МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное казенное
образовательное учреждение высшего образования
«Казанский юридический институт
Министерства внутренних дел Российской Федерации»

Кафедра оперативно-разыскной деятельности

Дипломная работа

на тему: Административный и процедурный уровень информационной безопасности, а также основные программно – технические меры в деятельности оперативных и иных подразделений полиции в борьбе с преступностью

Выполнил: С.И. Гвоздев
специальность - Правоохранительная деятельность, год набора 2011, учебная группа №311,
капитан полиции
Руководитель:
Старший преподаватель кафедры ОРД КЮИ МВД России, кандидат педагогических наук,
подполковник полиции П.В. Матижев
Консультант:
_____
(ученая степень, ученое звание, должность, специальное звание)

_____
(фамилия, имя, отечество)

К защите _____
(допущена, не допущена)

Начальник кафедры ОРД _____
Дата защиты «__» _____ 2017 г. Оценка _____

Рег. №_____ от __.__.2017 г.

Казань 2017 г.

Оглавление

1. Введение

Актуальность выбранной темы обусловлена тем, что формирование правового государства, укрепление законности и правопорядка требуют повышения эффективности работы всех правоохранительных органов, в том числе и органов внутренних дел.

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 направлен-

ных 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).

Информационные системы 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 информационные системы 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.

Задача работы – изучить литературу об административном и процедурном уровне информационной безопасности, информационной системе органов внутренних дел и на основе этих знаний дать всестороннюю глубокую характеристику административному и процедурному уровню, раскрыть сущность и задачи.

2. Глава первая.
Актуальные проблемы информационной безопасности в деятельности органов внутренних дел.

Современная Российская преступность становится все более профессиональной. В качестве показателя профессионализма преступного мира можно назвать появление такой, раннее не имевшей в России столь широкого распространения формы преступности как компьютерная преступность. Ее современные масштабы таковы, что требуют самой активной работы по защите информации от «электронных пиратов».

Издержки конверсии обусловили отток умов из многих, ранее элитных, сфер науки и производства. Так, например, самыми опытными в области компьютерной преступности считаются российские электронщики. На компьютерную преступность в республиках бывшего СССР работает около 100 тысяч человек постоянно и еще 3 млн. человек - время от времени. Центрами компьютерной преступности считаются Москва, Санкт-Петербург, Украина и Урал. Российская компьютерная преступность вызывает все более растущую озабоченность за рубежом, ибо в результате умелых компьютерных махинаций, проводимых электронными пиратами России, иностранные банки теряют крупные суммы денег, исчезающие в неизвестном направлении.

Компьютерная преступность стала настоящим бичом экономики развитых государств. Так, например, 90% фирм и организаций в Великобритании в разное время становились объектами электронного пиратства или находились под его угрозой, в Нидерландах жертвами компьютерной преступности стали 20% различного рода предприятий . В ФРГ с использованием компьютеров ежегодно похищается 4 млрд. марок, а во Франции - 1 млрд. франков. Специалисты отмечают высокий уровень латентности этого вида преступлений, т.к. в 85% случаев факты компьютерного пиратства не раскрываются.

Ситуация усугубляется и тем, что сами правоохранительные органы тоже становятся объектом внимания преступников, вооруженных современной вы-

числительной техникой. Поэтому сегодня весьма актуальной для органов внутренних дел стала задача защиты собственной информации.

Информационная безопасность - это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры[1].

Проблема информационной безопасности, особенно для органов внутренних дел, на сегодняшний день представляет наибольший интерес. Борьба с компьютерной преступностью - одна из самых важных задач правоохранительных органов на фоне колоссального развития информационных систем, локальных и глобальных сетей.

Проблема обеспечения информационной безопасности носит комплексный характер, для решения которой необходимо сочетание законодательных, организационных и программно-технических мер.

Необходимо своевременное и эффективное совершенствование законодательства, т.к. имеющаяся на данный момент законодательная база в этой области значительно отстает от практических потребностей.

