ИНТЕРНЕТ УНИВЕРСИТЕТ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Основы информационной безопасности

Курс лекций

В.А. Галатенко

Интернет-Университет Информационных Технологий
www.intuit.ru
Москва
2003

ИНТЕРНЕТ УНИВЕРСИТЕТ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Основы информационной безопасности

Курс лекций

В.А. Галатенко
Под редакцией члена-корреспондента РАН В.Б. Бетелина

Допущено УМО в области прикладной информатики для студентов высших учебных заведений, обучающихся по специальности 351400 "Прикладная информатика"

Серия "Основы информационных технологий"

Интернет-Университет Информационных Технологий
www.intuit.ru
Москва
2003

ББК 67.401+32.973.2-018.2
Г15
УДК 002:34+004.056.5
Г-151
Г15 Основы информационной безопасности / Галатенко В. А. Под редакцией члена-корреспондента РАН В.Б. Бетелина / М.: ИНТУИТ.РУ "Интернет-Университет Информационных Технологий", 2003. – 280 с.
ISBN 5-9556-0003-5

В курс включены сведения, необходимые всем специалистам в области информационной безопасности (ИБ). Рассматриваются основные понятия ИБ, структура мер в области ИБ, кратко описываются меры законодательного, административного, процедурного и программно-технического уровней.

Допущено УМО в области прикладиой информатики для студентов высших учебных заведений, обучающихся по специальности 351400 "Прикладная информатика".

Библиогр. 29

Издание осуществлено при финансовой и технической поддержке компаний Издательство "Открытые системы", "РМ Телеком", СДМ-Банк и Издательство "ЭКОМ"

Курс лекций по информационным технологиям
Интернет-Университета Информационных Технологий
www.intuit.ru
Руководитель проекта – А.В. Шкред

Основы информационной безопасности

Курс лекций

Серия "Основы информационных технологий"

Формат 60x90 $^{1}/_{16}$. Усл. печ. л. 17,5. Бумага офсетная.
Подписано в печать 25.04.2003. Тираж 3000 экз. Заказ № 6485.

ООО "ИНТУИТ.ру" Интернет-Университет Информационных Технологий, www.intuit.ru, 123056, Москва, Электрический пер., 8, стр. 3.

Отпечатано с готовых диапозитивов в ФГУП "Смоленский полиграфический комбинат", 214020, г. Смоленск, ул. Смольянинова, 1

ISBN 5-9556-0003-5

О проекте

Интернет-Университет Информационных Технологий – это первое в России высшее учебное заведение, которое предоставляет возможность получить дополнительное образование во Всемирной Сети. Web-сайт университета находится по адресу www.intuit.ru.

Мы рады, что вы решили расширить свои знания в области компьютерных технологий. Современный мир – это мир компьютеров и информации. Компьютерная индустрия – самый быстрорастущий сектор экономики, и ее рост будет продолжаться еще долгое время. Во времена жесткой конкуренции от уровня развития информационных технологий, достижений научной мысли и перспективных инженерных решений зависит успех не только отдельных людей и компаний, но и целых стран. Вы выбрали самое подходящее время для изучения компьютерных дисциплин. Профессионалы в области информационных технологий сейчас востребованы везде: в науке, экономике, образовании, медицине и других областях, в государственных и частных компаниях, в России и за рубежом. Анализ данных, прогнозы, организация связи, создание программного обеспечения, построение моделей процессов – вот далеко не полный список областей применения знаний для компьютерных специалистов.

Обучение в университете ведется по собственным учебным планам, разработанным ведущими российскими специалистами на основе международных образовательных стандартов Computer Curricula 2001 Computer Science. Изучать учебные курсы можно самостоятельно по учебникам или на сайте Интернет-университета, задания выполняются только на сайте. Для обучения необходимо зарегистрироваться на сайте университета. Удостоверение об окончании учебного курса или специальности выдается при условии выполнения всех заданий к лекциям и успешной сдачи итогового экзамена.

Книга, которую вы держите в руках, очередная в многотомной серии "Основы информационных технологий", выпускаемой Интернет-Университетом Информационных Технологий. В этой серии будут выпущены учебники по всем базовым областям знаний, связанным с компьютерными дисциплинами.

Добро пожаловать в Интернет-Университет Информационных Технологий!

Анатолий Шкред
anatoli@shkred.ru

Предисловие

Информационная безопасность (ИБ) – сравнительно молодая, быстро развивающаяся область информационных технологий (ИТ), для успешного освоения которой важно с самого начала усвоить современный, согласованный с другими ветвями ИТ базис. Это первая задача курса, для решения которой применяется объектно-ориентированный подход.

Успех в области ИБ может принести только комплексный подход. Описание общей структуры и отдельных уровней такого подхода – вторая задача курса. Для ее решения рассматриваются меры законодательного, административного, процедурного и программно-технического уровней. Приводятся сведения о российском и зарубежном законодательстве в области ИБ, о проблемах, существующих в настоящее время в российском законодательстве. На административном уровне рассматриваются политика и программа безопасности, их типовая структура, меры по выработке и сопровождению. На процедурном уровне описываются нетехнические меры безопасности, связанные с людьми. Формулируются основные принципы, обеспечивающие успех таких мер.

Программно-технический уровень, в соответствии с объектным подходом, трактуется как совокупность сервисов. Дается описание каждого сервиса.

Предполагается, что большинство понятий, введенных в данном курсе, более подробно будет рассмотренно в других, специальных курсах.

Цель курса – заложить методически правильные основы знаний, необходимые будущим специалистам-практикам в области информационной безопасности.

Об авторе

Галатенко Владимир Антонович

Доктор физико-математических наук, заведующий сектором в отделе информационной безопасности НИИ системных исследований РАН. Автор теоретических и практических разработок, книг, учебных пособий и статей по информационной безопасности и технологии программирования.

Лекции

Содержание

Лекция 1. Понятие информационной безопасности. Основные составляющие. Важность проблемы

Под информационной безопасностью (ИБ) следует понимать защиту интересов субъектов информационных отношений. Ниже описаны основные ее составляющие – конфиденциальность, целостность, доступность. Приводится статистика нарушений ИБ, описываются наиболее характерные случаи.

Ключевые слова: информационная безопасность, защита информации, субъект информационных отношений, неприемлемый ущерб, поддерживающая инфраструктура, доступность, целостность, конфиденциальность, доктрина информационной безопасности Российской Федерации, компьютерное преступление, жизненный цикл информационных систем.

Понятие информационной безопасности

Словосочетание "информационная безопасность" в разных контекстах может иметь различный смысл.

В Доктрине информационной безопасности Российской Федерации термин "информационная безопасность" используется в широком смысле. Имеется в виду состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

В Законе РФ "Об участии в международном информационном обмене" информационная безопасность определяется аналогичным образом – как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

В данном курсе наше внимание будет сосредоточено на хранении, обработке и передаче информации вне зависимости от того, на каком языке (русском или каком-либо ином) она закодирована, кто или что является ее источником и какое психологическое воздействие она оказывает на людей. Поэтому термин "информационная безопасность" будет использоваться в узком смысле, так, как это принято, например, в англоязычной литературе.

Под информационной безопасностью мы будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственно-

го характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры. (Чуть дальше мы поясним, что следует понимать под поддерживающей инфраструктурой.)

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Таким образом, правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС). Угрозы информационной безопасности – это оборотная сторона использования информационных технологий.

Из этого положения можно вывести два важных следствия:

1 Трактовка проблем, связанных с информационной безопасностью, для разных категорий субъектов может существенно различаться. Для иллюстрации достаточно сопоставить режимные государственные организации и учебные институты. В первом случае "пусть лучше все сломается, чем враг узнает хоть один секретный бит", во втором – "да нет у нас никаких секретов, лишь бы все работало".

2 Информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации, это принципиально более широкое понятие. Субъект информационных отношений может пострадать (понести убытки и/или получить моральный ущерб) не только от несанкционированного доступа, но и от поломки системы, вызвавшей перерыв в работе. Более того, для многих открытых организаций (например, учебных) собственно защита от несанкционированного доступа к информации стоит по важности отнюдь не на первом месте.

Возвращаясь к вопросам терминологии, отметим, что термин "компьютерная безопасность" (как эквивалент или заменитель ИБ) представляется нам слишком узким. Компьютеры – только одна из составляющих информационных систем, и хотя наше внимание будет сосредоточено в первую очередь на информации, которая хранится, обрабатывается и передается с помощью компьютеров, ее безопасность определяется всей совокупностью составляющих и, в первую очередь, самым слабым звеном, которым в подавляющем большинстве случаев оказывается человек (записавший, например, свой пароль на "горчичнике", прилепленном к монитору).

Согласно определению информационной безопасности, она зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электро-, водо- и теплоснабжения, кон-

дционеры, средства коммуникаций и, конечно, обслуживающий персонал. Эта инфраструктура имеет самостоятельную ценность, но нас будет интересовать лишь то, как она влияет на выполнение информационной системой предписанных ей функций.

Обратим внимание, что в определении ИБ перед существительным "ущерб" стоит прилагательное "неприемлемый". Очевидно, застраховаться от всех видов ущерба невозможно, тем более невозможно сделать это экономически целесообразным способом, когда стоимость защитных средств и мероприятий не превышает размер ожидаемого ущерба. Значит, с чем-то приходится мириться и защищаться следует только от того, с чем смириться никак нельзя. Иногда таким недопустимым ущербом является нанесение вреда здоровью людей или состоянию окружающей среды, но чаще порог неприемлемости имеет материальное (денежное) выражение, а целью защиты информации становится уменьшение размеров ущерба до допустимых значений.

Основные составляющие информационной безопасности

Информационная безопасность – многогранная, можно даже сказать, многомерная область деятельности, в которой успех может принести только систематический, комплексный подход.

Спектр интересов субъектов, связанных с использованием информационных систем, можно разделить на следующие категории: обеспечение доступности, целостности и конфиденциальности информационных ресурсов и поддерживающей инфраструктуры.

Иногда в число основных составляющих ИБ включают защиту от несанкционированного копирования информации, но, на наш взгляд, это слишком специфический аспект с сомнительными шансами на успех, поэтому мы не станем его выделять.

Поясним понятия доступности, целостности и конфиденциальности.

Доступность – это возможность за приемлемое время получить требуемую информационную услугу.

Под целостностью подразумевается актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Наконец, конфиденциальность – это защита от несанкционированного доступа к информации.

Информационные системы создаются (приобретаются) для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, это, очевидно, наносит ущерб всем субъектам информационных отношений. Поэтому, не противопоставляя доступность осталь-

ным аспектам, мы выделяем ее как важнейший элемент информационной безопасности.

Особенно ярко ведущая роль доступности проявляется в разного рода системах управления – производством, транспортом и т.п. Внешне менее драматичные, но также весьма неприятные последствия – и материальные, и моральные – может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей (продажа железнодорожных и авиабилетов, банковские услуги и т.п.).

Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий (транзакций)). Средства контроля динамической целостности применяются, в частности, при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений.

Целостность оказывается важнейшим аспектом ИБ в тех случаях, когда информация служит "руководством к действию". Рецептура лекарств, предписанные медицинские процедуры, набор и характеристики комплектующих изделий, ход технологического процесса – все это примеры информации, нарушение целостности которой может оказаться в буквальном смысле смертельным. Неприятно и искажение официальной информации, будь то текст закона или страница Web-сервера какой-либо правительственной организации.

Конфиденциальность – самый проработанный у нас в стране аспект информационной безопасности. К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем наталкивается в России на серьезные трудности. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные препоны и технические проблемы.

Если вернуться к анализу интересов различных категорий субъектов информационных отношений, то почти для всех, кто реально использует ИС, на первом месте стоит доступность. Практически не уступает ей по важности целостность – какой смысл в информационной услуге, если она содержит искаженные сведения?

Наконец, конфиденциальные моменты есть также у многих организаций (даже в упоминавшихся выше учебных институтах стараются не разглашать сведения о зарплате сотрудников) и отдельных пользователей (например, пароли).

Важность и сложность проблемы информационной безопасности

Информационная безопасность является одним из важнейших аспектов интегральной безопасности, на каком бы уровне мы ни рассматривали последнюю – национальном, отраслевом, корпоративном или персональном.

Для иллюстрации этого положения ограничимся несколькими примерами.

- В Доктрине информационной безопасности Российской Федерации (здесь, подчеркнем, термин "информационная безопасность" используется в широком смысле) защита от несанкционированного доступа к информационным ресурсам, обеспечение безопасности информационных и телекоммуникационных систем выделены в качестве важных составляющих национальных интересов РФ в информационной сфере.
- По распоряжению президента США Клинтона (от 15 июля 1996 года, номер 13010) была создана Комиссия по защите критически важной инфраструктуры как от физических нападений, так и от атак, предпринятых с помощью информационного оружия. В начале октября 1997 года при подготовке доклада президенту глава вышеупомянутой комиссии Роберт Марш заявил, что в настоящее время ни правительство, ни частный сектор не располагают средствами защиты от компьютерных атак, способных вывести из строя коммуникационные сети и сети энергоснабжения.
- Американский ракетный крейсер "Йорктаун" был вынужден вернуться в порт из-за многочисленных проблем с программным обеспечением, функционировавшим на платформе Windows NT 4.0 (Government Computer News, июль 1998). Таким оказался побочный эффект программы ВМФ США по максимально широкому использованию коммерческого программного обеспечения с целью снижения стоимости военной техники.
- Заместитель начальника управления по экономическим преступлениям Министерства внутренних дел России сообщил, что российские хакеры с 1994 по 1996 год предприняли почти 500 попыток проникновения в компьютерную сеть Центрального банка России. В 1995 году ими было похищено 250 миллиардов рублей (ИТАР-ТАСС, АР, 17 сентября 1996 года).
- Как сообщил журнал Internet Week от 23 марта 1998 года, потери крупнейших компаний, вызванные компьютерными вторжениями, продолжают увеличиваться, несмотря на рост затрат на средства обеспечения безопасности. Согласно результатам совместного исследования Института информационной безо-

пасности и ФБР, в 1997 году ущерб от компьютерных преступлений достиг 136 миллионов долларов, что на 36% больше, чем в 1996 году. Каждое компьютерное преступление наносит ущерб примерно в 200 тысяч долларов.

- В середине июля 1996 года корпорация General Motors отозвала 292860 автомобилей марки Pontiac, Oldsmobile и Buick моделей 1996 и 1997 годов, поскольку ошибка в программном обеспечении двигателя могла привести к пожару.
- В феврале 2001 года двое бывших сотрудников компании Commerce One, воспользовавшись паролем администратора, удалили с сервера файлы, составлявшие крупный (на несколько миллионов долларов) проект для иностранного заказчика. К счастью, имелась резервная копия проекта, так что реальные потери ограничились расходами на следствие и средства защиты от подобных инцидентов в будущем. В августе 2002 года преступники предстали перед судом.
- Одна студентка потеряла стипендию в 18 тысяч долларов в Мичиганском университете из-за того, что ее соседка по комнате воспользовалась их общим системным входом и отправила от имени своей жертвы электронное письмо с отказом от стипендии.

Понятно, что подобных примеров множество, можно вспомнить и другие случаи – недостатка в нарушениях ИБ нет и не предвидится. Чего стоит одна только "Проблема 2000" – стыд и позор программистского сообщества!

При анализе проблематики, связанной с информационной безопасностью, необходимо учитывать специфику данного аспекта безопасности, состоящую в том, что информационная безопасности есть составная часть информационных технологий – области, развивающейся беспрецедентно высокими темпами. Здесь важны не столько отдельные решения (законы, учебные курсы, программно-технические изделия), находящиеся на современном уровне, сколько механизмы генерации новых решений, позволяющие жить в темпе технического прогресса.

К сожалению, современная технология программирования не позволяет создавать безошибочные программы, что не способствует быстрому развитию средств обеспечения ИБ. Следует исходить из того, что необходимо конструировать надежные системы (информационной безопасности) с привлечением ненадежных компонентов (программ). В принципе, это возможно, но требует соблюдения определенных архитектурных принципов и контроля состояния защищенности на всем протяжении жизненного цикла ИС.

Приведем еще несколько цифр. В марте 1999 года был опубликован очередной, четвертый по счету, годовой отчет "Компьютерная преступность и безопасность-1999: проблемы и тенденции" (Issues and Trends: 1999 CSI/FBI

Computer Crime and Security Survey). В отчете отмечается резкий рост числа обращений в правоохранительные органы по поводу компьютерных преступлений (32% из числа опрошенных); 30% респондентов сообщили о том, что их информационные системы были взломаны внешними злоумышленниками; атакам через Internet подвергались 57% опрошенных; в 55% случаях отмечались нарушения со стороны собственных сотрудников. Примечательно, что 33% респондентов на вопрос "были ли взломаны ваши Web-серверы и системы электронной коммерции за последние 12 месяцев?" ответили "не знаю".

В аналогичном отчете, опубликованном в апреле 2002 года, цифры изменились, но тенденция осталась прежней: 90% респондентов (преимущественно из крупных компаний и правительственных структур) сообщили, что за последние 12 месяцев в их организациях имели место нарушения информационной безопасности; 80% констатировали финансовые потери от этих нарушений; 44% (223 респондента) смогли и/или захотели оценить потери количественно, общая сумма составила более 455 млн. долларов. Наибольший ущерб нанесли кражи и подлоги (более 170 и 115 млн. долларов соответственно).

Столь же тревожные результаты содержатся в обзоре InformationWeek, опубликованном 12 июля 1999 года. Лишь 22% респондентов заявили об отсутствии нарушений информационной безопасности. Наряду с распространением вирусов отмечается резкий рост числа внешних атак.

Увеличение числа атак – еще не самая большая неприятность. Хуже то, что постоянно обнаруживаются новые уязвимые места в программном обеспечении (выше мы указывали на ограниченность современной технологии программирования) и, как следствие, появляются новые виды атак.

Так, в информационном письме Национального центра защиты инфраструктуры США (National Infrastructure Protection Center, NIPC) от 21 июля 1999 года сообщается, что за период с 3 по 16 июля 1999 года выявлено девять проблем с ПО, риск использования которых оценивается как средний или высокий (общее число обнаруженных уязвимых мест равно 17). Среди "пострадавших" операционных платформ – почти все разновидности ОС Unix, Windows, MacOS, так что никто не может чувствовать себя спокойно, поскольку новые ошибки тут же начинают активно использоваться злоумышленниками.

В таких условиях системы информационной безопасности должны уметь противостоять разнообразным атакам, как внешним, так и внутренним, атакам автоматизированным и скоординированным. Иногда нападение длится доли секунды; порой прощупывание уязвимых мест ведется медленно и растягивается на часы, так что подозрительная активность практически незаметна. Целью злоумышленников может быть нарушение всех составляющих ИБ – доступности, целостности или конфиденциальности.

Вариант 1

1. Меры информационной безопасности направлены на защиту от:

- ☐ нанесения неприемлемого ущерба
- ☐ нанесения любого ущерба
- ☐ подглядывания в замочную скважину

2. Что из перечисленного не относится к числу основных аспектов информационной безопасности?

- ☐ доступность
- ☐ целостность
- ☐ конфиденциальность
- ☐ *правдивое отражение действительности*

3. Затраты организаций на информационную безопасность:

- ☐ растут
- ☐ остаются на одном уровне
- ☐ снижаются

4. В отчете "Компьютерная преступность и безопасность-2002" 25 респондентов заявили о случаях подлогов. Средний ущерб от подлога составляет:

- ☐ около 1 млн. долларов
- ☐ около 4,5 млн. долларов
- ☐ около 9,8 млн. долларов

Вариант 2

1. Что такое защита информации?

- ☐ защита от несанкционированного доступа к информации
- ☐ выпуск бронированных коробочек для дискет
- ☐ комплекс мероприятий, направленных на обеспечение информационной безопасности

2. Что из перечисленного не относится к числу основных аспектов информационной безопасности?

- ☐ доступность
- ☐ масштабируемость
- ☐ целостность
- ☐ конфиденциальность

3. Компьютерная преступность в мире:

- ☐ остается на одном уровне
- ☐ снижается
- ☐ растет

4. В отчете "Компьютерная преступность и безопасность-2002" 26 респондентов заявили о случаях краж. Средний ущерб от кражи составляет:

- ☐ около 1 млн. долларов
- ☐ около 6,5 млн. долларов
- ☐ около 12,8 млн. долларов

Вариант 3

1. Что понимается под информационной безопасностью?

- ☐ защита душевного здоровья телезрителей
- ☐ защита от нанесения неприемлемого ущерба субъектам информационных отношений
- ☐ обеспечение информационной независимости России

2. Что из перечисленного не относится к числу основных аспектов информационной безопасности?

- ☐ доступность
- ☐ целостность
- ☐ защита от копирования
- ☐ конфиденциальность

3. Средний ущерб от компьютерного преступления в США составляет примерно:

- ☐ сотни тысяч долларов
- ☐ десятки долларов
- ☐ копейки

4. В отчете "Компьютерная преступность и безопасность-2002" использованы результаты опроса:

- ☐ около 100 респондентов
- ☐ около 500 респондентов
- ☐ около 1000 респондентов

Лекция 2. Распространение объектно-ориентированного подхода на информационную безопасность

В этой лекции закладываются методические основы курса. Кратко формулируются необходимые понятия объектно-ориентированного подхода, в соответствии с ним выделяются уровни мер в области ИБ с небольшим числом сущностей на каждом из них.

Ключевые слова: сложные системы, принцип "разделяй и властвуй", декомпозиция, структурный подход, объектно-ориентированный подход, класс, объект, метод объекта, инкапсуляция, наследование, полиморфизм, грань объекта, уровень детализации, компонентная объектная среда, компонент, контейнер, ортогональные совокупности граней, уровень детализации ИС, деление на субъекты и объекты, безопасность повторного использования объектов, учет семантики, троянские программы, операционная система как сервис безопасности.

О необходимости объектно-ориентированного подхода к информационной безопасности

В настоящее время информационная безопасность является относительно замкнутой дисциплиной, развитие которой не всегда синхронизировано с изменениями в других областях информационных технологий. В частности, в ИБ пока не нашли отражения основные положения объектно-ориентированного подхода, ставшего основой при построении современных информационных систем. Не учитываются в ИБ и достижения в технологии программирования, основанные на накоплении и многократном использовании программистских знаний. На наш взгляд, это очень серьезная проблема, затрудняющая прогресс в области ИБ.

Попытки создания больших систем еще в 60-х годах вскрыли многочисленные проблемы программирования, главной из которых является сложность создаваемых и сопровождаемых систем. Результатами исследований в области технологии программирования стали сначала структурированное программирование, затем объектно-ориентированный подход.

Объектно-ориентированный подход является основой современной технологии программирования, испытанным методом борьбы со сложностью систем. Представляется естественным и, более того, необходимым,

стремление распространить этот подход и на системы информационной безопасности, для которых, как и для программирования в целом, имеет место упомянутая проблема сложности.

Сложность эта имеет двоякую природу. Во-первых, сложны не только аппаратно-программные системы, которые необходимо защищать, но и сами средства безопасности. Во-вторых, быстро нарастает сложность семейства нормативных документов, таких, например, как профили защиты на основе "Общих критериев", речь о которых впереди. Эта сложность менее очевидна, но ею также нельзя пренебрегать; необходимо изначально строить семейства документов по объектному принципу.

Любой разумный метод борьбы со сложностью опирается на принцип "devide et impera" – "разделяй и властвуй". В данном контексте этот принцип означает, что сложная система (информационной безопасности) на верхнем уровне должна состоять из небольшого числа относительно независимых компонентов. Относительная независимость здесь и далее понимается как минимизация числа связей между компонентами. Затем декомпозиции подвергаются выделенные на первом этапе компоненты, и так далее до заданного уровня детализации. В результате система оказывается представленной в виде иерархии с несколькими уровнями абстракции.

Важнейший вопрос, возникающий при реализации принципа "разделяй и властвуй", – как, собственно говоря, разделять. Упоминавшийся выше структурный подход опирается на алгоритмическую декомпозицию, когда выделяются функциональные элементы системы. Основная проблема структурного подхода состоит в том, что он неприменим на ранних этапах анализа и моделирования предметной области, когда до алгоритмов и функций дело еще не дошло. Нужен подход "широкого спектра", не имеющий такого концептуального разрыва с анализируемыми системами и применимый на всех этапах разработки и реализации сложных систем. Мы постараемся показать, что объектно-ориентированный подход удовлетворяет таким требованиям.

Основные понятия объектно-ориентированного подхода

Объектно-ориентированный подход использует объектную декомпозицию, то есть поведение системы описывается в терминах взаимодействия объектов.

Что же понимается под объектом и каковы другие основополагающие понятия данного подхода?

Прежде всего, введем понятие класса. Класс – это абстракция множества сущностей реального мира, объединенных общностью структуры и поведения.

Объект – это элемент класса, то есть абстракция определенной сущности.

Подчеркнем, что объекты активны, у них есть не только внутренняя структура, но и поведение, которое описывается так называемыми методами объекта. Например, может быть определен класс "пользователь", характеризующий "пользователя вообще", то есть ассоциированные с пользователями данные и их поведение (методы). После этого может быть создан объект "пользователь Иванов" с соответствующей конкретизацией данных и, возможно, методов.

К активности объектов мы еще вернемся.

Следующую группу важнейших понятий объектного подхода составляют инкапсуляция, наследование и полиморфизм.

Основным инструментом борьбы со сложностью в объектно-ориентированном подходе является инкапсуляция – сокрытие реализации объектов (их внутренней структуры и деталей реализации методов) с предоставлением вовне только строго определенных интерфейсов.

Понятие "полиморфизм" может трактоваться как способность объекта принадлежать более чем одному классу. Введение этого понятия отражает необходимость смотреть на объекты под разными углами зрения, выделять при построении абстракций разные аспекты сущностей моделируемой предметной области, не нарушая при этом целостности объекта. (Строго говоря, существуют и другие виды полиморфизма, такие как перегрузка и параметрический полиморфизм, но нас они сейчас не интересуют.)

Наследование означает построение новых классов на основе существующих с возможностью добавления или переопределения данных и методов. Наследование является важным инструментом борьбы с размножением сущностей без необходимости. Общая информация не дублируется, указывается только то, что меняется. При этом класс-потомок помнит о своих "корнях".

Очень важно и то, что наследование и полиморфизм в совокупности наделяют объектно-ориентированную систему способностью к относительно безболезненной эволюции. Средства информационной безопасности приходится постоянно модифицировать и обновлять, и если нельзя сделать так, чтобы это было экономически выгодно, ИБ из инструмента защиты превращается в обузу.

Мы еще вернемся к механизму наследования при рассмотрении ролевого управления доступом.

Пополним рассмотренный выше классический набор понятий объектно-ориентированного подхода еще двумя понятиями: грани объекта и уровня детализации.

Объекты реального мира обладают, как правило, несколькими относительно независимыми характеристиками. Применительно к объектной

модели будем называть такие характеристики гранями. Мы уже сталкивались с тремя основными гранями ИБ – доступностью, целостностью и конфиденциальностью. Понятие грани позволяет более естественно, чем полиморфизм, смотреть на объекты с разных точек зрения и строить разноплановые абстракции.

Понятие уровня детализации важно не только для визуализации объектов, но и для систематического рассмотрения сложных систем, представленных в иерархическом виде. Само по себе оно очень простое: если очередной уровень иерархии рассматривается с уровнем детализации $n > 0$, то следующий – с уровнем $(n - 1)$. Объект с уровнем детализации 0 считается атомарным.

Понятие уровня детализации показа позволяет рассматривать иерархии с потенциально бесконечной высотой, варьировать детализацию как объектов в целом, так и их граней.

Весьма распространенной конкретизацией объектно-ориентированного подхода являются компонентные объектные среды, к числу которых принадлежит, например, JavaBeans. Здесь появляется два новых важных понятия: компонент и контейнер.

Неформально компонент можно определить как многократно используемый объект, допускающий обработку в графическом инструментальном окружении и сохранение в долговременной памяти.

Контейнеры могут включать в себя множество компонентов, образуя общий контекст взаимодействия с другими компонентами и с окружением. Контейнеры могут выступать в роли компонентов других контейнеров.

Компонентные объектные среды обладают всеми достоинствами, присущими объектно-ориентированному подходу:

- инкапсуляция объектных компонентов скрывает сложность реализации, делая видимым только предоставляемый вовне интерфейс;
- наследование позволяет развивать созданные ранее компоненты, не нарушая целостность объектной оболочки;
- полиморфизм по сути дает возможность группировать объекты, характеристики которых с некоторой точки зрения можно считать сходными.

Понятия же компонента и контейнера необходимы нам потому, что с их помощью мы можем естественным образом представить защищаемую ИС и сами защитные средства. В частности, контейнер может определять границы контролируемой зоны (задавать так называемый "периметр безопасности").

На этом мы завершаем описание основных понятий объектно-ориентированного подхода.

Применение объектно-ориентированного подхода к рассмотрению защищаемых систем

Попытаемся применить объектно-ориентированный подход к вопросам информационной безопасности.

Проблема обеспечения информационной безопасности – комплексная, защищать приходится сложные системы, и сами защитные средства тоже сложны, поэтому нам понадобятся все введенные понятия. Начнем с понятия грани.

Фактически три грани уже были введены: это доступность, целостность и конфиденциальность. Их можно рассматривать относительно независимо, и считается, что если все они обеспечены, то обеспечена и ИБ в целом (то есть субъектам информационных отношений не будет нанесен неприемлемый ущерб).

Таким образом, мы структурировали нашу цель. Теперь нужно структурировать средства ее достижения. Введем следующие грани:

- законодательные меры обеспечения информационной безопасности;
- административные меры (приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами);
- процедурные меры (меры безопасности, ориентированные на людей);
- программно-технические меры.

В дальнейшей части курса мы поясним подробнее, что понимается под каждой из выделенных граней. Здесь же отметим, что, в принципе, их можно рассматривать и как результат варьирования уровня детализации (по этой причине мы будем употреблять словосочетания "законодательный уровень", "процедурный уровень" и т.п.). Законы и нормативные акты ориентированы на всех субъектов информационных отношений независимо от их организационной принадлежности (это могут быть как юридические, так и физические лица) в пределах страны (международные конвенции имеют даже более широкую область действия), административные меры – на всех субъектов в пределах организации, процедурные – на отдельных людей (или небольшие категории субъектов), программно-технические – на оборудование и программное обеспечение. При такой трактовке в переходе с уровня на уровень можно усмотреть применение наследования (каждый следующий уровень не отменяет, а дополняет предыдущий), а также полиморфизма (субъекты выступают сразу в нескольких ипостасях – например, как инициаторы административных мер и как обычные пользователи, обязанные этим мерам подчиняться).

Очевидно, для всех выделенных, относительно независимых граней действует принцип инкапсуляции (это и значит, что грани "относительно независимы"). Более того, эти две совокупности граней можно назвать ортогональными, поскольку для фиксированной грани в одной совокупности (например, доступности) грани в другой совокупности должны пробегать все множество возможных значений (нужно рассмотреть законодательные, административные, процедурные и программно-технические меры). Ортогональных совокупностей не должно быть много; думается, двух совокупностей с числом элементов, соответственно, 3 и 4 уже достаточно, так как они дают 12 комбинаций.

Продемонстрируем теперь, как можно рассматривать защищаемую ИС, варьируя уровень детализации.

Пусть интересы субъектов информационных отношений концентрируются вокруг ИС некой организации, располагающей двумя территориально разнесенными производственными площадками, на каждой из которых есть серверы, обслуживающие своих и внешних пользователей, а также пользователи, нуждающиеся во внутренних и внешних сервисах. Одна из площадок оборудована внешним подключением (то есть имеет выход в Internet).

При взгляде с нулевым уровнем детализации мы увидим лишь то, что у организации есть информационная система (см. рис. 2.0).

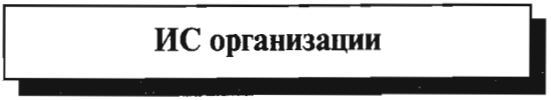

Рис. 2.0. ИС при рассмотрении с уровнем детализации 0.

Подобная точка зрения может показаться несостоятельной, но это не так. Уже здесь необходимо учесть законы, применимые к организациям, располагающим информационными системами. Возможно, какую-либо информацию нельзя хранить и обрабатывать на компьютерах, если ИС не была аттестована на соответствие определенным требованиям. На административном уровне могут быть декларированы цели, ради которых создавалась ИС, общие правила закупок, внедрения новых компонентов, эксплуатации и т.п. На процедурном уровне нужно определить требования к физической безопасности ИС и пути их выполнения, правила противопожарной безопасности и т.п. На программно-техническом уровне могут быть определены предпочтительные аппаратно-программные платформы и т.п.

По каким критериям проводить декомпозицию ИС – в значительной степени дело вкуса. Будем считать, что на первом уровне детализации делаются видимыми сервисы и пользователи, точнее, разделение на клиентскую и серверную часть (рис. 2.1).

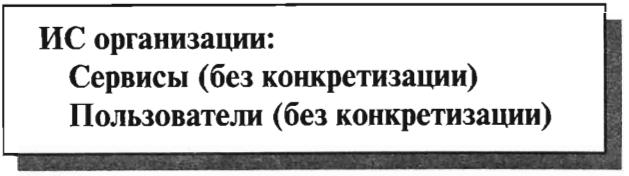

Рис. 2.1. ИС при рассмотрении с уровнем детализации 1.

На этом уровне следует сформулировать требования к сервисам (к самому их наличию, к доступности, целостности и конфиденциальности предоставляемых информационных услуг), изложить способы выполнения этих требований, определить общие правила поведения пользователей, необходимый уровень их предварительной подготовки, методы контроля их поведения, порядок поощрения и наказания и т.п. Могут быть сформулированы требования и предпочтения по отношению к серверным и клиентским платформам.

На втором уровне детализации мы увидим следующее (см. рис. 2.2).

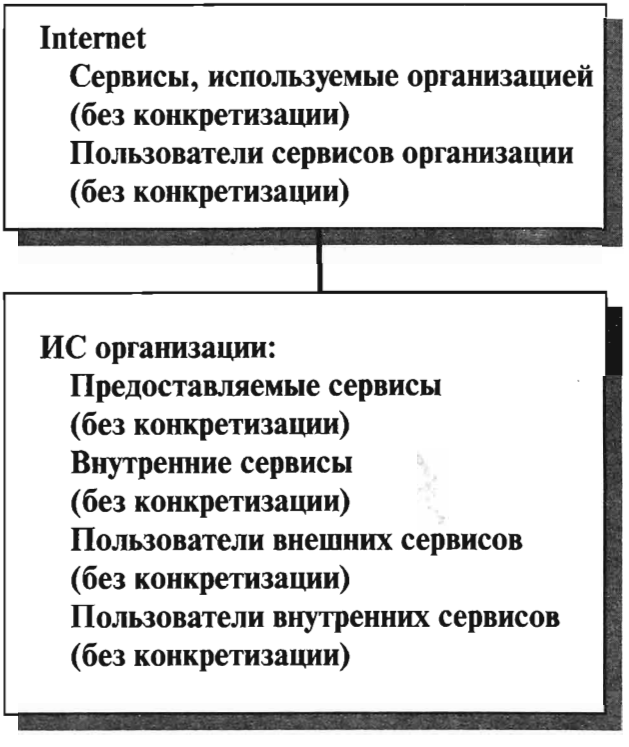

Рис. 2.2. ИС при рассмотрении с уровнем детализации 2.

На этом уровне нас все еще не интересует внутренняя структура ИС организации, равно как и детали Internet. Констатируется только существование связи между этими сетями, наличие в них пользователей, а также предоставляемых и внутренних сервисов. Что это за сервисы, пока неважно.

Находясь на уровне детализации 2, мы должны учитывать законы, применимые к организациям, ИС которых снабжены внешними подключениями. Речь идет о допустимости такого подключения, о его защите, об ответственности пользователей, обращающихся к внешним сервисам, и об ответственности организаций, открывающих свои сервисы для внешнего доступа. Конкретизация аналогичной направленности, с учетом наличия внешнего подключения, должна быть выполнена на административном, процедурном и программно-техническом уровнях.

Обратим внимание на то, что контейнер (в смысле компонентной объектной среды) "ИС организации" задает границы контролируемой зоны, в пределах которых организация проводит определенную политику. Internet живет по другим правилам, которые организация должна принимать, как данность.

Увеличивая уровень детализации, можно разглядеть две разнесенные производственные площадки и каналы связи между ними, распределение сервисов и пользователей по этим площадкам и средства обеспечения безопасности внутренних коммуникаций, специфику отдельных сервисов, разные категории пользователей и т.п. Мы, однако, на этом остановимся.

Недостатки традиционного подхода к информационной безопасности с объектной точки зрения

Исходя из основных положений объектно-ориентированного подхода, следует в первую очередь признать устаревшим традиционное деление на активные и пассивные сущности (субъекты и объекты в привычной для дообъектной ИБ терминологии). Подобное деление устарело, по крайней мере, по двум причинам.

Во-первых, в объектном подходе пассивных объектов нет. Можно считать, что все объекты активны одновременно и при необходимости вызывают методы друг друга. Как реализованы эти методы (и, в частности, как организован доступ к переменным и их значениям) – внутреннее дело вызываемого объекта; детали реализации скрыты, инкапсулированы. Вызывающему объекту доступен только предоставляемый интерфейс.

Во-вторых, нельзя сказать, что какие-то программы (методы) выполняются от имени пользователя. Реализации объектов сложны, так что последние нельзя рассматривать всего лишь как инструменты выполне-

ния воли пользователей. Скорее можно считать, что пользователь прямо или (как правило) косвенно, на свой страх и риск, "просит" некоторый объект об определенной информационной услуге. Когда активизируется вызываемый метод, объект действует скорее от имени (во всяком случае, по воле) своего создателя, чем от имени вызвавшего его пользователя. Можно считать, что объекты обладают достаточной "свободой воли", чтобы выполнять действия, о которых пользователь не только не просил, но даже не догадывается об их возможности. Особенно это справедливо в сетевой среде и для программного обеспечения (ПО), полученного через Internet, но может оказаться верным и для коммерческого ПО, закупленного по всем правилам у солидной фирмы.

Для иллюстрации приведем следующий гипотетический пример. Банк, ИС которого имеет соединение с Internet, приобрел за рубежом автоматизированную банковскую систему (АБС). Только спустя некоторое время в банке решили, что внешнее соединение нуждается в защите, и установили межсетевой экран.

Изучение регистрационной информации экрана показало, что время от времени за рубеж отправляются IP-пакеты, содержащие какие-то непонятные данные (наверное, зашифрованные, решили в банке). Стали разбираться, куда же пакеты направляются, и оказалось, что идут они в фирму, разработавшую АБС. Возникло подозрение, что в АБС встроена закладка, чтобы получать информацию о деятельности банка. Связались с фирмой; там очень удивились, поначалу все отрицали, но в конце концов выяснили, что один из программистов не убрал из поставленного в банк варианта отладочную выдачу, которая была организована через сеть (как передача IP-пакетов специфического вида, с явно заданным IP-адресом рабочего места этого программиста). Таким образом, никакого злого умысла не было, однако некоторое время информация о платежах свободно гуляла по сетям.

В дальнейшей части курса, в лекции, посвященной разграничению доступа, мы обсудим, как можно кардинальным образом решить подобные проблемы. Здесь отметим лишь, что при определении допустимости доступа важно не только (и не столько), кто обратился к объекту, но и то, какова семантика действия. Без привлечения семантики нельзя определить так называемые "троянские программы", выполняющие, помимо декларированных, некоторые скрытые (обычно негативные) действия.

По-видимому, следует признать устаревшим и положение о том, что разграничение доступа направлено на защиту от злоумышленников. Приведенный выше пример показывает, что внутренние ошибки распределенных ИС представляют не меньшую опасность, а гарантировать их отсутствие в сложных системах современная технология программирования не позволяет.

В дообъектной ИБ одним из важнейших требований является безопасность повторного использования пассивных сущностей (таких, например, как динамически выделяемые области памяти). Очевидно, подобное требование вступает в конфликт с таким фундаментальным принципом, как инкапсуляция. Объект нельзя очистить внешним образом (заполнить нулями или случайной последовательностью бит), если только он сам не предоставляет соответствующий метод. При наличии такого метода надежность очистки зависит от корректности его реализации и вызова.

Одним из самых прочных стереотипов среди специалистов по ИБ является трактовка операционной системы как доминирующего средства безопасности. На разработку защищенных ОС выделяются значительные средства, зачастую в ущерб остальным направлениям защиты и, следовательно, в ущерб реальной безопасности. В современных ИС, выстроенных в многоуровневой архитектуре клиент/сервер, ОС не контролирует объекты, с которыми работают пользователи, равно как и действия самих пользователей, которые регистрируются и учитываются прикладными средствами. Основной функцией безопасности ОС становится защита возможностей, предоставляемых привилегированным пользователям, от атак пользователей обычных.

Это важно, но безопасность такими мерами не исчерпывается. Далее мы рассмотрим подход к построению программно-технического уровня ИБ в виде совокупности сервисов безопасности.

Вариант 1

1. Объектно-ориентированный подход помогает справляться с:

- ☐ сложностью систем
- ☐ недостаточной реактивностью систем
- ☐ некачественным пользовательским интерфейсом

2. Объектно-ориентированный подход использует:

- ☐ семантическую декомпозицию
- ☐ объектную декомпозицию
- ☐ алгоритмическую декомпозицию

3. Требование безопасности повторного использования объектов противоречит:

- ☐ инкапсуляции
- ☐ наследованию
- ☐ полиморфизму

4. Предположим, что при разграничении доступа учитывается семантика программ. В таком случае на текстовый редактор могут быть наложены следующие ограничения:

- ☐ запрет на чтение каких-либо файлов, кроме редактируемых и конфигурационных
- ☐ запрет на изменение каких-либо файлов, кроме редактируемых и конфигурационных
- ☐ запрет на выполнение каких-либо файлов

Вариант 2

1. Любой разумный метод борьбы со сложностью опирается на принцип:

- ☐ не следует умножать сущности сверх необходимого
- ☐ отрицания отрицания
- ☐ разделяй и властвуй

2. В число основных понятий объектного подхода не входит:

- ☐ инкапсуляция
- ☐ наследование
- ☐ полифонизм

3. Деление на активные и пассивные сущности противоречит:

- ☐ классической технологии программирования
- ☐ основам объектно-ориентированного подхода
- ☐ стандарту на язык программирования Си

4. Предположим, что при разграничении доступа учитывается семантика программ. В таком случае на просмотрщик файлов определенного формата могут быть наложены следующие ограничения:

- ☐ запрет на чтение файлов, кроме просматриваемых и конфигурационных
- ☐ запрет на изменение файлов, кроме просматриваемых и конфигурационных
- ☐ запрет на изменение каких-либо файлов

Вариант 3

1. Структурный подход опирается на:

- ☐ семантическую декомпозицию
- ☐ алгоритмическую декомпозицию
- ☐ декомпозицию структур данных

2. Контейнеры в компонентных объектных средах предоставляют:

- ☐ общий контекст взаимодействия с другими компонентами и окружением
- ☐ средства для сохранения компонентов
- ☐ механизмы транспортировки компонентов

3. Метод объекта реализует волю:

- ☐ вызвавшего его пользователя
- ☐ владельца информационной системы
- ☐ разработчика объекта

4. Предположим, что при разграничении доступа учитывается семантика программ. В таком случае на игровую программу могут быть наложены следующие ограничения:

- ☐ запрет на чтение каких-либо файлов, кроме конфигурационных
- ☐ запрет на изменение каких-либо файлов, кроме конфигурационных
- ☐ запрет на установление сетевых соединений

Лекция 3. Наиболее распространенные угрозы

Знание возможных угроз, а также уязвимых мест защиты, которые эти угрозы обычно эксплуатируют, необходимо для того, чтобы выбирать наиболее экономичные средства обеспечения безопасности.

Ключевые слова: угроза, атака, уязвимость, окно опасности, источник угрозы, злоумышленник, непреднамеренные ошибки, отказ пользователей, внутренний отказ, отказ поддерживающей инфраструктуры, обиженные сотрудники, стихийные бедствия, повреждение оборудования, аварии поддерживающей инфраструктуры, агрессивное потребление ресурсов, локальное потребление, удаленное потребление, вредоносное ПО, бомба, вирус, червь, троянская программа, переполнение буфера, активное содержимое, мобильные агенты, статическая целостность, динамическая целостность, целостность данных, целостность программной среды, неотказуемость, кража, подлог, перехват данных, злоупотребление полномочиями, маскарад, методы морально-психологического воздействия.

Основные определения и критерии классификации угроз

Угроза – это потенциальная возможность определенным образом нарушить информационную безопасность.

Попытка реализации угрозы называется атакой, а тот, кто предпринимает такую попытку, – злоумышленником. Потенциальные злоумышленники называются источниками угрозы.

Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем (таких, например, как возможность доступа посторонних лиц к критически важному оборудованию или ошибки в программном обеспечении).

Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется окном опасности, ассоциированным с данным уязвимым местом. Пока существует окно опасности, возможны успешные атаки на ИС.

Если речь идет об ошибках в ПО, то окно опасности "открывается" с появлением средств использования ошибки и ликвидируется при наложении заплат, ее исправляющих.

Для большинства уязвимых мест окно опасности существует сравнительно долго (несколько дней, иногда – недель), поскольку за это время должны произойти следующие события:

- должно стать известно о средствах использования пробела в защите;
- должны быть выпущены соответствующие заплаты;
- заплаты должны быть установлены в защищаемой ИС.

Мы уже указывали, что новые уязвимые места и средства их использования появляются постоянно; это значит, во-первых, что почти всегда существуют окна опасности и, во-вторых, что отслеживание таких окон должно производиться постоянно, а выпуск и наложение заплат – как можно более оперативно.

Отметим, что некоторые угрозы нельзя считать следствием каких-то ошибок или просчетов; они существуют в силу самой природы современных ИС. Например, угроза отключения электричества или выхода его параметров за допустимые границы существует в силу зависимости аппаратного обеспечения ИС от качественного электропитания.

Рассмотрим наиболее распространенные угрозы, которым подвержены современные информационные системы. Иметь представление о возможных угрозах, а также об уязвимых местах, которые эти угрозы обычно эксплуатируют, необходимо для того, чтобы выбирать наиболее экономичные средства обеспечения безопасности. Слишком много мифов существует в сфере информационных технологий (вспомним все ту же "Проблему 2000"), поэтому незнание в данном случае ведет к перерасходу средств и, что еще хуже, к концентрации ресурсов там, где они не особенно нужны, за счет ослабления действительно уязвимых направлений.

Подчеркнем, что само понятие "угроза" в разных ситуациях зачастую трактуется по-разному. Например, для подчеркнуто открытой организации угроз конфиденциальности может просто не существовать — вся информация считается общедоступной; однако в большинстве случаев нелегальный доступ представляется серьезной опасностью. Иными словами, угрозы, как и все в ИБ, зависят от интересов субъектов информационных отношений (и от того, какой ущерб является для них неприемлемым).

Мы попытаемся взглянуть на предмет с точки зрения типичной (на наш взгляд) организации. Впрочем, многие угрозы (например, пожар) опасны для всех.

Угрозы можно классифицировать по нескольким критериям:

- по аспекту информационной безопасности (доступность, целостность, конфиденциальность), против которого угрозы направлены в первую очередь;

- по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);
- по способу осуществления (случайные/преднамеренные действия природного/техногенного характера);
- по расположению источника угроз (внутри/вне рассматриваемой ИС).

В качестве основного критерия мы будем использовать первый (по аспекту ИБ), привлекая при необходимости остальные.

Наиболее распространенные угрозы доступности

Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы.

Иногда такие ошибки и являются собственно угрозами (неправильно введенные данные или ошибка в программе, вызвавшая крах системы), иногда они создают уязвимые места, которыми могут воспользоваться злоумышленники (таковы обычно ошибки администрирования). По некоторым данным, до 65% потерь – следствие непреднамеренных ошибок.

Пожары и наводнения не приносят столько бед, сколько безграмотность и небрежность в работе.

Очевидно, самый радикальный способ борьбы с непреднамеренными ошибками – максимальная автоматизация и строгий контроль.

Другие угрозы доступности классифицируем по компонентам ИС, на которые нацелены угрозы:

- отказ пользователей;
- внутренний отказ информационной системы;
- отказ поддерживающей инфраструктуры.

Обычно применительно к пользователям рассматриваются следующие угрозы:

- нежелание работать с информационной системой (чаще всего проявляется при необходимости осваивать новые возможности и при расхождении между запросами пользователей и фактическими возможностями и техническими характеристиками);
- невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т.п.);
- невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т.п.).

Основными источниками внутренних отказов являются:

- отступление (случайное или умышленное) от установленных правил эксплуатации;
- выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.);
- ошибки при (пере)конфигурировании системы;
- отказы программного и аппаратного обеспечения;
- разрушение данных;
- разрушение или повреждение аппаратуры.

По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

- нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования;
- разрушение или повреждение помещений;
- невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т.п.).

Весьма опасны так называемые "обиженные" сотрудники – нынешние и бывшие. Как правило, они стремятся нанести вред организации-"обидчику", например:

- испортить оборудование;
- встроить логическую бомбу, которая со временем разрушит программы и/или данные;
- удалить данные.

Обиженные сотрудники, даже бывшие, знакомы с порядками в организации и способны нанести немалый ущерб. Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа (логического и физического) к информационным ресурсам аннулировались.

Опасны, разумеется, стихийные бедствия и события, воспринимаемые как стихийные бедствия,– пожары, наводнения, землетрясения, ураганы. По статистике, на долю огня, воды и тому подобных "злоумышленников" (среди которых самый опасный – перебой электропитания) приходится 13% потерь, нанесенных информационным системам.

Некоторые примеры угроз доступности

Угрозы доступности могут выглядеть грубо – как повреждение или даже разрушение оборудования (в том числе носителей данных). Такое повреждение может вызываться естественными причинами (чаще всего –

грозами). К сожалению, находящиеся в массовом использовании источники бесперебойного питания не защищают от мощных кратковременных импульсов, и случаи выгорания оборудования – не редкость.

В принципе, мощный кратковременный импульс, способный разрушить данные на магнитных носителях, можно сгенерировать и искусственным образом – с помощью так называемых высокоэнергетических радиочастотных пушек. Но, наверное, в наших условиях подобную угрозу следует все же признать надуманной.

