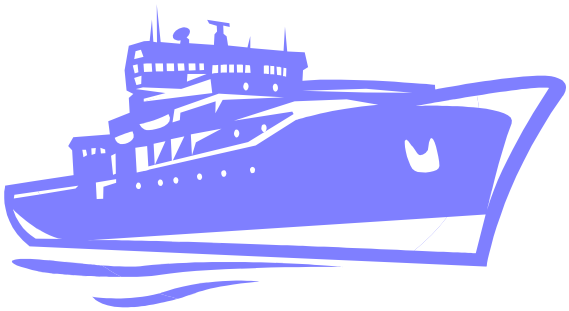
МЕТОДЫ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Материалы XVIII
научно-технической конференции

29 июня - 02 июля 2009 года



Санкт-Петербург
2009

ОРГАНИЗАТОРЫ КОНФЕРЕНЦИИ

Министерство образования и науки РФ; Комитет по информатизации и связи Правительства Санкт-Петербурга; Комитет по науке и высшей школе Правительства Санкт-Петербурга; Санкт-Петербургский государственный политехнический университет; Московский государственный инженерно-физический институт (государственный университет); Институт криптографии, связи и информатики Академии ФСБ РФ; МОО «Ассоциация Защиты Информации»; ЗАО «РНТ»; ЗАО «НПП «СТЗИ»; ЗАО «ГОЛЛАРД»; ЗАО «РЦЗИ «ФОРТ»; ЗАО «Инфосистемы Джет»; НИИАС; ИПИ РАН; ООО «НеоБИТ».

ОРГКОМИТЕТ КОНФЕРЕНЦИИ

- *ЗЕГЖДА П.Д. – Д.Т.Н., ПРОФЕССОР,* ***ПРЕДСЕДАТЕЛЬ***
- *РУДСКОЙ А.И., ЧЛЕН-КОРРЕСПОНДЕНТ РАН, ПРОРЕКТОР ПО НАУЧНОЙ И ИННОВАЦИОННОЙ ДЕЯТЕЛЬНОСТИ ГОУ «СПБГПУ»,* ***СОПРЕДСЕДАТЕЛЬ***
- *ВАСИЛЬЕВ Ю.С., АКАДЕМИК РАН, ПРЕЗИДЕНТ ГОУ «СПБГПУ»*
- *ГЛУХОВ В.В., Д.Т.Н., ПРОФЕССОР, ПРОРЕКТОР ПО УЧЕБНОЙ РАБОТЕ ГОУ «СПБГПУ»*
- *АДАДУРОВ С.Е., Д.Т.Н., ДИРЕКТОР ОАО «НИИАС»*
- *БАРАНОВ А.П., Д.Т.Н., ЦЕНТР БЕЗОПАСНОСТИ ФСБ РОССИИ*
- *ДУХВАЛОВ А.П., ГЛАВНЫЙ АРХИТЕКТОР ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»*
- *МАКСИМОВ А.С., К.Т.Н., ПРЕДСЕДАТЕЛЬ КОМИТЕТА ПО НАУКЕ И ВЫСШЕЙ ШКОЛЕ ПРАВИТЕЛЬСТВА САНКТ-ПЕТЕРБУРГА*
- *ЕМЕЛЬЯНОВ Г.В., К.Ф.-М.Н., ПРЕДСЕДАТЕЛЬ СОВЕТА МОО «АССОЦИАЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ»*
- *ГОРБАТОВ В.С., К.Т.Н., ПЕРВЫЙ ЗАМЕСТИТЕЛЬ ДЕКАНА ФАКУЛЬТЕТА "ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ", МИФИ*
- *НОВИКОВ А.А., К.Т.Н., ГЕНЕРАЛЬНЫЙ ДИРЕКТОР КОМПАНИИ «РНТ»*
- *ВАСИЛЬЕВ Г.Б., НАЧАЛЬНИК УПРАВЛЕНИЯ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ ПО СЕВЕРО-ЗАПАДНОМУ ФЕДЕРАЛЬНОМУ ОКРУГУ*
- *ПОЧАТКОВ А.Л., ЗАМЕСТИТЕЛЬ ПРЕДСЕДАТЕЛЯ КОМИТЕТА ПО ИНФОРМАТИЗАЦИИ И СВЯЗИ ПРАВИТЕЛЬСТВА САНКТ-ПЕТЕРБУРГА*
- *ВАСИЛЬЕВА Л.Б., НАЧАЛЬНИК УПРАВЛЕНИЯ ПО ЗАЩИТЕ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ РОССВЯЗЬКОМНАДЗОРА*
- *ШМИД А.В., Д.Т.Н., ПРОФЕССОР, ПРЕДСЕДАТЕЛЬ СОВЕТА ДИРЕКТОРОВ ЗАО «ЕС-ЛИЗИНГ»*
- *ТРИФАЛЕНКОВ И.А., К.Т.Н., ДИРЕКТОР ЦЕНТРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЗАО «ИНФОСИСТЕМЫ ДЖЕТ»*
- *СОКОЛОВ И.Г., АКАДЕМИК РАН, ДИРЕКТОР ИПИ РАН*
- *БУДЗКО В.И., Д.Т.Н., ПРОФЕССОР, ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ИПИ РАН*
- *ЭРКИН А.Г., ГЕНЕРАЛЬНЫЙ ДИРЕКТОР ЗАО «РЦЗИ «ФОРТ»*
- *ФЕДУЛОВ В.В., ЗАМЕСТИТЕЛЬ ДИРЕКТОРА МВП «СВЕМЕЛ»*
- *ИВАНОВА Е.Г., ВЕДУЩИЙ СПЕЦИАЛИСТ КОМИТЕТА ПО ИНФОРМАТИЗАЦИИ И СВЯЗИ ПРАВИТЕЛЬСТВА САНКТ-ПЕТЕРБУРГА*
- *РОМАНЕЦ Ю.В., ГЕНЕРАЛЬНЫЙ ДИРЕКТОР ООО ФИРМА «АНКАД»*

СПОНСОРЫ

- ***Главный спонсор конференции***
  ИБМ ВОСТОЧНАЯ ЕВРОПА/АЗИЯ
- ***Генеральный спонсор: ЗАО «ГОЛЛАРД»; ЗАО ««РЦЗИ «ФОРТ», ЗАО «Лаборатория Касперского», ЗАО «ЕС-ЛИЗИНГ»***
- ***Спонсор: ЗАО «НПП «СТЗИ»; ООО «НеоБИТ»;***
- ***Партнёр конференции: ОАО НИИАС, ИПИ РАН; ЗАО «РНТ»; МВП «СВЕМЕЛ»; ЗАО «Инфосистемы Джет»***

ВВЕДЕНИЕ

С каждым годом вопросам управления информационной безопасностью уделяется все больше внимания как со стороны ИТ, так и со стороны высшего руководства компаний. Последние исследования, проведенные компанией «Эрнст энд Янг», показали, что функция информационной безопасности становится все более важным элементом корпоративного управления.

Большинство экспертов отмечают относительно стабильное распределение сравнительной опасности угроз (см. Рис.) в области телекоммуникаций, что подчёркивает неослабевающую актуальность проблемы.

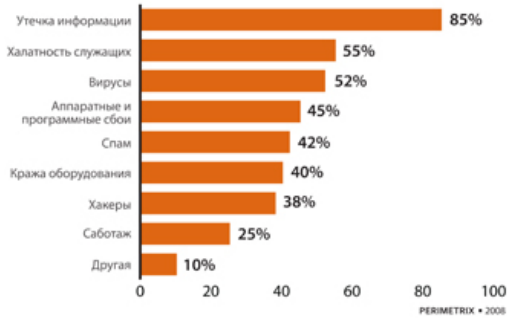


Рис. Наиболее опасные угрозы в области телекоммуникации

Как и в прошлом году, наиболее опасной угрозой внутренней ИБ была признана утечка информации, которую отметили более половины (55%) респондентов. Однако наибольший рост показала вторая по опасности угроза, связанная с искажением корпоративной (и преимущественно финансовой) документации. В нынешнем году её опасность подскочила сразу на 17% и практически сравнялась с опасностью утечек информации.

Не менее страшны и угрозы, исходящие от хакеров. Так, по заявлению генерала Д.Дэвиса, ответственность за кибер защиту в Пентагоне, за 6 месяцев Министерство обороны США потратило не менее 100 миллиона долларов на защиту своих сетей от хакеров.

Изложенное позволяет заключить, что в современных условиях актуальной проблемой при создании региональных защищённых информационных систем является интеграция усилий разработчиков с целью создания комплексных решений, адекватных современным угрозам и механизмам нарушения безопасности, в связи с чем конференция сопровождается выставкой, демонстрирующей опытные образцы перспективных систем защиты информации. Работа конференции охватывает следующие направления:

- Безопасность информационно-телекоммуникационных систем, созданных с использованием современных отечественных и зарубежных технологий и решений.
- Криптографические методы и средства в защите информации.
- Безопасность информационных систем государственных учреждений в свете закона о защите персональных данных.
- Анализ, контроль и управление безопасностью программного обеспечения.
- Проблемы подготовки кадров по информационной безопасности в условиях реформы высшей школы.

Учредителями конференции являются: **МОО «АЗИ», Комитет по информатизации и связи Правительства Санкт-Петербурга, Комитет по науке и высшей школе Правительства Санкт-Петербурга, ГОУ «СПбГПУ», ЗАО «НПП «СТЗИ», ООО «НеоБИТ», ЗАО «РНТ», ЗАО «РЦЗИ «ФОРТ», ЗАО «ГОЛЛАРД», ЗАО «Инфосистемы Джет», ООО «НПП «НТТ», Академия криптографии, Институт криптографии, связи и информатики Академии ФСБ РФ**.

Оргкомитет конференции

Раздел 1.
Современные технологии обеспечения безопасности информационных систем и телекоммуникаций

Раздел 1.1.
Перспективные направления в защите информационных систем

Баранов П.А.

ПРОБЛЕМЫ ЗАЩИТЫ ТЕРРИТОРИАЛЬНО РАЗНЕСЕННЫХ РАСПРЕДЕЛЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

г.Москва, Банк России

В настоящее время в России задача обеспечения защиты автоматизированных систем хранения и обработки данных (далее АС), характеризующихся сильной территориальной распределенностью их компонент и относительной самостоятельностью разработки отдельных узлов, подразумевает преодоление ряда трудностей, для которых разработчик системы защиты должен определить меры и способы их преодоления. Данное обстоятельство связано со следующими факторами:

- развитие информатизации общества и производственных процессов в России происходило неравномерно по регионам, и в значительной мере, стихийно;
- степень осознания угроз безопасности информации в компаниях и учреждениях стала повышаться только в последние годы, оставаясь на низком уровне все остальное время с момента проникновения информационных систем в производство;
- отсутствие или неприменимость отечественных разработок для ряда направлений реализации защиты информации;
- централизация управления, финансовых потоков, удаленность ряда регионов от центра и неодинаковая доступность региональных представительств ввиду различной пропускной способности каналов связи, часовых поясов, транспортной доступности.

Приводимые ниже тезисы и заключения основаны на опыте создания и сопровождения систем защиты информации централизованных АС, насчитывающих, помимо центральной компоненты, более 70 региональных узлов с разной степенью технической оснащенности, подготовки персонала, транспортной и информационной доступности.

В условиях необходимости обеспечения конфиденциальности, доступности и целостности данных, которыми оперирует автоматизированная система, следует предусматривать наличие угроз, количество которых постоянно увеличивается. Эти угрозы должны быть классифицированы с тем, чтобы в дальнейшем обеспечить возможность выбора средств защиты. На практике угрозы классифицируются по источнику (внешний или внутренний нарушитель, отказ в обслуживании со стороны оборудования, ошибки в программном обеспечении), по типу наносимого вреда: компрометирующие конфиденциальность информации (кража сведений), препятствующие ее доступности (отказ в обслуживании), нарушающие целостность данных (искажение передаваемых сообщений). После выбора критериев классификации следует создание модели угроз.

В зависимости от построенной модели угроз и характера защищаемой информации (ее критичности, приоритета обеспечения ее свойств) выбираются те или

иные инструменты защиты. При создании реальных систем защиты информации применяются встроенные средства защиты ОС/целевого ПО, средства разграничения доступа, аппаратно-программные средства защиты от несанкционированного доступа, средства защиты от вредоносного кода (антивирусные программы), средства шифрования трафика/сообщений, средства разграничения сетевых сегментов, средства контроля целостности состава программных ресурсов, функционирующих на узлах системы, средства контроля использования съемных носителей информации и использования портов ввода-вывода, организационные меры.

Специфика защиты информации в настоящее время такова, что организационные меры являются неотъемлемым элементом системы обеспечения информационной безопасности АС. Вместе с тем, опыт показывает, что при возможности контроля тех или иных путей нарушения информационной безопасности системы, как организационными мерами, так и с помощью аппаратных или программных автоматизированных средств защиты следует включать последние наряду с организационными мерами (при прочих равных показателях технической и экономической целесообразности внедрения автоматизированных средств).

При планировании разработки и регулировании хода внедрения комплекса защиты информации необходимо принимать во внимание отказоустойчивость самой системы обеспечения информационной безопасности. На практике данное свойство обеспечивается оборудованием горячего или холодного резерва, созданием резервных копий ПО/данных, обеспечением постоянного дежурства обслуживающего персонала.

Учитывая все вышесказанное следует заметить, что планирование и разработка решений по защите информации в период создания АС, нежели чем после создания АС, позволяет более адекватно оценить риски информационной безопасности, выработать схему взаимодействия средств защиты между собой и с остальными средствами АС и в конечном итоге избежать ограничений, накладываемых уже сложившейся инфраструктурой системы или объекта информатизации на спектр возможных для использования инструментов защиты.

Баранов Ю.А.

ИСПОЛЬЗОВАНИЕ СТАТИСТИЧЕСКОГО МЕТОДА АВТОРУБРИКАЦИИ ТЕКСТОВ ПРИ РЕАЛИЗАЦИИ МЕХАНИЗМА ТЕМАТИЧЕСКОГО РАЗГРАНИЧЕНИЯ ДОСТУПА К ТЕКСТОВЫМ ДОКУМЕНТАМ

г.Москва, ИПИ РАН

Требование разграничения доступа является одним из основополагающих моментов при создании информационно поисковых систем (ИПС), в которых обрабатывается конфиденциальная информация или информация ограниченного распространения. Методы и способы реализации этого требования могут быть различными в зависимости от степени жесткости ограничений.

Разработанная математическая модель и построенная на ее основании методика предлагается для применения при решении задачи информационной безопасности, состоящей в тематическом разграничении доступа.

Решение задачи разграничения доступа к сведениям ограниченного распространения, хранящимся в виде неструктурированных текстовых документов, может быть основано на разделении данных на тематические классы. Тематическое разграничение доступа к сведениям может заключаться в определении смысловой направленности запрашиваемого документа (авторубрикации), и принятии решения о доступе или отказа в доступе к нему пользователю. В этом случае решение принимается на основании таблицы доступа каждого пользователя к заранее созданным тематикам существующих в системе документов. Тогда, с целью автоматизации процесса принятия решения, подобная система разграничения доступа может быть основана на подсистеме автоматического определения тематики запрашиваемого документа.

Построение подсистемы автоматической рубрикации текстов, в свою очередь основывается, на определении меры статистической близости рубрицируемого текста к обучающим текстовым массивам рубрикатора. Теоретической базой данного механизма является векторное представление текстов из обучающего массива и рубрицируемого текста в виде частот появления s-цепочек последовательных символов текста, и вычисление по ним статистики мощности рассеивания. На основании получаемых значений определяется принадлежность рубрицируемого текста к каждой рубрике рубрикатора.

С целью экспериментального исследования правильности работы описываемого механизма тематического разграничения доступа была смоделирована система хранения электронных документов с документами заведомо известных рубрик. Каждый из запрашиваемых документов проходил процедуру авторубрикации, по результатам которой устанавливалась возможность доступа к нему. Эксперименты показали, следующие результаты: для документов объёмом 5.000 символов и более, при обучающих массивах объёмами 250.000 для каждой рубрики рубрикатора содержащего 20 рубрик вероятность правильного определения «чужого» для рубрикатора текста равна 0.92, а вероятность правильного распознавания тематики «своего» для рубрикатора текста равна 0.9.

Быструев Д.А.

РЕШЕНИЯ КОМПАНИИ IBM ДЛЯ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА

г.Москва, ИБМ Восточная Европа/Азия

Опыт работы компании IBM с государственным сектором. Опыт разработки решений с учётом российской специфики. Что такое «электронное правительство» в понимании IBM. Наше понимание задач, стоящих перед государственными органами. Разработка электронных регламентов. Отображение и ввод информации через веб-порталы. Электронное взаимодействие с гражданами, организациями и между различными государственными органами. Возможности по бюджетному планированию. Повышение эффективности работы с помощью средств коллективной работы. Системы документооборота для применения в государственных органах. Создание и управление системами электронных архивов. Анализ эффективности работы электронного правительства. Необходимость систем обеспечения безопасности. Примеры внедрённых решений в Российской Федерации и в зарубежных странах. Дальнейшие шаги.

Быструев Д.А.

ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ. ОПЫТ IBM

г.Москва, ИБМ Восточная Европа/Азия

В последнее время популярным способом повышения общественной безопасности стали повсеместные внедрения систем видеонаблюдения. Однако, к сожалению, эффективность работы таких систем, как в России, так и в мире, не всегда устраивает заказчиков – муниципальные, региональные и федеральные власти. Зачастую критика систем безопасности выплёскивается на страницы открытой печати и телевидения. В результате, основная модель использования таких систем остаётся, как правило, в сфере расследования уже совершённых преступлений, а не предотвращения их в реальном масштабе времени.

Не претендуя на полноту охвата темы, хотелось бы осветить тот опыт, который в данной области накопила компания IBM. Прежде всего, это внедрение интеллектуальных систем видеонаблюдения IBM, которые не конкурируют с существующими решениями, а дополняют их, позволяя наиболее полно использовать их потенциал. Будет рассмотрен пример наиболее известного из таких решений в мире – видеоаналитика для Олимпиады 2008 в Пекине, где всего лишь 130 операторов смогли отслеживать в реальном времени 5 тыс. камер.

М.А. Голубев, В.К. Драгальчук,
А.А. Емагулов, М.П. Левин, Е.А. Попов,
Санг Мин Ли, Сан Док Мо, И.В. Набирушкин,
Санг Бум Со, А.С. Трофимов

БЕЗОПАСНАЯ СИСТЕМА ВИРТУАЛЬНЫХ ОКОН

г.Москва, Исследовательский центр Самсунг

Безопасная Система Виртуальных Окон (БСВО) предназначена для унификации графического представления Виртуализованной Встраиваемой Операционной Системы (ВВОС) с пользовательскими интерфейсами ввода и вывода информации. В данном докладе рассказано о прототипе БСВО, который поддерживает ввод и вывод двух и более одновременно выполняющихся ВВОС с использованием виртуализированного дисплея и устройств интерфейса пользователя (Human Interface Device).

Основная задача, решённая в предлагаемом решении, заключалась в проработке архитектуры (дизайна) системы виртуальных окон. Необходимость в данной разработке возникла в связи отсутствием эквивалентного унифицированного решения. Система выполнена на базе проекта Secure Xen on ARM и является его логическим продолжением. Прототип представляет собой набор из гипервизора Secure Xen on ARM и двух гостевых систем: привилегированного домена №0 и непривилегированного домена №1. Каждый домен работает под управлением ОС на базе паравиртуализированного ядра Linux. Возможно лёгкое масштабирование системы по числу непривилегированных доменов.

После анализа области было выявлено две возможности построения подобной системы. Первая возможность базировалась на клиент-серверном подходе к построению драйверов (т.н. сплит-архитектура). Данная архитектура должна была представлять из себя управляющий окнами сервер работающий в ядре домена №0 и предоставляющий возможность клиентам из гостевых доменов подключаться для вывода графической информации. Вторая возможность базировалась на графической библиотеке X (TinyX / XFree). Второй путь был выбран как базовый для первого прототипа.

Система реализована для ARM9/xScale310 и содержит следующие компоненты:

- Базовый набор библиотек: Серверная часть TinyX/XFree для домена №0, клиентская часть TinyX/XFree для доменов №1(2), библиотеки GPE, GTK, GDK, ALSA, Pango, Cairo и др.;
- Базовый набор программ для привилегированного домена: Integrated Desktop на базе оконного менеджера Matchbox, Integrated Task Manager, Intergated Software Installer, Dilo browser (trusted, для internet banking), VOIP Linphone;
- Базовый набор программ для непривилегированного домена: Audio Player, Video Player, GTK Benchmark, Dilo browser (untrusted);
- Менеджер Запуска Приложений (МЗП). Эта компонента отвечает за состояние приложений в системе (запуск, остановка, текущее состояние);
- Менеджер Регистрации Приложений (МРП). Эта компонента отвечает за

установку, удаление приложений, а так же за отображаемые ярлыки на объединённом рабочем столе;

- Сплит-драйвер Междоменного Канала (СДМК). Эта компонента предоставляет подобие интерфейса loopback для взаимодействия приложений, запущенных в разных доменах (компонента заменяет в системе Socket-транспорт);
- Сплит-драйвер Аудио (СДА). Эта компонента отвечает за поддержку микшированного вывода звука в системе и поддерживает как OSS, так и ALSA стандарты.

В докладе рассмотрены все компоненты системы, особое внимание уделено вопросу безопасности.

Емельянов В.Г.

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ СОСТАВЛЯЮЩАЯ В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ БИЗНЕСА

г.Москва, МОО АЗИ

На протяжении последнего десятилетия дискуссия на тему необходимости информационно-аналитического сопровождения различных бизнес-процессов хозяйствующих субъектов потеряла былую остроту. Потребность в данной деятельности признаётся на всех уровнях менеджмента и в различных сферах рыночных отношений. В частности, это касается и такого внутреннего бизнес-процесса, как обеспечение безопасности деятельности хозяйствующего субъекта. При этом под безопасностью в данном случае понимается весь спектр её приложений – кадровая, объектовая, экономическая, имиджевая, финансовая, информационная и т.д. Конечно, для каждого вида будут различаться формулировки запросов на информационные продукты, используемые информационные ресурсы и методы поиска по ним, алгоритмы обработки и анализа полученных сведений и пр. Но суть информационно-аналитической составляющей (далее по тексту – ИАС) в обеспечении безопасности бизнеса остаётся единой.

Как правило, под ИАС понимается сбор, обработка, анализ, учет и предоставление заинтересованным лицам тех сведений, которые могут обеспечить хозяйствующему субъекту определенные конкурентные преимущества; повысить уровень его экономической, финансовой, информационной и иной безопасности; предотвратить прием на работу сотрудников, представляющих потенциальную угрозу для деятельности хозяйствующего субъекта; своевременно выявить действия сотрудников, идущие вразрез с интересами хозяйствующего субъекта и т.д., а также любой иной информации, помогающей в процессе принятия решений в рамках проводимых бизнес-процессов.

В общем случае роль ИАС в обеспечении безопасности бизнеса обычно сводится к трем составляющим: превентивная, сопровождающая и реагирующая.

Превентивная роль ИАС направлена на недопущение происхождения какого-либо невыгодного в широком смысле для деятельности субъекта события. При этом выявляются угрозы и их носители; слабые места в защите от этих угроз; сценарии происхождения события; меры, направленные на недопущение события, исполнители этих мер, необходимые для этого ресурсы и т.п.

Сопровождающая роль ИАС проявляется при обеспечении безопасности какого-либо наступившего и длящегося процесса. Отслеживаются обычно такие моменты, как: поведение участников сделки; изменение их статуса и состава; достигаемый результат в реперных точках; нештатные ситуации; документальное сопровождение; работа ответственных лиц.

Реагирующая роль ИАС заключается в нивелировании последствий произошедшего события, приведшего к нанесению какого-либо ущерба компании (т.е. «пробоя» в системе её безопасности). Здесь выделяются такие направления ИАС, как: выяснение и изучение факторов и условий, сделавших возможным наступление события; выявление последствий (имеющихся и ожидаемых) наступившего события; описание мер, направленных на минимизацию ущерба от этих последствий, определение исполнителей этих мер, и требующихся для этого ресурсов; контроль за реализацией мер и работой исполнителей; анализ всего процесса и выработка мер для

недопущения повторения аналогичных событий в дальнейшем, контроль за их реализацией.

На практике разграничить роль ИАС в повседневном применении довольно непросто. Часто одновременно проявляются две-три роли ИАС или они периодически - попеременно берут верх одна над другой по своей важности и приоритетности.

Теперь рассмотрим основные составные части ИАС, которые должны присутствовать для эффективного использования ИАС в обеспечении безопасности бизнеса.

В общем случае ИАС состоит из следующих процессов:

- уяснение сути проблемы, исследования, темы и т.д., грамотное описание исходных данных и поставленной задачи, четкая постановка цели;
- выработка технологии по решению поставленной задачи, согласование её со всеми участниками и заинтересованными лицами;
- определение ресурсов и исполнителей для реализации выбранной технологии, разбиение для них исходной задачи на соответствующие подзадачи;
- получение требуемой информации, её обработка и анализ, оценка достоверности, снятие пробельных моментов и информационных противоречий, подготовка результирующих документов, выводов, прогнозов и пр., их обоснованность;
- выработка на основании полученных результатов и проведенного анализа конкретных мер, предложений, ответов по поставленной задаче, определение исполнителей и необходимых ресурсов, контроль за реализацией;
- обязательный учет всей проделанной работы во внутренней среде «интеллектуального» архива (базы знаний).

Несколько вопросов, на которых хотелось бы остановиться подробнее.

Получение информации. Источников получения информации существует достаточно много. Наиболее доступными из них являются:

- внутренняя среда организации (имеющиеся у сотрудников опыт – знания - навыки, «интеллектуальный» архив (база знаний), документарный контур и т.д.);
- различные профессиональные базы данных по соответствующим тематикам;
- сеть Интернет и архивы СМИ;
- специализированные информационные агентства и государственные органы соответствующей направленности;
- беседы, опросы, интервью, построенные правильным образом и проводимые в соответствующих аудиториях, а также выставки, презентации, семинары, круглые столы и пр.;
- специальные документы (маркетинговые исследования, малотиражные сборники конференций, внутрифирменные отчеты и т.п.).

Способы получения информации также весьма разнообразны – от обработки электронных массивов и открытого общения до бизнес-разведки и промышленного шпионажа.

Ряд источников информации и способов её получения государством регламентированы. В частности, об этом говорится в федеральных законах № 152 «О персональных данных», № 2487-1 «О частной детективной сыскной и охранной деятельности в РФ», № 144 «Об оперативно-розыскной деятельности», № 24 «Об информации, информатизации и защите информации», № 218 «О кредитных историях», № 2124-1 «О средствах массовой информации», в Постановлении правительства РФ № 35 «О перечне сведений, которые не могут составлять коммерческую тайну» и другие. Что касается оставшегося, то здесь всё отдано на откуп таланту, фантазии и умению

работающего. Но не стоит забывать о том, что иногда вольно или невольно можно переступить грань закона. Поэтому в ИАС обязательно должна присутствовать юридическая поддержка, к помощи которой можно незамедлительно прибегнуть в случае необходимости.

В этом месте будет уместно вспомнить главные сходство и различия бизнес-разведки и промышленного шпионажа. Сходство состоит в том, что у них общая цель - получение информации и одинаковый характер деятельности – закрытый (например, от конкурентов, внутренних злоумышленников, контролирующих органов). А вот различие у них существенное и состоит в методах получения информации: в бизнес-разведке – без нарушения норм законодательства, в промышленном шпионаже – любыми способами и средствами.

Отдельно остановимся на следующих трех понятиях, на практике занимающих в ИАС важное место:

- достоверность информации;
- пробельные моменты (неполнота информации);
- информационные противоречия.

Достоверность информации – это некоторая характеристика её истинности, которая позволяет без дополнительной оглядки ей верить, строить на её основе дальнейшие рассуждения и т.д. Достоверность информации обычно проверяется сравнением сведений из различных независимых друг от друга источников, а также привлечением логики.

Пробельный момент (неполнота информации) – это когда на некоторый вопрос вообще нет никакого ответа. В этом случае, во-первых, необходимо оценить насколько важен требуемый ответ в общем поставленном исходном вопросе, а во-вторых, если важен, привлечь «нетипичные» ресурсы.

Информационные противоречия – это противоречивость сведений, полученных в отношении конкретного вопроса. В этом случае применяются уже описанные выше методы, т.е. сравнение сведений из разных источников и «нетипичные» ресурсы.

Наконец, об учетно-архивном моменте. Несмотря на то, что все прекрасно понимают его важность, на практике нередко к этому участку работы относятся как к второстепенному. Хотя грамотный учет и накопление сделанных по линии ИАС работ в дальнейшем экономит время, средства и трудоресурсы хозяйствующего субъекта при возникновении необходимости решения схожих вопросов или изучения и проработки вопросов смежных. Помимо этого нередко возникает потребность восстановить не только результаты какой-либо работы, но и ход, и участников её выполнения. При реализации учетно-архивного момента неплохо зарекомендовали себя объектно-ориентированные СУБД, на базе которых создаются так называемые «интеллектуальные» архивы или базы знаний. Пользователями такого ресурса имеет смысл делать широкий круг сотрудников (конечно с соблюдением условий конфиденциальности и разграничения прав доступа).

Важным нюансом в ИАС является форма выдачи результата. Ведь одну и ту же информацию можно представить различными способами – зачитать вслух, оформить в виде документа (наиболее распространенный способ), визуализировать в виде схем и контентов, разыграть в деловой ситуационной игре и т.д. Здесь желательно знать и учитывать личностные особенности потребителя информации в восприятии им окружающего мира (сенсорный, вербальный, зрительный и пр.), а также стараться комбинировать различные способы представления результатов ИАС. Тогда восприятие

результатов ИАС будет полнее и эффективнее, а значит возрастёт и уверенность в правильности принимаемых на основе ИАС бизнес-решений.

Немного о кадровом обеспечении ИАС. Тут интересную закономерность подметил один мой коллега, и мне хотелось бы ей поделиться. Проще будет воспринимать её в виде таблицы профессиональных и личностных характеристик сотрудников из различных социальных сред.

Среда / Характерис-тика	Из спецслужб «чекисты»	Из науки, журналистики, промышленности «интеллигенты»	Из учебных заведений «студенты»
ПРЕИМУЩЕСТВА	- знают оперативную работу; - дисциплинированы; -ответственны; - умеют работать с людьми; -способны принимать самостоятельные решения; - хорошо знают законодательство.	- знают экономику; - умеют работать в условиях рынка; - обучаемы; - умеют работать с новыми IT-технологиями; - соблюдают этический кодекс.	- легко обучаемы; - хорошо работают с новыми IT-технологиями; - хорошо адаптируются к изменяющейся среде.
НЕДОСТАТКИ	- не знают экономики; - не умеют работать в условиях рынка; - консервативны; - не умеют работать с новыми IT-технологиями (искл. – «молодые чекисты» - могут не соблюдать этический кодекс.	- не знают оперативной работы; - часто недисциплинированны; - как правило слабо знают законодательство.	- часто недисциплинированны; - не способны принимать самостоятельные решения; - не знают оперативной работы; - ориентированы на «быстрые» деньги; - не знают законодательство; - могут не соблюдать этический кодекс.

В конце рассмотрим ряд информационно-аналитических продуктов, на практике готовившихся в рамках ИАС в коммерческих структурах и зарекомендовавших себя в качестве востребованных и доступных. Это следующие продукты.

- профиль (характеризующие сведения) юридического лица, аналитическая выжимка для ускорения процесса принятия решений;

- экспресс-оценка соискателя с целью выявления сведений, препятствующих его приёму на работу (например, претензии со стороны правоохранительных или контролирующих органов; судебные разбирательства с его участием; неблаговидные поступки по предыдущим местам работы или по общепринятым моральным нормам; факты мошенничества или использования служебного положения для достижения личных целей; поступки и действия, направленные против работодателя или в интересах его конкурентов и т.п.) или иных представляющих интерес сведений (учредительская и/или руководящая деятельность; публикации/интервью в СМИ; деловые/родственные связи и т.д.);

- схемы аффилированности юридических и физических лиц по различным критериям взаимосвязей и зависимости. Контент-анализы, в т.ч. временные;

- тематические продукты (информационная записка, аналитический обзор, отчет-исследование);

- Интернет- и СМИ- мониторинги и обзоры по конкретным темам и направлениям;

- деловые ситуационные игры;

- база знаний «Интеллектуальный учет и архив»;

- специализированные электронные контуры с соответствующим информационно-аналитическим инструментарием.

И последнее. Очень часто при недостаточном информационно-аналитическом обеспечении коммерческой сделки, например:

- не были собраны данные о фирмах - потенциальных покупателях;
- не была создана картина предложений конкурентов;
- не были выявлены экологические, правовые и иные ограничения;
- была произведена неполная или неверная оценка собственных ресурсов

происходило, что:

- неверно выбирался потенциальный покупатель,
- завышалась/занижалась цена,
- товар не пользовался спросом и пр.,

в результате чего сделка либо вообще не происходила, либо условия её оказывались невыгодными для хозяйствующего субъекта.

Зегжда Д.П.

ТЕХНОЛОГИЯ ВИРТУАЛИЗАЦИИ – БАЗА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

г.Санкт-Петербург, ГОУ «СПбГПУ»

Предлагается в качестве подхода к обеспечению безопасности использовать технологию гибридных операционных систем суть которой заключается в том, что в рамках одной операционной системы (её назвают «базовой») создаётся среда, в которой может функционировать другая операционная система (её называют «встроенной»), что позволяет запускать на компьютере одновременно несколько разных ОС и переключаться между ними без перезагрузки.

Для реализации технологии гибридных систем используется известный достаточно давно механизм виртуальных машин, который позволяет организовать на одном компьютере несколько виртуальных машин, на каждой из которых можно запустить отдельную встроенную ОС. Виртуальная машина включает в себя все устройства, необходимые для работы встроенной ОС: процессор, оперативную память, дисковые накопители, сетевые устройства, устройства ввода-вывода. Эти устройства эмулируются виртуальной машиной при помощи ресурсов реальной вычислительной системы посредством обращения к сервисам, предоставляемым базовой ОС. Задействованные виртуальной машиной ресурсы либо отдаются в монопольное потребление виртуальной машине и исключаются из основного пула ресурсов (как, например, происходит с оперативной памятью), либо используются базовой и встроенной системами совместно — как это происходит с процессором, накопителями и сетевыми адаптерами. Поскольку все эти возможности предоставляются за счет разделения ресурсов одного реального компьютера, то требования к его аппаратным ресурсам повышаются, однако при современном уровне развития компьютерной техники выполнение этих требований не требует существенных затрат.

Основная задача виртуальной машины — изолировать встроенную ОС от аппаратуры и создать подходящую для нее вычислительную среду на основе прикладного программного интерфейса базовой ОС. При этом виртуальная машина может поддерживать различные аппаратные конфигурации — например, можно задать, сколько памяти получит та или иная виртуальная машина и будет ли в ней доступна работа с сетью.

С точки зрения безопасности важно, что в гибридной системе базовая ОС полностью контролирует аппаратуру вычислительной системы, а встроенная ОС не имеет доступа к аппаратуре и взаимодействует только с виртуальной машиной. Таким образом, базовая ОС полностью контролирует работу встроенной ОС и при этом может быть полностью прозрачна для пользователей и приложений встроенных ОС.

Благодаря этим свойствам технология гибридных ОС может быть применена для построения защищенной и доверенной операционной среды, в которой базовая защищенная ОС и система виртуализации обеспечивают безопасность и доверие, а встроенные ОС — удобный пользовательский интерфейс и совместимость с приложениями и технологиям их разработки. Для этого необходимо, во-первых, обеспечить возможность запуска встроенной ОС в составе обычного пользовательского процесса базовой ОС и, во-вторых, реализовать возможность доступа приложений встроенной ОС к ресурсам базовой ОС, под контролем входящих в ее состав средств защиты.

При соблюдении этих условий можно получить гибридную систему, безопасность и доверенность которой будут определяться только свойствами базовой и системы виртуализации ОС и не зависеть от свойств встроенных ОС, так же как безопасность и доверенность обычных ОС не зависят от безопасности и доверенности используемых в ней приложений.

В такой гибридной операционной системе средства безопасности базовой операционной системы, должны решать две основные задачи: обеспечивать защиту компонентов встроенных операционных систем от влияния друг на друга, и осуществлять контроль доступа к ресурсам базовой системы со стороны приложений встроенных систем.

Следовательно, использование при построении доверенных защищенных ОС технологии гибридных систем позволяет избежать постоянного процесса исследования степени доверия новых операционных систем, которых требуют новые приложения, поскольку обеспечив один раз безопасность и доверенность базовой ОС и системы виртуализации в качестве встроенных можно безопасно использовать не только ОС, существующие в настоящее время, но и те, что появятся в будущем.

Это позволит создать защищенную и доверенную вычислительную среду, обладающую способностью адаптироваться к быстро меняющимся требованиям современных технологий обработки информации.

Перечисленные свойства гибридных систем позволяют использовать эту технологию в качестве платформы для типовых решений, представляющих собой специализированные системы с несколькими изолированными средами для обработки различной информации.

Зегжда Д.П., Рудина Е.А.

МОДЕЛИРОВАНИЕ БЕЗОПАСНОСТИ ОБРАБОТКИ ИНФОРМАЦИИ В ВИРТУАЛЬНЫХ СИСТЕМАХ

г.Санкт-Петербург, ГОУ «СПбГПУ»

В общем случае виртуализация — это представление вычислительных ресурсов, которое позволяет получить новые качества при их использовании. В частности, виртуализация вычислительных машин открывает широкие возможности по увеличению эффективности использования высокопроизводительных компьютерных систем и повышению их отказоустойчивости .

В данном докладе для виртуализация определяется через описанное в [1] понятие гипервизора. Гипервизор должен обеспечивать выполнение по крайней мере, двух условий: инвариантность функционирования виртуальной системы по отношению к реальной, полная изоляция виртуализуемых ресурсов. Гипервизор работает как обычная программа под управлением (обычно реальной) системы и не исключает одновременного использования других прикладных программ в этой системы. Таким образом, могут быть рассмотрены как гипервизоры, реализующие аппаратную виртуализацию вычислительных машин (такие, как описаны в [1]), так и программные гипервизоры, работающие под управлением базовой ОС [2].