Наблюдается огромная нехватка высококвалифицированных кадров в ОВД. Эта проблема, на наш взгляд, может быть решена следующими способами:

- в связи со значительным сокращением кадров вооруженных сил Р.Ф., среди которых немало хороших специалистов в области работы на ЭВМ, возможно, их привлечение к работе в правоохранительных органах; введением специальных курсов по первоначальной и профессиональной подготовке работы на персональных компьютерах, введение в учебную программу курса "Информационная безопасность и применение информационных технологий в

[1] Закон Российской Федерации «О безопасности», 5 марта 1992 г. Ст. 13

борьбе с преступностью"[2]; необходимо улучшить финансирование организаций и учреждений, входящих в состав МВД России, для закупки хорошего оборудования и современного программного обеспечения, т.к. материальная база МВД РФ в области информационной безопасности на данный момент находится на недостаточном уровне;

- представляется возможным постановка вопроса о совершенствовании процесса подготовки сотрудников ОВД, специализирующихся на работе в области информационной безопасности. С этой целью, на наш взгляд, необходима дифференциальная система обучения, т.к. солидная подготовка в области информатики не может быть получена в рамках традиционного высшего учебного заведения МВД РФ;
- создать благоприятные условия принятия на работу в ОВД высококвалифицированных специалистов, работающих в интересующей нас области. Обеспечить соответствующие размеры оплаты труда, так как сегодня, с материальной точки зрения, гораздо выгоднее работать по данной специальности в банковских структурах и частных фирмах.

Для поддержания режима информационной безопасности наиболее важны программно-технические меры, так как известно, что основная угроза компьютерным системам исходит от них самих, что может выражаться в ошибках программного обеспечения, сбоях оборудования, неудовлетворительной работе сотрудников, а также руководителей организаций и учреждений, относящихся к системе ОВД[3].

В.А. Галатенко выделяет следующие ключевые механизмы безопасности: идентификация и аутентификация, управление доступом, протоколирование и аудит, криптография и экранирование, для эффективного использования, которых необходим опережающий анализ возможных угроз.

---

[2] утвержденного Главным управлением кадров МВД России 1 июня 1997 года в образовательных учреждениях высшего профессионального образования МВД России по специальности Юриспруденция (специализация "Информационная безопасность"

[3] Галатенко В. Информационная безопасность. // Открытые системы, 1996. – № 1.

Информационная безопасность не сможет обеспечиваться без строгого распределения функций пользователей, администраторов локальных сетей и серверов, а также руководителей учреждений ОВД.

Причем обязанности и функции перечисленных групп сотрудников ОВД должны разрабатываться и утверждаться заранее, в зависимости от того, на достижении каких целей они будут направлены. Можно выделить несколько типичных функций, присущих для сотрудников любого управления или отдела ОВД.

Начальники подразделений отвечают за доведение утвержденных положений и принципов политики безопасности до пользователей и администраторов локальных сетей и серверов, там же за контакты, с ними информируя об изменении статуса каждого из подчиненных (увольнение из органов внутренних дел, назначение на другую должность и т.п.).

Эта функция наиболее важна вследствие того, что сотрудник, уволенный по каким-либо причинам, может представлять наиболее существенную опасность для того отдела или управления, где он работал.

Проблема "обиженного" сотрудника существовала всегда и будет существовать. Зная основные принципы функционирования системы, он может, руководствуясь негативными побуждениями, попытаться удалить, изменить, исправить какие-либо данные. Поэтому необходимо следить за тем, чтобы при увольнении сотрудника его права доступа к информационным ресурсам аннулировались. Примерами возникновения данной проблемы могут служить зарубежные фильмы, сюжет которых основывается на реальных событиях наших дней;

Нельзя также ставить на второй план проблему тайлерантности т.е. проблему соотношения целей и средств. Действительно, затраты на приобретение комплексных мер защиты не должны превышать стоимость возможного ущерба.

Администраторы локальной сети, должны обеспечивать бесперебойное функционирование сети, ответственных за реализацию технических мер, эф-

фективное применение средств защиты, тем самым обеспечивая политику безопасности.

Администраторы серверов отвечают за закрепленные за ними серверы и следят за тем, чтобы используемые механизмы, обеспечивающие режим информационной конфиденциальности, соответствовали общим принципам политики безопасности.

Пользователи обязаны работать с локальной сетью, руководствуясь политикой безопасности, выполнять приказы и распоряжения сотрудников, отвечающих за отдельные аспекты информационной безопасности, незамедлительно докладывать руководству обо всех подозрительных ситуациях.