Действительно опасны протечки водопровода и отопительной системы. Часто организации, чтобы сэкономить на арендной плате, снимают помещения в домах старой постройки, делают косметический ремонт, но не меняют ветхие трубы. Автору курса довелось быть свидетелем ситуации, когда прорвало трубу с горячей водой, и системный блок компьютера (это была рабочая станция производства Sun Microsystems) оказался заполнен кипятком. Когда кипяток вылили, а компьютер просушили, он возобновил нормальную работу, но лучше таких опытов не ставить...

Летом, в сильную жару, норовят сломаться кондиционеры, установленные в серверных залах, набитых дорогостоящим оборудованием. В результате значительный ущерб наносится и репутации, и кошельку организации.

Общеизвестно, что периодически необходимо производить резервное копирование данных. Однако даже если это предложение выполняется, резервные носители зачастую хранят небрежно (к этому мы еще вернемся при обсуждении угроз конфиденциальности), не обеспечивая их защиту от вредного воздействия окружающей среды. И когда требуется восстановить данные, оказывается, что эти самые носители никак не желают читаться.

Перейдем теперь к угрозам доступности, которые будут похитрее засоров канализации. Речь пойдет о программных атаках на доступность.

В качестве средства вывода системы из штатного режима эксплуатации может использоваться агрессивное потребление ресурсов (обычно – полосы пропускания сетей, вычислительных возможностей процессоров или оперативной памяти). По расположению источника угрозы такое потребление подразделяется на локальное и удаленное. При просчетах в конфигурации системы локальная программа способна практически монополизировать процессор и/или физическую память, сведя скорость выполнения других программ к нулю.

Простейший пример удаленного потребления ресурсов – атака, получившая наименование "SYN-наводнение". Она представляет собой попытку переполнить таблицу "полуоткрытых" TCP-соединений сервера (установление соединений начинается, но не заканчивается). Такая атака по меньшей мере затрудняет установление новых соединений со стороны легальных пользователей, то есть сервер выглядит как недоступный.

По отношению к атаке "Papa Smurf" уязвимы сети, воспринимающие ping-пакеты с широковещательными адресами. Ответы на такие пакеты "съедают" полосу пропускания.

Удаленное потребление ресурсов в последнее время проявляется в особенно опасной форме – как скоординированные распределенные атаки, когда на сервер с множества разных адресов с максимальной скоростью направляются вполне легальные запросы на соединение и/или обслуживание. Временем начала "моды" на подобные атаки можно считать февраль 2000 года, когда жертвами оказались несколько крупнейших систем электронной коммерции (точнее – владельцы и пользователи систем). Отметим, что если имеет место архитектурный просчет в виде разбалансированности между пропускной способностью сети и производительностью сервера, то защититься от распределенных атак на доступность крайне трудно.

Для выведения систем из штатного режима эксплуатации могут использоваться уязвимые места в виде программных и аппаратных ошибок. Например, известная ошибка в процессоре Pentium I дает возможность локальному пользователю путем выполнения определенной команды "подвесить" компьютер, так что помогает только аппаратный RESET.

Программа "Teardrop" удаленно "подвешивает" компьютеры, эксплуатируя ошибку в сборке фрагментированных IP-пакетов.

Вредоносное программное обеспечение

Одним из опаснейших способов проведения атак является внедрение в атакуемые системы вредоносного программного обеспечения.

Мы выделим следующие грани вредоносного ПО:

- вредоносная функция;
- способ распространения;
- внешнее представление.

Часть, осуществляющую разрушительную функцию, будем называть "бомбой" (хотя, возможно, более удачными терминами были бы "заряд" или "боеголовка"). Вообще говоря, спектр вредоносных функций неограничен, поскольку "бомба", как и любая другая программа, может обладать сколь угодно сложной логикой, но обычно "бомбы" предназначаются для:

- внедрения другого вредоносного ПО;
- получения контроля над атакуемой системой;
- агрессивного потребления ресурсов;
- изменения или разрушения программ и/или данных.

По механизму распространения различают:

- вирусы – код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы;

- "черви" – код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение (для активизации вируса требуется запуск зараженной программы).

Вирусы обычно распространяются локально, в пределах узла сети; для передачи по сети им требуется внешняя помощь, такая как пересылка зараженного файла. "Черви", напротив, ориентированы в первую очередь на путешествия по сети.

Иногда само распространение вредоносного ПО вызывает агрессивное потребление ресурсов и, следовательно, является вредоносной функцией. Например, "черви" "съедают" полосу пропускания сети и ресурсы почтовых систем. По этой причине для атак на доступность они не нуждаются во встраивании специальных "бомб".

Вредоносный код, который выглядит как функционально полезная программа, называется троянским. Например, обычная программа, будучи пораженной вирусом, становится троянской; порой троянские программы изготавливают вручную и подсовывают доверчивым пользователям в какой-либо привлекательной упаковке.

Отметим, что данные нами определения и приведенная классификация вредоносного ПО отличаются от общепринятых. Например, в ГОСТ Р 51275-99 "Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения" содержится следующее определение:

"Программный вирус – это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах".

На наш взгляд, подобное определение неудачно, поскольку в нем смешаны функциональные и транспортные аспекты.

Окно опасности для вредоносного ПО появляется с выпуском новой разновидности "бомб", вирусов и/или "червей" и перестает существовать с обновлением базы данных антивирусных программ и наложением других необходимых заплат.

По традиции из всего вредоносного ПО наибольшее внимание общественности приходится на долю вирусов. Однако до марта 1999 года с полным правом можно было утверждать, что "несмотря на экспоненциальный рост числа известных вирусов, аналогичного роста количества инцидентов, вызванных ими, не зарегистрировано. Соблюдение несложных правил "компьютерной гигиены" практически сводит риск заражения к нулю. Там, где работают, а не играют, число зараженных компьютеров составляет лишь доли процента".

В марте 1999 года, с появлением вируса "Melissa", ситуация кардинальным образом изменилась. "Melissa" – это макровирус для файлов MS-Word, распространяющийся посредством электронной почты в присоединенных файлах. Когда такой (зараженный) присоединенный файл открывают, он рассылает свои копии по первым 50 адресам из адресной книги Microsoft Outlook. В результате почтовые серверы подвергаются атаке на доступность.

В данном случае нам хотелось бы отметить два момента.

1. Как уже говорилось, пассивные объекты отходят в прошлое; так называемое активное содержимое становится нормой. Файлы, которые по всем признакам должны были бы относиться к данным (например, документы в форматах MS-Word или Postscript, тексты почтовых сообщений), способны содержать интерпретируемые компоненты, которые могут запускаться неявным образом при открытии файла. Как и всякое в целом прогрессивное явление, такое "повышение активности данных" имеет свою оборотную сторону (в рассматриваемом случае – отставание в разработке механизмов безопасности и ошибки в их реализации). Обычные пользователи еще не скоро научатся применять интерпретируемые компоненты "в мирных целях" (или хотя бы узнают об их существовании), а перед злоумышленниками открылось по существу неограниченное поле деятельности. Как ни банально это звучит, но если для стрельбы по воробьям выкатывается пушка, то пострадает в основном стреляющий.
2. Интеграция разных сервисов, наличие среди них сетевых, всеобщая связность многократно увеличивают потенциал для атак на доступность, облегчают распространение вредоносного ПО (вирус "Melissa" – классический тому пример). Образно говоря, многие информационные системы, если не принять защитных мер, оказываются "в одной лодке" (точнее – в корабле без переборок), так что достаточно одной пробоины, чтобы "лодка" тут же пошла ко дну.

Как это часто бывает, вслед за "Melissa" появилась на свет целая серия вирусов, "червей" и их комбинаций: "Explorer.zip" (июнь 1999), "Bubble Boy" (ноябрь 1999), "ILOVEYOU" (май 2000) и т.д. Не то что бы от них был особенно большой ущерб, но общественный резонанс они вызвали немалый.

Активное содержимое, помимо интерпретируемых компонентов документов и других файлов данных, имеет еще одно популярное обличье – так называемые мобильные агенты. Это программы, которые загружаются на другие компьютеры и там выполняются. Наиболее известные примеры мобильных агентов – Java-апплеты, загружаемые на пользовательский компьютер и интерпретируемые Internet-навигаторами. Оказалось,

что разработать для них модель безопасности, оставляющую достаточно возможностей для полезных действий, не так-то просто; еще сложнее реализовать такую модель без ошибок. В августе 1999 года стали известны недочеты в реализации технологий ActiveX и Java в рамках Microsoft Internet Explorer, которые давали возможность размещать на Web-серверах вредоносные апплеты, позволяющие получать полный контроль над системой-визитером.

Для внедрения "бомб" часто используются ошибки типа "переполнение буфера", когда программа, работая с областью памяти, выходит за границы допустимого и записывает в нужные злоумышленнику места определенные данные. Так действовал еще в 1988 году знаменитый "червь Морриса"; в июне 1999 года хакеры нашли способ использовать аналогичный метод по отношению к Microsoft Internet Information Server (IIS), чтобы получить контроль над Web-сервером. Окно опасности охватило сразу около полутора миллионов серверных систем...

Не забыты современными злоумышленниками и испытанные троянские программы. Например, "троянцы" Back Orifice и Netbus позволяют получить контроль над пользовательскими системами с различными вариантами MS-Windows.

Таким образом, действие вредоносного ПО может быть направлено не только против доступности, но и против других основных аспектов информационной безопасности.

Основные угрозы целостности

На втором месте по размерам ущерба (после непреднамеренных ошибок и упущений) стоят кражи и подлоги. По данным газеты USA Today, еще в 1992 году в результате подобных противоправных действий с использованием персональных компьютеров американским организациям был нанесен общий ущерб в размере 882 миллионов долларов. Можно предположить, что реальный ущерб был намного больше, поскольку многие организации по понятным причинам скрывают такие инциденты; не вызывает сомнений, что в наши дни ущерб от такого рода действий вырос многократно.

В большинстве случаев виновниками оказывались штатные сотрудники организаций, отлично знакомые с режимом работы и мерами защиты. Это еще раз подтверждает опасность внутренних угроз, хотя говорят и пишут о них значительно меньше, чем о внешних.

Ранее мы проводили различие между статической и динамической целостностью. С целью нарушения статической целостности злоумышленник (как правило, штатный сотрудник) может:

- ввести неверные данные;
- изменить данные.

Иногда изменяются содержательные данные, иногда – служебная информация. Показательный случай нарушения целостности имел место в 1996 году. Служащая Oracle (личный секретарь вице-президента) предъявила судебный иск, обвиняя президента корпорации в незаконном увольнении после того, как она отвергла его ухаживания. В доказательство своей правоты женщина привела электронное письмо, якобы отправленное ее начальником президенту. Содержание письма для нас сейчас не важно; важно время отправки. Дело в том, что вице-президент предъявил, в свою очередь, файл с регистрационной информацией компании сотовой связи, из которого явствовало, что в указанное время он разговаривал по мобильному телефону, находясь вдалеке от своего рабочего места. Таким образом, в суде состоялось противостояние "файл против файла". Очевидно, один из них был фальсифицирован или изменен, то есть была нарушена его целостность. Суд решил, что подделали электронное письмо (секретарша знала пароль вице-президента, поскольку ей было поручено его менять), и иск был отвергнут...

(Теоретически возможно, что оба фигурировавших на суде файла были подлинными, корректными с точки зрения целостности, а письмо отправили пакетными средствами, однако, на наш взгляд, это было бы очень странное для вице-президента действие.)

Из приведенного случая можно сделать вывод не только об угрозах нарушения целостности, но и об опасности слепого доверия компьютерной информации. Заголовки электронного письма могут быть подделаны; письмо в целом может быть фальсифицировано лицом, знающим пароль отправителя (мы приводили соответствующие примеры). Отметим, что последнее возможно даже тогда, когда целостность контролируется криптографическими средствами. Здесь имеет место взаимодействие разных аспектов информационной безопасности: если нарушена конфиденциальность, может пострадать целостность.

Еще один урок: угрозой целостности является не только фальсификация или изменение данных, но и отказ от совершенных действий. Если нет средств обеспечить "неотказуемость", компьютерные данные не могут рассматриваться в качестве доказательства.

Потенциально уязвимы с точки зрения нарушения целостности не только данные, но и программы. Внедрение рассмотренного выше вредоносного ПО – пример подобного нарушения.

Угрозами динамической целостности являются нарушение атомарности транзакций, переупорядочение, кража, дублирование данных или внесение дополнительных сообщений (сетевых пакетов и т.п.). Соответствующие действия в сетевой среде называются активным прослушиванием.

Основные угрозы конфиденциальности

Конфиденциальную информацию можно разделить на предметную и служебную. Служебная информация (например, пароли пользователей) не относится к определенной предметной области, в информационной системе она играет техническую роль, но ее раскрытие особенно опасно, поскольку оно чревато получением несанкционированного доступа ко всей информации, в том числе предметной.

Даже если информация хранится в компьютере или предназначена для компьютерного использования, угрозы ее конфиденциальности могут носить некомпьютерный и вообще нетехнический характер.

Многим людям приходится выступать в качестве пользователей не одной, а целого ряда систем (информационных сервисов). Если для доступа к таким системам используются многоразовые пароли или иная конфиденциальная информация, то наверняка эти данные будут храниться не только в голове, но и в записной книжке или на листках бумаги, которые пользователь часто оставляет на рабочем столе, а то и попросту теряет. И дело здесь не в неорганизованности людей, а в изначальной непригодности парольной схемы. Невозможно помнить много разных паролей; рекомендации по их регулярной (по возможности – частой) смене только усугубляют положение, заставляя применять несложные схемы чередования или вообще стараться свести дело к двум-трем легко запоминаемым (и столь же легко угадываемым) паролям.

Описанный класс уязвимых мест можно назвать размещением конфиденциальных данных в среде, где им не обеспечена (зачастую – и не может быть обеспечена) необходимая защита. Угроза же состоит в том, что кто-то не откажется узнать секреты, которые сами просятся в руки. Помимо паролей, хранящихся в записных книжках пользователей, в этот класс попадает передача конфиденциальных данных в открытом виде (в разговоре, в письме, по сети), которая делает возможным перехват данных. Для атаки могут использоваться разные технические средства (подслушивание или прослушивание разговоров, пассивное прослушивание сети и т.п.), но идея одна – осуществить доступ к данным в тот момент, когда они наименее защищены.

Угрозу перехвата данных следует принимать во внимание не только при начальном конфигурировании ИС, но и, что очень важно, при всех изменениях. Весьма опасной угрозой являются... выставки, на которые многие организации, недолго думая, отправляют оборудование из производственной сети, со всеми хранящимися на них данными. Остаются прежними пароли, при удаленном доступе они продолжают передаваться в открытом виде. Это плохо даже в пределах защищенной сети организации; в объединенной сети выставки — это слишком суровое испытание честности всех участников.

Еще один пример изменения, о котором часто забывают, – хранение данных на резервных носителях. Для защиты данных на основных носителях применяются развитые системы управления доступом; копии же нередко просто лежат в шкафах и получить доступ к ним могут многие.

Перехват данных – очень серьезная угроза, и если конфиденциальность действительно является критичной, а данные передаются по многим каналам, их защита может оказаться весьма сложной и дорогостоящей. Технические средства перехвата хорошо проработаны, доступны, просты в эксплуатации, а установить их, например на кабельную сеть, может кто угодно, так что эту угрозу нужно принимать во внимание по отношению не только к внешним, но и к внутренним коммуникациям.

Кражи оборудования являются угрозой не только для резервных носителей, но и для компьютеров, особенно портативных. Часто ноутбуки оставляют без присмотра на работе или в автомобиле, иногда просто теряют.

Опасной нетехнической угрозой конфиденциальности являются методы морально-психологического воздействия, такие как маскарад – выполнение действий под видом лица, обладающего полномочиями для доступа к данным (см., например, статью Айрэ Винклера "Задание: шпионаж" в Jet Info, 1996, 19).

К неприятным угрозам, от которых трудно защищаться, можно отнести злоупотребление полномочиями. На многих типах систем привилегированный пользователь (например системный администратор) способен прочитать любой (незашифрованный) файл, получить доступ к почте любого пользователя и т.д. Другой пример – нанесение ущерба при сервисном обслуживании. Обычно сервисный инженер получает неограниченный доступ к оборудованию и имеет возможность действовать в обход программных защитных механизмов.

Таковы основные угрозы, которые наносят наибольший ущерб субъектам информационных отношений.

Вариант 1

1. Окно опасности — это:

- ☐ промежуток времени
- ☐ часть пространства
- ☐ плохо закрепленная деталь строительной конструкции

2. Самыми опасными угрозами являются:

- ☐ непреднамеренные ошибки штатных сотрудников
- ☐ вирусные инфекции
- ☐ атаки хакеров

3. Дублирование сообщений является угрозой:

- ☐ доступности
- ☐ конфиденциальности
- ☐ целостности

4. Melissa - это:

- ☐ бомба
- ☐ вирус
- ☐ червь

Вариант 2

1. Окно опасности появляется, когда:

- ☐ становится известно о средствах использования уязвимости
- ☐ появляется возможность использовать уязвимость
- ☐ устанавливается новое ПО

2. Самыми опасными источниками угроз являются:

- ☐ внутренние
- ☐ внешние
- ☐ пограничные

3. Перехват данных является угрозой:

- ☐ доступности
- ☐ конфиденциальности
- ☐ целостности

4. Melissa - это:

- ☐ макровирус для файлов MS-Word
- ☐ макровирус для файлов PDF
- ☐ макровирус для файлов Postscript

Вариант 3

1. Окно опасности перестает существовать, когда:

- ☐ администратор безопасности узнает об угрозе
- ☐ производитель ПО выпускает заплату
- ☐ заплата устанавливается в защищаемой ИС

2. Самыми опасными источниками внутренних угроз являются:

- ☐ некомпетентные руководители
- ☐ обиженные сотрудники
- ☐ любопытные администраторы

3. Агрессивное потребление ресурсов является угрозой:

- ☐ доступности
- ☐ конфиденциальности
- ☐ целостности

4. Melissa подвергает атаке на доступность:

- ☐ системы электронной коммерции;
- ☐ геоинформационные системы;
- ☐ системы электронной почты.

Лекция 4. Законодательный уровень информационной безопасности

Эта лекция посвящена российскому и зарубежному законодательству в области ИБ и проблемам, которые существуют в настоящее время в российском законодательстве.

Ключевые слова: комплексный подход к ИБ, законодательный уровень, ограничительные меры, направляющие и координирующие меры, право на информацию, право на личную и семейную тайну, банковская тайна, государственная тайна, коммерческая тайна, служебная тайна, средства защиты информации, информация, документированная информация, документ, информационные процессы, информационная система, информационные ресурсы, информация о гражданах, персональные данные, конфиденциальная информация, пользователь информации, лицензия, лицензируемый вид деятельности, лицензирование, лицензирующие органы, лицензиат, электронный документ, электронная цифровая подпись, владелец сертификата ключа подписи, средства электронной цифровой подписи, сертификат средств электронной цифровой подписи, закрытый ключ электронной цифровой подписи, открытый ключ электронной цифровой подписи, сертификат ключа подписи, подтверждение подлинности электронной цифровой подписи в электронном документе, пользователь сертификата ключа подписи, информационная система общего пользования, корпоративная информационная система, план обеспечения ИБ, программа безопасности, добровольный стандарт, анализ рисков, оценка уязвимостей, инфраструктура открытых ключей, резервная инфраструктура, защита персональных данных, субъект данных, ответственность, глобальные сети, нормативные документы.

Что такое законодательный уровень информационной безопасности и почему он важен

В деле обеспечения информационной безопасности успех может принести только комплексный подход. Мы уже указывали, что для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих уровней:

- законодательного;
- административного (приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами);

- процедурного (меры безопасности, ориентированные на людей);
- программно-технического.

Законодательный уровень является важнейшим для обеспечения информационной безопасности. Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это осуждается и/или наказывается обществом, потому, что так поступать не принято.

Мы будем различать на законодательном уровне две группы мер:

- меры, направленные на создание и поддержание в обществе негативного (в том числе с применением наказаний) отношения к нарушениям и нарушителям информационной безопасности (назовем их мерами ограничительной направленности);
- направляющие и координирующие меры, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности (меры созидательной направленности).

На практике обе группы мер важны в равной степени, но нам хотелось бы выделить аспект осознанного соблюдения норм и правил ИБ. Это важно для всех субъектов информационных отношений, поскольку рассчитывать только на защиту силами правоохранительных органов было бы наивно. Необходимо это и тем, в чьи обязанности входит наказывать нарушителей, поскольку обеспечить доказательность при расследовании и судебном разбирательстве компьютерных преступлений без специальной подготовки невозможно.

Самое важное (и, вероятно, самое трудное) на законодательном уровне – создать механизм, позволяющий согласовать процесс разработки законов с реалиями и прогрессом информационных технологий. Законы не могут опережать жизнь, но важно, чтобы отставание не было слишком большим, так как на практике, помимо прочих отрицательных моментов, это ведет к снижению информационной безопасности.

Обзор российского законодательства в области информационной безопасности

Правовые акты общего назначения, затрагивающие вопросы информационной безопасности

Основным законом Российской Федерации является Конституция, принятая 12 декабря 1993 года.

В соответствии со статьей 24 Конституции, органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и ма-

териалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Статья 41 гарантирует право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, статья 42 – право на знание достоверной информации о состоянии окружающей среды.

В принципе, право на информацию может реализовываться средствами бумажных технологий, но в современных условиях наиболее практичным и удобным для граждан является создание соответствующими законодательными, исполнительными и судебными органами информационных серверов и поддержание доступности и целостности представленных на них сведений, то есть обеспечение их (серверов) информационной безопасности.

Статья 23 Конституции гарантирует право на личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, статья 29 – право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Современная интерпретация этих положений включает обеспечение конфиденциальности данных, в том числе в процессе их передачи по компьютерным сетям, а также доступ к средствам защиты информации.

В Гражданском кодексе Российской Федерации (в своем изложении мы опираемся на редакцию от 15 мая 2001 года) фигурируют такие понятия, как банковская, коммерческая и служебная тайна. Согласно статье 139, информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности. Это подразумевает, как минимум, компетентность в вопросах ИБ и наличие доступных (и законных) средств обеспечения конфиденциальности.

Весьма продвинутым в плане информационной безопасности является Уголовный кодекс Российской Федерации (редакция от 14 марта 2002 года). Глава 28 – "Преступления в сфере компьютерной информации" – содержит три статьи:

- статья 272. Неправомерный доступ к компьютерной информации;
- статья 273. Создание, использование и распространение вредоносных программ для ЭВМ;
- статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Первая имеет дело с посягательствами на конфиденциальность, вторая – с вредоносным ПО, третья – с нарушениями доступности и целостности, повлекшими за собой уничтожение, блокирование или модифика-

цию охраняемой законом информации ЭВМ. Включение в сферу действия УК РФ вопросов доступности информационных сервисов представляется нам очень своевременным.

Статья 138 УК РФ, защищая конфиденциальность персональных данных, предусматривает наказание за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Аналогичную роль для банковской и коммерческой тайны играет статья 183 УК РФ.

Интересы государства в плане обеспечения конфиденциальности информации нашли наиболее полное выражение в Законе "О государственной тайне" (с изменениями и дополнениями от 6 октября 1997 года). В нем гостайна определена как защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Там же дается определение средств защиты информации. Согласно данному Закону, это технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну; средства, в которых они реализованы, а также средства контроля эффективности защиты информации. Подчеркнем важность последней части определения.

Закон "Об информации, информатизации и защите информации"

Основополагающим среди российских законов, посвященных вопросам информационной безопасности, следует считать закон "Об информации, информатизации и защите информации" от 20 февраля 1995 года номер 24-ФЗ (принят Государственной Думой 25 января 1995 года). В нем даются основные определения и намечаются направления развития законодательства в данной области.

Процитируем некоторые из этих определений:

- **информация** – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;
- **документированная информация (документ)** – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;
- **информационные процессы** – процессы сбора, обработки, накопления, хранения, поиска и распространения информации;
- **информационная система** – организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы;

- **информационные ресурсы** – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);
- **информация о гражданах (персональные данные)** – сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;
- **конфиденциальная информация** – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации;
- **пользователь (потребитель) информации** – субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

Мы, разумеется, не будем обсуждать качество данных в Законе определений. Обратим лишь внимание на гибкость определения конфиденциальной информации, которая не сводится к сведениям, составляющим государственную тайну, а также на понятие персональных данных, закладывающее основу защиты последних.

Закон выделяет следующие цели защиты информации:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- предотвращение угроз безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
- предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
- сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;
- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Отметим, что Закон на первое место ставит сохранение конфиденциальности информации. Целостность представлена также достаточно полно, хотя и на втором месте. О доступности ("предотвращение несанк-

ционированных действий по ... блокированию информации") сказано довольно мало.

Продолжим цитирование:

"Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу".

По сути, это положение констатирует, что защита информации направлена на обеспечение интересов субъектов информационных отношений.

Далее. "Режим защиты информации устанавливается:

- в отношении сведений, отнесенных к государственной тайне, – уполномоченными органами на основании Закона Российской Федерации "О государственной тайне";
- в отношении конфиденциальной документированной информации – собственником информационных ресурсов или уполномоченным лицом на основании настоящего Федерального закона;
- в отношении персональных данных – федеральным законом."

Здесь явно выделены три вида защищаемой информации, ко второму из которых принадлежит, в частности, коммерческая информация. Поскольку защите подлежит только документированная информация, необходимым условием является фиксация коммерческой информации на материальном носителе и снабжение ее реквизитами. Отметим, что в данном месте Закона речь идет только о конфиденциальности; остальные аспекты ИБ забыты.

Обратим внимание, что защиту государственной тайны и персональных данных берет на себя государство; за другую конфиденциальную информацию отвечают ее собственники.

Как же защищать информацию? В качестве основного закон предлагает для этой цели мощные универсальные средства: лицензирование и сертификацию. Процитируем статью 19.

1. Информационные системы, базы и банки данных, предназначенные для информационного обслуживания граждан и организаций, подлежат сертификации в порядке, установленном Законом Российской Федерации "О сертификации продукции и услуг".
2. Информационные системы органов государственной власти Российской Федерации и органов государственной власти субъектов Российской Федерации, других государственных органов, организаций, которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих систем подлежат обязательной сертификации. Порядок сертификации определяется законодательством Российской Федерации.

3. Организации, выполняющие работы в области проектирования, производства средств защиты информации и обработки персональных данных, получают лицензии на этот вид деятельности. Порядок лицензирования определяется законодательством Российской Федерации.
4. Интересы потребителя информации при использовании импортной продукции в информационных системах защищаются таможенными органами Российской Федерации на основе международной системы сертификации.

Здесь трудно удержаться от риторического вопроса: а есть ли в России информационные системы без импортной продукции? Получается, что на защите интересов потребителей стоит в данном случае только таможня...

И еще несколько пунктов, теперь из статьи 22:

2. Владелец документов, массива документов, информационных систем обеспечивает уровень защиты информации в соответствии с законодательством Российской Федерации.
3. Риск, связанный с использованием несертифицированных информационных систем и средств их обеспечения, лежит на собственнике (владельце) этих систем и средств. Риск, связанный с использованием информации, полученной из несертифицированной системы, лежит на потребителе информации.
4. Собственник документов, массива документов, информационных систем может обращаться в организации, осуществляющие сертификацию средств защиты информационных систем и информационных ресурсов, для проведения анализа достаточности мер защиты его ресурсов и систем и получения консультаций.
5. Владелец документов, массива документов, информационных систем обязан оповещать собственника информационных ресурсов и (или) информационных систем о всех фактах нарушения режима защиты информации.

Из пункта 5 следует, что должны обнаруживаться все (успешные) атаки на ИС. Вспомним в этой связи один из результатов опроса (см. лекцию 1): около трети респондентов-американцев не знали, были ли взломаны их ИС за последние 12 месяцев. По нашему законодательству их можно было бы привлечь к ответственности...

Далее, статья 23 "Защита прав субъектов в сфере информационных процессов и информатизации" содержит следующий пункт:

2. Защита прав субъектов в указанной сфере осуществляется судом, арбитражным судом, третейским судом с учетом специфики правонарушений и нанесенного ущерба.

Очень важными являются пункты статьи 5, касающиеся юридической силы электронного документа и электронной цифровой подписи:

3. Юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных информационных и телекоммуникационных систем, может подтверждаться электронной цифровой подписью.

   Юридическая сила электронной цифровой подписи признается при наличии в автоматизированной информационной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдении установленного режима их использования.
4. Право удостоверять идентичность электронной цифровой подписи осуществляется на основании лицензии. Порядок выдачи лицензий определяется законодательством Российской Федерации.

Таким образом, Закон предлагает действенное средство контроля целостности и решения проблемы "неотказуемости" (невозможности отказаться от собственной подписи).

Таковы важнейшие, на наш взгляд, положения Закона "Об информации, информатизации и защите информации". На следующей странице будут рассмотрены другие законы РФ в области информационной безопасности.

Другие законы и нормативные акты

Следуя логике Закона "Об информации, информатизации и защите информации", мы продолжим наш обзор Законом "О лицензировании отдельных видов деятельности" от 8 августа 2001 года номер 128-ФЗ (Принят Государственной Думой 13 июля 2001 года). Начнем с основных определений.

"Лицензия – специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю.

Лицензируемый вид деятельности – вид деятельности, на осуществление которого на территории Российской Федерации требуется получение лицензии в соответствии с настоящим Федеральным законом.

Лицензирование – мероприятия, связанные с предоставлением лицензий, переоформлением документов, подтверждающих наличие лицензий, приостановлением и возобновлением действия лицензий, аннулированием лицензий и контролем лицензирующих органов за соблюдением лицензиатами при осуществлении лицензируемых видов деятельности соответствующих лицензионных требований и условий.

Лицензирующие органы – федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации, осуществляющие лицензирование в соответствии с настоящим Федеральным законом.

Лицензиат – юридическое лицо или индивидуальный предприниматель, имеющие лицензию на осуществление конкретного вида деятельности."

Статья 17 Закона устанавливает перечень видов деятельности, на осуществление которых требуются лицензии. Нас будут интересовать следующие виды:

- распространение шифровальных (криптографических) средств;
- техническое обслуживание шифровальных (криптографических) средств;
- предоставление услуг в области шифрования информации;
- разработка и производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;
- выдача сертификатов ключей электронных цифровых подписей, регистрация владельцев электронных цифровых подписей, оказание услуг, связанных с использованием электронных цифровых подписей и подтверждением подлинности электронных цифровых подписей;
- выявление электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- разработка и (или) производство средств зашиты конфиденциальной информации;
- техническая защита конфиденциальной информации;
- разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность.

Необходимо учитывать, что, согласно статье 1, действие данного Закона не распространяется на следующие виды деятельности:

- деятельность, связанная с защитой государственной тайны;
- деятельность в области связи;
- образовательная деятельность.

Подчеркнем в этой связи, что данный Закон не препятствует организации Интернет-Университетом учебных курсов по информационной безопасности (не требует получения специальной лицензии; ранее подобная лицензия была необходима). В свою очередь, Федеральный Закон "Об образовании" не содержит каких-либо специальных положений, касающихся образовательной деятельности в области ИБ.

Основными лицензирующими органами в области защиты информации являются Федеральное агентство правительственной связи и информации (ФАПСИ) и Гостехкомиссия России. ФАПСИ ведает всем, что связано с криптографией, Гостехкомиссия лицензирует деятельность по защите конфиденциальной информации. Эти же организации возглавляют работы по сертификации средств соответствующей направленности. Кроме того, ввоз и вывоз средств криптографической защиты информации (шифровальной техники) и нормативно-технической документации к ней может осуществляться исключительно на основании лицензии Министерства внешних экономических связей Российской Федерации, выдаваемой на основании решения ФАПСИ. Все эти вопросы регламентированы соответствующими указами Президента и постановлениями Правительства РФ, которые мы здесь перечислять не будем.

В эпоху глобальных коммуникаций важную роль играет Закон "Об участии в международном информационном обмене" от 4 июля 1996 года номер 85-ФЗ (принят Государственной Думой 5 июня 1996 года). В нем, как и в Законе "Об информации...", основным защитным средством являются лицензии и сертификаты. Процитируем несколько пунктов из статьи 9.

2. Защита конфиденциальной информации государством распространяется только на ту деятельность по международному информационному обмену, которую осуществляют физические и юридические лица, обладающие лицензией на работу с конфиденциальной информацией и использующие сертифицированные средства международного информационного обмена.

   Выдача сертификатов и лицензий возлагается на Комитет при Президенте Российской Федерации по политике информатизации, Государственную техническую комиссию при Президенте Российской Федерации, Федеральное агентство правительственной связи и информации при Президенте Российской Федерации. Порядок выдачи сертификатов и лицензий устанавливается Правительством Российской Федерации.

3. При обнаружении нештатных режимов функционирования средств международного информационного обмена, то есть возникновения ошибочных команд, а также команд, вызванных несанкционированными действиями обслуживающего персонала или иных лиц, либо ложной информацией собственник или владелец этих средств должен своевременно сообщить об этом в органы контроля за осуществлением международного информационного обмена и собственнику или владельцу взаимодействующих средств международного информационного обмена, в противном случае он несет ответственность за причиненный ущерб.

При желании здесь можно усмотреть обязательность выявления нарушителя информационной безопасности – положение, вне всяких сомнений, очень важное и прогрессивное.

Еще одна цитата – теперь из статьи 17 того же Закона.

Статья 17: "Сертификация информационных продуктов, информационных услуг, средств международного информационного обмена.

1. При ввозе информационных продуктов, информационных услуг в Российскую Федерацию импортер представляет сертификат, гарантирующий соответствие данных продуктов и услуг требованиям договора. В случае невозможности сертификации ввозимых на территорию Российской Федерации информационных продуктов, информационных услуг ответственность за использование данных продуктов и услуг лежит на импортере.
2. Средства международного информационного обмена, которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих средств подлежат обязательной сертификации.
3. Сертификация сетей связи производится в порядке, определяемом Федеральным законом "О связи"."

Читая пункт 2, трудно удержаться от вопроса: "А нужно ли сертифицировать средства защиты средств защиты этих средств?" Ответ, конечно, положительный...

10 января 2002 года Президентом был подписан очень важный закон "Об электронной цифровой подписи" номер 1-ФЗ (принят Государственной Думой 13 декабря 2001 года), развивающий и конкретизирующий приведенные выше положения закона "Об информации...". Его роль поясняется в статье 1.

1. Целью настоящего Федерального закона является обеспечение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.
2. Действие настоящего Федерального закона распространяется на отношения, возникающие при совершении гражданско-правовых сделок и в других предусмотренных законодательством Российской Федерации случаях. Действие настоящего Федерального закона не распространяется на отношения, возникающие при использовании иных аналогов собственноручной подписи.

Закон вводит следующие основные понятия:

Электронный документ – документ, в котором информация представлена в электронно-цифровой форме.

Электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Владелец сертификата ключа подписи – физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).

Средства электронной цифровой подписи – аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.

Сертификат средств электронной цифровой подписи – документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям.

Закрытый ключ электронной цифровой подписи – уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.

Открытый ключ электронной цифровой подписи – уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.

Сертификат ключа подписи – документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.

Подтверждение подлинности электронной цифровой подписи в электронном документе – положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе.

Пользователь сертификата ключа подписи – физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи.

Информационная система общего пользования – информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.

Корпоративная информационная система – информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

Пересказать такие определения своими словами невозможно... Обратим внимание на неоднозначное использование термина "сертификат", которое, впрочем, не должно привести к путанице. Кроме того, данное здесь определение электронного документа слабее, чем в Законе "Об информации...", поскольку нет упоминания реквизитов.

Согласно Закону, электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

- сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
- подтверждена подлинность электронной цифровой подписи в электронном документе;
- электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

Закон определяет сведения, которые должен содержать сертификат ключа подписи:

- уникальный регистрационный номер сертификата ключа подписи, даты начала и окончания срока действия сертификата ключа подписи, находящегося в реестре удостоверяющего центра;
- фамилия, имя и отчество владельца сертификата ключа подписи или псевдоним владельца. В случае использования псевдо-

нима запись об этом вносится удостоверяющим центром в сертификат ключа подписи;
- открытый ключ электронной цифровой подписи;
- наименование средств электронной цифровой подписи, с которыми используется данный открытый ключ электронной цифровой подписи;
- наименование и местонахождение удостоверяющего центра, выдавшего сертификат ключа подписи;
- сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение.

Интересно, много ли Федеральных законов, содержащих такое количество технической информации и столь зависимых от конкретной технологии?

На этом мы заканчиваем обзор законов РФ, относящихся к информационной безопасности.

Обзор зарубежного законодательства в области информационной безопасности

Конечно, излишняя амбициозность заголовка очевидна. Разумеется, мы лишь пунктиром очертим некоторые законы нескольких стран (в первую очередь – США), поскольку только в США таких законодательных актов около 500.

Ключевую роль играет американский "Закон об информационной безопасности" (Computer Security Act of 1987, Public Law 100-235 (H.R. 145), January 8, 1988). Его цель – реализация минимально достаточных действий по обеспечению безопасности информации в федеральных компьютерных системах, без ограничений всего спектра возможных действий.

Характерно, что уже в начале Закона называется конкретный исполнитель – Национальный институт стандартов и технологий (НИСТ), отвечающий за выпуск стандартов и руководств, направленных на защиту от уничтожения и несанкционированного доступа к информации, а также от краж и подлогов, выполняемых с помощью компьютеров. Таким образом, имеется в виду как регламентация действий специалистов, так и повышение информированности всего общества.

Согласно Закону, все операторы федеральных ИС, содержащих конфиденциальную информацию, должны сформировать планы обеспечения ИБ. Обязательным является и периодическое обучение всего персонала таких ИС. НИСТ, в свою очередь, обязан проводить исследования природы и масштаба уязвимых мест, вырабатывать экономически оправданные меры защиты. Результаты исследований рассчитаны на применение не только в государственных системах, но и в частном секторе.

Закон обязывает НИСТ координировать свою деятельность с другими министерствами и ведомствами, включая Министерство обороны, Министерство энергетики, Агентство национальной безопасности (АНБ) и т.д., чтобы избежать дублирования и несовместимости.

Помимо регламентации дополнительных функций НИСТ, Закон предписывает создать при Министерстве торговли комиссию по информационной безопасности, которая должна:

- выявлять перспективные управленческие, технические, административные и физические меры, способствующие повышению ИБ;
- выдавать рекомендации Национальному институту стандартов и технологий, доводить их до сведения всех заинтересованных ведомств.

С практической точки зрения важен раздел 6 Закона, обязывающий все правительственные ведомства сформировать план обеспечения информационной безопасности, направленный на то, чтобы компенсировать риски и предотвратить возможный ущерб от утери, неправильного использования, несанкционированного доступа или модификации информации в федеральных системах. Копии плана направляются в НИСТ и АНБ.

В 1997 году появилось продолжение описанного закона – законопроект "О совершенствовании информационной безопасности" (Computer Security Enhancement Act of 1997, H.R. 1903), направленный на усиление роли Национального института стандартов и технологий и упрощение операций с криптосредствами.

В законопроекте констатируется, что частный сектор готов предоставить криптосредства для обеспечения конфиденциальности и целостности (в том числе аутентичности) данных, что разработка и использование шифровальных технологий должны происходить на основании требований рынка, а не распоряжений правительства. Кроме того, здесь отмечается, что за пределами США имеются сопоставимые и общедоступные криптографические технологии, и это следует учитывать при выработке экспортных ограничений, чтобы не снижать конкурентоспособность американских производителей аппаратного и программного обеспечения.

Для защиты федеральных ИС рекомендуется более широко применять технологические решения, основанные на разработках частного сектора. Кроме того, предлагается оценить возможности общедоступных зарубежных разработок.

Очень важен раздел 3, в котором от НИСТ требуется по запросам частного сектора готовить добровольные стандарты, руководства, средства и методы для инфраструктуры открытых ключей (см. выше Закон РФ об

ЭЦП), позволяющие сформировать негосударственную инфраструктуру, пригодную для взаимодействия с федеральными ИС.

В разделе 4 особое внимание обращается на необходимость анализа средств и методов оценки уязвимых мест других продуктов частного сектора в области ИБ.

Приветствуется разработка правил безопасности, нейтральных по отношению к конкретным техническим решениям, использование в федеральных ИС коммерческих продуктов, участие в реализации шифровальных технологий, позволяющее в конечном итоге сформировать инфраструктуру, которую можно рассматривать как резервную для федеральных ИС.

Важно, что в соответствии с разделами 10 и далее предусматривается выделение конкретных (и немалых) сумм, называются точные сроки реализации программ партнерства и проведения исследований инфраструктуры с открытыми ключами, национальной инфраструктуры цифровых подписей. В частности, предусматривается, что для удостоверяющих центров должны быть разработаны типовые правила и процедуры, порядок лицензирования, стандарты аудита.

В 2001 году был одобрен Палатой представителей и передан в Сенат новый вариант рассмотренного законопроекта – Computer Security Enhancement Act of 2001 (H.R. 1259 RFS). В этом варианте примечательно как то, что, по сравнению с предыдущей редакцией, было убрано, так и то, что добавилось.

За четыре года (1997-2001 гг.) на законодательном и других уровнях информационной безопасности США было сделано многое. Смягчены экспортные ограничения на криптосредства (в январе 2000 г.). Сформирована инфраструктура с открытыми ключами. Разработано большое число стандартов (например, новый стандарт электронной цифровой подписи – FIPS 186-2, январь 2000 г.). Все это позволило не заострять более внимания на криптографии как таковой, а сосредоточиться на одном из ее важнейших приложений – аутентификации, рассматривая ее по отработанной на криптосредствах методике. Очевидно, что, независимо от судьбы законопроекта, в США будет сформирована национальная инфраструктура электронной аутентификации. В данном случае законотворческая деятельность идет в ногу с прогрессом информационных технологий.

Программа безопасности, предусматривающая экономически оправданные защитные меры и синхронизированная с жизненным циклом ИС, упоминается в законодательстве США неоднократно. Согласно пункту 3534 ("Обязанности федеральных ведомств") подглавы II ("Информационная безопасность") главы 35 ("Координация федеральной информационной политики") рубрики 44 ("Общественные издания и документы"), такая программа должна включать:

- периодическую оценку рисков с рассмотрением внутренних и внешних угроз целостности, конфиденциальности и доступности систем, а также данных, ассоциированных с критически важными операциями и ресурсами;
- правила и процедуры, позволяющие, опираясь на проведенный анализ рисков, экономически оправданным образом уменьшить риски до приемлемого уровня;
- обучение персонала с целью информирования о существующих рисках и об обязанностях, выполнение которых необходимо для их (рисков) нейтрализации;
- периодическую проверку и (пере)оценку эффективности правил и процедур;
- действия при внесении существенных изменений в систему;
- процедуры выявления нарушений информационной безопасности и реагирования на них; эти процедуры должны помочь уменьшить риски, избежать крупных потерь; организовать взаимодействие с правоохранительными органами.

Конечно, в законодательстве США имеются в достаточном количестве и положения ограничительной направленности, и директивы, защищающие интересы таких ведомств, как Министерство обороны, АНБ, ФБР, ЦРУ, но мы не будем на них останавливаться. Желающие могут прочитать раздел "Законодательная база в области защиты информации" в превосходной статье О. Беззубцева и А. Ковалева "О лицензировании и сертификации в области защиты информации" (Jet Info, 1997, 4).

В законодательстве ФРГ выделим весьма развернутый (44 раздела) Закон о защите данных (Federal Data Protection Act of December 20, 1990 (BGBl.I 1990 S.2954), amended by law of September 14, 1994 (BGBl. I S. 2325)). Он целиком посвящен защите персональных данных.

Как, вероятно, и во всех других законах аналогичной направленности, в данном случае устанавливается приоритет интересов национальной безопасности над сохранением тайны частной жизни. В остальном права личности защищены весьма тщательно. Например, если сотрудник фирмы обрабатывает персональные данные в интересах частных компаний, он дает подписку о неразглашении, которая действует и после перехода на другую работу.

Государственные учреждения, хранящие и обрабатывающие персональные данные, несут ответственность за нарушение тайны частной жизни "субъекта данных", как говорится в Законе. В материальном выражении ответственность ограничена верхним пределом в 250 тысяч немецких марок.

Из законодательства Великобритании упомянем семейство так называемых добровольных стандартов BS 7799, помогающих организациям на практике сформировать программы безопасности. В последующих

лекциях мы еще вернемся к рассмотрению этих стандартов; здесь же отметим, что они действительно работают, несмотря на "добровольность" (или благодаря ей?).

В современном мире глобальных сетей законодательная база должна быть согласована с международной практикой. В этом плане поучителен пример Аргентины. В конце марта 1996 года компетентными органами Аргентины был арестован Хулио Цезар Ардита, 21 года, житель Буэнос-Айреса, системный оператор электронной доски объявлений "Крик", известный в компьютерном подполье под псевдонимом "El Griton". Ему вменялись в вину систематические вторжения в компьютерные системы ВМС США, НАСА, многих крупнейших американских университетов, а также в компьютерные системы Бразилии, Чили, Кореи, Мексики и Тайваня. Однако, несмотря на тесное сотрудничество компетентных органов Аргентины и США, Ардита был отпущен без официального предъявления обвинений, поскольку по аргентинскому законодательству вторжение в компьютерные системы не считается преступлением. Кроме того, в силу принципа "двойной криминальности", действующего в международных правовых отношениях, Аргентина не может выдать хакера американским властям. Дело Ардита показывает, каким может быть будущее международных компьютерных вторжений при отсутствии всеобщих или хотя бы двусторонних соглашений о борьбе с компьютерной преступностью.

О текущем состоянии российского законодательства в области информационной безопасности

Как уже отмечалось, самое важное (и, вероятно, самое трудное) на законодательном уровне – создать механизм, позволяющий согласовать процесс разработки законов с реалиями и прогрессом информационных технологий. Пока такого механизма нет и, увы, не предвидится. Сейчас бессмысленно задаваться вопросом, чего не хватает российскому законодательству в области ИБ, это все равно что интересоваться у пунктирного отрезка, чего тому не хватает, чтобы покрыть всю плоскость. Даже чисто количественное сопоставление с законодательством США показывает, что наша законодательная база явно неполна.

Справедливости ради необходимо отметить, что ограничительная составляющая в российском законодательстве представлена существенно лучше, чем координирующая и направляющая. Глава 28 Уголовного кодекса достаточно полно охватывает основные аспекты информационной безопасности, однако обеспечить реализацию соответствующих статей пока еще сложно.

Положения базового Закона "Об информации, информатизации и защите информации" носят весьма общий характер, а основное содержа-

ние статей, посвященных информационной безопасности, сводится к необходимости использовать исключительно сертифицированные средства, что, в общем, правильно, но далеко не достаточно. Характерно, что Закон разъясняет вопросы ответственности в случае использования несертифицированных средств, но что делать, если нарушение ИБ произошло в системе, построенной строго по правилам? Кто возместит ущерб субъектам информационных отношений? Поучителен в этом отношении рассмотренный выше закон ФРГ о защите данных.

Законодательством определены органы, ведающие лицензированием и сертификацией. (Отметим в этой связи, что Россия – одна из немногих стран (в список еще входят Вьетнам, Китай, Пакистан), сохранивших жесткий государственный контроль за производством и распространением внутри страны средств обеспечения ИБ, в особенности продуктов криптографических технологий.) Но кто координирует, финансирует и направляет проведение исследований в области ИБ, разработку отечественных средств защиты, адаптацию зарубежных продуктов? Законодательством США определена главная ответственная организация – НИСТ, которая исправно выполняет свою роль. В Великобритании имеются содержательные добровольные стандарты ИБ, помогающие организациям всех размеров и форм собственности. У нас пока ничего такого нет.

В области информационной безопасности законы реально преломляются и работают через нормативные документы, подготовленные соответствующими ведомствами. В этой связи очень важны Руководящие документы Гостехкомиссии России, определяющие требования к классам защищенности средств вычислительной техники и автоматизированных систем. Особенно выделим утвержденный в июле 1997 года Руководящий документ по межсетевым экранам, вводящий в официальную сферу один из самых современных классов защитных средств.

В современном мире глобальных сетей нормативно-правовая база должна быть согласована с международной практикой. Особое внимание следует обратить на то, что желательно привести российские стандарты и сертификационные нормативы в соответствие с международным уровнем информационных технологий вообще и информационной безопасности в частности. Есть целый ряд оснований для того, чтобы это сделать. Одно из них – необходимость защищенного взаимодействия с зарубежными организациями и зарубежными филиалами российских компаний. Второе (более существенное) – доминирование аппаратно-программных продуктов зарубежного производства.

На законодательном уровне должен быть решен вопрос об отношении к таким изделиям. Здесь необходимо выделить два аспекта: независимость в области информационных технологий и информационную безопасность. Использование зарубежных продуктов в некоторых критически

важных системах (в первую очередь, военных), в принципе, может представлять угрозу национальной безопасности (в том числе информационной), поскольку нельзя исключить вероятности встраивания закладных элементов. В то же время, в подавляющем большинстве случаев потенциальные угрозы информационной безопасности носят исключительно внутренний характер. В таких условиях незаконность использования зарубежных разработок (ввиду сложностей с их сертификацией) при отсутствии отечественных аналогов затрудняет (или вообще делает невозможной) защиту информации без серьезных на то оснований.

Проблема сертификации аппаратно-программных продуктов зарубежного производства действительно сложна, однако, как показывает опыт европейских стран, решить ее можно. Сложившаяся в Европе система сертификации по требованиям информационной безопасности позволила оценить операционные системы, системы управления базами данных и другие разработки американских компаний. Вхождение России в эту систему и участие российских специалистов в сертификационных испытаниях в состоянии снять имеющееся противоречие между независимостью в области информационных технологий и информационной безопасностью без какого-либо ущерба для национальной безопасности.

Подводя итог, можно наметить следующие основные направления деятельности на законодательном уровне:

- разработка новых законов с учетом интересов всех категорий субъектов информационных отношений;
- обеспечение баланса созидательных и ограничительных (в первую очередь преследующих цель наказать виновных) законов;
- интеграция в мировое правовое пространство;
- учет современного состояния информационных технологий.

Вариант 1

1. Уголовный кодекс РФ не предусматривает наказания за:

- ☐ неправомерный доступ к компьютерной информации
- ☐ создание, использование и распространение вредоносных программ
- ☐ массовую рассылку незапрошенной рекламной информации.