В последнее время наблюдается тенденция к использованию виртуализации процессов обработки информации с целью повышения ее безопасности, например, использование программной виртуализации для выполнения недоверенных приложений и систем под управлением безопасной базовой ОС. Программы, которые не могут быть выполнены непосредственно под управлением этой ОС, могут быть запущены на ней под управлением виртуальной машины. При этом доступ этих приложений к данным, безопасность которых критична, должен контролироваться механизмами базовой ОС. В этом случае расширение функциональности базовой ОС с одновременным сохранением присущих ей свойств безопасности, будет достигнуто с наименьшими затратами.

В то же время нельзя наверняка утверждать, какие свойства (в том числе формально обоснованные), как базовой системы, так и виртуализуемой, будут выполнены для виртуальной машины. В [1] для описания свойства инвариантности поведения программ множество состояний виртуальной машины рассматривается как гомоморфный образ множества состояний реальной машины. Какие свойства виртуализуемой системы сохраняет этот гомоморфизм? При каких условиях виртуальная машина сможет унаследовать свойства не только виртуализуемой, но и базовой системы?

Для разрешения поставленных вопросов описана модель вычислительной системы, включающая множества процессов ВС *P*, ресурсов *R*, функций *F*, описывающих архитектуру системы в целом, программ *Prg*, описываемых как алгоритмические последовательности функций и сопоставляемых процессам из *P* функцией φ. Ресурсы ВС типизированы (в связи с тем, что в реальной системе ресурс не есть только именованный объект, содержащий данные, каждый ресурс характеризуется также способом доступа к нему, или его интерпретации с целью получения содержащихся в нем данных). Соответственно, в модель ВС также включены множество типов ее ресурсов *TR*, функции типизации ресурса τ и интерпретации ресурса δ с целью получения его данных *D*.

Пусть:

1. Виртуализуемая система А и базовая система Н описываются моделью вычислительной системы $\boldsymbol{M}=(P, R, TR, D, \tau, \delta, F, Prg, \varphi)$. Представление данных *D* для систем А и Н идентично.
2. Существуют предикат, описывающий выполнение аспекта безопасности $VER: D \rightarrow \{true, false\}$ и условие безопасности данных $\forall r \in R(\tau(r) \in CR \Rightarrow VER(\delta(r)))$,

   где $CR \subseteq R$ – множество типов т.н. чувствительных (конфиденциальных) ресурсов.
3. Система А, описываемая моделью М, может быть виртуализована под управлением системы Н в виде третьей системы V, описываемой моделью $\boldsymbol{M^V}$, являющейся уточнением модели М; $\boldsymbol{M^V}=(P^{\boldsymbol{V}}, R^{\boldsymbol{V}}, TR^{\boldsymbol{V}}, D, \tau^{\boldsymbol{V}}, \delta, F, Prg^{\boldsymbol{V}})$.
4. Для виртуализуемой системы А, выполнены следующие (формально описываемые) свойства относительно виртуальной системы V: инвариантность А относительно V, контроль ресурсов типов $VR \subseteq TR^A$ гипервизором виртуализации.
5. Для базовой системы Н , описываемой моделью выполнены свойства $P^{\boldsymbol{H}} \subseteq P^{\boldsymbol{V}}$, $R^{\boldsymbol{H}} \subseteq R^{\boldsymbol{V}}$, $TR^{\boldsymbol{H}} \subseteq TR^{\boldsymbol{V}}$, $\forall r \in R^H \Rightarrow \tau^V(r) = \tau^H(r)$.
6. Множества программ выполнимых в А, Н, V соотносятся как $Prg^{\boldsymbol{V}} = Prg^{\boldsymbol{A}} \cup Prg^{\boldsymbol{H}}$ и выполнено $\forall p \in P^H \Rightarrow \varphi^V(r) = \varphi^H(r)$
7. Ресурсы, используемые для хранения и/или передачи чувствительных данных в системе А, являются подмножеством виртуализуемых ресурсов $CR^A \subseteq VR$
8. Существуют программы, не выполнимые под управлением системы Н, но выполнимые под управлением системы А $\exists \Pr g_{susp} \subseteq \Pr g_A, \Pr g_{susp} \not\subset \Pr g_H$. Неизвестно, безопасно ли поведение программ системы А. Поведение гипервизора виртуализации в базовой системе Н безопасно.

В докладе показано, что, при выполнении условия гомоморфного отображения функций типизации ресурсов из $\boldsymbol{M^A}$ в $\boldsymbol{M^V}$ и замкнутости этого отображения относительно множеств типов чувствительных ресурсов, если поведение некоторой программы в реальной системе A небезопасно, то поведение этой программы в виртуальной системе V под управлением базовой системы H будет изменено так, чтобы отвечать условию безопасности.

Список литературы

1. G.J.Popek, R.P.Goldberg "Formal Requirements for Virtualizable Third Generation Architectures", Association for Computing Machinery, Inc., 1974.

2. Keith Adams, Ole Agesen. "A Comparison of Software and Hardware Techniques for x86 Virtualization", VMware, 2006.

Калинкина Т.И.

ОСОБЕННОСТИ ОЦЕНКИ НАДЕЖНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ НА БАЗЕ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

г. Рязань, Государственное образовательное учреждение
высшего профессионального образования
«Рязанский государственный радиотехнический университет»

Современная информационная система на базе вычислительной сети представляет собой распределенную компьютерную систему. Такого типа системы характеризуются достаточно сложной структурой взаимосвязных подсистем и элементов. С течением времени эти связи могут меняться. Передача информации в системах такого типа может иметь различные пути. Такую систему можно разбить на подсистемы по ряду признаков. На основе изложенного информационную систему на базе вычислительной сети отнесем к сложным техническим системам.

При оценке надежности информационной системы в защищенном исполнении на базе вычислительной сети (далее - ИС) должны учитываться ряд ее особенностей: функциональная, аппаратная и программная разнородность элементов ИС, структурные связи ее подсистем и элементов между собой. В составе ИС можно выделить особую подсистему – подсистему защиты информации. При расчете надежности ИС необходимо учитывать влияние механизмов защиты информации на функционирование остальных подсистем ИС и ее элементов. От работоспособности подсистемы защиты информации зависит работоспособность всей ИС. Отказ элемента подсистемы защиты информации может привести к отказу всей ИС.

При оценке факторов, влияющих на работоспособность ИС, надо учитывать угрозы безопасности информации, циркулирующей в ИС.

Современные модели расчета надежности информационных систем позволяют отдельно оценить либо функциональную, либо аппаратную, либо программную надежность. Однако при использовании таких моделей тяжело, а иногда и невозможно оценить проектируемую систему в целом (а именно такая оценка необходима на системном этапе проектирования). В связи с этим возникает задача разработки интегральной модели надежности ИС, позволяющей объединить и учесть взаимное влияние всех элементов и подсистем ИС.

Корт С.С.

ОРГАНИЗАЦИЯ ДОСТУПА НАСЕЛЕНИЯ К ИНФОРМАЦИОННЫМ РЕСУРСАМ МУНИЦИПАЛЬНЫХ ОРГАНОВ

г.Санкт-Петербург, ГОУ «СПбГПУ»

В настоящее время муниципальные органы являются наиболее близкой к населению властной структурой. Как следствие этого целесообразным является использование вычислительной системы муниципальных органов как своеобразного «посредника» между населением и информационными ресурсами региональных и федеральных органов. Являясь таким посредником, вычислительная система муниципальных органов может предоставлять данные о:

1) населении в соответствии с требованиями закона о персональных данных для использования в вычислительных системах региональных и федеральных органов;

2) деятельности муниципальных органов в вычислительные системы региональных и федеральных органов, а также населению.

На требования по безопасности, предъявляемые к функционированию вычислительных систем муниципальных органов, оказывают влияние следующие федеральные законы: «О персональных данных» от 27 июля 2006 года № 152-ФЗ, «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ. С 1 января 2010 года вступает в силу Федеральный закон от 9 февраля 2009 года № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления».

Как следствие данной ситуации желательно внедрить механизмы безопасности в вычислительные сети муниципальных органов и федеральных органов, отвечающие за хранение и обработку информации в вычислительной системе, а также за передачу информации за ее пределы.

Рассматривая архитектурные требования к вычислительной системе можно отметить то, что для связи с федеральными и региональными органами желательно иметь единую точку входа для муниципальных органов к информационным ресурсам федеральных органов. Наличие единой точки входа в виде портала позволяет интегрировать вычислительные системы муниципальных и федеральных органов уже на уровне пользовательского интерфейса, формируя его в унифицированном и единообразном виде. Кроме того, желательно организовать доступ к ресурсам в форме тонкого клиента на базе веб-браузера, а в качестве форматов данных — *.txt (текстовый

документ), *. odt (текстовый документ формата Open Document Text), *.html (гипертекстовый документ).

Рассматривая функции защиты, следует отметить необходимость присутствия в вычислительной системе средств защиты, реализующих следующие функции: надежную аутентификацию абонентов, нормализация и обезличивание информации, а также защищенность системы. При получении пользовательской информации, а также при передаче информации между вычислительными системами муниципальных и федеральных органов должна выполняться нормализация данных, включающая следующие процедуры:

1) Проверка отсутствия атак, использующих формы ввода.

2) Очистка данных от персональной информации в том случае, если они могут быть переданы за пределы информационной системы.

3) Очистка конфиденциальной информации.

Рассмотренные выше требования должны найти отражение в профиле защиты, который должен быть разработан для вычислительной системы муниципальной организации в соответствии с требованиями ГОСТ.

Котылевский А.С.

РАСПРЕДЕЛЕННЫЙ КОНТРОЛЬ ПОТОКОВ ДАННЫХ В ИТКС С ПОМОЩЬЮ СЕТЕЙ СВЯЗИ С РАЗГРАНИЧЕНИЕМ ДОСТУПА

г.Санкт-Петербург, ООО «НеоБИТ»

Идея реализации функций контроля и управления доступом на уровне инфраструктуры сети является аналогией сетей шифрованной связи. Создание технических средств, позволяющих строить сети связи с контролируемым и управляемым доступом, обеспечит в ИТКС надежную защиту от внутреннего нарушителя подобно тому, как сети шифрованной связи обеспечивают защиту от внешнего нарушителя.

Задача распределенного контроля потоков данных в ИТКС состоит в мониторинге и управлении передачей информации между территориально распределенными узлами системы, объединенными сетью связи. Под потоком данных понимается *о*дно- или двунаправленный обмен данными между двумя узлами сети ограниченный по времени. В общем случае действующие в ИТКС приложения и сервисы могут требовать обмена данными между узлами сети по различным схемам – напрямую, либо через центральный узел, либо по какой-то иной схеме. Таким образом, множество узлов ИТКС, осуществляя обмен данными посредством передачи потоков данных по определенной схеме, образуют сеансы связи. Информация, циркулирующая в пределах сеансов связи, рассматривается как объект доступа.

Задача распределенного контроля потоков данных в ИТКС может быть решена различными методами. Идентификация узлов связи может быть выполнена на основе сетевого адреса, либо с привлечением средств идентификации и аутентификации пользователей. Отнесение потоков данных к сеансам связи может быть выполнено на основе анализа пересылаемых данных, маркировки данных перед отправкой приложениями, либо по указанию от пользователя узла связи. Механизмы мониторинга и управления передачей информации могут быть реализованы на узлах связи, либо в сети на основе шлюзовых технологий; в случае, если все сеансы связи организуются через единый сервер связи, механизмы управления передачей потоков данных могут располагаться на этом сервере.

Применение концепции сетей связи с разграничением доступа (ССРД) позволяет решить задачу распределенного контроля потоков данных без необходимости модификации приложений и сервисов ИТКС. Другим существенным преимуществом предлагаемого подхода является существенное снижение сложности сертификационных исследований ИТКС на основе ССРД. Точно также как применение сертифицированных потоковых шифраторов снимает необходимость реализации и последующей сертификации подсистем криптографической защиты каналов связи, применение ССРД снимет необходимость разработки и последующей сертификации подсистем контроля и управления доступом, регистрации и учета событий.

Построение ССРД на практике связано с множеством трудностей. Так в одной ИТКС, как правило, функционирует множество приложений, каждое из которых использует свои протоколы связи. Существует также служебный трафик, такой как ARP, ICMP, DHCP, DNS и пр. Большой объем протоколов связи усложняет детектирующие механизмы сети связи. Также необходимо определить будет ли применяемая политика безопасности единой для всех приложений, или для каждого приложения будет отдельная политика. Одним из самых серьезных вопросов разработки сетей связи с разграничением доступа является механизм интеграции с

целевой ИТКС. От этого зависят подсистемы идентификации, аутентификации, детектирования и др.

Вопросы разработки сетей связи с разграничением доступа достаточно актуальны. И по мере того, как будут усложняться ИТКС, актуальность этих вопросов будет возрастать, поскольку на сегодняшний день не существует иных способов снижения трудоемкости процесса сертификации, кроме использования готовых сертифицированных компонентов при построении ИТКС.

Краснопевцев А.А.

РАЗРАБОТКА СИСТЕМЫ АВТОМАТИЧЕСКОЙ ЗАЩИТЫ .NET ПРИЛОЖЕНИЙ

г.Москва, Московский Инженерно-Физический Институт (Национальный исследовательский ядерный университет)

В последнее время, защита программного обеспечения от копирования является актуальной проблемой, так как несанкционированное копирование программного обеспечения наносит серьезный финансовый урон фирмам, выпускающим это программное обеспечение на рынок. На момент написания данной работы, практически все программное обеспечение является в той или иной мере платным, то есть для полноценного функционирования программы пользователю необходимо приобрести лицензию, дающую ему право на использование конкретного программного продукта. При использовании «классических» средств разработки программного обеспечения, таких, как языки C++, Assembler, то есть компилирующих приложение в машинный код, защита программного обеспечения от копирования сводилась, в основном, к тому, что код приложения, отвечающий за проверку лицензии данного приложения, был скрыт от злоумышленника. Для такого сокрытия кода использовались различные способы защиты от исследования приложения, как в статическом режиме, то есть с использованием только дизассемблера, так и в динамическом режиме, то есть с использование различных отладчиков, трассировщиков и так далее. Большинство способов, используемых для защиты приложений от исследования, основывались на недостатках архитектуры представления кода приложения и обрабатываемых этим приложением данных, то есть архитектуры Фон-Неймана.

Однако при появлении технологий разработки приложений, с применением которых создаются приложения, компилируемые в некоторое промежуточное представление, у разработчиков возникла проблема с защитой своих продуктов от несанкционированного копирования и распространения. Основная причина отсутствия надежных средств защиты связана с тем, что приложения, компилируемые в промежуточное представление в результате достаточно просты для анализа и исследования злоумышленником. Таким образом, модификация защищенного приложения и его компрометация является достаточно простым делом.

В рамках данной работы предлагается разработка программно-аппаратного комплекса по защите приложений, компилируемых в промежуточное представление (на примере технологии .NET), с использованием внешнего аппаратного модуля, в виде которого используется электронный ключ с загружаемым кодом. В отличие от аналогов, данный программный комплекс позволяет защищать .NET приложения, используя технологии аппаратного черного ящика не доступного для чтения и модификации злоумышленнику. Общий принцип работы комплекса заключается в перенесении части кода защищаемого приложения на электронный ключ с загружаем кодом и выполнение вынесенного кода внутри электронного ключа. В результате такой

защиты получается приложение, которое просто не может функционировать без электронного ключа, вследствие отсутствия части кода.

Аналогичные системы защиты приложений от несанкционированного копирования в своей основе используют методы построении программного черного ящика, например вынесение части кода приложения в библиотеку, скомпилированную в машинный код. Программный черный ящик в результате использования не защитит приложение от компрометации, а всего лишь увеличит время требуемое на компрометацию защищенного приложения.

Лукомский Е.А.

КОНТРОЛЬ ФУНКЦИОНИРОВАНИЯ И ВЗАИМОДЕЙСТВИЯ ПРИЛОЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ ВИРТУАЛИЗАЦИИ

г.Санкт-Петербург, ООО «НеоБИТ»

При построении защищенных информационных систем встает задача безопасного исполнения недоверенных приложений в доверенной среде и задача контроля взаимодействия приложений, в частности, доверенного разделения информационных потоков различных категорий при взаимодействии приложений друг с другом.

С точки зрения обозначенных задач, современные технологии аппаратной и программной виртуализации позволяют реализовать две важные функции контроля по отношению к гостевым ОС:

1. Контроль функционирования гостевой ОС и ее приложений.
2. Контроль взаимодействия гостевой ОС и хостовых аппаратных ресурсов.

Применение технологий виртуализации позволяет свести задачу безопасного исполнения недоверенных приложений (и даже ОС) в доверенной среде к задаче контроля функционирования приложений гостевой ОС.

Виртуализация в данном контексте позволяют разработать доверенную систему мониторинга и управления процессами гостевых ОС.

Технологически достижимым для такой системы является следующий набор функций контроля:

- разграничение доступа к ресурсам между прикладными процессами и процессами администрирования;
- изоляция процессов различных гостевых ОС друг от друга, процессов гостевой ОС от хостовой ОС и наоборот;
- управление механизмами планирования гостевых ОС;
- подтверждение работоспособности приложений.

Реализация такой системы предполагает ее настройку для работы с конкретными гостевыми ОС, что в случае закрытых ОС является достаточно трудоемкой, но решаемой задачей.

Возможности механизмов аппаратной виртуализации по контролю взаимодействия гостевой ОС с аппаратными ресурсами хостовой ОС позволяют предложить решение обозначенной задачи доверенного разделения на одной физической машине.

На основе данной технологии разделения может быть разработана система, реализующая мультиплексирующий удаленный терминал для нескольких Windows-машинам с гарантией невлияния и изоляции информации между ними.

Гипервизор, как программная основа средства виртуализации в такой системе, позволит гарантировать:

- взаимодействие драйвера сетевой карты только с назначенным ему устройством;
- формирование канала с участием только двух сетевых карт и исключение участия в канале данных других сетевых карт.

Предложенный подход к построению такой системы также позволяет использовать готовую реализацию драйверов сетевых карт для распространенных ОС. В этом случае изоляция в гипервизоре может основываться на унифицированных механизмах взаимодействия драйверов сетевых карт с устройствами.

Современные технологии виртуализации значительно упрощают построение защищенных информационных систем, обрабатывающих конфиденциальную информацию различных категорий и обеспечивающих с помощью контроля функционирования заданный уровень доверия без предъявления требований к исполняемым приложениям.

Матиев Д.М.

МЕТОДОЛОГИЯ ОРГАНИЗАЦИИ РАБОТ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

г.Москва, ЗАО «Рэйнвокс»

В 2006 году вступил в силу Федеральный закон 152-ФЗ О персональных данных. На сегодняшний день, когдаа до конца срока приведения информационных систем персональных данных Операторов в соответствие требованиям законодательства и нормативно-методических документов ФСТЭК России и ФСБ России остается менее чем полгода, очень важным для организации является четкое понимание методологии организации работ по защите персональных данных.

Обеспечение безопасности персональных данных осуществляется путём выполнения организационных и технических мероприятий, реализуемых в рамках создаваемой системы защиты персональных данных. Структура, состав и основные функции системы защиты определяются исходя из класса информационной системы персональных данных. Система защиты персональных данных включает организационные меры и технические средства защиты информации, а также используемые в информационной системе информационные технологии.

Создание системы защиты персональных данных должно носить комплексный характер и обеспечить достаточный уровень соответствия требованиям по безопасности для информационной системы персональных данных при выполнении принципа дифференцированного подхода к обеспечению уровня безопасности персональных, с учётом анализа взаимодействия информационных систем персональных данных с внешними информационными системами.

Использование разработанной отраслевой нормативно-методической базы в области защиты персональных данных («отраслевой стандарт») в значительной степени может облегчить создание системы защиты персональных данных для организации .

Разработка «отраслевого стандарта» предполагает проведение работ по исследованию отраслевой специфики обработки персональных данных организаций отрасли и разработка нормативно – методических документов, регламентирующих мероприятия по обеспечению защиты персональных данных.

«Отраслевой стандарт» по защите персональных данных создается с целью разработки отраслевой организационно-технической документации, предназначенной для формализации мероприятий и процессов по защите персональных данных, обрабатываемых организациями отрасли.

Такой подход позволит упростить и ускорить процесс приведения информационных систем персональных данных организаций в соответствие требованиям законодательства и нормативно-методических документов ФСТЭК России и ФСБ России.

Ныркова А.П., Сикарев И.А.

О ВЛИЯНИИ РАСПОЛОЖЕНИЯ ИСТОЧНИКА ВЗАИМНОЙ ПОМЕХИ НА ДАЛЬНОСТЬ ДЕЙСТВИЯ РАДИОЛИНИЙ АВТОМАТИЗИРОВАННЫХ ИДЕНТИФИКАЦИОННЫХ СИСТЕМ

г.Санкт-Петербург, Санкт-Петербургский государственный Университет водных коммуникаций

В последние 5–7 лет значительный интерес у специалистов водного транспорта для повышения безопасности, улучшения мониторинга и эффективности судоходства на внутренних водных путях (ВВП) вызывают возможности информационной технологии рубежа XX–XXI веков, получившей название «Автоматизированная идентификационная система» (АИС), ставшей уже неотъемлемой частью речных АСУ ДС. Возникновение технологии АИС можно поставить в один ряд с появлением на морском и речном транспорте радиолокационных станций или спутниковой навигации. Вхождение АИС в состав АСУ ДС предполагает не только наличие на судах и у лоцманского корпуса соответствующих транспондеров, но и, прежде всего, оборудования берегового сегмента, состоящего, в первую очередь, из цепи береговых станций АИС, включающей базовые станции (БС), симплексные и дуплексные репитеры, а также сети передачи данных АИС в структурах АСУ ДС и речных информационных служб (РИС).

Размеры зон действия базовых станций (БС), определяемые их радиусами действия, исследовались уже в целом ряде отечественных и зарубежных работ, однако их зависимость от воздействия взаимных помех остается в значительной мере открытой.

В настоящей работе рассматривается зависимость радиуса сотовой зоны от влияния взаимных помех.

Под взаимными помехами на линии судовой транспондер (СТ)–(БС) являются, прежде всего, характерные для этого участка УКВ диапазона (155 мГц–162 мГц) помехи одновременно работающих радиостанций морского диапазона частот и других служб, а также промышленных источников. Ими могут быть и заградительные или прицельные преднамеренные помехи.

Анализируется зависимость радиуса действия БС от расстояния источника взаимной помехи до (СТ). Показано, что для систем класса АИС1 и АИС2 влияние взаимных помех различно причем системы АИС2 при прочих равных условиях более устойчивы к воздействию помех типа моногармонических, полигармонических и ЧТ передач ЧТ цифровым сигналам АИС1 и АИС2.

Панченко А.А.

МОНИТОРИНГ ЭФФЕКТИВНОСТИ РАБОТЫ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО КАНАЛАМ ПЭМИН

г.Рязань, ГОУВПО «Рязанский государственный радиотехнический университет»

В настоящее время всё больше автоматизированных систем (АС) в защищённом исполнении оснащаются техническими средствами защиты информации (ТСЗИ) от утечки по каналам побочных электромагнитных излучений и наводок (ПЭМИН). Если раньше ТСЗИ ПЭМИН применялись в основном для защиты АС, предназначенных для обработки информации, содержащей сведения, составляющие государственную тайну, то в последние годы был принят ряд законов, а также выпущены нормативные и руководящие документы ФСБ России и ФСТЭК России, определяющие необходимость применения ТСЗИ ПЭМИН в АС, обрабатывающих персональные данные, служебную тайну, а также информацию, составляющую коммерческую тайну.

При проектировании современных АС наиболее широкое применение получают ТСЗИ ПЭМИН двух видов: активные (генераторы электромагнитного шума, ГШ) и пассивные (сетевые помехоподавляющие фильтры, ПФ). Настройка и проверка эффективности работы ГШ и ПФ для каждой конкретной АС выполняются при проведении аттестационных испытаний, а также впоследствии при проведении контроля эффективности (КЭ) защиты информации. Несоблюдение рекомендаций по регулярному выполнению КЭ в силу различных причин, а также тот факт, что среднее время наработки на отказ для некоторых часто применяемых сертифицированных пассивных ПФ составляет около 10000 часов, что лишь ненамного превышает рекомендуемую периодичность КЭ, делают актуальной задачу постоянного мониторинга эффективности работы ТСЗИ ПЭМИН, применяемых в ответственных АС. Усугубляют проблему неизбежные процессы старения активных радиоэлементов как в самих ТСЗИ ПЭМИН, так и в защищаемых с их помощью технических средствах обработки информации, что, в свою очередь, приводит к изменению характеристик затухания и усиления, сдвигу частотных спектров, возможному появлению паразитной генерации и т.п.

В предлагаемый комплекс средств мониторинга входят: управляющая ЭВМ, портативный прибор для измерения частоты и мощности сигнала с подключенным к нему индукционным токосъемником (для мониторинга цепей электропитания и заземления), компьютерный сканирующий приемник (для анализа сигналов в эфире), а также, при необходимости, вспомогательные датчики, такие как обнаружитель включенных сотовых телефонов. Все используемые приборы имеют интерфейсы подключения к ПЭВМ и управляются с помощью специального программного обеспечения, позволяющего получить картину ПЭМИН от средств обработки информации при выключенных ТСЗИ ПЭМИН, при включенных и настроенных ТСЗИ ПЭМИН после проведения аттестации объекта (начальные эталонные значения), и в ходе дальнейшей эксплуатации АС проводить автоматический мониторинг текущего состояния и отслеживать изменении параметров ПЭМИН от средств обработки информации и контролировать качество закрытия каналов утечки информации за счет ПЭМИН с помощью ТСЗИ ПЭМИН.

При обнаружении тенденции изменения параметров ПЭМИН от средств обработки информации и (или) ухудшения качества работы ТСЗИ ПЭМИН администратору безопасности выдается соответствующее предупреждение, а в случае сбоя или отказа ТСЗИ ПЭМИН или иной критической ситуации процесс обработки конфиденциальной информации автоматически останавливается.

Солодков М.Н.

МЭЙНФРЕЙМ IBM SYSTEM Z - ПЛАТФОРМА ДЛЯ ПОСТРОЕНИЯ БЕЗОПАСНЫХ ИС С ВЫСОКОЙ КОНЦЕНТРАЦИЕЙ ДАННЫХ

г.Москва, ИБМ Восточная Европа/Азия

Одной из тенденций развития информационных систем (ИС) является тенденция централизации информационно-вычислительных ресурсов, предназначенных для обеспечения систем управления различного назначения информацией, необходимой для принятия эффективных управленческих решений. В условиях современности, которые характеризуются динамично меняющейся обстановкой, эффективное и оперативное управление становится просто жизненно необходимым.

Информация является не только ключевым звеном любой системы управления, но и в большей степени главнейшим ресурсом любой компании или организации. Вот почему вопросы информационной безопасности при организации узлов обработки и хранения данных имеют первостепенное значение, особенно при высокой концентрации этого ресурса.

Исходя из трактовки информационной безопасности как совокупности трёх составляющих: **конфиденциальности, целостности и доступности** данных, можно сделать вывод, что платформа, на которой строится ИС, содержащая критически важную информацию, обязательно должна соответствовать **всем** этим трём требованиям.

В докладе представляется платформа серверов **System z** компании IBM, которая является флагманом линейки серверов компании, «технологическим прототипом» всех серверных продуктов корпорации, особенно в части касающейся технологий информационной безопасности и позиционируется как центральная часть любой достаточно крупной системы с большой концентрацией критических данных.

В свете требований по информационной безопасности, рассматриваются особенности этой аппаратно-программной платформы, позволяющие выделить её в ряду аналогичных продуктов IBM и других мировых производителей.

К таким особенностям можно отнести:

- набор программно-технических средств, обеспечивающих **конфиденциальность** хранимых и обрабатываемых данных:
  - изоляция процессов
  - встроенные технологии шифрования, защита трактов обмена данными и предотвращения вторжений
  - программные средства разграничения доступа и мониторинга безопасности, в том числе и реализованные в СУБД DB2

- встроенный функционал для построения удостоверяющих центров PKI, и многое другое;

- ряд уникальных архитектурных и технологических решений, предназначенных для обеспечения **целостности** обрабатываемых и хранимых данных:
  - контроль корректности данных в процессе вычислений
  - резервирование всех узлов системы и трактов обмена информацией с автоматической реконфигурацией
  - технологии «зеркалирования» данных, хранящихся на внешних носителях и т.п.;
- конструктивные и архитектурные особенности, а также кластерные технологии, позволяющие достигнуть высочайшего уровня **доступности** систем на уровне приложений и данных:
  - возможность проведения работ с оборудованием в большинстве случаев даже без остановки приложений
  - многоуровневая виртуализация аппаратных ресурсов, обеспечивающая высокую живучесть комплекса
  - программно-аппаратный кластер Parallel Sysplex
  - архитектура географически разнесённых информационных ресурсов GDPS для построения катастрофоустойчивых решений и многое другое.

Широкий опыт использования платформы для построения ИС, к которым предъявляются повышенные требования по информационной безопасности (в первую очередь в таких областях, как государственные органы управления, банковский сектор, управление транспортом) доказывает, что решения на базе технологий IBM System z заслуживают самого пристального внимания со стороны разработчиков информационно-телекоммуникационных систем.

Суворов А.А.

АРХИТЕКТУРА СЕТЕЙ СВЯЗИ С РАЗГРАНИЧЕНИЕМ ДОСТУПА НА ОСНОВЕ ШЛЮЗОВ КОНТРОЛЯ ДОСТУПА

г.Санкт-Петербург, ГОУ «СПбГПУ»

В сетях связи с разграничением доступа, существует проблема распределенного контроля потоков данных между узлами сети, состоящая в контроле и мониторинге установления сеансов связи по одной из трех возможных схем: «точка-точка», «звезда» или «каждый с каждым», в рамках которых осуществляется одно- или двунаправленный обмен данными между двумя или несколькими узлами сети. Для решения этой проблемы предлагается архитектура сетей связи с разграничением доступа, основанная на использовании шлюзовых технологий, объектом доступа в которой является информация, циркулирующая в переделах сеансов связи.

Для организации защиты сети связи с разграничением доступа должны быть добавлены следующие компоненты: шлюзы контроля доступа (ШКД), центр управления доступом (ЦУД) и Пульты Управления (ПУ). Шлюзы контроля доступа обеспечивают распределенную защиту узлов сети и производят непосредственный контроль над установлением сеансов связи. Каждый оконечный узел системы подключается к сети связи через ШКД. Центр управления доступом используется как рабочее место администратора сети, обеспечивающее автоматизированное централизованное принятие решений о возможности установления сеансов связи между кончеными узлами сети, отправляя на соответствующие ШКД управляющие команды. Пульты управления предназначены для инициации сеансов связи абонентами системы: создание новых сеансов, подключение и выход из установленных, и отклонение, при необходимости, входящих запросов на установление сеанса. Также ПУ предоставляет абоненту информацию о текущем состоянии и список пользователей сети и сеансов, к которым возможно подключение.

Центр управления доступом принимает решение о доступе основываясь на гибкой политике безопасности и текущем состоянии системы. В качестве модели контроля доступа используются мандатный и дискреционный контроля доступа. Шлюзы контроля доступа решают задачу контроля потоков данных путем осуществления коммутации соединений между узлами и сетью передачи данных. В состоянии бездействия все соединения между узлами запрещены. В момент создания сеанса связи абонент указывает участников сеанса, используя пульт управления. Центр управления доступом проверяет легитимность запрашиваемого сеанса связи и отправляет на ШКД команды, разрешающие создать между участниками сеанса каналы связи, по которым будет передаваться информация.

Предлагаемая архитектура накладывает несколько ограничений: требуется сеть шифрованной связи, возможно использование только одного приложения в сети связи и за оконечным узлом сети может работать только один абонент. Таким образом, решение может быть использовано для построения защищенных информационно-технических каналов связи, таких как VoIP и видеоконференцсвязь. При этом

обеспечивается автоматизация принятия решений распределенного контроля доступа к потокам данных, основывающаяся не только на используемой модели контроля доступа, но и на состоянии системы. Используемое централизованное управление предоставляет администратору возможность контролировать все происходящие в системе события в режиме реального времени. Применение пультов предоставляет пользователю два основных преимущества: возможность отказа от установления сеанса связи и возможность отслеживания состояний установленных с ним сеансов связи. Также важным преимуществом решения является его прозрачность для всего оборудования и программного обеспечения сети связи. Предложенное решение показывает возможность применения шлюзовых технологий для решения проблемы распределенного контроля потоков данных в сетях связи с разграничением доступа.

Яковенко П.Н., Бурдонов И.Б., Косачёв А.С.

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ АППАРАТНОЙ ВИРТУАЛИЗАЦИИ ДЛЯ ЗАЩИТЫ ВЫПОЛНЕНИЯ ПРИЛОЖЕНИЯ В НЕДОВЕРЕННОЙ ОПЕРАЦИОННОЙ СИСТЕМЕ

г.Москва, Институт системного программирования РАН

Современные массовые операционные системы (Linux, Windows и пр.) характеризуются сравнительно большим размером кода и недостаточной надежностью. Большой объем кода затрудняет аттестацию операционной системы (ОС) на отсутствие недокументированных возможностей (закладок) даже в условиях наличия доступа к исходным текстам ОС. Недостаточная надежность обусловлена монолитной архитектурой ядра ОС, слабо изолирующей подсистемы ядра. Воспользовавшись уязвимостью в одной из компонент ядра (например, в драйвере устройства), злоумышленник может получить полный контроль над ресурсами компьютера.

Такое состояние массовых ОС ставит под вопрос целесообразность их использования на компьютерах, обрабатывающих конфиденциальные данные, в условиях наличия публичного канала связи. Однако, наличие большого числа существующих приложений для таких ОС не позволяет полностью отказаться от них, что делает задачу построения системы безопасности, обеспечивающей защиту выполнения критически важного приложения в недоверенной ОС, актуальной.

Технология аппаратной виртуализации позволяет выполнять ОС в виртуальной машине (ВМ) под контролем сравнительно небольшой по размеру системной программы – монитора виртуальных машин (гипервизора). Гипервизор выполняется на более высоком уровне аппаратных привилегий по сравнению с ядром ОС и полностью контролирует доступ ОС к аппаратным ресурсам. Система безопасности, реализованная на уровне гипервизора, аппаратно защищена от атак со стороны ОС, а использование специализированных процессорных инструкций обеспечивает ей высокую эффективность.

Система безопасности гарантирует надежное обнаружение атак на исполняемый код и данные приложения, расположенные в памяти компьютера, даже в условиях работы системы свопинга в ОС. Гипервизор перехватывает все переключения контекста между защищаемым процессом и ядром ОС, а также все операции записи в физические ячейки памяти, занятые кодом и данными защищаемого процесса, выполняемые из недоверенного контекста (например, контекста ядра ОС). Гипервизор гарантирует, что любое несанкционированное изменение ресурсов процесса: изменение потока управления (адреса возврата из прерывания), порча ячеек памяти, занятых кодом и данными процесса, - будет обнаружено до того, как процесс выполнит хотя бы одну инструкцию испорченного кода или получит доступ к испорченным данным.

Такая система защиты может служить основой для предоставления доверенному процессу (и только ему) монопольного доступа к сети Интернет. Для этого гипервизор перехватывает системные вызовы доверенного процесса, относящие к сетевому взаимодействию, и делегирует их выполнение другой ВМ, выполняющейся

параллельно на этом же компьютере. Исходная ВМ физически изолирована от сети, поэтому передача конфиденциальных данных вредоносным кодом (в т. ч. в ядре ОС) на удаленный компьютер не представляется возможной. В свою очередь, попытка использовать контекст доверенного процесса для передачи украденных данных, требующая внедрения вредоносного кода в адресное пространство процесса, будет немедленно обнаружена и пресечена гипервизором.

Раздел 1.
Современные технологии обеспечения безопасности информационных систем и телекоммуникаций

Раздел 1.2.
Безопасность распределённых систем и обнаружение вторжений

Борисов В.В.

ТЕХНОЛОГИИ ЗАЩИТЫ СИСТЕМ УПРАВЛЕНИЯ СЕТЕВЫМИ УСТРОЙСТВАМИ

г.Санкт-Петербург, ЗАО «НПП «СТЗИ»

Необходимость создания и сертификации защищенной системы управления сетевыми устройствами: коммутаторами, маршрутизаторами, серверами и шлюзами обусловлена наличием большого количества распределенных систем и сетей, требующих стойких механизмов защиты информации.

В отличие от традиционных систем хранения и обработки данных, для систем управления характерны не только основные угрозы нарушения конфиденциальности, целостности и доступности. Для систем управления также имеют место угрозы отказа администратора от ответственности за конфигурацию управляемого оборудования и угроза распространения атакующих воздействий на всю сетевую инфраструктуру.

Защищенная система управления должна реализовывать централизованный унифицированный контроль доступа к различным объектам управления, что позволит использовать один экземпляр системы управления для управления множеством экземпляров разнородного сетевого оборудования, обрабатывающего информацию различных категорий. При этом система контроля доступа должна позволять использовать дискреционный и мандатный контроль доступа администраторов к управлению сетевым оборудованием, обеспечивать возможность гибкой настройки политики безопасности.

Централизованный аудит всех событий управления с установлением ответственности администратора также является необходимым условием решения задач доверенного управления. Подсистема хронологического контроля событий, выявления ошибок в настройках сетевого оборудования, фактов злоупотребления или нарушений со стороны обслуживающего персонала позволит формализовать процесс управления и задания критериев корректной конфигурации. Отдельными задачами при этом являются: обеспечение резервного копирования журналов, а также создание доверенного сервиса регистрации событий уровня сетевого оборудования, информация о которых передается с управляемого оборудования на систему управления.