Особый интерес на наш взгляд, с точки зрения соблюдения информационной безопасности, вызывает статус пользователей персональных компьютеров. Дело в том, что значительная часть информационных потерь приходится на случайные и преднамеренные ошибки сотрудников, работающих на информационно – вычислительной технике. В силу своей возможной халатности и небрежности они могут ввести заведомо неверные данные, пропустить ошибки в программном обеспечении, создав тем самым брешь в системе защиты. Все это заставляет задуматься о том, что внутренняя угроза, исходящая непосредственно от пользователей персональных компьютеров значительнее и опаснее внешних воздействий[4].

В заключении необходимо напомнить, что соблюдение информационной безопасности это задача не отдельной страны, а всего человечества, так как высокоразвитая компьютерная преступность наших дней давно вышла на мировой уровень. Поэтому эффективная борьба с ней возможна только при тесном сотрудничестве правоохранительных органов разных стран мира. Необходимо строить совместный комплекс мер и средств, набирать и готовить высококвалифицированные кадры, детально разрабатывать основные принципы политики безопасности, без которых невозможно нормальное развитие информационных коммуникаций.

[4] Черняк Ю.Д. Информация и управление. М., 2004.

2.1. Основные понятие информационной безопасности.

Под информационной безопасностью следует понимать защиту интересов субъектов информационных отношений.

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[5].

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[6].

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 искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в

[5] Доктрина информационной безопасности Российской Федерации. Утверждена поручением Президента Российской Федерации от 9 сентября 2000 г. № Пр-1897 (см. приложение 3).

[6] Федеральный закон "Об участии в международном информационном обмене" от 04.07.1996 N 85-ФЗ

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. Угрозы информационной безопасности - это оборотная сторона использования информационных технологий.

Из этого положения можно вывести два важных следствия:

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 случае** "да нет у нас никаких секретов, лишь бы все работало".

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[7].

[7] Стрельцов А. А. «Обеспечение информационной безопасности России. Теоретические и методологические основы», МЦНМО, 2002

Возвращаясь к вопросам терминологии, отметим, что термин "компьютерная безопасность" (как эквивалент или заменитель информационной безопасности) 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)[8].

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

[8] Н.*И.Журавленко, В.Е.Кадулин, К.К.Борзунов.* Основы информационной безопасности: Учебное пособие. – М.: МосУ МВД России. 2007.

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 информационной безопасности 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.

Целостность - актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

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 остальным 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, которы-

ми 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 информационной безопасности 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 информационные системы, 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[9].

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, функцио-

---

9 Указ Президента РФ от 5 декабря 2016 г. № 646 “Об утверждении Доктрины информационной безопасности Российской Федерации”.

нировавшим 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).

Понятно, что подобных примеров множество, можно вспомнить и другие случаи - недостатка в нарушениях информационной безопасности 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 безопасность 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 информационной безопасности. 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 информационной системы.

Приведем еще несколько цифр. В марте 1999 года был опубликован очередной, четвертый по счету, годовой отчет "Компьютерная преступность и безопасность-1999: проблемы и тенденции[10]". 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 про-

[10] Issues and Trends: 1999 CSI/FBI Computer Crime and Security Survey

блем 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 информационной безопасности - доступности, целостности или конфиденциальности.

2.2. Основные определения и критерии классификации угроз информационной безопасности

Угроза - это потенциальная возможность определенным образом нарушить информационную безопасность[11].

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 информационную систему.

[11] Закон Российской Федерации «О безопасности».

Если речь идет об ошибках в программном обеспечении, 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 информационной системе.

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 информационных систем. Например, угроза отключения электричества или выхода его параметров за допустимые границы существует в силу зависимости аппаратного обеспечения информационной системы 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 концентра-

ции 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 информационной безопасности, 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 информационной системы).

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

Наиболее распространенные угрозы доступности

Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки штатных пользователей, операторов, сис-

темных 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 информационной системы, 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.

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 программного обеспечения:

- 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 программного обеспечения;
- 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 информационной системе 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 программного обеспечения 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 программного обеспечения 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[12]».