2. Согласно Закону "Об информации, информатизации и защите информации", персональные данные — это:

- ☐ сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность
- ☐ данные, хранящиеся в персональном компьютере
- ☐ данные, находящиеся в чьей-либо персональной собственности

3. Согласно Закону "О лицензировании отдельных видов деятельности", лицензия — это:

- ☐ специальное разрешение на осуществление конкретного вида деятельности
- ☐ удостоверение, подтверждающее высокое качество изделия
- ☐ документ, гарантирующий безопасность программного продукта

4. В законопроекте "О совершенствовании информационной безопасности" (США, 2001 год) особое внимание обращено на:

- ☐ системы электронной коммерции
- ☐ инфраструктуру для электронных цифровых подписей
- ☐ средства электронной аутентификации

Вариант 2

1. Уголовный кодекс РФ не предусматривает наказания за:

- ☐ увлечение компьютерными играми в рабочее время
- ☐ неправомерный доступ к компьютерной информации
- ☐ нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

2. Согласно Закону "Об информации, информатизации и защите информации", конфиденциальная информация — это:

- ☐ информация с грифом "секретно"
- ☐ документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации
- ☐ информация, доступ к которой ограничивается сертифицированными техническими средствами

3. Действие Закона "О лицензировании отдельных видов деятельности" не распространяется на:

- ☐ деятельность по технической защите конфиденциальной информации
- ☐ образовательную деятельность в области защиты информации
- ☐ предоставление услуг в области шифрования информации

4. В следующих странах сохранилось жесткое государственное регулирование разработки и распространения криптосредств на внутреннем рынке:

- ☐ Китай
- ☐ Россия
- ☐ Франция

Вариант 3

1. Уголовный кодекс РФ не предусматривает наказания за:

- ☐ создание, использование и распространение вредоносных программ
- ☐ ведение личной корреспонденции на производственной технической базе
- ☐ нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

2. Согласно Закону "Об информации, информатизации и защите информации", риск, связанный с использованием информации, полученной из несертифицированной системы, лежит на:

- ☐ владельце этой системы
- ☐ собственнике документов
- ☐ потребителе информации

3. Действие Закона "О лицензировании отдельных видов деятельности" распространяется на:

- ☐ деятельность по использованию шифровальных (криптографических) средств
- ☐ деятельность по рекламированию шифровальных (криптографических) средств
- ☐ деятельность по распространению шифровальных (криптографических) средств

4. В законопроекте "О совершенствовании информационной безопасности" (США, 2001 год) особое внимание обращено на:

- ☐ смягчение ограничений на экспорт криптосредств
- ☐ разработку средств электронной аутентификации
- ☐ создание инфраструктуры с открытыми ключами

Лекция 5. Стандарты и спецификации в области информационной безопасности

Дается обзор международных и национальных стандартов и спецификаций в области ИБ – от "Оранжевой книги" до ISO 15408. Демонстрируются как сильные, так и слабые стороны этих документов.

Ключевые слова: безопасная система, доверенная система, степень доверия, политика безопасности, уровень гарантированности, подотчетность, доверенная вычислительная база, монитор обращений, изолированность, полнота, верифицируемость, ядро безопасности, периметр безопасности, произвольное (дискреционное) управление доступом, принудительное (мандатное) управление доступом, безопасность повторного использования объектов, метки безопасности, идентификация, аутентификация, предоставление доверенного пути, анализ регистрационной информации (аудит), операционная гарантированность, технологическая гарантированность, тайный канал передачи информации, жизненный цикл системы, проектирование, реализация, тестирование, продажа, сопровождение, класс безопасности, изоляция процессов, разделение адресных пространств, списки управления доступом, администратор безопасности, восстановление после сбоя, формальные спецификации верхнего уровня, верификация, эталонная семиуровневая модель, аутентификация партнеров по общению, аутентификация источника данных, управление доступом, конфиденциальность данных, конфиденциальность трафика, избирательная конфиденциальность, целостность с восстановлением, избирательная целостность, неотказуемость, шифрование, электронная цифровая подпись, дополнение трафика, управление маршрутизацией, нотаризация, администрирование средств безопасности, реагирование, аудит, безопасное восстановление, генерация криптографических ключей, распределение криптографических ключей, управление шифрованием, общие критерии, требования безопасности, параметризация требований, функциональные требования, требования доверия безопасности, объект оценки, цели безопасности, среда безопасности, класс, семейство, компонент, элемент, профиль защиты, задание по безопасности, функциональный пакет, защита данных пользователя, защита функций безопасности, управление безопасностью, аудит безопасности, доступ к объекту оценки, криптографическая поддержка, связь, доверенный маршрут/канал,

приватность, анонимность, псевдонимность, невозможность ассоциации, скрытность, использование ресурсов, отказоустойчивость, обслуживание по приоритетам, распределение ресурсов, доверие безопасности, разработчик, свидетельство, оценщик, оценка уязвимостей, поставка и эксплуатация, поддержка доверия, функциональные спецификации, проект верхнего уровня, проект нижнего уровня, демонстрация соответствия, модель политики безопасности, спонсор, конфиденциальность, целостность, доступность, система, продукт, функция безопасности, сервис безопасности, механизм безопасности, эффективность, корректность, мощность, сетевая доверенная вычислительная база, криптография, избыточность, реконфигурирование, рассредоточенность управления, единая точка отказа, нейтрализация отказов, подсеть, изоляция пользователей, автоматизированная система, защита от несанкционированного доступа, межсетевой экран, фильтрация информации.

Оценочные стандарты и технические спецификации. "Оранжевая книга" как оценочный стандарт

Основные понятия

Мы приступаем к обзору стандартов и спецификаций двух разных видов:

- оценочных стандартов, направленных на классификацию информационных систем и средств защиты по требованиям безопасности;
- технических спецификаций, регламентирующих различные аспекты реализации средств защиты.

Важно отметить, что между эти видами нормативных документов нет глухой стены. Оценочные стандарты выделяют важнейшие, с точки зрения ИБ, аспекты ИС, играя роль архитектурных спецификаций. Другие технические спецификации определяют, как строить ИС предписанной архитектуры.

Исторически первым оценочным стандартом, получившим широкое распространение и оказавшим огромное влияние на базу стандартизации ИБ во многих странах, стал стандарт Министерства обороны США "Критерии оценки доверенных компьютерных систем".

Данный труд, называемый чаще всего по цвету обложки "Оранжевой книгой", был впервые опубликован в августе 1983 года. Уже одно его название требует комментария. Речь идет не о безопасных, а о доверенных

системах, то есть системах, которым можно оказать определенную степень доверия.

"Оранжевая книга" поясняет понятие безопасной системы, которая "управляет, с помощью соответствующих средств, доступом к информации, так что только должным образом авторизованные лица или процессы, действующие от их имени, получают право читать, записывать, создавать и удалять информацию".

Очевидно, однако, что абсолютно безопасных систем не существует, это абстракция. Есть смысл оценивать лишь степень доверия, которое можно оказать той или иной системе.

В "Оранжевой книге" доверенная система определяется как "система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа".

Обратим внимание, что в рассматриваемых Критериях и безопасность, и доверие оцениваются исключительно с точки зрения управления доступом к данным, что является одним из средств обеспечения конфиденциальности и целостности (статической). Вопросы доступности "Оранжевая книга" не затрагивает.

Степень доверия оценивается по двум основным критериям.

1. **Политика безопасности** – набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. В частности, правила определяют, в каких случаях пользователь может оперировать конкретными наборами данных. Чем выше степень доверия системе, тем строже и многообразнее должна быть политика безопасности. В зависимости от сформулированной политики можно выбирать конкретные механизмы обеспечения безопасности. Политика безопасности – это активный аспект защиты, включающий в себя анализ возможных угроз и выбор мер противодействия.
2. **Уровень гарантированности** – мера доверия, которая может быть оказана архитектуре и реализации ИС. Доверие безопасности может проистекать как из анализа результатов тестирования, так и из проверки (формальной или нет) общего замысла и реализации системы в целом и отдельных ее компонентов. Уровень гарантированности показывает, насколько корректны механизмы, отвечающие за реализацию политики безопасности. Это пассивный аспект защиты.

Важным средством обеспечения безопасности является механизм подотчетности (протоколирования). Доверенная система должна фиксировать все события, касающиеся безопасности. Ведение протоколов должно дополняться аудитом, то есть анализом регистрационной информации.

Концепция доверенной вычислительной базы является центральной при оценке степени доверия безопасности. Доверенная вычислительная база – это совокупность защитных механизмов ИС (включая аппаратное и программное обеспечение), отвечающих за проведение в жизнь политики безопасности. Качество вычислительной базы определяется исключительно ее реализацией и корректностью исходных данных, которые вводит системный администратор.

Вообще говоря, компоненты вне вычислительной базы могут не быть доверенными, однако это не должно влиять на безопасность системы в целом. В результате, для оценки доверия безопасности ИС достаточно рассмотреть только ее вычислительную базу, которая, как можно надеяться, достаточно компактна.

Основное назначение доверенной вычислительной базы – выполнять функции монитора обращений, то есть контролировать допустимость выполнения субъектами (активными сущностями ИС, действующими от имени пользователей) определенных операций над объектами (пассивными сущностями). Монитор проверяет каждое обращение пользователя к программам или данным на предмет согласованности с набором действий, допустимых для пользователя.

Монитор обращений должен обладать тремя качествами:

Изолированность. Необходимо предупредить возможность отслеживания работы монитора.

Полнота. Монитор должен вызываться при каждом обращении, не должно быть способов обойти его.

Верифицируемость. Монитор должен быть компактным, чтобы его можно было проанализировать и протестировать, будучи уверенным в полноте тестирования.

Реализация монитора обращений называется ядром безопасности. Ядро безопасности – это основа, на которой строятся все защитные механизмы. Помимо перечисленных выше свойств монитора обращений, ядро должно гарантировать собственную неизменность.

Границу доверенной вычислительной базы называют периметром безопасности. Как уже указывалось, компоненты, лежащие вне периметра безопасности, вообще говоря, могут не быть доверенными. С развитием распределенных систем понятию "периметр безопасности" все чаще придают другой смысл, имея в виду границу владений определенной организации. То, что находится внутри владений, считается доверенным, а то, что вне, – нет.

Механизмы безопасности

Согласно "Оранжевой книге", политика безопасности должна обязательно включать в себя следующие элементы:

- произвольное управление доступом;
- безопасность повторного использования объектов;
- метки безопасности;
- принудительное управление доступом.

Произвольное управление доступом (называемое иногда дискреционным) – это метод разграничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит. Произвольность управления состоит в том, что некоторое лицо (обычно владелец объекта) может по своему усмотрению предоставлять другим субъектам или отбирать у них права доступа к объекту.

Безопасность повторного использования объектов – важное дополнение средств управления доступом, предохраняющее от случайного или преднамеренного извлечения конфиденциальной информации из "мусора". Безопасность повторного использования должна гарантироваться для областей оперативной памяти (в частности, для буферов с образами экрана, расшифрованными паролями и т.п.), для дисковых блоков и магнитных носителей в целом.

Как мы указывали ранее, современный объектно-ориентированный подход резко сужает область действия данного элемента безопасности, затрудняет его реализацию. То же верно и для интеллектуальных устройств, способных буферизовать большие объемы данных.

Для реализации принудительного управления доступом с субъектами и объектами ассоциируются метки безопасности. Метка субъекта описывает его благонадежность, метка объекта – степень конфиденциальности содержащейся в нем информации.

Согласно "Оранжевой книге", метки безопасности состоят из двух частей – уровня секретности и списка категорий. Уровни секретности образуют упорядоченное множество, категории – неупорядоченное. Назначение последних – описать предметную область, к которой относятся данные.

Принудительное (или мандатное) управление доступом основано на сопоставлении меток безопасности субъекта и объекта.

Субъект может читать информацию из объекта, если уровень секретности субъекта не ниже, чем у объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта. В таком случае говорят, что метка субъекта доминирует над меткой объекта. Смысл сформулированного правила понятен – читать можно только то, что положено.

Субъект может записывать информацию в объект, если метка безопасности объекта доминирует над меткой субъекта. В частности, "конфиденциальный" субъект может записывать данные в секретные файлы, но не может – в несекретные (разумеется, должны также выполняться ограничения на набор категорий).

Описанный способ управления доступом называется принудительным, поскольку он не зависит от воли субъектов (даже системных администраторов). После того, как зафиксированы метки безопасности субъектов и объектов, оказываются зафиксированными и права доступа.

Если понимать политику безопасности узко, то есть как правила разграничения доступа, то механизм подотчетности является дополнением подобной политики. Цель подотчетности – в каждый момент времени знать, кто работает в системе и что делает. Средства подотчетности делятся на три категории:

- идентификация и аутентификация;
- предоставление доверенного пути;
- анализ регистрационной информации.

Обычный способ идентификации – ввод имени пользователя при входе в систему. Стандартное средство проверки подлинности (аутентификации) пользователя – пароль.

Доверенный путь связывает пользователя непосредственно с доверенной вычислительной базой, минуя другие, потенциально опасные компоненты ИС. Цель предоставления доверенного пути – дать пользователю возможность убедиться в подлинности обслуживающей его системы.

Анализ регистрационной информации (аудит) имеет дело с действиями (событиями), так или иначе затрагивающими безопасность системы.

Если фиксировать все события, объем регистрационной информации, скорее всего, будет расти слишком быстро, а ее эффективный анализ станет невозможным. "Оранжевая книга" предусматривает наличие средств выборочного протоколирования, как в отношении пользователей (внимательно следить только за подозрительными), так и в отношении событий.

Переходя к пассивным аспектам защиты, укажем, что в "Оранжевой книге" рассматривается два вида гарантированности – операционная и технологическая. Операционная гарантированность относится к архитектурным и реализационным аспектам системы, в то время как технологическая – к методам построения и сопровождения.

Операционная гарантированность включает в себя проверку следующих элементов:

- архитектура системы;
- целостность системы;
- проверка тайных каналов передачи информации;
- доверенное администрирование;
- доверенное восстановление после сбоев.

Операционная гарантированность – это способ убедиться в том, что архитектура системы и ее реализация действительно реализуют избранную политику безопасности.

Технологическая гарантированность охватывает весь жизненный цикл системы, то есть периоды проектирования, реализации, тестирования, продажи и сопровождения. Все перечисленные действия должны выполняться в соответствии с жесткими стандартами, чтобы исключить утечку информации и нелегальные "закладки".

Классы безопасности

"Критерии ..." Министерства обороны США открыли путь к ранжированию информационных систем по степени доверия безопасности.

В "Оранжевой книге" определяется четыре уровня доверия – D, C, B и A. Уровень D предназначен для систем, признанных неудовлетворительными. По мере перехода от уровня C к A к системам предъявляются все более жесткие требования. Уровни C и B подразделяются на классы (C1, C2, B1, B2, B3) с постепенным возрастанием степени доверия.

Всего имеется шесть классов безопасности – C1, C2, B1, B2, B3, A1. Чтобы в результате процедуры сертификации систему можно было отнести к некоторому классу, ее политика безопасности и уровень гарантированности должны удовлетворять заданным требованиям, из которых мы упомянем лишь важнейшие.

Класс C1:

- доверенная вычислительная база должна управлять доступом именованных пользователей к именованным объектам;
- пользователи должны идентифицировать себя, прежде чем выполнять какие-либо иные действия, контролируемые доверенной вычислительной базой. Для аутентификации должен использоваться какой-либо защитный механизм, например пароли. Аутентификационная информация должна быть защищена от несанкционированного доступа;
- доверенная вычислительная база должна поддерживать область для собственного выполнения, защищенную от внешних воздействий (в частности, от изменения команд и/или данных) и от попыток слежения за ходом работы;
- должны быть в наличии аппаратные и/или программные средства, позволяющие периодически проверять корректность функционирования аппаратных и микропрограммных компонентов доверенной вычислительной базы;
- защитные механизмы должны быть протестированы на предмет

соответствия их поведения системной документации. Тестирование должно подтвердить, что у неавторизованного пользователя нет очевидных способов обойти или разрушить средства защиты доверенной вычислительной базы;

- должны быть описаны подход к безопасности, используемый производителем, и применение этого подхода при реализации доверенной вычислительной базы.

Класс C2 (в дополнение к C1):

- права доступа должны гранулироваться с точностью до пользователя. Все объекты должны подвергаться контролю доступа;
- при выделении хранимого объекта из пула ресурсов доверенной вычислительной базы необходимо ликвидировать все следы его использования;
- каждый пользователь системы должен уникальным образом идентифицироваться. Каждое регистрируемое действие должно ассоциироваться с конкретным пользователем;
- доверенная вычислительная база должна создавать, поддерживать и защищать журнал регистрационной информации, относящейся к доступу к объектам, контролируемым базой;
- тестирование должно подтвердить отсутствие очевидных недостатков в механизмах изоляции ресурсов и защиты регистрационной информации.

Класс B1 (в дополнение к C2):

- доверенная вычислительная база должна управлять метками безопасности, ассоциируемыми с каждым субъектом и хранимым объектом;
- доверенная вычислительная база должна обеспечить реализацию принудительного управления доступом всех субъектов ко всем хранимым объектам;
- доверенная вычислительная база должна обеспечивать взаимную изоляцию процессов путем разделения их адресных пространств;
- группа специалистов, полностью понимающих реализацию доверенной вычислительной базы, должна подвергнуть описание архитектуры, исходные и объектные коды тщательному анализу и тестированию;
- должна существовать неформальная или формальная модель политики безопасности, поддерживаемой доверенной вычислительной базой.

Класс B2 (в дополнение к B1):

- снабжаться метками должны все ресурсы системы (например, ПЗУ), прямо или косвенно доступные субъектам;
- к доверенной вычислительной базе должен поддерживаться доверенный коммуникационный путь для пользователя, выполняющего операции начальной идентификации и аутентификации;
- должна быть предусмотрена возможность регистрации событий, связанных с организацией тайных каналов обмена с памятью;
- доверенная вычислительная база должна быть внутренне структурирована на хорошо определенные, относительно независимые модули;
- системный архитектор должен тщательно проанализировать возможности организации тайных каналов обмена с памятью и оценить максимальную пропускную способность каждого выявленного канала;
- должна быть продемонстрирована относительная устойчивость доверенной вычислительной базы к попыткам проникновения;
- модель политики безопасности должна быть формальной. Для доверенной вычислительной базы должны существовать описательные спецификации верхнего уровня, точно и полно определяющие ее интерфейс;
- в процессе разработки и сопровождения доверенной вычислительной базы должна использоваться система конфигурационного управления, обеспечивающая контроль изменений в описательных спецификациях верхнего уровня, иных архитектурных данных, реализационной документации, исходных текстах, работающей версии объектного кода, тестовых данных и документации;
- тесты должны подтверждать действенность мер по уменьшению пропускной способности тайных каналов передачи информации.

Класс B3 (в дополнение к B2):

- для произвольного управления доступом должны обязательно использоваться списки управления доступом с указанием разрешенных режимов;
- должна быть предусмотрена возможность регистрации появления или накопления событий, несущих угрозу политике безопасности системы. Администратор безопасности должен немедленно извещаться о попытках нарушения политики безопасности, а система, в случае продолжения попыток, должна пресекать их наименее болезненным способом;

- доверенная вычислительная база должна быть спроектирована и структурирована таким образом, чтобы использовать полный и концептуально простой защитный механизм с точно определенной семантикой;
- процедура анализа должна быть выполнена для временных тайных каналов;
- должна быть специфицирована роль администратора безопасности. Получить права администратора безопасности можно только после выполнения явных, протоколируемых действий;
- должны существовать процедуры и/или механизмы, позволяющие произвести восстановление после сбоя или иного нарушения работы без ослабления защиты;
- должна быть продемонстрирована устойчивость доверенной вычислительной базы к попыткам проникновения.

Класс А1 (в дополнение к В3):

- тестирование должно продемонстрировать, что реализация доверенной вычислительной базы соответствует формальным спецификациям верхнего уровня;
- помимо описательных, должны быть представлены формальные спецификации верхнего уровня. Необходимо использовать современные методы формальной спецификации и верификации систем;
- механизм конфигурационного управления должен распространяться на весь жизненный цикл и все компоненты системы, имеющие отношение к обеспечению безопасности;
- должно быть описано соответствие между формальными спецификациями верхнего уровня и исходными текстами.

Такова классификация, введенная в "Оранжевой книге". Коротко ее можно сформулировать так:

- уровень С – произвольное управление доступом;
- уровень В – принудительное управление доступом;
- уровень А – верифицируемая безопасность.

Конечно, в адрес "Критериев ..." можно высказать целый ряд серьезных замечаний (таких, например, как полное игнорирование проблем, возникающих в распределенных системах). Тем не менее, следует подчеркнуть, что публикация "Оранжевой книги" без всякого преувеличения стала эпохальным событием в области информационной безопасности. Появился общепризнанный понятийный базис, без которого даже обсуждение проблем ИБ было бы затруднительным.

Отметим, что огромный идейный потенциал "Оранжевой книги" пока во многом остается невостребованным. Прежде всего это касается концеп-

ции технологической гарантированности, охватывающей весь жизненный цикл системы – от выработки спецификаций до фазы эксплуатации. При современной технологии программирования результирующая система не содержит информации, присутствующей в исходных спецификациях, теряется информация о семантике программ. Важность данного обстоятельства мы планируем продемонстрировать далее, в лекции об управлении доступом.

Информационная безопасность распределенных систем. Рекомендации X.800

Сетевые сервисы безопасности

Следуя скорее исторической, чем предметной логике, мы переходим к рассмотрению технической спецификации X.800, появившейся немногим позднее "Оранжевой книги", но весьма полно и глубоко трактующей вопросы информационной безопасности распределенных систем.

Рекомендации X.800 – документ довольно обширный. Мы остановимся на специфических сетевых функциях (сервисах) безопасности, а также на необходимых для их реализации защитных механизмах.

Выделяют следующие сервисы безопасности и исполняемые ими роли:

Аутентификация. Данный сервис обеспечивает проверку подлинности партнеров по общению и проверку подлинности источника данных. Аутентификация партнеров по общению используется при установлении соединения и, быть может, периодически во время сеанса. Она служит для предотвращения таких угроз, как маскарад и повтор предыдущего сеанса связи. Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной).

Управление доступом. Обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети.

Конфиденциальность данных. Обеспечивает защиту от несанкционированного получения информации. Отдельно упомянем конфиденциальность трафика (это защита информации, которую можно получить, анализируя сетевые потоки данных).

Целостность данных подразделяется на подвиды в зависимости от того, какой тип общения используют партнеры – с установлением соединения или без него, защищаются ли все данные или только отдельные поля, обеспечивается ли восстановление в случае нарушения целостности.

Неотказуемость (невозможность отказаться от совершенных действий) обеспечивает два вида услуг: неотказуемость с подтверждением подлинности источника данных и неотказуемость с подтверждением доставки. Побочным продуктом неотказуемости является аутентификация источника данных.

В следующей таблице указаны уровни эталонной семиуровневой модели OSI, на которых могут быть реализованы функции безопасности. Отметим, что прикладные процессы, в принципе, могут взять на себя поддержку всех защитных сервисов.

Функции безопасности	Уровень						
	1	2	3	4	5	6	7
Аутентификация	–	–	+	+	–	–	+
Управление доступом	–	–	+	+	–	–	+
Конфиденциальность соединения	+	+	+	+	–	+	+
Конфиденциальность вне соединения	–	+	+	+	–	+	+
Избирательная конфиденциальность	–	–	–	–	–	+	+
Конфиденциальность трафика	+	–	+	–	–	–	+
Целостность с восстановлением	–	–	–	+	–	–	+
Целостность без восстановления	–	–	+	+	–	–	+
Избирательная целостность	–	–	–	–	–	–	+
Целостность вне соединения	–	–	+	+	–	–	+
Неотказуемость	–	–	–	–	–	–	+

"+" данный уровень может предоставить функцию безопасности;
"–" данный уровень не подходит для предоставления функции безопасности.

Табл. 5.1. Распределение функций безопасности по уровням эталонной семиуровневой модели OSI.

Сетевые механизмы безопасности

Для реализации сервисов (функций) безопасности могут использоваться следующие механизмы и их комбинации:

- шифрование;
- электронная цифровая подпись;
- механизмы управления доступом. Могут располагаться на любой из участвующих в общении сторон или в промежуточной точке;
- механизмы контроля целостности данных. В рекомендациях X.800 различаются два аспекта целостности: целостность отдельного сообщения или поля информации и целостность потока сообщений или полей информации. Для проверки целостности потока сообщений (то есть для защиты от кражи, переупорядочивания, дублирования и вставки сообщений) используются порядковые номера, временные штампы, криптографическое связывание или иные аналогичные приемы;
- механизмы аутентификации. Согласно рекомендациям X.800, аутентификация может достигаться за счет использования паролей, личных карточек или иных устройств аналогичного назначения, криптографических методов, устройств измерения и анализа биометрических характеристик;
- механизмы дополнения трафика;
- механизмы управления маршрутизацией. Маршруты могут выбираться статически или динамически. Оконечная система, зафиксировав неоднократные атаки на определенном маршруте, может отказаться от его использования. На выбор маршрута способна повлиять метка безопасности, ассоциированная с передаваемыми данными;
- механизмы нотаризации. Служат для заверения таких коммуникационных характеристик, как целостность, время, личности отправителя и получателей. Заверение обеспечивается надежной третьей стороной, обладающей достаточной информацией. Обычно нотаризация опирается на механизм электронной подписи.

В следующей таблице сведены сервисы (функции) и механизмы безопасности. Таблица показывает, какие механизмы (по отдельности или в комбинации с другими) могут использоваться для реализации той или иной функции.

Механизмы / Функции	Шифрование	Электронная подпись	Управление доступом	Целостность	Аутентификация	Дополнение трафика	Управление маршрутизацией	Нотаризация
Аутентификация партнеров	+	+	–	–	+	–	–	–
Аутентификация источника	+	+	–	–	–	–	–	–
Управление доступом	–	–	+	–	–	–	–	–
Конфиденциальность	+	–	+	–	–	–	+	–
Избирательная конфиденциальность	+	–	–	–	–	–	–	–
Конфиденциальность трафика	+	–	–	–	–	+	+	–
Целостность соединения	+	–	–	+	–	–	–	–
Целостность вне соединения	+	+	–	+	–	–	–	–
Неотказуемость	–	+	–	+	–	–	–	+

"+" механизм пригоден для реализации данной функцию безопасности;
"–" механизм не предназначен для реализации данной функции безопасности.

Табл. 5.2. Взаимосвязь функций и механизмов безопасности.

Администрирование средств безопасности

Администрирование средств безопасности включает в себя распространение информации, необходимой для работы сервисов и механизмов безопасности, а также сбор и анализ информации об их функционировании. Примерами могут служить распространение криптографических ключей, установка значений параметров защиты, ведение регистрационного журнала и т.п.

Концептуальной основой администрирования является информационная база управления безопасностью. Эта база может не существовать как единое (распределенное) хранилище, но каждая из оконечных систем

должна располагать информацией, необходимой для реализации избранной политики безопасности.

Согласно рекомендациям X.800, усилия администратора средств безопасности должны распределяться по трем направлениям:

- администрирование информационной системы в целом;
- администрирование сервисов безопасности;
- администрирование механизмов безопасности.

Среди действий, относящихся к ИС в целом, отметим обеспечение актуальности политики безопасности, взаимодействие с другими административными службами, реагирование на происходящие события, аудит и безопасное восстановление.

Администрирование сервисов безопасности включает в себя определение защищаемых объектов, выработку правил подбора механизмов безопасности (при наличии альтернатив), комбинирование механизмов для реализации сервисов, взаимодействие с другими администраторами для обеспечения согласованной работы.

Обязанности администратора механизмов безопасности определяются перечнем задействованных механизмов. Типичный список таков:

- управление ключами (генерация и распределение);
- управление шифрованием (установка и синхронизация криптографических параметров). К управлению шифрованием можно отнести и администрирование механизмов электронной подписи. Управление целостностью, если оно обеспечивается криптографическими средствами, также тяготеет к данному направлению;
- администрирование управления доступом (распределение информации, необходимой для управления – паролей, списков доступа и т.п.);
- управление аутентификацией (распределение информации, необходимой для аутентификации – паролей, ключей и т.п.);
- управление дополнением трафика (выработка и поддержание правил, задающих характеристики дополняющих сообщений – частоту отправки, размер и т.п.);
- управление маршрутизацией (выделение доверенных путей);
- управление нотаризацией (распространение информации о нотариальных службах, администрирование этих служб).

Мы видим, что администрирование средств безопасности в распределенной ИС имеет много особенностей по сравнению с централизованными системами.

Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий"

Основные понятия

Мы возвращаемся к теме оценочных стандартов, приступая к рассмотрению самого полного и современного среди них – "Критериев оценки безопасности информационных технологий" (издан 1 декабря 1999 года). Этот международный стандарт стал итогом почти десятилетней работы специалистов нескольких стран, он вобрал в себя опыт существовавших к тому времени документов национального и межнационального масштаба.

По историческим причинам данный стандарт часто называют "Общими критериями" (или даже ОК). Мы также будем использовать это сокращение.

"Общие критерии" на самом деле являются метастандартом, определяющим инструменты оценки безопасности ИС и порядок их использования. В отличие от "Оранжевой книги", ОК не содержат предопределенных "классов безопасности". Такие классы можно строить, исходя из требований безопасности, существующих для конкретной организации и/или конкретной информационной системы.

С программистской точки зрения ОК можно считать набором библиотек, помогающих писать содержательные "программы" – задания по безопасности, типовые профили защиты и т.п. Программисты знают, насколько хорошая библиотека упрощает разработку программ, повышает их качество. Без библиотек, "с нуля", программы не пишут уже очень давно; оценка безопасности тоже вышла на сопоставимый уровень сложности, и "Общие критерии" предоставили соответствующий инструментарий.

Важно отметить, что требования могут быть параметризованы, как и полагается библиотечным функциям.

Как и "Оранжевая книга", ОК содержат два основных вида требований безопасности:

- функциональные, соответствующие активному аспекту защиты, предъявляемые к функциям безопасности и реализующим их механизмам;
- требования доверия, соответствующие пассивному аспекту, предъявляемые к технологии и процессу разработки и эксплуатации.

Требования безопасности предъявляются, а их выполнение проверяется для определенного объекта оценки – аппаратно-программного продукта или информационной системы.

Очень важно, что безопасность в ОК рассматривается не статично, а в привязке к жизненному циклу объекта оценки. Выделяются следующие этапы:

- определение назначения, условий применения, целей и требований безопасности;
- проектирование и разработка;
- испытания, оценка и сертификация;
- внедрение и эксплуатация.

В ОК объект оценки рассматривается в контексте среды безопасности, которая характеризуется определенными условиями и угрозами.

В свою очередь, угрозы характеризуются следующими параметрами:

- источник угрозы;
- метод воздействия;
- уязвимые места, которые могут быть использованы;
- ресурсы (активы), которые могут пострадать.

Уязвимые места могут возникать из-за недостатка в:

- требованиях безопасности;
- проектировании;
- эксплуатации.

Слабые места по возможности следует устранить, минимизировать или хотя бы постараться ограничить возможный ущерб от их преднамеренного использования или случайной активизации.

С точки зрения технологии программирования в ОК использован устаревший библиотечный (не объектный) подход. Чтобы, тем не менее, структурировать пространство требований, в "Общих критериях" введена иерархия класс-семейство-компонент-элемент.

Классы определяют наиболее общую, "предметную" группировку требований (например, функциональные требования подотчетности).

Семейства в пределах класса различаются по строгости и другим нюансам требований.

Компонент – минимальный набор требований, фигурирующий как целое.

Элемент – неделимое требование.

Как и между библиотечными функциями, между компонентами ОК могут существовать зависимости. Они возникают, когда компонент сам по себе недостаточен для достижения цели безопасности. Вообще говоря, не все комбинации компонентов имеют смысл, и понятие зависимости в какой-то степени компенсирует недостаточную выразительность библиотечной организации, хотя и не заменяет объединение функций в содержательные объектные интерфейсы.

Как указывалось выше, с помощью библиотек могут формироваться два вида нормативных документов: профиль защиты и задание по безопасности.

Профиль защиты (ПЗ) представляет собой типовой набор требований, которым должны удовлетворять продукты и/или системы определенного класса (например, операционные системы на компьютерах в правительственных организациях).

Задание по безопасности содержит совокупность требований к конкретной разработке, выполнение которых обеспечивает достижение поставленных целей безопасности.

Выше мы отмечали, что в ОК нет готовых классов защиты. Сформировать классификацию в терминах "Общих критериев" – значит определить несколько иерархически упорядоченных (содержащих усиливающиеся требования) профилей защиты, в максимально возможной степени использующих стандартные функциональные требования и требования доверия безопасности.

Выделение некоторого подмножества из всего множества профилей защиты во многом носит субъективный характер. По целому ряду соображений (одним из которых является желание придерживаться объектно-ориентированного подхода) целесообразно, на наш взгляд, сформировать сначала отправную точку классификации, выделив базовый (минимальный) ПЗ, а дополнительные требования компоновать в функциональные пакеты.

Функциональный пакет – это неоднократно используемая совокупность компонентов, объединенных для достижения определенных целей безопасности. "Общие критерии" не регламентируют структуру пакетов, процедуры верификации, регистрации и т.п., отводя им роль технологического средства формирования ПЗ.

Базовый профиль защиты должен включать требования к основным (обязательным в любом случае) возможностям. Производные профили получаются из базового путем добавления необходимых пакетов расширения, то есть подобно тому, как создаются производные классы в объектно-ориентированных языках программирования.

Функциональные требования

Функциональные требования сгруппированы на основе выполняемой ими роли или обслуживаемой цели безопасности. Всего в "Общих критериях" представлено 11 функциональных классов, 66 семейств, 135 компонентов. Это, конечно, значительно больше, чем число аналогичных сущностей в "Оранжевой книге".

Перечислим классы функциональных требований ОК:

- идентификация и аутентификация;
- защита данных пользователя;

- защита функций безопасности (требования относятся к целостности и контролю данных сервисов безопасности и реализующих их механизмов);
- управление безопасностью (требования этого класса относятся к управлению атрибутами и параметрами безопасности);
- аудит безопасности (выявление, регистрация, хранение, анализ данных, затрагивающих безопасность объекта оценки, реагирование на возможное нарушение безопасности);
- доступ к объекту оценки;
- приватность (защита пользователя от раскрытия и несанкционированного использования его идентификационных данных);
- использование ресурсов (требования к доступности информации);
- криптографическая поддержка (управление ключами);
- связь (аутентификация сторон, участвующих в обмене данными);
- доверенный маршрут/канал (для связи с сервисами безопасности).

Опишем подробнее два класса, демонстрирующие особенности современного подхода к ИБ.

Класс "Приватность" содержит 4 семейства функциональных требований.

Анонимность. Позволяет выполнять действия без раскрытия идентификатора пользователя другим пользователям, субъектам и/или объектам. Анонимность может быть полной или выборочной. В последнем случае она может относиться не ко всем операциям и/или не ко всем пользователям (например, у уполномоченного пользователя может оставаться возможность выяснения идентификаторов пользователей).

Псевдонимность. Напоминает анонимность, но при применении псевдонима поддерживается ссылка на идентификатор пользователя для обеспечения подотчетности или для других целей.

Невозможность ассоциации. Семейство обеспечивает возможность неоднократного использования информационных сервисов, но не позволяет ассоциировать случаи использования между собой и приписать их одному лицу. Невозможность ассоциации защищает от построения профилей поведения пользователей (и, следовательно, от получения информации на основе подобных профилей).

Скрытность. Требования данного семейства направлены на то, чтобы можно было использовать информационный сервис с сокрытием факта использования. Для реализации скрытности может применяться, например, широковещательное распространение информации, без указания

конкретного адресата. Годятся для реализации скрытности и методы стеганографии, когда скрывается не только содержание сообщения (как в криптографии), но и сам факт его отправки.

Еще один показательный (с нашей точки зрения) класс функциональных требований – "Использование ресурсов", содержащий требования доступности. Он включает три семейства.

Отказоустойчивость. Требования этого семейства направлены на сохранение доступности информационных сервисов даже в случае сбоя или отказа. В ОК различаются активная и пассивная отказоустойчивость. Активный механизм содержит специальные функции, которые активизируются в случае сбоя. Пассивная отказоустойчивость подразумевает наличие избыточности с возможностью нейтрализации ошибок.

Обслуживание по приоритетам. Выполнение этих требований позволяет управлять использованием ресурсов так, что низкоприоритетные операции не могут помешать высокоприоритетным.

Распределение ресурсов. Требования направлены на защиту (путем применения механизма квот) от несанкционированной монополизации ресурсов.

Мы видим, что "Общие критерии" – очень продуманный и полный документ с точки зрения функциональных требований. В то же время, хотелось бы обратить внимание и на некоторые недостатки.

Первый мы уже отмечали – это отсутствие объектного подхода. Функциональные требования не сгруппированы в осмысленные наборы (объектные интерфейсы), к которым могло бы применяться наследование. Подобное положение, как известно из технологии программирования, чревато появлением слишком большого числа комбинаций функциональных компонентов, несопоставимых между собой.

В современном программировании ключевым является вопрос накопления и многократного использования знаний. Стандарты – одна из форм накопления знаний. Следование в ОК "библиотечному", а не объектному подходу сужает круг фиксируемых знаний, усложняет их корректное использование.

К сожалению, в "Общих критериях" отсутствуют архитектурные требования, что является естественным следствием избранного старомодного программистского подхода "снизу вверх". На наш взгляд, это серьезное упущение. Технологичность средств безопасности, следование общепризнанным рекомендациям по протоколам и программным интерфейсам, а также апробированным архитектурным решениям, таким как менеджер/агент, – необходимые качества изделий информационных технологий, предназначенных для поддержки критически важных функций, к числу которых, безусловно, относятся функции безопасности. Без рассмотрения интерфейсных аспектов системы оказыва-

ются нерасширяемыми и изолированными. Очевидно, с практической точки зрения это недопустимо. В то же время, обеспечение безопасности интерфейсов – важная задача, которую желательно решать единообразно.

Требования доверия безопасности

Установление доверия безопасности, согласно "Общим критериям", основывается на активном исследовании объекта оценки.

Форма представления требований доверия, в принципе, та же, что и для функциональных требований. Специфика состоит в том, что каждый элемент требований доверия принадлежит одному из трех типов:

- действия разработчиков;
- представление и содержание свидетельств;
- действия оценщиков.

Всего в ОК 10 классов, 44 семейства, 93 компонента требований доверия безопасности. Перечислим классы:

- разработка (требования для поэтапной детализации функций безопасности от краткой спецификации до реализации);
- поддержка жизненного цикла (требования к модели жизненного цикла, включая порядок устранения недостатков и защиту среды разработки);
- тестирование;
- оценка уязвимостей (включая оценку стойкости функций безопасности);
- поставка и эксплуатация;
- управление конфигурацией;
- руководства (требования к эксплуатационной документации);
- поддержка доверия (для поддержки этапов жизненного цикла после сертификации);
- оценка профиля защиты;
- оценка задания по безопасности.

Применительно к требованиям доверия в "Общих критериях" сделана весьма полезная вещь, не реализованная, к сожалению, для функциональных требований. А именно, введены так называемые оценочные уровни доверия (их семь), содержащие осмысленные комбинации компонентов.

Оценочный уровень доверия 1 (начальный) предусматривает анализ функциональной спецификации, спецификации интерфейсов, эксплуатационной документации, а также независимое тестирование. Уровень применим, когда угрозы не рассматриваются как серьезные.

Оценочный уровень доверия 2, в дополнение к первому уровню, предусматривает наличие проекта верхнего уровня объекта оценки, выбо-

рочное независимое тестирование, анализ стойкости функций безопасности, поиск разработчиком явных уязвимых мест.

На третьем уровне ведется контроль среды разработки и управление конфигурацией объекта оценки.

На уровне 4 добавляются полная спецификация интерфейсов, проекты нижнего уровня, анализ подмножества реализации, применение неформальной модели политики безопасности, независимый анализ уязвимых мест, автоматизация управления конфигурацией. Вероятно, это самый высокий уровень, которого можно достичь при существующей технологии программирования и приемлемых затратах.

Уровень 5, в дополнение к предыдущим, предусматривает применение формальной модели политики безопасности, полуформальных функциональной спецификации и проекта верхнего уровня с демонстрацией соответствия между ними. Необходимо проведение анализа скрытых каналов разработчиками и оценщиками.

На уровне 6 реализация должна быть представлена в структурированном виде. Анализ соответствия распространяется на проект нижнего уровня.

Оценочный уровень 7 (самый высокий) предусматривает формальную верификацию проекта объекта оценки. Он применим к ситуациям чрезвычайно высокого риска.

На этом мы заканчиваем краткий обзор "Общих критериев".

Гармонизированные критерии Европейских стран

Наше изложение "Гармонизированных критериев" основывается на версии 1.2, опубликованной в июне 1991 года от имени соответствующих органов четырех стран – Франции, Германии, Нидерландов и Великобритании.

Принципиально важной чертой Европейских Критериев является отсутствие требований к условиям, в которых должна работать информационная система. Так называемый спонсор, то есть организация, запрашивающая сертификационные услуги, формулирует цель оценки, то есть описывает условия, в которых должна работать система, возможные угрозы ее безопасности и предоставляемые ею защитные функции. Задача органа сертификации – оценить, насколько полно достигаются поставленные цели, то есть насколько корректны и эффективны архитектура и реализация механизмов безопасности в описанных спонсором условиях. Таким образом, в терминологии "Оранжевой книги", Европейские Критерии относятся к гарантированности безопасной работы системы. Требования к политике безопасности и наличию защитных механизмов не являются составной частью Критериев. Впрочем, чтобы облегчить формулировку цели оцен-

ки, Критерии содержат в качестве приложения описание десяти классов функциональности, типичных для правительственных и коммерческих систем.

Европейские Критерии рассматривают все основные составляющие информационной безопасности – конфиденциальность, целостность, доступность.

В Критериях проводится различие между системами и продуктами. Система – это конкретная аппаратно-программная конфигурация, построенная с вполне определенными целями и функционирующая в известном окружении. Продукт – это аппаратно-программный "пакет", который можно купить и по своему усмотрению встроить в ту или иную систему. Таким образом, с точки зрения информационной безопасности основное отличие между системой и продуктом состоит в том, что система имеет конкретное окружение, которое можно определить и изучить сколь угодно детально, а продукт должен быть рассчитан на использование в различных условиях.

Из практических соображений важно обеспечить единство критериев оценки продуктов и систем – например, чтобы облегчить оценку системы, составленной из ранее сертифицированных продуктов. По этой причине для систем и продуктов вводится единый термин – объект оценки.

Каждая система и/или продукт предъявляет свои требования к обеспечению конфиденциальности, целостности и доступности. Чтобы удовлетворить эти требования, необходимо предоставить соответствующий набор функций (сервисов) безопасности, таких как идентификация и аутентификация, управление доступом или восстановление после сбоев.

Сервисы безопасности реализуются посредством конкретных механизмов. Чтобы объекту оценки можно было доверять, необходима определенная степень уверенности в наборе функций и механизмов безопасности. Степень уверенности мы будем называть гарантированностью. Гарантированность может быть большей или меньшей в зависимости от тщательности проведения оценки.

Гарантированность затрагивает два аспекта – эффективность и корректность средств безопасности. При проверке эффективности анализируется соответствие между целями, сформулированными для объекта оценки, и имеющимся набором функций безопасности. Точнее говоря, рассматриваются вопросы адекватности функциональности, взаимной согласованности функций, простоты их использования, а также возможные последствия эксплуатации известных слабых мест защиты. Кроме того, в понятие эффективности входит способность механизмов защиты противостоять прямым атакам (мощность механизма). Определяются три градации мощности – базовая, средняя и высокая.

Под корректностью понимается правильность реализации функций и механизмов безопасности. В Критериях определяется семь возможных уровней гарантированности корректности – от E0 до E6 (в порядке возрастания). Уровень E0 означает отсутствие гарантированности. При проверке корректности анализируется весь жизненный цикл объекта оценки – от проектирования до эксплуатации и сопровождения.

Общая оценка системы складывается из минимальной мощности механизмов безопасности и уровня гарантированности корректности.

Гармонизированные критерии Европейских стран явились для своего времени весьма передовым стандартом, они создали предпосылки для появления "Общих критериев".

Интерпретация "Оранжевой книги" для сетевых конфигураций

В 1987 году Национальным центром компьютерной безопасности США была опубликована интерпретация "Оранжевой книги" для сетевых конфигураций. Данный документ состоит из двух частей. Первая содержит собственно интерпретацию, во второй рассматриваются сервисы безопасности, специфичные или особенно важные для сетевых конфигураций.

В первой части вводится минимум новых понятий. Важнейшее из них – сетевая доверенная вычислительная база, распределенный аналог доверенной вычислительной базы изолированных систем. Сетевая доверенная вычислительная база формируется из всех частей всех компонентов сети, обеспечивающих информационную безопасность. Доверенная сетевая система должна обеспечивать такое распределение защитных механизмов, чтобы общая политика безопасности реализовывалась, несмотря на уязвимость коммуникационных путей и на параллельную, асинхронную работу компонентов.

Прямой зависимости между вычислительными базами компонентов, рассматриваемых как изолированные системы, и фрагментами сетевой вычислительной базы не существует. Более того, нет прямой зависимости и между уровнями безопасности отдельных компонентов и уровнем безопасности всей сетевой конфигурации. Например, в результате объединения двух систем класса B1, обладающих несовместимыми правилами кодирования меток безопасности, получается сеть, не удовлетворяющая требованию целостности меток. В качестве противоположного примера рассмотрим объединение двух компонентов, один из которых сам не обеспечивает протоколирование действий пользователя, но передает необходимую информацию другому компоненту, который и ведет протокол. В таком случае распределенная система в целом, несмотря на слабость компонента, удовлетворяет требованию подотчетности.

Чтобы понять суть положений, вошедших в первую часть, рассмотрим интерпретацию требований к классу безопасности С2. Первое требование к этому классу – поддержка произвольного управления доступом. Интерпретация предусматривает различные варианты распределения сетевой доверенной вычислительной базы по компонентам и, соответственно, различные варианты распределения механизмов управления доступом. В частности, некоторые компоненты, закрытые для прямого доступа пользователей, могут вообще не содержать подобных механизмов.

Интерпретация отличается от самих "Критериев" учетом динамичности сетевых конфигураций. Предусматривается наличие средств проверки подлинности и корректности функционирования компонентов перед их включением в сеть, наличие протокола взаимной проверки компонентами корректности функционирования друг друга, а также присутствие средств оповещения администратора о неполадках в сети. Сетевая конфигурация должна быть устойчива к отказам отдельных компонентов или коммуникационных путей.

Среди защитных механизмов в сетевых конфигурациях на первом месте стоит криптография, помогающая поддерживать как конфиденциальность, так и целостность. Следствием использования криптографических методов является необходимость реализации механизмов управления ключами.

Систематическое рассмотрение вопросов доступности является новшеством по сравнению не только с "Оранжевой книгой", но и с рекомендациями X.800. Сетевой сервис перестает быть доступным, когда пропускная способность коммуникационных каналов падает ниже минимально допустимого уровня или сервис не в состоянии обслуживать запросы. Удаленный ресурс может стать недоступным и вследствие нарушения равноправия в обслуживании пользователей. Доверенная система должна иметь возможность обнаруживать ситуации недоступности, уметь возвращаться к нормальной работе и противостоять атакам на доступность.

Для обеспечения непрерывности функционирования могут применяться следующие защитные меры:

- внесение в конфигурацию той или иной формы избыточности (резервное оборудование, запасные каналы связи и т.п.);
- наличие средств реконфигурирования для изоляции и/или замены узлов или коммуникационных каналов, отказавших или подвергшихся атаке на доступность;
- рассредоточенность сетевого управления, отсутствие единой точки отказа;
- наличие средств нейтрализации отказов (обнаружение отказавших компонентов, оценка последствий, восстановление после отказов);
- выделение подсетей и изоляция групп пользователей друг от друга.

Одним из важнейших в "Оранжевой книге" является понятие монитора обращений. Применительно к структурированию сетевой конфигурации можно сформулировать следующее утверждение, обеспечивающее достаточное условие корректности фрагментирования монитора обращений.

Пусть каждый субъект (то есть процесс, действующий от имени какого-либо пользователя) заключен внутри одного компонента и может осуществлять непосредственный доступ к объектам только в пределах этого компонента. Далее, пусть каждый компонент содержит свой монитор обращений, отслеживающий все локальные попытки доступа, и все мониторы реализуют согласованную политику безопасности. Пусть, наконец, коммуникационные каналы, связывающие компоненты, сохраняют конфиденциальность и целостность передаваемой информации. Тогда совокупность всех мониторов образует единый монитор обращений для всей сетевой конфигурации.

Данное утверждение является теоретической основой декомпозиции распределенной ИС в объектно-ориентированном стиле в сочетании с криптографической защитой коммуникаций.

Руководящие документы Гостехкомиссии России

Гостехкомиссия России ведет весьма активную нормотворческую деятельность, выпуская Руководящие документы (РД), играющие роль национальных оценочных стандартов в области информационной безопасности. В качестве стратегического направления Гостехкомиссия России выбрала ориентацию на "Общие критерии", что можно только приветствовать.

В своем обзоре мы рассмотрим два важных, хотя и не новых, Руководящих документа – Классификацию автоматизированных систем (АС) по уровню защищенности от несанкционированного доступа (НСД) и аналогичную Классификацию межсетевых экранов (МЭ).

Согласно первому из них, устанавливается девять классов защищенности АС от НСД к информации.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите.

Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

Третья группа классифицирует АС, в которых работает один пользователь, имеющий доступ ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса – 3Б и 3А.

Вторая группа классифицирует АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обра-

батываемой и (или) хранящейся на носителях различного уровня конфиденциальности.

Группа содержит два класса – 2Б и 2А.

Первая группа классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов – 1Д, 1Г, 1В, 1Б и 1А.

Сведем в таблицу требования ко всем девяти классам защищенности АС.