Защищенное управление сетевыми устройствами должно осуществляться с использованием доверенного канала передачи информации (управления) на основе стека протоколов TCP/IP, защищаемого с помощью средств криптографической защиты информации, что должно обеспечить защиту от внешнего нарушителя и недобросовестных поставщиков каналов связи. Отдельной задачей является обеспечение изоляции скомпрометированных сетевых сегментов, обеспечение невлияния локальных ошибок на распределенную систему в целом.

Для эффективного управления в распределенных сетях передачи данных требуется решение задач графического представления, мониторинга производительности и других параметров сетевых ресурсов в рамках модели FCAPS (ISO/IEC 10040). Защищенная система управления должна реализовывать функции управления отказами, конфигурацией, учетом, производительностью и безопасностью. Указанные функции могут быть реализованы самой системой управления или с помощью внешних систем представления, мониторинга и управления информационной инфраструктурой, основанных на общепринятом протоколе управления сетевым оборудованием SNMP. Средства защищенной системы управления должны обеспечивать контроль функционирования указанных внешних систем.

Разрабатываемые варианты защищенных систем управления должны основываться на доверенных компонентах и сопровождаться полным комплектом конструкторской и эксплуатационной документации, а также набором исходных текстов. Это позволит провести сертификацию на заданный уровень требований к информационной безопасности, и далее использовать разработанную систему управления в реальных защищенных информационных средах с предъявлением требований к информационной безопасности.

Построение защищенных систем управления на основе предлагаемых технологий обеспечит соответствие современным требования к информационной безопасности и защиты от компьютерных атак, отвечая потребностям конечных потребителей.

Зегжда Д.П., Калинин М.О.

НЕОБХОДИМОСТЬ СЕРТИФИКАЦИИ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

г.Санкт-Петербург, ГОУ "Санкт-Петербургский государственный политехнический университет"

Система обеспечения информационной безопасности (СОИБ) интегрирует систему информационной безопасности (СИБ), включающую средства защиты информации (СЗИ), их ресурсное и административное обеспечение и процессы эксплуатации, а также систему управления информационной безопасностью (СУИБ), образованную средствами установления, мониторинга и совершенствования средств защиты [1].

Для установления и подтверждения того факта, что СОИБ выполняет поставленные перед ней задачи, применяется сертификация разрабатываемых решений. Система сертификации СЗИ в РФ представляет собой устоявшийся институт. В рамках процедуры сертификации при испытаниях и исследованиях завяленных СЗИ верифицируется, что данные средства обеспечивают указанный уровень безопасности. При успешном прохождении испытаний производителю СЗИ выдается сертификат, удостоверяющий, что СЗИ допускается использовать при осуществлении деятельности, требующей по закону обязательного использования сертифицированных средств. Однако наличие сертификата на СЗИ не гарантирует стационарности выполнения технических условий работы СЗИ и, как следствие, стабильного обеспечения работоспособности, безопасности защищаемых систем и постоянного соблюдения защитных мер, адекватных рискам реализации угроз информационной безопасности.

Для выполнения сертифицированными СЗИ заявленных функций должен соблюдаться установленный для них режим эксплуатации, который определяется совокупностью параметров самих СЗИ (в т.ч. системной конфигурацией, настройками совместимости ПО, рабочими установками, настройками безопасности, пользовательским составом). В этой связи, главные причины инцидентов информационной безопасности, происходящих с сертифицированными СЗИ, обусловлены не ошибками производителей и сертификационных лабораторий, а нарушениями, допущенными при управлении программной рабочей средой этих средств. Поскольку подобные просчеты характерны для любого СЗИ, а постоянно контролировать соблюдение регламента функционирования сертифицированного СЗИ в современных гетерогенных системах весьма затруднительно, то в настоящее время для решения данной проблемы наряду с СЗИ развивается целый класс средств сопряжения, осуществляющих мониторинг и воздействие на СЗИ и рабочую среду. Совокупность таких средств образует СУИБ. В рамках информационных систем СУИБ обеспечивает поддержку параметров основных и вспомогательных процессов информационной безопасности в заданных пределах и их корректировку в случае изменения внешних и внутренних условий функционирования и безопасности.

Поскольку СУИБ не только контролируют СЗИ, но и оказывают управляющие воздействия на их параметры, а также на параметры рабочей среды, то одновременно с осознанием потребности в СУИБ возникает необходимость в подтверждении корректности их работы. В этой связи становится весьма актуальной задача сертификации СУИБ.

Согласно [2] к СЗИ относятся технические, криптографические, программные и др. средства, предназначенные для защиты сведений, составляющих гостайну,

средства, в которых они реализованы, а также средства контроля эффективности защиты информации. Следуя данному определению, СУИБ не относится к СЗИ, хотя непосредственным образом обеспечивает безопасность информационных систем путем настройки и поддержания стабильности параметров СЗИ и цельности характеристик рабочей среды. Таким образом, СУИБ не подпадает под действие нормативных документов и стандартов, определяющих процедуру сертификации СЗИ. С другой стороны, на корпоративном уровне для СУИБ, называемых в этом случае системами менеджмента информационной безопасности (СМИБ), проводятся сертификационные испытания в рамках международной системы стандартов ИСО 27001 [3].

С учетом этого и на основе анализа требований стандартов, касающихся верификации СМИБ, авторами поднимается вопрос о необходимости разработки совокупности требований для программных СУИБ с целью расширения существующей в РФ нормативной базы сертификации программных средств обеспечения информационной безопасности и привязки СУИБ к уровням защиты СЗИ и классам обрабатываемой информации.

Исследование задач, перечисленных в стандартах семейств ИСО 27001 [3], 13335 [4], 18044 [5], приводит к заключению об этапности и цикличности процесса управления информационной безопасностью, что позволяет сформулировать по отношению к СУИБ требования, затрагивающие управляющие процедуры: формирование условий функционирования и безопасности активов, контроль текущей системной конфигурации на предмет соблюдения этих условий и адаптация параметров безопасности.

Наличие в СУИБ аппарата критериев безопасности позволяет сформировать некую область безопасности, в которую входят управляемые активы и множество параметров, обеспечивающих безопасность информационной системы. СЗИ, их рабочая среда, как и информационная система в целом, изменяются в ходе эксплуатации и реализации угроз безопасности. Поэтому условия служат индикаторами безопасности, и их нарушение является признаком отклонений в конфигурации системы, требующих вмешательства со стороны СУИБ с целью предотвращения эскалации угроз. При этом проверка условий должна быть периодичной.

Для реализации управления необходимы требования моделирования процессов, происходящих в управляемых системах, в части описания механизмом функционирования средств защиты, воздействия параметров системы, влияния внутренней и внешней среды на конфиденциальность, целостность и доступность информационных ресурсов.

СУИБ должна также включать механизм адаптации управляемых систем. Для обеспечения согласованности параметров СЗИ и условий реализации заданных условий функционирования и безопасности требования, предъявляемые к СУИБ, должны затрагивать функционал управления безопасностью, срабатывающий в случае возникновения нарушений. Воздействие, как и контроль, должно выполняется посредством направленного влияния на параметры безопасности информационных систем.

Таким образом, являясь средством сопровождения информационной безопасности, которое обеспечивает не только анализ безопасности, но и позволяет воздействовать на параметры управляемых защищенных систем с целью достижения ими стационарности, СУИБ нуждаются в построении системы сертификационных требований, отражающих эту специфику систем управления.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Стандарт Банка России СТО БР ИББС-1.0-2008. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения. 2008.

2. Пост. Прав-ва РФ "О сертификации средств защиты информации" №608, 26.06.1995.

3. ГОСТ Р ИСО/МЭК 27001. Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования. 2005.

4. ГОСТ Р ИСО/МЭК 13335. Информационная технология. Методы и средства обеспечения безопасности. Ч.1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. 2006.

5. ГОСТ Р ИСО/МЭК 18044. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. 2007.

Зегжда Д.П., Калинин М.О., Москвин Д.А.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПОЛНОФУНКЦИОНАЛЬНЫХ ИНФОРМАЦИОННЫХ КОМПЛЕКСОВ БИЗНЕС-ПРИЛОЖЕНИЙ

г.Санкт-Петербург, ГОУ "Санкт-Петербургский государственный политехнический университет"

Для обработки больших объемов различных данных используют полнофункциональные комплексы интегрированных бизнес-приложений и мощные развитые СУБД для их хранения. Если обрабатываемые данные носят конфиденциальный характер, то для их обработки и хранения требуется использовать сертифицированные программные средства. Однако существующие сертифицированные решения не обладают достаточной функциональностью. Полнофункциональные программные комплексы и СУБД, такие как Oracle E-Business Suite и Oracle Database, напротив, обеспечивают всю необходимую функциональность, но не сертифицированы в РФ. Дополнительной проблемой является то, что Oracle E-Business Suite основан на Java-технологиях. Если сертификация Java-машины — трудоемкая, но решаемая задача, то сертификация различных серверов Java-приложений и других Java-программ невозможна ввиду их "объемности", многообразия и изменяемости (постоянные обновления, выпуски новых версий и т.д.). Поэтому необходим подход, позволяющий использовать популярные бизнес-приложения и базы данных (БД) для хранения конфиденциальной информации. Следовательно, возникает задача обеспечения защиты функционального программного обеспечения (ПО) в информационных системах с ограниченным уровнем доступа.

Для решения данной задачи и сокращения объемов сертификационных исследований применимы два подхода:

1. Разработка и применение условий, при эксплуатации в которых функциональное ПО можно не сертифицировать.

2. Разработка программной "прослойки" — набора специального ПО, которое позволит контролировать работу функционального ПО и СУБД, избегая необходимости их сертификации.

Основной угрозой при работе с недоверенным ПО является возможное наличие в нем программных закладок, благодаря активации которых злоумышленники могут получить несанкционированный доступ к данным, исказить или уничтожить их. Поэтому для использования недоверенного ПО необходимо предложить решение позволяющее обеспечить конфиденциальность, целостность и доступность данных на всем протяжении эксплуатации информационной системы.

Наибольшие сложности возникают с обеспечением доступности данных. Так, например, невозможно гарантировать, что в СУБД в определенный момент времени не активируется программная закладка, которая уничтожит всю хранимую в БД информацию.

Угроза конфиденциальности возникает тогда, когда существует некоторый суперпользователь, который в обход системы контроля доступа сможет манипулировать информацией в БД или перехватить информацию в процессе ее обработки в функциональном ПО. Для решения этой проблемы информационную систему предлагается разделить на несколько контуров. В разных контурах должна храниться и обрабатываться информация разной степени секретности. Тогда в одном контуре будет храниться равносекретная информация. Все пользователи, работающие в некотором контуре, должны обладать полномочиями полного доступа ко всем данным

в этом контуре. В этом случае утечки информации или несанкционированный доступ к ней становятся невозможными.

Для устранения угрозы целостности необходимо гарантировать, что данные не искажаются во время хранения в БД или во время обработки в функциональном ПО. Для контроля целостности во время хранения необходимо вычислять значение некоторой хеш-функции от данных — маркера целостности. "Традиционно" при контроле целостности эталонные значения маркеров целостности вычисляются сразу после добавления данных в БД. Однако такой подход не позволяет гарантировать вычисление эталона от целостных данных, т.к. данные могут быть искажены уже в процессе добавления в БД. Эталонные значения маркеров целостности для данных, хранимых в БД, должны вычислять в тот момент, когда возможные программные закладки гарантированно не активированы или не могут исказить данные. Следовательно, наиболее подходящим моментом является тот, когда данные еще не добавлены в БД. Сами же эталонные значения маркеров целостности должны храниться в некоторой доверенной БД, предоставляющей базовую функциональность.

Для контроля целостности данных при их обработке в функциональном ПО необходимо обеспечить контроль запросов к БД. Другими словами, необходимо гарантировать, что на одинаковые запросы всегда выдаются одинаковые правильные ответы. Для этого требуется вычислять маркеры целостности также для ответов на все запросы к БД. Поскольку объем множества возможных запросов к БД стремится к бесконечности, необходимо его ограничить запросами, используемыми функциональным ПО. Для всех таких запросов должны быть заранее, до сохранения данных в БД, вычислены маркеры целостности от правильных ответов на них. В дальнейшем, при добавлении или изменении данных в БД, все маркеры целостности ответов на запросы должны вычисляться заново.

Таким образом, для контроля целостности данных при их хранении в недоверенных БД и обработке недоверенным функциональным ПО необходимо (см. рис.):

1. Обеспечить "перехват" всех данных, поступающих на вход СУБД и функционального ПО.
2. Вычислять эталонные маркеры целостности для этих входных данных.
3. Вычислять маркеры целостности всех выходных данных, а также ответов на запросы, получаемых из СУБД и функционального ПО.
4. Сравнивать полученные значения маркеров целостности выходных данных с эталонными.

При использовании данного подхода эталонные значения маркеров целостности вычисляются от гарантированно неискаженных данных. Следовательно, все возможные искажения, вносимые в данные функциональным ПО или СУБД будут выявлены.

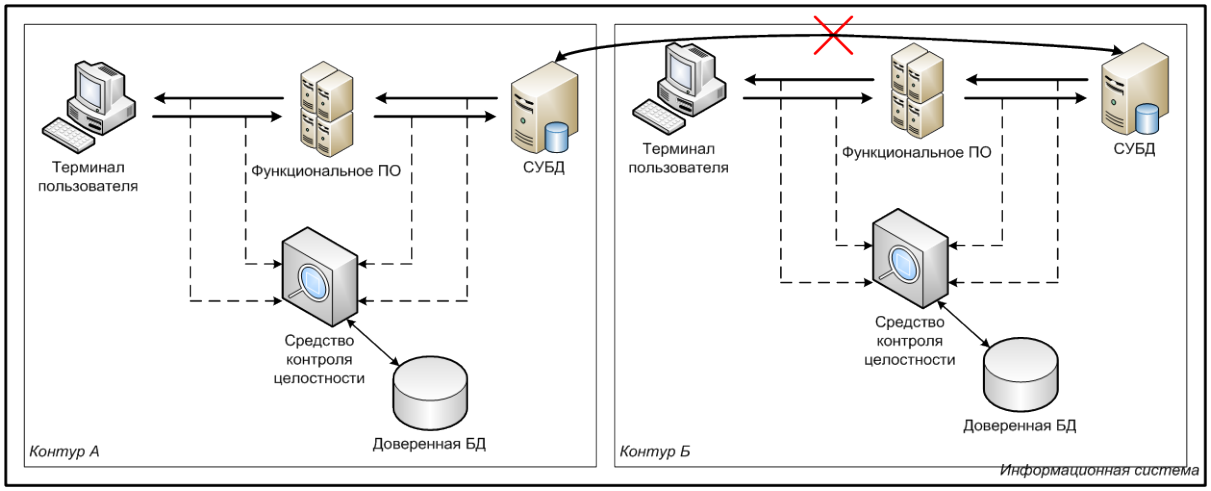


Рис. Схема обеспечения безопасности информационной системы

Перечисленные методы позволяют хранить и обрабатывать конфиденциальную информацию в полнофункциональных комплексах интегрированных бизнес-приложений и СУБД, защищая их от угроз нарушения конфиденциальности и целостности.

Казаков А.А.

ПРОТИВОДЕЙСТВИЕ СЕТЕВЫМ АТАКАМ В INTERNET И КЛАССИФИКАЦИЯ МЕТОДОВ ЗАЩИТЫ

г.Санкт-Петербург, ГОУ «СПбГПУ»

В докладе рассматриваются следующие вопросы:

- Определение угроз безопасности узлов Internet и их классификация.
- Существующие подходы к защите узлов Internet от рассмотренных угроз.
- Анализ и классификация методов защиты узлов Internet.

Угрозы безопасности узлов Internet могут быть подразделены на два типа:

1) Вызванные атаками, использующими уязвимость в реализации программного обеспечения узла.

Как правило, данные атаки не требуют посылки больших объемов данных, достаточно нескольких пакетов специального для используемой уязвимости содержания существуют исключительные ситуации, например, когда уязвимость атакуется посылкой нескольких очередей пакетов, когда резкие всплески интенсивности обрабатываемых данных вызывают сбой.

2) Вызванные большими объемами трафика предназначаемого для атакуемого узла, что ведет к поглощению ресурсов самого узла (процессорное время, память), а также монополизирует канал. Последствием данной атаки является не возможность атакуемого узла обрабатывать запросы реальных пользователей.

Наиболее существенной угрозой безопасности для систем, предоставляющих прикладные сервисы для пользователя является распределенный отказ в обслуживании, большинство рассмотренных методов защиты в данном докладе посвящены защите от распределенного отказа в обслуживании.

Существующие подходы к защите узлов Internet можно поделить на два типа:

1) Защита средствами сетевого узла. Методы данного типа целиком реализуют механизмы защиты непосредственно на защищаемом узле.

В качестве примеров данного типа выступают: Методы определения отправителя, в данном случае отдельный сетевой узел пытается, основываясь на различных критериях установить аутентичность источника трафика, например в Hop Count Filtering(метод проверки аутентичности отправителя) это сопоставление значения TTL и адреса источника, TCP/IP proxy(метод защиты узла от уязвимостей в реализации TCP/IP) решения, которые являются посредником между клиентом и штатной реализацией протоколов, что предостерегает узел от известных уязвимостей.

2) Защита средствами маршрутизации. Данные подходы работают как динамические механизмы маршрутизации, тем самым создается Overlay Network(множество доверенных узлов создающих сеть), где при передаче сообщений от клиента путь их прохождения выбирается динамически. Например сети компании Akamai, технология MONET руководствуются данным принципом.

Приведена классификация методов защиты узлов Internet рассмотренных в данном материале, основываясь на различных признаках, например: тип угрозы, от которой обеспечивается защита, условия реализации атаки, которой способен противостоять рассматриваемый метод защиты, например количество атакующих узлов в заданной топологии сети, количество и специфика ложных срабатываний, применимость метода в сетях Internet и т д.

На основе проведенной классификации сформулированы требования к методам защиты узлов Internet от сетевых угроз и сделано предположение о комплексном подходе к защите от отказа в обслуживании.

Калинин М.О.

ТЕХНОЛОГИЯ ПОСТРОЕНИЯ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

г.Санкт-Петербург, ГОУ "Санкт-Петербургский государственный политехнический университет"

Указанная в нормативных документах (ГОСТ семейства 27001, 13335, 18044) номенклатура задач, решаемых системами организационного менеджмента информационной безопасности, определяют необходимость и актуальность создания систем управления информационной безопасностью (СУИБ), на системном уровне выполняющих функции регулятора защитных механизмов в информационно-телекоммуникационных системах (ИТКС), а также позволяют сформулировать перечень требований, выдвигаемых к СУИБ. Являясь частью общей системы обеспечения безопасности, СУИБ должна реализовывать и поддерживать защиту активов, адекватную угрозам, как случайным, так и преднамеренным, с соблюдением принципа постоянного контроля, анализа и улучшения средств защиты, используемых в ИТКС (т.н. модель PDCA). Поэтому жизненный цикл СУИБ состоит из следующих этапов:

- формирование условий функционирования и безопасности активов ИТКС;
- контроль текущей системной конфигурации на предмет соблюдения этих условий;
- управление безопасностью информации.

Указанный перечень определяет состав и назначение структурных компонентов СУИБ. Задачей СУИБ является контроль и удержание безопасности на приемлемом уровне. Поэтому при построении СУИБ требуется обеспечить задание необходимого уровня безопасности. Поскольку он определяется набором условий функционирования и безопасности, сформированных из целей создания ИТКС, ее назначения, особенностей эксплуатации, актуального множества угроз информационной безопасности, требований безопасности, сформулированных в стандартах, правилах корпоративной политики информационной безопасности, ТУ функционирования сертифицированного ПО, то данные действия сопряжены с набором мероприятий по системному анализу ИТКС. Для описания этих условий широко применяются языковые средства, так как они обеспечивают универсальное и формализованное представление ограничений. Для определения источников актуальных угроз информационной безопасности в ИТКС и оценки вероятности их реализации полезным является перечень наиболее часто встречающихся угроз (примеры типовых угроз приведены в приложении С стандарта ГОСТ 13335-3). Также необходимо использовать каталоги угроз, соответствующие конкретной сфере применения ИТКС. Для анализа угроз безопасности ИТКС необходимо:

- установить область безопасности ИТКС;
- проанализировать уязвимости ИТКС;
- оценить риски информационной безопасности

В область безопасности должны быть включены наиболее ценные активы ИТКС, для которых необходимо управление. При установлении активов используется два способа. Первый заключается в инвентаризации всех активов и согласовании масштабов возможного ущерба. При этом оценка важности активов может быть как количественной (например, в денежном выражении), так и качественной (например, по

шкале "низкий-высокий"). Второй подход основан на оценке рисков и финансовых затрат организации по причине утраты конфиденциальности, целостности или доступности активов вследствие инцидентов. Анализ уязвимостей ИТКС заключается в идентификации источников (причин угроз) и объектов (элементов ИТКС, которые могут подвергнуться воздействию) угроз информационной безопасности. При этом необходимо оценить, насколько велика степень уязвимости или насколько вероятно ее использовать. Оценка рисков информационной безопасности позволяет связать оценку важности активов и оценку угроз. Методики оценки рисков разнообразны, что позволяет выбрать наиболее удобные для организации и применения в рассматриваемой ИТКС.

Реализованные в ИТКС защитные меры должны удовлетворять требованиям, выявленным на этапах оценки и обработки активов. Активная составляющая СУИБ заключается в контроле соблюдения заданных условий функционирования и безопасности, а также в управлении безопасностью информации в случае возникновения нарушений данных условий. При этом безопасность ИТКС обеспечивается следующим набором защитных мер:

- идентификация и аутентификация пользователей;
- выполнение правил контроля доступа;
- обеспечение регистрации происходящих в ИТКС событий;
- функционирование криптографических подсистем.

ИТКС и среда ее функционирования постоянно изменяются в результате функционирования самой системы, применяемых средств защиты и срабатывания угроз. С целью обеспечения взаимосогласованности (функциональной совместимости) защитных средств и реализации заданного уровня безопасности ИТКС СУИБ должна содержать средства подключения/отключения, контроля состояния и управления конфигурацией. Для этого средства СУИБ должны реализовывать следующие процедуры:

- обнаружение нарушений условий функционирования и безопасности в текущем состоянии ИТКС;
- определение результативности мер защиты при нарушениях;
- осуществление надлежащих корректирующих и предупреждающих действий.

Для осуществления контрольных и управленческих функций СУИБ должна содержать средства фиксации и изменения параметров безопасности ИТКС (состава используемых средств защиты; параметров их совместимости; конфигураций безопасности системного и пользовательского ПО). На этапе контроля также допустимо выполнение периодического анализа рисков нарушений безопасности и остаточных рисков с целью оценки возможных финансовых затрат организации. Необходимым условием реализации приведенного функционала является наличие интерфейса, позволяющего обеспечить необходимый уровень безопасности при осуществлении функций фиксации, проверки и тестированиям параметров безопасности ИТКС путем настройки параметров безопасности. Подсистема управления безопасностью на основании информации по инцидентам и заданным условиям функционирования и безопасности ИТКС должна обеспечит устранение выявленных нарушений безопасности. Средства настройки должны выполнять:

- подготовку, включая предупреждающие меры, рекомендации и процедуры по обработке инцидентов (включая сохранение доказательных данных, обслуживание файлов регистрации событий и уведомительную связь);

– оценку, включая процедуры по анализу состава нарушений и определению уровня их опасности;

– управление, включая процедуры по обработке нарушений, снижению ущерба от них и уведомлению пользователей;

– восстановление, включая процедуры по возобновлению нормальной работы ИТКС после серьезных нарушений безопасности.

СУИБ должна содержать механизмы документирования для обеспечения прослеживаемости действий и воспроизводимости результатов управления.

Таким образом, содержание процесса управления информационной безопасностью определяет необходимый состав и функциональное назначение компонентов СУИБ, а также технологию их построения.

Марков Я.А., Калинин М.О.

ПРИМЕНЕНИЕ АЛГОРИТМА СРАВНЕНИЯ ГЕНЕТИЧЕСКИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЛЯ ОБНАРУЖЕНИЯ МОДИФИЦИРОВАННЫХ АТАК

г.Санкт-Петербург, ГОУ "Санкт-Петербургский государственный политехнический университет"

Защищаемая информационная система представляется как множество взаимодействующих сущностей. Взаимодействие называется информационным, если его целью и основным содержанием является изменение имеющейся информации хотя бы у одной из них. Информационное взаимодействие осуществляется в результате разрешения и выполнения т.н. команд, составляющих множество C. Множество возможных взаимодействий в дискретных системах конечно и определяется семантикой системы и заданным уровнем абстракции (например, на системном уровне ОС Unix определены взаимодействия "чтение", "запись" и "исполнение"). Команды выполняются при истинности заданных в системе условий доступа (например, когда в ячейке матрицы доступа соответствующей данным субъекту и объекту разрешен данный вид взаимодействия). При срабатывании условий и выполнении команд в результате информационного взаимодействия система выполняет переход из одного состояния в другое. Таким образом, зная, что в интервале времени $[t_1, t_2]$ выполнялись команды $C_1, C_2, \ldots, C_n$, $C_i \in C$, $i \in \mathbf{Z}^+$, указанной последовательности, можно определить траекторию системы $Tr(t_1,t_2) = s_{t_1} \xrightarrow{C_1} s_1 \xrightarrow{C_2} s_2 \xrightarrow{C_3} \ldots \xrightarrow{C_n} s_{t_2}$. Траектория является небезопасной, если при выполнении последовательности команд система становится небезопасной в терминах заданных условий при выполнении некоторой команды $C' \in C$. Атака, т.е. негативное воздействие на защищаемую систему, которое выводит ее из безопасного состояния вследствие реализации небезопасной траектории, всегда является элементом небезопасной последовательности команд. Задача обнаружения атаки состоит в том, чтобы, анализируя цепочку выполняющихся команд, выявить, присутствуют ли в ней последовательность команд, характерная для той или иной атаки.

Современным методом обнаружения атак является сопоставление текущей последовательности команд с имеющимися образцами атак (сигнатурный метод). Его недостатками являются:

– неограниченный рост базы сигнатур. Размер базы сигнатур определяется количеством атак, которое в последние годы растет экспоненциально, что определяет будущую неэффективность данного метода;

– защита от ограниченного множества атак. Система защищена только от тех атак, которые указаны в базе сигнатур;

– защита от известного множества атак. Система защищена от атак, которые проанализированы и занесены в актуальную базу. Для этого необходимы постоянный мониторинг нарушений и распространение обновленных баз;

– неэффективность при модифицированных атаках, команды которых совпадают с точностью до последовательности, но отличаются количеством команд.

Для устранения указанных недостатков авторами предлагается применять для обнаружения атак метод сравнения последовательностей, используемый в биоинформатике для сравнения ДНК[1]. Метод заключается в определении схожих

участков у нескольких последовательностей путем применения алгоритма выравнивания. Растягивая последовательности относительно друг друга и вставляя в них пустые участки, становится возможным получить оптимальное расположение последовательностей по отношению друг к другу, при котором их сходство максимально. В зависимости от особенностей разделяют локальное и глобальное выравнивания. Глобальное выравнивание растягивает меньшую последовательность вдоль большей. Локальное выравнивание, более известное как алгоритм Смита-Уотермана [2], применяется, когда длина одной последовательности значительно меньше, чем длина другой. Для обнаружения атак наиболее применим локальный метод, поскольку текущая последовательность команд значительно превышает длину последовательности команд атаки.

Рассмотрим пример обнаружения модифицированных атак с помощью алгоритма сравнения генетических последовательностей с локальным выравниванием. Пусть существует некоторая программа, которая из-за ошибки в реализации, уязвима к переполнению буфера. При использовании этой уязвимости специальной программой-эксплоитом выполняется следующая последовательность системных вызовов

```
setreuid(0,0);
open("/etc/passwd", O_APPEND|O_WRONLY);
write(fd, "newuser:password:0:0::/:/bin/sh", 31);
close(fd);
exit(0);
```

Данная последовательность команд в ОС Unix изменяет содержимое файла учетных записей, добавляя новую учетную запись суперпользователя. Если для данной атаки задана сигнатура, в точности повторяющая последовательность команд атаки, то модифицированная атака вида

```
setreuid(0,0);
     fork(); brk();
open("/etc/passwd", O_APPEND|O_WRONLY);
     time(); brk();
write(fd, "newuser:password:0:0::/:/bin/sh", 31);
     time(); fork();
close(fd);
     time(); brk();
exit(0);
```

с помощью сигнатурного метода обнаружена не будет.

Результатом работы алгоритма Смита-Уотермана являются выровненные последовательности *a* и *b*:

```
a = {setreuid, fork, brk, open, time, brk, write, time, fork,
close, time, brk, exit}
b = {setreuid, -   , -   , open, -  , -  , write, -   , -   ,
close, -   , -  , exit}
```

а также значение характеристической функции $R(a, b)$, определяющей степень сходства двух последовательностей. Атака определяется по граничному пороговому значению n: если $R(a, b) > n$, то это свидетельствует о наличии атаки.

Применение алгоритма Смита-Уотермана для решения задачи обнаружения атак, позволяет не только обнаруживать атаки, которые отсутствуют в базе сигнатур, но и модифицированные сигнатурные атаки. Также становится возможным формировать приоритеты команд, встречающихся в последовательностях, и указывать, какие из них

являются более опасными, какие не оказывают влияния на безопасность системы, что облегчает задачу построения вариативных программных датчиков атак в системах управления информационной безопасностью.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. **Mount D. W.** Bioinformatics: Sequence and Genome Analysis. Cold Spring Harbor Laboratory Press: Cold Spring Harbor, NY. 2004.

2. **Smith T. F, Waterman M. S.** Identification of Common Molecular Subsequences // Journal of Molecular Biology, 1984. 147(1), pp. 195–197.

Корт С.С.

ПОДХОД К ПЕРИОДИЧНОСТИ ОБУЧЕНИЯ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

г.Санкт-Петербург, ГОУ «СПбГПУ»

Во многих существующих подходах к построению системы обнаружения вторжений обычно используется статическое обучение классификатора. Однако, данный процесс подразумевает стационарность распознаваемого процесса. В общем случае данные, поступающие в систему, не является стационарным по следующим причинам:

- изменение поведения пользователя в течение времени;
- изменение окружения (появление в сети новых компьютеров и сервисов);
- изменение природы атак на систему;
- зависимости поведения пользователя в определенный момент времени от его поведения до этого момента времени.

Список этих причин можно расширить, но уже он показывает, что говорить о стационарности соответствующих процессов в системе некорректно. Как следствие этого, в идеальном случае обучение должно быть динамическим, а система должна быть адаптивной, периодически переобучаясь. Можно выделить три подхода к переобучению системы:

1) Переобучение системы инициируется пользователем. В том случае, если в системе отсутствует переобучение, она может оценивать поведение пользователя, которое можно охарактеризовать как стационарное.

2) Система обучается постоянно. Каждое новое событие вызывает переобучение. Переобучение при поступлении каждого события приводит к необходимости построения самообновляющегося профиля. К достоинствам данного подхода можно отнести преодоление проблемы адекватного описания модели системы, включающего условие стационарности. К недостаткам подхода можно отнести подверженность атакам на механизм обучения и неэффективность подхода, выражающаяся в слишком частой необходимости перестроения базы знаний.

3) Система переобучается при наступлении какого-то особого события. Данный подход к переобучению является адаптивным и устраняющим недостатки предыдущих двух подходов. Переобучение в данном случае выполняется при наступлении некоторого события, после возникновения которого соответствующий процесс не может оцениваться как стационарный и появляется необходимость перестроения базы знаний системы.

Вне зависимости от типа информации, на основании которой обучается система (нормальному поведению или данным об атаках), можно выделить три типа операций: разрешенные политикой безопасности, запрещенные политикой безопасности и неопределенные.

С точки зрения системы обнаружения вторжений неопределенной является операция, которая может быть оценена как принадлежащая и безопасному поведению и поведению нарушителя. Неопределенная операция может выполняться как нарушителем, так и авторизованным пользователем, как безопасной программой, так и разрушающим программным обеспечением. Необходимо отметить, что четко определенная политика безопасности системы должна уменьшать количество неопределенных операций.

Таким образом, факт выполнения неопределенной операции, являясь большой проблемой систем обнаружения вторжений, может служить событием-триггером, по которому целесообразно проводить переобучение системы обнаружения вторжений. Тогда переобучение системы обнаружения вторжений можно выполнять следующим образом:

1) том случае, если пользователь выполнил запрещенную политикой безопасности операцию: соответствующую аномальному поведению (система обучалась нормальному поведению) или атаку (система обучалась атакам);

2) в том случае если пользователь выполнил неопределенную операцию: неспецифицированную как нормальную операцию политикой безопасности, или операцию, разрешенную политикой безопасности, которая может быть выполнена при вторжении.

Корт С.С.

МОДЕЛЬ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ КАК СИСТЕМЫ РАСПОЗНАВАНИЯ ОБРАЗОВ

г.Санкт-Петербург, ГОУ «СПбГПУ»

В настоящем докладе рассматриваются основные модели систем обнаружения вторжений, описанные в литературе, а также предлагается модель системы обнаружения вторжений как системы распознавания образов.

В работе [1] рассматривается классическая модель системы обнаружения вторжений CIDF. Вследствие ее популярности подробно рассматриваться она не будет. Критика данной модели приводится в работе [2].

В работе [3] была сформулирована модель СОВ, описывающая процесс обнаружения вторжений и атак с точки зрения теории Байеса. В данной работе функционирование СОВ рассматривается как оценка параметров случайного процесса, сформированного из данных, принадлежащих нормальному и аномальному поведению. После этого описываются вероятности того, что некоторое действие принадлежит нормальному или аномальному процессу N. Детектор, предложенный в работе, функционирует в соответствии с выражением, оценивающим байесовскую вероятность того, что действие принадлежит нормальному или аномальному процессу.

В работе [4] была сформулирована модель СОВ, объединяющая в едином формализме методы обнаружения вторжений, основанные на выявлении аномалий и поиске сигнатур. Требования к системе обнаружения вторжений в рамках модели основываются на понятиях теории сложности и криптографических понятиях. При этом используются понятия вычислительной различимости и различимости для одиночного образца распределения, определяющие чувствительность системы к обнаружению вторжений.

В работе [5] была представлена модель СОВ, предназначенная для оценки количества информации, передаваемой между компонентами СОВ. В предлагаемой модели система обнаружения вторжений описывается как кортеж, описывающий структуры данных и алгоритмы, используемые в системе обнаружения вторжений. В модели достаточно полно описаны процедуры преобразования данных в процессе обнаружения вторжений.

Таким образом, на основании проведенного анализа можно сделать следующие выводы.

1) Модель CIDF является первой моделью систем обнаружения вторжений и предлагает общую структуру данных систем. К недостаткам модели CIDF можно отнести то, что она не учитывает процессов, происходящих в модуле сбора данных и в модуле анализа, а также не отражает самого процесса обнаружения вторжений.

2) Достоинством Байесовской модели системы обнаружения вторжений является то, что она впервые ввела понятие вероятности в алгоритм обнаружения вторжений. К недостаткам можно отнести недостаточную выразительность байесовских алгоритмов.

3) Достоинством криптографической модели является то, что она опирается на хорошо разработанную криптографическую теорию. К недостаткам можно отнести отсутствие в модели характеристик алгоритмов, используемых для обнаружения вторжений, в том числе вопросов, связанных с формулировкой безопасного и небезопасного поведения.

4) Информационная модель впервые отражает алгоритмы и структуры данных, используемые на различных этапах работы системы обнаружения вторжений. К

сожалению, авторы модели использовали ее только для получения единой метрики, описывающей ошибки системы обнаружения вторжений.

Постановка проблемы обнаружения вторжений как задачи распознавания образов позволяет:

1) Описать математическую постановку задачи обнаружения вторжений как задачу распознавания образов.

2) Использовать разработанный аппарат задач распознавания образов и обучения для решения задачи обнаружения вторжений.

3) Исследовать и характеризовать трансформации, обеспечивающие преобразование данных к виду, удобному для обнаружения вторжений.

4) Разработать формальные конструкций для описания алгоритмов, используемых системами обнаружения вторжений.

5) Выявить ограничения, присущие различным методам обнаружения вторжений.

6) Разработать систематические методы автоматического выбора алгоритма обнаружения вторжений для конкретной системы.

Для того, чтобы рассматривать систему обнаружения вторжений как систему распознавания образов, необходимо учесть специфику данной области. Это, в частности, связано со следующими фундаментальными результатами теории обучения и распознавания образов:

1) Не существует свободных от контекста и проблемно-независимых критериев, показывающих предпочтение одного метода обучения или классификации перед другими. Преимущества алгоритма или множества алгоритмов могут выявиться вследствие природы исследуемой проблемы или распределения данных.

2) Не существует предпочтительного набора признаков для представления шаблонов.

Таким образом, при описании модели системы обнаружения вторжений как системы распознавания образов необходимо отделять понятия, описывающие предметную область от понятий, применяющихся в теории обучения и распознавания образов. Как следствие данного положения вводится множество аксиом (A_{sec}), используемых в системе обнаружения вторжений. Под аксиомами понимается использование в системе некоторого подмножества эвристик, описывающих предметную область, истинность которых не ставится под сомнение. В качестве примеров аксиом можно ввести следующие положения:

- статистические характеристики множества данных, описывающего атаки, существенно отличаются от статистических характеристик данных, представляющих нормальное поведение (аномальность редких событий, малая плотность в пространстве аномальных событий и т.д.);
- поведение пользователя стационарно;
- в системе, в которой используется система обнаружения вторжений введена нормативная политика безопасности.

Анализ аксиоматики, используемой системой обнаружения вторжений, может показать ее ограничения, связанные с невозможностью обеспечения истинности аксиом в конкретной вычислительной системе.

D – множество данных;

TS – множество данных, используемых для обучения системы;

R = G(D) – множество признаков; вид функции выделения признаков может определяться экспертом или на основании стандартных алгоритмов признаков с учетом предметной области;

C – множество классов, в соответствии с которыми будут описываться данные;

$F = \{f_i\}_{i=1}^{N}$ – множество решающих правил, на основании которых выполняется классификация образцов; множество решающих правил определяется на основании процесса обучения и может быть описано как $\{f_i\}_{i=1}^{L} = \arg\min(f \in F) \sum_{(TS,C)\in S} l(f(G(TS)), C, A_{\text{sec}})$,

где $l(f(G(TS)), C, A_{sec})$ – функция стоимости, описывающая ошибки классификации. Набор решающих правил f_i может различаться в зависимости от системы, в которой функционирует СОВ. Набор решающих правил может задаваться экспертом или строится в процессе обучения.

