью прочтения, замены зашифрованного сообщения или вычисления ключа шифрования.

При определении стойкости алгоритма шифрования проводится тестирование алгоритма. И, прежде всего, это связано со статистическим анализом. Исследуются возможности взлома алгоритма шифрования на основе изучения статистических закономерностей в зашифрованных текстах. Как правило, при этом проводится статистический анализ, который включает: построение гистограмм, вычисление корреляций (в вертикальном, горизонтальном и диагональном направлениях) двух соседних пикселей в зашифрованном изображении, анализ ключевого пространства и анализ информационной энтропии. Кроме этого, определяется чувствительность алгоритма к исходному изображению,

которая определяется при использовании параметров: процент пикселей, изменивших значения, и среднее значение интенсивности.

Гистограммы изображения, построенные нами для красного, зеленого и синего цветов тестового цветного изображения «Lena», значительно различаются для исходного и зашифрованного изображения. При этом для исходного изображения на гистограммах имеются хорошо различимые пики для определенной яркости цвета, причем для каждого компонента пики находятся на разных интенсивностях. Для зашифрованного же изображения характерно равномерное распределение яркости цвета, поэтому нельзя точно сказать, какой цвет является преобладающим в зашифрованном изображении, а, следовательно, анализ гистограммы не может дать злоумышленникам информации об исходном распределении пикселей по цветам.

Коэффициент корреляции показывает взаимосвязь двух соседних пикселей в изображении. Вычисление коэффициентов корреляции производилось нами для тестовых изображений «Lena», «Peppers», «Salvador Daly»в горизонтальном, вертикальном и диагональном направлениях. Полученные данные показали, что коэффициенты корреляции соседних пикселей для исходного изображения стремятся к 1, а коэффициенты корреляции для зашифрованного изображения стремятся к 0. Это означает, что при зашифровании изображений происходит снижение корреляции пикселей и уменьшается взаимосвязь соседних пикселей.

По Шеннону, как известно, энтропия или информационная энтропия является мерой неопределенности, связанной со случайной величиной. Она дает количественную оценку информации, содержащейся в данных, как правило, в битах. Если источник выдает 2^8 символов с равной вероятностью, тогда энтропия такого случайного процесса будет равна 8. Как показали полученные нами при анализе результаты, для каждого компонента цвета энтропия в зашифрованном изображении стремится к идеальному, равному восьми, значению. Это означает, что визуально и по значениям энтропии зашифрованных изображений практически невозможно определить исходное изображение, что вызывает доверие к рассматриваемому алгоритму изображений.

Чувствительность алгоритма шифрования к исходному изображению, которая связана с изменением одного пикселя в исходном изображении, определялась нами при использовании параметров: процент пикселей, изменивших значение и среднее значение интенсивности для каждого цветового компонента в зашифрованном тестовом изображении.

Полученные значения параметров незначительно изменяются относительно идеальных значений, что подтверждает чувствительность алгоритма к малым изменениям в исходном изображении. Приведенные количественные результаты тестирования показали стойкость рассмотренного алгоритма шифрования с использованием хаотической динамики. Таким образом, рассмотрены основные принципы обеспечения защиты информации с использованием хаотической динамики.

УПРАВЛЯЕМЫЕ КОММУТАТОРЫ USB-КАНАЛА СЕМЕЙСТВА «ПРЕРЫВАТЕЛЬ»

В.А. ТЮНИН
Закрытое акционерное общество «ОКБ САПР»

В статье рассматривается назначение, внутренняя структура, принципы функционирования устройств семейства «Прерыватель», разработанных в ОКБ САПР. Описаны

различные области применения этих изделий: автоматизированное тестирование USB-устройств, управление подключением и отключением программно-аппаратных «мобильных» СЗИ, USB 3.0-повторитель.

Ключевые слова: автоматизация тестирования, «мобильные» программно-аппаратные СЗИ, коммутатор USB-канала, USB 3.0-повторитель.

Важными особенностями шины USB являются возможность «горячего» подключения/отключения периферийных устройств и возможность питания от шины USB периферийных устройств. Эти особенности сыграли немалую роль в приобретении популярности интерфейсом USB. В настоящее время интерфейсом USB оснащено большинство средств вычислительной техники (СВТ). Для многих из этих СВТ интерфейс USB является единственным проводным коммуникационным интерфейсом.

Однако указанные особенности требуют от разработчиков USB-устройств приложения дополнительных усилий при тестировании этих функций [1]. Именно автоматизация тестирования USB-устройств была основной целью разработки в ОКБ САПР семейства изделий «Прерыватель», в которое входят два устройства: «Прерыватель 2.0» (Рис.1) и «Прерыватель 3.0» (Рис.2).

«Прерыватель 2.0» и «Прерыватель 3.0» представляют собой управляемые коммутаторы USB-канала, образованного устройством с ролью USB-Host с одной стороны и устройством с ролью USB-Device с другой стороны. Интерфейсом управления этих двух представителей семейства «Прерыватель» является USB 2.0. При помощи этого интерфейса управляющий компьютер общается с управляющим блоком на микроконтроллере и с его помощью может подавать команды на подключение и отключение информационных цепей и цепей питания управляемого USB-канала. Коммутация этих цепей может осуществляться как синхронно, так и независимо.