Подсистемы и требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
1. Подсистема управления доступом									
1.1. Идентификация, проверка подлинности и контроль доступа субъектов: в систему;	+	+	+	+	+	+	+	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ;	–	–	–	+	–	+	+	+	+
к программам;	–	–	–	+	–	+	+	+	+
к томам, каталогам, файлам, записям, полям записей.	–	–	–	+	–	+	+	+	+
1.2. Управление потоками информации	–	–	–	+	–	–	+	+	+
2. Подсистема регистрации и учета									
2.1. Регистрация и учет: входа/выхода субъектов доступа в/из системы (узла сети);	+	+	+	+	+	+	+	+	+

Подсистемы и требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
выдачи печатных (графических) выходных документов;	–	+	–	+	–	+	+	+	+
запуска/завершения программ и процессов (заданий, задач);	–	–	–	+	–	+	+	+	+
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей;	–	–	–	+	–	+	+	+	+
изменения полномочий субъектов доступа;	–	–	–	–	–	–	+	+	+
создаваемых защищаемых объектов доступа.	–	–	–	+	–	–	+	+	+
2.2. Учет носителей информации.	+	+	+	+	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей.	–	+	–	+	–	+	+	+	+
2.4. Сигнализация попыток нарушения защиты.	–	–	–	–	–	–	+	+	+

Подсистемы и требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
3. Криптографическая подсистема 3.1. Шифрование конфиденциальной информации.	–	–	–	+	–	–	–	+	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах.	–	–	–	–	–	–	–	–	+
3.3. Использование аттестованных (сертифицированных) криптографических средств.	–	–	–	+	–	–	–	+	+
4. Подсистема обеспечения целостности 4.1. Обеспечение целостности программных средств и обрабатываемой информации.	+	+	+	+	+	+	+	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации.	+	+	+	+	+	+	+	+	+
4.3. Наличие администратора (службы защиты) информации в АС.	–	–	–	+	–	–	+	+	+

Подсистемы и требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
4.4. Периодическое тестирование СЗИ НСД.	+	+	+	+	+	+	+	+	+
4.5. Наличие средств восстановления СЗИ НСД.	+	+	+	+	+	+	+	+	+
4.6. Использование сертифицированных средств защиты.	–	+	–	+	–	–	+	+	+

Обозначения:

"–"	нет требований к данному классу;
"+"	есть требования к данному классу;
"СЗИ НСД"	система защиты информации от несанкционированного доступа

Табл. 5.3. Требования к защищенности автоматизированных систем.

По существу перед нами – минимум требований, которым необходимо следовать, чтобы обеспечить конфиденциальность информации. Целостность представлена отдельной подсистемой (номер 4), но непосредственно к интересующему нас предмету имеет отношение только пункт 4.1. Доступность (точнее, восстановление) предусмотрено только для самих средств защиты.

Переходя к рассмотрению второго РД Гостехкомиссии России – Классификации межсетевых экранов — укажем, что данный РД представляется нам принципиально важным, поскольку в нем идет речь не о целостном продукте или системе, а об отдельном сервисе безопасности, обеспечивающем межсетевое разграничение доступа.

Данный РД важен не столько содержанием, сколько самим фактом своего существования.

Основным критерием классификации МЭ служит протокольный уровень (в соответствии с эталонной семиуровневой моделью), на котором осуществляется фильтрация информации. Это понятно: чем выше уровень, тем больше информации на нем доступно и, следовательно, тем более тонкую и надежную фильтрацию можно реализовать.

Значительное внимание в РД уделено собственной безопасности служб обеспечения защиты и вопросам согласованного администрирования распределенных конфигураций.

Вариант 1

1. Уровень безопасности С, согласно "Оранжевой книге", характеризуется:

- ☐ произвольным управлением доступом
- ☐ принудительным управлением доступом
- ☐ верифицируемой безопасностью

2. Согласно рекомендациям X.800, аутентификация может быть реализована на:

- ☐ сетевом уровне
- ☐ транспортном уровне
- ☐ прикладном уровне

3. "Общие критерии" содержат следующие виды требований:

- ☐ функциональные
- ☐ доверия безопасности
- ☐ экономической целесообразности

Вариант 2

1. Уровень безопасности B, согласно "Оранжевой книге", характеризуется:

- ☐ произвольным управлением доступом
- ☐ принудительным управлением доступом
- ☐ верифицируемой безопасностью

2. Согласно рекомендациям X.800, целостность с восстановлением может быть реализована на:

- ☐ сетевом уровне
- ☐ транспортном уровне
- ☐ прикладном уровне

3. В число классов функциональных требований "Общих критериев" входят:

- ☐ анонимность
- ☐ приватность
- ☐ связь

Вариант 3

1. Уровень безопасности А, согласно "Оранжевой книге", характеризуется:

- ☐ произвольным управлением доступом
- ☐ принудительным управлением доступом
- ☐ верифицируемой безопасностью

2. Согласно рекомендациям X.800, неотказуемость может быть реализована на:

- ☐ сетевом уровне
- ☐ транспортном уровне
- ☐ прикладном уровне

3. В число классов требований доверия безопасности "Общих критериев" входят:

- ☐ разработка
- ☐ оценка профиля защиты
- ☐ сертификация

Лекция 6. Административный уровень информационной безопасности

Вводятся ключевые понятия – политика безопасности и программа безопасности. Описывается структура соответствующих документов, меры по их разработке и сопровождению. Меры безопасности увязываются с этапами жизненного цикла информационных систем.

Ключевые слова: административный уровень ИБ, политика безопасности, программа безопасности, анализ рисков, уровень детализации, карта ИС, классификация ресурсов, физическая защита, правила разграничения доступа, порядок разработки, непрерывная работа, оценка рисков, координация, стратегическое планирование, контроль, жизненный цикл, инициация, закупка, установка, эксплуатация, выведение из эксплуатации.

Основные понятия

К административному уровню информационной безопасности относятся действия общего характера, предпринимаемые руководством организации.

Главная цель мер административного уровня – сформировать программу работ в области информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Основой программы является политика безопасности, отражающая подход организации к защите своих информационных активов. Руководство каждой организации должно осознать необходимость поддержания режима безопасности и выделения на эти цели значительных ресурсов.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы и стратегия защиты определена, составляется программа обеспечения информационной безопасности. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т.п.

Термин "политика безопасности" является не совсем точным переводом английского словосочетания "security policy", однако в данном случае калька лучше отражает смысл этого понятия, чем лингвистически более верные "правила безопасности". Мы будем иметь в виду не отдельные правила или их наборы (такого рода решения выносятся на процедурный

уровень, речь о котором впереди), а стратегию организации в области информационной безопасности. Для выработки стратегии и проведения ее в жизнь нужны, несомненно, политические решения, принимаемые на самом высоком уровне.

Под политикой безопасности мы будем понимать совокупность документированных решений, принимаемых руководством организации и направленных на защиту информации и ассоциированных с ней ресурсов.

Такая трактовка, конечно, гораздо шире, чем набор правил разграничения доступа (именно это означал термин "security policy" в "Оранжевой книге" и в построенных на ее основе нормативных документах других стран).

ИС организации и связанные с ней интересы субъектов – это сложная система, для рассмотрения которой необходимо применять объектно-ориентированный подход и понятие уровня детализации. Целесообразно выделить, по крайней мере, три таких уровня, что мы уже делали в примере и сделаем еще раз далее.

Чтобы рассматривать ИС предметно, с использованием актуальных данных, следует составить карту информационной системы. Эта карта, разумеется, должна быть изготовлена в объектно-ориентированном стиле, с возможностью варьировать не только уровень детализации, но и видимые грани объектов. Техническим средством составления, сопровождения и визуализации подобных карт может служить свободно распространяемый каркас какой-либо системы управления.

Политика безопасности

С практической точки зрения политику безопасности целесообразно рассматривать на трех уровнях детализации. К верхнему уровню можно отнести решения, затрагивающие организацию в целом. Они носят весьма общий характер и, как правило, исходят от руководства организации. Примерный список подобных решений может включать в себя следующие элементы:

- решение сформировать или пересмотреть комплексную программу обеспечения информационной безопасности, назначение ответственных за продвижение программы;
- формулировка целей, которые преследует организация в области информационной безопасности, определение общих направлений в достижении этих целей;
- обеспечение базы для соблюдения законов и правил;
- формулировка административных решений по тем вопросам реализации программы безопасности, которые должны рассматриваться на уровне организации в целом.

Для политики верхнего уровня цели организации в области информационной безопасности формулируются в терминах целостности, дос-

тупности и конфиденциальности. Если организация отвечает за поддержание критически важных баз данных, на первом плане может стоять уменьшение числа потерь, повреждений или искажений данных. Для организации, занимающейся продажей компьютерной техники, вероятно, важна актуальность информации о предоставляемых услугах и ценах и ее доступность максимальному числу потенциальных покупателей. Руководство режимного предприятия в первую очередь заботится о защите от несанкционированного доступа, то есть о конфиденциальности.

На верхний уровень выносится управление защитными ресурсами и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем и взаимодействие с другими организациями, обеспечивающими или контролирующими режим безопасности.

Политика верхнего уровня должна четко очерчивать сферу своего влияния. Возможно, это будут все компьютерные системы организации (или даже больше, если политика регламентирует некоторые аспекты использования сотрудниками своих домашних компьютеров). Возможна, однако, и такая ситуация, когда в сферу влияния включаются лишь наиболее важные системы.

В политике должны быть определены обязанности должностных лиц по выработке программы безопасности и проведению ее в жизнь. В этом смысле политика безопасности является основой подотчетности персонала.

Политика верхнего уровня имеет дело с тремя аспектами законопослушности и исполнительской дисциплины. Во-первых, организация должна соблюдать существующие законы. Во-вторых, следует контролировать действия лиц, ответственных за выработку программы безопасности. Наконец, необходимо обеспечить определенную степень исполнительности персонала, а для этого нужно выработать систему поощрений и наказаний.

Вообще говоря, на верхний уровень следует выносить минимум вопросов. Подобное вынесение целесообразно, когда оно сулит значительную экономию средств или когда иначе поступить просто невозможно.

Британский стандарт BS 7799:1995 рекомендует включать в документ, характеризующий политику безопасности организации, следующие разделы:

- вводный, подтверждающий озабоченность высшего руководства проблемами информационной безопасности;
- организационный, содержащий описание подразделений, комиссий, групп и т.д., отвечающих за работы в области информационной безопасности;
- классификационный, описывающий имеющиеся в организации материальные и информационные ресурсы и необходимый уровень их защиты;

- штатный, характеризующий меры безопасности, применяемые к персоналу (описание должностей с точки зрения информационной безопасности, организация обучения и переподготовки персонала, порядок реагирования на нарушения режима безопасности и т.п.);
- раздел, освещающий вопросы физической защиты;
- управляющий раздел, описывающий подход к управлению компьютерами и компьютерными сетями;
- раздел, описывающий правила разграничения доступа к производственной информации;
- раздел, характеризующий порядок разработки и сопровождения систем;
- раздел, описывающий меры, направленные на обеспечение непрерывной работы организации;
- юридический раздел, подтверждающий соответствие политики безопасности действующему законодательству.

К среднему уровню можно отнести вопросы, касающиеся отдельных аспектов информационной безопасности, но важные для различных эксплуатируемых организацией систем. Примеры таких вопросов – отношение к передовым (но, возможно, недостаточно проверенным) технологиям, доступ в Internet (как совместить свободу доступа к информации с защитой от внешних угроз?), использование домашних компьютеров, применение пользователями неофициального программного обеспечения и т.д.

Политика среднего уровня должна для каждого аспекта освещать следующие темы:

Описание аспекта. Например, если рассмотреть применение пользователями неофициального программного обеспечения, последнее можно определить как ПО, которое не было одобрено и/или закуплено на уровне организации.

Область применения. Следует определить, где, когда, как, по отношению к кому и чему применяется данная политика безопасности. Например, касается ли политика, связанная с использованием неофициального программного обеспечения, организаций-субподрядчиков? Затрагивает ли она сотрудников, пользующихся портативными и домашними компьютерами и вынужденных переносить информацию на производственные машины?

Позиция организации по данному аспекту. Продолжая пример с неофициальным программным обеспечением, можно представить себе позиции полного запрета, выработки процедуры приемки подобного ПО и т.п. Позиция может быть сформулирована и в гораздо более общем виде, как набор целей, которые преследует организация в данном аспекте. Вообще стиль документов, определяющих политику

безопасности (как и их перечень), в разных организациях может сильно отличаться.

Роли и обязанности. В "политический" документ необходимо включить информацию о должностных лицах, ответственных за реализацию политики безопасности. Например, если для использования неофициального программного обеспечения сотрудникам требуется разрешение руководства, должно быть известно, у кого и как его можно получить. Если неофициальное программное обеспечение использовать нельзя, следует знать, кто следит за выполнением данного правила.

Законопослушность. Политика должна содержать общее описание запрещенных действий и наказаний за них.

Точки контакта. Должно быть известно, куда следует обращаться за разъяснениями, помощью и дополнительной информацией. Обычно "точкой контакта" служит определенное должностное лицо, а не конкретный человек, занимающий в данный момент данный пост.

Политика безопасности нижнего уровня относится к конкретным информационным сервисам. Она включает в себя два аспекта – цели и правила их достижения, поэтому ее порой трудно отделить от вопросов реализации. В отличие от двух верхних уровней, рассматриваемая политика должна быть определена более подробно. Есть много вещей, специфичных для отдельных видов услуг, которые нельзя единым образом регламентировать в рамках всей организации. В то же время, эти вещи настолько важны для обеспечения режима безопасности, что относящиеся к ним решения должны приниматься на управленческом, а не техническом уровне. Приведем несколько примеров вопросов, на которые следует дать ответ в политике безопасности нижнего уровня:

- кто имеет право доступа к объектам, поддерживаемым сервисом?
- при каких условиях можно читать и модифицировать данные?
- как организован удаленный доступ к сервису?

При формулировке целей политики нижнего уровня можно исходить из соображений целостности, доступности и конфиденциальности, но нельзя на этом останавливаться. Ее цели должны быть более конкретными. Например, если речь идет о системе расчета заработной платы, можно поставить цель, чтобы только сотрудникам отдела кадров и бухгалтерии позволялось вводить и модифицировать информацию. В более общем случае цели должны связывать между собой объекты сервиса и действия с ними.

Из целей выводятся правила безопасности, описывающие, кто, что и при каких условиях может делать. Чем подробнее правила, чем более формально они изложены, тем проще поддержать их выполнение программно-техническими средствами. С другой стороны, слишком жесткие пра-

вила могут мешать работе пользователей, вероятно, их придется часто пересматривать. Руководству предстоит найти разумный компромисс, когда за приемлемую цену будет обеспечен приемлемый уровень безопасности, а сотрудники не окажутся чрезмерно связаны. Обычно наиболее формально задаются права доступа к объектам ввиду особой важности данного вопроса.

Программа безопасности

После того, как сформулирована политика безопасности, можно приступать к составлению программы ее реализации и собственно к реализации.

Чтобы понять и реализовать какую-либо программу, ее нужно структурировать по уровням, обычно в соответствии со структурой организации. В простейшем и самом распространенном случае достаточно двух уровней – верхнего, или центрального, который охватывает всю организацию, и нижнего, или служебного, который относится к отдельным услугам или группам однородных сервисов.

Программу верхнего уровня возглавляет лицо, отвечающее за информационную безопасность организации. У этой программы следующие главные цели:

- управление рисками (оценка рисков, выбор эффективных средств защиты);
- координация деятельности в области информационной безопасности, пополнение и распределение ресурсов;
- стратегическое планирование;
- контроль деятельности в области информационной безопасности.

В рамках программы верхнего уровня принимаются стратегические решения по обеспечению безопасности, оцениваются технологические новинки. Информационные технологии развиваются очень быстро, и необходимо иметь четкую политику отслеживания и внедрения новых средств.

Контроль деятельности в области безопасности имеет двустороннюю направленность. Во-первых, необходимо гарантировать, что действия организации не противоречат законам. При этом следует поддерживать контакты с внешними контролирующими организациями. Во-вторых, нужно постоянно отслеживать состояние безопасности внутри организации, реагировать на случаи нарушений и дорабатывать защитные меры с учетом изменения обстановки.

Следует подчеркнуть, что программа верхнего уровня должна занимать строго определенное место в деятельности организации, она должна

официально приниматься и поддерживаться руководством, а также иметь определенный штат и бюджет.

Цель программы нижнего уровня – обеспечить надежную и экономичную защиту конкретного сервиса или группы однородных сервисов. На этом уровне решается, какие следует использовать механизмы защиты; закупаются и устанавливаются технические средства; выполняется повседневное администрирование; отслеживается состояние слабых мест и т.п. Обычно за программу нижнего уровня отвечают администраторы сервисов.

Синхронизация программы безопасности с жизненным циклом систем

Если синхронизировать программу безопасности нижнего уровня с жизненным циклом защищаемого сервиса, можно добиться большего эффекта с меньшими затратами. Программисты знают, что добавить новую возможность к уже готовой системе на порядок сложнее, чем изначально спроектировать и реализовать ее. То же справедливо и для информационной безопасности.

В жизненном цикле информационного сервиса можно выделить следующие этапы:

Инициация. На данном этапе выявляется необходимость в приобретении нового сервиса, документируется его предполагаемое назначение.

Закупка. На данном этапе составляются спецификации, прорабатываются варианты приобретения, выполняется собственно закупка.

Установка. Сервис устанавливается, конфигурируется, тестируется и вводится в эксплуатацию.

Эксплуатация. На данном этапе сервис не только работает и администрируется, но и подвергается модификациям.

Выведение из эксплуатации. Происходит переход на новый сервис.

Рассмотрим действия, выполняемые на каждом из этапов, более подробно.

На этапе инициации оформляется понимание того, что необходимо приобрести новый или значительно модернизировать существующий сервис; определяется, какими характеристиками и какой функциональностью он должен обладать; оцениваются финансовые и иные ограничения.

С точки зрения безопасности важнейшим действием здесь является оценка критичности как самого сервиса, так и информации, которая с его помощью будет обрабатываться. Требуется сформулировать ответы на следующие вопросы:

- какого рода информация предназначается для обслуживания новым сервисом?

- каковы возможные последствия нарушения конфиденциальности, целостности и доступности этой информации?
- каковы угрозы, по отношению к которым сервис и информация будут наиболее уязвимы?
- есть ли какие-либо особенности нового сервиса (например, территориальная распределенность компонентов), требующие принятия специальных процедурных мер?
- каковы характеристики персонала, имеющие отношение к безопасности (квалификация, благонадежность)?
- каковы законодательные положения и внутренние правила, которым должен соответствовать новый сервис?

Результаты оценки критичности являются отправной точкой в составлении спецификаций. Кроме того, они определяют ту меру внимания, которую служба безопасности организации должна уделять новому сервису на последующих этапах его жизненного цикла.

Этап закупки – один из самых сложных. Нужно окончательно сформулировать требования к защитным средствам нового сервиса, к компании, которая может претендовать на роль поставщика, и к квалификации, которой должен обладать персонал, использующий или обслуживающий закупаемый продукт. Все эти сведения оформляются в виде спецификации, куда входят не только аппаратура и программы, но и документация, обслуживание, обучение персонала. Разумеется, особое внимание должно уделяться вопросам совместимости нового сервиса с существующей конфигурацией. Подчеркнем также, что нередко средства безопасности являются необязательными компонентами коммерческих продуктов, и нужно проследить, чтобы соответствующие пункты не выпали из спецификации.

Когда продукт закуплен, его необходимо установить. Несмотря на кажущуюся простоту, установка является очень ответственным делом. Во-первых, новый продукт следует сконфигурировать. Как правило, коммерческие продукты поставляются с отключенными средствами безопасности; их необходимо включить и должным образом настроить. Для большой организации, где много пользователей и данных, начальная настройка может стать весьма трудоемким и ответственным делом.

Во-вторых, новый сервис нуждается в процедурных регуляторах. Следует позаботиться о чистоте и охране помещения, о документах, регламентирующих использование сервиса, о подготовке планов на случай экстренных ситуаций, об организации обучения пользователей и т.п.

После принятия перечисленных мер необходимо провести тестирование. Его полнота и комплексность могут служить гарантией безопасности эксплуатации в штатном режиме.

Период эксплуатации – самый длительный и сложный. С психологической точки зрения наибольшую опасность в это время представляют незначительные изменения в конфигурации сервиса, в поведении пользователей и администраторов. Если безопасность не поддерживать, она ослабевает. Пользователи не столь ревностно выполняют должностные инструкции, администраторы менее тщательно анализируют регистрационную информацию. То один, то другой пользователь получает дополнительные привилегии. Кажется, что в сущности ничего не изменилось; на самом же деле от былой безопасности не осталось и следа.

Для борьбы с эффектом медленных изменений приходится прибегать к периодическим проверкам безопасности сервиса. Разумеется, после значительных модификаций подобные проверки являются обязательными.

При выведении из эксплуатации затрагиваются аппаратно-программные компоненты сервиса и обрабатываемые им данные. Аппаратура продается, утилизируется или выбрасывается. Только в специфических случаях необходимо заботиться о физическом разрушении аппаратных компонентов, хранящих конфиденциальную информацию. Программы, вероятно, просто стираются, если иное не предусмотрено лицензионным соглашением.

При выведении данных из эксплуатации их обычно переносят на другую систему, архивируют, выбрасывают или уничтожают. Если архивирование производится с намерением впоследствии прочитать данные в другом месте, следует позаботиться об аппаратно-программной совместимости средств чтения и записи. Информационные технологии развиваются очень быстро, и через несколько лет устройств, способных прочитать старый носитель, может просто не оказаться. Если данные архивируются в зашифрованном виде, необходимо сохранить ключ и средства расшифровки. При архивировании и хранении архивной информации нельзя забывать о поддержании конфиденциальности данных.

Вариант 1

1. Главная цель мер, предпринимаемых на административном уровне:

- ☐ сформировать программу безопасности и обеспечить ее выполнение
- ☐ выполнить положения действующего законодательства
- ☐ отчитаться перед вышестоящими инстанциями

2. В число целей политики безопасности верхнего уровня входят:

- ☐ решение сформировать или пересмотреть комплексную программу безопасности
- ☐ обеспечение базы для соблюдения законов и правил
- ☐ обеспечение конфиденциальности почтовых сообщений

3. В число этапов жизненного цикла информационного сервиса входят:

- ☐ закупка
- ☐ продажа
- ☐ выведение из эксплуатации

Вариант 2

1. Политика безопасности:

- ☐ фиксирует правила разграничения доступа
- ☐ отражает подход организации к защите своих информационных активов
- ☐ описывает способы защиты руководства организации

2. В число целей политики безопасности верхнего уровня входят:

- ☐ формулировка административных решений по важнейшим аспектам реализации программы безопасности
- ☐ выбор методов аутентификации пользователей
- ☐ обеспечение базы для соблюдения законов и правил

3. В число этапов жизненного цикла информационного сервиса входят:

- ☐ инициация
- ☐ терминация
- ☐ установка

Вариант 3

1. Политика безопасности строится на основе:

- ☐ общих представлений об ИС организации
- ☐ изучения политик родственных организаций
- ☐ анализа рисков

2. В число целей политики безопасности верхнего уровня входят:

- ☐ определение правил разграничения доступа
- ☐ формулировка целей, которые преследует организация в области информационной безопасности
- ☐ определение общих направлений в достижении целей безопасности

3. В число этапов жизненного цикла информационного сервиса входят:

- ☐ эксплуатация
- ☐ спецификация прав человека
- ☐ выведение из эксплуатации

Лекция 7. Управление рисками

Информационная безопасность должна достигаться экономически оправданными мерами. В лекции описывается методика, позволяющая сопоставить возможные потери от нарушений ИБ со стоимостью защитных средств.

Ключевые слова: управление рисками, оценка рисков, нейтрализация рисков, ликвидация риска, уменьшение риска, принятие риска, переадресация риска, методология оценки рисков, идентификация активов, анализ угроз, идентификация уязвимых мест, остаточный риск, жизненный цикл ИС, инициация, закупка, разработка, установка, эксплуатация, выведение из эксплуатации, выбор анализируемых объектов, выбор уровня детализации, миссия организации, карта ИС, идентификация угроз, источник угрозы, вероятность осуществления угрозы, предполагаемый ущерб, экранирование.

Основные понятия

Управление рисками рассматривается нами на административном уровне ИБ, поскольку только руководство организации способно выделить необходимые ресурсы, инициировать и контролировать выполнение соответствующих программ.

Вообще говоря, управление рисками, равно как и выработка собственной политики безопасности, актуально только для тех организаций, информационные системы которых и/или обрабатываемые данные можно считать нестандартными. Обычную организацию вполне устроит типовой набор защитных мер, выбранный на основе представления о типичных рисках или вообще без всякого анализа рисков (особенно это верно с формальной точки зрения, в свете проанализированного нами ранее российского законодательства в области ИБ). Можно провести аналогию между индивидуальным строительством и получением квартиры в районе массовой застройки. В первом случае необходимо принять множество решений, оформить большое количество бумаг, во втором достаточно определиться лишь с несколькими параметрами. Более подробно данный аспект рассмотрен в статье Сергея Симонова "Анализ рисков, управления рисками" (Jet Info, 1999, 1).

Использование информационных систем связано с определенной совокупностью рисков. Когда возможный ущерб неприемлемо велик, необходимо принять экономически оправданные меры защиты. Периоди-

ческая (пере)оценка рисков необходима для контроля эффективности деятельности в области безопасности и для учета изменений обстановки.

С количественной точки зрения уровень риска является функцией вероятности реализации определенной угрозы (использующей некоторые уязвимые места), а также величины возможного ущерба.

Таким образом, суть мероприятий по управлению рисками состоит в том, чтобы оценить их размер, выработать эффективные и экономичные меры снижения рисков, а затем убедиться, что риски заключены в приемлемые рамки (и остаются таковыми). Следовательно, управление рисками включает в себя два вида деятельности, которые чередуются циклически:

- (пере)оценка (измерение) рисков;
- выбор эффективных и экономичных защитных средств (нейтрализация рисков).

По отношению к выявленным рискам возможны следующие действия:

- ликвидация риска (например, за счет устранения причины);
- уменьшение риска (например, за счет использования дополнительных защитных средств);
- принятие риска (и выработка плана действия в соответствующих условиях);
- переадресация риска (например, путем заключения страхового соглашения).

Процесс управления рисками можно разделить на следующие этапы:

1. Выбор анализируемых объектов и уровня детализации их рассмотрения.
2. Выбор методологии оценки рисков.
3. Идентификация активов.
4. Анализ угроз и их последствий, выявление уязвимых мест в защите.
5. Оценка рисков.
6. Выбор защитных мер.
7. Реализация и проверка выбранных мер.
8. Оценка остаточного риска.

Этапы 6 и 7 относятся к выбору защитных средств (нейтрализации рисков), остальные – к оценке рисков.

Уже перечисление этапов показывает, что управление рисками – процесс циклический. По существу, последний этап – это оператор конца цикла, предписывающий вернуться к началу. Риски нужно контролировать постоянно, периодически проводя их переоценку. Отметим, что добросовестно выполненная и тщательно документированная первая оценка может существенно упростить последующую деятельность.

Управление рисками, как и любую другую деятельность в области информационной безопасности, необходимо интегрировать в жизненный цикл ИС. Тогда эффект оказывается наибольшим, а затраты – минимальными. Ранее мы определили пять этапов жизненного цикла. Кратко опишем, что может дать управление рисками на каждом из них.

На этапе инициации известные риски следует учесть при выработке требований к системе вообще и средствам безопасности в частности.

На этапе закупки (разработки) знание рисков поможет выбрать соответствующие архитектурные решения, которые играют ключевую роль в обеспечении безопасности.

На этапе установки выявленные риски следует учитывать при конфигурировании, тестировании и проверке ранее сформулированных требований, а полный цикл управления рисками должен предшествовать внедрению системы в эксплуатацию.

На этапе эксплуатации управление рисками должно сопровождать все существенные изменения в системе.

При выведении системы из эксплуатации управление рисками помогает убедиться в том, что миграция данных происходит безопасным образом.

Подготовительные этапы управления рисками

В этом разделе будут описаны первые три этапа процесса управления рисками.

Выбор анализируемых объектов и уровня детализации их рассмотрения – первый шаг в оценке рисков. Для небольшой организации допустимо рассматривать всю информационную инфраструктуру; однако если организация крупная, всеобъемлющая оценка может потребовать неприемлемых затрат времени и сил. В таком случае следует сосредоточиться на наиболее важных сервисах, заранее соглашаясь с приближенностью итоговой оценки. Если важных сервисов все еще много, выбираются те из них, риски для которых заведомо велики или неизвестны.

Мы уже указывали на целесообразность создания карты информационной системы организации. Для управления рисками подобная карта особенно важна, поскольку она наглядно показывает, какие сервисы выбраны для анализа, а какими пришлось пренебречь. Если ИС меняется, а карта поддерживается в актуальном состоянии, то при переоценке рисков сразу станет ясно, какие новые или существенно изменившиеся сервисы нуждаются в рассмотрении.

Вообще говоря, уязвимым является каждый компонент информационной системы – от сетевого кабеля, который могут прогрызть мыши, до базы данных, которая может быть разрушена из-за неумелых действий администратора. Как правило, в сферу анализа невозможно включить каж-

дый винтик и каждый байт. Приходится останавливаться на некотором уровне детализации, опять-таки отдавая себе отчет в приближенности оценки. Для новых систем предпочтителен детальный анализ; старая система, подвергшаяся небольшим модификациям, может быть проанализирована более поверхностно.

Очень важно выбрать разумную методологию оценки рисков. Целью оценки является получение ответа на два вопроса: приемлемы ли существующие риски, и если нет, то какие защитные средства стоит использовать. Значит, оценка должна быть количественной, допускающей сопоставление с заранее выбранными границами допустимости и расходами на реализацию новых регуляторов безопасности. Управление рисками – типичная оптимизационная задача, и существует довольно много программных продуктов, способных помочь в ее решении (иногда подобные продукты просто прилагаются к книгам по информационной безопасности). Принципиальная трудность, однако, состоит в неточности исходных данных. Можно, конечно, попытаться получить для всех анализируемых величин денежное выражение, высчитать все с точностью до копейки, но большого смысла в этом нет. Практичнее пользоваться условными единицами. В простейшем и вполне допустимом случае можно пользоваться трехбалльной шкалой. Далее мы продемонстрируем, как это делается.

При идентификации активов, то есть тех ресурсов и ценностей, которые организация пытается защитить, следует, конечно, учитывать не только компоненты информационной системы, но и поддерживающую инфраструктуру, персонал, а также нематериальные ценности, такие как репутация организации. Отправной точкой здесь является представление о миссии организации, то есть об основных направлениях деятельности, которые желательно (или необходимо) сохранить в любом случае. Выражаясь объектно-ориентированным языком, следует в первую очередь описать внешний интерфейс организации, рассматриваемой как абстрактный объект.

Одним из главных результатов процесса идентификации активов является получение детальной информационной структуры организации и способов ее (структуры) использования. Эти сведения целесообразно нанести на карту ИС в качестве граней соответствующих объектов.

Информационной основой сколько-нибудь крупной организации является сеть, поэтому в число аппаратных активов следует включить компьютеры (серверы, рабочие станции, ПК), периферийные устройства, внешние интерфейсы, кабельное хозяйство, активное сетевое оборудование (мосты, маршрутизаторы и т.п.). К программным активам, вероятно, будут отнесены операционные системы (сетевая, серверные и клиентские), прикладное программное обеспечение, инструментальные

средства, средства управления сетью и отдельными системами. Важно зафиксировать, где (в каких узлах сети) хранится программное обеспечение, и из каких узлов оно используется. Третьим видом информационных активов являются данные, которые хранятся, обрабатываются и передаются по сети. Следует классифицировать данные по типам и степени конфиденциальности, выявить места их хранения и обработки, способы доступа к ним. Все это важно для оценки последствий нарушений информационной безопасности.

Управление рисками – процесс далеко не линейный. Практически все его этапы связаны между собой, и по завершении почти любого из них может возникнуть необходимость возврата к предыдущему. Так, при идентификации активов может оказаться, что выбранные границы анализа следует расширить, а степень детализации – увеличить. Особенно труден первичный анализ, когда многократные возвраты к началу неизбежны.

Основные этапы управления рисками

Этапы, предшествующие анализу угроз, можно считать подготовительными, поскольку, строго говоря, они напрямую с рисками не связаны. Риск появляется там, где есть угрозы.

Краткий перечень наиболее распространенных угроз был рассмотрен нами ранее. К сожалению, на практике угроз гораздо больше, причем далеко не все из них носят компьютерный характер. Так, вполне реальной угрозой является наличие мышей и тараканов в занимаемых организацией помещениях. Первые могут повредить кабели, вторые вызвать короткое замыкание. Как правило, наличие той или иной угрозы является следствием пробелов в защите информационной системы, которые, в свою очередь, объясняются отсутствием некоторых сервисов безопасности или недостатками в реализующих их защитных механизмах. Опасность прогрызания кабелей возникает не просто там, где есть мыши, она связана с отсутствием или недостаточной прочностью защитной оболочки.

Первый шаг в анализе угроз – их идентификация. Рассматриваемые виды угроз следует выбирать исходя из соображений здравого смысла (исключив, например, землетрясения, однако не забывая о возможности захвата организации террористами), но в пределах выбранных видов провести максимально подробный анализ.

Целесообразно выявлять не только сами угрозы, но и источники их возникновения – это поможет в выборе дополнительных средств защиты. Например, нелегальный вход в систему может стать следствием воспроизведения начального диалога, подбора пароля или подключения к сети неавторизованного оборудования. Очевидно, для противодействия каждому из перечисленных способов нелегального входа нужны свои механизмы безопасности.

После идентификации угрозы необходимо оценить вероятность ее осуществления. Допустимо использовать при этом трехбалльную шкалу (низкая (1), средняя (2) и высокая (3) вероятность).

Кроме вероятности осуществления, важен размер потенциального ущерба. Например, пожары бывают нечасто, но ущерб от каждого из них, как правило, велик. Тяжесть ущерба также можно оценить по трехбалльной шкале.

Оценивая размер ущерба, необходимо иметь в виду не только непосредственные расходы на замену оборудования или восстановление информации, но и более отдаленные, такие как подрыв репутации, ослабление позиций на рынке и т.п. Пусть, например, в результате дефектов в управлении доступом к бухгалтерской информации сотрудники получили возможность корректировать данные о собственной заработной плате. Следствием такого состояния дел может стать не только перерасход бюджетных или корпоративных средств, но и полное разложение коллектива, грозящее развалом организации.

Уязвимые места обладают свойством притягивать к себе не только злоумышленников, но и сравнительно честных людей. Не всякий устоит перед искушением немного увеличить свою зарплату, если есть уверенность, что это сойдет в рук. Поэтому, оценивая вероятность осуществления угроз, целесообразно исходить не только из среднестатистических данных, но учитывать также специфику конкретных информационных систем. Если в подвале дома, занимаемого организацией, располагается сауна, а сам дом имеет деревянные перекрытия, то вероятность пожара, к сожалению, оказывается существенно выше средней.

После того, как накоплены исходные данные и оценена степень неопределенности, можно переходить к обработке информации, то есть собственно к оценке рисков. Вполне допустимо применить такой простой метод, как умножение вероятности осуществления угрозы на предполагаемый ущерб. Если для вероятности и ущерба использовать трехбалльную шкалу, то возможных произведений будет шесть: 1, 2, 3, 4, 6 и 9. Первые два результата можно отнести к низкому риску, третий и четвертый – к среднему, два последних – к высокому, после чего появляется возможность снова привести их к трехбалльной шкале. По этой шкале и следует оценивать приемлемость рисков. Правда, граничные случаи, когда вычисленная величина совпала с приемлемой, целесообразно рассматривать более тщательно из-за приближенного характера результата.

Если какие-либо риски оказались недопустимо высокими, необходимо их нейтрализовать, реализовав дополнительные меры защиты. Как правило, для ликвидации или нейтрализации уязвимого места, сделавшего угрозу реальной, существует несколько механизмов безопасности, различных по эффективности и стоимости. Например, если велика вероят-

ность нелегального входа в систему, можно потребовать, чтобы пользователи выбирали длинные пароли (скажем, не менее восьми символов), задействовать программу генерации паролей или закупить интегрированную систему аутентификации на основе интеллектуальных карт. Если есть вероятность умышленного повреждения сервера баз данных, что может иметь серьезные последствия, можно врезать замок в дверь серверной комнаты или поставить около каждого сервера по охраннику.

Оценивая стоимость мер защиты, приходится, разумеется, учитывать не только прямые расходы на закупку оборудования и/или программ, но и расходы на внедрение новинки и, в частности, обучение и переподготовку персонала. Эту стоимость также можно оценить по трехбалльной шкале и затем сопоставить ее с разностью между вычисленным и допустимым риском. Если по этому показателю новое средство оказывается экономически выгодным, его можно взять на заметку (подходящих средств, вероятно, будет несколько). Однако если средство окажется дорогим, его не следует сразу отбрасывать, памятуя о приближенности расчетов.

Выбирая подходящий способ защиты, целесообразно учитывать возможность экранирования одним механизмом обеспечения безопасности сразу нескольких прикладных сервисов. Так поступили в Массачусетском технологическом институте, защитив несколько тысяч компьютеров сервером аутентификации Kerberos.

Важным обстоятельством является совместимость нового средства со сложившейся организационной и аппаратно-программной структурой, с традициями организации. Меры безопасности, как правило, носят недружественный характер, что может отрицательно сказаться на энтузиазме сотрудников. Порой сохранение духа открытости важнее минимизации материальных потерь. Впрочем, такого рода ориентиры должны быть расставлены в политике безопасности верхнего уровня.

Можно представить себе ситуацию, когда для нейтрализации риска не существует эффективных и приемлемых по цене мер. Например, компания, базирующаяся в сейсмически опасной зоне, не всегда может позволить себе строительство защищенной штаб-квартиры. В таком случае приходится поднимать планку приемлемого риска и переносить центр тяжести на смягчение последствий и выработку планов восстановления после аварий, стихийных бедствий и иных происшествий. Продолжая пример с сейсмоопасностью, можно рекомендовать регулярное тиражирование данных в другой город и овладение средствами восстановления первичной базы данных.

Как и всякую иную деятельность, реализацию и проверку новых регуляторов безопасности следует предварительно планировать. В плане необходимо учесть наличие финансовых средств и сроки обуче-

ния персонала. Если речь идет о программно-техническом механизме защиты, нужно составить план тестирования (автономного и комплексного).

Когда намеченные меры приняты, необходимо проверить их действенность, то есть убедиться, что остаточные риски стали приемлемыми. Если это на самом деле так, значит, можно спокойно намечать дату ближайшей переоценки. В противном случае придется проанализировать допущенные ошибки и провести повторный сеанс управления рисками немедленно.

Вариант 1

1. Риск является функцией:

- ☐ вероятности реализации угрозы
- ☐ размера возможного ущерба
- ☐ числа уязвимых мест в системе

2. В число возможных стратегий нейтрализации рисков входят:

- ☐ ликвидация риска
- ☐ игнорирование риска
- ☐ принятие риска

3. В число этапов управления рисками входят:

- ☐ идентификация активов
- ☐ ликвидация пассивов
- ☐ выбор анализируемых объектов

4. Первый шаг в анализе угроз - это:

- ☐ идентификация угроз
- ☐ аутентификация угроз
- ☐ ликвидация угроз

Вариант 2

1. Риск является функцией:

- ☐ размера возможного ущерба
- ☐ числа уязвимых мест в системе
- ☐ уставного капитала организации

2. В число возможных стратегий нейтрализации рисков входят:

- ☐ уменьшение риска
- ☐ сокрытие риска
- ☐ афиширование риска

3. В число этапов управления рисками входят:

- ☐ оценка рисков
- ☐ выбор уровня детализации анализируемых объектов
- ☐ наказание за создание уязвимостей

4. После идентификации угрозы необходимо оценить:

- ☐ вероятность ее осуществления
- ☐ ущерб от ее осуществления
- ☐ частоту ее осуществления

Вариант 3

1. Риск является функцией:

- ☐ вероятности реализации угрозы
- ☐ стоимости защитных средств
- ☐ числа уязвимых мест в системе

2. В число возможных стратегий нейтрализации рисков входят:

- ☐ переадресация риска
- ☐ деноминация риска
- ☐ декомпозиция риска

3. В число этапов управления рисками входят:

- ☐ анализ угроз
- ☐ угрозы проведения анализа
- ☐ выявление уязвимых мест

4 При анализе стоимости защитных мер не следует учитывать:

- ☐ расходы на закупку оборудования
- ☐ расходы на закупку программ
- ☐ расходы на обучение персонала

Лекция 8. Процедурный уровень информационной безопасности

Описываются основные классы мер процедурного уровня. Формулируются принципы, позволяющие обеспечить надежную защиту.

Ключевые слова: процедурный уровень ИБ, управление персоналом, физическая защита, поддержание работоспособности, реагирование на нарушения режима безопасности, планирование восстановительных работ, разделение обязанностей, минимизация привилегий, описание должности, обучение, непрерывность защиты в пространстве и времени, физическое управление доступом, периметр безопасности, контролируемая территория, объектный подход, противопожарные меры, защита поддерживающей инфраструктуры, защита от перехвата данных, защита мобильных систем, поддержка пользователей, поддержка программного обеспечения, конфигурационное управление, резервное копирование, управление носителями, документирование, регламентные работы, локализация инцидента, уменьшение наносимого вреда, прослеживание нарушителя, предупреждение повторных нарушений, отслеживание новых уязвимых мест, критически важные функции, идентификация ресурсов, стратегия восстановительных работ, персонал, информационная инфраструктура, физическая инфраструктура.

Основные классы мер процедурного уровня

Мы приступаем к рассмотрению мер безопасности, которые ориентированы на людей, а не на технические средства. Именно люди формируют режим информационной безопасности, и они же оказываются главной угрозой, поэтому "человеческий фактор" заслуживает особого внимания.

В российских компаниях накоплен богатый опыт регламентирования и реализации процедурных (организационных) мер, однако дело в том, что они пришли из "докомпьютерного" прошлого, поэтому требуют переоценки.

Следует осознать ту степень зависимости от компьютерной обработки данных, в которую попало современное общество. Без всякого преувеличения можно сказать, что необходима информационная гражданская оборона. Спокойно, без нагнетания страстей, нужно разъяснять общест-

ву не только преимущества, но и опасности, связанные с использованием информационных технологий. Акцент следует делать не на военной или криминальной стороне дела, а на гражданских аспектах, связанных с поддержанием нормального функционирования аппаратного и программного обеспечения, то есть концентрироваться на вопросах доступности и целостности данных.

На процедурном уровне можно выделить следующие классы мер:

- управление персоналом;
- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

Управление персоналом

Управление персоналом начинается с приема нового сотрудника на работу и даже раньше – с составления описания должности. Уже на данном этапе желательно подключить к работе специалиста по информационной безопасности для определения компьютерных привилегий, ассоциируемых с должностью. Существует два общих принципа, которые следует иметь в виду:

- разделение обязанностей;
- минимизация привилегий.

Принцип разделения обязанностей предписывает так распределять роли и ответственность, чтобы один человек не мог нарушить критически важный для организации процесс. Например, нежелательна ситуация, когда крупные платежи от имени организации выполняет один человек. Надежнее поручить одному сотруднику оформление заявок на подобные платежи, а другому – заверять эти заявки. Другой пример – процедурные ограничения действий суперпользователя. Можно искусственно "расщепить" пароль суперпользователя, сообщив первую его часть одному сотруднику, а вторую – другому. Тогда критически важные действия по администрированию ИС они смогут выполнить только вдвоем, что снижает вероятность ошибок и злоупотреблений.

Принцип минимизации привилегий предписывает выделять пользователям только те права доступа, которые необходимы им для выполнения служебных обязанностей. Назначение этого принципа очевидно – уменьшить ущерб от случайных или умышленных некорректных действий.

Предварительное составление описания должности позволяет оценить ее критичность и спланировать процедуру проверки и отбора кандидатов. Чем ответственнее должность, тем тщательнее нужно проверять кандидатов: навести о них справки, быть может, побеседовать с бывшими сослужив-

цами и т.д. Подобная процедура может быть длительной и дорогой, поэтому нет смысла дополнительно усложнять ее. В то же время, неразумно и совсем отказываться от предварительной проверки, чтобы случайно не принять на работу человека с уголовным прошлым или психическим заболеванием.

Когда кандидат определен, он, вероятно, должен пройти обучение; по крайней мере, его следует подробно ознакомить со служебными обязанностями, а также с нормами и процедурами информационной безопасности. Желательно, чтобы меры безопасности были им усвоены до вступления в должность и до заведения его системного счета с входным именем, паролем и привилегиями.

С момента заведения системного счета начинается его администрирование, а также протоколирование и анализ действий пользователя. Постепенно изменяется окружение, в котором работает пользователь, его служебные обязанности и т.п. Все это требует соответствующего изменения привилегий. Техническую сложность представляют временные перемещения пользователя, выполнение им обязанностей взамен сотрудника, ушедшего в отпуск, и иные обстоятельства, когда полномочия нужно сначала предоставить, а через некоторое время взять обратно. В такие периоды профиль активности пользователя резко меняется, что создает трудности при выявлении подозрительных ситуаций. Определенную аккуратность следует соблюдать и при выдаче новых постоянных полномочий, не забывая ликвидировать старые права доступа.

Ликвидация системного счета пользователя, особенно в случае конфликта между сотрудником и организацией, должна производиться максимально оперативно (в идеале – одновременно с извещением о наказании или увольнении). Возможно и физическое ограничение доступа к рабочему месту. Разумеется, если сотрудник увольняется, у него нужно принять все его компьютерное хозяйство и, в частности, криптографические ключи, если использовались средства шифрования.

К управлению сотрудниками примыкает администрирование лиц, работающих по контракту (например, специалистов фирмы-поставщика, помогающих запустить новую систему). В соответствии с принципом минимизации привилегий, им нужно выделить ровно столько прав, сколько необходимо, и изъять эти права сразу по окончании контракта. Проблема, однако, состоит в том, что на начальном этапе внедрения "внешние" сотрудники будут администрировать "местных", а не наоборот. Здесь на первый план выходит квалификация персонала организации, его способность быстро обучаться, а также оперативное проведение учебных курсов. Важны и принципы выбора деловых партнеров.

Иногда внешние организации принимают на обслуживание и администрирование ответственные компоненты компьютерной системы, например, сетевое оборудование. Нередко администрирование выполняется в удаленном

режиме. Вообще говоря, это создает в системе дополнительные уязвимые места, которые необходимо компенсировать усиленным контролем средств удаленного доступа или, опять-таки, обучением собственных сотрудников.

Мы видим, что проблема обучения – одна из основных с точки зрения информационной безопасности. Если сотрудник не знаком с политикой безопасности своей организации, он не может стремиться к достижению сформулированных в ней целей. Не зная мер безопасности, он не сможет их соблюдать. Напротив, если сотрудник знает, что его действия протоколируются, он, возможно, воздержится от нарушений.

Физическая защита

Безопасность информационной системы зависит от окружения, в котором она функционирует. Необходимо принять меры для защиты зданий и прилегающей территории, поддерживающей инфраструктуры, вычислительной техники, носителей данных.

Основной принцип физической защиты, соблюдение которого следует постоянно контролировать, формулируется как "непрерывность защиты в пространстве и времени". Ранее мы рассматривали понятие окна опасности. Для физической защиты таких окон быть не должно.

Мы кратко рассмотрим следующие направления физической защиты:

- физическое управление доступом;
- противопожарные меры;
- защита поддерживающей инфраструктуры;
- защита от перехвата данных;
- защита мобильных систем.

Меры физического управления доступом позволяют контролировать и при необходимости ограничивать вход и выход сотрудников и посетителей. Контролироваться может все здание организации, а также отдельные помещения, например, те, где расположены серверы, коммуникационная аппаратура и т.п.

При проектировании и реализации мер физического управления доступом целесообразно применять объектный подход. Во-первых, определяется периметр безопасности, ограничивающий контролируемую территорию. На этом уровне детализации важно продумать внешний интерфейс организации – порядок входа/выхода штатных сотрудников и посетителей, вноса/выноса техники. Все, что не входит во внешний интерфейс, должно быть инкапсулировано, то есть защищено от нелегальных проникновений.

Во-вторых, производится декомпозиция контролируемой территории, выделяются (под)объекты и связи (проходы) между ними. При такой, более глубокой детализации следует выделить среди подъобектов наиболее критичные с точки зрения безопасности и обеспечить им повышенное

внимание. Декомпозиция должна быть семантически оправданной, обеспечивающей разграничение разнородных сущностей, таких как оборудование разных владельцев или персонал, работающий с данными разной степени критичности. Важно сделать так, чтобы посетители, по возможности, не имели непосредственного доступа к компьютерам или, в крайнем случае, позаботиться о том, чтобы от окон и дверей не просматривались экраны мониторов и принтеры. Необходимо, чтобы посетителей по внешнему виду можно было отличить от сотрудников. Если отличие состоит в том, что посетителям выдаются идентификационные карточки, а сотрудники ходят "без опознавательных знаков", злоумышленнику достаточно снять карточку, чтобы его считали "своим". Очевидно, соответствующие карточки нужно выдавать всем.

Средства физического управления доступом известны давно. Это охрана, двери с замками, перегородки, телекамеры, датчики движения и многое другое. Для выбора оптимального (по критерию стоимость/эффективность) средства целесообразно провести анализ рисков (к этому мы еще вернемся). Кроме того, есть смысл периодически отслеживать появление технических новинок в данной области, стараясь максимально автоматизировать физическую защиту.

Более подробно данная тема рассмотрена в статье В. Барсукова "Физическая защита информационных систем" (Jet Info, 1997, 1).

Профессия пожарника – одна из древнейших, но пожары по-прежнему случаются и наносят большой ущерб. Мы не собираемся цитировать параграфы противопожарных инструкций или изобретать новые методы борьбы с огнем – на это есть профессионалы. Отметим лишь необходимость установки противопожарной сигнализации и автоматических средств пожаротушения. Обратим также внимание на то, что защитные меры могут создавать новые слабые места. Если на работу взят новый охранник, это, вероятно, улучшает физическое управление доступом. Если же он по ночам курит и пьет, то ввиду повышенной пожароопасности подобная мера защиты может только навредить.

К поддерживающей инфраструктуре можно отнести системы электро-, водо- и теплоснабжения, кондиционеры и средства коммуникаций. В принципе, к ним применимы те же требования целостности и доступности, что и к информационным системам. Для обеспечения целостности нужно защищать оборудование от краж и повреждений. Для поддержания доступности следует выбирать оборудование с максимальным временем наработки на отказ, дублировать ответственные узлы и всегда иметь под рукой запчасти.