Принимая во внимание введенные понятия можно определить модель системы обнаружения вторжений как $IDS = \{A_{\text{sec}}, TS, D, C, F\}$

Предлагаемая модель имеет следующие преимущества:

1) Позволяет ввести в модель положения аксиоматики предметной области и положения теории систем обнаружения вторжений.

2) Дает возможность сравнивать на уровне модели системы обнаружения вторжений, построенные на основании различных принципах обнаружения.

3) Предоставляет математический аппарат для перенесения фундаментальных результатов, полученных в рамках одних методов обнаружения для использования в рамках других методов обнаружения вторжений.

Литература

1) Denning D. «An intrusion-detection model», IEEE Transactions on Software Engineering, vol. Se-13, no. 2, February 1987, 222-232.

2) Корт С.С., Рудина Е.А. «Архитектура универсального ядра систем мониторинга и защиты от вторжений» СПб.: Изд-во Политехн. ун-та, журнал «Проблемы информационной безопасности. Компьютерные системы» № 1, 2008 г.

3) P. Helman, G. Liepins «Statistical foundations of audit trail analysis for the detectionof computer misuse», Software Engineering, IEEE Transactions on Volume 19, Issue 9, Sep 1993

4) G. Di Crescenzo, A. Ghosh, R. Talpade «Towards a Theory of Intrusion Detection», «ESORICS 2005» 2005

5) Guofei Gu, Prahlad Fogla, David Dagon, Wenke Lee and Boris Skoric «Towards an Information-Theoretic Framework for Analyzing Intrusion Detection Systems» Proceedings of The 11th European Symposium Research Computer Security (ESORICS 2006), Hamburg, Germany, September 2006.

Корт С.С., Павличенко М.В., Рудина Е.А.

ОБОБЩЕНИЕ АЛГОРИТМА АНАЛИЗА ДИНАМИКИ РАЗВИТИЯ СЕТЕВОГО ВТОРЖЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ РАСПРЕДЕЛЕННЫХ ВТОРЖЕНИЙ

г.Санкт-Петербург, ГОУ «СПбГПУ»

Система обнаружения вторжений "Авгур" использует при своей работе алгоритм анализа динамики развития атаки. В основу этого алгоритма заложены типовые сценарии вторжений, основанные на взаимосвязи их различных этапов. Этот алгоритм анализирует состояние внешних станций по отношению к защищаемым сетевым сервисам. Данные для анализа с использованием метода верификации сценария атаки поступают от генератора событий. Далее, поток событий для каждого защищаемого сервиса (идентифицируемого по IP адресу сервера и номеру порта) демультиплексируется в соответствии с IP адресами удаленных станций.

Верификация сценария вторжения производится на основе установленной классификации сообщений генератора событий: сообщениях о попытках сканирования защищаемых сервисов и операционной системы сервера, сообщениях о попытках непосредственной эксплуатации уязвимостей – атаках, о консолидации по окончании атаки, об обращениях с неконтролируемых портов защищаемого сервера и т.п. Кроме того, при верификации учитываются данные о версиях операционной системы и программного обеспечения защищаемого сервера. Определенным образом упорядоченные события, атрибуты которых скоррелированы как между собой, так и с известными данными о сервисе, могут быть объединены в единый сценарий вторжения.

СОВ "Авгур" может эффективно использоваться для обнаружения и верификации сценариев вторжений по схеме "один нарушитель – одна жертва", где нарушитель однозначно определяется по IP-адресу. Но данный подход не позволяет обнаруживать даже простейшие распределенные атаки.

Предлагаемое обобщение алгоритма динамики развития сетевого вторжения исключает из схемы обработки потока событий демультиплексор по адресу источника события. Попытка восстановления сценария развития вторжения в этом случае будет производиться по общему потоку событий. Предполагается, что условий верификации сценария вторжения достаточно для приблизительной оценки связи событий между собой даже без гарантии того, что каждое из них инициировано одним и тем же источником. При верификации сценария по общему потоку событий можно произвести уточнение возможности связи источников составляющих его событий между собой по ряду корреляционных признаков.

Для корреляции источников предполагаемого вторжения можно предложить следующие группы признаков, используемые как по отдельности, так и совместно друг с другом.

1. Корреляция по IP адресам. Признаком является совпадение IP адресов или принадлежность этих адресов к одной подсети. Возможно формирование более сложных методов корреляции на основе IP адресов (например, базирующихся на их статистической обработке) .

2. Корреляция по расстоянию до подозрительных хостов. Расположенные рядом хосты должны иметь близкие значения времени жизни пакета.
3. Корреляция на основе дополнительных полей протоколов сетевого и транспортного уровня.
4. Корреляция по содержимому сетевых пакетов. В основе лежит предположение о том, что при выполнении распределенных атак генерируются пакеты с одинаковым или схожим содержимым.
5. Корреляция на основе соответствия конфигурации ОС и сетевых сервисов подозрительных хостов. Подразумевает использование активных методов сетевой разведки системой обнаружения вторжений относительно атакующих станций. По результатам обратного сканирования можно выполнить анализ схожести версии и конфигурации ОС и сетевых сервисов этих станций (как правило, при организации бот-сети нарушитель использует одну и ту же известную уязвимость ОС или сетевого сервиса).

Описываемое обобщение алгоритма динамики развития вторжения (дополненного некоторыми сценариями вторжений) позволит применить этот алгоритм к обнаружению распределенных вторжений, в том числе распределенных атак отказа в обслуживании, вторжений с использованием т.н. бот-сетей.

Котенко И.В.

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ИНФРАСТРУКТУРНЫХ АТАК

г.Санкт-Петербург, СПИИРАН

В связи с большой сложностью компьютерных сетей и невозможностью воспроизведения реальных исследуемых событий в сети Интернет, в том числе в силу возможных негативных событий, моделирование играет первостепенную роль в исследованиях, связанных с защитой от инфраструктурных атак, таких как атаки “распределенный отказ в обслуживании” (DDoS), распространение сетевых червей, атаки на DNS, атаки на маршрутизаторы и др.

Доклад посвящен разработке методологического подхода к исследованию инфраструктурных атак и механизмов защиты от них на основе комплексного подхода к моделированию, базирующегося на интеграции агентно-ориентированного и имитационного моделирования на уровне сетевых пакетов, аналитического моделирования, методов эмуляции и виртуализации сетевых процессов, моделей и методов использования зафиксированных записей трафика, генерации трафика на основе моделей и др.

В докладе вначале приводится анализ основных моделей, используемых для исследования механизмов защиты от инфраструктурных атак. Модели рассматриваются с точки зрения требований к масштабируемости и точности. Описывается ряд подходов и программных средств для моделирования. Все методы рассматриваются в двух основных разрезах, а именно масштабируемости и точности моделирования. При рассмотрении также учитывается скорость моделирования (соотнесенная со временем, которое затрачивается реальным моделируемым процессом). Масштабируемость метода определяется как число узлов сети (конечных хостов и маршрутизаторов), которое можно моделировать, используя данный метод. Точность метода определяется как используемая при моделировании степень детализации сети и конечных хостов.

Далее в докладе представлен общий подход к гибридному моделированию и архитектура среды для исследования инфраструктурных атак и механизмов защиты от них. Предлагаемый подход основан на представлении сетевых систем в виде комплекса команд взаимодействующих компонентов (агентов), которые могут взаимодействовать или быть в состоянии антагонистического противостояния. Агрегированное поведение системы выражается в локальных взаимодействиях агентов.

Используемый подход к моделированию предполагает наличие следующих компонентов системы моделирования: базовую систему имитационного моделирования, модуль моделирования сети Интернет, подсистему моделирования базовых компонентов, а также модуль (библиотеку) имитации инфраструктурных атак и механизмов защиты от них.

Эксперименты, проведенные с разработанными моделями инфраструктурных атак и механизмов защиты от них, показали возможность использования предложенного подхода как для теоретических задач моделирования новых механизмов защиты и проигрывания возможных сценариев развития распределенных атак, так и для практических задач анализа механизмов защиты проектируемых сетей.

Работа выполняется при финансовой поддержке РФФИ (проект №07-01-00547), программы фундаментальных исследований ОНИТ РАН и при частичной финансовой поддержке, осуществляемой в рамках проекта Евросоюза RE-TRUST.

Москвин Д.А.

ОПТИМИЗАЦИЯ ПРИМЕНЕНИЯ ПОЛИТИК БЕЗОПАСНОСТИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

г. Санкт-Петербург, ГОУ "Санкт-Петербургский государственный политехнический университет"

Современные информационные системы (ИС) подвержены деструктивным воздействиям, вызывающим нарушение функционирования или несанкционированное использование ресурсов. Основными причинами возникновения несанкционированного доступа к информации и нарушений работы программных средств ИС являются: невыполнение политики информационной безопасности; невыполнение требований нормативных документов и стандартов по безопасности; неэффективное администрирование программных средств контроля доступа (ПСКД); неунифицированная настройка типовых рабочих станций.

Для устранения перечисленных причин необходимо решение следующих задач:

1. Настройка и контроль выполнения правил политики информационной безопасности

Под политикой информационной безопасности понимается совокупность правил, регулирующих параметры безопасности и полномочия пользователей в ИС. Для применения политики безопасности ее требования необходимо реализовать с помощью настройки конфигурационных параметров ПСКД. Такая настройка выполнима различными способами и производится администратором безопасности. При этом администратор должен учитывать все конфигурационные параметры ПСКД и их взаимное влияние. Сложная структура и неочевидная зависимость конфигурационных параметров является причиной ошибок администрирования. Например, администратор безопасности ОС Windows при назначении полномочий пользователям зачастую ограничивается настройкой прав доступа, забывая о системных привилегиях, которые позволяют пользователям получать полный доступ к объектам независимо от установленных прав. Для исключения этой ситуации необходимо автоматически преобразовывать требования политики информационной безопасности в набор конфигурационных параметров ПСКД.

2. Автоматизированное выполнение требований нормативных документов и стандартов информационной безопасности

При настройке конфигурационных параметров ПСКД необходимо учитывать требования нормативных документов, т.к. заданные по умолчанию параметры не обеспечивают требуемого уровня защиты. Например, в ОС Windows заданные по умолчанию разрешения на доступ к службам позволяют непривилегированному пользователю получить полный контроль над системой. Рекомендации по настройке обычно оформляются в виде т.н. "шаблонов" настроек безопасности. Такие шаблоны описывают значения для тысяч различных параметров, поэтому их применение администратором вручную практически невозможно. Следовательно, необходимо использовать методы автоматизации применения в системе таких шаблонов.

3. Эффективное администрирование безопасности

Многие прикладные программы, устанавливаемые по умолчанию автоматически, не требуются пользователям для выполнения их обязанностей. Наличие таких программ не только расходует ресурсы системы, но и существенно снижает ее безопасность, т.к. ошибки и уязвимости в этих программах могут привести к получению неавторизованного доступа к информационным ресурсам. Также

неэффективным является решение использовать в одной системе различных походов к администрированию ПСКД, что приводит к усложнению понимания конфигурации системы и существенно затрудняет работу администратора. Например, при смене администратора безопасности новому человеку очень сложно разобраться в действующих настройках, что неизбежно приводит к ошибкам. Указанные проблемы являются следствием неэффективного администрирования. Для их исключения необходимо регулярно выполнять контроль эффективности администрирования и оптимизировать настройки конфигурационных параметров ПСКД ИС.

4. Унификация и простота настройки типовых рабочих станций

Обычно в ИС рабочие станции сгруппированы по функциональным назначениям. Функциональное назначение определяется ролью рабочей станции в информационной среде. Все рабочие станции, входящие в состав функциональной группы, имеют единый состав ПО, следовательно, должны иметь и одинаковый уровень защищенности. Для этого необходимо обеспечить унификацию конфигурации рабочих станций в рамках функциональной группы и неизменность этой конфигурации в процессе эксплуатации ИС. Разные значения конфигурационных параметров ПСКД рабочих станций одного назначения свидетельствуют о невыполнении принципа унификации функциональной группы. При изменении значений конфигурационных параметров ПСКД их сравнение с установленными ранее позволит выявить причины негативных изменений. Следовательно, для выявления нарушений унификации настройки конфигурационных параметров ПСКД необходим механизм сравнения конфигураций разных рабочих станций.

Таким образом, решение задач настройки и контроля выполнения правил политики информационной безопасности, выполнения требований нормативных документов и стандартов информационной безопасности, эффективного администрирование безопасности и унификации настройки является актуальным и необходимым.

Результаты анализа существующих программных средств, применяемых для настройки и контроля конфигурационных параметров ПСКД, показывают их основные недостатки: отсутствуют средства, осуществляющие полный анализ конфигурационных параметров безопасности; не предоставляются возможности для формирования собственных проверок конфигурационных параметров безопасности; не предоставляются инструкции по устранению нарушений безопасности; не выполняются настройка и анализ безопасности; отсутствуют средства сравнения конфигурационных параметров ПСКД разных рабочих станций; не выполняется оценка эффективности администрирования.

Наличие перечисленных недостатков в существующих программных средствах существенно снижает эффективность их применения в ИС. Следовательно, актуально создание программного комплекса, который должен: выполнять настройку и сбор информации по всем идентифицируемым сущностям, их атрибутам безопасности и системным установкам; моделировать доступность пользователям информационных и программных ресурсов; генерировать описания причин возникновения нарушений безопасности и набор инструкций по их устранению; настраивать конфигурационные параметры безопасности, приводя их в соответствие с принятой политикой информационной безопасности.

В настоящее время в большинстве современных ИС не обеспечивается достижение следующих характеристик: выполнение политики информационной безопасности в части задания значений конфигурационных параметров ПСКД;

автоматизированная настройка и управление доступом, что позволяет избежать ошибок, связанных с "человеческим фактором"; эффективность управления доступом к информационным ресурсам с целью оптимизации настройки конфигурационных параметров ПСКД; простота и унификация настройки и контроля конфигурационных параметров ПСКД ИС.

Для обеспечения перечисленных характеристик автором разрабатывается набор методов и программных средств, решающие следующие задачи: обеспечение защиты информационных ресурсов, предотвращение несанкционированного доступа к информации в ИС и нарушений работы программных средств; повышение эффективности использования информационных ресурсов ИС путем оптимизации настройки конфигурационных параметров ПСКД; обеспечение контроля безопасности функционирования компонентов ПСКД ИС.

Достижение поставленных целей позволит повысить безопасность ИС и упростить процесс администрирования. Использование разрабатываемых программных средств позволит автоматизировать настройку и контроль конфигурационных параметров ПСКД, оптимизацию состава ПО, контроль эффективности администрирования, унификацию настройки типовых рабочих станций.

Платонов В.В.

ПРИМЕНЕНИЕ МЕТОДА ОПОРНЫХ ВЕКТОРОВ ДЛЯ ОБНАРУЖЕНИЯ МНОЖЕСТВА КЛАССОВ СЕТЕВЫХ АТАК

г.Санкт-Петербург, ГОУ "СПбГПУ"

Метод опорных векторов, который разработали В.Н.Вапник и А.Я.Червоненкис, позволяет в случае линейной разделимости двух классов исходных векторов большой размерности построить разделяющую гиперплоскость, максимально удаленную от множеств векторов, представляющих различные классы. Данную задачу называют дихотомным или двоичным разделением. В случае линейной неразделимости классов разработан подход, основывающийся на использовании ядерных функций, который позволяет, увеличив размерность исходных векторов, свести задачу к линейной разделимости. Многочисленные публикации, посвященные применению метода опорных векторов для решения различных задач распознавания, показывают применимость данного метода, например, для распознавания текстов, фотографий и т.п. Этот метод для случая двух классов может быть использован в задачах обнаружения сетевых атак и вторжений для построения профиля нормального поведения. В этом случае оптимальная гиперплоскость позволит определять аномальные отклонения от построенного профиля.

Значительный интерес представляет использование метода опорных векторов для классификации множества векторов на заданное число классов большее двух. Для задач обнаружения и предупреждения сетевых атак и вторжений необходимо знать не только факт наличия аномального поведения, но и установить вид нарушения, к которому относится данная аномальность. Прямое решение задачи квадратичного программирования для нахождения разделяющих гиперплоскостей затрудняется большой размерностью векторов, поэтому на практике используются различные подходы, например, последовательное применение дихотомной классификации к исходному множеству векторов, применение метода голосования для определения наилучшей попарной классификации и др. В докладе рассматриваются основные подходы к построению систем, использующих метод опорных векторов, для классификации множества векторов на заданное число классов, которые могут использоваться для систем обнаружения сетевых атак и вторжений.

Платонов В.В., Поникаровский К.В.

ПРИМЕНЕНИЕ SVM ДЛЯ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК

г.Санкт-Петербург, ГОУ "СПбГПУ"

Метод опорных векторов (Support Vector Machines, SVM) – это набор алгоритмов обучения с учителем, использующихся в задачах классификации и регрессионного анализа. Основная идея метода опорных векторов – поиск разделяющих параллельных гиперплоскостей с максимальным расстоянием между ними, разделяющих два класса данных. Метод основывается на предположении, что чем больше расстояние между этими гиперплоскостями, тем будет меньше средняя ошибка классификатора. Входные данные метода представляются в виде $\{(x_1, y_1), (x_2, y_2),\ldots, (x_n, y_n)\}$, где $y_i \in \{-1, 1\}$, в зависимости от того, к какому классу принадлежит входной вектор x_i. Каждый входной вектор x_i представляет собой d-мерный вектор, который обычно нормализуется. Нормализация проводится для того, чтобы вектора с большими отклонениями от средних значений координат не влияли на поведение классификатора. Если под классами понимать принадлежность сетевого пакета к атаке (например, $y = 1$) или к нормальному функционированию системы ($y = -1$), а координатами вектора x_i служат параметры сетевых пакетов или сетевого трафика, то можно применить технологию SVM – классификатора для обнаружения сетевых атак. Для метода SVM, как и любого метода обучения с учителем, достаточно сложной задачей является подготовка обучающего множества (рабочей выборки). В этой задаче можно выделить на два этапа: экспертную оценку принадлежности каждого вектора к классу нормального или аномального поведения и снижение размерности рабочей выборки (удаление неинформативных и лишних атрибутов).

Для формирования прототипа системы обнаружения атак были использованы исходные данные KDD 99, подготовленные DARPA (Defense Advanced Research Projects Agency) для оценки качества систем обнаружения вторжений. Принадлежность векторов к атакам или нормальному поведению определена заданным перечнем атак.

Для снижения размерности планируется применение различных методик: метод главных компонент, методы факторного анализа, метод перекрестной проверки и т.п. Перекрестная проверка (cross-validation) - метод формирования обучающего и тестового множества для обучения аналитических моделей в условиях недостаточности исходных данных или неравномерного представления классов. Для оценки методов используются общедоступные библиотеки и программы (libSVM, WEKA).

Чечулин А.А., Котенко И.В.

ОБНАРУЖЕНИЕ И ПРОТИВОДЕЙСТВИЕ СЕТЕВЫМ АТАКАМ НА ОСНОВЕ КОМБИНИРОВАННЫХ МЕХАНИЗМОВ АНАЛИЗА ТРАФИКА

г.Санкт-Петербург, СПИИРАН

В настоящее время актуальной задачей в области обеспечения безопасности информационных ресурсов является защита от сетевых атак, основанных на протоколах транспортного и сетевого уровней стека TCP/IP. Существующие средства защиты не всегда справляются с новыми экземплярами таких атак, поэтому важным направлением исследований и разработок является создание систем защиты, способных защищать не от конкретных атак, а от целых классов атак. Сложность процессов обнаружения и блокирования атак существенно увеличивается вследствие современных тенденций развития информационно-телекоммуникационных технологий, в том числе связанных с ростом размеров и производительности сетей, усложнением их топологии, возрастанием объема “быстрого трафика”, обусловленного функционированием peer-to-peer-приложений, VoIP-трафиком, работой сканеров безопасности и т.д.

Существующие сетевые атаки можно разделить на четыре основных класса: сбор информации, использующий анализ результата обработки пакетов; атаки, основанные на ошибках в обработке пакетов; сканирование хостов и сетей, базирующееся на использовании ошибок в обработке сессий; сканирование, основанное на корректном установлении соединений.

Для каждого класса атак в докладе предлагается разработать свои механизмы защиты (методы фильтрации и нормализации отдельных пакетов, методы анализа сессий, методы анализа сетевого взаимодействия).

Также в докладе предлагается реализовать подход к многоуровневому комбинированию алгоритмов в виде системы базовых классификаторов, обрабатывающих данные о трафике, и мета-классификатора, осуществляющего выбор весовых коэффициентов для каждого алгоритма, что позволяет объединить достоинства отдельных методов и уменьшить их недостатки. Выбор весовых коэффициентов может осуществляться отдельно для каждого узла сети, что позволит учесть особенности работающих сетевых приложений на каждом хосте.

Общий механизм обнаружения и противодействия сетевым атакам можно представить как совокупность следующих компонентов: сенсор – анализатор сетевого трафика; детектор – механизм обнаружения, принимающий на вход данные от анализаторов сетевого трафика и дающий на выходе правила фильтрации; мета-классификатор – модуль, принимающий на вход правила фильтрации от детекторов и дающий на выходе итоговые правила фильтрации, учитывающие вычисленные на основе данных от анализаторов весовые коэффициенты каждого детектора; фильтр – компонент блокирования, модификации или сдерживания трафика на основе правил, полученных от мета-классификатора.

Анализ эффективности предлагаемого подхода базируется на проведении большой серии испытаний на основе моделирования реального трафика с использованием моделей сетевых атак.

Работа выполняется при финансовой поддержке РФФИ (проект №07-01-00547), программы фундаментальных исследований ОНИТ РАН и при частичной финансовой поддержке, осуществляемой в рамках проекта Евросоюза RE-TRUST.

Явно Д.М.

СПОСОБЫ УСТАНОВЛЕНИЯ ПОДЛИННОГО IP-АДРЕСА ИСТОЧНИКА АТАКИ В СЕТИ ИНТЕРНЕТ

г.Санкт-Петербург, ГОУ «СПбГПУ»

В настоящее время при проведении атак в сети Интернет многие злоумышленники стараются скрыть свои личные данные, чтобы максимально затруднить их поиск и минимизировать вероятность поимки.

Необходимы отработанные подходы, позволяющие находить злоумышленника для того, чтобы можно было привлечь его к ответственности.

При навигации в сети пользователь оставляет на сайтах свой IP-адрес, данные о системе и об используемом интернет-обозревателе, а также списки страниц, которые он посетил в рамках этого сайта, и прочую служебную информацию. Эти данные записываются в журналы протоколов на удаленном сервере, где хранятся некоторое время. Такие действия в первую очередь обусловлены необходимостью каждого сайта собирать информацию об активности посетителей в тех или иных разделах или составлять статистику. Чтобы избежать появления своих данных в подобных журналах, злоумышленник может воспользоваться одним из следующих приемов:

- анонимными прокси-серверами
- веб-прокси
- предварительно взломанными компьютерами

Способы установления истинного IP-адреса, применимые в каждой ситуации, зависят от того, какие способы скрытия применял нарушитель. В общем случае существуют следующие возможности:

- Получение журналов протоколов непосредственно у владельца промежуточного сервера (обычно применимо только к прокси-серверам)
- Получение журналов протоколов у поставщика услуг связи и последующий анализ интенсивности потоков данных
- Если злоумышленник использует контролируемые пользовательские компьютеры, то можно попытаться отследить не саму цепочку, а адрес, с которого проводился захват контроля. Большинство злоумышленников не проводят такие операции напрямую со своего компьютера, но чаще всего такая цепочка будет значительно короче и может состоять всего из одного узла.
- Также в отдельных случаях нарушитель может выдать свою личность, например, используя почтовый ящик, который он указывал где-то еще, или оставляя другие следы, ведущие к реальным данным. В этом случае необходим тщательный анализ всех данных, оставленных на сайтах злоумышленником, и выявление информации, способной раскрыть его личность в обход анализа цепочки промежуточных серверов.

Первый и второй из приведенных способов являются применимыми независимо от предпринятых злоумышленником мер. Последний способ дает результаты только в том случае, если злоумышленник был небрежен и оставил следы.

Для отслеживания нарушителя, использующего цепочку разнородных серверов, требуется последовательно посылать запросы владельцам каждого сервера с целью установления следующего звена в цепочке. Если в процессе отслеживания нарушителя расследование выходит за пределы одного государства, то официальное взаимодействие необходимо проводить с привлечением международных правоохранительных организаций. Это замедляет процесс и уменьшает вероятность того, что владелец proxy-сервера сможет предоставить информацию о том, кем этот адрес был использован на момент атаки. Кроме того, такое расследование может вообще не дать результата в силу конфликтов в законодательстве разных государств.

Таким образом, вероятность того, что грамотно действующего нарушителя удастся отследить, является достаточно низкой. Даже в случае использования цепочки из шести-семи серверов, расположенных на территории разных государств, расследование занимает не менее нескольких месяцев. За это время информация, на основании которой возможно установление личности злоумышленника, может быть удалена из-за истечения срока давности.

Яковлев В.А., Лёвин И.И.

КОМПЛЕКСНЫЙ ПОДХОД К ЗАЩИТЕ ОТ РАСПРЕДЕЛЕННЫХ СЕТЕВЫХ АТАК

г.Санкт-Петербург, СПбГУТ им. проф. М.А. Бонч-Бруевича

DDoS-атаки (отказ в обслуживании) стали одним из самых распространенных преступлений в сети Интернет. DDoS-атака направлена на нарушение или полное прекращение доступа легальных пользователей к сетям, серверам, службам и другим ресурсам. Для осуществления атаки злоумышленники создают бот-сети (сеть зараженных компьютеров), и, используя их, осуществляют рассылку огромного количества пакетов с зараженных машин. В бот-сети могут входить сотни или тысячи машин разбросанные по всему миру. Поскольку эти атаки проводятся с разных IP-адресов, обнаружить и блокировать нападение очень сложно.

Существующие на сегодняшний день методы защиты от DDoS-атак не обладают оперативностью и автоматизмом работы, и носят скорее оборонительный характер. Известно большое количество методов автоматического определения источников DDoS-атак и их блокирования [1, 2]. По принципу работы они основываются на внесении меток маршрутизаторами в проходящие сетевые пакеты. В метках содержится информация о части пути, по которому прошел данный пакет. Метка вносится в малоиспользуемые поля IP-заголовка, как правило это поле идентификации, используемое только в случае фрагментации пакета. Метки могут вноситься как в обязательном порядке каждым маршрутизатором (детерминированная метка пакетов) так и с некоторой вероятностью (вероятностная метка пакетов). Атакуемый, анализируя метки в принятых пакетах, сможет восстановить путь следования пакетов в сети и вычислить атакующие хосты, которые затем можно будет заблокировать.

В докладе рассматривается комплексный подход к обнаружению источников DDoS-атак, который объединяет методы применяемые на маршрутизаторах (в частности, метод обязательной метки пакетов случайной хеш-функцией) и методы, применяемые на хостах. Его отличительными особенностями являются:

1. Редукция сети. Метки в пакеты вносятся не всеми маршрутизаторами, а только пограничными маршрутизаторами автономных систем, образующих глобальную сеть, при этом за счет уменьшения количества меток увеличивается длина поля для хранения меток маршрутизатора.
2. Комплексность. Метод предполагает внедрение как на элементах сети - маршрутизаторах (это позволяет отследить действительные источники DDoS-атак), так и на конечных хостах - атакуемых системах (это позволяет поддерживать работоспособность системы даже во время DDoS-атаки).
3. Случайность. Метки вносятся всеми пограничными маршрутизаторами автономных систем. Метка представляет собой хеш-код IP-адреса маршрутизатора. Для генерации меток применяется несколько хеш-функций, а номер используемой хеш-функции выбирается случайным образом.
4. Приоритетность. Легальный трафик обслуживается в первую очередь даже во время атаки за счет поддержки таблицы активных соединений (ТАС) и таблицы ожидающих соединений (ТОС) на стороне атакуемого. На основе данных таблиц происходит отсеивание пакетов атакующего.
5. Оперативность. Процесс восстановления обратного пути следования пакетов возможен уже после получения всего нескольких пакетов от источника.

Данную систему комплексной защиты можно охарактеризовать следующими параметрами:

P_{false} - вероятность ложного обнаружения источника атаки. Введение этого параметра обусловлено тем, что существует вероятность коллизии метки от одного маршрутизатора с меткой другого маршрутизатора, что может привести к обнаружению и блокированию трафика легального пользователя вместо трафика нарушителя.

P_{miss} - вероятность пропуска действительного источника атаки. Причина возможности пропуска реального источника атаки состоит в том, что структура больших сетей, таких как Интернет, непостоянна. Пакеты от одного и того же источника могут доходить до получателя разными путями. Поэтому, если во время атаки пакеты проходили по одному пути, а к моменту активизации метода автоматического отслеживания атаки структура сети изменилась и атакующий перестал посылать пакеты на некоторое время, то есть вероятность, что его не удастся обнаружить.

N_{resp} - количество пакетов, необходимое для обнаружения источника атаки. Время обнаружения атаки зависит от времени анализа (числа принятых пакетов) и методов, используемых для их мечения. Для методов с обязательным внесением меток в пакеты эта величина меньше, чем для методов с вероятностным внесением меток, так как каждый маршрутизатор в обязательном порядке вставляет свою метку в пакет. Для некоторых алгоритмов с обязательным внесением меток достаточно одного пакета, чтобы инициализировать процесс восстановления пути. Однако, длина используемого хеша у таких методов меньше, чем у методов с вероятностным внесением меток, поэтому вероятность ложного обнаружения источника атаки P_{false} у них значительно выше. Методы с вероятностным внесением меток, позволяют применить хеш-коды большей длины, за счет того, что после прохождения пакета от источника до получателя в нем будет содержатся метка только одного маршрутизатора, а не всех сразу. Однако, для восстановления обратного пути от получателя до источника необходимо получить метки от каждого маршрутизатора в цепочке. Так как метки вносятся в каждый пакет с некоторой вероятностью, то количество пакетов, необходимых для восстановления обратного пути в лучшем случае будет равно количеству маршрутизаторов на пути от источника до получателя.

В докладе приводятся оценки эффективности обнаружения источника DDoS-атаки при выполнении следующих условий:

$$N_{resp} \to \min,$$

$$P_{false} \le P_{false}^{\text{admis}},$$

$$P_{miss} \le P_{miss}^{admis}.$$

Список литературы

1. Dawn Song and Adrian Perrig. Advanced and authenticated marking schemes for IP traceback. In Proceedings IEEE Infocomm 2001, April 2001.
2. Abraham Yaar, Adrian Perrig, and Dawn Song. Pi: A Path Identification mechanism to defend against DDoS attacks. In Proceedings IEEE Infocomm 2003, May 2003.

РАЗДЕЛ 2.
КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ В ЗАЩИТЕ ИНФОРМАЦИИ

Александров С.В., Котлова Т.Г., Мареева Е.В., Петренко С.А., Эркин А.Г.

ПРИМЕНЕНИЕ ШИФРАТОРОВ В IP-СЕТЯХ

г. Санкт-Петербург, ЗАО «РЦЗИ «ФОРТ»

В настоящее время широкое распространение IP-сетей и их способность передавать практически любую информации (аудио-видео конференции, потоковое видео, передача данных и т.д.) привело к тому, что гораздо более эффективно сконцентрироваться на проблеме защиты на базе IP-сетей, вне зависимости от физических каналов связи. Наличие большого количества преобразователей интерфейсов позволяет транслировать практически любой интерфейс, в интерфейс поддерживающий IP (например E1-Ethernet, ADSL-технологии и т.д.) и при наличии IP-шифратора защитить передаваемую информацию на уровне IP-пакетов.

Однако часть информации (а именно IP-заголовок) передается в открытом виде, что создаёт потенциальную возможность для различных атак.

Для шифрсредств всегда актуальной была проблема управления. При использовании единой IP-технологии становится возможным проведение дистанционного управления ключевой сетью по каналам связи с обеспечением передачи зашифрованной информации. Для передачи управляющей информации создаётся защищённое соединение между центром управления и шифраппаратурой. Управляющая информация может содержать различные управляющие воздействия, например: шифрограммы ключей, запрет использования ключей, разрешение использования ключей. Кроме того, по этому же каналу связи можно собирать информацию о состоянии шифрсредства, журналы работы, сетевые статистики и т.д.

Для того чтобы IP-шифратор не нарушал корректную работу в IP-сетях, он должен поддерживать многие сложные функции, не связанные с шифрованием: например, маршрутизацию пакетов, фрагментацию пакетов, поддержку таблиц ARP (в Ethernet сетях) и т.д. В результате IP-шифратор превращается в довольно сложное устройство, как правило, реализующее стек протоколов TCP/IP, функции маршрутизации и т.д. Перспективным является продолжение тенденции усложнения шифратора и оснащения его дополнительными функциями, обеспечивающими межсетевое экранирование, анализатор СОА и т.д.

Аносов В.Д.

АЛГЕБРАИЧЕСКИЕ СООТНОШЕНИЯ НАД МНОГООСНОВНЫМИ АЛГЕБРАИЧЕСКИМИ СИСТЕМАМИ И ИХ ПРИМЕНЕНИЕ

г. Москва, ФСБ России

Ранее Х. Лауш и В. Небауэр [1], обобщая ряд классических результатов, связанных с разрешимостью уравнений, с полей на общие классы универсальных алгебр, рассматривали системы алгебраических уравнений с предметными переменными над произвольной одноосновной универсальной алгеброй A. На основе использования гомоморфизмов многоосновных алгебраических систем [2], при которых могут отождествляться как элементы основных множеств, так и операторы и предикаты, предложенный подход развивается для систем соотношений над многоосновными алгебраическими системами, в число неизвестных которых могут входить как элементы основных множеств, так и преобразования и предикаты [3].

На примере алгебр Шеннона демонстрируется возможность использования алгебраических соотношений в теоретической криптографии, устанавливаются связи класса методов группирования неизвестных при решении систем соотношений с методами, использования гомоморфизмов и их обобщений.

Приводятся методы решения систем соотношений над многоосновной алгебраической системой, использующие гомоморфизмы и их обобщения [4]. Приводятся общие алгоритмы поиска гомоморфизмов конечной многоосновной алгебраической системы.

Литература

1. Lausch H., Nobauer W. Algebra of polynomials. Amsterdam, London, New–York: North–Holland Publishing Company, American Elsevier Publishing Company Inc., 1973.
2. Аносов В.Д. О гомоморфизмах многоосновных алгебраических систем в связи с криптографическими применениями // Дискретная математика. 2007. Том 19. В. 2. С. 27-44.
3. Аносов В.Д. Уравнения над многоосновными алгебраическими системами и методы их решения // Материалы XVII Общероссийской научно-технической конференции «методы и технические средства обеспечения безопасности информации», СПбГПУ, Санкт-Петербург, 2008. С. 40.
4. Горчинский Ю.Н. О $\bar{\pi}$–гомоморфизмах конечных многоосновных универсальных алгебр. // Дискретная математика. 1999. Том 11. В. 2. С. 3-19.

Артамонов А.В., Маховенко Е.Б.

ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ ПРОТОКОЛОВ ГРУППОВОЙ ПОДПИСИ В СИСТЕМАХ ДОКУМЕНТООБОРОТА

г.Санкт-Петербург, ГОУ «Санкт-Петербургский государственный политехнический университет»

Отправной точкой теоретического и практического развития протоколов групповой подписи стала статья Чома и ван Хейста в 1991 году [1]. С тех пор теме групповой подписи было посвящено множество статей и выявлен ряд практических областей применения. Одной из таких областей являются системы электронного документооборота (СЭД).

Применительно к СЭД, протоколы групповой подписи позволяют эффективно решить следующие задачи, решение которых посредством обычных протоколов электронно-цифровой подписи (ЭЦП) является не оптимальным или не возможным:

- формирование ЭЦП анонимно от имени отдела (для внутренних документов) или компании (для исходящих документов);
- выявление конкретного автора подписи в случае спорной ситуации;
- поддержка динамического изменения состава участников группы, обладающих правом подписи (эта возможность есть в некоторых протоколах групповой подписи) [2].

В рамках данной работы разрабатывается архитектура функционального модуля СЭД на базе платформы Documentum, использующего протокол групповой подписи BBS [3]. Сама платформа Documentum предполагает построение СЭД по клиент-серверной архитектуре со взаимодействием пользователей с системой посредством браузера.

Общий вид архитектуры представлен на рис. 1.

Архитектура обеспечивает возможность подписи версии произвольного документа (dm_document и производных типов) в любом формате, с произвольным количеством объектов контента. В подпись включаются только основные (rendition=0) объекты контента, то есть, представления (в терминах Documentum) не подписываются.

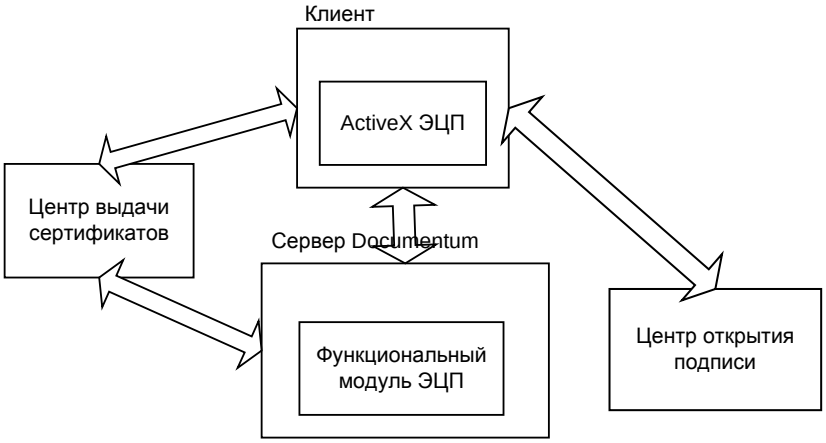


Рисунок 1. Общий вид архитектуры функционального модуля

Функциональный модуль разработан с учётом возможности увеличения в будущем количества различных типов подписей для одного документа, то есть, возможности для одного пользователя подписать документ несколько раз, но не более одного экземпляра подписи каждого типа на документ от одного пользователя системы (из соображений здравого смысла) – например, для многоэтапного согласования с подтверждением визирования.