[12] ГОСТ Р 50922 «Защита информации. Основные термины и определения» п. 3.10

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

Окно опасности для вредоносного программного обеспечения 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 программного обеспечения 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[13].

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 "по-

[13] "W97M.Melissa.A" . Symantec . Источник +9 февраля 2013 .

вышение 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 программного обеспечения (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"[14]; 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 программного обеспечения 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

[14] СМИ и история компьютерных вирусов (вирус «Микеланджело», 1992) // 13 ноября 2016

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 (секретарь 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 программного обеспечения - 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 информационной системы, 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[15].

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.

3. Глава вторая. Административный и процедурный уровень информационной безопасности.

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

[15] статья Айрэ Винклера "Задание: шпионаж" в Jet Info, 1996, 19

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 информационной системы, 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[16], предлагающий типовой каркас.

Разработка программы и политики безопасности может служить примером использования понятия уровня детализации. Он должны подразделяться на несколько уровней, трактующих вопросы разной степени специфичности. Важным элементом программы является разработка и поддержание в актуальном состоянии карты информационной системы.

Необходимым условием для построения надежной, экономичной защиты является рассмотрение жизненного цикла информационной системе и синхронизация с ним мер безопасности. Выделяют следующие этапы жизненного цикла:

- инициация;
- закупка;

[16] В настоящее время Британский стандарт **BS 7799** поддерживается в **27** странах мира, в числе которых страны Британского Содружества, а также Швеция, Нидерланды, Россия.

- 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 применим 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 крайне важно 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 информационной безопасности 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 информационной безопасности. 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 крайне важно 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 реализации выбранной стратегии;
- проверка стратегии.

3.1. Административный уровень информационной безопасности. Управление рисками.

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[17].

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[18]).

Информационная система 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 информационную систему 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:

[17] Информационное общество: Информационные войны. Информационное управление. Информационная безопасность. СПб., СПб. ун-т, 1999.

[18] «Оранжевая книга» была впервые опубликован в августе 1983 года.

- 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, доступности 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. **В – третьих**, 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 программное обеспечение, 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 программного обеспечения 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[19].

Приведем несколько примеров вопросов, на которые следует дать ответ в политике безопасности ***нижнего уровня***:

- кто имеет право доступа к объектам, поддерживаемым сервисом?

[19] Закон Российской Федерации «О безопасности».

- 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 правила 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 мень-

шими 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[20].

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?

[20] «Основы информационной безопасности систем и сетей передачи данных» М., СИНТЕГ, 2000. Устинов Г.Н.

- 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, сле-

дует 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.

К *процедурному уровню* относятся меры безопасности, реализуемые людьми. В отечественных организациях накоплен богатый опыт составления и реализации процедурных (организационных) мер, однако проблема состоит в том, что они пришли из докомпьютерного прошлого, и поэтому нуждаются в существенном пересмотре.

Можно выделить следующие группы процедурных мер, направленных на обеспечение информационной безопасности:

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

Управление персоналом в контексте информационной безопасности является в России белым пятном. **Во-первых**, для каждой должности должны существовать квалификационные требования по информационной безопасности**. Во-вторых**, в должностные инструкции должны входить разделы, касающиеся информационной безопасности. **В-третьих**, каждого работника нужно научить мерам безопасности теоретически и оттренировать выполнение этих мер практически (и проводить подобные тренировки дважды в год).

Без всякого преувеличения, нужна информационная гражданская оборона. Спокойно, без нагнетания страстей, нужно разъяснять обществу не только преимущества, но и опасности, вытекающие из использования информационных технологий. Акцент, на наш взгляд, следует делать не на военной или криминальной стороне дела, а на чисто гражданских аспектах, связанных с под-

держанием нормального функционирования аппаратного и программного обеспечения, то есть концентрироваться на вопросах доступности и целостности данных.

Разумеется, разделы, касающиеся информационной безопасности, должны стать частью школьных и, тем более, ВУЗовских курсов информатики.

Меры физической защиты, известные с давних времен, нуждаются в доработке в связи с распространением сетевых технологий и миниатюризацией вычислительной техники. Прежде всего, следует защититься от утечки информации по техническим каналам. Этим занимается Гостехкомиссия России.