Отдельную проблему составляют аварии водопровода. Они происходят нечасто, но могут нанести огромный ущерб. При размещении компьютеров необходимо принять во внимание расположение водопроводных и

канализационных труб и постараться держаться от них подальше. Сотрудники должны знать, куда следует обращаться при обнаружении протечек.

Перехват данных (о чем мы уже писали) может осуществляться самыми разными способами. Злоумышленник может подсматривать за экраном монитора, читать пакеты, передаваемые по сети, производить анализ побочных электромагнитных излучений и наводок (ПЭМИН) и т.д. Остается уповать на повсеместное использование криптографии (что, впрочем, сопряжено у нас в стране со множеством технических и законодательных проблем), стараться максимально расширить контролируемую территорию, разместившись в тихом особнячке, поодаль от других домов, пытаться держать под контролем линии связи (например, заключать их в надувную оболочку с обнаружением прокалывания), но самое разумное, вероятно, – постараться осознать, что для коммерческих систем обеспечение конфиденциальности является все-таки не главной задачей.

Желающим подробнее ознакомиться с вопросом мы рекомендуем прочитать статью В. Барсукова "Блокирование технологических каналов утечки информации" (Jet Info, 1998, 5-6).

Мобильные и портативные компьютеры – заманчивый объект кражи. Их часто оставляют без присмотра, в автомобиле или на работе, и похитить такой компьютер совсем несложно. То и дело средства массовой информации сообщают о том, что какой-нибудь офицер английской разведки или американский военный лишился таким образом движимого имущества. Мы настоятельно рекомендуем шифровать данные на жестких дисках таких компьютеров.

Вообще говоря, при выборе средств физической защиты следует производить анализ рисков. Так, принимая решение о закупке источника бесперебойного питания, необходимо учесть качество электропитания в здании, занимаемом организацией (впрочем, почти наверняка оно окажется плохим), характер и длительность сбоев электропитания, стоимость доступных источников и возможные потери от аварий (поломка техники, приостановка работы организации и т.п.) (см. также статью В.Барсукова "Защита компьютерных систем от силовых деструктивных воздействий" в Jet Info, 2000, 2). В то же время, во многих случаях решения очевидны. Меры противопожарной безопасности обязательны для всех организаций. Стоимость реализации многих мер (например, установка обычного замка на дверь серверной комнаты) либо мала, либо хоть и заметна, но все же явно меньше, чем возможный ущерб. В частности, имеет смысл регулярно копировать большие базы данных.

Поддержание работоспособности

Далее рассмотрим ряд рутинных мероприятий, направленных на поддержание работоспособности информационных систем. Именно

здесь таится наибольшая опасность. Нечаянные ошибки системных администраторов и пользователей грозят повреждением аппаратуры, разрушением программ и данных; в лучшем случае они создают бреши в защите, которые делают возможной реализацию угроз.

Недооценка факторов безопасности в повседневной работе – ахиллесова пята многих организаций. Дорогие средства безопасности теряют смысл, если они плохо документированы, конфликтуют с другим программным обеспечением, а пароль системного администратора не менялся с момента установки.

Можно выделить следующие направления повседневной деятельности:

- поддержка пользователей;
- поддержка программного обеспечения;
- конфигурационное управление;
- резервное копирование;
- управление носителями;
- документирование;
- регламентные работы.

Поддержка пользователей подразумевает прежде всего консультирование и оказание помощи при решении разного рода проблем. Иногда в организациях создают для этой цели специальный "справочный стол", но чаще от пользователей отбивается системный администратор. Очень важно в потоке вопросов уметь выявлять проблемы, связанные с информационной безопасностью. Так, многие трудности пользователей, работающих на персональных компьютерах, могут быть следствием заражения вирусами. Целесообразно фиксировать вопросы пользователей, чтобы выявлять их типичные ошибки и выпускать памятки с рекомендациями для распространенных ситуаций.

Поддержка программного обеспечения – одно из важнейших средств обеспечения целостности информации. Прежде всего, необходимо следить за тем, какое программное обеспечение установлено на компьютерах. Если пользователи будут устанавливать программы по своему усмотрению, это может привести к заражению вирусами, а также появлению утилит, действующих в обход защитных средств. Вполне вероятно также, что "самодеятельность" пользователей постепенно приведет к хаосу на их компьютерах, а исправлять ситуацию придется системному администратору.

Второй аспект поддержки программного обеспечения – контроль за отсутствием неавторизованного изменения программ и прав доступа к ним. Сюда же можно отнести поддержку эталонных копий программных систем. Обычно контроль достигается комбинированием средств физического и логического управления доступом, а также использованием утилит проверки и обеспечения целостности.

Конфигурационное управление позволяет контролировать и фиксировать изменения, вносимые в программную конфигурацию. Прежде всего, необходимо застраховаться от случайных или непродуманных модификаций, уметь как минимум возвращаться к прошлой, работающей, версии. Фиксация изменений позволит легко восстановить текущую версию после аварии.

Лучший способ уменьшить количество ошибок в рутинной работе – максимально автоматизировать ее. Правы те "ленивые" программисты и системные администраторы, которые, окинув взглядом море однообразных задач, говорят: "Я ни за что не буду делать этого; я напишу программу, которая сделает все за меня". Автоматизация и безопасность зависят друг от друга; тот, кто заботится в первую очередь об облегчении своей задачи, на самом деле оптимальным образом формирует режим информационной безопасности.

Резервное копирование необходимо для восстановления программ и данных после аварий. И здесь целесообразно автоматизировать работу, как минимум, сформировав компьютерное расписание создания полных и инкрементальных копий, а как максимум – воспользовавшись соответствующими программными продуктами (см., например, Jet Info, 2000, 12). Нужно также наладить размещение копий в безопасном месте, защищенном от несанкционированного доступа, пожаров, протечек, то есть от всего, что может привести к краже или повреждению носителей. Целесообразно иметь несколько экземпляров резервных копий и часть из них хранить вне территории организации, защищаясь таким образом от крупных аварий и аналогичных инцидентов.

Время от времени в тестовых целях следует проверять возможность восстановления информации с копий.

Управлять носителями необходимо для обеспечения физической защиты и учета дискет, лент, печатных выдач и т.п. Управление носителями должно обеспечивать конфиденциальность, целостность и доступность информации, хранящейся вне компьютерных систем. Под физической защитой здесь понимается не только отражение попыток несанкционированного доступа, но и предохранение от вредных влияний окружающей среды (жары, холода, влаги, магнетизма). Управление носителями должно охватывать весь жизненный цикл – от закупки до выведения из эксплуатации.

Документирование – неотъемлемая часть информационной безопасности. В виде документов оформляется почти все – от политики безопасности до журнала учета носителей. Важно, чтобы документация была актуальной, отражала именно текущее состояние дел, причем в непротиворечивом виде.

К хранению одних документов (содержащих, например, анализ уязвимых мест системы и угроз) применимы требования обеспечения кон-

фиденциальности, к другим, таким как план восстановления после аварий – требования целостности и доступности (в критической ситуации план необходимо найти и прочитать).

Регламентные работы – очень серьезная угроза безопасности. Сотрудник, осуществляющий регламентные работы, получает исключительный доступ к системе, и на практике очень трудно проконтролировать, какие именно действия он совершает. Здесь на первый план выходит степень доверия к тем, кто выполняет работу.

Реагирование на нарушения режима безопасности

Программа безопасности, принятая организацией, должна предусматривать набор оперативных мероприятий, направленных на обнаружение и нейтрализацию нарушений режима информационной безопасности. Важно, чтобы в подобных случаях последовательность действий была спланирована заранее, поскольку меры нужно принимать срочные и скоординированные.

Реакция на нарушения режима безопасности преследует три главные цели:

- локализация инцидента и уменьшение наносимого вреда;
- выявление нарушителя;
- предупреждение повторных нарушений.

В организации должен быть человек, доступный 24 часа в сутки (лично, по телефону, пейджеру или электронной почте), который отвечает за реакцию на нарушения. Все должны знать координаты этого человека и обращаться к нему при первых признаках опасности. В общем, как при пожаре, нужно знать, куда звонить, и что делать до приезда пожарной команды.

Важность быстрой и скоординированной реакции можно продемонстрировать на следующем примере. Пусть локальная сеть предприятия состоит из двух сегментов, администрируемых разными людьми. Далее, пусть в один из сегментов был внесен вирус. Почти наверняка через несколько минут (или, в крайнем случае, несколько десятков минут) вирус распространится и на другой сегмент. Значит, меры нужно принять немедленно. "Вычищать" вирус необходимо одновременно в обоих сегментах; в противном случае сегмент, восстановленный первым, заразится от другого, а затем вирус вернется и во второй сегмент.

Нередко требование локализации инцидента и уменьшения наносимого вреда вступает в конфликт с желанием выявить нарушителя. В политике безопасности организации приоритеты должны быть расставлены заранее. Поскольку, как показывает практика, выявить злоумышленника очень сложно, на наш взгляд, в первую очередь следует заботиться об уменьшении ущерба.

Чтобы найти нарушителя, нужно заранее выяснить контактные координаты поставщика сетевых услуг и договориться с ним о самой возможности и порядке выполнения соответствующих действий. Более подробно данная тема рассматривается в статье Н. Браунли и Э. Гатмэна "Как реагировать на нарушения информационной безопасности (RFC 2350, BCP 21)" (Jet Info, 2000, 5).

Чтобы предотвратить повторные нарушения, необходимо анализировать каждый инцидент, выявлять причины, накапливать статистику. Каковы источники вредоносного ПО? Какие пользователи имеют обыкновение выбирать слабые пароли? На подобные вопросы и должны дать ответ результаты анализа.

Необходимо отслеживать появление новых уязвимых мест и как можно быстрее ликвидировать ассоциированные с ними окна опасности. Кто-то в организации должен курировать этот процесс, принимать краткосрочные меры и корректировать программу безопасности для принятия долгосрочных мер.

Планирование восстановительных работ

Ни одна организация не застрахована от серьезных аварий, вызванных естественными причинами, действиями злоумышленника, халатностью или некомпетентностью. В то же время, у каждой организации есть функции, которые руководство считает критически важными, они должны выполняться несмотря ни на что. Планирование восстановительных работ позволяет подготовиться к авариям, уменьшить ущерб от них и сохранить способность к функционированию хотя бы в минимальном объеме.

Отметим, что меры информационной безопасности можно разделить на три группы, в зависимости от того, направлены ли они на предупреждение, обнаружение или ликвидацию последствий атак. Большинство мер носит предупредительный характер. Оперативный анализ регистрационной информации и некоторые аспекты реагирования на нарушения (так называемый активный аудит) служат для обнаружения и отражения атак. Планирование восстановительных работ, очевидно, можно отнести к последней из трех перечисленных групп.

Процесс планирования восстановительных работ можно разделить на следующие этапы:

- выявление критически важных функций организации, установление приоритетов;
- идентификация ресурсов, необходимых для выполнения критически важных функций;
- определение перечня возможных аварий;
- разработка стратегии восстановительных работ;

- подготовка к реализации *выбранной стратегии*;
- проверка стратегии.

Планируя восстановительные работы, следует отдавать себе отчет в том, что полностью сохранить функционирование организации не всегда возможно. Необходимо выявить критически важные функции, без которых организация теряет свое лицо, и даже среди критичных функций расставить приоритеты, чтобы как можно быстрее и с минимальными затратами возобновить работу после аварии.

Идентифицируя ресурсы, необходимые для выполнения критически важных функций, следует помнить, что многие из них имеют некомпьютерный характер. На данном этапе желательно подключать к работе специалистов разного профиля, способных в совокупности охватить все аспекты проблемы. Критичные ресурсы обычно относятся к одной из следующих категорий:

- персонал;
- информационная инфраструктура;
- физическая инфраструктура.

Составляя списки ответственных специалистов, следует учитывать, что некоторые из них могут непосредственно пострадать от аварии (например, от пожара), кто-то может находиться в состоянии стресса, часть сотрудников, возможно, будет лишена возможности попасть на работу (например, в случае массовых беспорядков). Желательно иметь некоторый резерв специалистов или заранее определить каналы, по которым можно на время привлечь дополнительный персонал.

Информационная инфраструктура включает в себя следующие элементы:

- компьютеры;
- программы и данные;
- информационные сервисы внешних организаций;
- документацию.

Нужно подготовиться к тому, что на "запасном аэродроме", куда организация будет эвакуирована после аварии, аппаратная платформа может отличаться от исходной. Соответственно, следует продумать меры поддержания совместимости по программам и данным.

Среди внешних информационных сервисов для коммерческих организаций, вероятно, важнее всего получить оперативную информацию и связь с государственными службами, курирующими данный сектор экономики.

Документация важна хотя бы потому, что не вся информация, с которой работает организация, представлена в электронном виде. Скорее всего, план восстановительных работ напечатан на бумаге.

К физической инфраструктуре относятся здания, инженерные коммуникации, средства связи, оргтехника и многое другое. Компьютерная

техника не может работать в плохих условиях, без стабильного электропитания и т.п.

Анализируя критичные ресурсы, целесообразно учесть временной профиль их использования. Большинство ресурсов требуются постоянно, но в некоторых нужда может возникать только в определенные периоды (например, в конце месяца или года при составлении отчета).

При определении перечня возможных аварий нужно попытаться разработать их сценарии. Как будут развиваться события? Каковы могут оказаться масштабы бедствия? Что произойдет с критичными ресурсами? Например, смогут ли сотрудники попасть на работу? Будут ли выведены из строя компьютеры? Возможны ли случаи саботажа? Будет ли работать связь? Пострадает ли здание организации? Можно ли будет найти и прочитать необходимые бумаги?

Стратегия восстановительных работ должна базироваться на наличных ресурсах и быть не слишком накладной для организации. При разработке стратегии целесообразно провести анализ рисков, которым подвергаются критичные функции, и попытаться выбрать наиболее экономичное решение.

Стратегия должна предусматривать не только работу по временной схеме, но и возвращение к нормальному функционированию.

Подготовка к реализации выбранной стратегии состоит в выработке плана действий в экстренных ситуациях и по их окончании, а также в обеспечении некоторой избыточности критичных ресурсов. Последнее возможно и без большого расхода средств, если заключить с одной или несколькими организациями соглашения о взаимной поддержке в случае аварий – те, кто не пострадал, предоставляют часть своих ресурсов во временное пользование менее удачливым партнерам.

Избыточность обеспечивается также мерами резервного копирования, хранением копий в нескольких местах, представлением информации в разных видах (на бумаге и в файлах) и т.д.

Имеет смысл заключить соглашение с поставщиками информационных услуг о первоочередном обслуживании в критических ситуациях или заключать соглашения с несколькими поставщиками. Правда, эти меры могут потребовать определенных расходов.

Проверка стратегии производится путем анализа подготовленного плана, принятых и намеченных мер.

Вариант 1

1. В число классов мер процедурного уровня входят:

- ☐ логическая защита
- ☐ физическая защита
- ☐ планирование восстановительных работ

2. В число принципов управления персоналом входят:

- ☐ "разделяй и властвуй"
- ☐ разделение обязанностей
- ☐ инкапсуляция наследования

3. В число этапов процесса планирования восстановительных работ входят:

- ☐ выявление критически важных функций организации
- ☐ определение перечня возможных аварий
- ☐ проведение тестовых аварий

Вариант 2

1. В число классов мер процедурного уровня входят:

- ☐ управление персоналом
- ☐ управление персоналками
- ☐ реагирование на нарушения режима безопасности

2. В число принципов управления персоналом входят:

- ☐ минимизация привилегий
- ☐ минимизация зарплаты
- ☐ максимизация зарплаты

3. В число этапов процесса планирования восстановительных работ входят:

- ☐ идентификация персонала
- ☐ проверка персонала
- ☐ идентификация ресурсов

Вариант 3

1 В число классов мер процедурного уровня входят:

- ☐ поддержание работоспособности
- ☐ поддержание физической формы
- ☐ физическая защита

2. В число принципов физической защиты входят:

- ☐ беспощадный отпор
- ☐ непрерывность защиты в пространстве и времени
- ☐ минимизация защитных средств

3. В число этапов процесса планирования восстановительных работ входят:

- ☐ разработка стратегии восстановительных работ
- ☐ сертификация стратегии
- ☐ проверка стратегии

Лекция 9. Основные программно-технические меры

Вводится понятие сервиса безопасности. Рассматриваются вопросы архитектурной безопасности, предлагается классификация сервисов.

Ключевые слова: информационный сервис, основной сервис, вспомогательный сервис, сервис безопасности, идентификация, аутентификация, управление доступом, протоколирование, аудит, шифрование, контроль целостности, экранирование, анализ защищенности, отказоустойчивость, безопасное восстановление, туннелирование, управление, приватность, полный набор защитных средств, превентивные меры, обнаружение нарушений, локализующие меры, прослеживание нарушителя, корпоративная сеть, Internet, сервер, активный агент, апплет, сервлет, доступность, непрерывность защиты, слабое звено, небезопасное состояние, эшелонированность обороны, избыточность, реконфигурирование, единая точка отказа, изоляция, потребительское устройство.

Основные понятия программно-технического уровня информационной безопасности

Программно-технические меры, то есть меры, направленные на контроль компьютерных сущностей – оборудования, программ и/или данных, образуют последний и самый важный рубеж информационной безопасности. Напомним, что ущерб наносят в основном действия легальных пользователей, по отношению к которым процедурные регуляторы малоэффективны. Главные враги – некомпетентность и неаккуратность при выполнении служебных обязанностей, и только программно-технические меры способны им противостоять.

Компьютеры помогли автоматизировать многие области человеческой деятельности. Вполне естественным представляется желание возложить на них и обеспечение собственной безопасности. Даже физическую защиту все чаще поручают не охранникам, а интегрированным компьютерным системам, что позволяет одновременно отслеживать перемещения сотрудников и по организации, и по информационному пространству.

Это вторая причина, объясняющая важность программно-технических мер.

Следует, однако, учитывать, что быстрое развитие информационных технологий не только предоставляет обороняющимся новые возможности, но и объективно затрудняет обеспечение надежной защиты, если опи-

раться исключительно на меры программно-технического уровня. Причин тому несколько:

- повышение быстродействия микросхем, развитие архитектур с высокой степенью параллелизма позволяет методом грубой силы преодолевать барьеры (прежде всего криптографические), ранее казавшиеся неприступными;
- развитие сетей и сетевых технологий, увеличение числа связей между информационными системами, рост пропускной способности каналов расширяют круг злоумышленников, имеющих техническую возможность организовывать атаки;
- появление новых информационных сервисов ведет и к образованию новых уязвимых мест как "внутри" сервисов, так и на их стыках;
- конкуренция среди производителей программного обеспечения заставляет сокращать сроки разработки, что приводит к снижению качества тестирования и выпуску продуктов с дефектами защиты;
- навязываемая потребителям парадигма постоянного наращивания мощности аппаратного и программного обеспечения не позволяет долго оставаться в рамках надежных, апробированных конфигураций и, кроме того, вступает в конфликт с бюджетными ограничениями, из-за чего снижается доля ассигнований на безопасность.

Перечисленные соображения лишний раз подчеркивают важность комплексного подхода к информационной безопасности, а также необходимость гибкой позиции при выборе и сопровождении программно-технических регуляторов.

Центральным для программно-технического уровня является понятие сервиса безопасности.

Следуя объектно-ориентированному подходу, при рассмотрении информационной системы с единичным уровнем детализации мы увидим совокупность предоставляемых ею информационных сервисов. Назовем их основными. Чтобы они могли функционировать и обладали требуемыми свойствами, необходимо несколько уровней дополнительных (вспомогательных) сервисов – от СУБД и мониторов транзакций до ядра операционной системы и оборудования.

К вспомогательным относятся сервисы безопасности (мы уже сталкивались с ними при рассмотрении стандартов и спецификаций в области ИБ); среди них нас в первую очередь будут интересовать универсальные, высокоуровневые, допускающие использование различными основными и вспомогательными сервисами. Далее мы рассмотрим следующие сервисы:

- идентификация и аутентификация;

- управление доступом;
- протоколирование и аудит;
- шифрование;
- контроль целостности;
- экранирование;
- анализ защищенности;
- обеспечение отказоустойчивости;
- обеспечение безопасного восстановления;
- туннелирование;
- управление.

Будут описаны требования к сервисам безопасности, их функциональность, возможные методы реализации и место в общей архитектуре.

Если сопоставить приведенный перечень сервисов с классами функциональных требований "Общих критериев", то бросается в глаза их существенное несовпадение. Мы не будем рассматривать вопросы, связанные с приватностью, по следующей причине. На наш взгляд, сервис безопасности, хотя бы частично, должен находиться в распоряжении того, кого он защищает. В случае же с приватностью это не так: критически важные компоненты сосредоточены не на клиентской, а на серверной стороне, так что приватность по существу оказывается свойством предлагаемой информационной услуги (в простейшем случае приватность достигается путем сохранения конфиденциальности серверной регистрационной информации и защитой от перехвата данных, для чего достаточно перечисленных сервисов безопасности).

С другой стороны, наш перечень шире, чем в "Общих критериях", поскольку в него входят экранирование, анализ защищенности и туннелирование. Эти сервисы имеют важное значение сами по себе и, кроме того, могут комбинироваться с другими сервисами для получения таких необходимых защитных средств, как, например, виртуальные частные сети.

Совокупность перечисленных выше сервисов безопасности мы будем называть полным набором. Считается, что его, в принципе, достаточно для построения надежной защиты на программно-техническом уровне, правда, при соблюдении целого ряда дополнительных условий (отсутствие уязвимых мест, безопасное администрирование и т.д.).

Для проведения классификации сервисов безопасности и определения их места в общей архитектуре меры безопасности можно разделить на следующие виды:

- превентивные, препятствующие нарушениям ИБ;
- меры обнаружения нарушений;
- локализующие, сужающие зону воздействия нарушений;
- меры по выявлению нарушителя;
- меры восстановления режима безопасности.

Большинство сервисов безопасности попадает в число превентивных, и это, безусловно, правильно. Аудит и контроль целостности способны помочь в обнаружении нарушений; активный аудит, кроме того, позволяет запрограммировать реакцию на нарушение с целью локализации и/или прослеживания. Направленность сервисов отказоустойчивости и безопасного восстановления очевидна. Наконец, управление играет инфраструктурную роль, обслуживая все аспекты ИС.

Особенности современных информационных систем, существенные с точки зрения безопасности

Информационная система типичной современной организации является весьма сложным образованием, построенным в многоуровневой архитектуре клиент/сервер, которое пользуется многочисленными внешними сервисами и, в свою очередь, предоставляет собственные сервисы вовне. Даже сравнительно небольшие магазины, обеспечивающие расчет с покупателями по пластиковым картам (и, конечно, имеющие внешний Web-сервер), зависят от своих информационных систем и, в частности, от защищенности всех компонентов систем и коммуникаций между ними.

С точки зрения безопасности наиболее существенными представляются следующие аспекты современных ИС:

- корпоративная сеть имеет несколько территориально разнесенных частей (поскольку организация располагается на нескольких производственных площадках), связи между которыми находятся в ведении внешнего поставщика сетевых услуг, выходя за пределы зоны, контролируемой организацией;
- корпоративная сеть имеет одно или несколько подключений к Internet;
- на каждой из производственных площадок могут находиться критически важные серверы, в доступе к которым нуждаются сотрудники, работающие на других площадках, мобильные пользователи и, возможно, сотрудники других организаций;
- для доступа пользователей могут применяться не только компьютеры, но и потребительские устройства, использующие, в частности, беспроводную связь;
- в течение одного сеанса работы пользователю приходится обращаться к нескольким информационным сервисам, опирающимся на разные аппаратно-программные платформы;
- к доступности информационных сервисов предъявляются жесткие требования, которые обычно выражаются в необходимости круглосуточного функционирования с максимальным временем простоя порядка нескольких минут;

- информационная система представляет собой сеть с активными агентами, то есть в процессе работы программные компоненты, такие как апплеты или сервлеты, передаются с одной машины на другую и выполняются в целевой среде, поддерживая связь с удаленными компонентами;
- не все пользовательские системы контролируются сетевыми и/или системными администраторами организации;
- программное обеспечение, особенно полученное по сети, не может считаться надежным, в нем могут быть ошибки, создающие проблемы в защите;
- конфигурация информационной системы постоянно изменяется на уровнях административных данных, программ и аппаратуры (меняется состав пользователей, их привилегии и версии программ, появляются новые сервисы, новая аппаратура и т.п.).

Следует учитывать еще по крайней мере два момента. Во-первых, для каждого сервиса основные грани ИБ (доступность, целостность, конфиденциальность) трактуются по-своему. Целостность с точки зрения системы управления базами данных и с точки зрения почтового сервера — вещи принципиально разные. Бессмысленно говорить о безопасности локальной или иной сети вообще, если сеть включает в себя разнородные компоненты. Следует анализировать защищенность сервисов, функционирующих в сети. Для разных сервисов и защиту строят по-разному. Во-вторых, основная угроза информационной безопасности организаций по-прежнему исходит не от внешних злоумышленников, а от собственных сотрудников.

В силу изложенных причин далее будут рассматриваться распределенные, разнородные, многосервисные, эволюционирующие системы. Соответственно, нас будут интересовать решения, ориентированные на подобные конфигурации.

Архитектурная безопасность

Сервисы безопасности, какими бы мощными они ни были, сами по себе не могут гарантировать надежность программно-технического уровня защиты. Только проверенная архитектура способна сделать эффективным объединение сервисов, обеспечить управляемость информационной системы, ее способность развиваться и противостоять новым угрозам при сохранении таких свойств, как высокая производительность, простота и удобство использования.

Теоретической основой решения проблемы архитектурной безопасности является следующее фундаментальное утверждение, которое мы уже приводили, рассматривая интерпретацию "Оранжевой книги" для сетевых конфигураций.

"Пусть каждый субъект (то есть процесс, действующий от имени какого-либо пользователя) заключен внутри одного компонента и может осуществлять непосредственный доступ к объектам только в пределах этого компонента. Далее пусть каждый компонент содержит свой монитор обращений, отслеживающий все локальные попытки доступа, и все мониторы проводят в жизнь согласованную политику безопасности. Пусть, наконец, коммуникационные каналы, связывающие компоненты, сохраняют конфиденциальность и целостность передаваемой информации. Тогда совокупность всех мониторов образует единый монитор обращений для всей сетевой конфигурации."

Обратим внимание на три принципа, содержащиеся в приведенном утверждении:

- необходимость выработки и проведения в жизнь единой политики безопасности;
- необходимость обеспечения конфиденциальности и целостности при сетевых взаимодействиях;
- необходимость формирования составных сервисов по содержательному принципу, чтобы каждый полученный таким образом компонент обладал полным набором защитных средств и с внешней точки зрения представлял собой единое целое (не должно быть информационных потоков, идущих к незащищенным сервисам).

Если какой-либо (составной) сервис не обладает полным набором защитных средств (состав полного набора описан выше), необходимо привлечение дополнительных сервисов, которые мы будем называть экранирующими. Экранирующие сервисы устанавливаются на путях доступа к недостаточно защищенным элементам; в принципе, один такой сервис может экранировать (защищать) сколь угодно большое число элементов.

С практической точки зрения наиболее важными являются следующие принципы архитектурной безопасности:

- непрерывность защиты в пространстве и времени, невозможность миновать защитные средства;
- следование признанным стандартам, использование апробированных решений;
- иерархическая организация ИС с небольшим числом сущностей на каждом уровне;
- усиление самого слабого звена;
- невозможность перехода в небезопасное состояние;
- минимизация привилегий;
- разделение обязанностей;
- эшелонированность обороны;
- разнообразие защитных средств;
- простота и управляемость информационной системы.

Поясним смысл перечисленных принципов.

Если у злоумышленника или недовольного пользователя появится возможность миновать защитные средства, он, разумеется, так и сделает. Определенные выше экранирующие сервисы должны исключить подобную возможность.

Следование признанным стандартам и использование апробированных решений повышает надежность ИС и уменьшает вероятность попадания в тупиковую ситуацию, когда обеспечение безопасности потребует непомерно больших затрат и принципиальных модификаций.

Иерархическая организация ИС с небольшим числом сущностей на каждом уровне необходима по технологическим соображениям. При нарушении данного принципа система станет неуправляемой и, следовательно, обеспечить ее безопасность будет невозможно.

Надежность любой обороны определяется самым слабым звеном. Злоумышленник не будет бороться против силы, он предпочтет легкую победу над слабостью. (Часто самым слабым звеном оказывается не компьютер или программа, а человек, и тогда проблема обеспечения информационной безопасности приобретает нетехнический характер.)

Принцип невозможности перехода в небезопасное состояние означает, что при любых обстоятельствах, в том числе нештатных, защитное средство либо полностью выполняет свои функции, либо полностью блокирует доступ. Образно говоря, если в крепости механизм подъемного моста ломается, мост оставляют поднятым, препятствуя проходу неприятеля.

Применительно к программно-техническому уровню принцип минимизации привилегий предписывает выделять пользователям и администраторам только те права доступа, которые необходимы им для выполнения служебных обязанностей. Этот принцип позволяет уменьшить ущерб от случайных или умышленных некорректных действий пользователей и администраторов.

Принцип разделения обязанностей предполагает такое распределение ролей и ответственности, чтобы один человек не мог нарушить критически важный для организации процесс или создать брешь в защите по заказу злоумышленников. В частности, соблюдение данного принципа особенно важно, чтобы предотвратить злонамеренные или неквалифицированные действия системного администратора.

Принцип эшелонированности обороны предписывает не полагаться на один защитный рубеж, каким бы надежным он ни казался. За средствами физической защиты должны следовать программно-технические средства, за идентификацией и аутентификацией – управление доступом и, как последний рубеж, – протоколирование и аудит. Эшелонированная оборона способна, по крайней мере, задержать злоумышленника, а благо-

даря наличию такого рубежа, как протоколирование и аудит, его действия не останутся незамеченными.

Принцип разнообразия защитных средств предполагает создание различных по своему характеру оборонительных рубежей, чтобы от потенциального злоумышленника требовалось овладение разнообразными и, по возможности, несовместимыми между собой навыками.

Очень важен принцип простоты и управляемости информационной системы в целом и защитных средств в особенности. Только для простого защитного средства можно формально или неформально доказать его корректность. Только в простой и управляемой системе можно проверить согласованность конфигурации различных компонентов и осуществлять централизованное администрирование. В этой связи важно отметить интегрирующую роль Web-сервиса, скрывающего разнообразие обслуживаемых объектов и предоставляющего единый, наглядный интерфейс. Соответственно, если объекты некоторого вида (например, таблицы базы данных) доступны через Web, необходимо заблокировать прямой доступ к ним, поскольку в противном случае система будет сложной и плохо управляемой.

Для обеспечения высокой доступности (непрерывности функционирования) необходимо соблюдать следующие принципы архитектурной безопасности:

- внесение в конфигурацию той или иной формы избыточности (резервное оборудование, запасные каналы связи и т.п.);
- наличие средств обнаружения нештатных ситуаций;
- наличие средств реконфигурирования для восстановления, изоляции и/или замены компонентов, отказавших или подвергшихся атаке на доступность;
- рассредоточенность сетевого управления, отсутствие единой точки отказа;
- выделение подсетей и изоляция групп пользователей друг от друга. Данная мера, являющаяся обобщением разделения процессов на уровне операционной системы, ограничивает зону поражения при возможных нарушениях информационной безопасности.

Еще один важный архитектурный принцип – минимизация объема защитных средств, выносимых на клиентские системы. Причин тому несколько:

- для доступа в корпоративную сеть могут использоваться потребительские устройства с ограниченной функциональностью;
- конфигурацию клиентских систем трудно или невозможно контролировать.

К необходимому минимуму следует отнести реализацию сервисов безопасности на сетевом и транспортном уровнях и поддержку механизмов аутентификации, устойчивых к сетевым угрозам.

Вариант 1

1. Протоколирование и аудит могут использоваться для:

- ☐ предупреждения нарушений ИБ
- ☐ обнаружения нарушений
- ☐ восстановления режима ИБ

2. Укажите наиболее существенные с точки зрения безопасности особенности современных российских ИС:

- ☐ доминирование платформы Wintel
- ☐ наличие подключения к Internet
- ☐ наличие разнородных сервисов

3. В число основных принципов архитектурной безопасности входят:

- ☐ применение наиболее передовых технических решений
- ☐ применение простых апробированных решений
- ☐ сочетание простых и сложных защитных средств

Вариант 2

1. Экранирование может использоваться для:

- ☐ предупреждения нарушений ИБ
- ☐ обнаружения нарушений
- ☐ локализации последствий нарушений

2. Укажите наиболее существенные с точки зрения безопасности особенности современных российских ИС:

- ☐ низкая пропускная способность большинства коммуникационных каналов
- ☐ сложность администрирования пользовательских компьютеров
- ☐ отсутствие достаточного набора криптографических аппаратно-программных продуктов

3. В число основных принципов архитектурной безопасности входят:

- ☐ следование признанным стандартам
- ☐ применение нестандартных решений, не известных злоумышленникам
- ☐ разнообразие защитных средств

Вариант 3

1. Контроль целостности может использоваться для:

- ☐ предупреждения нарушений ИБ
- ☐ обнаружения нарушений
- ☐ локализации последствий нарушений

2. Укажите наиболее существенные с точки зрения безопасности особенности современных российских ИС:

- ☐ использование ПО с активными агентами
- ☐ использование пиратского ПО
- ☐ использование свободно распространяемого ПО

3. В число основных принципов архитектурной безопасности входят:

- ☐ усиление самого слабого звена
- ☐ укрепление наиболее вероятного объекта атаки
- ☐ эшелонированность обороны

Лекция 10. Идентификация и аутентификация, управление доступом

В данной лекции кратко описываются традиционные сервисы безопасности – идентификация и аутентификация, управление доступом. Сервисы безопасности мы будем рассматривать применительно к распределенным, разнородным системам, содержащим большое число компонентов.

Ключевые слова: идентификация, аутентификация, аутентификатор, односторонняя аутентификация, двусторонняя аутентификация, взаимная аутентификация, перехват, изменение, воспроизведение, единый вход в сеть, парольная аутентификация, управление сроком действия паролей, наложение технических ограничений, генератор паролей, многоразовый пароль, одноразовый пароль, односторонняя функция, S/KEY, сервер аутентификации, Kerberos, доверенная третья сторона, билет, секретный ключ, биометрия, биометрический шаблон, отпечатки пальцев, роговица, сетчатка, геометрия руки, геометрия лица, голос, речь, динамика подписи, динамика работы с клавиатурой, субъект, объект, права доступа, матрица доступа, списки управления доступом, произвольное управление доступом, дискреционное управление доступом, принудительное управление доступом, мандатное управление доступом, ограничивающий интерфейс, ролевое управление доступом, пользователь, сеанс работы пользователя, роль, операция, приписывание пользователя роли, приписывание права доступа роли, наследование ролей, иерархия ролей, разделение обязанностей, статическое разделение обязанностей, динамическое разделение обязанностей, минимизация привилегий, временное ограничение доверия, административные функции, вспомогательные функции, информационные функции, Java, апплет, песочница, источник программы, множество прав, контекст выполнения, привилегированный интервал программы, объектная среда, метод, контейнер, политика безопасности, интерфейс, дескриптор интерфейса, трансляция интерфейсов, правила разграничения доступа (ПРД), монитор обращений, предикат, фактический параметр, формальный параметр, входной параметр, выходной параметр, добровольно налагаемые ограничения.

Идентификация и аутентификация

Основные понятия

Идентификацию и аутентификацию можно считать основой программно-технических средств безопасности, поскольку остальные сервисы рассчитаны на обслуживание именованных субъектов. Идентификация и аутентификация – это первая линия обороны, "проходная" информационного пространства организации.

Идентификация позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя). Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает. В качестве синонима слова "аутентификация" иногда используют словосочетание "проверка подлинности".

(Заметим в скобках, что происхождение русскоязычного термина "аутентификация" не совсем понятно. Английское "authentication" скорее можно прочитать как "аутентикация"; трудно сказать, откуда в середине взялось еще "фи" – может, из идентификации? Тем не менее, термин устоялся, он закреплен в Руководящих документах Гостехкомиссии России, использован в многочисленных публикациях, поэтому исправить его уже невозможно.)

Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной). Пример односторонней аутентификации – процедура входа пользователя в систему.

В сетевой среде, когда стороны идентификации/аутентификации территориально разнесены, у рассматриваемого сервиса есть два основных аспекта:

- что служит аутентификатором (то есть используется для подтверждения подлинности субъекта);
- как организован (и защищен) обмен данными идентификации/аутентификации.

Субъект может подтвердить свою подлинность, предъявив по крайней мере одну из следующих сущностей:

- нечто, что он знает (пароль, личный идентификационный номер, криптографический ключ и т.п.);
- нечто, чем он владеет (личную карточку или иное устройство аналогичного назначения);
- нечто, что есть часть его самого (голос, отпечатки пальцев и т.п., то есть свои биометрические характеристики).

В открытой сетевой среде между сторонами идентификации/аутентификации не существует доверенного маршрута; это значит, что в общем случае данные, переданные субъектом, могут не совпадать с данными, полученными и использованными для проверки подлинности. Необходимо

обеспечить защиту от пассивного и активного прослушивания сети, то есть от перехвата, изменения и/или воспроизведения данных. Передача паролей в открытом виде, очевидно, неудовлетворительна; не спасает положение и шифрование паролей, так как оно не защищает от воспроизведения. Нужны более сложные протоколы аутентификации.

Надежная идентификация и аутентификация затруднена не только из-за сетевых угроз, но и по целому ряду причин. Во-первых, почти все аутентификационные сущности можно узнать, украсть или подделать. Во-вторых, имеется противоречие между надежностью аутентификации, с одной стороны, и удобствами пользователя и системного администратора с другой. Так, из соображений безопасности необходимо с определенной частотой просить пользователя повторно вводить аутентификационную информацию (ведь на его место мог сесть другой человек), а это не только хлопотно, но и повышает вероятность того, что кто-то может подсмотреть за вводом данных. В-третьих, чем надежнее средство защиты, тем оно дороже.

Современные средства идентификации/аутентификации должны поддерживать концепцию единого входа в сеть. Единый вход в сеть – это, в первую очередь, требование удобства для пользователей. Если в корпоративной сети много информационных сервисов, допускающих независимое обращение, то многократная идентификация/аутентификация становится слишком обременительной. К сожалению, пока нельзя сказать, что единый вход в сеть стал нормой, доминирующие решения пока не сформировались.

Таким образом, необходимо искать компромисс между надежностью, доступностью по цене и удобством использования и администрирования средств идентификации и аутентификации.

Любопытно отметить, что сервис идентификации/аутентификации может стать объектом атак на доступность. Если система сконфигурирована так, что после определенного числа неудачных попыток устройство ввода идентификационной информации (такое, например, как терминал) блокируется, то злоумышленник может остановить работу легального пользователя буквально несколькими нажатиями клавиш.

Парольная аутентификация

Главное достоинство парольной аутентификации – простота и привычность. Пароли давно встроены в операционные системы и иные сервисы. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее, по совокупности характеристик их следует признать самым слабым средством проверки подлинности.

Чтобы пароль был запоминающимся, его зачастую делают простым (имя подруги, название спортивной команды и т.п.). Однако простой па-

роль нетрудно угадать, особенно если знать пристрастия данного пользователя. Известна классическая история про советского разведчика Рихарда Зорге, объект внимания которого через слово говорил "карамба"; разумеется, этим же словом открывался сверхсекретный сейф.

Иногда пароли с самого начала не хранятся в тайне, так как имеют стандартные значения, указанные в документации, и далеко не всегда после установки системы производится их смена.

Ввод пароля можно подсмотреть. Иногда для подглядывания используются даже оптические приборы.

Пароли нередко сообщают коллегам, чтобы те могли, например, подменить на некоторое время владельца пароля. Теоретически в подобных случаях более правильно задействовать средства управления доступом, но на практике так никто не поступает; а тайна, которую знают двое, это уже не тайна.

Пароль можно угадать "методом грубой силы", используя, скажем, словарь. Если файл паролей зашифрован, но доступен для чтения, его можно скачать к себе на компьютер и попытаться подобрать пароль, запрограммировав полный перебор (предполагается, что алгоритм шифрования известен).

Тем не менее, следующие меры позволяют значительно повысить надежность парольной защиты:

- наложение технических ограничений (пароль должен быть не слишком коротким, он должен содержать буквы, цифры, знаки пунктуации и т.п.);
- управление сроком действия паролей, их периодическая смена;
- ограничение доступа к файлу паролей;
- ограничение числа неудачных попыток входа в систему (это затруднит применение "метода грубой силы");
- обучение пользователей;
- использование программных генераторов паролей (такая программа, основываясь на несложных правилах, может порождать только благозвучные и, следовательно, запоминающиеся пароли).

Перечисленные меры целесообразно применять всегда, даже если наряду с паролями используются другие методы аутентификации.

Одноразовые пароли

Рассмотренные выше пароли можно назвать многоразовыми; их раскрытие позволяет злоумышленнику действовать от имени легального пользователя. Гораздо более сильным средством, устойчивым к пассивному прослушиванию сети, являются одноразовые пароли.

Наиболее известным программным генератором одноразовых паролей является система S/KEY компании Bellcore. Идея этой системы сос-

тоит в следующем. Пусть имеется односторонняя функция f (то есть функция, вычислить обратную которой за приемлемое время не представляется возможным). Эта функция известна и пользователю, и серверу аутентификации. Пусть, далее, имеется секретный ключ K, известный только пользователю.

На этапе начального администрирования пользователя функция f применяется к ключу K n раз, после чего результат сохраняется на сервере. После этого процедура проверки подлинности пользователя выглядит следующим образом:

- сервер присылает на пользовательскую систему число (n-1);
- пользователь применяет функцию f к секретному ключу K (n-1) раз и отправляет результат по сети на сервер аутентификации;
- сервер применяет функцию f к полученному от пользователя значению и сравнивает результат с ранее сохраненной величиной. В случае совпадения подлинность пользователя считается установленной, сервер запоминает новое значение (присланное пользователем) и уменьшает на единицу счетчик (n).

На самом деле реализация устроена чуть сложнее (кроме счетчика, сервер посылает затравочное значение, используемое функцией f), но для нас сейчас это не важно. Поскольку функция f необратима, перехват пароля, равно как и получение доступа к серверу аутентификации, не позволяют узнать секретный ключ K и предсказать следующий одноразовый пароль.

Система S/KEY имеет статус Internet-стандарта (RFC 1938).

Другой подход к надежной аутентификации состоит в генерации нового пароля через небольшой промежуток времени (например, каждые 60 секунд), для чего могут использоваться программы или специальные интеллектуальные карты (с практической точки зрения такие пароли можно считать одноразовыми). Серверу аутентификации должен быть известен алгоритм генерации паролей и ассоциированные с ним параметры; кроме того, часы клиента и сервера должны быть синхронизированы.

Сервер аутентификации Kerberos

Kerberos – это программный продукт, разработанный в середине 1980-х годов в Массачусетском технологическом институте и претерпевший с тех пор ряд принципиальных изменений. Клиентские компоненты Kerberos присутствуют в большинстве современных операционных систем.

Kerberos предназначен для решения следующей задачи. Имеется открытая (незащищенная) сеть, в узлах которой сосредоточены субъекты – пользователи, а также клиентские и серверные программные системы. Каждый субъект обладает секретным ключом. Чтобы субъект C мог доказать свою подлинность субъекту S (без этого S не станет обслуживать C), он должен не только назвать себя, но и продемонстрировать знание секретного ключа. C не мо-

жет просто послать S свой секретный ключ, во-первых, потому, что сеть открыта (доступна для пассивного и активного прослушивания), а, во-вторых, потому, что S не знает (и не должен знать) секретный ключ C. Требуется менее прямолинейный способ демонстрации знания секретного ключа.

Система Kerberos представляет собой доверенную третью сторону (то есть сторону, которой доверяют все), владеющую секретными ключами обслуживаемых субъектов и помогающую им в попарной проверке подлинности.

Чтобы с помощью Kerberos получить доступ к S (обычно это сервер), C (как правило – клиент) посылает Kerberos запрос, содержащий сведения о нем (клиенте) и о запрашиваемой услуге. В ответ Kerberos возвращает так называемый билет, зашифрованный секретным ключом сервера, и копию части информации из билета, зашифрованную секретным ключом клиента. Клиент должен расшифровать вторую порцию данных и переслать ее вместе с билетом серверу. Сервер, расшифровав билет, может сравнить его содержимое с дополнительной информацией, присланной клиентом. Совпадение свидетельствует о том, что клиент смог расшифровать предназначенные ему данные (ведь содержимое билета никому, кроме сервера и Kerberos, недоступно), то есть продемонстрировал знание секретного ключа. Значит, клиент – именно тот, за кого себя выдает. Подчеркнем, что секретные ключи в процессе проверки подлинности не передавались по сети (даже в зашифрованном виде) – они только использовались для шифрования. Как организован первоначальный обмен ключами между Kerberos и субъектами и как субъекты хранят свои секретные ключи – вопрос отдельный.

Проиллюстрируем описанную процедуру.

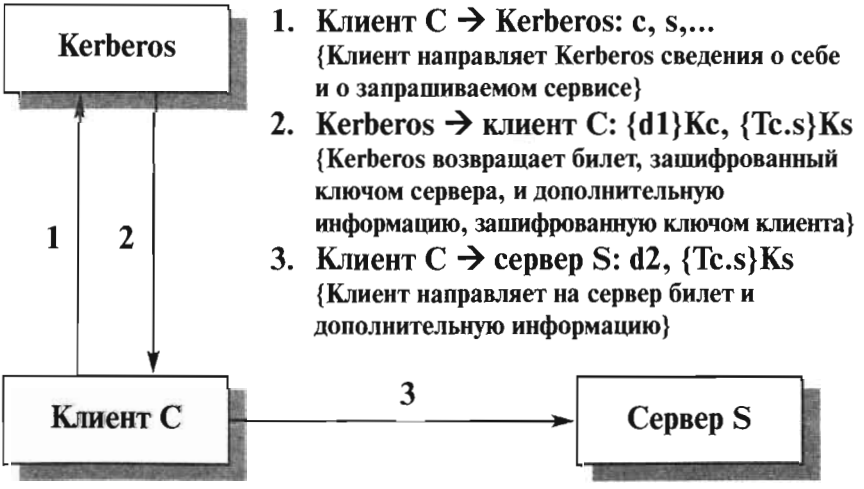

Рис. 10.1. Проверка сервером S подлинности клиента C.

Здесь c и s – сведения (например, имя), соответственно, о клиенте и сервере, d1 и d2 – дополнительная (по отношению к билету) информация, Tc.s – билет для клиента C на обслуживание у сервера S, Kc и Ks – секретные ключи клиента и сервера, {info}K – информация info, зашифрованная ключом K.

Приведенная схема – крайне упрощенная версия реальной процедуры проверки подлинности. Более подробное рассмотрение системы Kerberos можно найти, например, в статье В. Галатенко "Сервер аутентификации Kerberos (Jet Info, 1996, 12-13). Нам же важно отметить, что Kerberos не только устойчив к сетевым угрозам, но и поддерживает концепцию единого входа в сеть.

Идентификация/аутентификация с помощью биометрических данных

Биометрия представляет собой совокупность автоматизированных методов идентификации и/или аутентификации людей на основе их физиологических и поведенческих характеристик. К числу физиологических характеристик принадлежат особенности отпечатков пальцев, сетчатки и роговицы глаз, геометрия руки и лица и т.п. К поведенческим характеристикам относятся динамика подписи (ручной), стиль работы с клавиатурой. На стыке физиологии и поведения находятся анализ особенностей голоса и распознавание речи.

Биометрией во всем мире занимаются очень давно, однако долгое время все, что было связано с ней, отличалось сложностью и дороговизной. В последнее время спрос на биометрические продукты, в первую очередь в связи с развитием электронной коммерции, постоянно и весьма интенсивно растет. Это понятно, поскольку с точки зрения пользователя гораздо удобнее предъявить себя самого, чем что-то запоминать. Спрос рождает предложение, и на рынке появились относительно недорогие аппаратно-программные продукты, ориентированные в основном на распознавание отпечатков пальцев.

В общем виде работа с биометрическими данными организована следующим образом. Сначала создается и поддерживается база данных характеристик потенциальных пользователей. Для этого биометрические характеристики пользователя снимаются, обрабатываются, и результат обработки (называемый биометрическим шаблоном) заносится в базу данных (исходные данные, такие как результат сканирования пальца или роговицы, обычно не хранятся).

В дальнейшем для идентификации (и одновременно аутентификации) пользователя процесс снятия и обработки повторяется, после чего производится поиск в базе данных шаблонов. В случае успешного поиска личность пользователя и ее подлинность считаются установленными.

Для аутентификации достаточно произвести сравнение с одним биометрическим шаблоном, выбранным на основе предварительно введенных данных.

Обычно биометрию применяют вместе с другими аутентификаторами, такими, например, как интеллектуальные карты. Иногда биометрическая аутентификация является лишь первым рубежом защиты и служит для активизации интеллектуальных карт, хранящих криптографические секреты; в таком случае биометрический шаблон хранится на той же карте.

Активность в области биометрии очень велика. Организован соответствующий консорциум (см. http://www.biometrics.org), активно ведутся работы по стандартизации разных аспектов технологии (формата обмена данными, прикладного программного интерфейса и т.п.), публикуется масса рекламных статей, в которых биометрия преподносится как средство обеспечения сверхбезопасности, ставшее доступным широким массам.

На наш взгляд, к биометрии следует относиться весьма осторожно. Необходимо учитывать, что она подвержена тем же угрозам, что и другие методы аутентификации. Во-первых, биометрический шаблон сравнивается не с результатом первоначальной обработки характеристик пользователя, а с тем, что пришло к месту сравнения. А, как известно, за время пути... много чего может произойти. Во-вторых, биометрические методы не более надежны, чем база данных шаблонов. В-третьих, следует учитывать разницу между применением биометрии на контролируемой территории, под бдительным оком охраны, и в "полевых" условиях, когда, например к устройству сканирования роговицы могут поднести муляж и т.п. В-четвертых, биометрические данные человека меняются, так что база шаблонов нуждается в сопровождении, что создает определенные проблемы и для пользователей, и для администраторов.