Функциональный модуль проверяет назначение сертификата, используемого при подписи, при выполнении подписи и при всех проверках валидности.

Обеспечивается подпись атрибутов документа. Набор подписываемых атрибутов определяется на уровне типа документа и наследуется всеми подтипами, если для подтипа не указан собственный набор атрибутов. Настройка атрибутов для подписи выполняется при установке системы и не может быть изменена в дальнейшем без потери валидности всех ранее подписанных документов. Документ может быть подписан одним или несколькими пользователями системы.

В дальнейшем в рамках работы предполагается опытная реализация разработанной архитектуры.

[1] D. Chaum and E. van Heyst (1991). "Group signatures". Advances in Cryptology — EUROCRYPT ’91, volume 547 of Lecture Notes in Computer Science: 257-265.

[2] M. Bellare, H. Shi and C. Zhang. Foundations of Group Signatures: The Case of Dynamic Groups. Topics in Cryptology - CT-RSA 2005 Proceedings, Lecture Notes in Computer Science Vol. 3376, A. Menezes ed, Springer-Verlag, 2005. (http://www-cse.ucsd.edu/users/mihir/papers/dgs.html)

[3] D. Boneh, X. Boyen, H. Shacham. Short Group Signatures. M. Franklin (Ed.): CRYPTO 2004, LNCS 3152, pp. 41–55, 2004.

Богданов А.Г.

ЗАЩИЩЕННАЯ РЕАЛИЗАЦИЯ АЛГОРИТМА AES

г.Санкт-Петербург, ГОУ «СПбГПУ»

Программа, реализующая алгоритм шифрования, может исполняться в недоверенной среде, причем нарушитель может иметь доступ к памяти и получить ключ шифрования или сообщения. Рассмотрим алгоритм AES с длиной ключа 128 бит. Если нарушитель имеет только доступ по чтению, безопасность может быть обеспечена секретным преобразованием, выполняемым перед передачей данных в недоверенную среду. В качестве такого преобразования используем 8-битную подстановку φ.

Для выполнения обратного преобразования над шифртекстом алгоритм шифрования должен быть модифицирован. При этом подстановка S заменяется подстановкой $S'=\varphi S\varphi^{-1}$, а операция сложения с ключом примет вид $XOR'(x', k') = \varphi(\varphi^{-1}(x') \oplus \varphi^{-1}(k'))$, где x', k' – переменные, соответствующие байтам шифртекста и ключа. Операция перемешивания столбцов может быть представлена как набор функций вида $f(x_1,x_2,x_3,x_4) = x_1 \oplus x_2 \oplus \{02\}\otimes x_3 \oplus \{03\}\otimes x_4$, где $\{02\},\{03\},x_i$ – элементы поля F_{256}, ⊗ – умножение элементов поля. Модифицированная операция будет иметь вид $f(x_1',x_2',x_3',x_4') = \varphi(\varphi^{-1}(x_1') \oplus \varphi^{-1}(x_2') \oplus \{02\}\otimes\varphi^{-1}(x_3') \oplus \{03\}\otimes\varphi^{-1}(x_4'))$ и потребует 4 Гб для хранения таблицы значений, поэтому целесообразно представить ее как композицию операций сложения над полем F_{256} и фиксированных подстановок, задающих умножение на элементы {02} и {03}. Все операции подстановок целесообразно объединить с операциями сложения, т.к. это уменьшит объем памяти, необходимый для хранения данных, и в ряде случаев повысит стойкость к атакам. Таким образом, алгоритм будет представлен как композиция операций вида $S'(x_1', x_2') = \varphi(S_3(S_1(\varphi^{-1}(x_1')) \oplus S_2(\varphi^{-1}(x_2'))))$, где S_i – различные 8-битные подстановки, известные нарушителю.

Представление алгоритма через композицию таких операций неоднозначно, но операция вида $S'(x_1', x_2') = \varphi(\varphi^{-1}(x_1') \oplus \varphi^{-1}(x_2'))$ будет присутствовать в любом из них. Полагая $x_1' = x_2'$, нарушитель может восстановить значение φ(0). При подстановке этого значение в любое другое уравнение вместо x_2', получим уравнение вида $S'(x') = \varphi(S(\varphi^{-1}(x')))$, где S – композиция операций подстановки, используемой в AES, умножения на {02}, {03} и сложения с константами. Число решений уравнения зависит от цикловой структуры подстановки S и определяется формулой $m_1!\cdot k_1^{m1} + \ldots + m_p!\cdot k_p^{mp}$, где k_i – число элементов в цикле, m_i – число циклов с таким числом элементов, p – число различных длин циклов в подстановке S (например, для подстановки, используемой в AES, получим порядка 22 миллионов решений). Подставляя φ(0) вместо x', нарушитель может найти множество значений φ(y) для всех y, лежащих в подстановке S в одном цикле с 0. Суммируя эти значения, нарушитель может получить значения φ для элементов, лежащих в других циклах и, таким образом, восстановить подстановку φ.

Для противодействия этой атаке необходимо использовать несколько секретных подстановок. При использовании подстановок φ и ψ нарушитель получит уравнения вида

$S'(x_1', x_2') = \psi(\varphi^{-1}(x_1') \oplus \varphi^{-1}(x_2'))$

$S'(x_1', x_2') = \varphi(\varphi^{-1}(x_1') \oplus \psi^{-1}(x_2'))$

Значение ψ(0) легко находится в обоих случаях, что позволяет в дальнейшем восстановить подстановку ψ описанным выше методом. Таким образом, для обеспечения стойкости в каждой операции должны быть задействованы три различных секретных подстановки.

Анализ схемы создания ключей, используемой в алгоритме AES, показывает, что для выполнения этого условия необходимо в общей сложности 4 подстановки. Обозначим их φ, ψ, δ, λ. Тогда каждое 32-битное слово исходного ключа может быть зашифровано отдельной подстановкой, при зашифровании последующих слов подстановки могут чередоваться в следующем порядке: φ, ψ, δ, λ, δ, λ, φ, ψ, φ, ψ, δ, λ, …. Модифицированная схема создания ключей будет включать 6 чередующихся бинарных операций и 10 дополнительных операций, учитывающих сложение с константами. Если 32-битные слова открытого текста шифровать с использованием той же последовательности подстановок, схема шифрования может быть реализована за счёт использования 12 дополнительных операций, общий объем необходимой памяти при этом составит порядка 2 Мб (возможны различные варианты реализации, но число операций в них будет примерно одинаковым).

Стойкость данного алгоритма определяется сложностью решения системы уравнений, соответствующих используемым операциям, и может быть повышена за счет увеличения числа задействованных подстановок.

Богданов А.Г., Ростовцев А.Г.

СИММЕТРИЧНОЕ ГОМОМОРФНОЕ ШИФРОВАНИЕ

г.Санкт-Петербург, ГОУ «СПбГПУ»

При построении защищенных информационных систем часто требуется обеспечение обработки зашифрованной информации. При этом вычислительная среда не должна иметь доступ к открытым данным, а результаты вычислений должны допускать эффективную проверку. Создание такого вычислительного процесса позволит строить защищенные корпоративные базы данных, системы мобильных агентов и т.п.

Рассмотрим возможность построения защищенного вычислительного процесса на примере симметричного шифра, когда недоверенный вычислитель (НВ) управляется с помощью доверенной машины (ДМ). При этом ДМ готовит данные, ключ и программу шифрования. НВ предположительно выполняет эту программу, но может наряду с этим выполнять и другие программы. Для простоты предположим, что НВ не имеет энергонезависимой памяти, не способна к обучению и не имеет каналов связи с нарушителем. ДМ должна иметь механизм контроля правильности выполненного шифрования, не шифруя данные.

Алгебраической основой безопасного шифрования служат секретные гомоморфизмы кольца полиномов Жегалкина $\rightharpoonup_m$. В качестве таких гомоморфизмов может использоваться, например, следующие отображения.

1. Гомоморфизмы из $\rightharpoonup_{2m}[\mathbf{x}, \mathbf{y}]$ в кольцо классов вычетов $\rightharpoonup_{2m}[\mathbf{x}, \mathbf{y}]/\ (S) \cong \rightharpoonup_m[\mathbf{x}]$ по идеалу секретного бинарного отображения $\mathbf{y} = S(\mathbf{x})$;

2. Гомоморфизм $\rightharpoonup_m[\mathbf{x}] \rightarrow\ _2$, который вычисляется как значение полинома в данной секретной точке;

3. Отображения кольца интерполяционных полиномов над полем из 2^m элементов в простое поле $_2$, которые вычисляются как секретные элементарные симметрические функции от автоморфизмов расширенного поля (при этом число m должно быть простым).

4. Гомоморфизм из кольца матриц над полем $_2$ в поле $_2$.

5. Автоморфизмы кольца $\rightharpoonup_m[\mathbf{x}]$, группа которых изоморфна группе всех подстановок множества из 2^m элементов.

Любое вычисление строится с использованием унарных и бинарных операций. Здесь унарной операцией может быть произвольное обратимое отображение множества векторов в себя, а бинарные операции должны кроме того задавать на множестве векторов структуру кольца.

В общих чертах безопасное шифрование n-битового текста выполняется следующим образом. ДМ знает рабочий и контрольный открытый текст, рабочий и контрольный ключ и контрольную шифрограмму как результат шифрования контрольного текста на контрольном ключе. Кроме того, ДМ знает алгоритм шифрования. Для зашифрования рабочего открытого текста на рабочем ключе ДМ строит случайный гомоморфизм кольца $\rightharpoonup_m[\mathbf{x}] \rightarrow\ _2$. При этом каждый бит текста, ключа представлен 2^m-битовым двоичным вектором (например, вектор задает полином от m переменных, значение полинома в некоторой точке равно данному биту). На

множестве двоичных векторов определяются гомоморфные образы операций сложения по модулю 2 и умножения так, чтобы существовал гомоморфизм из множества векторов в поле $_2$. Простейший случай: полиномы складываются (+) и умножаются (·). Однако можно использовать и более сложные варианты арифметики. Например, если для случайной подстановки φ *m*-битовых слов определить сложение

$$\mathbf{x} +_\varphi \mathbf{y} = \varphi(\varphi^{-1}(\mathbf{x}) + \varphi^{-1}(\mathbf{y}))$$

и умножение

$$\mathbf{x} \cdot_\varphi \mathbf{y} = \varphi(\varphi^{-1}(\mathbf{x})\cdot\varphi^{-1}(\mathbf{y})).$$

Вложение поля $_2$ в кольцо векторов позволяет одним полиномом представить пару значений бита — контрольной и рабочее. Подстановка φ может меняться от операции к операции, что выполняется с помощью умножения подстановок. Это соответствует изменению контрольных и рабочих точек, что затрудняет статистический (корреляционный) криптоанализ.

На основе алгоритма шифрования и указанного гомоморфизма колец ДМ адаптирует входные данные и программу шифрования на уровне битовых операций, программа оперирует с 2^m-битовыми векторами и передает их в НВ. При этом каждая битовая операция, выполняемая в ходе шифрования, кодируется своим полиномом и своей парой контрольных и рабочих точек.

Результатом шифрования является набор из 2^m-битовых векторов, представляющих зашифрованный текст, которые НВ передает в ДМ. ДМ проверяет, что значения полиномов в контрольных точках равно зашифрованному тексту. Если это так, то, по-видимому, шифрование выполнено правильно, то есть значения полиномов в рабочих точках задает шифрограмму.

Такой подход к построению вычислительного процесса создает предпосылки к построению защищенных информационных систем, когда вычислительная среда выполняет обработку секретных данных, не зная значение этих данных, и не может подменить результат обработки.

Габов А.А., Котлова Т.Г., Мареева Е.В., Петренко С.А., Шемякина О.В., Эркин А.Г.

ОСОБЕННОСТИ РЕАЛИЗАЦИИ ЗАЩИЩЁННЫХ ПРОТОКОЛОВ ОБМЕНА ПРИ ОСУЩЕСТВЛЕНИИ МОБИЛЬНЫХ ПЛАТЕЖЕЙ

г. Санкт-Петербург, ЗАО «РЦЗИ «ФОРТ»

Мобильная коммерция – одна из наиболее быстро развивающихся услуг, пользуется всё большей популярностью у потребителей. Многие банки и организации внедрили за последние годы целый ряд сервисов, связанных с платёжными системами, доступных абонентам мобильных телефонов.

Принципиальным вопросом при создании и использовании систем мобильной коммерции на территории Российской Федерации является использование сертифицированных решений, реализовать которые возможно только при использовании отечественных криптоалгоритмов. В качестве примера такого сертифицированного решения можно привести российский модуль безопасности (РМБ) – изделие М-529 разработки ЗАО «РЦЗИ «ФОРТ», функциональный аналог Host Security Module (HSM).

При планировании развёртывания системы мобильных платежей существенное внимание оказывается транспортной среде, через которую будут осуществляться транзакции. Наиболее привлекательным для банков и пользователей оказывается SMS транспорт, в силу своей огромной распространённости, ведь этот сервис провайдеры сотовой связи предоставляют по умолчанию и все модели телефонов поддерживают данную технологию. В то же время размер SMS-сообщения вводит существенные ограничения на объем передаваемых данных.

Основу системы составляет наличие секретного ключа, доступного банку и абоненту. В подобных системах схема распределения ключей обычно осуществляется следующими двумя способами:

- доставкой ключа из банка клиенту на индивидуальном носителе. Для этого используются бумажные носители – ПИН-конверты либо банковские чеки;
- доставкой секретного ключа с использованием несимметричных алгоритмов при наличии обмена открытыми ключами между банком и клиентом.

Важной проблемой, встающей при внедрении систем мобильных платежей, является надёжность хранения секретного ключа. Большинство современных моделей телефонов не позволяют разграничить доступ к хранимым ключам аппаратными средствами телефона, что вынуждает хранить ключ непосредственно в памяти телефона. Мобильный телефон не может храниться так же, как, например, банковская карта, к которой доступа посторонних нет. При этом секретный ключ, хранимый в телефоне, может быть считан злоумышленником. Таким образом, возникает необходимость использовать такие программные средства разграничение доступа, как шифрование ключей хранимых в телефоне, на паролях пользователей. При этом важно обеспечить устойчивость шифрограмм к атакам перебора, поскольку стойкость шифрования определяется размером пароля пользователя.

Еще одной проблемой является необходимость в генераторе случайных чисел в мобильном телефоне. В качестве исходных данных такого генератора может выступать значения, полученные из банка перед первым запуском приложения (например, в ПИН-конверте). При этом возможно периодическое улучшение качества генератора с добавлением случайного числа, выработанного достоверным генератором банка и переданного по каналу связи.

Гель Ю.В., Ростовцев А.Г.

ПОДПИСЬ НА ИЗОГЕНИЯХ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

г.Санкт-Петербург, ГОУ «СПбГПУ»

Безопасность систем электронной цифровой подписи основана на двух математических задачах: вычисление дискретного логарифма в циклической группе простого порядка и вычисление порядка и структуры конечной группы. Обе эти задачи могут быть решены с полиномиальной сложностью на квантовом компьютере. Для вскрытия ключа подписи разрядность квантового компьютера должна быть около 1000 кубитов. В настоящее время компания D-Wave Systems разработала модель квантового компьютера на сверхпроводящих торах разрядностью 512 кубитов. Поэтому существующие стандарты подписи могут рухнуть в недалеком времени.

Для противодействия квантовым атакам за рубежом в 2007 г. предложили строить систему подписи на дискретных -модулях (решетках). Сотрудники СПбГПУ в 2001 г. предложили построить криптосистему с открытым ключом на новой задаче: вычисление морфизма в категории абелевых групп. Применительно в эллиптическим кривым над конечным полем — вычисление изогении. Эта задача представляется стойкой по отношению к квантовому компьютеру и является аналогом криптосистем на решетках.

Пусть $E(\ _p)$ — эллиптическая кривая. При переходе к алгебраически замкнутому полю точки кривой $E(\ _p)$ остаются неподвижными под действием отображения Фробениуса π, дульного отображения $\hat{\pi}$ и тождественного отображения 1. Поэтому ядро эндоморфизма $1 - \pi$ состоит в точности из точек кривой $E(\ _p)$ и $\#E(\mathbb{F}_p) = (1-\pi)(1-\hat{\pi}) = 1 - T(\pi) + p$. Отображение Фробениуса удовлетворяет уравнению $\pi^2 - T\pi + p = 0$ с дискриминантом $D_\pi = Df^2 < 0$ для целого кондуктора f.

Эллиптическая кривая с точностью до изоморфизма (над исходным полем $_p$ или его квадратичным расширением) характеризуется своим инвариантом j. В этом случае идеал (p) раскладывается в мнимом квадратичном порядке дискриминанта D как произведение двух сопряженных главных идеалов. Инвариант j эллиптической кривой является корнем полинома, задающего поле классов мнимого квадратичного порядка дискриминанта D_π и любого его подпорядка с дискриминантом $D_1 = Df_1^2$, $f_1 \mid f$. Тогда группа точек кривой $E(\ )$ над полем комплексных чисел изоморфна факторгруппе $/\alpha L$, для некоторого $\alpha \in$, где L — решетка с базисом $\left[1, \sqrt{D}\right]$ или $\left[1, \frac{1+\sqrt{D}}{2}\right]$.

Инвариант определяется как корень над полем $_p$ полинома $H_D(X)$, задающего поле классов мнимого квадратичного порядка, являющегося подпорядком порядка с дискриминантом D_π. При этом $\deg(H_D) = h_D$ — число классов идеалов мнимого квадратичного порядка, определенных с точностью до главного идеала. Полином $H_D(X)$ раскладывается на линейные множители над $_p$ и любой его корень задает эллиптическую кривую с одним и тем же числом точек.

Изогения эллиптических кривых — бирациональный гомоморфизм, мощность ядра которого над алгебраически замкнутым полем равна степени изогении. Изогения между эллиптическими кривыми существует тогда и только тогда, когда эти кривые имеют одинаковое число точек, то есть их инварианты являются корнями одного и того же полинома $H_D(X)$. При композиции изогений их степени умножаются. Изогения действует как перестановка на множестве j-инвариантов, то есть как автоморфизм из группы Галуа полинома $H_D(X) \pmod p$. Две изогении степеней l_1, l_2 эквивалентны, если идеалы с нормами l_1, l_2 эквивалентны (различаются на главный идеал). Поэтому изогении образуют абелеву группу Isog($_p$), изоморфную группе классов Cl(D), причем при сегодняшнем уровне развитии математики этот изоморфизм не вычислим ни в одну сторону ни на обычном, ни на квантовом компьютере (требуемая разрядность квантового компьютера растет как экспонента от числа классов). Изогения степени l между эллиптическими кривыми с инвариантами j_1, j_2 существует тогда и только тогда, когда (j_1, j_2) — точка классической модулярной кривой, заданной модулярным полиномом $\Phi_l(U, V)$.

Если l — нечетное простое число, то модулярный полином $\Phi_l(U, j)$ имеет 2 корня при $\left(\frac{D_\pi}{l}\right)=1$, 0 корней при $\left(\frac{D_\pi}{l}\right)=-1$, 1 или $l + 1$ корень при $\left(\frac{D_\pi}{l}\right)=0$. Число классов может быть нечетным только для простого D_π.

В криптосистеме используется случай $\left(\frac{D_\pi}{l}\right)=1$, эллиптические кривые представлены своими j-инвариантами. Тогда граф изогений является звездой.

Число классов имеет большой простой делитель r, если числа D, f простые и $f-\left(\frac{D}{f}\right)=2r$. Альтернативный способ генерации эллиптической кривой — выбор кривой так, что D_π является большим простым числом (D_π можно вычислить алгоритмом Чуфа).

Протокол подписи аналогичен ГОСТ Р 34.10–2001 с тем отличием, что вместо точек эллиптической кривой используются j-инварианты изогенных кривых из группы классов, а вместо сложения и удвоения точек используется отображение j-инвариантов с помощью изогений малых простых степеней l, для которых $\left(\frac{D_\pi}{l}\right)=1$.

Еремеев М.А., Ломако А.Г., Сергиенко П.В.

ПОДХОД К ИССЛЕДОВАНИЮ СТОЙКОСТИ БЛОЧНЫХ ШИФРОВ, ИСПОЛЬЗУЕМЫХ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

г. Санкт-Петербург, Военно-космическая академия имени А.Ф. Можайского

В настоящее время в телекоммуникационных системах используются различные механизмы обеспечения защищенности информации, среди которых блочные шифры занимают особое место в качестве основного средства обеспечения конфиденциальности информации. Существующие сервисы сетевой безопасности предоставляют возможность опционального выбора блочного алгоритма шифрования. При этом встает вопрос о проведении сравнительного анализа их стойкости. Для полного исследования стойкости алгоритма шифрования необходимо проведение всесторонних длительных исследований, состоящих в применении к исследуемому шифру различных, известных на момент исследования, методов криптоанализа. Такое исследование может занять большое количество ресурсов: временных, вычислительных, человеческих и др. В качестве альтернативы может быть использован подход к анализу стойкости блочных шифров, заключающийся в декомпозиции блочного алгоритма шифрования с последующим исследованием характеристик его составляющих элементов.

В докладе рассматривается подход к исследованию отдельных компонентов блочных алгоритмов шифрования на примере нелинейного преобразования. В подавляющем большинстве случаев в качестве нелинейного преобразования используются блоки подстановок различной размерности. Характеристиками нелинейного преобразования применительно к основным направлениям криптоанализа являются:

- дифференциальная однородность, используемая при проведении дифференциального криптоанализа;
- нелинейность, используемая при проведении линейного криптоанализа;
- размерность нелинейного компонента;
- алгебраическая структура, используемая при проведении алгебраических методов криптоанализа;
- биективность, используемая при проведении интегрального криптоанализа.

Для определения этих характеристик создан специальный программный комплекс оценивания параметров нелинейного преобразования. Эти параметры могут быть объединены в некоторую характеристику качества нелинейного преобразования исследуемого алгоритма, которая может быть как специализированной, то есть соответствовать стойкости к определенному методу криптоанализа, так и комплексной, отображающей стойкость этого компонента к различным методам криптоанализа.

Разработанный подход исследования свойств блочных шифров позволяет получить сравнительную характеристику различных алгоритмов и помочь в выборе оптимального алгоритма на этапе проектирования криптосистемы. Подобный подход, детально рассматривающий характеристики всех составляющих частей алгоритма шифрования, может использоваться как самостоятельно, для проведения предварительного экспресс-анализа свойств блочного шифра, так и стать основой для более глубоких исследований, например, при исследовании взаимного влияния компонентов шифра, или непосредственно при проведении криптоанализа.

Зубов Н. А. Марков Я. А.

МОДУЛЬНОЕ УМНОЖЕНИЕ С ПОМОЩЬЮ ПРЕОБРАЗОВАНИЯ МОНТГОМЕРИ В КОЛЬЦЕ $Z[\sqrt{-2}]$

г.Санкт-Петербург, ГОУ «СПбГПУ»

Алгоритм модульного умножения Монтгомери построен на основе преобразования Монтгомери, предложенного в 1985 г. По сравнению с другими алгоритмами модульного умножения он позволяет получить результат без использования операции деления, что снижает его трудоемкость и позволяет существенно ускорить арифметику больших чисел в алгоритмах криптографии. Для своей работы алгоритм требует более простую архитектуру вычислителя, что уменьшает его цену и позволяет увеличить производительность. Данные особенности этого алгоритма находят применение в криптосистемах, оперирующих с большими числами, например, RSA и DSA.

В некоторых криптографических алгоритмах повышение быстродействия достигается за счет использования арифметики чисел из кольца $Z[\sqrt{-2}]$. Существенного ускорения модульного умножения в этом кольце можно добиться за счет использования схожего с преобразованием Монтгомери подхода, который описывается в работе.

Предлагаемый алгоритм базируется на представлении комплексных чисел в позиционной системе счисления (ПСС) с основанием $\sqrt{-2}$. Для записи любого числа из кольца $\sqrt{-2}$ в такой ПСС требуется только две цифры, благодаря чему арифметика легко реализуется на традиционной цифровой элементной базе.

Подобное представление чисел позволяет эффективно реализовать деление и умножение на степень основания ПСС, используя операцию сдвига.

Особенностью ПСС с основанием $\sqrt{-2}$ является то, что для получения представления комплексного числа в виде суммы вещественной и мнимой части нет необходимости в выполнении каких-либо операций, так как четные разряды в ПСС с основанием $\sqrt{-2}$ соответствуют мнимой части, а нечетные – вещественной, записанным в негабинарной ПСС (негабинарная СС — ПСС с основанием -2).

В работе предложены алгоритмы выполнения основных арифметических операций над числами, записанными в негабинарной ПСС. Операции над числами из кольца $\sqrt{-2}$, такие как умножение, сложение, можно выразить через операции с целыми числами, записанными в негабинарной СС, алгоритмы выполнения так же предложение в работе.

Получить биты негабинарного представления целого числа можно, последовательно получая остаток от деления на -2. Для перевода числа в ПСС с основанием $\sqrt{-2}$ необходимо перевести вещественную и мнимую часть в негабинарную ПСС. Биты вещественной части записываются на нечетные позиции результата, биты мнимой части — на четные позиции.

Существенного прироста производительности алгоритмов можно добиться, если аппаратная реализация будет поддерживать одновременно работу как с числом, представленным в ПСС с основанием $\sqrt{-2}$, так и с парой чисел, записанных в негабинарной ПСС, чего можно добиться, «проецируя» одни и те же физические биты на два различных логических регистра вычислителя. Изменения, произведенные над содержимым одного регистра, отразятся на содержимом связанного с ним парного регистра.

Незначительным отличием от оригинального алгоритма Монтгомери является то обстоятельство, что на заключительной стадии преобразования Монтгомери достаточно сделать четыре вычитания, а не два, поскольку результат получается не на прямой, а на комплексной плоскости.

За счет использования такой ПСС алгоритм умножения комплексных чисел из кольца $Z[\sqrt{-2}]$ практически не отличается от классического алгоритма Монтгомери и полностью наследует его преимущества.

Предложенные подходы позволили расширить область применения хорошо зарекомендовавшего себя алгоритма Монтгомери на числа из кольца $Z[\sqrt{-2}]$. В работе предложена программная реализация изложенных подходов.

Котлова Т.Г., Мареева Е.В.,
Петренко С.А., Шемякина О.В., Эркин А.Г.

ОПЫТ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ УПРАВЛЕНИЯ СРЕДСТВАМИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ

г. Санкт-Петербург, ЗАО «РЦЗИ «ФОРТ»

В настоящее время с развитием сетей передачи данных возрастают требования к функциональности средств защиты. Сейчас к средствам защиты предъявляются требования интегрирования криптографической и сетевой защиты. Кроме того, крупные распределенные сети должны иметь централизованное управление.

Уже существуют изделия, реализующие эти требования. Теперь стоит задача упростить управление, сделать его эффективнее. Простота не противоречит, но способствует эффективности: средства управления могут обладать большим набором возможностей и функций, но если использование этих функций требует глубокого знания работы системы и выполнения значительного числа операций, то управление будет затруднено.

Цели управления средствами криптографической защиты сетей конфиденциальной связи включают централизованное дистанционное задание параметров защиты, контроль состояния объектов сети, оперативное реагирование на нештатные ситуации. Главной особенностью сетей, в которых применяются средства криптографической защиты, являются высокие требования по обеспечению надежности и отказоустойчивости. Поэтому основными требованиями к управлению являются своевременное обнаружение и быстрое устранение нештатных ситуаций.

Для эффективного управления необходимо выполнения следующих условий:

- пользователь в каждый момент времени владеет всей необходимой для принятия решений информацией;
- интерфейс является простым в восприятии;
- система управления автоматически собирает и обрабатывает данные, выдавая пользователю результат обработки, и, после принятия пользователем определенного решения, автоматически осуществляет управляющие воздействия.

В то же время система, помимо результатов обработки, должна при необходимости предоставлять исходные данные для разбора спорных ситуаций.

Еще одна особенность автоматизированных систем управления средствами криптографической защиты заключается в небольшом количестве пользователей (операторов), решающих фиксированное множество задач. Это позволяет, подробно изучив работу пользователей, определить наиболее удобный способ представления данных и набор инструментов для решения оперативных задач.

Такой подход к созданию систем управления средствами криптографической защиты позволяет достигнуть поставленных целей: пользователь в любой момент времени имеет представление о состоянии каждого объекта сети и может оперативно реагировать на возникновение нештатных ситуаций.

Павлов Д.С.

ШИФРОВАНИЕ ЖУРНАЛОВ ПРИЛОЖЕНИЙ С УЧЕТОМ ТРЕБОВАНИЙ СТАНДАРТА PCI-DSS

г.Санкт-Петербург, ГОУ «СПбГПУ»

Журналы работы приложения в процессинговом центре банка могут содержать персональные данные о клиентах, их счетах, объемах транзакций и другую информацию, которая может позволить злоумышленникам подделать карту клиента или иным образом завладеть чужими финансовыми средствами.

Шифрование журналов приложений позволяет защитить информацию от утечки и модификации. Шифрование предлагается производить не как шифрование абстрактного байтового потока данных (файла), а с учетом структуры и характера информации.

Записываемый журнал приложения предлагается разбить на записи (сообщения журнала), каждая из которых будет обладать набором полей в зависимости от типа приложения. Такими полями могут быть текст сообщения, подробный текст, время, ассоциированные данные и т.д. Для каждого типа поля определяются правила преобразования в бинарные данные. Перед записью в журнал сообщение преобразуется в последовательность байтов, например, при помощи схемы тэг (определяет тип поля) – длина – значение.

Для обеспечения большей криптостойкости следует применить алгоритм сжатия данных. Для журналов приложения достаточно использовать простейший алгоритм сжатия, предполагающий исключение одинаковых значений поля для записей, идущих подряд. Так, например, одна и та же дата сообщения может повторяться в журнале большое количество раз. Такой подход при использовании схемы тэг-длина-значение можно реализовать за счет использования нулевой длины значения или отсутствия значения в записи.

Кроме применения алгоритмов сжатия следует также сохранять поля записи в нефиксированном порядке, так как в противном случае возможно повторение первого байта (тэга первого поля) для множества записей.

Применение ассиметричного шифрования позволяет защитить ранее зашифрованные журналы от раскрытия в случае получения доступа к серверу. В этом случае не произойдет и компрометация закрытых ключей, так как на сервере хранятся только открытые компоненты ключей. Зашифрование данных производится на открытых ключах авторизованных для доступа к данным журналов сотрудников банка и, возможно, службы поддержки поставщика программного обеспечения. Использование ключа службы поддержки позволит решить проблему безопасной передачи журналов в службу поддержки для разрешения проблем в работе ПО.

Ассиметричное шифрование предлагается использовать в комбинации с симметричным алгоритмом, который будет шифровать непосредственно данные журнала. Ключ шифрования симметричного алгоритма вырабатывается случайным образом и подлежит зашифрованию под каждым из ключей шифрования пользователей.

Такая схема позволяет защитить информацию журнала от неавторизованного просмотра, как сотрудниками банка, так и сервисными службами, в которые, возможно, попадает носитель информации при ремонте ЭВМ.

Для защиты от модификации данных журнала предлагается использовать код аутентичности сообщения с использованием случайного ключа, значение которого зашифровано совместно с ключом шифрования данных. Таким образом, авторизованные пользователи будут иметь возможность проверить целостность данных журнала, а изменение содержимого записи без знания ключа кода аутентичности сообщения будет невозможна. С

использованием такого подхода возможно также разделить и полномочия пользователей в модификации данных после записи журнала.

Кроме того, для защиты от вставки записи в середину следует применить схему, аналогичную гаммированию в шифрах, при которой значение кода аутентичности сообщения для предыдущей записи учитывается в вычислении кода для текущего сообщения журнала. Для этих же целей следует использовать симметричный шифр в режиме гаммирования.

Для защиты от угрозы подмены открытого ключа шифрования журналов и от добавления ключа злоумышленника к конфигурации приложения используются сертификаты с электронной цифровой подписью, которые выдаются для каждого ключа шифрования журналов. Возможно использовать два подхода, как по отдельности, так и совместно. Первый подразумевает использование удостоверяющего центра (CA) внутри банка. Второй заключается в том, что сертификаты ключам выдаются поставщиком программного обеспечения, а модуль, ведущий записи журналов, содержит внутри кода значение открытого ключа подписи поставщика ПО.

Атака при использовании первого подхода возможна только в случае подмены в конфигурации приложения адреса CA и организации злоумышленником своего CA, что много сложнее подмены ключа, а кроме того, может быть обнаружено в сети при помощи системы обнаружения вторжений. Нарушение безопасности при использовании второго подхода возможно только при нарушении целостности ПО, ведущего записи журналов, что равносильно внедрению в ПО вредоносного модуля, передающего все данные приложения злоумышленнику.

Если вышестоящим ключом в цепочке сертификатов ключа шифрования сотрудника банка является ключ поставщика ПО, то создание и обновление ключей шифрования журналов будет достаточно сложной процедурой, так как потребуется совместная работа двух организации. Поэтому в цепочку сертификатов удобно ввести и промежуточный сертификат, выдаваемый службой банка авторизованным сотрудникам. Тогда создание, обновление и отзыв ключей пользователей будет производится в рамках одной организации без привлечения поставщика ПО.

Недостатками предлагаемого метода записи журналов является невозможность дописывать данные в конец ранее закрытого приложением журнала, требуется создание нового файла, а также необходимость чтения журнала только от начала к концу (случайный доступ невозможен) вследствие использования MAC-chaining, гаммирования и сжатия. Однако необходимости в такой функциональности, как запись в конец закрытого журнала, в сложных системах обычно нет.

Применение такого подхода позволяет защитить журналы от несанкционированного доступа как извне, так и со стороны сотрудников банка. Выполняются следующие требования стандарта PCI-DSS: о приведении к нечитаемому виду номеров карт клиентов; о защите от внесения изменений в журналы регистрации событий; о разрешении просмотра журналов регистрации событий только тем сотрудникам, которым это необходимо.

Появляется возможность для безопасной передачи журналов в службу поддержки поставщика ПО, а также (в соответствии с требованием о ежедневном просмотре журналов событий для всех компонентов) в систему сбора и анализа событий. Упрощается и разработка ПО для контроля целостности и генерации предупреждений в случае нарушения целостности журналов.

Ростовцев А.Г.

РЕАЛИЗАЦИЯ СТАНДАРТОВ ПОДПИСИ: УСКОРЕНИЕ С ЗАЩИТОЙ ОТ АТАК ПО ВНЕШНЕМУ КАНАЛУ

г.Санкт-Петербург, ГОУ «СПбГПУ»

Стандарты электронной цифровой подписи многих стран используют эллиптические кривые над конечными полями. В основе стандартов подписи лежат протоколы Эль-Гамаля и Шнорра. Покажем, что можно ускорить реализацию стандартов подписи, одновременно повысив защищенность ключа от атак по внешнему каналу.

Пусть $E(\mathbf{F}_q)$ эллиптическая кривая над полем из q элементов. Точки эллиптической кривой образуют конечную абелеву группу по сложению. Пусть $Q \in E(\mathbf{F}_q)$ — точка простого порядка r. Секретным ключом является показатель $l \in \mathbf{F}_r$, открытым ключом является точка $P = lQ$.

В ходе формирования подписи стандарты предусматривают формирование случайного показателя k, вычисление точки $R = kQ$, координата которой является частью подписи. Справедливо следующее утверждение.

Теорема 1. Если показатель k известен, то вскрытие ключа сводится к решению линейного уравнения.

Таким образом, однократное вычисление или предсказание показателя k ведет к вскрытию ключа. Умножение точки на показатель выполняется путем удвоений и сложений. Поэтому для вычисления показателя k достаточно различать операции удвоения и сложения в реальном масштабе времени. Обычно для вычисления показателя k используются атаки по внешнему каналу, основанные на измерении физических параметров, сопровождающих процесс формирования подписи.

Стандартами подписи предусмотрено использование эллиптической кривой в форме Вейерштрасса $Y^2Z = X^3 + AXZ^2 + BZ^3$. Операции сложения и удвоения точек на этой кривой существенно различны: выполняются по разным формулам и требуют различных временных затрат. Так, анализ мгновенной потребляемой мощности ведет к вскрытию ключа (такие атаки возможны, например, если подпись формируется смарткартой, которая вставляется во внешний терминал).

Скорость формирования и проверки подписи удобно измерять в числе операций модульного умножения. Удвоение точки кривой в форме Вейерштрасса требует 12 модульных умножений, сложение точек требует 15 модульных умножений.

Эллиптическая кривая допускает задание уравнением в форме Гессе $U^3 + V^3 + W^3 = 3mUVW$. Кривая в форме Гессе допускает более быструю арифметику, чем кривая в форме Вейерштрасса: сложение точек требует 9 модульных умножений, а сложение точек — 12 модульных умножений. Известно, что кривые в форме Вейерштрасса и Гессе бирационально эквивалентны. Это отображение частично определено и неудобно для вычисления. Основной результат основан на следующем утверждении.

Теорема 2. Если число точек эллиптической кривой в форме Вейерштрасса кратно 3, то существует линейная эквивалентность между кривыми в форме Вейерштрасса и в форме Гессе. Отображение кривой в форме Вейерштрасса в кривую в форму Гессе требует 5 модульных умножений, обратное отображение кривой в форме Гессе в кривую в форме Вейерштрасса требует 4 модульных умножений.

Ускорение формирования и проверки подписи достигается так. Кривая в форме Вейерштрасса отображается в кривую в форме Гессе, выполняются предусмотренные стандартами арифметические операции на кривой в форме Гессе, затем выполняется обратное отображение. Сложность указанных отображений кривых пренебрежимо мала по сравнению со сложностью формирования и проверки подписи. Данный способ позволяет ускорить формирование и проверку подписи в 1,37 раза, если при умножении точки на число используется популярный метод знакового двоичного окна.

Защита от атак по внешнему каналу основана на следующем утверждении.