В коммутаторах питания (на Рис. 1 и Рис. 2 обозначены как SW2) управляемого USB-канала установлены датчики, которые следят за протекающим по ним токам и при превышении порога понижают напряжение и выдают сигнал в микроконтроллер, а он в свою очередь передаёт сообщение об этом событии в управляющий компьютер. Таким образом, источник питания защищается от токовой перегрузки (в том числе от короткого замыкания) в устройстве с ролью USB-Device.

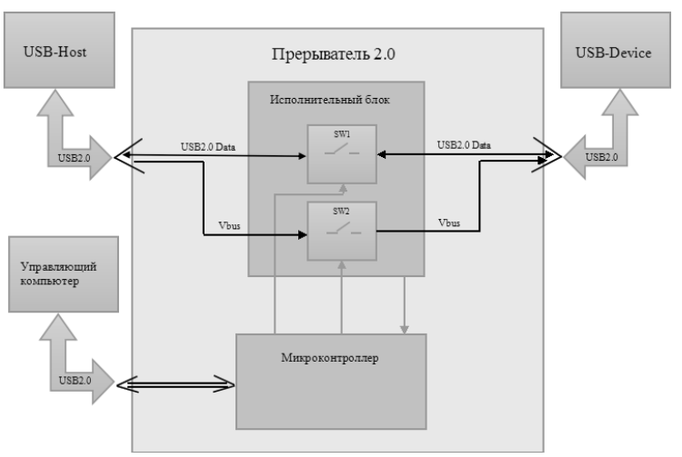


Рис. 1. Схема устройства «Прерыватель 2.0»

«Прерыватель 2.0» коммутирует USB-канал стандарта USB 2.0, а «Прерыватель 3.0» — USB 3.0.

Увеличение скорости передачи данных для стандарта USB 3.0 ужесточает требования к параметрам кабеля, влияющим на качество передачи информации, таким, как длина кабеля и качество его изготовления. Чтобы иметь возможность подстроиться под используемые кабели для получения максимальной производительности в «Прерывателе 3.0» применена микросхема эквалайзера-повторителя USB 3.0. Для совместимости в стандарте USB 3.0 оставлены цепи, удовлетворяющие стандарту USB 2.0, поэтому в «Прерывателе 3.0», кроме элемента коммутации, информационных цепей USB 3.0(на Рис. 2 обозначен как «Redriver USB 3.0») присутствует элемент коммутации информационных цепей USB 2.0(на Рис. 1 и Рис. 2 обозначены как SW1). Управление включением и отключением этих линий осуществляется независимо.

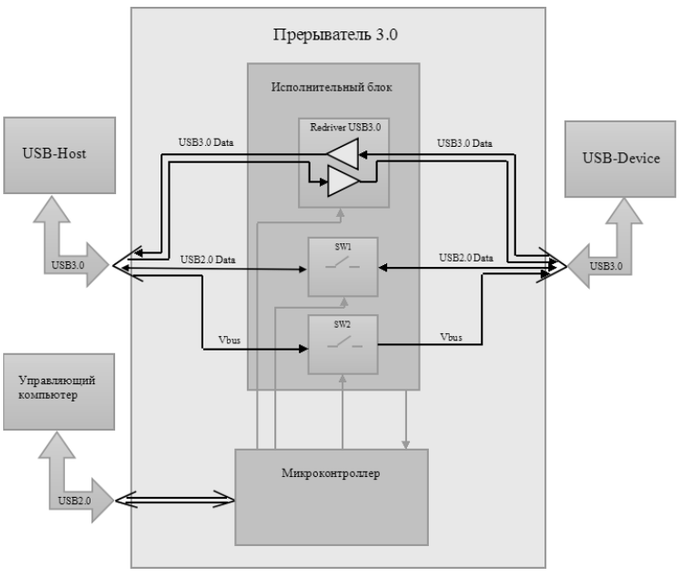


Рис. 2. Схема устройства «Прерыватель 3.0»

«Прерыватель 3.0» можно использовать для канала USB 2.0 вместо «Прерывателя 2.0», но следует помнить про порог ограничения тока в цепи питания, который для «Прерывателя 2.0» составляет 500 мА, а для «Прерывателя 3.0» — 900мА.

Как указано в [1], управляемые подключение и отключение информационных цепей и цепи питания USB-канала являются важными функциями при автоматизированном тестировании USB-устройств и управляемой блокировке доступа к USB-каналу «мобильным» программно-аппаратным СЗИ. «Прерыватель» во втором случае можно рассматривать как исполнительный элемент СЗИ, которое разрешает или запрещает использование данного USB-канала. В качестве «управляющего компьютера» может быть любое СВТ, способное работать в роли USB-Host с соответствующим программным обеспечением. Функции «управляющего компьютера» может исполнять СВТ, которому принадлежит управляемый USB-канал.