Но главная опасность состоит в том, что любая "пробоина" для биометрии оказывается фатальной. Пароли, при всей их ненадежности, в крайнем случае можно сменить. Утерянную аутентификационную карту можно аннулировать и завести новую. Палец же, глаз или голос сменить нельзя. Если биометрические данные окажутся скомпрометированы, придется как минимум производить существенную модернизацию всей системы.

Управление доступом

Основные понятия

С традиционной точки зрения средства управления доступом позволяют специфицировать и контролировать действия, которые субъекты (пользователи и процессы) могут выполнять над объектами (информаци-

ей и другими компьютерными ресурсами). В данном разделе речь идет о логическом управлении доступом, которое, в отличие от физического, реализуется программными средствами. Логическое управление доступом – это основной механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность объектов и, до некоторой степени, их доступность (путем запрещения обслуживания неавторизованных пользователей).

Рассмотрим формальную постановку задачи в традиционной трактовке. Имеется совокупность субъектов и набор объектов. Задача логического управления доступом состоит в том, чтобы для каждой пары "субъект-объект" определить множество допустимых операций (зависящее, быть может, от некоторых дополнительных условий) и контролировать выполнение установленного порядка.

Отношение "субъекты-объекты" можно представить в виде матрицы доступа, в строках которой перечислены субъекты, в столбцах – объекты, а в клетках, расположенных на пересечении строк и столбцов, записаны дополнительные условия (например, время и место действия) и разрешенные виды доступа. Фрагмент матрицы может выглядеть, например, так:

	Файл	**Программа**	**Линия_связи**	**Реляционная_таблица**
Пользователь_1	**orw с системной консоли**	**e**	**rw с 8:00 до 18:00**	
Пользователь_2				**a**
"o" – обозначает разрешение на передачу прав доступа другим пользователям, "r" – чтение, "w" – запись, "e" – выполнение, "a" – добавление информации				

Табл. 10.1. Фрагмент матрицы доступа.

Тема логического управления доступом – одна из сложнейших в области информационной безопасности. Дело в том, что само понятие объекта (а тем более видов доступа) меняется от сервиса к сервису. Для операционной системы к объектам относятся файлы, устройства и процессы. Применительно к файлам и устройствам обычно рассматриваются права на чтение, запись, выполнение (для программных файлов), иногда на

удаление и добавление. Отдельным правом может быть возможность передачи полномочий доступа другим субъектам (так называемое право владения). Процессы можно создавать и уничтожать. Современные операционные системы могут поддерживать и другие объекты.

Для систем управления реляционными базами данных объект – это база данных, таблица, представление, хранимая процедура. К таблицам применимы операции поиска, добавления, модификации и удаления данных, у других объектов иные виды доступа.

Разнообразие объектов и применимых к ним операций приводит к принципиальной децентрализации логического управления доступом. Каждый сервис должен сам решать, позволить ли конкретному субъекту ту или иную операцию. Теоретически это согласуется с современным объектно-ориентированным подходом, на практике же приводит к значительным трудностям. Главная проблема в том, что ко многим объектам можно получить доступ с помощью разных сервисов (возможно, при этом придется преодолеть некоторые технические трудности). Так, до реляционных таблиц можно добраться не только средствами СУБД, но и путем непосредственного чтения файлов или дисковых разделов, поддерживаемых операционной системой (разобравшись предварительно в структуре хранения объектов базы данных). В результате при задании матрицы доступа нужно принимать во внимание не только принцип распределения привилегий для каждого сервиса, но и существующие связи между сервисами (приходится заботиться о согласованности разных частей матрицы). Аналогичная трудность возникает при экспорте/импорте данных, когда информация о правах доступа, как правило, теряется (поскольку на новом сервисе она не имеет смысла). Следовательно, обмен данными между различными сервисами представляет особую опасность с точки зрения управления доступом, а при проектировании и реализации разнородной конфигурации необходимо позаботиться о согласованном распределении прав доступа субъектов к объектам и о минимизации числа способов экспорта/импорта данных.

Контроль прав доступа производится разными компонентами программной среды – ядром операционной системы, сервисами безопасности, системой управления базами данных, программным обеспечением промежуточного слоя (таким, как монитор транзакций) и т.д. Тем не менее, можно выделить общие критерии, на основании которых решается вопрос о предоставлении доступа, и общие методы хранения матрицы доступа.

При принятии решения о предоставлении доступа обычно анализируется следующая информация:

- идентификатор субъекта (идентификатор пользователя, сетевой адрес компьютера и т.п.). Подобные идентификаторы являются основой произвольного (или дискреционного) управления доступом;

- атрибуты субъекта (метка безопасности, группа пользователя и т.п.). Метки безопасности – основа принудительного (мандатного) управления доступом.

Матрицу доступа, ввиду ее разреженности (большинство клеток – пустые), неразумно хранить в виде двухмерного массива. Обычно ее хранят по столбцам, то есть для каждого объекта поддерживается список "допущенных" субъектов вместе с их правами. Элементами списков могут быть имена групп и шаблоны субъектов, что служит большим подспорьем администратору. Некоторые проблемы возникают только при удалении субъекта, когда приходится удалять его имя из всех списков доступа; впрочем, эта операция производится нечасто.

Списки доступа – исключительно гибкое средство. С их помощью легко выполнить требование о гранулярности прав с точностью до пользователя. Посредством списков несложно добавить права или явным образом запретить доступ (например, чтобы наказать нескольких членов группы пользователей). Безусловно, списки являются лучшим средством произвольного управления доступом.

Подавляющее большинство операционных систем и систем управления базами данных реализуют именно произвольное управление доступом. Основное достоинство произвольного управления – гибкость. Вообще говоря, для каждой пары "субъект-объект" можно независимо задавать права доступа (особенно легко это делать, если используются списки управления доступом). К сожалению, у "произвольного" подхода есть ряд недостатков. Рассредоточенность управления доступом ведет к тому, что доверенными должны быть многие пользователи, а не только системные операторы или администраторы. Из-за рассеянности или некомпетентности сотрудника, владеющего секретной информацией, эту информацию могут узнать и все остальные пользователи. Следовательно, произвольность управления должна быть дополнена жестким контролем за реализацией избранной политики безопасности.

Второй недостаток, который представляется основным, состоит в том, что права доступа существуют отдельно от данных. Ничто не мешает пользователю, имеющему доступ к секретной информации, записать ее в доступный всем файл или заменить полезную утилиту ее "троянским" аналогом. Подобная "разделенность" прав и данных существенно осложняет проведение несколькими системами согласованной политики безопасности и, главное, делает практически невозможным эффективный контроль согласованности.

Возвращаясь к вопросу представления матрицы доступа, укажем, что для этого можно использовать также функциональный способ, когда матрицу не хранят в явном виде, а каждый раз вычисляют содержимое со-

ответствующих клеток. Например, при принудительном управлении доступом применяется сравнение меток безопасности субъекта и объекта.

Удобной надстройкой над средствами логического управления доступом является ограничивающий интерфейс, когда пользователя лишают самой возможности попытаться совершить несанкционированные действия, включив в число видимых ему объектов только те, к которым он имеет доступ. Подобный подход обычно реализуют в рамках системы меню (пользователю показывают лишь допустимые варианты выбора) или посредством ограничивающих оболочек, таких как restricted shell в ОС Unix.

В заключение подчеркнем важность управления доступом не только на уровне операционной системы, но и в рамках других сервисов, входящих в состав современных приложений, а также, насколько это возможно, на "стыках" между сервисами. Здесь на первый план выходит существование единой политики безопасности организации, а также квалифицированное и согласованное системное администрирование.

Ролевое управление доступом

При большом количестве пользователей традиционные подсистемы управления доступом становятся крайне сложными для администрирования. Число связей в них пропорционально произведению количества пользователей на количество объектов. Необходимы решения в объектно-ориентированном стиле, способные эту сложность понизить.

Таким решением является ролевое управление доступом (РУД). Суть его в том, что между пользователями и их привилегиями появляются промежуточные сущности – роли. Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему определенные права (см. рис. 10.2).

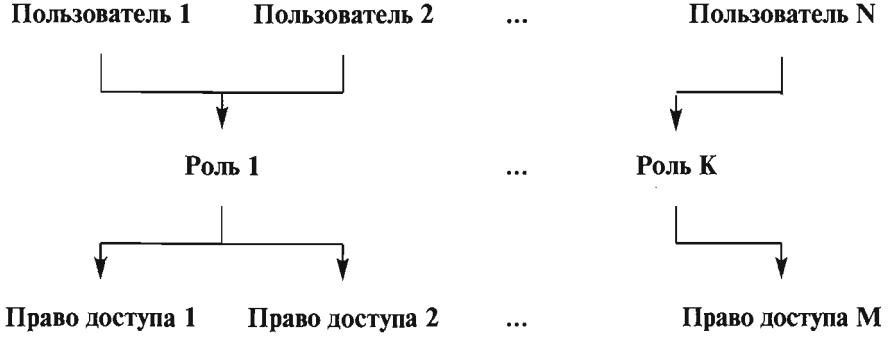

Рис. 10.2. Пользователи, объекты и роли.

Ролевой доступ нейтрален по отношению к конкретным видам прав и способам их проверки; его можно рассматривать как объектно-ориентированный каркас, облегчающий администрирование, поскольку он позволяет сделать подсистему разграничения доступа управляемой при сколь угодно большом числе пользователей, прежде всего за счет установления между ролями связей, аналогичных наследованию в объектно-ориентированных системах. Кроме того, ролей должно быть значительно меньше, чем пользователей. В результате число администрируемых связей становится пропорциональным сумме (а не произведению) количества пользователей и объектов, что по порядку величины уменьшить уже невозможно.

Ролевой доступ развивается более 10 лет (сама идея ролей, разумеется, значительно старше) как на уровне операционных систем, так и в рамках СУБД и других информационных сервисов. В частности, существуют реализации ролевого доступа для Web-серверов.

В 2001 году Национальный институт стандартов и технологий США предложил проект стандарта ролевого управления доступом (см. http://csrc.nist.gov/rbac/), основные положения которого мы и рассмотрим.

Ролевое управление доступом оперирует следующими основными понятиями:

- пользователь (человек, интеллектуальный автономный агент и т.п.);
- сеанс работы пользователя;
- роль (обычно определяется в соответствии с организационной структурой);
- объект (сущность, доступ к которой разграничивается; например, файл ОС или таблица СУБД);
- операция (зависит от объекта; для файлов ОС – чтение, запись, выполнение и т.п.; для таблиц СУБД – вставка, удаление и т.п., для прикладных объектов операции могут быть более сложными);
- право доступа (разрешение выполнять определенные операции над определенными объектами).

Ролям приписываются пользователи и права доступа; можно считать, что они (роли) именуют отношения "многие ко многим" между пользователями и правами. Роли могут быть приписаны многие пользователи; один пользователь может быть приписан нескольким ролям. Во время сеанса работы пользователя активизируется подмножество ролей, которым он приписан, в результате чего он становится обладателем объединения прав, приписанных активным ролям. Одновременно пользователь может открыть несколько сеансов.

Между ролями может быть определено отношение частичного порядка, называемое наследованием. Если роль r2 является наследницей r1, то все права r1 приписываются r2, а все пользователи r2 приписываются r1. Очевид-

но, что наследование ролей соответствует наследованию классов в объектно-ориентированном программировании, только правам доступа соответствуют методы классов, а пользователям – объекты (экземпляры) классов.

Отношение наследования является иерархическим, причем права доступа и пользователи распространяются по уровням иерархии навстречу друг другу. В общем случае наследование является множественным, то есть у одной роли может быть несколько предшественниц (и, естественно, несколько наследниц, которых мы будем называть также преемницами).

Можно представить себе формирование иерархии ролей, начиная с минимума прав (и максимума пользователей), приписываемых роли "сотрудник", с постепенным уточнением состава пользователей и добавлением прав (роли "системный администратор", "бухгалтер" и т.п.), вплоть до роли "руководитель" (что, впрочем, не значит, что руководителю предоставляются неограниченные права; как и другим ролям, в соответствии с принципом минимизации привилегий, этой роли целесообразно разрешить только то, что необходимо для выполнения служебных обязанностей). Фрагмент подобной иерархии ролей показан на рис. 10.3.

Рис. 10.3. Фрагмент иерархии ролей.

Для реализации еще одного упоминавшегося ранее важного принципа информационной безопасности вводится понятие разделения обязанностей, причем в двух видах: статическом и динамическом.

Статическое разделение обязанностей налагает ограничения на приписывание пользователей ролям. В простейшем случае членство в некоторой роли запрещает приписывание пользователя определенному множеству других ролей. В общем случае данное ограничение задается как пара "множество ролей – число" (где множество состоит, по крайней мере, из двух ролей, а число должно быть больше 1), так что никакой пользователь не может быть приписан указанному (или большему) числу ролей из заданного множества. Например, может существовать пять бухгалтерских ролей, но политика безопасности допускает членство не более чем в двух таких ролях (здесь число=3).

При наличии наследования ролей ограничение приобретает несколько более сложный вид, но суть остается простой: при проверке членства в ролях нужно учитывать приписывание пользователей ролям-наследницам.

Динамическое разделение обязанностей отличается от статического только тем, что рассматриваются роли, одновременно активные (быть может, в разных сеансах) для данного пользователя (а не те, которым пользователь статически приписан). Например, один пользователь может играть роль и кассира, и контролера, но не одновременно; чтобы стать контролером, он должен сначала закрыть кассу. Тем самым реализуется так называемое временное ограничение доверия, являющееся аспектом минимизации привилегий.

Рассматриваемый проект стандарта содержит спецификации трех категорий функций, необходимых для администрирования РУД:

1. **Административные функции** (создание и сопровождение ролей и других атрибутов ролевого доступа): создать/удалить роль/пользователя, приписать пользователя/право роли или ликвидировать существующую ассоциацию, создать/удалить отношение наследования между существующими ролями, создать новую роль и сделать ее наследницей/предшественницей существующей роли, создать/удалить ограничения для статического/динамического разделения обязанностей.
2. **Вспомогательные функции** (обслуживание сеансов работы пользователей): открыть сеанс работы пользователя с активацией подразумеваемого набора ролей; активировать новую роль, деактивировать роль; проверить правомерность доступа.
3. **Информационные функции** (получение сведений о текущей конфигурации с учетом отношения наследования). Здесь проводится разделение на обязательные и необязательные функции. К числу первых принадлежат получение списка пользователей, приписанных роли, и списка ролей, которым приписан пользователь.

Все остальные функции отнесены к разряду необязательных. Это получение информации о правах, приписанных роли, о правах заданного пользователя (которыми он обладает как член множества ролей), об активных в данный момент сеанса ролях и правах, об операциях, которые роль/пользователь правомочны совершить над заданным объектом, о статическом/динамическом разделении обязанностей.

Можно надеяться, что предлагаемый стандарт поможет сформировать единую терминологию и, что более важно, позволит оценивать РУД-продукты с единых позиций, по единой шкале.

Управление доступом в Java-среде

Java – это объектно-ориентированная система программирования, поэтому и управление доступом в ней спроектировано и реализовано в объектном стиле. По этой причине рассмотреть Java-среду для нас очень

важно. Подробно о Java-технологии и безопасности Java-среды рассказано в статье А. Таранова и В. Цишевского "Java в три года" (Jet Info, 1998, 11-12). С разрешения авторов далее используются ее фрагменты.

Прежде всего, остановимся на эволюции модели безопасности Java. В JDK 1.0 была предложена концепция "песочницы" (sandbox) – замкнутой среды, в которой выполняются потенциально ненадежные программы (апплеты, поступившие по сети). Программы, располагающиеся на локальном компьютере, считались абсолютно надежными, и им было доступно все, что доступно виртуальной Java-машине.

В число ограничений, налагаемых "песочницей", входит запрет на доступ к локальной файловой системе, на сетевое взаимодействие со всеми хостами, кроме источника апплета, и т.п. Независимо от уровня достигаемой при этом безопасности (а проблемы возникали и с разделением свой/чужой, и с определением источника апплета), наложенные ограничения следует признать слишком обременительными: возможности для содержательных действий у апплетов почти не остается.

Чтобы справиться с этой проблемой, в JDK 1.1 ввели деление источников (точнее, распространителей) апплетов на надежные и ненадежные (источник определялся по электронной подписи). Надежные апплеты приравнивались в правах к "родному" коду. Сделанное послабление решило проблемы тех, кому прав не хватало, но защита осталась неэшелонированной и, следовательно, неполной.

В JDK 1.2 сформировалась модель безопасности, используемая и в Java 2. От модели "песочницы" отказались. Оформились три основных понятия:

- источник программы;
- право и множество прав;
- политика безопасности.

Источник программы определяется парой (URL, распространители программы). Последние задаются набором цифровых сертификатов.

Право – это абстрактное понятие, за которым, как и положено в объектной среде, стоят классы и объекты. В большинстве случаев право определяется двумя цепочками символов – именем ресурса и действием. Например, в качестве ресурса может выступать файл, а в качестве действия – чтение. Важнейшим методом "правовых" объектов является implies(). Он проверяет, следует ли одно право (запрашиваемое) из другого (имеющегося).

Политика безопасности задает соответствие между источником и правами поступивших из него программ (формально можно считать, что каждому источнику соответствует своя "песочница"). В JDK 1.2 "родные" программы не имеют каких-либо привилегий в плане безопасности, и политика по отношению к ним может быть любой. В результате получился традиционный для современных ОС и СУБД механизм прав доступа со следующими особенностями:

- Java-программы выступают не от имени пользователя, их запустившего, а от имени источника программы. (Это весьма глубокая и прогрессивная трактовка, если ее правильно развить, см. следующий раздел);
- нет понятия владельца ресурсов, который мог бы менять права; последние задаются исключительно политикой безопасности (формально можно считать, что владельцем всего является тот, кто формирует политику);
- механизмы безопасности снабжены объектной оберткой.

Весьма важным понятием в модели безопасности JDK 1.2 является контекст выполнения. Когда виртуальная Java-машина проверяет права доступа объекта к системному ресурсу, она рассматривает не только текущий объект, но и предыдущие элементы стека вызовов. Доступ предоставляется только тогда, когда нужным правом обладают все объекты в стеке. Разработчики Java называют это реализацией принципа минимизации привилегий.

На первый взгляд, учет контекста представляется логичным. Нельзя допускать, чтобы вызов какого-либо метода расширял права доступа хотя бы по той причине, что доступ к системным ресурсам осуществляется не напрямую, а с помощью системных объектов, имеющих все права.

К сожалению, подобные доводы противоречат одному из основных принципов объектного подхода – принципу инкапсуляции. Если объект A обращается к объекту B, он не может и не должен знать, как реализован B и какими ресурсами он пользуется для своих целей. Если A имеет право вызывать какой-либо метод B с некоторыми значениями аргументов, B обязан обслужить вызов. В противном случае при формировании политики безопасности придется учитывать возможный граф вызовов объектов, что, конечно же, нереально.

Разработчики Java осознавали эту проблему. Чтобы справиться с ней, они ввели понятие привилегированного интервала программы. При выполнении такого интервала контекст игнорируется. Привилегированная программа отвечает за себя, не интересуясь предысторией. Аналогом привилегированных программ являются файлы с битами переустановки идентификатора пользователя/группы в ОС Unix, что лишний раз подтверждает традиционность подхода, реализованного в JDK 1.2. Известны угрозы безопасности, которые привносят подобные файлы. Теперь это не лучшее средство ОС Unix перекочевало в Java.

Рассмотрим дисциплину контроля прав доступа более формально.

Класс AccessController (встроенный менеджер безопасности) предоставляет единый метод для проверки заданного права в текущем контексте – checkPermission (Permission). Это лучше (по причине параметризуемости), чем множество методов вида checkXXX, присутствующих в SecurityManager – динамически изменяемом менеджере безопасности из ранних версий JDK.

Пусть текущий контекст выполнения состоит из N стековых фреймов (верхний соответствует методу, вызвавшему checkPermission(p)). Метод checkPermission реализует следующий алгоритм (см. Листинг 10.1).

```
i = N;
while (i > 0) {
    if (метод, породивший i-й фрейм, не имеет проверяемого
    права) {
        throw AccessControlException
        } else if (i-й фрейм помечен как привилегированный) {
            return;
        }
    i = i – 1;
};
// Выясним, есть ли проверяемое право у унаследованного
контекста
inheritedContext.checkPermission (p);
```

Листинг 10.1. Алгоритм работы метода checkPermission класса AccessController.

Сначала в стеке ищется фрейм, не обладающий проверяемым правом. Проверка производится до тех пор, пока либо не будет исчерпан стек, либо не встретится "привилегированный" фрейм, созданный в результате обращения к методу doPrivileged(PrivilegedAction) класса AccessController. Если при порождении текущего потока выполнения был сохранен контекст inheritedContext, проверяется и он. При положительном результате проверки метод checkPermission(p) возвращает управление, при отрицательном возникает исключительная ситуация AccessControlException.

Выбранный подход имеет один недостаток – тяжеловесность реализации. В частности, при порождении нового потока управления с ним приходится ассоциировать зафиксированный "родительский" контекст и, соответственно, проверять последний в процессе контроля прав доступа.

Отметим, что этот подход не распространяется на распределенный случай (хотя бы потому, что контекст имеет лишь локальный смысл, как, впрочем, и политика безопасности).

В целом средства управления доступом в JDK 1.2 можно оценить как "наполовину объектные". Реализация оформлена в виде интерфейсов и классов, однако по-прежнему разграничивается доступ к необъектным сущностям – ресурсам в традиционном понимании. Не учитывается семантика доступа. Имеют место и другие отмеченные выше концептуальные проблемы.

Возможный подход к управлению доступом в распределенной объектной среде

Представляется, что в настоящее время проблема управления доступом существует в трех почти не связанных между собой проявлениях:

- традиционные модели (дискреционная и мандатная);
- модель "песочница" (предложенная для Java-среды и близкой ей системы Safe-Tcl);
- модель фильтрации (используемая в межсетевых экранах).

На наш взгляд, необходимо объединить существующие подходы на основе их развития и обобщения.

Формальная постановка задачи разграничения доступа может выглядеть следующим образом.

Рассматривается множество объектов (в смысле объектно-ориентированного программирования). Часть объектов может являться контейнерами, группирующими объекты-компоненты, задающими для них общий контекст, выполняющими общие функции и реализующими перебор компонентов. Контейнеры либо вложены друг в друга, либо не имеют общих компонентов.

С каждым объектом ассоциирован набор интерфейсов, снабженных дескрипторами (ДИ). К объекту можно обратиться только посредством ДИ. Разные интерфейсы могут предоставлять разные методы и быть доступными для разных объектов.

Каждый контейнер позволяет опросить набор ДИ объектов-компонентов, удовлетворяющих некоторому условию. Возвращаемый результат в общем случае зависит от вызывающего объекта.

Объекты изолированы друг от друга. Единственным видом межобъектного взаимодействия является вызов метода.

Предполагается, что используются надежные средства аутентификации и защиты коммуникаций. В плане разграничения доступа локальные и удаленные вызовы не различаются.

Предполагается также, что разрешение или запрет на доступ не зависят от возможного параллельного выполнения методов (синхронизация представляет отдельную проблему, которая здесь не рассматривается).

Разграничивается доступ к интерфейсам объектов, а также к методам объектов (с учетом значений фактических параметров вызова). Правила разграничения доступа (ПРД) задаются в виде предикатов над объектами.

Рассматривается задача разграничения доступа для выделенного контейнера СС, компонентами которого должны являться вызывающий и/или вызываемый объекты. ДИ этого контейнера полагается общеизвестным. Считается также, что между внешними по отношению к выделенному контейнеру объектами возможны любые вызовы.

Выполнение ПРД контролируется монитором обращений.

При вызове метода мы будем разделять действия, производимые вызывающим объектом (инициация вызова) и вызываемым методом (прием и завершение вызова).

При инициации вызова может производиться преобразование ДИ фактических параметров к виду, доступному вызываемому методу ("трансляция интерфейса"). Трансляция может иметь место, если вызываемый объект не входит в тот же контейнер, что и вызывающий.

Параметры методов могут быть входными и/или выходными. При приеме вызова возникает информационный поток из входных параметров в вызываемый объект. В момент завершения вызова возникает информационный поток из вызываемого объекта в выходные параметры. Эти потоки могут фигурировать в правилах разграничения доступа.

Структурируем множество всех ПРД, выделив четыре группы правил:

- политика безопасности контейнера;
- ограничения на вызываемый метод;
- ограничения на вызывающий метод;
- добровольно налагаемые ограничения.

Правила, общие для всех объектов, входящих в контейнер С, назовем политикой безопасности данного контейнера.

Пусть метод М1 объекта О1 в точке Р1 своего выполнения должен вызвать метод М объекта О. Правила, которым должен удовлетворять М, можно разделить на три следующие подгруппы:

- правила, описывающие требования к формальным параметрам вызова;
- правила, описывающие требования к семантике М;
- реализационные правила, накладывающие ограничения на возможные реализации М;
- правила, накладывающие ограничения на вызываемый объект О.

Метод М объекта О, потенциально доступный для вызова, может предъявлять к вызывающему объекту следующие группы требований:

- правила, описывающие требования к фактическим параметрам вызова;
- правила, накладывающие ограничения на вызывающий объект.

Можно выделить три разновидности предикатов, соответствующих семантике и/или особенностям реализации методов:

- утверждения о фактических параметрах вызова метода М в точке Р1;
- предикат, описывающий семантику метода М;
- предикат, описывающий особенности реализации метода М.

Перечисленные ограничения можно назвать добровольными, поскольку они соответствуют реальному поведению объектов и не связаны с какими-либо внешними требованиями.

Предложенная постановка задачи разграничения доступа соответствует современному этапу развития программирования, она позволяет выразить сколь угодно сложную политику безопасности, найти баланс между богатством выразительных возможностей и эффективностью работы монитора обращений.

Вариант 1

1. В качестве аутентификатора в сетевой среде могут использоваться:

- ☐ координаты субъекта
- ☐ фамилия субъекта
- ☐ секретный криптографический ключ

2. Аутентификация на основе пароля, переданного по сети в открытом виде, плоха, потому что не обеспечивает защиты от:

- ☐ перехвата
- ☐ воспроизведения
- ☐ атак на доступность

3. В число основных понятий ролевого управления доступом входят:

- ☐ роль
- ☐ исполнитель роли
- ☐ пользователь роли

Вариант 2

1. В качестве аутентификатора в сетевой среде могут использоваться:

- ☐ сетевой адрес субъекта
- ☐ пароль
- ☐ цифровой сертификат субъекта

2. Аутентификация на основе пароля, переданного по сети в зашифрованном виде, плоха, потому что не обеспечивает защиты от:

- ☐ перехвата
- ☐ воспроизведения
- ☐ атак на доступность

3. В число основных понятий ролевого управления доступом входят:

- ☐ объект
- ☐ субъект
- ☐ метод

Вариант 3

1. В качестве аутентификатора в сетевой среде могут использоваться:

- ☐ кардиограмма субъекта
- ☐ номер карточки пенсионного страхования
- ☐ результат работы генератора одноразовых паролей

2. Аутентификация на основе пароля, переданного по сети в зашифрованном виде и снабженного открытой временной меткой, плоха, потому что не обеспечивает защиты от:

- ☐ перехвата
- ☐ воспроизведения
- ☐ атак на доступность

3. Ролевое управление доступом использует следующие средства объектно-ориентированного подхода

- ☐ инкапсуляция
- ☐ наследование
- ☐ полиморфизм

Лекция 11. Протоколирование и аудит, шифрование, контроль целостности

Описываются протоколирование и аудит, а также криптографические методы защиты. Показывается их место в общей архитектуре безопасности.

Ключевые слова: протоколирование, выборочное протоколирование, событие, сервис, регистрационная информация, аудит, подотчетность, детализация, доступность, подозрительная активность, злоумышленная активность, автоматическое реагирование, атака, злоупотребление полномочиями, сигнатура атаки, порог, профиль поведения, долгосрочный профиль, краткосрочный профиль, ошибка первого рода, пропуск атаки, ошибка второго рода, ложная тревога, эшелонированная оборона, менеджер, агент, интерфейс, сенсор, анализ, решатель, экспертная система, администратор безопасности, шифрование, симметричное шифрование, асимметричное шифрование, секретный ключ, открытый ключ, составной ключ, генерация ключей, распространение ключей, расшифрование, псевдослучайная последовательность, хэш-функция, дайджест, односторонняя функция, электронная цифровая подпись – ЭЦП, выработка ЭЦП, проверка ЭЦП, глобальная служба каталогов, удостоверяющий центр, цифровой сертификат.

Протоколирование и аудит

Основные понятия

Под протоколированием понимается сбор и накопление информации о событиях, происходящих в информационной системе. У каждого сервиса свой набор возможных событий, но в любом случае их можно разделить на внешние (вызванные действиями других сервисов), внутренние (вызванные действиями самого сервиса) и клиентские (вызванные действиями пользователей и администраторов).

Аудит – это анализ накопленной информации, проводимый оперативно, в реальном времени или периодически (например, раз в день). Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.

Реализация протоколирования и аудита решает следующие задачи:

- обеспечение подотчетности пользователей и администраторов;

- обеспечение возможности реконструкции последовательности событий;
- обнаружение попыток нарушений информационной безопасности;
- предоставление информации для выявления и анализа проблем.

Протоколирование требует для своей реализации здравого смысла. Какие события регистрировать? С какой степенью детализации? На подобные вопросы невозможно дать универсальные ответы. Необходимо следить за тем, чтобы, с одной стороны, достигались перечисленные выше цели, а, с другой, расход ресурсов оставался в пределах допустимого. Слишком обширное или подробное протоколирование не только снижает производительность сервисов (что отрицательно сказывается на доступности), но и затрудняет аудит, то есть не увеличивает, а уменьшает информационную безопасность.

Разумный подход к упомянутым вопросам применительно к операционным системам предлагается в "Оранжевой книге", где выделены следующие события:

- вход в систему (успешный или нет);
- выход из системы;
- обращение к удаленной системе;
- операции с файлами (открыть, закрыть, переименовать, удалить);
- смена привилегий или иных атрибутов безопасности (режима доступа, уровня благонадежности пользователя и т.п.).

При протоколировании события рекомендуется записывать, по крайней мере, следующую информацию:

- дата и время события;
- уникальный идентификатор пользователя – инициатора действия;
- тип события;
- результат действия (успех или неудача);
- источник запроса (например, имя терминала);
- имена затронутых объектов (например, открываемых или удаляемых файлов);
- описание изменений, внесенных в базы данных защиты (например, новая метка безопасности объекта).

Еще одно важное понятие, фигурирующее в "Оранжевой книге", – выборочное протоколирование, как в отношении пользователей (внимательно следить только за подозрительными), так и в отношении событий.

Характерная особенность протоколирования и аудита – зависимость от других средств безопасности. Идентификация и аутентификация служат отправной точкой подотчетности пользователей, логическое управле-

ние доступом защищает конфиденциальность и целостность регистрационной информации. Возможно, для защиты привлекаются и криптографические методы.

Возвращаясь к целям протоколирования и аудита, отметим, что обеспечение подотчетности важно в первую очередь как сдерживающее средство. Если пользователи и администраторы знают, что все их действия фиксируются, они, возможно, воздержатся от незаконных операций. Очевидно, если есть основания подозревать какого-либо пользователя в нечестности, можно регистрировать все его действия, вплоть до каждого нажатия клавиши. При этом обеспечивается не только возможность расследования случаев нарушения режима безопасности, но и откат некорректных изменений (если в протоколе присутствуют данные до и после модификации). Тем самым защищается целостность информации.

Реконструкция последовательности событий позволяет выявить слабости в защите сервисов, найти виновника вторжения, оценить масштабы причиненного ущерба и вернуться к нормальной работе.

Обнаружение попыток нарушений информационной безопасности – функция активного аудита, о котором пойдет речь в следующем разделе. Обычный аудит позволяет выявить подобные попытки с опозданием, но и это оказывается полезным. В свое время поимка немецких хакеров, действовавших по заказу КГБ, началась с выявления подозрительного расхождения в несколько центов в ежедневном отчете крупного вычислительного центра.

Выявление и анализ проблем могут помочь улучшить такой параметр безопасности, как доступность. Обнаружив узкие места, можно попытаться переконфигурировать или перенастроить систему, снова измерить производительность и т.д.

Непросто осуществить организацию согласованного протоколирования и аудита в распределенной разнородной системе. Во-первых, некоторые компоненты, важные для безопасности (например, маршрутизаторы), могут не обладать своими ресурсами протоколирования; в таком случае их нужно экранировать другими сервисами, которые возьмут протоколирование на себя. Во-вторых, необходимо увязывать между собой события в разных сервисах.

Активный аудит

Основные понятия

Под подозрительной активностью понимается поведение пользователя или компонента информационной системы, являющееся злоумышленным (в соответствии с заранее определенной политикой безопасности) или нетипичным (согласно принятым критериям).

Задача активного аудита – оперативно выявлять подозрительную активность и предоставлять средства для автоматического реагирования на нее.

Активность, не соответствующую политике безопасности, целесообразно разделить на атаки, направленные на незаконное получение полномочий, и на действия, выполняемые в рамках имеющихся полномочий, но нарушающие политику безопасности.

Атаки нарушают любую осмысленную политику безопасности. Иными словами, активность атакующего является разрушительной независимо от политики. Следовательно, для описания и выявления атак можно применять универсальные методы, инвариантные относительно политики безопасности, такие как сигнатуры и их обнаружение во входном потоке событий с помощью аппарата экспертных систем.

Сигнатура атаки – это совокупность условий, при выполнении которых атака считается имеющей место, что вызывает заранее определенную реакцию. Простейший пример сигнатуры – "зафиксированы три последовательные неудачные попытки входа в систему с одного терминала", пример ассоциированной реакции – блокирование терминала до прояснения ситуации.

Действия, выполняемые в рамках имеющихся полномочий, но нарушающие политику безопасности, мы будем называть злоупотреблением полномочиями. Злоупотребления полномочиями возможны из-за неадекватности средств разграничения доступа выбранной политике безопасности. Простейшим примером злоупотреблений является неэтичное поведение суперпользователя, просматривающего личные файлы других пользователей. Анализируя регистрационную информацию, можно обнаружить подобные события и сообщить о них администратору безопасности, хотя для этого необходимы соответствующие средства выражения политики безопасности.

Выделение злоупотреблений полномочиями в отдельную группу неправомерных действий, выявляемых средствами активного аудита, не является общепринятым, однако, на наш взгляд, подобный подход имеет право на существование и мы будем его придерживаться, хотя наиболее радикальным решением было бы развитие средств разграничения доступа (см. "Возможный подход к управлению доступом в распределенной объектной среде").

Нетипичное поведение выявляется статистическими методами. В простейшем случае применяют систему порогов, превышение которых является подозрительным. (Впрочем, "пороговый" метод можно трактовать и как вырожденный случай сигнатуры атаки, и как тривиальный способ выражения политики безопасности.) В более развитых системах производится сопоставление долговременных характеристик работы (назы-

ваемых долгосрочным профилем) с краткосрочными профилями. (Здесь можно усмотреть аналогию биометрической аутентификации по поведенческим характеристикам.)

Применительно к средствам активного аудита различают ошибки первого и второго рода: пропуск атак и ложные тревоги, соответственно. Нежелательность ошибок первого рода очевидна; ошибки второго рода не менее неприятны, поскольку отвлекают администратора безопасности от действительно важных дел, косвенно способствуя пропуску атак.

Достоинства сигнатурного метода – высокая производительность, малое число ошибок второго рода, обоснованность решений. Основной недостаток – неумение обнаруживать неизвестные атаки и вариации известных атак.

Основные достоинства статистического подхода – универсальность и обоснованность решений, потенциальная способность обнаруживать неизвестные атаки, то есть минимизация числа ошибок первого рода. Минусы заключаются в относительно высокой доле ошибок второго рода, плохой работе в случае, когда неправомерное поведение является типичным, когда типичное поведение плавно меняется от легального к неправомерному, а также в случаях, когда типичного поведения нет (как показывает статистика, таких пользователей примерно 5-10%).

Средства активного аудита могут располагаться на всех линиях обороны информационной системы. На границе контролируемой зоны они могут обнаруживать подозрительную активность в точках подключения к внешним сетям (не только попытки нелегального проникновения, но и действия по "прощупыванию" сервисов безопасности). В корпоративной сети, в рамках информационных сервисов и сервисов безопасности, активный аудит в состоянии обнаружить и пресечь подозрительную активность внешних и внутренних пользователей, выявить проблемы в работе сервисов, вызванные как нарушениями безопасности, так и аппаратно-программными ошибками. Важно отметить, что активный аудит, в принципе, способен обеспечить защиту от атак на доступность.

К сожалению, формулировка "в принципе, способен обеспечить защиту" не случайна. Активный аудит развивается более десяти лет, и первые результаты казались весьма многообещающими. Довольно быстро удалось реализовать распознавание простых типовых атак, однако затем было выявлено множество проблем, связанных с обнаружением заранее неизвестных атак, атак распределенных, растянутых во времени и т.п. Было бы наивно ожидать полного решения подобный проблем в ближайшее время. (Оперативное пополнение базы сигнатур атак таким решением, конечно, не является.) Тем не менее, и на нынешней стадии развития активный аудит полезен как один из рубежей (вернее, как набор прослоек) эшелонированной обороны.

Функциональные компоненты и архитектура

В составе средств активного аудита можно выделить следующие функциональные компоненты:

- компоненты генерации регистрационной информации. Они находятся на стыке между средствами активного аудита и контролируемыми объектами;
- компоненты хранения сгенерированной регистрационной информации;
- компоненты извлечения регистрационной информации (сенсоры). Обычно различают сетевые и хостовые сенсоры, имея в виду под первыми выделенные компьютеры, сетевые карты которых установлены в режим прослушивания, а под вторыми – программы, читающие регистрационные журналы операционной системы. На наш взгляд, с развитием коммутационных технологий это различие постепенно стирается, так как сетевые сенсоры приходится устанавливать в активном сетевом оборудовании и, по сути, они становятся частью сетевой ОС;
- компоненты просмотра регистрационной информации. Могут помочь при принятии решения о реагировании на подозрительную активность;
- компоненты анализа информации, поступившей от сенсоров. В соответствии с данным выше определением средств активного аудита, выделяют пороговый анализатор, анализатор нарушений политики безопасности, экспертную систему, выявляющую сигнатуры атак, а также статистический анализатор, обнаруживающий нетипичное поведение;
- компоненты хранения информации, участвующей в анализе. Такое хранение необходимо, например, для выявления атак, протяженных во времени;
- компоненты принятия решений и реагирования ("решатели"). "Решатель" может получать информацию не только от локальных, но и от внешних анализаторов, проводя так называемый корреляционный анализ распределенных событий;
- компоненты хранения информации о контролируемых объектах. Здесь могут храниться как пассивные данные, так и методы, необходимые, например, для извлечения из объекта регистрационной информации или для реагирования;
- компоненты, играющие роль организующей оболочки для менеджеров активного аудита, называемые мониторами и объединяющие анализаторы, "решатели", хранилище описаний объектов и интерфейсные компоненты. В число последних входят компоненты интерфейса с другими мониторами, как равно-

правными, так и входящими в иерархию. Такие интерфейсы необходимы, например, для выявления распределенных, широкомасштабных атак;

- компоненты интерфейса с администратором безопасности.

Средства активного аудита строятся в архитектуре менеджер/агент. Основными агентскими компонентами являются сенсоры. Анализ, принятие решений – функции менеджеров. Очевидно, между менеджерами и агентами должны быть сформированы доверенные каналы.

Подчеркнем важность интерфейсных компонентов. Они полезны как с внутренней для средств активного аудита точки зрения (обеспечивают расширяемость, подключение компонентов различных производителей), так и с внешней точки зрения. Между менеджерами (между компонентами анализа и "решателями") могут существовать горизонтальные связи, необходимые для анализа распределенной активности. Возможно также формирование иерархий средств активного аудита с вынесением на верхние уровни информации о наиболее масштабной и опасной активности.

Обратим также внимание на архитектурную общность средств активного аудита и управления, являющуюся следствием общности выполняемых функций. Продуманные интерфейсные компоненты могут существенно облегчить совместную работу этих средств.

Шифрование

Мы приступаем к рассмотрению криптографических сервисов безопасности, точнее, к изложению элементарных сведений, помогающих составить общее представление о компьютерной криптографии и ее месте в общей архитектуре информационных систем.

Криптография необходима для реализации, по крайней мере, трех сервисов безопасности:

- шифрование;
- контроль целостности;
- аутентификация (этот сервис был рассмотрен нами ранее).

Шифрование – наиболее мощное средство обеспечения конфиденциальности. Во многих отношениях оно занимает центральное место среди программно-технических регуляторов безопасности, являясь основой реализации многих из них, и в то же время последним (а подчас и единственным) защитным рубежом. Например, для портативных компьютеров только шифрование позволяет обеспечить конфиденциальность данных даже в случае кражи.

В большинстве случаев и шифрование, и контроль целостности играют глубоко инфраструктурную роль, оставаясь прозрачными и для приложений, и для пользователей. Типичное место этих сервисов безопасности – на сетевом и транспортном уровнях реализации стека сетевых протоколов.

Различают два основных метода шифрования: симметричный и асимметричный. В первом из них один и тот же ключ (хранящийся в секрете) используется и для зашифрования, и для расшифрования данных. Разработаны весьма эффективные (быстрые и надежные) методы симметричного шифрования. Существует и национальный стандарт на подобные методы – ГОСТ 28147-89 "Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования".

Рис. 11.1 иллюстрирует использование симметричного шифрования. Для определенности мы будем вести речь о защите сообщений, хотя события могут развиваться не только в пространстве, но и во времени, когда зашифровываются и расшифровываются никуда не перемещающиеся файлы.

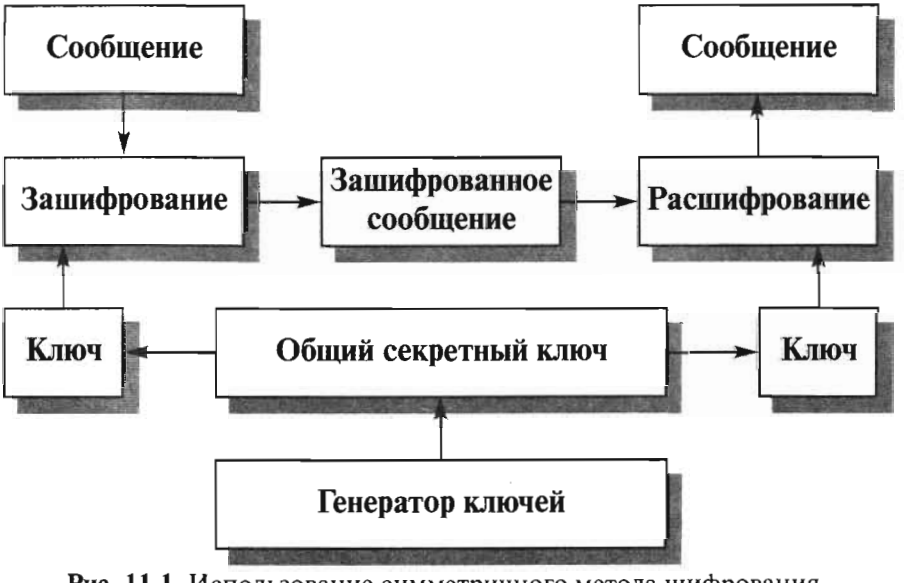

Рис. 11.1. Использование симметричного метода шифрования.

Основным недостатком симметричного шифрования является то, что секретный ключ должен быть известен и отправителю, и получателю. С одной стороны, это создает новую проблему распространения ключей. С другой стороны, получатель на основании наличия зашифрованного и расшифрованного сообщения не может доказать, что он получил это сообщение от конкретного отправителя, поскольку такое же сообщение он мог сгенерировать самостоятельно.

В асимметричных методах используются два ключа. Один из них, несекретный (он может публиковаться вместе с другими открытыми сведениями о пользователе), применяется для шифрования, другой (секретный, известный только получателю) – для расшифрования. Самым попу-

лярным из асимметричных является метод RSA (Райвест, Шамир, Адлеман), основанный на операциях с большими (скажем, 100-значными) простыми числами и их произведениями.

Проиллюстрируем использование асимметричного шифрования (см. рис. 11.2).

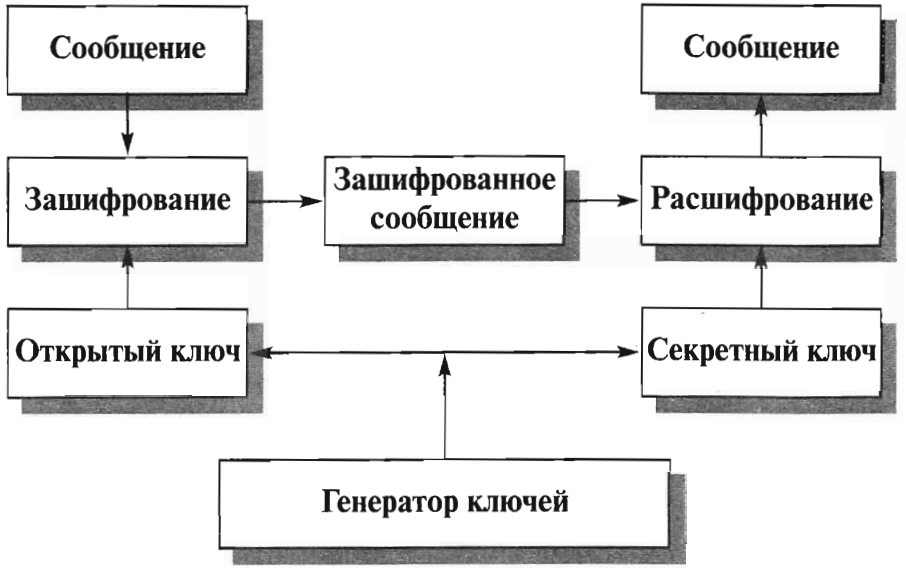

Рис. 11.2. Использование асимметричного метода шифрования.

Существенным недостатком асимметричных методов шифрования является их низкое быстродействие, поэтому данные методы приходится сочетать с симметричными (асимметричные методы на 3 – 4 порядка медленнее). Так, для решения задачи эффективного шифрования с передачей секретного ключа, использованного отправителем, сообщение сначала симметрично зашифровывают случайным ключом, затем этот ключ зашифровывают открытым асимметричным ключом получателя, после чего сообщение и ключ отправляются по сети.

Рис. 11.3 иллюстрирует эффективное шифрование, реализованное путем сочетания симметричного и асимметричного методов.

На рис. 11.4 показано расшифрование эффективно зашифрованного сообщения.

Отметим, что асимметричные методы позволили решить важную задачу совместной выработки секретных ключей (это существенно, если стороны не доверяют друг другу), обслуживающих сеанс взаимодействия, при изначальном отсутствии общих секретов. Для этого используется алгоритм Диффи-Хелмана.

Рис. 11.3. Эффективное шифрование сообщения.

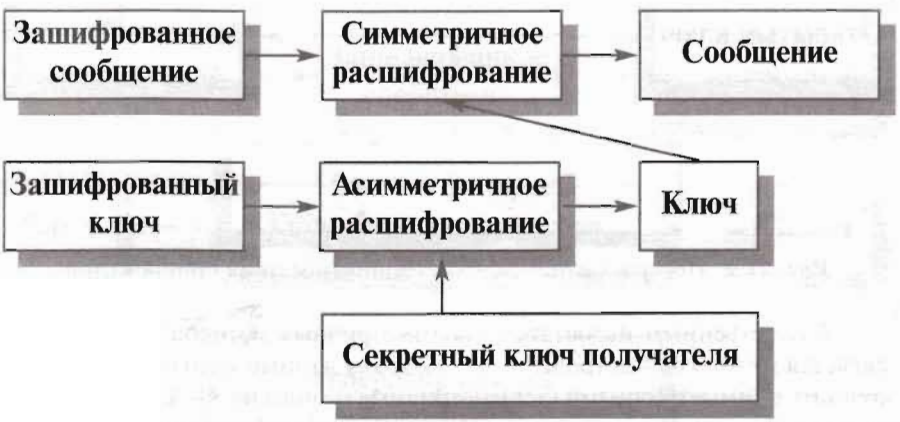

Рис. 11.4. Расшифрование эффективно зашифрованного сообщения.

Определенное распространение получила разновидность симметричного шифрования, основанная на использовании составных ключей. Идея состоит в том, что секретный ключ делится на две части, хранящиеся отдельно. Каждая часть сама по себе не позволяет выполнить расшифрование. Если у правоохранительных органов появляются подозрения относительно лица, использующего некоторый ключ, они могут в установленном порядке получить половинки ключа и дальше действовать обычным для симметричного расшифрования образом.

Порядок работы с составными ключами – хороший пример следования принципу разделения обязанностей. Он позволяет сочетать права на разного рода тайны (персональную, коммерческую) с возможностью эф-

фективно следить за нарушителями закона, хотя, конечно, здесь очень много тонкостей и технического, и юридического плана.

Многие криптографические алгоритмы в качестве одного из параметров требуют псевдослучайное значение, в случае предсказуемости которого в алгоритме появляется уязвимость (подобное уязвимое место было обнаружено в некоторых вариантах Web-навигаторов). Генерация псевдослучайных последовательностей – важный аспект криптографии, на котором мы, однако, останавливаться не будем.

Более подробную информацию о компьютерной криптографии можно почерпнуть из статьи Г. Семенова "Не только шифрование, или Обзор криптотехнологий" (Jet Info, 2001, 3).

Контроль целостности

Криптографические методы позволяют надежно контролировать целостность как отдельных порций данных, так и их наборов (таких как поток сообщений); определять подлинность источника данных; гарантировать невозможность отказаться от совершенных действий ("неотказуемость").

В основе криптографического контроля целостности лежат два понятия:

- хэш-функция;
- электронная цифровая подпись (ЭЦП).

Хэш-функция – это труднообратимое преобразование данных (односторонняя функция), реализуемое, как правило, средствами симметричного шифрования со связыванием блоков. Результат шифрования последнего блока (зависящий от всех предыдущих) и служит результатом хэш-функции.

Пусть имеются данные, целостность которых нужно проверить, хэш-функция и ранее вычисленный результат ее применения к исходным данным (так называемый дайджест). Обозначим хэш-функцию через h, исходные данные – через T, проверяемые данные – через T'. Контроль целостности данных сводится к проверке равенства h(T') = h(T). Если оно выполнено, считается, что T' = T. Совпадение дайджестов для различных данных называется коллизией. В принципе, коллизии, конечно, возможны, поскольку мощность множества дайджестов меньше, чем мощность множества хэшируемых данных, однако то, что h есть функция односторонняя, означает, что за приемлемое время специально организовать коллизию невозможно.