Теорема 3. На эллиптической кривой в форме Гессе для любой точки (U, V, W) точки (W, U, V), (V, W, U) различны и справедливо равенство $2(U, V, W) = (W, U, V) + (V, W, U)$.

Защита от атак по внешнему каналу осуществляется заменой операции удвоения точек операцией сложения точек. Здесь анализ физических параметров, сопровождающих процесс формирования подписи, не позволяет различить операции сложения и удвоения точек. С учетом указанной защиты от атак по внешнему каналу формирование подписи выполняется примерно в 1,16 раза быстрее по сравнению с известным способом, который такую защиту не обеспечивает, а проверка подписи выполняется в 1,37 раза быстрее.

Ростовцев А.Г.

ПОЗВОЛЯЕТ ЛИ ВЫБОР СПЕЦИАЛЬНЫХ ПОДСТАНОВОК ПОВЫСИТЬ СТОЙКОСТЬ ШИФРА?

г.Санкт-Петербург, ГОУ «СПбГПУ»

Современные блочные шифры строятся по методу Шеннона, на основе композиции нелинейных операций перемешивания (подстановок, действующих на коротких словах), аффинных операций рассеивания, действующих на всем блоке, и операции сложения с ключом.

Для повышения стойкости шифра обычно используют специально подобранные подстановки, которые обладают наилучшими криптографическими свойствами. В частности, для противодействия линейному и дифференциальному методам выбираются подстановки, обладающие наилучшим возможным распределением дифференциалов и линейных сумм. Целью данного сообщения является обобщение известных методов криптоанализа, из которого вытекает предположение, что специально подобранные подстановки не лучше, чем случайные.

Определение 1. Шифры $y = C(k, x)$ и $y' = C'(k', x')$ изоморфны, если существует обратимое вычислимое в обе стороны отображение $C \leftrightarrow C'$, $x \leftrightarrow x'$, $y \leftrightarrow y'$, $k \leftrightarrow k'$. Указанное отображение называется изоморфизмом шифров.

Теорема 1. Шифр уязвим по отношению к некоторому методу анализа тогда и только тогда, когда изоморфный шифр уязвим по отношению к этому же методу анализа.

Число шифров, изоморфных данному шифру, чрезвычайно велико. Для снижения его стойкости достаточно найти слабый (по отношению к некоторому методу криптоанализа) изоморфный шифр.

Определение 2. Атака на шифр, реализуемая выбором соответствующего изоморфизма, называется атакой на основе виртуальных изоморфизмов.

Примерами изоморфизмов шифров являются аффинная эквивалентность и сопряжение. Рассмотрим еще один вод изоморфизма.

Пусть шифр C имеет r циклов шифрования и описывается уравнением

$$y = F(k_r + F(k_{r-1} + \ldots + F(k_1 + x)\ldots)) \quad (1)$$

и φ — произвольная подстановка, действующая на блоках текста и циклового ключа. Обозначим $x' = \varphi(x)$, $y' = \varphi(y)$, $k_i' = \varphi(k_i)$, $F' = \varphi F \varphi^{-1}$, $a +_\varphi b = \varphi(\varphi^{-1}(a) + \varphi^{-1}(b))$. Тогда уравнение (1) можно записать в виде

$$y' = F'(k_r' +_\varphi F'(k_{r-1}' +_\varphi \ldots + F'(k_1' +_\varphi x')\ldots)) \quad (2)$$

Определение 3. Изоморфные шифры, задаваемые уравнениями (1), (2), называются сопряженными.

Теорема 2. n-битовые подстановки S, S' сопряжены (существует такая подстановка φ, что $S' = \varphi S \varphi$) тогда и только тогда, когда они имеют одинаковый цикленный тип. Сложность вычисления подстановки φ по заданным S, S' равна $O(2^n)$.

Например, если подстановка задается обращением в поле из 2^n элементов, то она почти всюду сопряжена с подстановкой, заданной сложением с ненулевой константой. Число сопрягающих подстановок φ близко к $\sqrt{2^n!}$.

Изоморфизм изоморфизмов является изоморфизмом, однако композиция значительного числа изоморфизмов ведет к усложнению вычисления результирующего изоморфизма. Для изменения цикленного типа подстановки изоморфного шифра можно использовать повторную композицию сопряжений и аффинных отображений. Криптоаналитик может выбирать произвольные изоморфизмы, которые оптимизируют свойства некоторых отображений, тогда как изоморфные образу других отображений ведут себя как случайные подстановки. Поэтому можно сформулировать

Предположение 1. Выбор специальных подстановок не позволяет повысить стойкость шифра по отношению к атакам на основе виртуальных изоморфизмов.

Применим метод виртуальных изоморфизмов к шифру AES. AES предусматривает выполнение операций с байтами: сложение с байтом ключа, подстановку *T* байта и линейное рассеивающее отображение, действующее на 16 байтах. Подстановка $T = AS$ задается как композиция обращения *S* в поле из 256 элементов (127 циклов длины 2 и 2 цикла длины 1) и аффинной подстановки *A*. Учтем подстановку *A* в рассеивающем отображении. Тогда результирующее рассеивающее отображение *W* является аффинным и может быть описано блочной матрицей 16*16, элементы матрицы — аффинные подстановки четырех видов, действующие на байтах.

Аппроксимируем подстановку *S* подстановкой, в которой все циклы имеют длину 2 (вероятность ошибки 2^{-7}). Выберем в качестве сопряженной подстановки $\varphi S\varphi^{-1}$ операцию инверсии младшего бита в байте. Почти все дифференциалы сопряженного образа точной подстановки *S* имеют вероятность 1, а линейные суммы имеют преобладание 0,5. Число таких вспомогательных подстановок байта φ превышает 10^{254}. Для оптимизации выбора подстановки φ можно использовать различные критерии: она должна иметь много неподвижных точек или во многих точках коммутировать с рассеивающей подстановкой и др.

Выбором сопрягающей подстановки φ удалось на порядок увеличить вероятности дифференциалов и преобладания линейных сумм. Сопряженный образ нелинейный подстановки стал почти аффинным, сопряженные образы операции рассеивания и сложения с ключом являются слабо нелинейными. Вероятности дифференциалов подстановок, входящих в операцию рассеивания, достигают 0,133 (в 8,5 раз выше, чем у исходной подстановки), преобладания линейных сумм достигают 0,2 (в 12,5 раз выше, чем у исходной подстановки). Вероятности дифференциалов и линейных сумм для сопряженного образа подстановки, заданной как сложение с ключом, зависят от ключа и для некоторых байтов ключа равны 1.

Семьянов П.В.

КРИПТОГРАФИЧЕСКИЕ ВЫЧИСЛЕНИЯ НА ГРАФИЧЕСКИХ ПРОЦЕССОРАХ

г.Санкт-Петербург, ГОУ «СПбГПУ»

Графические процессоры (*GPU*) в последнее время стали опережать центральные процессоры по производительности (1000 гигафлопс против 200), во многом за счет того, что они предлагают высокопараллельные вычисления. Более того, кроме использовавшихся недавно только узкоспециализированных вычислений для вывода графики появились и активно развиваются технологии вычислений общего назначения на GPU (*GPGPU*): технология CUDA от NVIDIA, ATI Stream от AMD и общий стандарт OpenCL. За счет этих технологий появилась возможность ускорять различные алгоритмы, допускающие параллельную обработку, в пределах от 4-8 до 100-150 раз.

Криптографические алгоритмы также возможно реализовывать на GPU, получая существенное ускорение в том случае, если возможно параллельное исполнение, т.е.:

1) в задачах перебора ключей или паролей;
2) при шифровании или хешировании больших объемов открытого текста.

К сожалению, многие криптографические алгоритмы плохо подходят для реализации второй задачи, т.к. шифрование или хеширование части данных зависит от предыдущих данных и не может быть сделано одновременно. В настоящее время разрабатываются новые алгоритмы, которые будут допускать параллельную обработку данных.

В рамках данного исследования был реализован перебор ключей/хешей с помощью технологии CUDA для следующих алгоритмов: MD5, SHA-1, RC4, AES. Были сомнения, что некоторые алгоритмы, если их и удастся реализовать на CUDA, дадут прирост скорости, однако эти сомнения успешно разрешились. Все они, особенно хеши семейства MD, подходят для реализации на GPU и дают существенное ускорение, представленное в таблице:

Таблица. Скорость вычислений криптографических функций с использование технологии CUDA, ключей (хешей)/секунду)

Алгоритм	CPU (Intel Core 2, 1.86 ГГЦ, одно ядро)	GPU (NVIDIA 8600GTS, 32 потоковых процессоров)	GPU (NVIDIA GTX 260, 216 потоковых процессоров)	Ускорение

MD5	14.000.000	50.000.000	350.000.000	x25
SHA-1	10.000.000	30.000.000	200.000.000	x20
AES (развертка ключа зашифрования)	8.000.000	нет данных	160.000.000	x20
AES (развертка ключа расшифрования)	3.000.000	нет данных	20.000.000	x7
RC4 (развертка ключа)	2.000.000	2.300.000	15.000.000	x8

Необходимо заметить, что переделка исходного текста криптофункций с языка C на язык CUDA была минимальна, однако для получения максимальной скорости сам код необходимо было оптимизировать, что не всегда было тривиальным. В таблице представлены результаты сравнения оптимизированных версии алгоритмов под CPU (SSE2-код) и GPU, что дает реальные значения ускорения.

Таким образом, использование технологии параллельных вычислений на GPU дает существенный эффект для многих существующих криптографических алгоритмов, причем достижение этого эффекта является недорогим с точки зрения разработки.

Мирончиков Е.Т., Титова Е.М.

СВЕРТОЧНЫЕ КОДЫ С КОДОВЫМ ЗАШУМЛЕНИЕМ

г.Санкт-Петербург, ПГУПС, ГУАП

В настоящее время основными требованиями, предъявляемыми к системам беспроводной связи, являются скорость передачи информации, надежность передачи (вероятность ошибки на символ или блок символов), а также обеспечение секретности. Поэтому задача передачи конфиденциальной информации по открытым каналам связи является достаточно актуальной.

Очевидно, что при беспроводной связи существует возможность перехвата информации злоумышленником (перехватчиком), который имеет возможность подключиться к каналу и получить информацию о передаваемых сообщениях. Такой канал называется каналом с перехватом [2,3]. Как обычно, предположим, что канал перехватчика хуже основного канала, то есть интенсивность шума, а соответственно и вероятность ошибочной передачи, при передаче по этому каналу выше, чем в основном канала. В работах [2,3] было показано, что для обеспечения достаточной защищенности каналов с перехватом целесообразно использовать специальную конструкцию кодов Рида-Соломона с эффектами кодового зашумления.

В данном докладе показано, что сверточные коды также можно использовать в каналах с перехватом для обеспечения конфиденциальности передаваемой информации. Однако предварительно требуется построить такие сверточные коды, свойства которых похожи на свойства кодов БЧХ или кодов Рида-Соломона. Прежде всего, это сверточные коды с большой длиной кодового ограничения, настолько большой, что алгоритм декодирования Витерби не может быть использован. Кроме того, эти сверточные коды должны декодироваться алгебраическими алгоритмами, которые исправляют заданное число ошибок в пределах известной границы БЧХ. Сверточные коды с нужными свойствами были построены [5] и здесь продемонстрирована возможность их использования в каналах с перехватом на примере простейшего сверточного кода.

Для рассматриваемого примера используем сверточный код со скоростью передачи $k/n = 5/7$, исправляющий одну ошибку на блок длины $n = 7$, построенный на основе кода Рида - Соломона $(15,13)$ над полем $GF(2^4)$.

Для получения этого сверточного кода используем проверочную матрицу H кода Рида – Соломона с генераторным полиномом $g(x) = (x-\alpha)(x-\alpha^2)$

$$H = \begin{bmatrix} \alpha & \alpha^2 & \alpha^3 & \dots & \alpha^{14} & 1 \\ \alpha^2 & \alpha^4 & \alpha^6 & \dots & \alpha^{13} & 1 \end{bmatrix},$$

где α - корень неприводимого в поле $GF(2)$ полинома $x^4 + x^3 + 1$.

Выберем из этой матрицы 14 столбцов и составим новую проверочную матрицу из двух подматриц одинакового размера $[H^{(1)} : H^{(2)}]$. Каждая подматрица содержит 7 столбцов. Теперь получим проверочную матрицу сверточного кода $H^{(1,2)}[1,5]$. Каждый элемент этой матрицы $H^{(1,2)}$ является полиномом вида

$$h^{(1,2)}(i,j) = h^{(1)}(i,j) + x \cdot h^{(2)}(i,j),$$

где $h^{(1)}(i,j)$ и $h^{(2)}(i,j)$ суть элементы подматриц $H^{(1)}$ и $H^{(2)}$ соответственно.

В результате получаем проверочную матрицу сверточного кода со скоростью $5/7$

$$H^{(1,2)} = \begin{bmatrix} \alpha^2 + x\alpha^8 & \alpha + x\alpha^9 & \alpha^3 + x\alpha^{10} & \alpha^4 + x\alpha^{11} & \dots & \alpha^7 + x\alpha^{14} \\ \alpha^4 + x\alpha & \alpha^2 + x\alpha^3 & \alpha^6 + x\alpha^5 & \alpha^8 + x\alpha^7 & \dots & \alpha^{14} + x\alpha^{13} \end{bmatrix}$$

По проверочной матрице можно построить порождающую матрицу. Одна из форм порождающей матрицы для этого кода представлена ниже.

$$G_f^{(1,2)} = \begin{bmatrix} \alpha^3x^2+\alpha^2x+\alpha^{12} & \alpha^2x^2+\alpha^2x+\alpha^{11} & \dots & \alpha^2x^2+\alpha x+\alpha^3+\alpha^2 \\ \alpha^8x^2+\alpha^7x+\alpha^2 & \alpha^{11}x^2+\alpha^{10}x+\alpha^5 & \dots & \alpha^{11}x^2+\alpha^{10}x+\alpha^{11} \\ \alpha^{12}x^2+\alpha^{11}x+\alpha^6 & \alpha^9x^2+\alpha^8x+\alpha^3 & \dots & \alpha^8x^2+\alpha^7x+\alpha^3 \\ \alpha^5x^2+\alpha^4x+\alpha^{14} & \alpha^3x^2+\alpha^2x+\alpha^{12} & \dots & \alpha^2+\alpha \\ \alpha^4x^2+\alpha^3x+\alpha^{13} & \alpha^2x^2+\alpha x+\alpha^{11} & \dots & \alpha^9x^2+\alpha^8x+\alpha^5 \end{bmatrix}$$

Чтобы убедиться в этом, достаточно перемножить порождающую матрицу и транспонированную проверочную матрицу. Это произведение равно нулю. Таким образом, сверточный код над полем $GF(2^4)$ со скоростью $5/7$ построен.

Отметим, что на каждом такте работы схемы кодирования на вход кодирующего устройства подаются 5 символов из поля $GF(2^4)$, а на выходе получаем 7 символов из того же поля. Для реализации кодового зашумления можно, например, на два входа подавать элементы поля $GF(2^4)$, выбираемые случайным образом. А на оставшиеся три входа можно подавать информационные символы тоже из поля $GF(2^4)$.

Благодаря добавлению случайных символов, каждому информационному сообщения сопоставляется множество различных кодовых слов на выходе кодера, близких в смысле расстояния Хемминга. Таким образом, злоумышленник по принятой последовательности должен найти переданное сообщение, которое представлено множеством кодовых слов, мало отличающихся друг от друга. Отметим, что длина кодового ограничения достаточно велика (это степень полиномов в генераторной матрице), количество входов также достаточно велико и символами являются элементы конечного поля с достаточно большим числом элементов. В результате кодовая решетка имеет огромное число состояний, так что использовать алгоритм Витерби для декодирования практически невозможно. По этой причине приходится использовать алгебраическое декодирование, основанное на использовании проверочной матрицы.

Из-за различия в качестве каналов перехватчик получает последовательность с большим количеством ошибок, чем легитимный пользователь. Поэтому всякий раз, когда в последовательности перехватчика ошибок больше, чем допускается границей БЧХ, он получает ошибочное сообщение. А если ошибок оказалось меньше, то перехватчик получит правильное сообщение. Такое событие называется успешным перехватом. Вероятность успешного перехвата определяется качеством каналов и характеристиками кода. Можно убедиться, что при правильно выбранных параметрах

кода вероятность успешного перехвата и вероятность ошибки в основном канале (канале без памяти) могут быть сделаны сколь угодно малыми[3].

Поясним работу декодера перехватчика, пытающегося исправить две ошибки на отрезке кодового слова длины 7. По проверочной матрице находим синдром и модифицируем его в соответствии с алгоритмом декодирования укороченных кодов Рида-Соломона Сона [4]. Далее, находим полином локаторов ошибок и вычисляем значения ошибочных символов на длине 7. В результате найдем, что алгоритм указывает ложные ошибки. При декодировании следующего блока кодового слова алгоритм предполагает, что ошибки сосредоточены на декодируемом в настоящий момент блоке длины 7, а на предыдущем они уже исправлены. Следовательно, в этом случае при декодировании перехватчиком кодовое слово будет не только неверным, но будет наблюдаться эффект размножения ошибок на следующих шагах декодирования, увеличивающий количество ошибок за счет того факта, что на предыдущем блоке они не было исправлены или были исправлены ложные искажения.

Исходя из вышеизложенного, можно сделать вывод, что в случае допущения о том, что пропускная способность канала перехватчика меньше, чем пропускная способность легитимного канала, злоумышленник не сможет осуществить декодирование кодовых слов без ошибок, то есть не сможет правильно определить информационное сообщение.

Таким образом, в случае использования кодового зашумления в сочетании со сверточными кодами, также как и в случае использования кодового зашумления в сочетании с кодами Рида-Соломона, удается повысить уровень защиты информационных сообщений при передаче по открытым каналам связи.

Литература.

1. Johanesson Rolf, Zigangirov Kamil Sh. Fundamentals of convolutional coding, New York: IEEE Press, 1999, 428 pp.

2. Савельев М.Ф. Защищенная передача сообщений по открытому каналу, Журнал «Проблемы информационной безопасности. Компьютерные системы», №2, 2003

3. Савельев М.Ф. Оценка вероятности успешного перехвата в каналах с кодовым зашумлением, Журнал «Проблемы информационной безопасности. Компьютерные системы», №2, 2003

4. Сон М. Об одном алгоритме декодирования кодов РС в каналах с кодовым зашумлением, Журнал «Проблемы информационной безопасности. Компьютерные системы», 2004

5. Титова Е.М., Мирончиков Е.Т. Сверточные коды с алгебраическим декодированием, Журнал «Программные продукты и системы», №4, 2008

Трифонов С.Е., Колючкин А.В.

ПРИМЕНЕНИЕ СОВРЕМЕННЫХ БИОМЕТРИЧЕСКИХ ТЕХНОЛОГИЙ ПРИ ВЫЧИСЛЕНИИ ЭЦП

г. Пенза, ФГУП «ПНИЭИ»

С помощью инфраструктуры удостоверяющих центров (УЦ) ЭЦП в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе. Однако, собственноручная подпись является индивидуальным биометрическим показателем человека, содержащим его тайный образ, а ЭЦП – результат совместной деятельности УЦ, выдающего сертификат на основе данных центра регистрации, и технических средств пользователя, осуществляющих работу с закрытым или открытым ключом ЭЦП. В последнем случае имеет место «опосредованность» пользователя, чьи биометрические параметры анализируются только однократно в процессе его первоначальной регистрации, как правило, на основе его регистрационных, учетных и паспортных данных.

В этой связи большую актуальность имеет задача использования биометрических параметров человека при формировании ЭЦП под каждым электронным документом, а также их верификации при обращении или взаимодействии каждого пользователя с УЦ. Для этого биометрические параметры пользователя должны быть включены в сертификаты открытого ключа подписи пользователя.

Таким образом может быть достигнута практически полная персонализация каждого действия при обращении к ресурсам электронного документооборота, так и персонализация собственно электронных документов через индивидуальные биометрические параметры их авторов.

Для выполнения поставленной задачи необходимо использовать современные биометрические технологии высоконадежной аутентификации. Одна из таких технологий, разработанная ФГУП «ПНИЭИ», построена на анализе динамики почерка. Почерк каждого человека уникален. На этом построена процедура рукописной подписи, имеющей юридическую значимость. Исследования показали, что наиболее удобен для автоматической идентификации человека анализ динамики «живой» рукописной надписи. При воспроизведении надписи осуществляется оцифровка колебаний пера X(t), Y(t) и давления пера на подложку Z(t). Эти оцифрованные данные являются «биометрическим образом» подписи пользователя.

Используя несколько «биометрических образов» удается обучить искусственную нейронную сеть автоматически преобразовывать «биометрический образ» подписи в ключ формирования ЭЦП пользователя, который в материальной форме на физическом носителе может вообще отсутствовать.

При корректном предъявлении биометрических параметров цифровой «образ» подписи успешно преобразуется в ключ ЭЦП, который однократно используется для вычисления ЭЦП и затем вновь уничтожается.

При сохранении в тайне биометрического рукописного пароля подобная система биометрической защиты обеспечивает стойкость к атакам подбора на уровне 10^{11} попыток до первой удачи.

Описанный подход был апробирован ФГУП «ПНИЭИ» в программном продукте «Биоконтейнер» с использованием СКЗИ «Верба-ДМ». «Биоконтейнер» обеспечивает выполнение следующих функций: формирование ключей ЭЦП (открытого и закрытого), «растворение» ключей ЭЦП в биометрических параметрах пользователя, восстановление закрытого ключа ЭЦП из биометрических параметров пользователя, формирование и верификацию ЭЦП электронной информации пользователя.

Трунцев В.И., Кабанов А.С.

ОЦЕНКИ СЛОЖНОСТИ ОСУЩЕСТВЛЕНИЯ АТАК НА СИСТЕМЫ ЗАЩИТЫ, ИСПОЛЬЗУЮЩИЕ ЭЛЕКТРОННЫЕ КЛЮЧИ И ИХ ПРИМЕНЕНИЕ

г.Москва, Московский институт электроники и математики

Одной из важных задач охраны авторских прав разработчиков программного обеспечения является разработка средств защиты от несанкционированного распространения. В настоящее время широко используются системы защиты от несанкционированного распространения программного обеспечения, реализованные на электронных ключах. В данной области существует много производителей, но, как правило, они не приводят каких-либо оценок сложности осуществления атак нарушителем. Новизна и практическая значимость работы состоит в построении оценок сложности осуществления атак на различные механизмы защиты и обоснование возможности их применения. Оценки получены в рамках уточненной и дополненной модели нарушителя четвертого уровня Руководящих документов.

В работе исследовалось два типа систем защиты на электронных ключах.

Первый тип. Системы защиты с частичным шифрованием защищаемого программного обеспечения – такие системы, в которых аутентификация электронного ключа защищаемой программой осуществляется проверкой работоспособности и корректности (при запуске), полученной от электронного ключа расшифрованной криптограммы, причем криптограммы, передаваемые электронному ключу от защищаемого приложения, являются результатом шифрования кода программы.

Второй тип. Системы защиты с механизмом запрос-ответ – такие системы, в которых аутентификация ключа защищаемой программой осуществляется сравнением полученного от ключа результата обработки запроса от защищаемой программы с правильным значением, которое может содержаться в программе, библиотеке защиты и т.д. В рамках исследования рассмотрены два типа данных систем защиты. В системах с механизмом запрос-ответ первого типа запрос к ключу является участком кода защищаемой программы. В системах второго типа запрос вырабатывается генератором случайных чисел, реализованным в программной части системы защиты.

В качестве протоколов передачи данных между компьютером и электронным ключом рассматривался плавающий протокол и шифрование, а также их комбинации. Под плавающим протоколом понимается протокол, в котором вместе с реальными данными передаются специально генерируемые, ничего не значащие последовательности («шум»).

В условиях модели нарушителя получены оценки сверху сложности осуществления атак на защищаемое программное обеспечение (с помощью дисассемблера и отладчика) и протокол передачи данных между компьютером и электронным ключом (с помощью анализатора). Полученные оценки целесообразно использовать для отбраковки заведомо неэффективных механизмов защиты. В случае отсутствия явной выраженности неэффективности механизмов защиты оценки можно использовать совместно с методом экспертных оценок. Таким образом, в рамках исследования получен математический аппарат который позволяет научно-обоснованно применять механизмы защиты при разработке систем защиты на электронных ключах, а также оценивать уровень защищенности используемых механизмов в существующих системах.

Фунтиков В.А., Трифонов С.Е.

ТЕХНОЛОГИИ ДОВЕРЕННЫХ ВЫЧИСЛЕНИЙ В РОССИИ

г. Пенза, ФГУП «ПНИЭИ»

В настоящее время весьма актуальна защита различных видов данных, обрабатываемых или сохраняемых вычислительными системами. Не менее важными и проблематичными являются задачи сохранения и контроля целостности программно-аппаратной среды вычислительных устройств, а также обеспечения свойства «доверенности» выполняемых в этой среде процессов.

Все перечисленные задачи информационной безопасности в мировой практике принято характеризовать термином – «доверенные вычисления». Методы и способы их решения называются «технологиями доверенных вычислений». Разработкой и продвижением стандартов по этому направлению занимается международная организация TCG.

Зарубежные производители средств вычислительной техники и программных продуктов в целях реализации технологий доверенных вычислений используют специализированные модули TPM, сертифицированные TCG, которые представляют собой интегральные сопроцессоры.

Однако, TPM осуществляют реализацию заданных функций на базе зарубежных криптографических алгоритмов. Уже в ближайшей перспективе это создаст в России условия, в которых невозможно будет разрабатывать и использовать сертифицированные в условиях российского законодательства средства вычислительной техники, а также программные приложения, требующие применения доверенных вычислений.

Таким образом, остро актуальными являются разработка и последующее серийное освоение отечественной интегральной микросхемы – аналога модуля TPM, реализующей технологии доверенных вычислений в соответствии со спецификациями TCG, но на базе отечественных криптографических алгоритмов.

Предприятием ФГУП «ПНИЭИ» для развития рассматриваемого направления с использованием ранее созданного задела предпринимаются следующие действия:

1. Предприятие – единственное в России, кто получил статус члена международной организации TCG.

2. В кооперации с одним из отечественных предприятий микроэлектронной промышленности создан центр совместного проектирования.

В рамках единой топологической конструкции кристалла отечественного модуля TPM ФГУП «ПНИЭИ» решаются задачи информационной безопасности, а предприятием микроэлектроники – задачи общего проектирования и изготовления микросхем.

3. Проводятся работы по макетированию отечественного модуля TPM на платформе системной платы ПЭВМ фирмы «ASUS», ориентированной на использование технологий доверенных вычислений.

4. В 2009г. совместно с рядом отечественных организаций предполагается проведение работ по разработке дополнений к международным спецификациям TCG с использованием российских криптографических алгоритмов.

Учитывая доступные технологии изготовления изделий микроэлектроники в отечественной промышленности на уровне 0,18 мкм, что соответствует мировым стандартам, можно констатировать следующее: поставленная цель создания условий для развития технологий доверенных вычислений в России на базе отечественных модулей – аналогов TPM, является реально достижимой.

Шехунова Н.А., Беззатеев С.В.

ПОМЕХОУСТОЙЧИВЫЕ КОДЫ В ПОСТКВАНТОВОЙ КРИПТОГРАФИИ

г.Санкт Петербург, Университет Аэрокосмического Приборостроения

С появлением квантовых компьютеров, эффективное использование которых прогнозируется в ближайшие 10 – 15 лет, большинство из используемых в настоящее время алгоритмов несимметричного шифрования окажется неэффективным с точки зрения уровня безопасности, который они обеспечивают сегодня . К сожалению, это касается и всех используемых в настоящее время стандартов шифрования и цифровой подписи (ГОСТ Р32.10-2001, DSA, ECDSA, RSA и пр.). Например, сложность вскрытия RSA в доквантовом криптоанализе определялась величиной $2^{(c+o(1))(\lg n)^{1/3}(\lg \lg n)^{2/3}}$ [1], где n- значение модуля, а c – некоторая константа. Эта оценка обеспечивала достаточно высокую надежность уже при $n > 1024$.

При использовании алгоритма Шора [1] для квантового компьютера сложность вскрытия RSA определяется величиной $(\lg n)^{2+o(1)}$ и единственным ограничением в настоящее время является размер квантового компьютера в $(\lg n)^{1+o(1)}$ кубит, который необходим для реализации алгоритма Шора с такими параметрами.

В то же время появление квантового компьютера практически не изменяет устойчивость алгоритмов шифрования, использующих помехоустойчивые коды. По современным оценкам сложность вскрытия таких алгоритмов составляет $2(0.5+o(1))^{n/\lg n}$, то есть, по-прежнему остается экспоненциальной функцией от n. Существенным недостатком алгоритмов, использующих помехоустойчивые коды, в доквантовой криптографии является большой размер открытого ключа $0{,}016\ b^3/(\lg b)^2$ по сравнению с классическими алгоритмами типа RSA - $b^2(\lg b)^2$. Однако, как указывалось выше, для обеспечения достаточно высокого качества в классических алгоритмах типа RSA, ECC и других придется катастрофически увеличивать размер ключа, и значение b для таких алгоритмов станет существенно больше, чем значение этого параметра для систем, построенных на помехоустойчивых кодах.

Следует так же отметить, что уже в настоящее время для систем, использующих помехоустойчивые коды, разработаны алгоритмы и примитивы, обеспечивающие решение таких задач информационной безопасности как:

1. Конфиденциальность (Алгоритмы McEliece, Niederreiter),
2. Целостность (Алгоритмы подписи и хэш- функций),
3. Скрытность вычислений,
4. Распределения ключей для коалиционных и иерархических систем разграничения доступа,
5. Обеспечение анонимности пользователей и устройств
6. Скрытность информации и защита авторских прав,

Все это позволяет говорить о важности дальнейших исследований в области возможных эффективных применений помехоустойчивых кодов для решения различных задач информационной безопасности.

В докладе приводится сравнительный анализ эффективности асимметричных криптографических систем, рассматриваемых в постквантовой криптографии.

Список литературы:

D. J. Bernstein, J. Buchmann, E.Dahmen, Post-Quantum Cryptography, 2009 Springer-Verlag, Berlin, Heidelberg.

РАЗДЕЛ 3.
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ ГОСУДАРСТВЕННЫХ УЧРЕЖДЕНИЙ

Макаров С.Б.

ТЕРМИНАЛЬНЫЕ КОМПЛЕКСЫ SUN RAY — ЗАЩИЩЕННОЕ РЕШЕНИЕ ПО УПРАВЛЕНИЮ ИНФОРМАЦИЕЙ И ОРГАНИЗАЦИИ ЗАЩИЩЕННОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

г.Москва, ЗАО "МВП "СВЕМЕЛ"

Основной спецификой создания информационных систем в интересах органов государственной власти и управления является необходимость обеспечения доверенности всех компонент, наличие сертифицированных средств защиты информации, масштабируемость, низкие расходы на эксплуатацию, их высокая надежность и сервисная поддержка.

Работы, проведенные ЗАО "МВП "Свемел" для реализации этих требований, привели к созданию доверенной ОС «Циркон – 10» и сертифицированного решения на его основе, реализующего принципы доверенной операционной среды, что позволяет на базе данной технологии обеспечить защищенный доступ к информационным ресурсам, разной степени конфиденциальности.

Рабочие места пользователей оснащаются «тонкими» клиентами — терминалами Sun Ray, что в максимальной степени соответствует требованиям защищенности и экономичности в эксплуатации.

Все задачи, решаемые в рамках выполнения органами государственной власти своих полномочий, так или иначе, связаны с обработкой документов – с их рассмотрением, согласованием и утверждением. Поэтому можно утверждать, что деловые процессы документооборота являются для них критически важными.

Электронный документооборот следует рассматривать как комплексное решение, включающее все задачи автоматизации работы с документами – с секретными, конфиденциальными и открытыми, с текущими и архивными.

Использование единой платформы для организации электронного документооборота всех категорий позволяет значительно сократить эксплуатационные расходы, также как и расходы на внедрение.

Единая платформа также используется для решения задач документооборота и архива. Различными будут лишь наборы функций и пользовательские интерфейсы.

Компания СВЕМЕЛ предлагает решение, которое полностью отвечает этим критериям:

- Инфраструктурный уровень – терминальные комплексы Sun Ray под управлением защищенной ОС "Циркон".
- Прикладной уровень – защищенная платформа управления документами "КЭДО" от компании СВЕМЕЛ.

Платформа "КЭДО" создана на основе импортной промышленной системы управления документами, которая успешно применяется во многих государственных учреждениях Великобритании и по своей функциональности соответствует международным стандартам (которые в настоящее время адаптируются для их принятия в качестве ГОСТов). Разработанные СВЕМЕЛ пользовательские интерфейсы учитывают специфику и практику российского документооборота.

Пилотные проекты по развертыванию защищенного терминального комплекса уже завершены в таких организациях как ФСТЭК, МЭРТ, МИД, РЖД.

Платонов В.В.

АНАЛИЗ ЗАРУБЕЖНЫХ ПОДХОДОВ К ОБЕПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

г.Санкт-Петербург, ГОУ "СПбГПУ"

Рассматривается состояние проблемы обеспечения безопасности персональных данных за рубежом на основе подходов Евросоюза и США.

В Евросоюзе основные принципы были заложены в «Конвенции о защите физических лиц при автоматизированной обработке персональных данных» 1081 г., дополненной в 1999 г. Статья 7 Конвенции «обязывает Стороны принимать надлежащие меры для охраны персональных данных, накопленных в автоматизированных базах данных, от случайного или несанкционированного разрушения или случайной утраты, а равно от несанкционированного доступа, изменения или распространения». Дальнейшее развитие данной проблемы определено в Директивах Европейского парламента и Совета 95/46/ЕС от 24.10.1995 "О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных" и 2002/58/ЕС от 12.07.2002 «Об обработке персональных данных и обеспечении их безопасности в секторе электронных коммуникаций».

В США проблема защиты персональных данных законодательно относится только к государственным организациям. В законе 2002 г. (Public Law 107-347) третий раздел (Federal Information Security Management Act of 2002 (FISMA)) отмечает важность информационной безопасности для экономики и национальных интересов США. В настоящее время решены поставленные Законом задачи:

- стандарты по категоризации информации и информационных систем (Standards for Security Categorization of Federal Information and Information Systems, FIPS 199, февраль 2004 г.).
- руководства, определяющие типы информации и информационных систем для каждой категории (Guide for Mapping Types of Information and Information Systems to Security Categories, NIST 800-60, август 2008 г.).
- минимальные требования по безопасности для информации и информационных систем каждой категории (Minimum Security Requirements for Federal Information and Information Systems, FIPS 200, март 2006 г.).

В докладе анализируется проект «Руководство по защите конфиденциальности персонально идентифицируемой информации» (Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)), NIST 800-122, январь 2009 г.

Поликуров О.В.

ПОЛИТИКА ДОПУСТИМОГО ИСПОЛЬЗОВАНИЯ СЕТИ ИНТЕРНЕТ В ОРГАНАХ ГОСУДАРСТВЕННОЙ ВЛАСТИ

г.Москва, МИФИ

В настоящее время одной из серьезных проблем безопасности для органов государственной власти (далее ОГВ) остается сеть Интернет. С одной стороны Интернет предоставляет колоссальные информационные ресурсы, которыми к тому же можно пользоваться оперативно. Но с другой стороны Интернет представляет серьезную угрозу как для эффективного использования своего рабочего времени сотрудниками ОГВ, так и для безопасности информации ограниченного распространения. Использование ресурсов организации в личных целях (загрузка видео, аудио, картинок, нелицензионного программного обеспечения, социальные сети), т.е. нецелевое использование приводит к потере продуктивности работников приблизительно на 30-40%. Опасность представляет и работа с информацией ограниченного распространения непосредственно на компьютере, подключенном к сети Интернет. Кроме того, возможно заражение корпоративной сети злонамеренными программами при переносе информации с компьютера, подключенного к сети Интернет на компьютер, подключенный к сети организации.

Обычно в ОГВ обеспечивают информационную безопасность своих ресурсов фрагментарно, проводя различные административные мероприятия и «внедряя в жизнь» организационно-распорядительные документы. Но зачастую подобные меры не способны решить задачу обеспечения информационной безопасности организации. Для успешного решения задачи комплексного обеспечения информационной безопасности необходимы политики информационной безопасности (далее ПИБ).

Создание эффективной политики безопасности в подобных организациях сопряжено с огромными трудностями. Дело даже не в том, как создать саму политику. Проблема заключается в ее исполнении всеми работниками организации. Необходимость ПИБ не всегда является очевидной для работников. Кроме того, внедрение политик зачастую приводит к возникновению проблем во взаимоотношениях между сотрудниками ОГВ и персонала службы технического обеспечения (ИТ-служба) организации. Некоторые служащие часто стараются не следовать каким-либо правилам безопасности, так как не хотят ограничивать себя в своих действиях. Другие заинтересованы в оперативном исполнении своих обязанностей и просто игнорируют положения политики безопасности, особенно если она требует дополнительных процедур. Для решения данной проблемы многие специалисты советуют разрабатывать ПИБ с учетом мнения *всех* заинтересованных сотрудников организации. До начала внедрения новой политики желательно предоставить работникам ее текст для ознакомления и внесения поправок и комментариев. Также надо учитывать, что без прав нет обязанностей, то есть сотрудники, на которых распространяются правила безопасности, должны обладать всеми необходимыми полномочиями для того, чтобы выполнять эти правила. Одновременно, необходимо активное участие руководства организации, которое должно не только обеспечить выполнение политики безопасности, но и само следовать этой политике. Возникает вопрос: как заинтересовать руководство в решении данной задачи? Автору видится необходимым разработка методики оценки эффективности политики допустимого использования сети Интернет в ОГВ, что даст возможность наглядно продемонстрировать эффект от внедрения таких организационных мер.

Трифонов С.Е., Колючкин А.В.