Схема стенда для тестирования USB-устройств представлена на Рис. 3. Персональный компьютер ПК1 выполняет функции «управляющего компьютера». «Прерыватель» устанавливается «в разрыв» между персональным компьютером ПК2 и USB-устройством,

и все вместе они образуют управляемый USB-канал. ПК1 даёт указания «Прерывателю» на подключение и отключение USB-устройства к ПК2 и отслеживает превышение тока в цепях питания управляемого USB-канала.

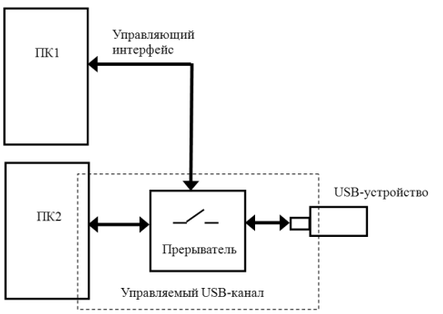


Рис. 3. Схема стенда для тестирования USB-устройств с двумя персональными компьютерами

В схеме на Рис. 4 в качестве управляющего USB-Host и управляемого USB-Host использованы USB-порты одного и того же персонального компьютера.

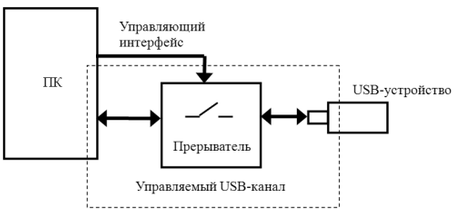


Рис. 4. Схема стенда для тестирования USB-устройств с одним персональным компьютером

В схеме на Рис. 5 «Прерыватель» помещён внутри персонального компьютера, в качестве управляющего USB-Host и управляемого USB-Host использованы внутренние USB-порты этого ПК, а на внешний разъём выведен USB-порт «Прерывателя» для подключения управляемого USB-устройства. Специальное ПО при необходимости может включать и выключать по заданному алгоритму присоединённые к данному разъёму USB-устройства и «мобильные» программно-аппаратные СЗИ (например, СН «Секрет» [2] и ПСКЗИ ШИПКА [3] производства ОКБ САПР).

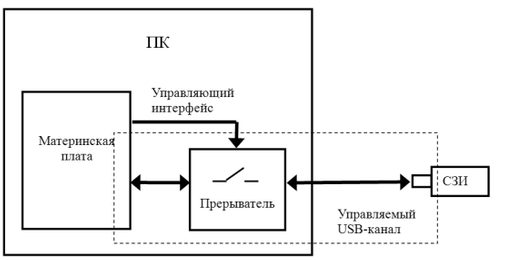


Рис. 5. Схема применения «Прерывателя» для коммутации USB-канала «мобильного» СЗИ

Способность восстанавливать амплитуду и форму сигналов информационных цепей USB 3.0 позволяет использовать «Прерыватель 3.0» в качестве повторителя в канале USB 3.0 для увеличения расстояния от источника до потребителя. При этом «Прерыватель 3.0» питается со стороны USB-Host управляемого USB-канала, а параметры подключенных кабелей берутся из энергонезависимой памяти микроконтроллера, куда они помещаются на этапе настройки канала через USB-интерфейс «управляющего компьютера». После настройки для исполнения роли повторителя «Прерыватель 3.0» работает автономно, без подключения к «управляющему компьютеру».

Развитием семейства изделий «Прерыватель» может стать дополнение его устройствами с интерфейсами с «управляющим компьютером», отличными от USB 2.0, а также устройствами, у которых функции управляющего компьютера выполняет управляющий микроконтроллер, к которому подключены необходимые средства ввода и отображения информации.

СПИСОК ЛИТЕРАТУРЫ

1. *Каннер Т. М.* Коммутатор USB-канала как техническое средство для тестирования программно-аппаратных СЗИ // Комплексная защита информации: материалы XXI научно-практической конференции, Смоленск, 17–19 мая 2016 г., — Москва, 2016 год
2. Специальный съёмный носитель информации. Патент на полезную модель № 94751. 27.05.2010, бюл. № 15.
3. Мобильное устройство защиты информации. Патент на полезную модель № 83862. 20.06.2009, бюл. № 17.

ПРОБЛЕМЫ РЕАЛИЗАЦИИ РАЗГРАНИЧЕНИЯ ДОСТУПА К ФУНКЦИЯМ УПРАВЛЕНИЯ ВИРТУАЛЬНЫХ СРЕД

Д. В. УГАРОВ, Д. А. ПОСТОЕВ
Закрытое акционерное общество «ОКБ САПР», Москва, Россия

Статья посвящена обзору проблем, которые возникают при реализации разграничения доступа к функциям управления виртуальных сред. Предложены требования к наложенному средству защиты информации, позволяющему избежать ограничений существующих решений.

Ключевые слова: виртуальная инфраструктура, виртуальная машина, разграничение доступа, сегментация виртуальных инфраструктур

В современных условиях реализация разграничения доступа к объектам инфраструктуры является неотъемлемой частью процесса построения защищенной информационной системы. Однако, несмотря на то, что для этого уже разработано множество моделей безопасности, независящих от конкретной информационной системы, большинство реализаций на практике имеют изъяны.