Рассмотрим теперь применение асимметричного шифрования для выработки и проверки электронной цифровой подписи. Пусть E(T) обозначает результат зашифрования текста T с помощью открытого ключа, а D(T) – результат расшифрования текста T (как правило,

шифрованного) с помощью секретного ключа. Чтобы асимметричный метод мог применяться для реализации ЭЦП, необходимо выполнение тождества

$$E(D(T)) = D(E(T)) = T$$

На рис. 11.5 показана процедура выработки электронной цифровой подписи, состоящая в шифровании преобразованием D дайджеста h(T).

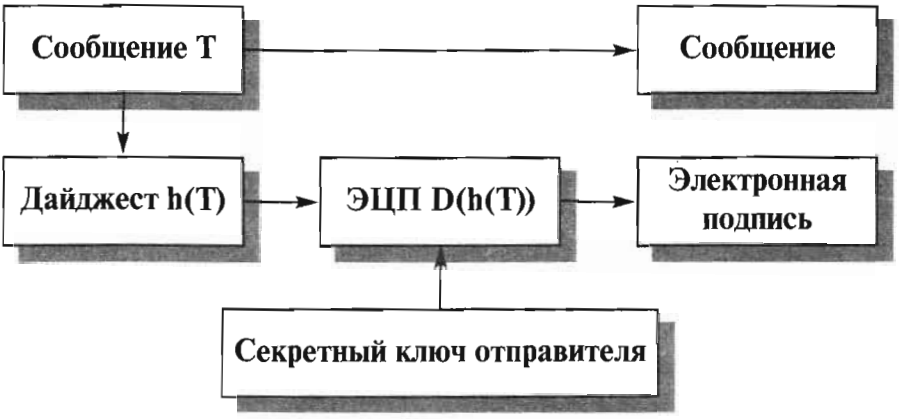

Рис. 11.5. Выработка электронной цифровой подписи.

Проверка ЭЦП может быть реализована так, как показано на рис. 11.6.

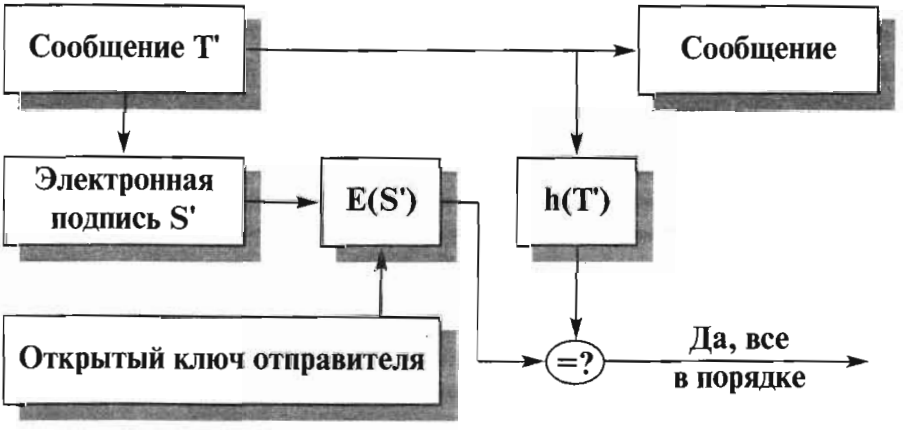

Рис. 11.6. Проверка электронной цифровой подписи.

Из равенства

$$E(S') = h(T')$$

следует, что S' = D(h(T') (для доказательства достаточно применить к обеим частям преобразование D и вычеркнуть в левой части тождественное преобразование D(E())). Таким образом, электронная цифровая подпись защищает целостность сообщения и удостоверяет личность отправителя, то есть защищает целостность источника данных и служит основой неотказуемости.

Два российских стандарта, ГОСТ Р 34.10-94 "Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма" и ГОСТ Р 34.11-94 "Функция хэширования", объединенные общим заголовком "Информационная технология. Криптографическая защита информации", регламентируют вычисление дайджеста и реализацию ЭЦП. В сентябре 2001 года был утвержден, а 1 июля 2002 года вступил в силу новый стандарт ЭЦП – ГОСТ Р 34.10-2001, разработанный специалистами ФАПСИ.

Для контроля целостности последовательности сообщений (то есть для защиты от кражи, дублирования и переупорядочения сообщений) применяют временные штампы и нумерацию элементов последовательности, при этом штампы и номера включают в подписываемый текст.

Цифровые сертификаты

При использовании асимметричных методов шифрования (и, в частности, электронной цифровой подписи) необходимо иметь гарантию подлинности пары (имя пользователя, открытый ключ пользователя). Для решения этой задачи в спецификациях X.509 вводятся понятия цифрового сертификата и удостоверяющего центра.

Удостоверяющий центр – это компонент глобальной службы каталогов, отвечающий за управление криптографическими ключами пользователей. Открытые ключи и другая информация о пользователях хранится удостоверяющими центрами в виде цифровых сертификатов, имеющих следующую структуру:

- порядковый номер сертификата;
- идентификатор алгоритма электронной подписи;
- имя удостоверяющего центра;
- срок годности;
- имя владельца сертификата (имя пользователя, которому принадлежит сертификат);
- открытые ключи владельца сертификата (ключей может быть несколько);

- идентификаторы алгоритмов, ассоциированных с открытыми ключами владельца сертификата;
- электронная подпись, сгенерированная с использованием секретного ключа удостоверяющего центра (подписывается результат хэширования всей информации, хранящейся в сертификате).

Цифровые сертификаты обладают следующими свойствами:

- любой пользователь, знающий открытый ключ удостоверяющего центра, может узнать открытые ключи других клиентов центра и проверить целостность сертификата;
- никто, кроме удостоверяющего центра, не может модифицировать информацию о пользователе без нарушения целостности сертификата.

В спецификациях X.509 не описывается конкретная процедура генерации криптографических ключей и управления ими, однако даются некоторые общие рекомендации. В частности, оговаривается, что пары ключей могут порождаться любым из следующих способов.

- ключи может генерировать сам пользователь. В таком случае секретный ключ не попадает в руки третьих лиц, однако нужно решать задачу безопасной связи с удостоверяющим центром;
- ключи генерирует доверенное лицо. В таком случае приходится решать задачи безопасной доставки секретного ключа владельцу и предоставления доверенных данных для создания сертификата;
- ключи генерируются удостоверяющим центром. В таком случае остается только задача безопасной передачи ключей владельцу.

Цифровые сертификаты в формате X.509 версии 3 стали не только формальным, но и фактическим стандартом, поддерживаемым многочисленными удостоверяющими центрами.

Вариант 1

1. Протоколирование само по себе не может обеспечить неотказуемость, потому что:

- ☐ регистрационная информация, как правило, имеет низкоуровневый характер, а неотказуемость относится к действиям прикладного уровня
- ☐ регистрационная информация имеет специфический формат, непонятный человеку
- ☐ регистрационная информация имеет слишком большой объем

2. Сигнатурный метод выявления атак хорош тем, что он:

- ☐ поднимает мало ложных тревог
- ☐ способен обнаруживать неизвестные атаки
- ☐ прост в настройке и эксплуатации

3. Цифровой сертификат содержит:

- ☐ открытый ключ пользователя
- ☐ секретный ключ пользователя
- ☐ имя пользователя

Вариант 2

1. Протоколирование само по себе не может обеспечить неотказуемость, потому что:

- ☐ регистрационная информация может быть рассредоточена по разным сервисам и разным компонентам распределенной ИС
- ☐ целостность регистрационной информации может быть нарушена
- ☐ должна соблюдаться конфиденциальность регистрационной информации, а проверка неотказуемости нарушит конфиденциальность

2. Статистический метод выявления атак хорош тем, что он:

- ☐ поднимает мало ложных тревог
- ☐ способен обнаруживать неизвестные атаки
- ☐ прост в настройке и эксплуатации

3. Цифровой сертификат содержит:

- ☐ открытый ключ удостоверяющего центра
- ☐ секретный ключ удостоверяющего центра
- ☐ имя удостоверяющего центра

Вариант 3

1. Протоколирование само по себе не может обеспечить неотказуемость, потому что:

- ☐ регистрационная информация относится к разным уровням стека сетевых протоколов
- ☐ объем регистрационной информации очень быстро растет, ее приходится перемещать на вторичные носители, чтение с которых сопряжено с техническими проблемами
- ☐ регистрационная информация для разных компонентов распределенной системы может оказаться рассогласованной

2. Пороговый метод выявления атак хорош тем, что он:

- ☐ поднимает мало ложных тревог
- ☐ способен обнаруживать неизвестные атаки
- ☐ прост в настройке и эксплуатации

3. Цифровой сертификат содержит:

- ☐ ЭЦП пользователя
- ☐ ЭЦП доверенного центра
- ☐ ЭЦП генератора криптографических ключей

Лекция 12. Экранирование, анализ защищенности

Рассматриваются сравнительно новые (развивающиеся с начала 1990-х годов) сервисы безопасности – экранирование и анализ защищенности.

Ключевые слова: экран, экранирование, разграничение доступа, протоколирование, фильтрация, фильтр, межсетевой экран (МЭ), доступность, конфиденциальность, частичное экранирование, ограничивающий интерфейс, Web-сервис, внутренний МЭ, внешний МЭ, двухкомпонентное экранирование, демилитаризованная зона, граничный маршрутизатор, многопротокольный МЭ, сервер-посредник, составной МЭ, персональный МЭ, персональное экранирующее устройство, архитектурная безопасность, эшелонированность обороны, простота, управляемость, невозможность перехода в небезопасное состояние, внешние угрозы, внутренние угрозы, экранирующий концентратор, экранирующий маршрутизатор, пакетный фильтр, порт, входная фильтрация, выходная фильтрация, транспортное экранирование, прикладной МЭ, комплексный МЭ, прозрачность, экранирующий агент, трансляция адресов, простота использования, собственная защищенность, централизованное администрирование, база правил, непротиворечивость базы правил, контроль "на лету", ПО промежуточного слоя, маршрутизация запросов, балансировка нагрузки, многозвенная архитектура клиент/сервер, анализ защищенности, сканер защищенности, база данных уязвимостей, сетевой сканер, антивирусная защита, автообнаружение.

Экранирование

Основные понятия

Формальная постановка задачи экранирования состоит в следующем. Пусть имеется два множества информационных систем. Экран – это средство разграничения доступа клиентов из одного множества к серверам из другого множества. Экран осуществляет свои функции, контролируя все информационные потоки между двумя множествами систем (рис. 12.1). Контроль потоков состоит в их фильтрации, возможно, с выполнением некоторых преобразований.

На следующем уровне детализации экран (полупроницаемую мембрану) удобно представлять как последовательность фильтров. Каждый из

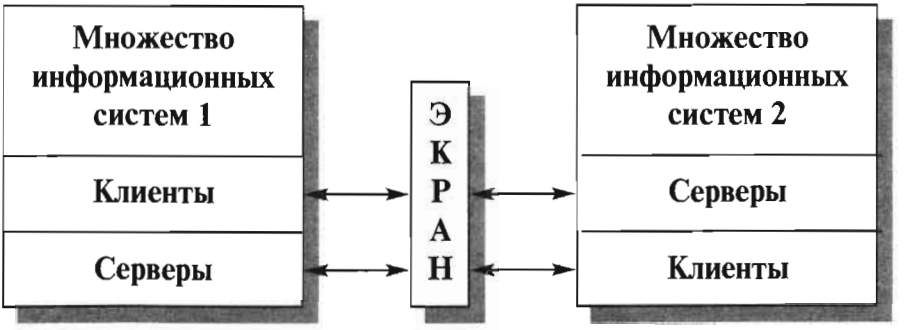

Рис. 12.1. Экран как средство разограничения доступа.

фильтров, проанализировав данные, может задержать (не пропустить) их, а может и сразу "перебросить" за экран. Кроме того, допускается преобразование данных, передача порции данных на следующий фильтр для продолжения анализа или обработка данных от имени адресата и возврат результата отправителю (рис. 12.2).

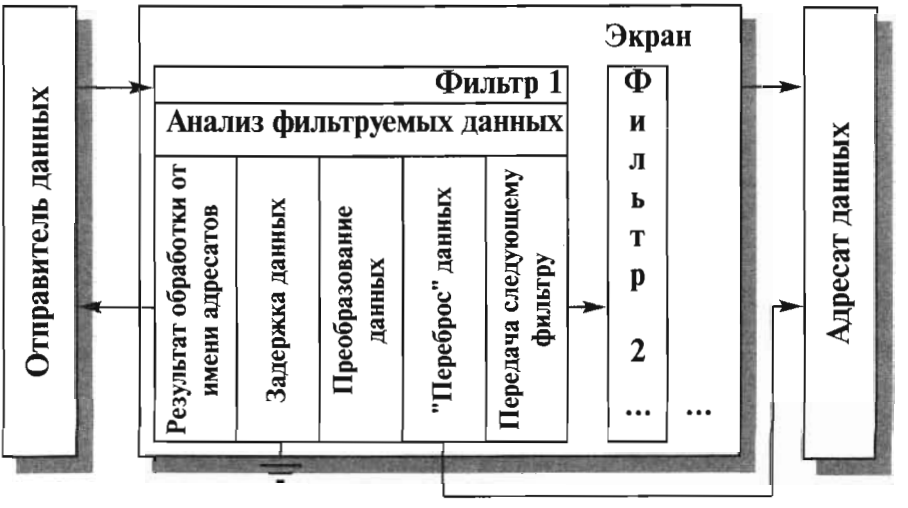

Рис. 12.2. Экран как последовательность фильтров.

Помимо функций разграничения доступа, экраны осуществляют протоколирование обмена информацией.

Обычно экран не является симметричным, для него определены понятия "внутри" и "снаружи". При этом задача экранирования формулируется как защита внутренней области от потенциально враждебной внешней. Так, межсетевые экраны (МЭ) (предложенный автором перевод английского термина firewall) чаще всего устанавливают для защиты корпо-

ративной сети организации, имеющей выход в Internet (см. следующий раздел).

Экранирование помогает поддерживать доступность сервисов внутренней области, уменьшая или вообще ликвидируя нагрузку, вызванную внешней активностью. Уменьшается уязвимость внутренних сервисов безопасности, поскольку первоначально злоумышленник должен преодолеть экран, где защитные механизмы сконфигурированы особенно тщательно. Кроме того, экранирующая система, в отличие от универсальной, может быть устроена более простым и, следовательно, более безопасным образом.

Экранирование дает возможность контролировать также информационные потоки, направленные во внешнюю область, что способствует поддержанию режима конфиденциальности в ИС организации.

Подчеркнем, что экранирование может использоваться как сервис безопасности не только в сетевой, но и в любой другой среде, где происходит обмен сообщениями. Важнейший пример подобной среды – объектно-ориентированные программные системы, когда для активизации методов объектов выполняется (по крайней мере, в концептуальном плане) передача сообщений. Весьма вероятно, что в будущих объектно-ориентированных средах экранирование станет одним из важнейших инструментов разграничения доступа к объектам.

Экранирование может быть частичным, защищающим определенные информационные сервисы. Экранирование электронной почты описано в статье "Контроль над корпоративной электронной почтой: система "Дозор-Джет"" (Jet Info, 2002, 5).

Ограничивающий интерфейс также можно рассматривать как разновидность экранирования. На невидимый объект трудно нападать, особенно с помощью фиксированного набора средств. В этом смысле Web-интерфейс обладает естественной защитой, особенно в том случае, когда гипертекстовые документы формируются динамически. Каждый пользователь видит лишь то, что ему положено видеть. Можно провести аналогию между динамически формируемыми гипертекстовыми документами и представлениями в реляционных базах данных, с той существенной оговоркой, что в случае Web возможности существенно шире.

Экранирующая роль Web-сервиса наглядно проявляется и тогда, когда этот сервис осуществляет посреднические (точнее, интегрирующие) функции при доступе к другим ресурсам, например таблицам базы данных. Здесь не только контролируются потоки запросов, но и скрывается реальная организация данных.

Архитектурные аспекты

Бороться с угрозами, присущими сетевой среде, средствами универсальных операционных систем не представляется возможным. Универсальная ОС

– это огромная программа, наверняка содержащая, помимо явных ошибок, некоторые особенности, которые могут быть использованы для нелегального получения привилегий. Современная технология программирования не позволяет сделать столь большие программы безопасными. Кроме того, администратор, имеющий дело со сложной системой, далеко не всегда в состоянии учесть все последствия производимых изменений. Наконец, в универсальной многопользовательской системе бреши в безопасности постоянно создаются самими пользователями (слабые и/или редко изменяемые пароли, неудачно установленные права доступа, оставленный без присмотра терминал и т.п.). Единственный перспективный путь связан с разработкой специализированных сервисов безопасности, которые в силу своей простоты допускают формальную или неформальную верификацию. Межсетевой экран как раз и является таким средством, допускающим дальнейшую декомпозицию, связанную с обслуживанием различных сетевых протоколов.

Межсетевой экран располагается между защищаемой (внутренней) сетью и внешней средой (внешними сетями или другими сегментами корпоративной сети). В первом случае говорят о внешнем МЭ, во втором – о внутреннем. В зависимости от точки зрения, внешний межсетевой экран можно считать первой или последней (но никак не единственной) линией обороны. Первой – если смотреть на мир глазами внешнего злоумышленника. Последней – если стремиться к защищенности всех компонентов корпоративной сети и пресечению неправомерных действий внутренних пользователей.

Межсетевой экран – идеальное место для встраивания средств активного аудита. С одной стороны, и на первом, и на последнем защитном рубеже выявление подозрительной активности по-своему важно. С другой стороны, МЭ способен реализовать сколь угодно мощную реакцию на подозрительную активность, вплоть до разрыва связи с внешней средой. Правда, нужно отдавать себе отчет в том, что соединение двух сервисов безопасности в принципе может создать брешь, способствующую атакам на доступность.

На межсетевой экран целесообразно возложить идентификацию/аутентификацию внешних пользователей, нуждающихся в доступе к корпоративным ресурсам (с поддержкой концепции единого входа в сеть).

В силу принципов эшелонированности обороны для защиты внешних подключений обычно используется двухкомпонентное экранирование (см. рис. 12.3). Первичная фильтрация (например, блокирование пакетов управляющего протокола SNMP, опасного атаками на доступность, или пакетов с определенными IP-адресами, включенными в "черный список") осуществляется граничным маршрутизатором (см. также следующий раздел), за которым располагается так называемая демилитаризованная зона (сеть с умеренным доверием безопасности, куда выносятся внешние информационные сервисы организации – Web, электронная почта и т.п.) и основной МЭ, защищающий внутреннюю часть корпоративной сети.

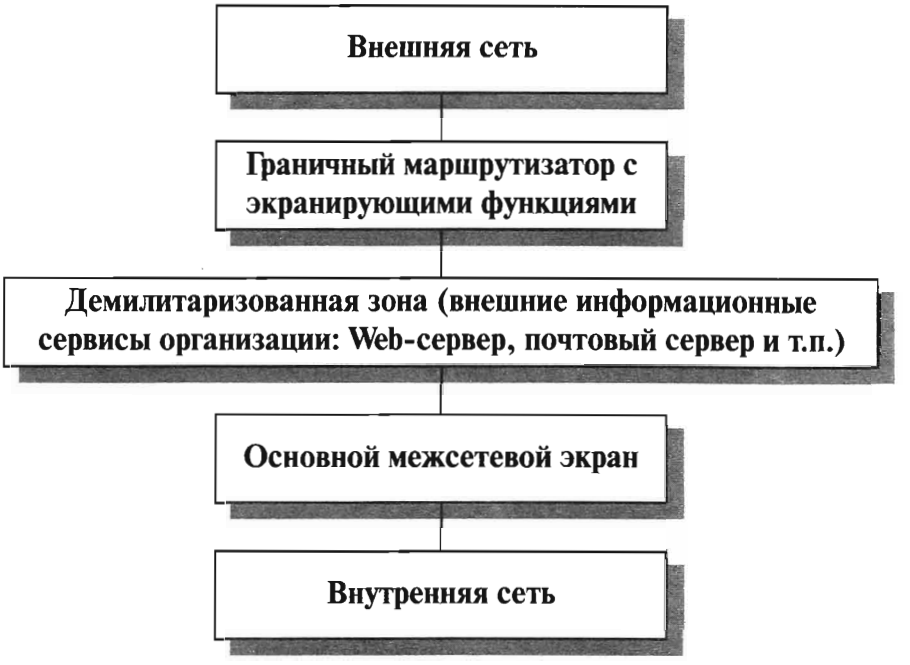

Рис. 12.3. Двухкомпонентное экранирование с демилитаризованной зоной.

Теоретически межсетевой экран (особенно внутренний) должен быть многопротокольным, однако на практике доминирование семейства протоколов TCP/IP столь велико, что поддержка других протоколов представляется излишеством, вредным для безопасности (чем сложнее сервис, тем он более уязвим).

Вообще говоря, и внешний, и внутренний межсетевой экран может стать узким местом, поскольку объем сетевого трафика имеет тенденцию быстрого роста. Один из подходов к решению этой проблемы предполагает разбиение МЭ на несколько аппаратных частей и организацию специализированных серверов-посредников. Основной межсетевой экран может проводить грубую классификацию входящего трафика по видам и передоверять фильтрацию соответствующим посредникам (например, посреднику, анализирующему HTTP-трафик). Исходящий трафик сначала обрабатывается сервером-посредником, который может выполнять и функционально полезные действия, такие как кэширование страниц внешних Web-серверов, что снижает нагрузку на сеть вообще и основной МЭ в частности.

Ситуации, когда корпоративная сеть содержит лишь один внешний канал, являются скорее исключением, чем правилом. Напротив, типична

ситуация, при которой корпоративная сеть состоит из нескольких территориально разнесенных сегментов, каждый из которых подключен к Internet. В этом случае каждое подключение должно защищаться своим экраном. Точнее говоря, можно считать, что корпоративный внешний межсетевой экран является составным, и требуется решать задачу согласованного администрирования (управления и аудита) всех компонентов.

Противоположностью составным корпоративным МЭ (или их компонентами) являются персональные межсетевые экраны и персональные экранирующие устройства. Первые являются программными продуктами, которые устанавливаются на персональные компьютеры и защищают только их. Вторые реализуются на отдельных устройствах и защищают небольшую локальную сеть, такую как сеть домашнего офиса.

При развертывании межсетевых экранов следует соблюдать рассмотренные нами ранее принципы архитектурной безопасности, в первую очередь позаботившись о простоте и управляемости, об эшелонированности обороны, а также о невозможности перехода в небезопасное состояние. Кроме того, следует принимать во внимание не только внешние, но и внутренние угрозы.

Классификация межсетевых экранов

При рассмотрении любого вопроса, касающегося сетевых технологий, основой служит семиуровневая эталонная модель ISO/OSI. Межсетевые экраны также целесообразно классифицировать по уровню фильтрации – канальному, сетевому, транспортному или прикладному. Соответственно, можно говорить об экранирующих концентраторах (мостах, коммутаторах) (уровень 2), маршрутизаторах (уровень 3), о транспортном экранировании (уровень 4) и о прикладных экранах (уровень 7). Существуют также комплексные экраны, анализирующие информацию на нескольких уровнях.

Фильтрация информационных потоков осуществляется межсетевыми экранами на основе набора правил, являющихся выражением сетевых аспектов политики безопасности организации. В этих правилах, помимо информации, содержащейся в фильтруемых потоках, могут фигурировать данные, полученные из окружения, например, текущее время, количество активных соединений, порт, через который поступил сетевой запрос, и т.д. Таким образом, в межсетевых экранах используется очень мощный логический подход к разграничению доступа.

Возможности межсетевого экрана непосредственно определяются тем, какая информация может использоваться в правилах фильтрации и какова может быть мощность наборов правил. Вообще говоря, чем выше уровень в модели ISO/OSI, на котором функционирует МЭ, тем более содержательная информация ему доступна и, следовательно, тем тоньше и надежнее он может быть сконфигурирован.

Экранирующие маршрутизаторы (и концентраторы) имеют дело с отдельными пакетами данных, поэтому иногда их называют пакетными фильтрами. Решения о том, пропустить или задержать данные, принимаются для каждого пакета независимо, на основании анализа адресов и других полей заголовков сетевого (канального) и, быть может, транспортного уровней. Еще один важный компонент анализируемой информации – порт, через который поступил пакет.

Экранирующие концентраторы являются средством не столько разграничения доступа, сколько оптимизации работы локальной сети за счет организации так называемых виртуальных локальных сетей. Последние можно считать важным результатом применения внутреннего межсетевого экранирования.

Современные маршрутизаторы позволяют связывать с каждым портом несколько десятков правил и фильтровать пакеты как на входе, так и на выходе. В принципе, в качестве пакетного фильтра может использоваться и универсальный компьютер, снабженный несколькими сетевыми картами.

Основные достоинства экранирующих маршрутизаторов – доступная цена (на границе сетей маршрутизатор нужен практически всегда, вопрос лишь в том, как задействовать его экранирующие возможности) и прозрачность для более высоких уровней модели OSI. Основной недостаток – ограниченность анализируемой информации и, как следствие, относительная слабость обеспечиваемой защиты.

Транспортное экранирование позволяет контролировать процесс установления виртуальных соединений и передачу информации по ним. С точки зрения реализации экранирующий транспорт представляет собой довольно простую, а значит, надежную программу.

По сравнению с пакетными фильтрами, транспортное экранирование обладает большей информацией, поэтому соответствующий МЭ может осуществлять более тонкий контроль за виртуальными соединениями (например, он способен отслеживать количество передаваемой информации и разрывать соединения после превышения определенного порога, препятствуя тем самым несанкционированному экспорту информации). Аналогично, возможно накопление более содержательной регистрационной информации. Главный недостаток – сужение области применения, поскольку вне контроля остаются датаграммные протоколы. Обычно транспортное экранирование применяют в сочетании с другими подходами, как важный дополнительный элемент.

Межсетевой экран, функционирующий на прикладном уровне, способен обеспечить наиболее надежную защиту. Как правило, подобный МЭ представляет собой универсальный компьютер, на котором функционируют экранирующие агенты, интерпретирующие протоколы приклад-

ного уровня (HTTP, FTP, SMTP, telnet и т.д.) в той степени, которая необходима для обеспечения безопасности.

При использовании прикладных МЭ, помимо фильтрации, реализуется еще один важнейший аспект экранирования. Субъекты из внешней сети видят только шлюзовой компьютер; соответственно, им доступна только та информация о внутренней сети, которую он считает нужным экспортировать. Прикладной МЭ на самом деле экранирует, то есть заслоняет, внутреннюю сеть от внешнего мира. В то же время, субъектам внутренней сети кажется, что они напрямую общаются с объектами внешнего мира. Недостаток прикладных МЭ – отсутствие полной прозрачности, требующее специальных действий для поддержки каждого прикладного протокола.

Если организация располагает исходными текстами прикладного МЭ и в состоянии эти тексты модифицировать, перед ней открываются чрезвычайно широкие возможности по настройке экрана с учетом собственных нужд. Дело в том, что при разработке систем клиент/сервер в многозвенной архитектуре появляются специфические прикладные протоколы, нуждающиеся в защите не меньше стандартных. Подход, основанный на использовании экранирующих агентов, позволяет построить такую защиту, не снижая безопасности и эффективности других приложений и не усложняя структуру связей в межсетевом экране.

Комплексные межсетевые экраны, охватывающие уровни от сетевого до прикладного, соединяют в себе лучшие свойства "одноуровневых" МЭ разных видов. Защитные функции выполняются комплексными МЭ прозрачным для приложений образом, не требуя внесения каких-либо изменений ни в существующее программное обеспечение, ни в действия, ставшие для пользователей привычными.

Комплексность МЭ может достигаться разными способами: "снизу вверх", от сетевого уровня через накопление контекста к прикладному уровню, или "сверху вниз", посредством дополнения прикладного МЭ механизмами транспортного и сетевого уровней.

Помимо выразительных возможностей и допустимого количества правил, качество межсетевого экрана определяется еще двумя очень важными характеристиками – простотой использования и собственной защищенностью. В плане простоты использования первостепенное значение имеют наглядный интерфейс при определении правил фильтрации и возможность централизованного администрирования составных конфигураций. В свою очередь, в последнем аспекте хотелось бы выделить средства централизованной загрузки правил фильтрации и проверки набора правил на непротиворечивость. Важен и централизованный сбор и анализ регистрационной информации, а также получение сигналов о попытках выполнения действий, запрещенных политикой безопасности.

Собственная защищенность межсетевого экрана обеспечивается теми же средствами, что и защищенность универсальных систем. Имеется в виду физическая защита, идентификация и аутентификация, разграничение доступа, контроль целостности, протоколирование и аудит. При выполнении централизованного администрирования следует также позаботиться о защите информации от пассивного и активного прослушивания сети, то есть обеспечить ее (информации) целостность и конфиденциальность. Крайне важно оперативное наложение заплат, ликвидирующих выявленные уязвимые места МЭ.

Хотелось бы подчеркнуть, что природа экранирования как сервиса безопасности очень глубока. Помимо блокирования потоков данных, нарушающих политику безопасности, межсетевой экран может скрывать информацию о защищаемой сети, тем самым затрудняя действия потенциальных злоумышленников. Мощным методом сокрытия информации является трансляция "внутренних" сетевых адресов, которая попутно решает проблему расширения адресного пространства, выделенного организации.

Отметим также следующие дополнительные возможности межсетевых экранов:

- контроль информационного наполнения (антивирусный контроль "на лету", верификация Java-апплетов, выявление ключевых слов в электронных сообщениях и т.п.);
- выполнение функций ПО промежуточного слоя.

Особенно важным представляется последний из перечисленных аспектов. ПО промежуточного слоя, как и традиционные межсетевые экраны прикладного уровня, скрывает информацию о предоставляемых услугах. За счет этого оно может выполнять такие функции, как маршрутизация запросов и балансировка нагрузки. Представляется вполне естественным, чтобы эти возможности были реализованы в рамках межсетевого экрана. Это существенно упрощает действия по обеспечению высокой доступности экспортируемых сервисов и позволяет осуществлять переключение на резервные мощности прозрачным для внешних пользователей образом. В результате к услугам, традиционно предоставляемым межсетевыми экранами, добавляется поддержка высокой доступности сетевых сервисов.

Пример современного межсетевого экрана представлен в статье "Z-2 – универсальный межсетевой экран высшего уровня защиты" (Jet Info, 2002, 5).

Анализ защищенности

Сервис анализа защищенности предназначен для выявления уязвимых мест с целью их оперативной ликвидации. Сам по себе этот сервис ни от чего не защищает, но помогает обнаружить (и устранить) пробелы в защите раньше, чем их сможет использовать злоумышленник. В первую оче-

редь, имеются в виду не архитектурные (их ликвидировать сложно), а "оперативные" бреши, появившиеся в результате ошибок администрирования или из-за невнимания к обновлению версий программного обеспечения.

Системы анализа защищенности (называемые также сканерами защищенности), как и рассмотренные выше средства активного аудита, основаны на накоплении и использовании знаний. В данном случае имеются в виду знания о пробелах в защите: о том, как их искать, насколько они серьезны и как их устранять.

Соответственно, ядром таких систем является база уязвимых мест, которая определяет доступный диапазон возможностей и требует практически постоянной актуализации.

В принципе, могут выявляться бреши самой разной природы: наличие вредоносного ПО (в частности, вирусов), слабые пароли пользователей, неудачно сконфигурированные операционные системы, небезопасные сетевые сервисы, неустановленные заплаты, уязвимости в приложениях и т.д. Однако наиболее эффективными являются сетевые сканеры (очевидно, в силу доминирования семейства протоколов TCP/IP), а также антивирусные средства. Антивирусную защиту мы причисляем к средствам анализа защищенности, не считая ее отдельным сервисом безопасности.

Сканеры могут выявлять уязвимые места как путем пассивного анализа, то есть изучения конфигурационных файлов, задействованных портов и т.п., так и путем имитации действий атакующего. Некоторые найденные уязвимые места могут устраняться автоматически (например, лечение зараженных файлов), о других сообщается администратору.

Системы анализа защищенности снабжены традиционным "технологическим сахаром": автообнаружением компонентов анализируемой ИС и графическим интерфейсом (помогающим, в частности, эффективно работать с протоколом сканирования).

С возможностями свободно распространяемого сканера Nessus можно ознакомиться, прочитав статью "Сканер защищенности Nessus: уникальное предложение на российском рынке" (Jet Info, 2000, 10).

Контроль, обеспечиваемый системами анализа защищенности, носит реактивный, запаздывающий характер, он не защищает от новых атак, однако следует помнить, что оборона должна быть эшелонированной, и в качестве одного из рубежей контроль защищенности вполне адекватен. Отметим также, что подавляющее большинство атак носит рутинный характер; они возможны только потому, что известные бреши в защите годами остаются неустраненными.

Вариант 1

1. Экран выполняет функции:

- ☐ разграничения доступа
- ☐ облегчения доступа
- ☐ усложнения доступа

2. На межсетевой экран целесообразно возложить функции:

- ☐ активного аудита
- ☐ анализа защищенности
- ☐ идентификации/аутентификации удаленных пользователей

3. Экранирование на сетевом уровне может обеспечить:

- ☐ разграничение доступа по сетевым адресам
- ☐ выборочное выполнение команд прикладного протокола
- ☐ контроль объема данных, переданных по TCP-соединению

Вариант 2

1. Экран выполняет функции:

- ☐ ускорения обмена информацией
- ☐ протоколирования обмена информацией
- ☐ замедления обмена информацией

2. Демилитаризованная зона располагается:

- ☐ перед внешним межсетевым экраном
- ☐ между межсетевыми экранами
- ☐ за внутренним межсетевым экраном

3. Экранирование на сетевом и транспортном уровнях может обеспечить:

- ☐ разграничение доступа по сетевым адресам
- ☐ выборочное выполнение команд прикладного протокола
- ☐ контроль объема данных, переданных по TCP-соединению

Вариант 3

1. Экран выполняет функции:

- ☐ очистки некоторых элементов передаваемых данных
- ☐ пополнения некоторых элементов передаваемых данных
- ☐ преобразования некоторых элементов передаваемых данных

2. К межсетевым экранам целесообразно применять следующие принципы архитектурной безопасности:

- ☐ усиление самого слабого звена
- ☐ эшелонированность обороны
- ☐ невозможность перехода в небезопасное состояние

3. Комплексное экранирование может обеспечить:

- ☐ разграничение доступа по сетевым адресам
- ☐ выборочное выполнение команд прикладного протокола
- ☐ контроль объема данных, переданных по TCP-соединению

Лекция 13. Обеспечение высокой доступности

Рассматриваются два вида средств поддержания высокой доступности: обеспечение отказоустойчивости (нейтрализация отказов, живучесть) и обеспечение безопасного и быстрого восстановления после отказов (обслуживаемость).

Ключевые слова: высокая доступность, информационный сервис, эффективность сервиса, время недоступности, отказоустойчивые системы, отказ, интенсивность отказов, среднее время наработки на отказ, слабое звено, показатель эффективности, избыточность, готовность, коэффициент готовности, структуризация, архитектурная безопасность, безотказность, пассивная безопасность, отказоустойчивость, нейтрализация отказов, живучесть, обслуживаемость, безопасное восстановление, полнота, систематичность, карта ИС, зона поражения, зона риска, зона нейтрализации, одиночная точка отказа, резервирование, локальные меры, распределенные меры, тиражирование, симметричное тиражирование, асимметричное тиражирование, синхронное тиражирование, асинхронное тиражирование, тиражирование внутренними средствами, тиражирование внешними средствами, "горячий" резерв, "теплый" резерв, программное обеспечение промежуточного слоя (ПО ПС), маршрутизация запросов, балансировка загрузки, тиражирование прикладных данных, отслеживание состояния приложений, переконфигурирование, наращивание, унификация, модульность, автоматическое обнаружение отказов, динамическое переконфигурирование, замена в горячем режиме, изоляция отказавших компонентов, сохранение работоспособности сервисов, (обслуживаемость пользователей).

Доступность

Основные понятия

Информационная система предоставляет своим пользователям определенный набор услуг (сервисов). Говорят, что обеспечен нужный уровень доступности этих сервисов, если следующие показатели находятся в заданных пределах:

Эффективность услуг. Эффективность услуги определяется в терминах максимального времени обслуживания запроса, количества под-

держиваемых пользователей и т.п. Требуется, чтобы эффективность не опускалась ниже заранее установленного порога.

Время недоступности. Если эффективность информационной услуги не удовлетворяет наложенным ограничениям, услуга считается недоступной. Требуется, чтобы максимальная продолжительность периода недоступности и суммарное время недоступности за некоторой период (месяц, год) не превышали заранее заданных пределов.

В сущности, требуется, чтобы информационная система почти всегда работала с нужной эффективностью. Для некоторых критически важных систем (например, систем управления) время недоступности должно быть нулевым, без всяких "почти". В таком случае говорят о вероятности возникновения ситуации недоступности и требуют, чтобы эта вероятность не превышала заданной величины. Для решения данной задачи создавались и создаются специальные отказоустойчивые системы, стоимость которых, как правило, весьма высока.

К подавляющему большинству коммерческих систем предъявляются менее жесткие требования, однако современная деловая жизнь и здесь накладывает достаточно суровые ограничения, когда число обслуживаемых пользователей может измеряться тысячами, время ответа не должно превышать нескольких секунд, а время недоступности – нескольких часов в год.

Задачу обеспечения высокой доступности необходимо решать для современных конфигураций, построенных в технологии клиент/сервер. Это означает, что в защите нуждается вся цепочка – от пользователей (возможно, удаленных) до критически важных серверов (в том числе серверов безопасности).

Основные угрозы доступности были рассмотрены нами ранее.

В соответствии с ГОСТ 27.002, под отказом понимается событие, которое заключается в нарушении работоспособности изделия. В контексте данной работы изделие – это информационная система или ее компонент.

В простейшем случае можно считать, что отказы любого компонента составного изделия ведут к общему отказу, а распределение отказов во времени представляет собой простой пуассоновский поток событий. В таком случае вводят понятие интенсивности отказов и среднего времени наработки на отказ, которые связаны между собой соотношением

$$T_i = \frac{1}{\lambda_i}$$

где i – номер компонента, λ_i– интенсивность отказов, T_i – среднее время наработки на отказ.

Интенсивности отказов независимых компонентов складываются:

$\lambda = \lambda_1 + \ldots + \lambda_n$

а среднее время наработки на отказ для составного изделия задается соотношением

$$T = \frac{1}{\lambda}$$

Уже эти простейшие выкладки показывают, что если существует компонент, интенсивность отказов которого много больше, чем у остальных, то именно он определяет среднее время наработки на отказ всей информационной системы. Это является теоретическим обоснованием принципа первоочередного укрепления самого слабого звена.

Пуассоновская модель позволяет обосновать еще одно очень важное положение, состоящее в том, что эмпирический подход к построению систем высокой доступности не может быть реализован за приемлемое время. При традиционном цикле тестирования/отладки программной системы по оптимистическим оценкам каждое исправление ошибки приводит к экспоненциальному убыванию (примерно на половину десятичного порядка) интенсивности отказов. Отсюда следует, что для того, чтобы на опыте убедиться в достижении необходимого уровня доступности, независимо от применяемой технологии тестирования и отладки, придется потратить время, практически равное среднему времени наработки на отказ. Например, для достижения среднего времени наработки на отказ 10^5 часов потребуется более $10^{4.5}$ часов, что составляет более трех лет. Значит, нужны иные методы построения систем высокой доступности, методы, эффективность которых доказана аналитически или практически за более чем пятьдесят лет развития вычислительной техники и программирования.

Пуассоновская модель применима в тех случаях, когда информационная система содержит одиночные точки отказа, то есть компоненты, выход которых из строя ведет к отказу всей системы. Для исследования систем с резервированием применяется иной формализм.

В соответствии с постановкой задачи будем считать, что существует количественная мера эффективности предоставляемых изделием информационных услуг. В таком случае вводятся понятия показателей эффективности отдельных элементов и эффективности функционирования всей сложной системы.

В качестве меры доступности можно принять вероятность приемлемости эффективности услуг, предоставляемых информационной системой, на всем протяжении рассматриваемого отрезка времени. Чем большим запасом эффективности располагает система, тем выше ее доступность.

При наличии избыточности в конфигурации системы вероятность того, что в рассматриваемый промежуток времени эффективность информационных сервисов не опустится ниже допустимого предела, зависит не толь-

ко от вероятности отказа компонентов, но и от времени, в течение которого они остаются неработоспособными, поскольку при этом суммарная эффективность падает, и каждый следующий отказ может стать фатальным. Чтобы максимально увеличить доступность системы, необходимо минимизировать время неработоспособности каждого компонента. Кроме того, следует учитывать, что, вообще говоря, ремонтные работы могут потребовать понижения эффективности или даже временного отключения работоспособных компонентов; такого рода влияние также необходимо минимизировать.

Несколько терминологических замечаний. Обычно в литературе по теории надежности вместо доступности говорят о готовности (в том числе о высокой готовности). Мы предпочли термин "доступность", чтобы подчеркнуть, что информационный сервис должен быть не просто "готов" сам по себе, но доступен для своих пользователей в условиях, когда ситуации недоступности могут вызываться причинами, на первый взгляд не имеющими прямого отношения к сервису (пример – отсутствие консультационного обслуживания).

Далее, вместо времени недоступности обычно говорят о коэффициенте готовности. Нам хотелось обратить внимание на два показателя – длительность однократного простоя и суммарную продолжительность простоев, поэтому мы предпочли термин "время недоступности" как более емкий.

Основы мер обеспечения высокой доступности

Основой мер повышения доступности является применение структурированного подхода, нашедшего воплощение в объектно-ориентированной методологии. Структуризация необходима по отношению ко всем аспектам и составным частям информационной системы – от архитектуры до административных баз данных, на всех этапах ее жизненного цикла – от инициации до выведения из эксплуатации. Структуризация, важная сама по себе, является одновременно необходимым условием практической реализуемости прочих мер повышения доступности. Только маленькие системы можно строить и эксплуатировать как угодно. У больших систем свои законы, которые, как мы уже указывали, программисты впервые осознали более 30 лет назад.

При разработке мер обеспечения высокой доступности информационных сервисов рекомендуется руководствоваться следующими архитектурными принципами, рассматривавшимися ранее:

- апробированность всех процессов и составных частей информационной системы;
- унификация процессов и составных частей;
- управляемость процессов, контроль состояния частей;
- автоматизация процессов;

- модульность архитектуры;
- ориентация на простоту решений.

Доступность системы в общем случае достигается за счет применения трех групп мер, направленных на повышение:

- безотказности (под этим понимается минимизация вероятности возникновения какого-либо отказа; это элемент пассивной безопасности, который дальше рассматриваться не будет);
- отказоустойчивости (способности к нейтрализации отказов, "живучести", то есть способности сохранять требуемую эффективность, несмотря на отказы отдельных компонентов);
- обслуживаемости (под обслуживаемостью понимается минимизация времени простоя отказавших компонентов, а также отрицательного влияния ремонтных работ на эффективность информационных сервисов, то есть быстрое и безопасное восстановление после отказов).

Главное при разработке и реализации мер обеспечения высокой доступности – полнота и систематичность. В этой связи представляется целесообразным составить (и поддерживать в актуальном состоянии) карту информационной системы организации (на что мы уже обращали внимание), в которой фигурировали бы все объекты ИС, их состояние, связи между ними, процессы, ассоциируемые с объектами и связями. С помощью подобной карты удобно формулировать намечаемые меры, контролировать их исполнение, анализировать состояние ИС.

Отказоустойчивость и зона риска

Информационную систему можно представить в виде графа сервисов, ребра в котором соответствуют отношению "сервис А непосредственно использует сервис В".

Пусть в результате осуществления некоторой атаки (источником которой может быть как человек, так и явление природы) выводится из строя подмножество сервисов S_1 (то есть эти сервисы в результате нанесенных повреждений становятся неработоспособными). Назовем S_1 зоной поражения.

В зону риска S мы будем включать все сервисы, эффективность которых при осуществлении атаки падает ниже допустимого предела. Очевидно, S_1 – подмножество S. S строго включает S_1, когда имеются сервисы, непосредственно не затронутые атакой, но критически зависящие от пораженных, то есть неспособные переключиться на использование эквивалентных услуг либо в силу отсутствия таковых, либо в силу невозможности доступа к ним. Например, зона поражения может сводиться к одному порту концентратора, обслуживающему критичный сервер, а зона риска охватывает все рабочие места пользователей сервера.

Чтобы система не содержала одиночных точек отказа, то есть оставалась "живучей" при реализации любой из рассматриваемых угроз, ни одна зона риска не должна включать в себя предоставляемые услуги. Нейтрализацию отказов нужно выполнять внутри системы, незаметно для пользователей, за счет размещения достаточного количества избыточных ресурсов.

С другой стороны, естественно соизмерять усилия по обеспечению "живучести" с рассматриваемыми угрозами. Когда рассматривается набор угроз, соответствующие им зоны поражения могут оказаться вложенными, так что "живучесть" по отношению к более серьезной угрозе автоматически влечет за собой и "живучесть" в более легких случаях. Следует учитывать, однако, что обычно стоимость переключения на резервные ресурсы растет вместе с увеличением объема этих ресурсов. Значит, для наиболее вероятных угроз целесообразно минимизировать зону риска, даже если предусмотрена нейтрализация объемлющей угрозы. Нет смысла переключаться на резервный вычислительный центр только потому, что у одного из серверов вышел из строя блок питания.

Зону риска можно трактовать не только как совокупность ресурсов, но и как часть пространства, затрагиваемую при реализации угрозы. В таком случае, как правило, чем больше расстояние дублирующего ресурса от границ зоны риска, тем выше стоимость его поддержания, поскольку увеличивается протяженность линий связи, время переброски персонала и т.п. Это еще один довод в пользу адекватного противодействия угрозам, который следует принимать во внимание при размещении избыточных ресурсов и, в частности, при организации резервных центров.

Введем еще одно понятие. Назовем зоной нейтрализации угрозы совокупность ресурсов, вовлеченных в нейтрализацию отказа, возникшего вследствие реализации угрозы. Имеются в виду ресурсы, режим работы которых в случае отказа изменяется. Очевидно, зона риска является подмножеством зоны нейтрализации. Чем меньше разность между ними, тем экономичнее данный механизм нейтрализации.

Все, что находится вне зоны нейтрализации, отказа "не чувствует" и может трактовать внутренность этой зоны как безотказную. Таким образом, в иерархически организованной системе грань между "живучестью" и обслуживаемостью, с одной стороны, и безотказностью, с другой стороны, относительна. Целесообразно конструировать целостную информационную систему из компонентов, которые на верхнем уровне можно считать безотказными, а вопросы "живучести" и обслуживаемости решать в пределах каждого компонента.

Обеспечение отказоустойчивости

Основным средством повышения "живучести" является внесение избыточности в конфигурацию аппаратных и программных средств, поддер-

живающей инфраструктуры и персонала, резервирование технических средств и тиражирование информационных ресурсов (программ и данных).

Меры по обеспечению отказоустойчивости можно разделить на локальные и распределенные. Локальные меры направлены на достижение "живучести" отдельных компьютерных систем или их аппаратных и программных компонентов (в первую очередь с целью нейтрализации внутренних отказов ИС). Типичные примеры подобных мер – использование кластерных конфигураций в качестве платформы критичных серверов или "горячее" резервирование активного сетевого оборудования с автоматическим переключением на резерв.

Если в число рассматриваемых рисков входят серьезные аварии поддерживающей инфраструктуры, приводящие к выходу из строя производственной площадки организации, следует предусмотреть распределенные меры обеспечения живучести, такие как создание или аренда резервного вычислительного центра. При этом, помимо дублирования и/или тиражирования ресурсов, необходимо предусмотреть средства автоматического или быстрого ручного переконфигурирования компонентов ИС, чтобы обеспечить переключение с основной площадки на резервную.

Аппаратура – относительно статичная составляющая, однако было бы ошибкой полностью отказывать ей в динамичности. В большинстве организаций информационные системы находятся в постоянном развитии, поэтому на протяжении всего жизненного цикла ИС следует соотносить все изменения с необходимостью обеспечения "живучести", не забывать "тиражировать" новые и модифицированные компоненты.

Программы и данные более динамичны, чем аппаратура, и резервироваться они могут постоянно, при каждом изменении, после завершения некоторой логически замкнутой группы изменений или по истечении определенного времени.

Резервирование программ и данных может выполняться многими способами – за счет зеркалирования дисков, резервного копирования и восстановления, репликации баз данных и т.п. Будем использовать для всех перечисленных способов термин "тиражирование".

Выделим следующие классы тиражирования:

Симметричное/асимметричное. Тиражирование называется симметричным, если все серверы, предоставляющие данный сервис, могут изменять принадлежащую им информацию и передавать изменения другим серверам. В противном случае тиражирование называется асимметричным.

Синхронное/асинхронное. Тиражирование называется синхронным, если изменение передается всем экземплярам сервиса в рамках одной распределенной транзакции. В противном случае тиражирование называется асинхронным.

Осуществляемое средствами сервиса, хранящего информацию/внешними средствами.

Рассмотрим, какие способы тиражирования предпочтительнее.

Безусловно, следует предпочесть стандартные средства тиражирования, встроенные в сервис.

Асимметричное тиражирование теоретически проще симметричного, поэтому целесообразно выбрать асимметрию.

Труднее всего выбрать между синхронным и асинхронным тиражированием. Синхронное идейно проще, но его реализация может быть тяжеловесной и сложной, хотя это внутренняя сложность сервиса, невидимая для приложений. Асинхронное тиражирование устойчивее к отказам в сети, оно меньше влияет на работу основного сервиса.

Чем надежнее связь между серверами, вовлеченными в процесс тиражирования, чем меньше время, отводимое на переключение с основного сервера на резервный, чем жестче требования к актуальности информации, тем более предпочтительным оказывается синхронное тиражирование.

С другой стороны, недостатки асинхронного тиражирования могут компенсироваться процедурными и программными мерами, направленными на контроль целостности информации в распределенной ИС. Сервисы, входящие в состав ИС, в состоянии обеспечить ведение и хранение журналов транзакций, с помощью которых можно выявлять операции, утерянные при переключении на резервный сервер. Даже в условиях неустойчивой связи с удаленными филиалами организации подобная проверка в фоновом режиме займет не более нескольких часов, поэтому асинхронное тиражирование может использоваться практически в любой ИС.