Поддержание работоспособности — еще одно белое пятно, образовавшееся сравнительно недавно. В эпоху господства больших ЭВМ удалось создать инфраструктуру, способную обеспечить по существу любой наперед заданный уровень работоспособности (доступности) на всем протяжении жизненного цикла информационной системы. Эта инфраструктура включала в себя как технические, так и процедурные регуляторы (обучение персонала и пользователей, проведение работ в соответствии с апробированными регламентами и т.п.). При переходе к персональным компьютерам и технологии клиент/сервер инфраструктура обеспечения доступности во многом оказалась утраченной, однако важность данной проблемы не только не уменьшилась, но, напротив, существенно возросла. Перед государственными и коммерческими организациями стоит задача соединения упорядоченности и регламентированности, присущих миру больших ЭВМ, с открытостью и гибкостью современных систем.

Реагирование на нарушения информационной безопасности — снова белое пятно. Допустим, пользователь или системный администратор понял, что имеет место нарушение. Что он должен делать? Попытаться проследить злоумышленника? Немедленно выключить оборудование? Позвонить в милицию? Проконсультироваться со специалистами ФАПСИ или Гостехкомиссии? Ни одно ведомство, причастное к информационной безопасности, не предложило регламента действий в подобной экстремальной ситуации или своей консультационной помощи. Необходимо организовать национальный центр информационной

безопасности, в круг обязанностей которого входило бы, в частности, отслеживание современного состояния этой области знаний, информирование пользователей всех уровней о появлении новых угроз и мерах противодействия, оперативная помощь организациям в случае нарушения их информационной безопасности[21].

Планирование восстановительных работ и вся проблематика, связанная с восстановлением работоспособности после аварий, также является белым пятном. А ведь ни одна организация от таких нарушений не застрахована. Здесь необходимо отработать действия персонала во время и после аварий, заранее позаботиться об организации резервных производственных площадок, отработать процедуру переноса на эти площадки основных информационных ресурсов, а также процедуру возвращения к нормальному режиму работы. Подчеркнем, что подобный план нужен не только сверхважным военным организациям, но и обычным коммерческим компаниям, если они не хотят понести крупные финансовые потери.

Основные понятия управление рисками.

Управление рисками рассматривается нами на административном уровне информационной безопасности, 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

[21] «Информация и собственность. Защита прав создателей и пользователей программ для ЭВМ и баз данных». Терещенко Л.К.

проанализированного нами ранее российского законодательства в области информационной безопасности). 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.

Использование информационных систем связано с определенной совокупностью рисков. Когда возможный ущерб неприемлемо велик, необходимо принять экономически оправданные меры защиты. Периодическая (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 информационной системы. 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 информационная система 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 каждый 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 информационной системы 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[22].

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 ин-

[22] Обеспечение информационной безопасности России . А.А. Стрельцов МЦНМО, 2002

формационной 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 с 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 вероятность 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 ре-

комендовать 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 обучения 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.

3.2. Процедурный уровень информационной безопасности

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 обществу 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[23].

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 информационной системы 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 служеб-

[23] Базаров, Т.Ю. Управление персоналом. Практикум: Учебное пособие / Т.Ю. Базаров. - М.: ЮНИТИ, 2014.

ных 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 сослуживцами 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 подобъектов 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 дос-

тупа 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.

Профессия **пожарного** - 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.

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. 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[24].

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.

[24] Липаев В.В. «Документирование и управление конфигурацией программных средств», М., «Синтег», 1998

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. 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 конфиденциальности, к другим, таким как план восстановления после аварий - требования цело-

стности и доступности (в критической ситуации план необходимо найти и прочитать)[25].

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, восстанов-

[25] Прохода А.Н. Обеспечение интернет-безопасности. Учебное пособие для вузов. – М.:Телеком, 2007.

ленный 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.

Чтобы предотвратить повторные нарушения, необходимо анализировать каждый инцидент, выявлять причины, накапливать статистику. Каковы источники вредоносного программного обеспечения? 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 преду-

предительный 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[26].

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;

[26] Теоретические основы информатики и информационная безопасность: монография / под ред. В. А. Минаева и В.Н. Саблина.— М.: Радио и связь, 2000.