Не обошла эта проблема и виртуальные инфраструктуры, где мы сталкиваемся со следующим фактом:

Администратор виртуальной инфраструктуры (АВИ) имеет максимальный уровень доступа ко всем объектам (в числе которых могут находиться ВМ, обрабатывающие информацию, различную как по уровню секретности, так и категориям доступа) и функциям управления информационной системы.

Какие проблемы это принесет архитектору при проектировании системы?

1. Для виртуальных сред в настоящее время не предусмотрено разделение ролей АВИ, то есть того, кто управляет объектами информационной системы, и администратора безопасности информации (АБИ), того, кто назначает права пользователям системы, в том числе и АВИ. Таким образом, возникает ситуация сосредоточения максимальных привилегий в рамках одной роли (пользователя), то есть **проблема «суперпользователя»**.

   Для большинства систем такое положение неприемлемо, АБИ должен иметь возможность ограничивать действия АВИ: запрещать критичные для безопасности действия и разрешать некоторые только по согласованию, например, к удалению виртуальной машины (нарушение целостности и доступности) или экспорту ее на диск (нарушение конфиденциальности).
2. Так как система может содержать различную информацию (иерархически категорируемую, то есть разного уровня секретности или неиерархически, то есть разного вида), может возникнуть ситуация, при которой она будет «перемешана». Например, случайное или умышленное переключение секретной ВМ в подсеть к несекретным или миграция ВМ разработчика на хранилище бухгалтерии.

К сожалению, данная задача не может быть решена средствами самой виртуальной инфраструктуры, так как существующие продукты не предполагают мандатного механизма разграничения доступа, а сетевого сегментирования (с помощью VLAN или средствами межсетевых экранов) недостаточно в случае, если необходимо обеспечить не только изоляцию сети, но и изоляцию среды обработки информации и средств ее хранения. По этой причине архитектор сталкивается **с проблемой сегментирования**, то есть разбиения системы на сегменты и обеспечения их изоляции.

Что приходится делать для решения рассмотренных задач в настоящее время?

Устранять проблему «суперпользователя» приходиться организационными мерами, например, заменять учетную запись АВИ на аналогичную с урезанными правами, а учетные данные «суперпользователя» запечатывать в конверте до возникновения нештатных ситуаций. Однако это не решает проблемы полностью, а только переносит ее на иной уровень. Более того, в больших инфраструктурах это и вовсе может быть неприменимо из-за необходимости частого доступа к вырезанным у АВИ функциям и их постоянного согласования с АБИ.

В свою очередь, на решение проблемы сегментирования претендуют следующие способы:

1. Полное физическое разделение, то есть под каждый сегмент (в нашем случае это ВМ бухгалтерии и разработчика, а также ВМ с секретными и несекретными данными) выделить отдельные сервера, не имеющие связи между собой (чтобы АВИ при желании не мог выполнить неправильное действие).

   Минус такого подхода заключается в значительно возрастающих расходах на оборудование. Помимо этого, разделение приведет к снижению эффективности использования физических ресурсов (инфраструктура более разрознена), что скажется на эффективности балансировки нагрузки и отказоустойчивости.
2. Для каждого сегмента сделать отдельную учетную запись АВИ.

   Недостаток такого способа в значительном увеличении количества учетных записей (например, вместо 1 учетной записи АВИ в нашем случае получим 4) и усложнении работы с системой (в частности отслеживании состояния всей системы).

Что в итоге?

Из рассмотренных решений следует, что они ведут либо к дополнительным значительным затратам ведущим к снижению эффективности использования средств виртуализации, либо к введению дополнительных организационных мер усложняющих работу АВИ. По этой причине логичным шагом является перенимание опыта из смежных областей и создание наложенного средства защиты для ухода от описанных проблем.

При этом данное средство защиты должно реализовывать:

- разграничение доступа к функциям управления виртуальной инфраструктурой, критичным, с точки зрения безопасности;
- возможность создания нескольких ролей (пользователей), между которыми будут разделены полномочия по управлению виртуальной инфраструктурой, а также осуществлять контроль назначения прав доступа с помощью отдельной учетной записи АБИ, которая имеет права только на чтение в рамках виртуальной системы;
- мандатную политику безопасности и изолировать доступ к разным сегментам информационной системы на основе иерархических и неиерархических меток;

В заключение отметим, что разработчикам СЗИ, в свою очередь, стоит обратить внимание на данную сферу, так как, несмотря на популярность систем виртуализации, решения для большинства сред до сих пор отсутствуют.

АВТОНОМНОЕ УСТРОЙСТВО ЛИЦЕНЗИРОВАНИЯ

А. Ю. ЧАДОВ
МФТИ

В тезисах описывается реализация механизма активации лицензий с использованием автономного устройства.

Ключевые слова: лицензия, ключ лицензии, код активации.