О НАУЧНЫХ РАЗРАБОТКАХ ФГУП «ПНИЭИ» В ОБЛАСТИ СИСТЕМ ЮРИДИЧЕСКИ ЗНАЧИМОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

г. Пенза, ФГУП «ПНИЭИ»

Неотъемлемыми свойствами любого документа, как материального, так и электронного являются: подлинность и авторство, а в ряде случаев и юридическая значимость, - обеспечиваемые либо собственноручной подписью автора, уполномоченного и ответственного лица, либо электронной цифровой подписью (ЭЦП). Таким образом, для того, чтобы файлы можно было классифицировать в качестве «электронного документа» необходимо, чтобы они имели в своем формате реквизит «ЭЦП».

По направлению создания систем юридически значимого электронного документооборота (ЭДО) с использованием ЭЦП предприятием ФГУП «ПНИЭИ» проводятся следующие работы: разрабатываются и внедряются средства ЭЦП в различных вариантах исполнения в различных классах защищенности, разрабатывается и внедряется инфраструктура УЦ с расширенным составом компонентов, разрабатываются и внедряются АРМ абонентов системы защищенной электронной почты и электронного документооборота.

Средства ЭЦП разрабатываются в двух вариантах исполнения: в виде программного продукта (криптопровайдер «Верба-ДМ»), в виде изделия «Криптофлэш-провайдер», внешне напоминающего обычную USB-Flash.

Для обеспечения возможности организации защищенной системы ЭДО и электронной почты с юридически значимой ЭЦП ФГУП «ПНИЭИ» разработаны компоненты инфраструктуры УЦ, имеющего несколько принципиальных отличий от аналогов:

- защита компонент УЦ от негативного воздействия со стороны сетей общего пользования по высокому классу защищенности;
- разветвленная многокомпонентная структура УЦ: центр сертификации, центр регистрации, центр обработки запросов – репозиторий, АРМ разбора конфликтных ситуаций, АРМ аудитора, Архив, сервис меток времени, сервис проверки актуальности сертификатов, межсетевой криптографический шлюз, удаленные пункты регистрации;
- взаимодействие абонентов с УЦ происходит только через центр обработки запросов – репозиторий по web-интерфейсу;
- автоматизированная рассылка служебных сообщений УЦ абонентам по электронной почте.

Разработка УЦ была проведена по техническому заданию, согласованному с руководством аппарата Правительства Пензенской области с учетом интересов региона. Развитие инфраструктуры УЦ в Пензенской области на базе технических средств ФГУП «ПНИЭИ» проводится по направлению создания электронного пространства доверия в регионе на базе юридически значимой ЭЦП, а также внедрение современных систем ЭДО в служебную деятельность ФГУП «ПНИЭИ», ряда других предприятий региона, а также аппарата Правительства Пензенской области. По данному направлению проводятся работы по развертыванию регионального УЦ.

Таким образом, в докладе рассмотрен комплексный подход предприятия ФГУП «ПНИЭИ» к решению задач создания современной системы ЭДО с юридически значимой ЭЦП. Разрабатываемый комплекс технических средств охватывает как абонентские приложения, так и инфраструктурные системо-образующие элементы. Разработка комплекса проводится с использованием современных и наукоемких технологий. В целом создаваемый задел может быть эффективно использован другими предприятиями России.

РАЗДЕЛ 4.
АНАЛИЗ И КОНТРОЛЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ КОМПЬЮТЕРНЫХ СЕТЕЙ

Баранов В.А.

ОБНАРУЖЕНИЕ МЕЖМОДУЛЬНЫХ УЯЗВИМОСТЕЙ СРЕДСТВАМИ ДИНАМИЧЕСКОГО АНАЛИЗА

г.Москва, МГУ им.М.В. Ломоносова

Существует такая разновидность уязвимостей веб-приложений, как уязвимость к внедрению кода, которая принадлежит к классу уязвимостей, связанных с некорректной обработкой пользовательского ввода. Уязвимости к внедрению кода можно разделить на одномодульные и межмодульные. Разница между ними заключается в том, что одномодульная уязвимость – свойство отдельного модуля веб-приложения, а межмодульные уязвимости появляются в результате зависимости нескольких модулей по данным и отсутствия корректной обработки этих данных.
Данная работа посвящена обнаружению межмодульных уязвимостей в веб-приложениях средствами динамического анализа. Конечными результатами работы являются:

- Описание модели поведения веб-приложения, с помощью которой можно обнаруживать межмодульные уязвимости;

- Программное средство, использующее разработанную модель для выявления уязвимостей рассматриваемого типа.

На данный момент классическим подходом к обнаружению уязвимостей, связанных с некорректной обработкой пользовательского ввода, является подход Tainted Mode. Однако, модель уязвимостей, используемая в этом подходе, обладает ограничением, которое делает невозможным применение ее для обнаружения межмодульных уязвимостей. Ограничение заключается в том, что с помощью этой модели можно анализировать лишь отдельные модули веб-приложения, но невозможно отследить, как модули связаны между собой по данным.

Разработанная модель базируется на классической модели Tainted Mode, но имеет ряд существенных доработок (анализируется граф зависимости по данным (Data/Program Dependency Graph) всего веб-приложения, а не отдельных его модулей).

Программное средство использует трассы динамического анализа веб-приложения и схему базы данных, используемой этим приложением, для построения графа зависимостей по данным для всего приложения. Анализ такого графа позволят отслеживать потоки данных через БД и выявлять межмодульные уязвимости. Программное средство пригодно для обнаружения, как одномодульных уязвимостей, так и межмодульных уязвимостей.

Гуцко Д.В.

ПОИСК НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ С ИСПОЛЬЗОВАНИЕМ МЕТОДА ПЕРЕХВАТА СИСТЕМНЫХ ВЫЗОВОВ

г.Москва, МИФИ, факультет "Информационная безопасность"

Современное законодательство РФ в области обнаружения недекларированных возможностей ПО ("Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей") основывается в первую очередь на статическом анализе исследуемого ПО (ИПО). Большой плюс данных методов - их способность обнаруживать вирусы и вредоносные действия в файлах прежде, чем эти скрытые опасности смогут инфицировать компьютеры и нанести какой-либо ущерб. Однако эти методы фактически не в состоянии обнаружить вирусы, кодирующие свое тело, скрывающие логику и применяющие средства защиты от исследования. Зачастую единственным способом определить, есть ли в интересующем нас файле вредные фрагменты кода - это выполнить его в реальных условиях и определить вред, который он нанес.

Анализ работающей программы (динамический анализ) и её окружения наиболее сложен и опасен, но при этом и наиболее информативен. Метод перехвата системных вызовов является одним из методов динамического анализа. Данный подход основан на анализе выполняемых ИПО операций в реальном режиме времени.

Основываясь на основных принципах информационной безопасности – обеспечение конфиденциальности, целостности, доступности, предлагается отслеживать только те операции ИПО, которые влияют на конфиденциальность, целостность, доступность хранимой или обрабатываемой информации. Данные действия можно разделить на четыре основные группы: операции с элементами файловой системы (например, чтение/запись файлов или каталогов), операции с элементами системного реестра (например, чтение/запись значений ключа реестра), Операции с приемом-передачей информации через вычислительную сеть (например, отправка/прием сетевых пакетов), операции с оперативной памятью (например, попытки чтения области памяти другого процесса).

В развитии данного метода предлагается для каждого ИПО составлять профили ИПО (список всех разрешенных действий ИПО: по доступу к файловой системе, системному реестру, вычислительной сети и с оперативной памятью). Например, ИПО разрешается чтение таких-то файлов, отсылка сетевых пакетов такому-то получателю, чтение таких-то веток реестра и т.д. Данный профиль должен быть легко интерпретируем, для анализа возможностей ИПО каждым пользователем и оценки потенциальных угроз при применении данного ПО в информационной системе. На ЭВМ устанавливается программная часть, осуществляющая в режиме реального времени проверку соответствия выполняемых действий ИПО – профилю (Назовем данное ПО – ПО для анализа соответствия профилю ИПО, сокращенно - ПАП). В случае обнаружения каких-либо несоответствий, данным ПО (ПАП) могут быть предприняты ряд сигнальных или ограничивающих действий.

В дополнение ПАП может выполнять функции по самогенерации профилей ИПО, например, в режиме мониторинга собирать и анализировать действия предпринимаемые ИПО, без какого-либо ограничения ИПО. В последствии данный профиль передается специалистам для дальнейшего изучения или сертификации ИПО.

Жилкин С.Д.

МЕТОДЫ ПОСТРОЕНИЯ МОДЕЛЕЙ ШТАТНОЙ РАБОТЫ ПО И АЛГОРИТМЫ ВЫЯВЛЕНИЯ АНОМАЛЬНОГО ПОВЕДЕНИЯ ПО

г.Москва, Московский инженерно-физический институт

Предпосылкой к данной работе является сложившаяся ситуация в сфере информационной безопасности. Существует множество антивирусов, препятствующих выполнению вредоносного кода. Большинство из них основываются на сигнатурном и эвристическом методах анализа исполняемого файла для выявления вредоносного кода. Меньшее внимание уделено проблеме выявления и локализации недекларированных возможностей ПО. Учитывая, что код, приводящий к НСД, сам по себе может не являться вредоносным с точки зрения антивирусов, становится очевидным, что одни антивирусы не обеспечивают должный уровень защиты данных от НСД и НДВ.

Для жёстко алгоритмизированного ПО уже создано множество механизмов выявления отклонений работы. Данная работа направлена на ПО, функционирование которого имеет высокую степень ветвления или зависит от действий пользователя. В данной работе заранее заданная эталонная модель строится по характеристикам штатной работы ПО. Профиль поведения процесса определяется основными характеристиками реального функционирования этого процесса. После того, как эталонная модель поведения построена, все создаваемые в реальном времени профили работы ПО сравниваются с эталонной моделью. Расхождение реального профиля и эталонного модели ПО расценивается как аномальное поведение ПО.

Реальный профиль работы является набором характеристик работы процесса (количественных, логических и статистических). Туда входят такие параметры, как число обращений к системным файлам, библиотекам и сетевым ресурсам и т.п. В данной работе предлагается задавать эталонную модель штатного поведения ПО нейронными сетями. На вход нейронной сети подаётся профиль реальной работы ПО. Параметры нейронной сети подобраны таким образом, чтобы её выход являлся вероятностью соответствия обработанного профиля той модели, которую данная нейронная сеть задаёт. Таким образом, в данном алгоритме основная задача состоит в построении эталонной модели поведения. Так как любое запущенное ПО проходит три фазы: 1) инициализация, 2) рабочий цикл и 3) завершение работы, модель поведения задаётся как минимум 3 нейросетями. Особое внимание уделяется обучению нейронных для рабочего цикла. Таких сетей может быть несколько, в зависимости от количества различных специфических действий, проявляющихся во время работы ПО.

Автоматизированное построение таких моделей подразумевает обучение нейронных сетей характеристиками ПО, полученных при штатной работе. Каждая сеть обучается (подвергается подборке коэффициентов и смещений нейронов) по наиболее эффективному методу обратного распространения ошибки так, чтобы на профилях штатной работы выдавать вероятность, близкую к 1. Такое обучение нейронных сетей позволяет с высокой вероятностью (не ниже 0.9) определять заданное ПО, когда как побочное ПО на данной сети будет показывать очень низкую вероятность соответствия.

Таким образом, любое аномальное поведение ПО, вызванное подменой или внедрением чужого кода, приведёт к резкому уменьшению вероятности соответствия эталонной модели и будет опознано. В отличие от обучения, проверка профиля реального поведения занимает очень короткое время, что позволяет одновременно следить за работой множества процессов.

Зегжда Д.П., Калинин М.О., Москвин Д.А.

ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ ПОСТОЯННЫХ И ИЗМЕНЯЮЩИХСЯ КОМПОНЕНТОВ ПРОГРАММНОЙ СРЕДЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

г.Санкт-Петербург, ГОУ "Санкт-Петербургский государственный политехнический университет"

Для любой современной информационно-телекоммуникационной системы (ИТКС) характерно непрерывное изменение и усложнение структуры программной среды, включающей системное, прикладное программное обеспечение и средства защиты.

Развитие информационных технологий с одной стороны позволяет повысить функциональный потенциал использования программной среды ИТКС, предоставляя новые возможности и эффективные средства по их реализации. С другой стороны, подобная вариативность решений открывает для внешних и внутренних злоумышленников новые возможности по нарушению информационной безопасности (ИБ) за счет возникновения новых уязвимостей.

Безопасность программной среды ИТКС обеспечивается включением в ее состав средств защиты, таких как антивирусное программное обеспечение, межсетевые экраны, системы обнаружения атак, системы аутентификации и разграничения доступа.

Все программные компоненты ИТКС можно разделить на две группы: постоянные и изменяющиеся. К постоянным относятся компоненты программной среды, состав и содержимое которых не изменяется на всем протяжении эксплуатации ИТКС. Целостность таких компонентов может контролироваться "традиционным" методом контрольного суммирования. К изменяющимся относятся компоненты программной среды, состав и содержимое которых может изменяться во время эксплуатации ИТКС. Изменения могут быть обусловлены установками различных обновлений, дополнений, исправлений и новых версий системного, прикладного программного обеспечения и средств защиты, их конфигурированием и установлением функциональной совместимости. Наличие таких изменений не позволяет контролировать целостность программной среды с помощью криптографических методов (контрольного суммирования, подсчета ЭЦП, хэшей). Поэтому необходим более гибкий механизм контроля и обеспечения целостности, который позволял бы обеспечивать и контролировать согласованность параметров функционирования и безопасности системного, прикладного программного обеспечения (ПО) и средств защиты с характеристиками программной среды ИТКС.

Функционирование программной среды ИТКС должно быть согласовано со следующими ее характеристиками, а также связями между ними:

- особенности конкретной программной среды ИТКС;
- условия эксплуатации средств защиты;
- назначение и состав используемого системного и прикладного ПО;
- актуальные угрозы безопасности.

Таким образом, целостность программной среды ИТКС — это состояние взаимного соответствия конфигурационных параметров системного, прикладного ПО и средств защиты. Следовательно, задача обеспечения целостности программной среды ИТКС представляется как достижение взаимоувязанности и единства используемых

средств защиты и характеристик программной среды ИТКС. Обеспечение целостности программной среды ИТКС осложняется наличием ряда факторов, таких как:

– применение разнообразного ПО с множеством функциональных свойств и настроек, предназначенного для обработки разнородной информации, поступающей из различных источников;

– гетерогенность вычислительных сетей ИТКС, в которых взаимодействуют компьютеры под управлением ОС различных семейств (MS Windows, UNIX/Linux и пр.);

– необходимость оперативной передачи информации между территориально удаленными подразделениями;

– необходимость учитывать изменения программной среды ИТКС, связанные с обновлением ПО, установкой различных обновлений и функциональных дополнений, изменением пользовательского состава;

– необходимость контроля, предупреждения и предотвращения нарушений ИБ.

В этой связи механизм обеспечения целостности основывается на следующих принципах:

– принцип моделирования поведения средств защиты (необходимо использование логической модели, описывающей и предсказывающей поведение средств защиты с учетом характеристик программной среды ИТКС);

– принцип эквивалентности состояний программной среды (задание отношений эквивалентности между состояниями программной среды ИТКС в виде простых критериев. Под состоянием программной среды понимается множество всех настроек и конфигурационных параметров безопасности (ПБ) системного, прикладного ПО и средств защиты, зафиксированное в некоторый момент времени);

– принцип допустимых отклонений (формирование с помощью критериев области, в которой допустимы отклонения для изменяемых ПБ и в которой методы контрольного суммирования имеют ограниченную применимость).

Указанные принципы позволят контролировать целостность программной среды ИТКС с учетом ее изменений, которые не нарушают цельность совокупности свойств и характеристик среды, связей между ними и внешними факторами. В соответствие с изложенными принципами авторами разработана технология обеспечения целостности программной среды, в основе которой лежит концепция области эквивалентности конфигурационных ПБ.

Область эквивалентности представляет собой объединение подмножеств конфигурационных ПБ системного, прикладного ПО и средств защиты, которые удовлетворяют требованиям безопасности и функционирования программной среды ИТКС. Любые сочетания конфигурационных ПБ программных компонентов, которые принадлежат области эквивалентности, удовлетворяют требованиям согласованности параметров функционирования и безопасности программных компонентов с характеристиками программной среды ИТКС. Если изменение состояния программной среды приводит к отклонению конфигурационных параметров программных компонентов, не выходящих за границы области эквивалентности, то целостность программной среды ИТКС сохраняется.

Данная технология позволяет автоматизировать решение задачи контроля целостности программных сред ИТКС и реализовать следующие функции:

1. Контроль соответствия программной среды требованиям безопасности и регламентам эксплуатации.

2. Контроль соответствия программной среды назначению ИТКС и текущим задачам ее применения.
3. Контроль инвариантности программной среды по всем компонентам ИТКС.
4. Оценка интегральных характеристик программной среды.
5. Вычисление нормализованного представления безопасности конфигурации.

Применение данной технологии позволяет оперативно, целенаправленно и эффективно реагировать на негативные изменения, происходящие в программной среде ИТКС в процессе ее эксплуатации, и тем самым поддерживать интегральную информационную устойчивость функционирования ИТКС, предотвращая недоступность ресурсов, отказы сервисов, сбои и нарушения безопасного функционирования элементов программной среды ИТКС. Применение данной технологии также позволяет оптимизировать управление ИБ, повысить эффективность эксплуатации инфраструктуры ИТКС, и при этом понизить требования к квалификации персонала.

Зегжда Д.П., Калинин М.О., Москвин Д.А., Разумовский Е.И.

ОПЫТ ПРИМЕНЕНИЯ ПРОГРАММНОГО КОМПЛЕКСА "ДЕКАРТ" ДЛЯ РЕШЕНИЯ ТИПОВЫХ ЗАДАЧ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ WINDOWS-СЕТЕЙ

г.Санкт-Петербург, ГОУ "Санкт-Петербургский государственный политехнический университет"

Современные информационные системы (ИС) подвержены воздействиям, которые могут носить деструктивный характер и приводить к нарушению функционирования систем и несанкционированному доступу к ее ресурсам. Для конфигурирования ИС в соответствии с выбранной политикой безопасности ее требования необходимо реализовать с помощью настройки конфигурационных параметров программных средств контроля доступа (ПСКД). Такая настройка выполнима различными способами и производится администратором безопасности. При этом администратор должен учитывать все конфигурационные параметры ПСКД и их взаимное влияние. Сложная структура и неочевидные зависимости конфигурационных параметров является причиной ошибок администрирования. Например, администратор безопасности ОС Windows при назначении полномочий пользователям зачастую ограничивается настройкой прав доступа, забывая о системных привилегиях, которые позволяют пользователям получать полный доступ к объектам независимо от установленных прав. Для исключения подобных ситуаций необходимо автоматически преобразовывать требования политики безопасности в набор конфигурационных параметров ПСКД.

При настройке конфигурационных параметров ПСКД необходимо учитывать требования нормативных документов и рекомендаций экспертов с целью обеспечения требуемого уровня защиты. Рекомендации по настройке обычно оформляются в виде шаблонов безопасности. Шаблоны описывают значения для тысяч различных параметров, поэтому их применение администратором вручную практически невозможно. Следовательно, необходимо использовать автоматизацию применения в системе таких шаблонов.

После настройки системы необходимо периодически контролировать выполнение требований безопасности. Если контролировать только стабильность настроек, то любые изменения в состоянии системы становятся невозможными с точки зрения ее безопасности. Например, добавление нового пользователя может не повлиять на выполнение политики безопасности, но приводит к изменению настроек системы. Поэтому для контроля выполнения политик безопасности и шаблонов требуется механизм, учитывающий иерархию и влияние настроек на полномочия пользователей системы.

Конфигурирование в соответствии с одной и той же политикой безопасности может быть выполнено различными способами. Например, права на файл могут быть назначены индивидуально или посредством наследования прав от каталога. Зачастую одновременно используются все доступные методы, что сильно усложняет понимание конфигурации системы, например, при смене администраторов или при необходимости внесения изменений в существующие настройки. Как следствие, возникают сложности управления безопасностью, которые приводят к ошибкам администрирования. Следовательно, необходимо анализировать сложность конфигурации системы с целью выявления закономерностей между простотой понимания системы и ее параметрами безопасности и оптимизации настройки.

В рамках локальной сети организации рабочие станции сгруппированы по функциональным назначениям, которые определяются ролями станций и пользователей ИС. Все станции, входящие в состав функциональной группы, должны иметь единый состав ПО и одинаковый уровень защищенности. Для этого необходима унификация системной конфигурации в рамках функциональных групп и поддержание неизменности этой конфигурации в процессе эксплуатации ИС.

Современные ИС характеризуются большим количеством рабочих станций, в силу чего ручное управление конфигурациями систем затруднено, поэтому требуется средство, позволяющее централизованно и в автоматическом режиме управлять состояниями удаленных систем, фиксируя текущую конфигурацию, выявляя и устраняя нарушения безопасности.

С целью решения указанных проблем авторами разработан программный комплекс (ПК) "Декарт", позволяющий автоматизировать управление безопасностью конфигураций в Windows-сетях. Данное решение в отличие от конкурирующих продуктов позволяет:

- анализировать полное множество конфигурационных параметров безопасности ОС;
- формировать собственные произвольные проверки подсистемы безопасности;
- анализировать состав нарушений безопасности, составлять и выполнять инструкции по устранению выявленных нарушений;
- оценивать эффективность администрирования безопасности;
- сопоставлять состояния безопасности ОС.

Автоматизируя указанные функции, ПК "Декарт" позволяет отказаться от "ручного" выполнения настройки и анализа безопасности системы. Таким образом, все функции управления безопасностью системы могут быть выполнены даже оператором, не обладающим квалификацией администратора.

ПК "Декарт" реализует запатентованные технологии, в том числе касающиеся определения множества доступных прав пользователей, оценки эффективности управления безопасностью, сопоставления состояний ОС, автоматизации оценки защищенности информационных систем. ПК "Декарт" удостоен серебряной медали премии "ЗУБР" как лучшее интеграционное решение.

ПК "Декарт" как сертифицированное средство применяется для удаленного управления и анализа безопасности в крупных информационных комплексах, например, в системе ОАО "Российские железные дороги". В таких критических системах выведение из строя одного звена может привести к нарушению функционирования всей системы, поэтому ошибки администрирования недопустимы. ПК "Декарт" автоматизирует процесс мониторинга и настройки политик безопасности. В случае выявления нарушений ПК "Декарт" позволяет выявить состав нарушений и устранить их путем переконфигурирования системы.

Для многих информационных систем, например в банковском секторе, критичной является целостность активов. При этом метод контрольного суммирования не всегда применим, т.к. среда функционирования систем изменяема: необходимо устанавливать обновления, дополнения, новые версии ПО, обновлять антивирусные базы. ПК "Декарт" использует метод обеспечения целостности программной среды, основанный на контроле допустимых отклонений от первоначальной настройки. Поэтому все изменения, происходящие в системе, проверяются в ПК "Декарт" на то,

остаются ли конфигурационные параметры системы в области допустимых отклонений.

ПК "Декарт" позволяет проконтролировать конфиденциальность данных (например, персональных данных) за счет контроля всего множества системных и пользовательских ресурсов и учета влияния настроек безопасности на фактическое распределение полномочий пользователей.

Возможности ПК "Декарт" позволяют его применять для решения широкого круга задач, включая процессы сертификационных испытаний и автоматизированного управления безопасностью.

Калинин М.О., Москвин Д.А.

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ОЦЕНКИ ПОЛНОМОЧИЙ ПОЛЬЗОВАТЕЛЕЙ ПУТЕМ ВЫЧИСЛЕНИЯ МНОЖЕСТВ ДОСТУПНЫХ ПРАВ

г.Санкт-Петербург, ГОУ "Санкт-Петербургский государственный политехнический университет"

Работа выполнена в рамках реализации аналитической ведомственной целевой программы "Развитие научного потенциала высшей школы (2009-2010 годы)"

Проблема проверки соблюдения требований информационной безопасности сводится к контролю выполнения условий безопасности состояний системы. Перечни таких условий имеют вид политик безопасности и эталонных состояний системы. В них указываются состав и значения конфигурационных параметров безопасности, ограничения на полномочия пользователей, при выполнении которых система считается безопасной. Задача сверки этих индикаторов безопасности с фактическим распределением значений конфигурационных параметров решается путем сопоставления множеств.

В случае проверки явных параметров, например, таких как имена пользователей или ресурсов, членов группы, установленных привилегий пользователей, списков контроля доступа, сопоставление множеств выполняется тривиально путем наложения "требуемого" множества на "реальное" и выявления их несовпадений. В случае проверки полномочий пользователей, когда необходимо проконтролировать выполнение ограничений на доступ к информационным ресурсам и проанализировать нарушения доступа, необходимо учитывать не только права, заданные в списке контроля доступа, но и влияние всего множества параметров безопасности на фактические возможности пользователей. Для этого обычного, как при проверке явных параметров, сопоставления двух множеств на уровне списков контроля доступа недостаточно. Но и прямой перебор множеств всех конфигурационных параметров с учетом всех возможных комбинаций затруднителен. С этой целью авторами предлагается способ повышения эффективности оценки полномочий пользователей путем свертки состояния конфигурационных параметров, участвующих в контроле доступа, в множество доступных прав.

В ОС семейства Microsoft Windows множество конфигурационных параметров образует иерархию факторов, влияющих на доступ. На каждом уровне иерархии выполняется расширение или замена соответствующего конфигурационного параметра на множество доступных прав. В общем случае, для i-го уровня иерархии множество доступных прав $EP_i = f(subject, EP_{i-1}, A_i)$, где $2 \le i < m$, m — количество уровней иерархии. Функция f вычисляет множество доступных прав EP_i, имеющихся у пользователя или группы $subject$, на i-ом уровне с учетом влияния атрибута безопасности A_i. Например, для уровня 5, на котором учитываются запреты, множество EP_5 вычисляется как $EP_5(subject) = EP_4^+(subject)$ XOR $EP_4^-(subject)$, где EP_4^+ — EP_4, вычисленный для прав, EP_4^- — для запретов, $subject$ — пользователь или группа; $EP_4(subject) = EP_3(subject)$ AND $EP_3(\{groups_j\} | \forall i\ subject \in groups_j)$; ...; $EP_1(subject) = \{bits_k\}$, где $\{bits_k\}$ — множество битов доступа в маске прав дискреционного списка прав доступа субъекта, приведенного в атрибутах объекта.

Таким образом, наличие указанной процедуры вычисления эффективных прав упрощает задачу проверки полномочий пользователей. Для состояния системы

вычисляется множество доступных прав, которыми можно воспользоваться в данном состоянии, и оно сопоставляется с множеством, заданным в условии безопасности системы. Наличие иерархии и однозначного соответствия "конфигурационный параметр-доступные права" позволяют при обнаружении любого нарушения безопасности, не только определять, что повлекло за собой выявленное нарушение, но и путем воздействия именно на этот фактор добиваться выполнения требований информационной безопасности.

Комашинский Д.В., Котенко И.В., Шоров А.В.

ТЕХНОЛОГИЯ ДЕТЕКТИРОВАНИЯ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА ОСНОВЕ МЕТОДОВ DATA MINING

г. Санкт-Петербург, СПИИРАН

Наблюдаемое в настоящее время активное смещение фокуса функциональности вредоносных программ на обеспечение требований скрытности, длительности и устойчивости функционирования, активного противодействия антивирусным программным комплексам все больше подчеркивает недостатки традиционно используемых методов их детектирования. Средства структурной и функциональной обфускации, техники поиска и использования уязвимостей повсеместно используемых клиентских и серверных приложений, постоянное появление новых средств разработки и вычислительных сред делают маловозможным продолжение использования устоявшейся парадигмы противодействия преступному сообществу, активно диверсифицирующему свои активы в средства осуществления преступлений в сфере информационных технологий. Успешное разрешение данных вызовов не может быть осуществлено без привлечения методов интеллектуального анализа данных, позволяющих при определенных условиях нивелировать недостатки существующих методов статического и динамического обнаружения вредоносного программного обеспечения.

Работа, предлагаемая к рассмотрению, представляет один из способов построения технологии, ориентированной на обнаружение вредоносного программного обеспечения, находящегося в активных фазах своего жизненного цикла (распространение / выполнение атакованным хостом). Подход базируется на сборе, обработке и анализе информации о приложении, степень опасности которого должна быть оценена.

Сбор информации учитывает структурные и поведенческие особенности исследуемого объекта. Понятие структуры включает в себя упорядоченный набор данных, которые могут быть извлечены из приложения за счет учета особенностей содержимого программных компонентов, обеспечивающих его функционирование. Понятие поведения основано на представлении функциональности приложения в виде групп событий, выполняемых им. Понятие терминального события базируется на факте однократного обращения приложения к ресурсам операционной системы. Терминальное событие включает в себя идентификатор перехваченной функции, набор переданных ей аргументов и возвращенное значение. Для проведения экспериментов выбран традиционный вариант пользовательского ПК, работающего под управлением ОС Windows XP. Мониторинг обращения к ресурсам ОС реализован перехватчиком вызовов Native API, являющего основным интерфейсом ядра операционных систем Windows NT и пользовательскими приложениями.

Задачи обработки и анализа собранных данных и вынесения по ним вердикта о степени вредоносности анализируемого приложения предлагается рассматривать как задачи оптимизации признакового пространства и классификации, решаемых подходами, объединенными дисциплиной интеллектуального анализа данных (Data Mining). Оптимизация набора признаков (выделение наиболее значимых) решается в рамках подзадач извлечения, выделения и конструирования аттрибутов, описывающих исследуемый объект. Задача подготовки классификатора является задачей обучения с учителем, и в данной работе решается использованием в качестве исходных данных

описаний как заведомо безопасных, так и различных классов вредоносных приложений.

Рассмотрены вопросы формирования пространства аттрибутов, присущих вредоносным и безопасным приложениям, на которых производится обучение и валидация классификаторов семейств Bayes, Decision Tree, Rule Induction. Развитие работы предполагает расширение набора исследуемых классификаторов, выбор оптимальных для частных случаев задач детектирования, оценку показателей скорости и ресурсопотребления процессов обучения и принятия решения.

Работа выполняется при финансовой поддержке РФФИ (проект №07-01-00547), программы фундаментальных исследований ОНИТ РАН и при частичной финансовой поддержке, осуществляемой в рамках проекта Евросоюза RE-TRUST.

Коноплев А.С., Москвин Д.А.

ИСПОЛЬЗОВАНИЕ МЕТОДА "ЧЕРНОГО СПИСКА" ДЛЯ ПРОТИВОДЕЙСТВИЯ ИСКУССТВЕННОМУ ПОВЫШЕНИЮ РЕЙТИНГА САЙТА В ПОИСКОВЫХ СИСТЕМАХ

г.Санкт-Петербург, ГОУ "Санкт-Петербургский государственный политехнический университет"

Задавая в поисковом запросе ключевые слова или фразы, пользователь должен получить ссылки на сайты, посвященные той тематике, к которой относятся указанные слова. Полученные ссылки располагаются в порядке понижения рейтинга сайта, на который они указывают. Рейтинг сайта задается поисковой системой. Существуют методы, позволяющие выдать страницу сайта за идеально подходящую под заданную тематику, несмотря на то, что она таковой не является. Такие методы будем называть методами искусственного повышения рейтинга.

Искусственное повышение рейтинга может использоваться для получения конфиденциальных данных пользователя посредством маскировки одного сайта под другой известный сайт. Если рейтинг такого подложного сайта высок, то пользователь может перейти по ведущей на него ссылке и скомпрометировать свои конфиденциальные данные. Искусственное повышение рейтинга запрещено в использовании поисковыми системами, т.к. оно снижает безопасность информационных систем.

Выделяют следующие основные методы искусственного повышения рейтинга:

1. Повышение плотности ключевых слов. Поисковые машины используют слова на страницах как главный фактор определения рейтинга сайтов. Особо важную роль играют слова, указанные в специальных метатегах, задающих тематику данной страницы. Поэтому увеличение количества ключевых слов приводит к повышению рейтинга сайта в поисковой системе.
2. Скрытие текста. Для сокрытия ключевых слов применяется текст, цвет которого совпадает с фоном страницы. В результате сайт может иметь высокий рейтинг по отличной от представляемой пользователям тематике.
3. "Кликерство". При расчете рейтинга учитывается популярность сайта, т.е. частота его посещения разными пользователями. "Кликерство" состоит в разработке утилит, которые постоянно переходят на страницу указанного сайта.
4. Повышение индекса цитирования. Индекс цитирования — это суммарное количество внешних ссылок на страницу, умноженное на тематический вес сайтов с данными ссылками. В Интернете существуют специальные сайты, на которых любой веб-мастер может бесплатно разместить ссылку на свой сайт.
5. Маскировка. Данный метод заключается в предоставлении разных страниц поисковому роботу и посетителю сайта. Для реализации этого метода необходимо иметь две версии страницы: одну — для посетителей, другую — для поисковых роботов. При написании страницы для посетителей нет необходимости использовать специальные слова или метатеги, поскольку такая страница является недоступной для поисковой системы. На второй странице можно использовать также другие методы искусственного повышения рейтинга.

Эффективность перечисленных методов определяется следующими показателями:

- безопасность метода — вероятность обнаружения применения метода поисковой системой;
- время, которое требуется для повышения рейтинга сайта;
- простота реализации метода на практике;

- эффект ранжирования — количество пунктов, на которые увеличится рейтинг сайта.

Наиболее эффективным методом является маскировка. Его преимуществом является тот факт, что, даже если страница, предназначенная для пользователя, будет обнаружена поисковой системой, это не приведет к штрафным санкциям, поскольку на такой странице нет запрещенных методов.

В настоящее время лишь некоторые поисковые системы обладают методами противодействия маскировке. Для выявления применения маскировки, используется метод, основанный на сравнении страниц, находящихся в кэше поисковой системы и вновь представленных на сайте. Такое сравнение должно производиться по специальным критериям отличия пользовательской и поисковой страниц. В основном, борьба с маскировкой происходит в ручном режиме, когда о наличии на сайте запрещенного метода сообщают сторонние лица. Такой метод борьбы не является эффективным, поэтому принимаются усилия по внедрению автоматизированных методов обнаружения маскировки.

Сравнение и анализ страниц всех сайтов при каждом индексировании — трудоемкий процесс, который негативно скажется на скорости работы поисковых машин. Поэтому поисковые системы подвергают анализу только страницы с высоким рейтингом. Такой подход является неправильным, поскольку по некоторым запросам пользователю могут быть представлены результаты, в которых даже на первых позициях не будет сайтов с высоким рейтингом.

Введем понятие "черного списка", куда будут попадать страницы, подозреваемые в применении маскировки. Тогда после очередной смены IP-адреса, когда злоумышленник еще не может отличить поискового робота от обычного пользователя, поисковая система будет проверять только те страницы, которые находятся в данный момент в этом списке. Заносить в список следует те страницы, рейтинг для которых будет значительно меняться при очередных переиндексациях и сменах IP-адреса поисковых роботов, т.к. это является поводом подозревать их в применении маскировки. Такой подход сужает область тестируемых сайтов. При этом увеличивается вероятность обнаружения сайтов, применяющих маскировку, и сокращается количество бесполезных проверок. Следовательно, увеличивается эффективность защиты без увеличения ресурсов поисковой системы.

Результат использования предложенного метода для обнаружения применения маскировки позволит повысить эффективность борьбы с искусственным повышением рейтинга. В результате сокращается количество подложных сайтов, направленных на компрометацию конфиденциальных данных пользователей, что способствует повышению безопасности работы в сети Интернет.

Корт С.С., Фарберов М.Ю.

ПРИМЕНЕНИЕ АППАРАТА ЦЕПЕЙ МАРКОВА ДЛЯ ОБНАРУЖЕНИЯ АНОМАЛИЙ В АКТИВНОСТИ ПО

г.Санкт-Петербург, ГОУ «СПбГПУ»

В докладе рассмотрена методика классификации активности ПО на основании модели нормального поведения в виде цепи Маркова.

В качестве событий, происходящих в процессе выполнения приложения, выбраны обращения к системным вызовам. Таким образом, активность приложения представляется последовательностью системных вызовов, сгенерированных процессом. Введение операций позволяет сгруппировать системные вызовы по их функциональному назначению. При построении цепи Маркова не учитываются значения параметров операций. В противном случае, учет значений параметров приведет к значительному увеличению мощности множества состояний. В результате, состояния цепи будут статистически однородны – распределение вероятностей стремится к равномерному с увеличением числа экспериментов, что не позволяет производить классификацию активности приложения, т.к. невозможно выделить наиболее и наименее вероятные переходы.

Основными предпосылками обнаружения аномалий является регулярность последовательностей операций, соответствующих нормальному поведению, и отличающихся от аномального поведения. Чем выше регулярность распределения, тем больше явных закономерностей в нормальном поведении, что облегчает построение модели нормального поведения. Следовательно, чем больше характеристика регулярности распределения, тем выше качество получаемого классификатора. Следовательно, методика выбора оптимального размера окна заключается в поиске модели с наибольшей регулярностью распределения. Для того необходимо перебирать различные значения размера окна, перестраивать цепь Маркова для обновленного окна, оценивать регулярность полученного распределения. Для оценки регулярности предлагается использовать теоретическую меру условной энтропии.

Цепь Маркова строится в процессе обучения. Для предотвращения переобучения используются автоматический выход из режима обучения при отсутствии изменений в конфигурации цепи Маркова в течение некоторого времени. Входными данными для построения классификатора активности является построенная цепь Маркова. Классификатор строится на основе расчета условной вероятности для каждой анализируемой последовательности операций. Активность признается аномальной, если значение вероятности становится ниже определенного граничного значения.

Однако анализ активности реальных приложений показывает, что появление перехода с низкой вероятностью не всегда является следствием аномального поведения, а происходит по причине низкой частоты реализации перехода от общего количества переходов в последовательностях, входящих в обучающее множество. Причем такие переходы являются частью нормального поведения и не должны приводить к срабатыванию классификатора. Данная проблема потребовала ряд модификаций алгоритма классификации, основанного на цепи Маркова, которые и рассмотрены в данном докладе.

Таким образом, представленные исследования показали невозможность реализации алгоритма классификации без применения ряда описанных модификаций. Проведены оценки оптимальных значений параметров классификатора. Качество классификатора зависит от полноты и качества процесса обучения. Важно не допустить воздействия нарушителя на контролируемое приложения в процессе обучения. Корректность классификации зависит от граничного значения срабатывания, являющегося экспертной оценкой.