- 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[27]:

- 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

[27] Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 02.07.2013) "Об информации, информационных технологиях и о защите информации"// Консультант Плюс

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.

4. Глава третья. Основные программно – технические меры

4.1. 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[28].

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.

Следует, однако, учитывать, что быстрое развитие информационных технологий не только предоставляет обороняющимся новые возможности, но и объективно затрудняет обеспечение надежной защиты, если опираться исключительно на меры программно-технического уровня.

Причин тому несколько:

[28] **Анин, Б.Ю.** Защита компьютерной информации. / Б.Ю.Анин - СПб.: БХВ-Петербург, 2000.

- 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 информационной безопасности); 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 информационной безопасности;
- 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,

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[29].

С точки зрения безопасности наиболее существенными представляются следующие аспекты современных информационных систем:

- 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

[29] Блинов, С.В. Технологии безопасности в деятельности правоохранительных органов, 2006.

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[30].

В силу изложенных причин далее будут рассматриваться распределенные, разнородные, многосервисные, эволюционирующие системы. Соответственно, нас будут интересовать решения, ориентированные на подобные конфигурации.

Архитектурная безопасность

---

[30] Административная деятельность органов внутренних дел. А.П.Корнеева. – М.: МЮНМВД России, 1996.

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[31]".

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 представ-

[31] Галатенко В.А. Стандарты информационной безопасности – М.: 2004

лял 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 информационных систем 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 информационных систем и уменьшает вероят-

ность попадания в тупиковую ситуацию, когда обеспечение безопасности потребует непомерно больших затрат и принципиальных модификаций.

Иерархическая организация информационной системы 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 иден-

тификацией и аутентификацией - управление доступом и, как последний рубеж, - протоколирование и аудит. Эшелонированная оборона способна, по крайней мере, задержать злоумышленника, а благодаря 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[32].

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.

4. Заключение

Главной задаче административного и процедурного уровня - это сформировать программу работ в области информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Административная деятельность направлена на обеспечение ликвидации угроз и рисков в сфере информационной безопасности является основным фактором ее структурирования, формирования и рассматривается как деятельность, имеющая целью предотвратить нанесение ущерба интересам личности, общества и государства в информационной сфере.

Основой программы является политика безопасности, отражающая подход организации к защите своих информационных активов.

[32] Мандиа К. Защита от вторжений. Расследование компьютерных преступлений. – СПб.: Лори, 2005.

Разработка политики, а так же программы информационной безопасности начинается с анализа рисков, первым этапом которого, в свою очередь, является ознакомление с наиболее распространенными угрозами.

Угроза - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения конфиденциальности, доступности и целостности информации, а так же внутренняя сложность информционной системы, непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы в ОВД.

В заключении необходимо напомнить, что соблюдение информационной безопасности - это задача не отдельной страны, а всего человечества, так как высокоразвитая компьютерная преступность наших дней давно вышла на мировой уровень. Поэтому эффективная борьба с ней возможна только при тесном сотрудничестве правоохранительных органов разных стран мира. Необходимо строить совместный комплекс мер и средств, набирать и готовить высококвалифицированные кадры, детально разрабатывать основные принципы политики безопасности, без которых невозможно нормальное развитие информационных коммуникаций.

Но в сожалению в нашей стране наблюдается огромная нехватка высококвалифицированных кадров в ОВД. Эта проблема, на мой взгляд, может быть решена не которыми способами:

- в связи со значительным сокращением кадров, среди которых немало хороших специалистов в области работы на ЭВМ в правоохранительных органах;
- введением специальных курсов по первоначальной и профессиональной подготовке работы на персональных компьютерах, введение в учебную программу курса "Информационная безопасность и применение информационных технологий в борьбе с преступностью", утвержденного Глав-

ным управлением кадров МВД России 1 июня 1997 года в образовательных учреждениях высшего профессионального образования МВД России по специальности Юриспруденция;

- необходимо улучшить финансирование организаций и учреждений, входящих в состав МВД России, для закупки хорошего оборудования и современного программного обеспечения (материальная база МВД РФ в области информационной безопасности на данный момент находится на недостаточном уровне);
- создать благоприятные условия принятия на работу в ОВД вы сококвалифицированных специалистов, работающих в интересующей нас области. Обеспечить соответствующие размеры оплаты труда, так как сегодня, с материальной точки зрения, гораздо выгоднее работать по данной специальности в банковских структурах и частных фирмах.