Некоторые продукты существуют в программном виде без жесткой привязки к аппаратной части. Пользователь покупает несколько копий продукта (для работы на соответствующем количестве рабочих станций), которые будут действовать в течение определённого времени. Если покупатель хочет установить продукт на большее количество рабочих станций или продолжить работать с ним после окончания срока действия, он должен оплатить покупку дополнительных копий. Механизм лицензирования позволяет проконтролировать, что продукт не будет использоваться по окончании срока действия и что будет задействовано не более того количества копий, которое было оплачено.

Лицензия — это разрешение на пользование продуктом. Приобретая такое разрешение, пользователь получает возможность работать с программным комплексом. Если попытаться использовать продукт без лицензии, то работать с ним будет затруднительно: может быть ограничена функциональность продукта, он может не запуститься или не установиться. В данном случае приобретение, собственно, лицензии и означает покупку единицы продукта [1].

Для того чтобы защититься от нелегального использования ПО, правообладателю необходимо применять защитные механизмы, контролирующие наличие у конечного пользователя разрешения на работу с данной копией продукта. Эти механизмы, как

и алгоритмы их обхода, постоянно совершенствуются. Как только появляется способ обойти старый механизм защиты, или он просто становится неудобным, появляются новые, компенсирующие недостатки старого [2].

Самый простой из таких механизмов защиты — выдавать пользователю сгенерированный по специальному алгоритму ключ, который он передаст программе. Очевидный недостаток — ключ может быть украден и в дальнейшем использован на другом компьютере.

Другой способ — использование USB-ключа. Защита в этом случае основана на том, что встроенные в ПО инструменты проверяют наличие подключенного USB-устройства. Однако эмулировать его не намного сложнее, чем введение лицензионного ключа [3].

Ещё один механизм выглядит следующим образом:

1. Покупатель приобретает ключ лицензии — уникальный набор данных и копию ПО.
2. Устанавливает на свой компьютер ПО.
3. Пользователь — самостоятельно или с помощью встроенных в ПО инструментов — собирает некую информацию о компьютере (идентификатор оборудования).
4. Ключ лицензии и идентификатор оборудования передаются фирме-продавцу.
5. Фирма-продавец высылает пользователю код активации — закодированное «разрешение» программе запуститься, если пользователь имеет «на руках» определенный ключ и определенный идентификатор оборудования [4].

Интересным моментом в этой схеме является передача данных фирме-продавцу и обратно. Это может быть реализовано двумя способами: автоматизированная передача через интернет при помощи сервера лицензирования, который затем автоматически сгенерирует и вышлет код активации или передача информации сотруднику фирмы-продавца (по телефону, почте, через интернет).

Оба способа имеют свои недостатки.

В первом случае необходима настройка и поддержание сервера лицензирования. Также, что важно, требуется обязательное наличие соединения с сетью интернет у клиента. Это серьёзная проблема, если фирма-покупатель не имеет выхода в интернет в силу каких-либо особенностей своей деятельности.

Во втором случае процесс активации лицензии может оказаться растянутым, занимать время и ресурсы сотрудников, которым приходится этим заниматься.

В данной статье описан новый вариант реализации механизма активации. Это устройство, решающее задачу выдачи, создания и активации лицензии без подключения к сети интернет и привлечения к процессу сотрудников фирмы-производителя и задачу защиты от нелегального использования ПО. Использование автономного устройства позволяет избежать недостатков других механизмов: нет необходимости в соединении с сетью интернет, нет необходимости участия сотрудников фирмы-продавца или развертывании сервера лицензирования в привычном смысле слова.

Процесс работы с устройством устроен следующим образом.

Если фирма-покупатель хочет использовать определённое количество копий продукта, она оплачивает нужное количество лицензий, получает у фирмы-продавца установочное ПО и устройство лицензирования, которое может выдать данное число лицензий на нужный продукт. Далее покупатель устанавливает ПО на рабочие станции и активирует лицензии при помощи устройства. Таким образом, нет необходимости хранить и использовать коды активации лицензии или получать файл лицензии от фирмы-производителя, соединение с интернетом так же не требуется.

Функционал устройства

Основная функция устройства — активация лицензии. Для защиты от копирования файла лицензий устройство использует механизм электронной подписи. Две ключевые пары генерируются на этапе создания устройства (ключевая пара для создания файла лицензии (КПдСФЛ) и ключевая пара для обмена лицензиями (КПдОЛ)). Ключи проверки подписи ключевых пар устройства подписываются для последующей проверки их подлинности. Для этого на этапе создания используется мастер-устройство: на его ключах подписи подписываются ключи проверки подписи, полученные подписи кладутся в устройство вместе с ключом проверки подписи мастер-устройства. Таким образом, гарантируется подлинность ключей проверки подписи устройства.

Подробнее алгоритм активации лицензии.

В процессе создания файла лицензии используются следующие данные, хранящиеся в устройстве:

- Ключевая пара для создания лицензии (КПдСФЛ).
- Подпись ключа проверки подписи КПдСФЛ на ключе подписи мастер-устройства.
- Уникальный идентификационный номер лицензии — список таких номеров заносится в устройство вместе с данными о количестве лицензий, которое оно может выдать.
- Название фирмы-производителя.
- Идентификационный номер устройства.