Кулишов Ф.Ю.

ОПТИМАЛЬНЫЕ АЛГОРИТМЫ АНТИВИРУСНОГО ПОИСКА ДЛЯ СОВРЕМЕННЫХ SIMD-ПРОЦЕССОРОВ

г.Москва, Московский Инженерно-Физический Институт (Национальный исследовательский ядерный университет)

В связи с бурным развитием Интернета и ростом его значимости как бизнес-инструмента все выше становится цена простоев IT-инфраструктуры, многие из которых вызываются вредоносным программным обеспечением. Дополнительную проблему представляют растущие скорости передачи данных по сетям. Для решения этой проблемы применяются в основном узкоспециализированные ASIC-решения и алгоритмы для них.

В последние годы наблюдается рост количества SIMD-процессоров общего назначения, способные эффективно выполнять типовые вычислительные задачи. Однако типовые алгоритмы сигнатурного поиска в основном не ориентируются на SIMD, в том числе на перспективные процессоры Cell Broadband Engine разработки IBM, Sony и Toshiba, и графические процессоры (GPU) компании Nvidia.

Данная работа представляет реализацию алгоритмов поиска регулярных выражений (РВ), являющихся основой производительного сетевого поиска, для процессора Cell BE. Рассматриваются недетерминированные конечные автоматы (НКА), их оптимальная реализация на Cell BE, а также SIMD-оптимизация алгоритма выполнения НКА.

Быстродействие НКА-алгоритма поиска простых регулярных выражений показывает 1.3 Гбит/сек на ядро при обработке до 512 состояний, а также допускает увеличение состояний до 7000 за счет быстродействия. Поддержка полного функционала регулярных выражений на НКА будет вестись на скорости 0.25 Гбит/сек на ядро для 512 состояний автомата. Предполагается, что обнаружение потенциально опасных вредоносных фрагментов в потоке трафика будет вестись при помощи НКА для простых выражений, а их дальнейшая обработка будет производиться на НКА с полной поддержкой РВ.

Существенные отличия от имеющихся аналогов следующие. Во-первых, в открытых источниках не было упоминаний о реализации алгоритмов поиска регулярных выражений на Cell BE. Во-вторых, по сравнению с алгоритмом Ахо-Корасик для поиска фиксированных строк, также реализованным на Cell и использующем ДКА, у представляемого включена поддержка поиска регулярных выражений, что заметно расширяет поисковые возможности представленного решения. Кроме того, описываемая реализация НКА работает с полным 256-символьным ASCII-алфавитом, в отличие от искусственно вводимого 32-символьного для упомянутой версии Ахо-Корасик, и не требует отдельного устройства — преобразователя сессий, изменяющего входной поток данных для удобства анализа.

Ломако А.Г., Еремеев М.А., Новиков В.А., Платонов А.А.

МЕТОД КОНТРОЛЯ ПРОГРАММ НА ОТСУТСТВИЕ НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ

г. Санкт-Петербург, Военно-космическая академия имени А.Ф. Можайского

В условиях широкого применения и использования в защищённых информационных системах импортных сетевых операционных систем, микрокода в аппаратной части средств защиты информации и общего программного обеспечения, стало недостаточным решение вопроса защиты от несанкционированного доступа без решения вопроса защиты от воздействий на информацию с целью ее уничтожения, искажения и блокирования. Спецификой сертификации импортного ПО является отсутствие исходных текстов. Наличие недекларированных возможностей (НДВ) в таком ПО порождает уязвимости, от которых зависит надежность и устойчивость функционирования систем в целом.

При поиске НДВ ПО испытательными лабораториями применяются следующие группы методов:

1) эвристические методы, основанные на ручном просмотре дампа памяти с применением эмпирически полученных знаний об особенностях реализации НДВ в ПО;

2) методы сравнения с эталоном;

3) методы с формальным решателем, основанные на контроле правильности выполнения синтаксических правил, контроле правдоподобия и методах верификации.

Анализ применяемых групп методов показал, что они являются либо очень длительными и не подходят для планово-периодического контроля ПО или обладают низкой полнотой вскрытия НДВ по при отсутствии исходных текстов ПО.

Предлагаемый в докладе подход основывается на утверждении, что любую программу можно описать с помощью системы состоящей из: денотационной (*st*), логической (*l*) и операционной (*d*) модели программ. В этом случае метод поиска НДВ программ при отсутствии их исходных текстов, основан на обнаруженных *stld* признаках недекларированных функций программ.

Содержание метода заключается в следующем. Программа дизассемблируется. Полученный листинг сканируется преобразователем, который преобразует код подпрограмм в вектора $\langle St, L, D \rangle$. Вектор поступает на вход решателя, который сначала пропускает его через распознаватель, состоящий из конечных автоматов Ω_{St}, Ω_L, Ω_D и получает выходной вектор $R = \langle R(\Omega_{St}), R(\Omega_L), R(\Omega_D) \rangle$. По значению выходного вектора определяется класс, к которому относится подпрограмма.

Время работы распознавателя, для среднестатистического файла размером 1,5 Мб, составляет примерно 2 часа, что на три порядка меньше чем при ручном анализе листинга программ. Результативность метода по полноте вскрытия, сопоставима с ручными методами.

Политов М.С., Мельников А.В.

АЛЬТЕРНАТИВНЫЙ ПОДХОД К ОЦЕНКЕ УРОВНЯ ЗАЩИЩЁННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

г.Челябинск, ГОУ ВПО «ЧелГУ»

На сегодняшний день общепринятым в отечественной и международной практике подходом к оценке уровня защищённости является проведение сертификационных испытаний (в основе которых лежат верификационный и экспертный методы оценки) систем на соответствие требованиям по защищенности. Вместе с тем, присущие этому подходу недостатки, в частности, значительные материальные и временные затраты на проведение испытаний, субъективность самой оценки и испытаний, привели к тому, что появилась необходимость в создании принципиально новой оценки, в основу которой положены объективные данные.

Суть предлагаемой оценки заключается в следующем:

1. Жизненный путь ИС оценивается в количестве выпущенных производителем версий и модификаций;
2. Виды и типы уязвимостей классифицируются следующим образом: Low, Midle, High;
3. Уровень защищённости информационной системы определяется, как отношение уязвимостей определённого класса к общему количеству версий.

Как известно, смена основных номеров версий программного продукта связана с существенными изменениями кода и функциональными преобразованиями. В пределах этих версий идёт доработка уже заложенного функционала и исправление ошибок.

Для прогнозирования числа уязвимостей в будущих версиях ИС предлагается использование модели временных рядов.

В процессе изменения количества уязвимостей предполагаются следующие зависимости от этапов развития самой ИС:

1. Между основными (major) версиями не происходит добавления нового функционала, но производится доработка запланированной функциональности и исправление обнаруженных недостатков;
2. Пик уязвимости приходится на выход новой основной версии, в силу добавления нового функционального кода;
3. В пределах основных версий прослеживается единая тенденция к снижению общего количества уязвимостей;

ЛИТЕРАТУРА

1. Двухуровневая оценка защищённости информационных систем / Политов М.С., Мельников А.В. / Вестник УГАТУ: Научный журнал Уфимского государственного авиационно-технического университета / серия «Управление, вычислительная техника и информатика», 2008. Т. 10 № 2 (27). С. 210 – 214.
2. Полаженко С. Оценка характеристик безопасности в рамках процесса оценки качества программных средств в соответствии с международными стандартами ISO/IEC.
3. ГОСТ/ИСО МЭК 15408-2002. Общие критерии оценки безопасности информационных технологий.

Проценко Л.Л.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ПРОТИВОДЕЙСТВИЯ ВРЕДОНОСНЫМ ПРОГРАММАМ И ИХ ДЕЯТЕЛЬНОСТИ

г.Москва, МИФИ

Задача проекта заключается в автоматизированном поиске вредоносного программного обеспечения и источников его распространения в сети Интернет. А так же в противодействии основным массовым атакам совершаемыми этими программами.

Идея, представленная в данном проекте, является ранее не реализованной. В распоряжение автора отсутствует информация о том, что аналогичные разработки, были созданы ранее на территории России или других стран.

Этот проект является логическим продолжением проектов: «Автоматизированный поиск вредоносного программного обеспечения и источников его распространения в сети Интернет» и «Новые технологии обнаружения вредоносных программ», которые получили ряд наград на различных конференциях международного и всероссийского уровня. Имеются 8 публикаций, которые сопровождают эти проекты. Кроме этого для каждого проекта были получены свидетельства Роспатента: Поисковая машина сетевых адресов самоустанавливающихся программ. - Свидетельство РОСПАТЕНТа № 2006611875, зарегистрировано 31 мая 2006 и Anti-Malware Scanner. - Свидетельство РОСПАТЕНТа № 2008610872, зарегистрировано 20 февраля 2008.

Противодействие DDoS и спаму является основным направлением исследования в данном проекте, так как эти угрозы являются самыми динамично развивающимися атаками и наносящие наибольший урон своим жертвам.

Для эффективного противодействия этим атакам необходим целый комплекс мер. Одна из таких мер это наиболее быстра реакция на новые версии вредоносных программ. В настоящее время становится все более очевидным, что одна антивирусная программа не в состоянии реагировать так быстро как необходимо. Только объединив усилия всех антивирусных решений, позволило бы ускорить эту реакцию

Но установить на один компьютер все антивирусы не возможно из-за возникающих конфликтов между ними и к тому, же является экономически не эффективным решением. Поэтому проверка должна проходить удаленно. Но и простой удаленной проверки мало. Необходим целый комплекс мер, который и представлен в данном проекте. Далее в тезисной форме представлены основные компоненты автоматизированной системы противодействия вредоносным программам и их деятельности.

Головной сервер – обеспечивает взаимодействие с локальными серверами. Обеспечивает управление распределенной системой.

Локальный рабочий сервер – работает в связке с головным сервером и/или локальным сервером для клиента. Работает в режиме спайдера и/или обеспечивает рабочий функционал системы (проверка файлов, формирование отчета, сравнительный анализ, пересылка потенциально вредоносных программ в антивирусную лаб. и т.д.).

Локальный сервер для клиента – обеспечивает взаимодействие с клиентами.

Клиент – защита клиентской машины и сбор необходимой информации.

Спайдер системы – умное сканирование адресов распространения вредоносных программ.

Веб сервис – сканирование файлов, статистика, функционал для работы независимых экспертов, доступ к отчетам экспертов и/или антивирусной лаборатории.

Андрей Тихонов, Вартан Падарян

ПРИМЕНЕНИЕ ПРОГРАММНОГО СЛАЙСИНГА ДЛЯ АНАЛИЗА БИНАРНОГО КОДА, ПРЕДСТАВЛЕННОГО ТРАССАМИ ВЫПОЛНЕНИЯ

г. Москва, Институт системного программирования РАН

Доклад посвящен технике извлечения анализируемого алгоритма на основе анализа низкоуровневых трасс, полученных при трассировке работы процессора.

Рассматривается задача выделения из трассы реализации алгоритма, которая будет работоспособна на максимально широком множестве входных данных. Предполагается, что доступен только бинарный код программы, и он защищен от анализа.

Применение разработчиком средств защиты кода и невозможность в общем случае получить полное множество инструкций и связей между ними по управлению и по данным делает применение статического анализа кода недостаточным, вследствие чего аналитик вынужден обратиться к средствам динамического анализа. Основными средствами динамического анализа кода являются отладчик и трассировщик, но применение средств защиты и большие объемы исследуемого кода настолько увеличивает время, требуемое для «ручного» анализа в отладчике, что единственной приемлемой возможностью становится автоматизированный анализ трасс.

В работе рассмотрены существующие методы слайсинга, используемые в рамках статического анализа, описаны новые методы слайсинга, разработанные в рамках работы над системой динамического анализа по трассе исполнения программы TrEx.

Разрабатываемая в Институте системного программирования РАН система TrEx позволяет значительно автоматизировать действия аналитика. В частности, решается задача автоматического выделения кода, относящегося к искомому алгоритму, при известных входных или выходных данных этого алгоритма.

Достаточно близкая задача решается путем динамического слайсинга программ, являющегося одним из методов статического анализа. Поскольку используемые в системе TrEx трассы эквиваленты понятию траектория, данному в работе Корела и Ласки, формальные определения как обратного, так и прямого слайса трассы строятся как адаптация *KL*-слайса, когда собственно программа определяется как производное от рассматриваемой траектории.

Восстанавливаемый по трассе CFG будет неполным, так как будет содержать не весь поток управления программы, а только ту его часть, которая реализовалась в конкретной трассе. Именно это является ограничением, не позволяющим в общем случае получить по трассе слайс эквивалентный динамическому слайсу программы. Однако построение зависимостей для выполнения слайсинга ограничивается лишь потоком данных, что далеко не всегда является достаточным для аналитика, поскольку будет приводить к удалению из слайса инструкций, которые на самом деле оказывают влияние на набор переменных из критерия.

Восстановленный CFG потенциально отличается от CFG исходной программы отсутствием блоков (и соответствующих переходов) для невыполнявшихся ветвей и наличием «склеенных» блоков. Тем не менее, в рамках заданной трассы «склеенные» блоки обладают всеми свойствами базовых блоков – передача управления в трассе осуществляется только на начало некоторого базового блока.

Шоров А.В., Коновалов А.М., Котенко И.В.

ИССЛЕДОВАТЕЛЬСКОЕ МОДЕЛИРОВАНИЕ БОТ-СЕТЕЙ И МЕХАНИЗМОВ ЗАЩИТЫ ОТ НИХ

г. Санкт-Петербург, СПИИРАН

Защита от различного рода атак с использованием бот-сетей сегодня является актуальной проблемой. Область применения бот-сетей довольно обширна, это рассылка спама, организация DDoS-атак, использование зараженных компьютеров для анонимного доступа в сеть, фишинг, удаленный перебор паролей и т.д. Для обеспечения противодействия бот-сетям необходимо исследовать методы их построения и функционирования, механизмы реализации атак с помощью бот-сетей, а также методы защиты от этих атак, в том числе методы обнаружения ботов, мониторига их действий (для расследования преступлений) и уничтожения.

Одной из метафор, представляющейся перспективной для построения новых средств защиты, является метафора, основанная на применении биологического подхода. В работе, в частности, исследуется механизм защиты от инфраструктурных атак бот-сетей на основе подхода, называемого "нервной системой сети". Данный подход предполагает создание интеллектуальной системы защиты, как распределенного механизма сбора и обработки информации, который координирует действия различных сетевых устройств, идентифицирует атаки и принимает меры для их отражения. Структура системы строится по аналогии со структурой нервной системы человека. В каждой подсети выделяется специальный компонент, который, с точки зрения биологического подхода, играет роль "сомы" в нейроне (сома является центральной частью нейрона). Этот компонент реализует большую часть процессов обработки и анализа информации, а также координацию действий близлежащих сетевых устройств. Функцию "дендритов" нейрона выполняют другие сетевые устройства (например маршрутизаторы), они передают большую часть информации о состоянии сети соме. Сомы связаны между собой с помощью виртуальной частной сети (VPN), которая выполняет роль "аксона" и передает обработанную информацию о состоянии данного сегмента сети (нейрона) другим сомам, находящимся в удаленных сегментах сетей, а также получает информацию о состоянии других нейронов (сетей).

Для оценивания предложенных подходов с помощью системы имитационного моделирования OMNeT++ с библиотекой классов INET Framework создаются прототипы моделей механизмов атаки и моделей механизмов защиты. В частности ведется создание моделей бот-сетей и моделей атак на основе реальных бот-сетей, в том числе с помощью анализа лог-файлов полученных с серверов, которые подвергались атакам такого рода. В соответствии с имеющимися данными определяется сценарий взаимодействия сетевых приложений (ботов) и определяются параметры соединений. Трафик, производимый бот-сетью, моделируется на пакетном уровне. Модели сетевых устройств реализуют создание, прием и маршрутизацию пакетов между узлами сети.

На основе полученных результатов проводится оценивание методов защиты от атак, проводимых с помощью бот-сетей, и определяется эффективность использованных методов противодействия атакам.

Работа выполняется при финансовой поддержке РФФИ (проект №07-01-00547), программы фундаментальных исследований ОНИТ РАН и при частичной финансовой поддержке, осуществляемой в рамках проекта Евросоюза RE-TRUST.

Явно Д.М., Югай В.В.

ОСОБЕННОСТИ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ МОБИЛЬНЫХ ОПЕРАЦИОННЫХ СИСТЕМ

г.Санкт-Петербург, ГОУ «СПбГПУ», ЗАО «НПП «СТЗИ»

В последнее время сфера применения мобильных устройств значительно расширилась. Широкое распространение получили мобильные устройства, имеющие большое количество дополнительных функций – навигация, интернет-обозреватель, электронная почта, редактирование и пересылка документов, хранение данных. Такое устройство, с одной стороны, удобно в использовании, а с другой, хранит большое количество ценной информации, чувствительной к утрате или хищению.

Одновременно с увеличением функциональности самих устройств выросли и возможности их доступа в сеть Интернет. На данный момент подавляющее большинство многофункциональных мобильных устройств периодически подключаются к всемирной сети.

Таким образом, подобное мобильное устройство становится ценным объектом для атаки злоумышленника, желающего получить личную информацию о владельце или нанести ему ущерб.

Многие мобильные операционные системы (ОС) обладают встроенными средствами защиты. Но эти средства не обеспечивают полной безопасности, а установка дополнительных защитных продуктов затруднена из-за ограниченности ресурсов.

Вредоносное программное обеспечение (ПО) для таких систем может очень сильно различаться в зависимости от того, как именно происходит заражение жертвы.

В докладе рассматриваются актуальные угрозы для трех лидирующих на рынке мобильных ОС: Microsoft Windows Mobile, Symbian OS и iPhone OS.

В результате анализа Symbian OS было выявлено, что данная система уязвима к двум типам угроз – эксплуатация уязвимостей встроенных приложений и создание корректно подписанных вредоносных файлов. Эксплуатация уязвимостей встроенных приложений позволяет выполнять действия с правами этих приложений, которые являются достаточно широкими для совершения практически любых вредоносных действий. Для реализации второго вида угроз можно использовать получение сертификата Publisher ID на несуществующее юридическое лицо. Такая возможность существует благодаря небрежности при проверке подлинности документов, предоставленных для сертифицирования.

Анализ Microsoft Windows Mobile показал, что система очень похожа на версию для персональных компьютеров. К отличиям можно отнести тот факт, что любая программа работает от имени администратора. Данное свойство только расширяет возможности злоумышленника. Для Windows Mobile возможно большинство атак, осуществимых для версии для персональных компьютеров.

Анализ iPhone OS показал, что создать для этой системы вирусную программу практически невозможно: все программы, устанавливаемые на устройства, загружаются с ресурса AppStore и перед этим проходят проверку специалистами Apple. Однако у этой системы существует другой недостаток: в целях удобства пользователя любой медиа-файл, загружаемый с помощью интернет-обозревателя, сразу же начинает открываться соответствующей ему программой. Это приводит к тому, что практически любая уязвимость может быть эксплуатирована «снаружи» – пользователю достаточно перейти по вредоносной ссылке.

Таким образом, только для ОС Windows Mobile может быть использовано вредоностное ПО, заражающее исполняемые файлы. Для ОС Symbian и iPhone OS наибольшие возможности злоумыщленнику предоставляет эксплуатация уязвимостей, что связано с применением сертификатов в случае Symbian OS и с проверкой всех приложений специалистами в случае iPhone OS.

В результате основной особенностью вредоносного ПО для мобильных ОС является ориентированность на использование уязвимостей. Большинство владельцев мобильных устройств пользуются ПО из небольшого набора, что с учетом недостаточной надежности такого ПО позволяет злоумышленникам находить уязвимости чаще и наносить больший ущерб, нежели в случае ОС для персональных компьютеров.

РАЗДЕЛ 5.
ПРОБЛЕМЫ ПОДГОТОВКИ КАДРОВ

Архангельская А.В.[1], Запечников С.В.[2]

РАСШИРЕННАЯ ПРОГРАММА КРИПТОЛОГИЧЕСКОГО ОБРАЗОВАНИЯ ДЛЯ СТУДЕНТОВ СТАРШИХ КУРСОВ И АСПИРАНТОВ

г.Москва, [1]ЗАО «Голлард», [2]Московский инженерно-физический институт (государственный университет)

В связи с постоянным расширением круга практических задач в области информационной безопасности, решаемых с привлечением средств криптографической защиты информации (СКЗИ), наблюдается серьезная проблема в преподавании криптологии на старших курсах. Она заключается в наличии существенного разрыва между сильной и глубокой теоретической подготовкой и слабой привязкой методов криптологии к их техническому воплощению в современных сложных компьютерных системах.

Практически любой вузовский курс «Криптографические методы защиты информации» предполагает изучение основного «инструментария» современной криптографии: блочных и поточных шифров, алгоритмов открытого шифрования и цифровой подписи, псевдослучайных генераторов, методов распределения ключей и т.д. Однако студенты и даже дипломированные специалисты, сталкиваясь в своей практической деятельности с настройкой и системной интеграцией средств защиты информации, с большим трудом осознают, что в них применяются те же самые методы и механизмы защиты, которые они уже «проходили» в вузе.

Таким образом, в учебном плане необходима дисциплина, которая послужила бы связующим звеном между теоретическими основами криптографии и практической деятельностью по интеграции уже готовых решений или разработке новых СКЗИ. В МИФИ она получила название *«Криптографические протоколы и стандарты»* и читается авторами настоящего доклада для студентов факультета «Информационная безопасность» с 2005/06 учебного года. В рамках этого курса студентам представляется систематизированный подход к проблемам синтеза и оценки стойкости сложных криптосистем, освещаются актуальные вопросы современной криптографии, такие как конструирование важнейших криптографических протоколов и анализ их свойств, стандартизация используемых в них примитивов, их корректное и эффективное практическое применение, проблемы устранения уязвимостей и верификации стойкости СКЗИ, а также нормативно-технологические аспекты разработки и применения аппаратных и программных СКЗИ. Курс лекций и практических занятий построен как своеобразный «экскурс» по дороге, ведущей от осознания основополагающих идей криптографии до их реализации в качественных и надёжных СКЗИ. Одна из важнейших идей курса заключается в том, что стойкость СКЗИ отнюдь не тождественна криптографической стойкости используемых в них примитивов и протоколов.

Для закрепления лекционного материала студентам предлагается ряд заданий для самостоятельной работы.

1. *Формализованное описание криптографических конструкций.* Предлагается перевести и изучить одну из статей с описанием новых криптографических конструкций (протоколов, криптосхем), взятую из источников в сети Интернет, указанных преподавателем. Конструкцию необходимо задокументировать в соответствии с выдаваемыми преподавателем формами документов.

2. *Жизненный цикл СКЗИ*. Предлагается изобразить в виде блок-схемы этапы жизненного цикла СКЗИ, учитывая всевозможные связи между ними и особенности СКЗИ. Особое внимание рекомендуется обратить на наличие секретных параметров – ключей, и возникающие вследствие этого задачи, связанные с их генерацией, распространением,

использованием, компрометацией, архивированием и уничтожением.

3. *Процесс разработки, производства, реализации и эксплуатации СКЗИ*. Предлагается изобразить в виде блок-схемы один из указанных процессов с указанием функций всех сторон, в них вовлекаемых, и ссылок на нормативные и иные документы, которыми необходимо руководствоваться на каждом этапе.

После изучения дисциплины «Криптографические протоколы и стандарты» у студентов формируются целостные профессионально-поведенческие модели. Таким образом, курс занимает важное место в общей системе профильной подготовки выпускника, связывая общенаучные и общеобразовательные дисциплины с профильными для будущего специалиста курсами.

Однако в современной образовательной среде помимо обучения студентов, получающих квалификацию «специалист по защите информации» (которая, по всей видимости, будет сохранена и с переходом основной массы учащихся на двухуровневые образовательные стандарты «бакалавр – магистр»), серьезно встает вопрос о продолжении образования за рамками вузовских учебных дисциплин. Для этой цели в 2008 году при участии авторов доклада впервые разработано содержание программы послевузовского образования аспирантов МИФИ по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность». Программа утверждена Учёным советом университета и планируется к реализации в объеме 93 часов для аспирантов первого года обучения. Основная часть программы построена по проблемно-ориентированному принципу. Один из разделов носит название *«Алгоритмические методы защиты информации в компьютерных системах. Актуальные проблемы криптографии и смежных дисциплин»* (18 часов). В него вошли следующие отдельные темы.

1. *Проблемные вопросы теории сложности вычислений.* Поиск вычислительно сложных задач. Проблема существования однонаправленных функций (ОНФ). Проблемы качества и критериев качества ОНФ. Возможности выхода в будущем за пределы полиномиальной модели вычислителя. Квантовая криптография.

2. *Проблемы теории кодирования и их связь с проблемами криптографии.* Проблемы эффективности кодирования и разработки кодов со специальными функциями. «Операции под шифром» и определение граничных условий их осуществимости.

3. *Проблемы поиска эффективного математического аппарата криптосистем.* Систематика вычислительно сложных задач, используемых для защиты информации. Поиск алгебраических структур, эффективно реализующих ОНФ на базе вычислительно сложных задач. Отображения между алгебраическими структурами.

4. *Проблемы доказательства стойкости криптографических конструкций.* Проблемы развития формальных и полуформальных методов анализа. Проблемы алгоритмизации и автоматизации анализа и доказательства стойкости. Создание библиотеки криптографических конструкций с доказанными оценками стойкости.

5. *Проблемы обеспечения живучести и стойкости криптосистем в условиях разрушения.* Безопасные многосторонние вычисления. Проблема универсальной компонуемости (universal composability) протоколов в сложных средах с непредсказуемыми воздействиями. Проблема стойкости к разрушению ключевой системы.

6. *Проблемы стеганографии и ее приложений.* Математические модели стегосистем и перспективы их реализации. Обеспечение анонимности, отказуемости (deniability). Перспективы решения прикладных задач.

Программа преследует цели расширения кругозора и научной компетентности будущих исследователей, содействия в выборе ими тем диссертационных работ.

Баяндин Н.И.

ПОДГОТОВКА АНАЛИТИКОВ ДЛЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

г.Москва, Московский государственный университет экономики, статистики и информатики (МЭСИ)

По данным компании Gartner Group, проблема обеспечения информационной безопасности становится одной из приоритетных проблем развития информационного общества. Важным инструментом обеспечения эффективного развития систем информационной безопасности становятся новые информационные технологии. Можно отметить, что в настоящее время наблюдается бурный рост технологий автоматического анализа данных. Это связано, главным образом, с новой областью компьютерных наук, обозначаемой как KDD (knowledge discovery in databases – обнаружение знаний в базах данных). Элементы автоматической обработки и анализа данных становятся неотъемлемой частью технологий получивших название data mining (извлечение знаний). Аналитические системы на базе этих технологий могут быть использованы для решения задач на основе анализа исторических данных, описывающих поведение изучаемого объекта, принятые в прошлом решения, их результаты и т.д. Эти решения могут включать, например, результаты аудита информационной безопасности предприятия, статистику инцидентов в компьютерных сетях, данные по компьютерным вирусам, статистику по «социальной инженерии» и др. Технологии извлечения и анализа информации, содержащейся в источниках различной природы, получили широкое распространение при создании единого безопасного информационного пространства организации. Предлагаемые технологии должны обеспечивать доступ к данным, как в структурированном, так и неструктурированном виде, давая возможность пользователю «раскрыть знания» из полученной информации. Аналитические системы, реализующие технологии data mining, обеспечивают поиск и классификацию любых данных (текст, изображение, видео, аудио) вне зависимости от способа и места их хранения, производят анализ и выделение информации с использованием семантических сетей и классификаторов, настроенных на предметную область пользователей.

Представляет практический интерес для задач информационной безопасности система мониторинга электронной почты, разработанная на основе технологий data mining. Эта система обеспечивает постоянный автоматический анализ содержания почтовых сообщений и вложений и немедленную их маршрутизацию в почтовый ящик администратора информационной безопасности, тем самым решая задачу фильтрации конфиденциальной исходящей информации или фильтрацию входящего спама.

Для подготовки специалистов, способных реализовывать эти технологии, необходимо введение в учебный план ряд новых дисциплин, таких как методы аналитической работы, введение в data mining, основы «социальной инженерии», информационные ресурсы, методы поиска информации и др.

Приводится фрагмент проекта учебного плана (вузовский компонент).

Приводятся проекты некоторых программ и обсуждаются вопросы создания лабораторного макета.

Жигулин Н.Н.

ПРИМЕНЕНИЕ ИДЕЙ ШЕННОНА ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ УЧЕБНОГО ПРОЦЕССА.

г.Москва, ИКСИ Академии ФСБ РФ

За последние полстолетия в вузах нашей страны сильно изменился характер и результаты учебного процесса по математическим дисциплинам. Одновременно с понижением уровня образования выпускников средней школы шел процесс усложнения и формализации языка преподавания в вузах. Вместо прежних единичных случаев теперь пересдачи экзаменов происходят фактически на дополнительных сессиях.

Часто происходит так, что современному студенту трудно овладеть специальным языком за короткое время. Тогда достаточно распространенный тип лекции можно представить в следующем виде. Преподаватель рассылает сообщение студентам. Сообщение большого объема состоит из кусков текста русского языка и кусков кодированного текста (сжатого формализованного текста с новыми понятиями). Студенты практически синхронно должны не только принимать сообщения, но и, непрерывно пополняя большую кодовую книгу часто с рассыпанными листами, должны осмысливать поступающую информацию. Неизвестные кодовые величины (неусвоенные понятия и их сочетания) воспринимаются, как «шум», который закрывает информацию.

Из основных идей К. Шеннона следует, что с криптографической точки зрения секретная система почти тождественна системе связи при наличии шума, что своевременность прочтения сообщения зависит от баланса между стойкостью системы закрытия связи и выделенным для прочтения сообщения временем, и, что в основе криптоанализа лежит избыточность в открытых текстах.

Следовательно, сочетание излишне формализованного и обширного учебного материала с одновременным дефицитом времени на его усвоение создает эффект применения системы закрытия информации. Это система временной стойкости, но она обеспечивает несвоевременность прочтения многих сообщений и торможение усвоения учебного материала.

Преодоление эффекта информационного противодействия возможно только при выполнении рекомендаций, направленных на уменьшение стойкости системы закрытия информации и увеличение времени на декодирование. По Шеннону, уменьшение стойкости достигается сокращением объема информации и числа необходимых новых понятий (это в совокупности дает резкое сокращение объема кодовой книги) при одновременном повышении избыточности применяемого языка обучения.

Эти рекомендации означают, например, такие педагогические установки. Язык преподавания сделать живым, неформальным. Объяснять не только «что», но и побольше «как» и «для чего». Именно: постановка задачи, выводы, связи между понятиями, теоремами, подробные ссылки, многочисленные примеры; выделение центральных тем, остальные менее подробно.

Актуальны столетней давности мысли нашего великого соотечественника Д.И. Менделеева, что при чрезмерном количестве знаний, сообщаемых человеку, он не будет успевать их осмыслить (получается вроде очага, заваленного топливом настолько, что огонь в нем не может разгореться). В своем знаменитом на весь мир учебнике «Основы химии» он заявляет, что главным предметом сочинения служат философские начала нашей науки, относящиеся к ее основным качественным и количественным сведениям.

Малыш В.Н.

О СПЕЦИАЛИЗАЦИЯХ СПЕЦИАЛЬНОСТИ 075300 – ОРГАНИЗАЦИЯ И ТЕХНОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ

г. Липецк, Государственный педагогический университет

Учебный план специальности 075300 – Организация и технология защиты информации в ГОУ ВПО "Липецкий государственный педагогический университет" содержит две специализации:

Проектная деятельность при организации защиты информации (на предприятии). Состав дисциплин:

- История и современная система защиты информации в России.
- Системы защиты информации в ведущих зарубежных странах.
- Организация и управление службой защиты информации.
- Основы теории электрических цепей.
- Аппаратные средства вычислительной техники и компьютерных сетей.
- Системы связи и каналы передачи данных.
- Теория информации и кодирования
- Информационная безопасность телекоммуникационных систем.
- Принципы функционирования и проектирования защищенных компьютерных сетей на предприятии.
- Принципы функционирования и проектирования систем антивирусной защиты.
- Аудит систем защиты информации на предприятии и консалтинг.
- Защита речевой информации.

Обеспечение безопасности объектов информатизации. Содержит следующие дисциплины:

- История и современная система защиты информации в России.
- Системы защиты информации в ведущих зарубежных странах.
- Организация и управление службой защиты информации.
- Основы электротехники.
- Основы теории электрических цепей.
- Квантовая и оптическая электроника.
- Основы телевидения и видеотехники.
- Системы контроля и управления доступом.
- Системы охранно-пожарной сигнализации.
- Системы видеоохраны и видеонаблюдения.
- Антенно-фидерные устройства и распространение радиоволн.
- Электромагнитная совместимость и информационная безопасность объектов информатизации.

Общий объем каждой из специализаций составляет 970 часов. Изучение дисциплин специализаций начинается на 3 курсе. В 8 семестре предусмотрено выполнение курсовой работы по дисциплинам специализаций.

Ростовцев А.Г

НОВЫЕ РАЗДЕЛЫ МАТЕМАТИКИ В РАМКАХ РЕГИОНАЛЬНОГО КОМПОНЕНТА ДЛЯ СПЕЦИАЛЬНОСТИ «КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ»

г.Санкт-Петербург, ГОУ «СПбГПУ»

Для того чтобы программный продукт был конкурентоспособен на мировом рынке, он должен обладать новым полезным качеством. Как правило, это означает, что программы должны работать быстрее существующих аналогов.

Применительно к рынку программных средств криптографической защиты информации увеличение скорости и получение нового качества возможно лишь за счет применения новых математических методов. Так, скорость формирования и проверки подписи можно увеличить в разы по сравнению с аналогами, если использовать систему счисления с целым алгебраическим основанием, например, $\sqrt[4]{\pm 2}$. Использование секретных гомоморфизмов алгебраических структур позволяет получить новое качество, например, защититься от копирования или реализовать технику мобильных агентов.

В последние годы появилась возможность патентовать вычислительные и криптографические алгоритмы, называя их способами обработки информации. Однако число российских патентов мало по сравнению с числом американских или европейских патентов. При этом значительная часть российских патентов принадлежит иностранцам. По-видимому, это следствие в том числе и уровня подготовки отечественных специалистов.

В Санкт-Петербурге работает много зарубежных компаний, которые занимаются разработкой систем и средств защиты информации, в том числе, криптографической. Эти компании используют зарубежные криптографические стандарты и несертифицированные алгоритмы. Поэтому при подготовке математиков по специальности «Компьютерная безопасность» СПбГПУ в рамках регионального компонента были введены расширенные учебные курсы математики, ориентированные на развитие у студентов знаний и навыков, необходимых для разработки конкурентоспособных алгоритмов и программ защиты информации.

Курс «Алгебраическая геометрия» изучается в 7-м семестре и используется при изучении криптосистем с открытым ключом и теории итерированных шифров (если линейная алгебра занимается решением систем линейных уравнений над полями, то алгебраическая геометрия занимается решением систем алгебраических уравнений над полями и над кольцами). В рамках этого курса изучаются основные свойства идеалов и алгебраических многообразий, координатное кольцо и поле функций на многообразии, регулярные и бирациональные отображения. Нормальные формы эллиптических кривых. Эллиптические кривые над полем комплексных чисел, эллиптические и модулярные функции, группа классов идеалов мнимых квадратичных порядком и поле классов, модулярная функция j, полиномы Гильберта, Вебера, Аткина–Морана. Эллиптические кривые над числовыми полями. Изоморфизмы, эндоморфизмы, изогении эллиптических кривых. Эллиптические кривые над конечными полями, отображение Фробениуса. Генерация эллиптической кривой для российского и зарубежных стандартов подписи. Дивизоры на алгебраических кривых. Спаривание Вейля. Группа классов дивизоров алгебраической кривой. Гиперэллиптические кривые, якобиан.

В ходе изучения этого курса студенты выполняют два расчетных задания. Первое задание — генерация эллиптической кривой для российского стандарта подписи с числом классов 1500–2000 (такие ограничения содержатся, например, в стандарте подписи Германии). При этом студенты выбирают дискриминант Фробениуса с требуемым числом классов, находят поле классов с использованием полиномов Вебера и генерируют эллиптическую кривую. Второе задание — вычисление спаривания Вейля на эллиптической кривой, которое позволяет строить новые перспективные криптосистемы с открытым ключом, в частности, позволяет вдвое сократить длину подписи по сравнению с действующими стандартами без снижения стойкости.

Курс «Быстрые вычислительные алгоритмы» изучается в 8-м семестре. Студенты изучают алгоритмы арифметики (умножение, деление, алгоритм Евклида в кольце целых и целых алгебраических чисел, полиномов над конечным полем). Алгоритмы разложения полиномов на множители. Алгоритмы решения систем алгебраических уравнений, вычисление базисов Гребнера. Извлечение квадратных и кубических корней в конечных полях. Быстрые вычислительные алгоритмы эллиптических и гиперэллиптических кривых. Алгоритм Чуфа–Элкиса–Аткина для вычисления числа точек кривой. Быстрое вычисление спаривания Вейля и спаривания Тейта. Алгоритмы вычисления группы классов идеалов и поля классов. Алгоритмы арифметики в группе классов мнимого квадратичного порядка и в якобиане гиперэллиптической кривой.

В ходе изучения дисциплины студенты выполняют ряд расчетных заданий.

1. Программная реализация алгоритмов умножения полиномов над полями характеристики 2, 3 в стандартном и нормальном базисе.
2. Разложение на простые множители полинома одной переменной над расширенным конечным полем.
3. Извлечение квадратного корня в конечном поле нечетной характеристики.
5. Быстрая реализация стандарта подписи на эллиптической кривой с использованием бирациональных изоморфизмов и системы счисления с целым алгебраическим основанием.
5. Реализация короткой подписи на эллиптической кривой на спаривании Вейля/Тейта, включая генерацию кривой.

СОДЕРЖАНИЕ