Используемая литература:

1. Селиванов Н. «Проблемы борьбы с компьютерной преступностью» // Законность, 1993. – № 8.

2. Галатенко В. «Информационная безопасность». // Открытые системы, 1996. – № 1.

3. Федеральный Закон "Об информации, информатизации и защите информации". // Российская газета, 1995. 22 февраля.

4. Президент Российской Федерации. Указ от 3 апреля 1995 г. № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации».

5. Галатенко В. Указ. соч.

6. «Теория и практика обеспечение информационной безопасности». Д.П. Зегжда, А.М. Ивашко.

7. статья В. Барсукова «Защита компьютерных систем от силовых деструктивных воздействий» в Jet Info, 2000, 2).

8. Белоглазов Е.Г. и др. «Основы информационной безопасности органов внутренних дел» Учебное пособие. – М.: МосУ МВД России, 2005.

9. Н.И. Журавленко, В.Е. Кадулин, К.К. Борзунов. «Основы информационной безопасности» Учебное пособие. – М.: МосУ МВД России. 2007.

10. Величко М.Ю. «Информационная безопасность в деятельности органов внутренних дел». - М.: Изд-во ИНИОН РАН, 2000.

11. Гафнер В.В. «Информационная безопасность» - Ростов на Дону: Феникс, 2010.

12. Горохов П. К. «Информационная безопасность». - М.: Радио и связь, 2012.

13. «Комплексный технический контроль эффективности мер безопасности систем управления в органах внутренних дел» Под ред. Чекалина А. - М.: 2006.

14. Партыка Т. Л., Попов И.И. «Информационная безопасность» - Москва: Форум, 2012.

15. Расторгуев С. П. «Основы информационной безопасности» - Москва: Академия, 2009.

16. Смирнов А. А. «Обеспечение информационной безопасности в условиях виртуализации общества». - М.: Юнити-Дана, 2012.

17. Тепляков А. А., Орлов А. В. «Основы безопасности и надежности информационных систем» - Мн.: Академия управления при Президенте Республики Беларусь, 2010.

18. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Словарь терминов и опреде- лений. Издание 2-е, дополненное. М., МГФ «Знание», 1999.

19. «Информация и собственность. Защита прав создателей и пользователей программ для ЭВМ и баз данных». Терещенко Л.К.

20. Базаров, Т.Ю. «Управление персоналом. Практикум»: Учебное пособие/Т.Ю. Базаров. - М.: ЮНИТИ, 2014.

21. Липаев В.В. «Документирование и управление конфигурацией программных средств», М., «Синтег», 1998

22. «Административная деятельность органов внутренних дел». А.П.Корнеева. – М.: МЮНМВД России, 1996.

23. Матижев П.В. «Основы информационной безопасности в органах внутренних дел». Учебное пособие - Чебоксары, 2008.

24. Стрельцов А. А. «Обеспечение информационной безопасности России. Теоретические и методологические основы», МЦНМО, 2002

25. Черняк Ю.Д. «Информация и управление» Москва, 2004.

26. Н.И. Журавленко, В.Е. Кадулин, К.К. Борзунов. «Основы информационной безопасности»: Учебное пособие. – М.: МосУ МВД России. 2007. С.-86.

27. Мандиа К. «Защита от вторжений. Расследование компьютерных преступлений». – СПб.: Лори, 2005.

28. «Теоретические основы информатики и информационная безопасность: монография» под ред. В. А. Минаева и В.Н. Саблина.— М.: Радио и связь, 2000.

29. Шевцов А. В. «Особенности полномочий органов внутренних дел по реализации регионального законодательства об административной ответственности», Российский следователь. - 2010.

30. Б. Анин. «Защита компьютерной информации». Спб. 2000,.

31. Скляров Д.В. «Искусство защиты и взлома информации». – Спб., 2004

32. Домарев В. В. «Защита информации и безопасность компьютерных систем». – К.: Издательство «Диа-Софт», 1999.

33. Козлов Ю.М. Административное право. – М.: Юристъ, 1999.