Устройство получает от установленного ПО данные для создания файла лицензии и добавляет к ним данные, хранящиеся в устройстве: идентификационный номер лицензии, название фирмы-продавца, название продукта, идентификационный номер устройства, затем всё это подписывается на ключе подписи КПдСФЛ.

Все подписанные устройством данные вместе с подписью, ключом проверки подписи КПдСФЛ и его подписью на ключе подписи мастер-устройства и есть лицензия.

Продукт принимает лицензию, проверяет подписи, сверяет данные и таким образом удостоверяется, что лицензия корректна.

Дополнительно в устройстве присутствует функция обмена лицензиями. Обмен лицензиями может использоваться интегратором для перераспределения количества лицензий на устройствах перед продажей, или пользователем для распределения между разными отделами или филиалами фирмы. Обмен происходит между двумя устройствами: устройством-получателем лицензий и устройством-отправителем. Процесс состоит из трёх шагов:

1. устройство получатель генерирует и посылает запрос устройству-отправителю
2. устройство-отправитель уменьшает у себя число доступных лицензий, генерирует пакет передачи лицензий и посылает его обратно
3. устройство-получатель принимает пакет и добавляет лицензии.

В этом процессе используются следующие данные, хранящиеся в устройствах.

Для устройства-получателя:

- Уникальный идентификационный номер устройства.
- Значение счётчика пополнения лицензий. Счётчик увеличивается каждый раз, когда данное устройство получает лицензии от другого устройства. Позволяет избежать повторного использования сгенерированного пакета передачи лицензий.

Для устройства-отправителя:

- Уникальный идентификационный номер устройства.
- Ключевая пара для обмена лицензиями (КПдОЛ), использующаяся для подписи сообщений, которыми устройства обмениваются в процессе передачи.
- Ключ проверки подписи мастер-устройства.

– Подпись ключа проверки подписи КПдОЛ на ключе мастер-устройства.

Рассмотрим подробнее этапы передачи:
1) Создание запроса на получение лицензии.
Запрос состоит из следующих данных:
– Идентификационный номер устройства
– Значение счётчика пополнения лицензий
– Число лицензий
– Название продукта, для которого запрашиваются лицензии

Число лицензий и название продукта вводится пользователем, идентификационный номер и значение счётчика хранятся внутри устройства.
2) Передача запроса от устройства-получателя лицензий к устройству-отправителю.
3) Создание пакета передачи лицензий:

Получив запрос, устройство-отправитель проверяет, что оно может выдать достаточное количество лицензий, затем создаёт пакет передачи. В него включены следующие данные:
– Идентификационный номер устройства-получателя
– Значение счётчика пополнения лицензий устройства-получателя
– Идентификационный номер устройства-отправителя
– Число лицензий, которые необходимо добавить
– Имя продукта
– Подпись на ключе подписи КПдОЛ устройства-отправителя данных из пунктов 1–5
– Ключ проверки подписи ключевой пары обмена устройства-отправителя.
4) Передача сформированного пакета в устройство-получатель.
5) Приём пакета передачи и установка лицензий в устройство:
Устройство-получатель принимает пакет, и проводит несколько проверок:
– проверяет подпись ключа проверки лицензии КПдОЛ устройства-отправителя
– проверяет подпись данных
– проверяет корректность самих данных.

Если всё верно, добавляет лицензии и увеличивает на единицу значение счётчика пополнения лицензий.

Пользователь может установить PIN-код, тогда операции создания лицензии и передачи лицензий будут запрашивать PIN-код перед началом работы.

Итог

Таким образом, автономное устройство лицензирования — продукт для удобной и быстрой работы с лицензиями, лишённый недостатков других механизмов контроля лицензий. Использование ЭП для активации лицензии и хранения ключей подписи внутри устройства позволяет защититься от несанкционированного копирования и повторного использования файла лицензии, использование автономного устройства позволяет не подключаться к интернету для активации лицензии и не связываться с сотрудниками фирмы-производителя в процессе активации лицензии. Появится возможность продавать лицензии интеграторам и не участвовать в их дальнейшей передаче конечным покупателям без риска потери контроля за распространением ПО.

СПИСОК ЛИТЕРАТУРЫ

1. Лицензия на программное обеспечение. [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Лицензия_на_программное_обеспечение (дата обращения: 10.05.2015).

2. К вопросу защиты авторских прав. [Электронный ресурс]. URL: http://www.okbsapr.ru/schastniy_2008_3.html (дата обращения: 10.05.2015).
3. Защита ПО от нелицензионного использования. [Электронный ресурс]. URL: http://www.okbsapr.ru/sol6.html (дата обращения: 10.05.2015).
4. Асимметричная криптография при лицензировании подписочного ПО на практическом примере. [Электронный ресурс]. URL: http://habrahabr.ru/post/123908/ (дата обращения: 10.05.2015).