Асинхронное тиражирование может производиться на сервер, работающий в режиме "горячего" резерва, возможно, даже обслуживающего часть пользовательских запросов, или на сервер, работающий в режиме "теплого" резерва, когда изменения периодически "накатываются", но сам резервный сервер запросов не обслуживает.

Достоинство "теплого" резервирования в том, что его можно реализовать, оказывая меньшее влияние на основной сервер. Это влияние вообще может быть сведено к нулю, если асинхронное тиражирование осуществляется путем передачи инкрементальных копий с основного сервера (резервное копирование необходимо выполнять в любом случае).

Основной недостаток "теплого" резерва состоит в длительном времени включения, что может быть неприемлемо для "тяжелых" серверов, таких как кластерная конфигурация сервера СУБД. Здесь необходимо проводить измерения в условиях, близких к реальным.

Второй недостаток "теплого" резерва вытекает из опасности малых изменений. Может оказаться, что в самый нужный момент срочный перевод резерва в штатный режим невозможен.

Учитывая приведенные соображения, следует в первую очередь рассматривать возможность "горячего" резервирования, либо тщательно контролировать использование "теплого" резерва и регулярно (не реже одного раза в неделю) проводить пробные переключения резерва в "горячий" режим.

Программное обеспечение промежуточного слоя

С помощью программного обеспечения промежуточного слоя (ПО ПС) можно для произвольных прикладных сервисов добиться высокой "живучести" с полностью прозрачным для пользователей переключением на резервные мощности.

О возможностях и свойствах ПО промежуточного слоя можно прочитать в статье Ф. Бернстайна "Middleware: модель сервисов распределенной системы" (Jet Info, 1997, 11).

Перечислим основные достоинства ПО ПС, существенные для обеспечения высокой доступности.

- ПО ПС уменьшает сложность создания распределенных систем. Подобное ПО берет на себя часть функций, которые в локальном случае выполняют операционные системы;
- ПО ПС берет на себя маршрутизацию запросов, позволяя тем самым обеспечить "живучесть" прозрачным для пользователей образом;
- ПО ПС осуществляет балансировку загрузки вычислительных мощностей, что также способствует повышению доступности данных;
- ПО ПС в состоянии осуществлять тиражирование любой информации, а не только содержимого баз данных. Следовательно, любое приложение можно сделать устойчивым к отказам серверов;
- ПО ПС в состоянии отслеживать состояние приложений и при необходимости тиражировать и перезапускать программы, что гарантирует "живучесть" программных систем;
- ПО ПС дает возможность прозрачным для пользователей образом выполнять переконфигурирование (и, в частности, наращивание) серверных компонентов, что позволяет масштабировать систему, сохраняя инвестиции в прикладные системы. Стабильность прикладных систем – важный фактор повышения доступности данных.

Ранее мы упоминали о достоинствах использования ПО ПС в рамках межсетевых экранов, которые в таком случае становятся элементом обеспечения отказоустойчивости предоставляемых информационных сервисов.

Обеспечение обслуживаемости

Меры по обеспечению обслуживаемости направлены на снижение сроков диагностирования и устранения отказов и их последствий.

Для обеспечения обслуживаемости рекомендуется соблюдать следующие архитектурные принципы:

- ориентация на построение информационной системы из унифицированных компонентов с целью упрощения замены отказавших частей;
- ориентация на решения модульной структуры с возможностью автоматического обнаружения отказов, динамического переконфигурирования аппаратных и программных средств и замены отказавших компонентов в "горячем" режиме.

Динамическое переконфигурирование преследует две основные цели:

- изоляция отказавших компонентов;
- сохранение работоспособности сервисов.

Изолированные компоненты образуют зону поражения реализованной угрозы. Чем меньше соответствующая зона риска, тем выше обслуживаемость сервисов. Так, при отказах блоков питания, вентиляторов и/или дисков в современных серверах зона риска ограничивается отказавшим компонентом; при отказах процессорных модулей весь сервер может потребовать перезагрузки (что способно вызвать дальнейшее расширение зоны риска). Очевидно, в идеальном случае зоны поражения и риска совпадают, и современные серверы и активное сетевое оборудование, а также программное обеспечение ведущих производителей весьма близки к этому идеалу.

Возможность программирования реакции на отказ также повышает обслуживаемость систем. Каждая организация может выбрать свою стратегию реагирования на отказы тех или иных аппаратных и программных компонентов и автоматизировать эту реакцию. Так, в простейшем случае возможна отправка сообщения системному администратору, чтобы ускорить начало ремонтных работ; в более сложном случае может быть реализована процедура "мягкого" выключения (переключения) сервиса, чтобы упростить обслуживание.

Возможность удаленного выполнения административных действий – важное направление повышения обслуживаемости, поскольку при этом ускоряется начало восстановительных мероприятий, а в идеале все работы (обычно связанные с обслуживанием программных компонентов) выполняются в удаленном режиме, без перемещения квалифицированного персонала, то есть с высоким качеством и в кратчайшие сроки. Для современных систем возможность удаленного администрирования – стандартное свойство, но важно позаботиться о его практической реализуемости в условиях разнородности конфигураций (в первую очередь

клиентских). Централизованное распространение и конфигурирование программного обеспечения, управление компонентами информационной системы и диагностирование – надежный фундамент технических мер повышения обслуживаемости.

Существенный аспект повышения обслуживаемости – организация консультационной службы для пользователей (обслуживаемость пользователей), внедрение программных систем для работы этой службы, обеспечение достаточной пропускной способности каналов связи с пользователями, в том числе в режиме пиковых нагрузок.

Вариант 1

1. Информационный сервис считается недоступным, если:

- ☐ его эффективность не удовлетворяет наложенным ограничениям
- ☐ подписка на него стоит слишком дорого
- ☐ не удается найти подходящий сервис

2. Среднее время наработки на отказ:

- ☐ пропорционально интенсивности отказов
- ☐ обратно пропорционально интенсивности отказов
- ☐ не зависит от интенсивности отказов

3. Достоинствами синхронного тиражирования являются:

- ☐ идейная простота
- ☐ простота реализации
- ☐ устойчивость к отказам сети

Вариант 2

1. Эффективность информационного сервиса может измеряться как:

- ☐ рентабельность работы сервиса
- ☐ максимальное время обслуживания запроса
- ☐ количество одновременно обслуживаемых пользователей

2. Интенсивности отказов независимых компонентов:

- ☐ складываются
- ☐ умножаются
- ☐ возводятся в квадрат и складываются

3. Достоинствами асинхронного тиражирования являются:

- ☐ идейная простота
- ☐ простота реализации
- ☐ устойчивость к отказам сети

Вариант 3

1. Обеспечение высокой доступности можно ограничить:

- ☐ критически важными серверами
- ☐ сетевым оборудованием
- ☐ всей цепочкой от пользователей до серверов

2. В число основных угроз доступности входят:

- ☐ отказ пользователей
- ☐ повышение цен на услуги связи
- ☐ отказ поддерживающей инфраструктуры

3. Основными функциями ПО промежуточного слоя, существенными для обеспечения высокой доступности, являются:

- ☐ маршрутизация запросов
- ☐ балансировка загрузки
- ☐ доступность свободно распространяемых реализаций

Лекция 14. Туннелирование и управление

Рассматриваются два сервиса безопасности очень разного масштаба — туннелирование и управление.

Ключевые слова: туннелирование, туннель, конвертование, обертывание, конфиденциальность, конфиденциальность трафика, виртуальные частные сети, межсетевой экран, криптография, инфраструктурный сервис, интегрирующая оболочка, мониторинг, контроль, координация, управление конфигурацией, управление отказами, управление производительностью, управление безопасностью, управление учетной информацией, атрибуты объекта, допустимые операции, извещения, менеджер, агент, управляющая консоль, многоуровневая архитектура, доверенное управление, делегированное управление, модель управляющей информации, пакет, дерево наследования, проактивное управление, упреждающее управление, управление, каркас, безопасность, загрузка, событие, хранение данных, проблемная ситуация, отчет, автообнаружение, менеджер безопасности, разграничение доступа, идентификация/аутентификация, политика безопасности, высокая доступность, резервное копирование, контроль производительности, активный аудит.

Туннелирование

На наш взгляд, туннелирование следует рассматривать как самостоятельный сервис безопасности. Его суть состоит в том, чтобы "упаковать" передаваемую порцию данных, вместе со служебными полями, в новый "конверт". В качестве синонимов термина "туннелирование" могут использоваться "конвертование" и "обертывание".

Туннелирование может применяться для нескольких целей:

- передачи через сеть пакетов, принадлежащих протоколу, который в данной сети не поддерживается (например, передача пакетов IPv6 через старые сети, поддерживающие только IPv4);
- обеспечения слабой формы конфиденциальности (в первую очередь конфиденциальности трафика) за счет сокрытия истинных адресов и другой служебной информации;
- обеспечения конфиденциальности и целостности передаваемых данных при использовании вместе с криптографическими сервисами.

Туннелирование может применяться как на сетевом, так и на прикладном уровнях. Например, стандартизовано туннелирование для IP и двойное конвертование для почты X.400.

На рис. 14.1 показан пример обертывания пакетов IPv6 в формат IPv4.

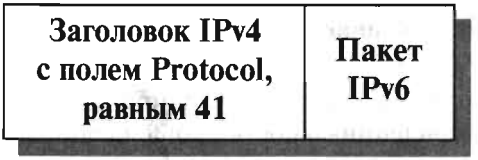

Рис. 14.1. Обертывание пакетов IPv6 в формат IPv4 с целью их туннелирования через сети IPv4.

Комбинация туннелирования и шифрования (наряду с необходимой криптографической инфраструктурой) на выделенных шлюзах и экранирования на маршрутизаторах поставщиков сетевых услуг (для разделения пространств "своих" и "чужих" сетевых адресов в духе виртуальных локальных сетей) позволяет реализовать такое важное в современных условиях защитное средство, как виртуальные частные сети. Подобные сети, наложенные обычно поверх Internet, существенно дешевле и гораздо безопаснее, чем собственные сети организации, построенные на выделенных каналах. Коммуникации на всем их протяжении физически защитить невозможно, поэтому лучше изначально исходить из предположения об их уязвимости и соответственно обеспечивать защиту. Современные протоколы, направленные на поддержку классов обслуживания, помогут гарантировать для виртуальных частных сетей заданную пропускную способность, величину задержек и т.п., ликвидируя тем самым единственное на сегодня реальное преимущество сетей собственных.

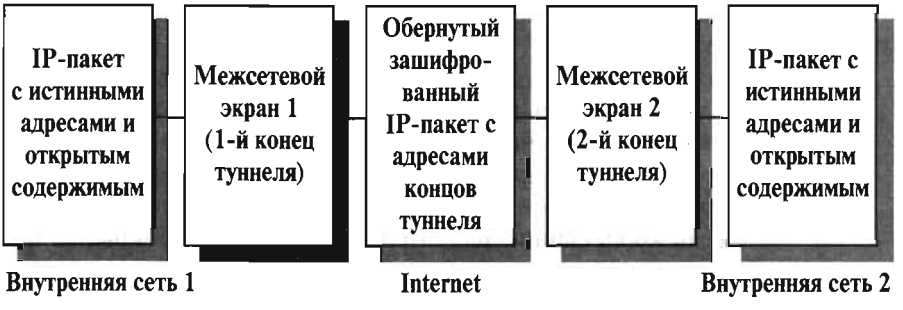

Рис. 14.2. Межсетевые экраны как точки реализации сервиса виртуальных частных сетей.

Концами туннелей, реализующих виртуальные частные сети, целесообразно сделать межсетевые экраны, обслуживающие подключение организаций к внешним сетям (см. рис. 14.2). В таком случае туннелирование и шифрование станут дополнительными преобразованиями, выполняемыми в процессе фильтрации сетевого трафика наряду с трансляцией адресов.

Концами туннелей, помимо корпоративных межсетевых экранов, могут быть мобильные компьютеры сотрудников (точнее, их персональные МЭ).

Управление

Основные понятия

Управление можно отнести к числу инфраструктурных сервисов, обеспечивающих нормальную работу компонентов и средств безопасности. Сложность современных систем такова, что без правильно организованного управления они постепенно деградируют как в плане эффективности, так и в плане защищенности.

Возможен и другой взгляд на управление – как на интегрирующую оболочку информационных сервисов и сервисов безопасности (в том числе средств обеспечения высокой доступности), обеспечивающую их нормальное, согласованное функционирование под контролем администратора ИС.

Согласно стандарту X.700, управление подразделяется на:

- мониторинг компонентов;
- контроль (то есть выдачу и реализацию управляющих воздействий);
- координацию работы компонентов системы.

Системы управления должны:

- позволять администраторам планировать, организовывать, контролировать и учитывать использование информационных сервисов;
- давать возможность отвечать на изменение требований;
- обеспечивать предсказуемое поведение информационных сервисов;
- обеспечивать защиту информации.

Иными словами, управление должно обладать достаточно богатой функциональностью, быть результативным, гибким и информационно безопасным.

В X.700 выделяется пять функциональных областей управления:

- управление конфигурацией (установка параметров для нормального функционирования, запуск и остановка компонен-

тов, сбор информации о текущем состоянии системы, прием извещений о существенных изменениях в условиях функционирования, изменение конфигурации системы);

- управление отказами (выявление отказов, их изоляция и восстановление работоспособности системы);
- управление производительностью (сбор и анализ статистической информации, определение производительности системы в штатных и нештатных условиях, изменение режима работы системы);
- управление безопасностью (реализация политики безопасности путем создания, удаления и изменения сервисов и механизмов безопасности, распространения соответствующей информации и реагирования на инциденты);
- управление учетной информацией (т.е. взимание платы за пользование ресурсами).

В стандартах семейства X.700 описывается модель управления, способная обеспечить достижение поставленных целей. Вводится понятие управляемого объекта как совокупности характеристик компонента системы, важных с точки зрения управления. К таким характеристикам относятся:

- атрибуты объекта;
- допустимые операции;
- извещения, которые объект может генерировать;
- связи с другими управляемыми объектами.

Согласно рекомендациям X.701, системы управления распределенными ИС строятся в архитектуре менеджер/агент. Агент (как программная модель управляемого объекта) выполняет управляющие действия и порождает (при возникновении определенных событий) извещения от его имени. В свою очередь, менеджер выдает агентам команды на управляющие воздействия и получает извещения.

Иерархия взаимодействующих менеджеров и агентов может иметь несколько уровней. При этом элементы промежуточных уровней играют двоякую роль: по отношению к вышестоящим элементам они являются агентами, а к нижестоящим – менеджерами. Многоуровневая архитектура менеджер/агент – ключ к распределенному, масштабируемому управлению большими системами.

Логически связанной с многоуровневой архитектурой является концепция доверенного (или делегированного) управления. При доверенном управлении менеджер промежуточного уровня может управлять объектами, использующими собственные протоколы, в то время как "наверху" опираются исключительно на стандартные средства.

Обязательным элементом при любом числе архитектурных уровней является управляющая консоль.

С точки зрения изучения возможностей систем управления следует учитывать разделение, введенное в X.701. Управление подразделяется на следующие аспекты:

- информационный (атрибуты, операции и извещения управляемых объектов);
- функциональный (управляющие действия и необходимая для них информация);
- коммуникационный (обмен управляющей информацией);
- организационный (разбиение на области управления).

Ключевую роль играет модель управляющей информации. Она описывается рекомендациями X.720. Модель является объектно-ориентированной с поддержкой инкапсуляции и наследования. Дополнительно вводится понятие пакета как совокупности атрибутов, операций, извещений и соответствующего поведения.

Класс объектов определяется позицией в дереве наследования, набором включенных пакетов и внешним интерфейсом, то есть видимыми снаружи атрибутами, операциями, извещениями и демонстрируемым поведением.

К числу концептуально важных можно отнести понятие "проактивного", то есть упреждающего управления. Упреждающее управление основано на предсказании поведения системы на основе текущих данных и ранее накопленной информации. Простейший пример подобного управления – выдача сигнала о возможных проблемах с диском после серии программно-нейтрализуемых ошибок чтения/записи. В более сложном случае определенный характер рабочей нагрузки и действий пользователей может предшествовать резкому замедлению работы системы; адекватным управляющим воздействием могло бы стать понижение приоритетов некоторых заданий и извещение администратора о приближении кризиса.

Возможности типичных систем

Развитые системы управления имеют, если можно так выразиться, двухмерную настраиваемость – на нужды конкретных организаций и на изменения в информационных технологиях. Системы управления живут (по крайней мере, должны жить) долго. За это время в различных предметных областях администрирования (например, в области резервного копирования) наверняка появятся решения, превосходящие изначально заложенные в управляющий комплект. Последний должен уметь эволюционировать, причем разные его компоненты могут делать это с разной скоростью. Никакая жесткая, монолитная система такого не выдержит.

Единственный выход – наличие каркаса, с которого можно снимать старое и "навешивать" новое, не теряя эффективности управления.

Каркас как самостоятельный продукт необходим для достижения по крайней мере следующих целей:

- сглаживание разнородности управляемых информационных систем, предоставление унифицированных программных интерфейсов для быстрой разработки управляющих приложений;
- создание инфраструктуры управления, обеспечивающей наличие таких свойств, как поддержка распределенных конфигураций, масштабируемость, информационная безопасность и т.д.;
- предоставление функционально полезных универсальных сервисов, таких как планирование заданий, генерация отчетов и т.п.

Вопрос о том, что, помимо каркаса, должно входить в систему управления, является достаточно сложным Во-первых, многие системы управления имеют мэйнфреймовое прошлое и попросту унаследовали некоторую функциональность, которая перестала быть необходимой. Во-вторых, для ряда функциональных задач появились отдельные, высококачественные решения, превосходящие аналогичные по назначению "штатные" компоненты. Видимо, с развитием объектного подхода, многоплатформенности важнейших сервисов и их взаимной совместимости, системы управления действительно превратятся в каркас. Пока же на их долю остается достаточно важных областей, а именно:

- управление безопасностью;
- управление загрузкой;
- управление событиями;
- управление хранением данных;
- управление проблемными ситуациями;
- генерация отчетов.

На уровне инфраструктуры присутствует решение еще одной важнейшей функциональной задачи – обеспечение автоматического обнаружения управляемых объектов, выявление их характеристик и связей между ними.

Отметим, что управление безопасностью в совокупности с соответствующим программным интерфейсом позволяет реализовать платформно-независимое разграничение доступа к объектам произвольной природы и (что очень важно) вынести функции безопасности из прикладных систем. Чтобы выяснить, разрешен ли доступ текущей политикой, приложению достаточно обратиться к менеджеру безопасности системы управления.

Менеджер безопасности осуществляет идентификацию/аутентификацию пользователей, контроль доступа к ресурсам и протоколирование неудачных попыток доступа. Можно считать, что менеджер безопасности

встраивается в ядро операционных систем контролируемых элементов ИС, перехватывает соответствующие обращения и осуществляет свои проверки перед проверками, выполняемыми ОС, так что он создает еще один защитный рубеж, не отменяя, а дополняя защиту, реализуемую средствами ОС.

Развитые системы управления располагают централизованной базой, в которой хранится информация о контролируемой ИС и, в частности, некоторое представление о политике безопасности. Можно считать, что при каждой попытке доступа выполняется просмотр сохраненных в базе правил, в результате которого выясняется наличие у пользователя необходимых прав. Тем самым для проведения единой политики безопасности в рамках корпоративной информационной системы закладывается прочный технологический фундамент.

Хранение параметров безопасности в базе данных дает администраторам еще одно важное преимущество – возможность выполнения разнообразных запросов. Можно получить список ресурсов, доступных данному пользователю, список пользователей, имеющих доступ к данному ресурсу и т.п.

Одним из элементов обеспечения высокой доступности данных является подсистема автоматического управления хранением данных, выполняющая резервное копирование данных, а также автоматическое отслеживание их перемещения между основными и резервными носителями.

Для обеспечения высокой доступности информационных сервисов используется управление загрузкой, которое можно подразделить на управление прохождением заданий и контроль производительности.

Контроль производительности – понятие многогранное. Сюда входят и оценка быстродействия компьютеров, и анализ пропускной способности сетей, и отслеживание числа одновременно поддерживаемых пользователей, и время реакции, и накопление и анализ статистики использования ресурсов. Обычно в распределенной системе соответствующие данные доступны "в принципе", они поставляются точечными средствами управления, но проблема получения целостной картины, как текущей, так и перспективной, остается весьма сложной. Решить ее способна только система управления корпоративного уровня.

Средства контроля производительности целесообразно разбить на две категории:

- выявление случаев неадекватного функционирования компонентов информационной системы и автоматическое реагирование на эти события;
- анализ тенденций изменения производительности системы и долгосрочное планирование.

Для функционирования обеих категорий средств необходимо выбрать отслеживаемые параметры и допустимые границы для них, выход за которые означает "неадекватность функционирования". После этого задача сводится к выявлению нетипичного поведения компонентов ИС, для чего могут применяться статистические методы.

Управление событиями (точнее, сообщениями о событиях) – это базовый механизм, позволяющий контролировать состояние информационных систем в реальном времени. Системы управления позволяют классифицировать события и назначать для некоторых из них специальные процедуры обработки. Тем самым реализуется важный принцип автоматического реагирования.

Очевидно, что задачи контроля производительности и управления событиями, равно как и методы их решения в системах управления, близки к аналогичным аспектам систем активного аудита. Налицо еще одно свидетельство концептуального единства области знаний под названием "информационная безопасность" и необходимости реализации этого единства на практике.

Вариант 1

1. Туннелирование может использоваться на следующих уровнях эталонной семиуровневой модели:

- ☐ канальном
- ☐ транспортном
- ☐ сеансовом

2. Согласно стандарту X.700, в число функций управления конфигурацией входят:

- ☐ запуск и остановка компонентов
- ☐ выбор закупаемой конфигурации
- ☐ изменение конфигурации системы

3. Каркас необходим системе управления для придания:

- ☐ гибкости
- ☐ жесткости
- ☐ устойчивости

Вариант 2

1. Туннелирование может использоваться на следующих уровнях эталонной семиуровневой модели:

- ☐ сетевом
- ☐ сеансовом
- ☐ уровне представления

2. Согласно стандарту X.700, в число функций управления отказами входят:

- ☐ предупреждение отказов
- ☐ выявление отказов
- ☐ устранение отказов

3. Выявление неадекватного поведения выполняется системами управления путем применения методов, типичных для:

- ☐ систем анализа защищенности
- ☐ систем активного аудита
- ☐ систем идентификации

Вариант 3

1. Туннелирование может использоваться на следующих уровнях эталонной семиуровневой модели:

- ☐ канальном
- ☐ сетевом
- ☐ транспортном

2. Согласно стандарту X.700, в число функций управления безопасностью входят:

- ☐ создание инцидентов
- ☐ реагирование на инциденты
- ☐ устранение инцидентов

3. Архитектурными элементами систем управления являются:

- ☐ агенты
- ☐ клиенты
- ☐ менеджеры

Лекция 15. Заключение

В последней лекции подводится итог курса.

Ключевые слова: информационная безопасность, ИБ, интерес, субъект, информационные отношения, важность, сложность, доступность, целостность, конфиденциальность, уязвимость, активный агент, нарушение, ущерб, рост, затраты, законодательный уровень, административный уровень, процедурный уровень, программно-технический уровень, объектно-ориентированный подход, инкапсуляция, наследование, полиморфизм, грань, уровень детализации, правовой акт, стандарт, координация, лицензирование, сертификация, "Оранжевая книга", "Общие критерии", сервис безопасности, классификация, X.800, сетевые конфигурации, механизм безопасности, функциональные требования, программа безопасности, политика безопасности, анализ рисков, угроза, базовый уровень ИБ, жизненный цикл, превентивные меры, обнаружение, локализация, прослеживание, восстановление, архитектурная безопасность, слабое звено, небезопасное состояние, простота, управляемость, идентификация, аутентификация, управление доступом, разграничение доступа, протоколирование, аудит, активный аудит, криптография, шифрование, контроль целостности, электронная цифровая подпись, экранирование, анализ защищенности, отказоустойчивость, безопасное восстановление, туннелирование, управление.

Что такое информационная безопасность. Основные составляющие информационной безопасности. Важность и сложность проблемы информационной безопасности

Цель мероприятий в области информационной безопасности – защитить интересы субъектов информационных отношений. Интересы эти многообразны, но все они концентрируются вокруг трех основных аспектов:

- доступность;
- целостность;
- конфиденциальность.

Первый шаг при построении системы ИБ организации – ранжирование и детализация этих аспектов.

Важность проблематики ИБ объясняется двумя основными причинами:

- ценностью накопленных информационных ресурсов;
- критической зависимостью от информационных технологий.

Разрушение важной информации, кража конфиденциальных данных, перерыв в работе вследствие отказа – все это выливается в крупные материальные потери, наносит ущерб репутации организации. Проблемы с системами управления или медицинскими системами угрожают здоровью и жизни людей.

Современные информационные системы сложны и, значит, опасны уже сами по себе, даже без учета активности злоумышленников. Постоянно обнаруживаются новые уязвимые места в программном обеспечении. Приходится принимать во внимание чрезвычайно широкий спектр аппаратного и программного обеспечения, многочисленные связи между компонентами.

Меняются принципы построения корпоративных ИС. Используются многочисленные внешние информационные сервисы; предоставляются вовне собственные; получило широкое распространение явление, обозначаемое исконно русским словом "аутсорсинг", когда часть функций корпоративной ИС передается внешним организациям. Развивается программирование с активными агентами.

Подтверждением сложности проблематики ИБ является параллельный (и довольно быстрый) рост затрат на защитные мероприятия и количества нарушений ИБ в сочетании с ростом среднего ущерба от каждого нарушения. (Последнее обстоятельство - еще один довод в пользу важности ИБ.)

Успех в области информационной безопасности может принести только комплексный подход, сочетающий меры четырех уровней:

- законодательного;
- административного;
- процедурного;
- программно-технического.

Проблема ИБ – не только (и не столько) техническая; без законодательной базы, без постоянного внимания руководства организации и выделения необходимых ресурсов, без мер управления персоналом и физической защиты решить ее невозможно. Комплексность также усложняет проблематику ИБ; требуется взаимодействие специалистов из разных областей.

В качестве основного инструмента борьбы со сложностью предлагается объектно-ориентированный подход. Инкапсуляция, наследование, полиморфизм, выделение граней объектов, варьирование уровня детализации – все это универсальные понятия, знание которых необходимо всем специалистам по информационной безопасности.

Законодательный, административный и процедурный уровни

Законодательный уровень является важнейшим для обеспечения информационной безопасности. Необходимо всячески подчеркивать важность проблемы ИБ; сконцентрировать ресурсы на важнейших направлениях исследований; скоординировать образовательную деятельность; создать и поддерживать негативное отношение к нарушителям ИБ – все это функции законодательного уровня.

На законодательном уровне особого внимания заслуживают правовые акты и стандарты.

Российские правовые акты в большинстве своем имеют ограничительную направленность. Но то, что для Уголовного или Гражданского кодекса естественно, по отношению к Закону об информации, информатизации и защите информации является принципиальным недостатком. Сами по себе лицензирование и сертификация не обеспечивают безопасности. К тому же в законах не предусмотрена ответственность государственных органов за нарушения ИБ. Реальность такова, что в России в деле обеспечения ИБ на помощь государства рассчитывать не приходится.

На этом фоне поучительным является знакомство с законодательством США в области ИБ, которое гораздо обширнее и многограннее российского.

Среди стандартов выделяются "Оранжевая книга", рекомендации X.800 и "Критерии оценки безопасности информационных технологий".

"Оранжевая книга" заложила понятийный базис; в ней определяются важнейшие сервисы безопасности и предлагается метод классификации информационных систем по требованиям безопасности.

Рекомендации X.800 весьма глубоко трактуют вопросы защиты сетевых конфигураций и предлагают развитый набор сервисов и механизмов безопасности.

Международный стандарт ISO 15408, известный как "Общие критерии", реализует более современный подход, в нем зафиксирован чрезвычайно широкий спектр сервисов безопасности (представленных как функциональные требования). Его принятие в качестве национального стандарта важно не только из абстрактных соображений интеграции в мировое сообщество; оно, как можно надеяться, облегчит жизнь владельцам информационных систем, существенно расширив спектр доступных сертифицированных решений.

Главная задача мер административного уровня – сформировать программу работ в области информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Основой программы является политика безопасности, отражающая подход организации к защите своих информационных активов.

Разработка политики и программы безопасности начинается с анализа рисков, первым этапом которого, в свою очередь, является ознакомление с наиболее распространенными угрозами.

Главные угрозы – внутренняя сложность ИС, непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы.

На втором месте по размеру ущерба стоят кражи и подлоги.

Реальную опасность представляют пожары и другие аварии поддерживающей инфраструктуры.

В общем числе нарушений растет доля внешних атак, но основной ущерб по-прежнему наносят "свои".

Для подавляющего большинства организаций достаточно общего знакомства с рисками; ориентация на типовые, апробированные решения позволит обеспечить базовый уровень безопасности при минимальных интеллектуальных и разумных материальных затратах.

Существенную помощь в разработке политики безопасности может оказать британский стандарт BS 7799:1995, предлагающий типовой каркас.

Разработка программы и политики безопасности может служить примером использования понятия уровня детализации. Они должны подразделяться на несколько уровней, трактующих вопросы разной степени специфичности. Важным элементом программы является разработка и поддержание в актуальном состоянии карты ИС.

Необходимым условием для построения надежной, экономичной защиты является рассмотрение жизненного цикла ИС и синхронизация с ним мер безопасности. Выделяют следующие этапы жизненного цикла:

- инициация;
- закупка;
- установка;
- эксплуатация;
- выведение из эксплуатации.

Безопасность невозможно добавить к системе; ее нужно закладывать с самого начала и поддерживать до конца.

Меры процедурного уровня ориентированы на людей (а не на технические средства) и подразделяются на следующие виды:

- управление персоналом;
- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

На этом уровне применимы важные принципы безопасности:

- непрерывность защиты в пространстве и времени;
- разделение обязанностей;

- минимизация привилегий.

Здесь также применимы объектный подход и понятие жизненного цикла. Первый позволяет разделить контролируемые сущности (территорию, аппаратуру и т.д.) на относительно независимые подобъекты, рассматривая их с разной степенью детализации и контролируя связи между ними.

Понятие жизненного цикла полезно применять не только к информационным системам, но и к сотрудникам. На этапе инициации должно быть разработано описание должности с требованиями к квалификации и выделяемыми компьютерными привилегиями; на этапе установки необходимо провести обучение, в том числе по вопросам безопасности; на этапе выведения из эксплуатации следует действовать аккуратно, не допуская нанесения ущерба обиженными сотрудниками.

Информационная безопасность во многом зависит от аккуратного ведения текущей работы, которая включает:

- поддержку пользователей;
- поддержку программного обеспечения;
- конфигурационное управление;
- резервное копирование;
- управление носителями;
- документирование;
- регламентные работы.

Элементом повседневной деятельности является отслеживание информации в области ИБ; как минимум, администратор безопасности должен подписаться на список рассылки по новым пробелам в защите (и своевременно знакомиться с поступающими сообщениями).

Нужно, однако, заранее готовиться к событиям неординарным, то есть к нарушениям ИБ. Заранее продуманная реакция на нарушения режима безопасности преследует три главные цели:

- локализация инцидента и уменьшение наносимого вреда;
- выявление нарушителя;
- предупреждение повторных нарушений.

Выявление нарушителя – процесс сложный, но первый и третий пункты можно и нужно тщательно продумать и отработать.

В случае серьезных аварий необходимо проведение восстановительных работ. Процесс планирования таких работ можно разделить на следующие этапы:

- выявление критически важных функций организации, установление приоритетов;
- идентификация ресурсов, необходимых для выполнения критически важных функций;
- определение перечня возможных аварий;
- разработка стратегии восстановительных работ;

- подготовка к реализации выбранной стратегии;
- проверка стратегии.

Программно-технические меры

Программно-технические меры, то есть меры, направленные на контроль компьютерных сущностей – оборудования, программ и/или данных, образуют последний и самый важный рубеж информационной безопасности.

На этом рубеже становятся очевидными не только позитивные, но и негативные последствия быстрого прогресса информационных технологий. Во-первых, дополнительные возможности появляются не только у специалистов по ИБ, но и у злоумышленников. Во-вторых, информационные системы все время модернизируются, перестраиваются, к ним добавляются недостаточно проверенные компоненты (в первую очередь программные), что затрудняет соблюдение режима безопасности.

Сложность современных корпоративных ИС, многочисленность и разнообразие угроз их безопасности можно наглядно представить, ознакомившись с информационной системой Верховного суда Российской Федерации.

Меры безопасности целесообразно разделить на следующие виды:

- превентивные, препятствующие нарушениям ИБ;
- меры обнаружения нарушений;
- локализующие, сужающие зону воздействия нарушений;
- меры по выявлению нарушителя;
- меры восстановления режима безопасности.

В продуманной архитектуре безопасности все они должны присутствовать.

С практической точки зрения важными также являются следующие принципы архитектурной безопасности:

- непрерывность защиты в пространстве и времени, невозможность миновать защитные средства;
- следование признанным стандартам, использование апробированных решений;
- иерархическая организация ИС с небольшим числом сущностей на каждом уровне;
- усиление самого слабого звена;
- невозможность перехода в небезопасное состояние;
- минимизация привилегий;
- разделение обязанностей;
- эшелонированность обороны;
- разнообразие защитных средств;
- простота и управляемость информационной системы.

Центральным для программно-технического уровня является понятие сервиса безопасности. В число таких сервисов входят:

- идентификация и аутентификация;
- управление доступом;
- протоколирование и аудит;
- шифрование;
- контроль целостности;
- экранирование;
- анализ защищенности;
- обеспечение отказоустойчивости;
- обеспечение безопасного восстановления;
- туннелирование;
- управление.

Эти сервисы должны функционировать в открытой сетевой среде с разнородными компонентами, то есть быть устойчивыми к соответствующим угрозам, а их применение должно быть удобным для пользователей и администраторов. Например, современные средства идентификации/аутентификации должны быть устойчивыми к пассивному и активному прослушиванию сети и поддерживать концепцию единого входа в сеть.

Выделим важнейшие моменты для каждого из перечисленных сервисов безопасности:

1. Предпочтительными являются криптографические методы аутентификации, реализуемые программным или аппаратно-программным способом. Парольная защита стала анахронизмом, биометрические методы нуждаются в дальнейшей проверке в сетевой среде.
2. В условиях, когда понятие доверенного программного обеспечения уходит в прошлое, становится анахронизмом и самая распространенная – произвольная (дискреционная) – модель управления доступом. В ее терминах невозможно даже объяснить, что такое "троянская" программа. В идеале при разграничении доступа должна учитываться семантика операций, но пока для этого есть только теоретическая база. Еще один важный момент – простота администрирования в условиях большого числа пользователей и ресурсов и непрерывных изменений конфигурации. Здесь может помочь ролевое управление.

Протоколирование и аудит должны быть всепроникающими и многоуровневыми, с фильтрацией данных при переходе на более высокий уровень. Это необходимое условие управляемости. Желательно применение средств активного аудита, однако нужно осознавать ограниченность их возможностей и рассматривать эти средства как один из рубежей эшелонированной обороны, причем не самый надежный. Следует конфигурировать их таким образом, чтобы минимизировать число ложных тревог и не совершать опасных действий при автоматическом реагировании.

Все, что связано к криптографией, сложно не столько с технической, сколько с юридической точки зрения; для шифрования это верно вдвой-

не. Данный сервис является инфраструктурным, его реализации должны присутствовать на всех аппаратно-программных платформах и удовлетворять жестким требованиям не только к безопасности, но и к производительности. Пока же единственным доступным выходом является применение свободно распространяемого ПО.

Надежный контроль целостности также базируется на криптографических методах с аналогичными проблемами и методами их решения. Возможно, принятие Закона об электронной цифровой подписи изменит ситуацию к лучшему, будет расширен спектр реализаций. К счастью, к статической целостности есть и некриптографические подходы, основанные на использовании запоминающих устройств, данные на которых доступны только для чтения. Если в системе разделить статическую и динамическую составляющие и поместить первую в ПЗУ или на компакт-диск, можно в корне пресечь угрозы целостности. Разумно, например, записывать регистрационную информацию на устройства с однократной записью; тогда злоумышленник не сможет "замести следы".

Экранирование – идейно очень богатый сервис безопасности. Его реализации – это не только межсетевые экраны, но и ограничивающие интерфейсы, и виртуальные локальные сети. Экран инкапсулирует защищаемый объект и контролирует его внешнее представление. Современные межсетевые экраны достигли очень высокого уровня защищенности, удобства использования и администрирования; в сетевой среде они являются первым и весьма мощным рубежом обороны. Целесообразно применение всех видов МЭ – от персонального до внешнего корпоративного, а контролю подлежат действия как внешних, так и внутренних пользователей.

Анализ защищенности – это инструмент поддержки безопасности жизненного цикла. С активным аудитом его роднит эвристичность, необходимость практически непрерывного обновления базы знаний и роль не самого надежного, но необходимого защитного рубежа, на котором можно расположить свободно распространяемый продукт.

Обеспечение отказоустойчивости и безопасного восстановления – аспекты высокой доступности. При их реализации на первый план выходят архитектурные вопросы, в первую очередь – внесение в конфигурацию (как аппаратную, так и программную) определенной избыточности, с учетом возможных угроз и соответствующих зон поражения. Безопасное восстановление – действительно последний рубеж, требующий особого внимания, тщательности при проектировании, реализации и сопровождении.

Туннелирование – скромный, но необходимый элемент в списке сервисов безопасности. Он важен не столько сам по себе, сколько в комбинации с шифрованием и экранированием для реализации виртуальных частных сетей.

Управление – это инфраструктурный сервис. Безопасная система должна быть управляемой. Всегда должна быть возможность узнать, что на самом деле происходит в ИС (а в идеале – и получить прогноз развития си-

туации). Возможно, наиболее практичным решением для большинства организаций является использование какого-либо свободно распространяемого каркаса с постепенным "навешиванием" на него собственных функций.

Миссия обеспечения информационной безопасности трудна, во многих случаях невыполнима, но всегда благородна.

Вариант 1

1. Некоторые авторы включают в число основных аспектов безопасности подотчетность. На Ваш взгляд, это:

- ☐ правильно, потому что без подотчетности не может быть безопасности
- ☐ неправильно, потому что подотчетность - не цель, а средство достижения безопасности
- ☐ не имеет значения, потому что все это словесная эквилибристика, далекая от реальной безопасности

2. На законодательном уровне информационной безопасности особенно важны:

- ☐ направляющие и координирующие меры
- ☐ ограничительные меры
- ☐ меры по обеспечению информационной независимости

3. Принцип усиления самого слабого звена можно переформулировать как:

- ☐ принцип равнопрочности обороны
- ☐ принцип удаления слабого звена
- ☐ принцип выявления главного звена, ухватившись за которое, можно вытянуть всю цепь

Вариант 2

1. Некоторые авторы включают в число основных аспектов безопасности приватность. На Ваш взгляд, это:

- ☐ правильно, потому что нарушение приватности может причинить ущерб субъекту информационных отношений
- ☐ неправильно, потому что приватность клиента реализуется на стороне поставщика информационной услуги и является одним из ее качеств
- ☐ неправильно, потому что приватность одних противоречит безопасности других

2. Самым актуальным из стандартов безопасности является:

- ☐ "Оранжевая книга"
- ☐ рекомендации X.800
- ☐ "Общие критерии"

3. Из принципа разнообразия защитных средств следует, что:

- ☐ в разных точках подключения корпоративной сети к Internet необходимо устанавливать разные межсетевые экраны
- ☐ каждую точку подключения корпоративной сети к Internet необходимо защищать несколькими видами средств безопасности
- ☐ защитные средства нужно менять как можно чаще

Вариант 3

1. Некоторые авторы включают в число основных аспектов безопасности актуальность информации. На Ваш взгляд, это:

- ☐ правильно, потому что получение неактуальной информации может причинить ущерб субъекту информационных отношений
- ☐ неправильно, потому что актуальность является одним из качеств информационной услуги
- ☐ не имеет значения, потому что все это словесная эквилибристика, далекая от реальной безопасности

2. Элементом процедурного уровня ИБ является:

- ☐ логическая защита
- ☐ техническая защита
- ☐ физическая защита

3. С информацией о новых уязвимых местах достаточно знакомиться:

- ☐ раз в день
- ☐ раз в неделю
- ☐ при получении очередного сообщения по соответствующему списку рассылки

Обязательная литература

1. Галатенко В.А.
Информационная безопасность: практический подход.
Под ред. Бетелина В.Б.- М.: Наука, 1998.

Дополнительная литература

1. Гайкович В., Першин А.
Безопасность электронных банковских систем.
М.: Единая Европа, 1994.

2. Трубачев А.П. и др.
Оценка безопасности информационных технологий.
Под общ. ред. Галатенко В.А. - М.: СИП РИА, 2001.

3. Russel D., Gangemi G.T.
Computer Security Basics.
O'Reilly & Associates, Inc., 1992.

Подготовительная литература

1. Буч Г.
Объектно-ориентированный анализ и проектирование с примерами приложений на C++, 2-е изд.
Бином, Невский диалект, 2001

Статьи по теме курса

1. Гостехкомиссия России. Руководящий документ. Концепция защиты СВТ и АС от НСД к информации
Москва, 1992.

2. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации
Москва, 1992.

3. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации
Москва, 1992.

4. Гостехкомиссия России. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники
Москва, 1992.

5. Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения
Москва, 1992.

6. Федеральный Закон "Об информации, информатизации и защите информации"
"Российская газета", 1995, 22 февраля.

7. Department of Defense Trusted Computer System Evaluation Criteria
DoD 5200.28-STD, 1993.

8. Information Technology Security Evaluation Criteria (ITSEC). Harmonized Criteria of France - Germany - the Netherlands - the United Kingdom
Department of Trade and Industry, London, 1991.

9. Security Architecture for Open Systems Interconnection for CCITT Applications. Recommendation X.800
CCITT, Geneva, 1991.

10. Holbrook P., Reynolds J., Site Security Handbook.
Request for Comments: 1244, 1991.

11. Винклер А., Задание: шпионаж
http://www.jetinfo.ru/1996/19/1/article1.19.1996.html

12. Беззубцев О., Ковалев А., О лицензировании и сертификации в области защиты информации
http://www.jetinfo.ru/1997/4/1/article1.4.1997.html

13. Симонов С., Анализ рисков, управление рисками
http://www.jetinfo.ru/1999/1/1/article1.1.1999.html

14. Барсуков В., Физическая защита информационных систем
http://www.jetinfo.ru/1997/1/1/article1.1.1997.html

15. Барсуков В., Блокирование технологических каналов утечки информации
http://www.jetinfo.ru/1998/5-6/1/article1.5-6.1998.html

16. Барсуков В., Защита компьютерных систем от силовых деструктивных воздействий
http://www.jetinfo.ru/2000/2/2/article2.2.2000.html

17. Бабернов В., Системы резервного копирования
http://www.jetinfo.ru/2000/12/1/article1.12.2000.html

18. Браунли Н., Гатмэн Э., Как реагировать на нарушения информационной безопасности (RFC 2350, BCP 21)
http://www.jetinfo.ru/2000/5/1/article1.5.2000.html

19. Таранов А., Цишевский В., Java в три года
http://www.jetinfo.ru/1998/11-12/1/article1.11-12.1998.html

20. Семенов Г., Не только шифрование, или Обзор криптотехнологий
http://www.jetinfo.ru/2001/3/2/article2.3.2001.html

21. Контроль над корпоративной электронной почтой: система "Дозор-Джет"
http://www.jetinfo.ru/2002/5/2/article2.5.2002.html

22. Z-2 = универсальный межсетевой экран высшего уровня защиты
http://www.jetinfo.ru/2002/5/3/article3.5.2002.html

23. Сканер защищенности Nessus: уникальное предложение на российском рынке
http://www.jetinfo.ru/2000/10/2/article2.10.2000.html

24. Бернстайн Ф.А., Middleware: модель сервисов распределенной системы
http://www.jetinfo.ru/1997/11/1/article1.11.1997.html

Сайты по теме курса

1. Web-сервер властных структур Российской Федерации.
   http://www.gov.ru/

2. Web-сервер Совета безопасности РФ.
   http://www.scrf.gov.ru/

3. Web-сервер Федерального агентства правительственной связи и информации при Президенте Российской Федерации.
   http://www.fagci.ru/

4. Web-сервер Государственной технической комиссии при Президенте Российской Федерации.
   http://www.infotecs.ru/gtc/

5. Сервер Государственной Думы Федерального Собрания РФ
   http://www.duma.gov.ru/

6. Web-сервер Верховного Суда Российской Федерации.
   http://www.supcourt.ru/

7. Web-сервер подразделения по выявлению и пресечению преступлений, совершаемых с использованием поддельных кредитных карт, и преступлений, совершаемых путем несанкционированного доступа в компьютерные сети и базы данных.
   http://www.cyberpolice.ru/

8. Два портала по информационной безопасности:
   http://infosecurity.report.ru/
   http://www.void.ru/

9. Российский криптографический портал.
   http://www.cryptography.ru/

10. Информационный бюллетень "Jet Info" с тематическим разделом по информационной безопасности.
    http://www.jetinfo.ru/

11. Журнал "Открытые системы", регулярно публикующий статьи по информационной безопасности.
    http://www.osp.ru/os/

12. Сервер компании НИП "Информзащита".
http://www.infosec.ru/

13. Сервер с информацией об аутентификации по биометрическим характеристикам (прежде всего - по отпечаткам пальцев).
http://biometrics.ru/

14. Два сервера с "хакерским" имиджем.
http://www.hackzone.ru/
http://www.nerf.ru/

15. Украинский Центр информационной безопасности.
http://www.bezpeka.com/

16. Сервер оперативной информации UA/Security Line.
http://hack.com.ua/

17. Библиотека Конгресса США.
http://thomas.loc.gov/

18. Сервер с материалами по законодательству Великобритании.
http://www.hmso.gov.uk/

19. Сервер Института информационной безопасности
http://www.gocsi.com/

20. Web-сервер подразделения Министерства юстиции США, предназначенный для освещения вопросов киберпреступности.
http://www.cybercrime.gov/

21. Web-сервер Национального института стандартов (НИСТ) США.
http://www.nist.gov/

22. Web-сервер Института национальной безопасности США.
http://www.nsi.org/

23. Сервер с материалами по "Общим критериям".
http://www.commoncriteria.org/

24. Сервер Тематической группы по технологии Internet.
http://www.ietf.org/.

25. Сервер координационного совета группы реагирования на нарушения ИБ.
http://www.cert.org/

26. Форум групп реагирования.
http://www.first.org/

27. Страница на сервере Агентства национальной безопасности (АНБ) США с материалами о версии свободно распространяемой ОС Linux с усовершенствованными средствами безопасности.
http://www.nsa.gov/selinux/

28. Подборка ответов на часто задаваемые вопросы по информационной безопасности.
http://www.faqs.org/faqs/computer-security/

29. Телеконференция по информационной безопасности.
news:comp.security.misc

30. Сервер с архивами сообщений и с возможностью подписки на списки рассылки по ИБ.
http://www.securityfocus.com/

31. Страница Р. Райвеста на сервере Массачусетского технологического института.
http://theory.csl.mit.edu/~rivest/

32. Web-сервер Брюса Шнейера.
http://www.counterpane.com/

33. Домашняя страница известного специалиста в области информационной безопасности Дороти Деннинг.
http://www.cs.georgetown.edu/~denning/

34. Материалы по безопасности Java-среды.
http://java.sun.com/security/

35. Подборка материалов по информационной безопасности.
http://www.linuxsecurity.com/

36. Сервер разработок ПО с открытым кодом.
http://www.opensource.org/

37. Хранилище разработок с открытым кодом.
http://www.sourceforge.net/

38. Сервер Института системного администрирования, сетевого обеспечения и безопасности.
http://www.sans.org/

39. Сервер консорциума аутентификации по биометрическим характеристикам.
http://www.biometrics.org/

40. Сервер Лаборатории проектирования систем Стэнфордского исследовательского института.
http://www.sdl.sri.com/

41. Сервер Информационного центра электронной приватности.
http://www.epic.org/

42. Сервер с материалами по протоколу SSL.
http://www.openssl.org/

43. Серверы с материалами по SSH.
http://www.ssh.com/
http://www.openssh.org/

44. Сервер с новостной информацией по ИБ.
http://www.infosecnews.com/

45. Сервер с реферативной информацией по ИБ.
http://www.isr.net/

46. Журнал по информационной безопасности.
http://www.securitymagazine.com/

47. Классический хакерский журнал 2600.
http://www.2600.com/

48. Сервер с хакерским имиджем.
http://www.insecure.org/

Серия "Основы информационных технологий"

В.А. Галатенко
Под редакцией члена-корреспондента РАН В. Б. Бетелина
Основы информационной безопасности
Курс лекций

Редактор, корректор Е. Петровичева
Технический редактор О. Новикова
Компьютерная верстка Н. Дородницына, А. Лошкова
Обложка М. Автономова

Формат 60×90 1/16. Усл. печ. л. 17,5. Бумага офсетная.
Подписано в печать 25.04.2003. Тираж 3000 экз. Заказ № 6485 (К-см).

ООО "ИНТУИТ.ру"
Интернет-Университет Информационных Технологий, www.intuit.ru
123056, Москва, Электрический пер., 8, стр. 3.

Отпечатано с готовых диапозитивов
в ФГУП "Смоленский полиграфический комбинат",
214020, г. Смоленск, ул. Смольянинова, 1

овы информационной безопасности

Курс лекций

Курс "Основы информационной безопасности" характеризуется фундаментальностью подхода, широтой и разнообразием привлекаемого материала, систематичностью изложения, новизной методологии. Рассмотрение проблематики информационной безопасности с позиций технологии программирования представляется весьма интересным и перспективным.

Владимир Бетелин
член-корреспондент РАН

Основное достоинство данного учебника заключается в том, что в изложении материала учтены методики преподавания и практического использования технологии программирования и объектно-ориентированного

Учебни
могли с
обеспеч
и сложн
компле

Анатолий Шкред

ISBN 5-9556-0003-5

ИНТЕРНЕТ УНИВЕРСИТЕТ
информационных технологий

http://www.intuit.ru