ОСНОВНЫЕ НАПРАВЛЕНИЯ НАУЧНО-ТЕХНИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

А.Г. ШУМИЛИН
Государственный комитет по науке и технологиям Республики Беларусь

В современном мире с каждым годом стремительно растет количество, интенсивность и сила воздействия кибератак. По результатам отчета глобального исследования о состоянии и перспективах развития сферы информационной безопасности в мире в 2015 году, проведенного компанией PwC[1], общее число подтвержденных и выявленных инцидентов в области информационной безопасности возросло на 37 % по сравнению с прошлым годом. Совокупный финансовый ущерб от всех видов инцидентоввозрос в среднем на 27 %, расходы на обеспечение информационной безопасности возросли на 24 % за тот же период.

Однако широко используемые методы предупреждения и обнаружения киберугроз в ряде случаев оказываются неэффективны в противостоянии высокоорганизованным интеллектуальным киберугрозам.

В связи с эти проблемы защиты информационной безопасности приобретают все большую актуальность. Инциденты в сфере информационной безопасности оказывают влияние на деятельность не только бизнес-сообществ, но и на систему государственного управления, военную сферу и др. Не только государственные и военные информационные ресурсы и системы требуют комплексной защиты информации, необходимо также обеспечить такую защиту коммерческих, банковских и персональных данных.

В Республике Беларусь государство создало и поддерживает комплексную систему обеспечивающую процесс информационной защиты информационных ресурсов и систем на разных уровнях управления. Концептуальные положения этой системы отражены в рамках Концепции национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 09.11.2010 № 575 [2].

В целях реализаций положений Концепции национальной безопасности Республики Беларусь, для обеспечения противодействия использованию потенциала информационно-коммуникационных технологий в целях угрозы национальным интересам Республики Беларусь, в 2011–2015 годах Государственный комитет по науке и технологиям Республики Беларусь сформировал и координировал выполнение государственной научно-технической программы «Развитие методов и средств системы комплексной защиты информации» (ГНТП «Защита информации — 2»). В рамках этой программы научными

коллективами семи научно-исследовательских организаций Республики Беларусь выполнено 14 заданий, продолжаются работы еще по двум заданиям. Фактический объем финансирования НИОКР данной программы за вышеуказанные годы составил более 26 млрд руб. Учеными Беларуси в сфере защиты информации создано 18 новшеств, наиболее значимые из них: локатор для обнаружения устройств несанкционированного съема информации ЛВ-2Р, комплекс проверки вычислительной техники на наличие аппаратных средств недекларированных возможностей.

В результате выполнения ГНТП «Защита информации — 2» получены результаты высокого мирового уровня, которые подтверждаются как научными публикациями в рецензируемых международных научных изданиях, так и востребованностью полученных результатов в виде внедренных разработок.Освоен выпуск инновационной продукции на общую сумму около 1,5 млн долл. США: генератор электромагнитного шума, устройство защиты от ВЧ-навязывания по телефонным линиям, сети питания, охранной и пожарной сигнализации, евро-совместимый сверх полостной сетевой помехоподавляющий фильтр, аппаратно-программный комплекс криптографической защиты стандартных цифровых потоков Е 1, метод обнаружения устройств записи речевой информации по электрическому и магнитному излучению электроакустических преобразователей в результате воздействия тестового акустического сигнала. Разработанные технологии и созданные приборы используются при проведении дальнейших исследований и разработок по автоматизации процессов подготовки и аттестации систем защиты информации информационных систем, как государственных органов, так и частного бизнеса. В подготовленных проектах стандартов определены подходы к оценке уровня информационной безопасности и установлены требования к безопасным информационным системам.

В 2016–2020 годы научные исследования в данной области будут продолжены в рамках ГНТП «Защита информации — 3», в которую в настоящее время включено 16 проектов заданий.

Выполнение научных исследований в области информационной безопасности, разработка методов и систем защиты информации требуют высоког24о уровня компетенций от специалистов в данной области.

В Республике Беларусь сформирована многоуровневая система подготовки кадров в области информационной безопасности:

- на первом базовом уровне — высшие учебные заведения Республики Беларусь выполняют подготовку специалистов по ряду специальностей направления «Информационная безопасность»;
- на втором — в рамках системы последипломного образования, специалисты органов государственного управления и реального сектора экономики повышают квалификацию на курсах переподготовки в области информационной безопасности;
- на третьем — формируется кадровый потенциал научного направления «Защита информации», отвечающий по своим количественным и качественным параметрам современным потребностям развития отрасли.

В 2011–2015 годах по специальности 05.13.19 «Методы и системы защиты информации. Информационная безопасность» защитили диссертационные работы и получили ученую степень 1 доктор технических наук и 28 кандидатов технических наук.

Перспективными направлениями научно-технической деятельности в сфере защиты информации являются следующие направления: криптографическая защита информации, разработка технических нормативных правовых актов в области информационной безо-

пасности, защита информации в трансграничном электронном документообороте, защита от уязвимостей в компьютерных сетях, стеганографические системы защиты информации.

ЛИТЕРАТУРА

1. The Global State of Information Security® Survey 2016 [Electronic resource] // Pricewaterhouse-Coopers. — Mode of access: http://www.pwc.com/gsiss. — Date of access: 29.03.2016.
2. Об утверждении Концепции национальной безопасности Республики Беларусь: Указ Президента Респ. Беларусь, 9 нояб. 2010 г., № 575 // Нац. реестр правовых актов Респ. Беларусь. — 2010. — № 276. — 1/12080.

РЕЗОЛЮЦИЯ XXI НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ «КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ»

С 17 по 19 мая 2016 г. в г. Смоленске состоялась XXI научно-практическая конференция «Комплексная защита информации» как мероприятие Союзного государства. Организаторы конференции: Парламентское Собрание Союза Беларуси и России, Постоянный Комитет Союзного государства, аппарат Совета Безопасности Российской Федерации. Организационную поддержку мероприятию оказали: Администрация Смоленской области, МОО «Ассоциация защиты информации», Медиа Группа «Авангард», Государственное предприятие «НИИ ТЗИ».

В работе конференции приняли участие свыше 100 представителей Беларуси и России. Среди участников конференции члены-корреспонденты (различных академий), доктора и кандидаты наук, профессора, доценты и старшие научные сотрудники, а также специалисты — практики, руководители государственных и коммерческих организаций, специализирующихся на вопросах выработки научно-практических решений в сфере информационной безопасности.

На пленарных и секционных заседаниях было заслушано и обсуждено более 65 докладов ученых, специалистов, представителей государственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных и практических направлений в области информационной безопасности, в том числе 10 докладов в рамках «Школы молодых ученых». Осуществлялся обмен опытом по вопросам использования защищенных информационных технологий в различных сферах жизни общества и государства.

На Конференции были обсуждены следующие темы:

- Актуальные вопросы информационной безопасности в Союзном государстве
- Вопросы стандартизации в области безопасности информации
- Актуальные проблемы кадрового обеспечения в области информационной безопасности
- Вопросы создания трансграничного пространства доверия
- Актуальные проблемы создания технических средств защиты информации
- Проблемы противодействия компьютерной преступности
- Новые идеи и подходы к обеспечению безопасности информационных технологий
- Защита автоматизированных систем управления технологическими процессами

Конференция отмечает:

- Необходимость дальнейшего развития совместных работ научных коллективов России и Беларуси по развитию современных информационных технологий в интересах создания новых защищенных импортозамещающих платформ.
- Необходимость развития профильного образования и популяризации профессий в области информационной безопасности.
- Принимая во внимание актуальность создания и развития трансграничного пространства доверия в Беларуси и в России, целесообразность активизации взаимодействия в данной области, включая законотворческую деятельность по данной проблематике в рамках Парламентского Собрания Союза Беларуси и России.

– Актуальность решения проблемы обеспечения защищенности персональных данных с использованием перспективных высоких технологий.
– Перспективность предложенной российскими учеными архитектуры компьютеров, характеризующейся высоким уровнем «вирусного иммунитета».
– Актуальность разработки системы сертификации специалистов как объективной основы подбора и расстановки кадров, включая разработку методик оценки лояльности и профессиональных компетенций кадров в отрасли информационной безопасности.

Положительной оценки заслуживает практика проведения в рамках Конференции «Школы молодых ученых» как одной из форм продвижения и поддержки перспективных специалистов, укрепления их интереса к научной работе в области информационной безопасности.

Участники конференции считают, что состоялся плодотворный обмен опытом по проведению исследований и разработок, а также внедрению теоретических и практических результатов в области информационной безопасности.

Участники конференции постановили:

1. Одобрить работу XXI научно-практической конференции «Комплексная защита информации».
2. Поддержать концепцию новой программы Союзного государства «Совершенствование системы защиты информационных ресурсов Союзного государства и государств-участников Договора о создании Союзного государства в условиях нарастания угроз в информационной сфере» на 2016–2020 годы (Паритет-2020).
3. Провести XXII научно-практическую конференцию «Комплексная защита информации» в 2017 году в Республике Беларусь.
4. Просить Постоянный Комитет Союзного государства сформировать рабочую группу для подготовки и осуществления организационных мероприятий. При формировании тематики Конференции предусмотреть более широкое привлечение студентов и аспирантов вузов России и Беларуси к проведению «Школы молодых ученых», конкурса на лучший совместный российско-белорусский доклад в рамках Конференции.
5. Проинформировать руководство Постоянного Комитета Союзного государства и Парламентского Собрания Союза Беларуси и России об итогах XXI научно-практической конференции «Комплексная защита информации».
6. Организовать публикацию материалов Конференции в третьем квартале 2016 года с целью популяризации и привлечения широкого внимания к затронутым проблемным вопросам.

Принята на пленарном заседании
19 мая 2016 г.
г.Смоленск

СОДЕРЖАНИЕ

ДЛЯ ЗАМЕТОК

Научное издание

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXI научно-практической конференции

17–19 мая 2016 года, г. Смоленск

Верстальщик *Н. С. Мельников*
Подписано в печать 21.07.2016. Формат 60×84 1/8.
Бумага офсетная. Ризография.
Тираж 100 экземпляров.

ООО «Медиа Группа «Авангард»
Россия, Москва, 127473, 3-й Самотечный пер., д. 21
www.avangardpro.ru