Е.В. Киргизова, А.В. Рубцов, С.С. Ахтамова

ИФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Министерство науки и высшего образования РФ
Сибирский федеральный университет
Лесосибирский педагогический институт

Е.В. Киргизова, А.В. Рубцов, С.С. Ахтамова

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебное пособие

Рекомендовано УМО РАЕ по классическому университетскому и техническому образованию в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению 44.03.01 – «Педагогическое образование» профиль «Информатика»; по направлению 44.03.05 – «Педагогическое образование» профиль «Информатика и экономика; по направлению 09.03.02 – «Информационные системы и технологии» профиль обучения «Информационно-управляющие системы» (Протокол № 672 от 27.11.2017 г.)

Красноярск-Лесосибирск, 2018

УДК 004.4, 004.7
ББК 32.973-018.2
К43

Рецензенты:
Н.И. Пак, д-р пед. наук, профессор (Красноярский государственный педагогический институт им. В.П. Астафьева);
К.В. Сафонов, д-р физ.-мат. наук, профессор**,** академик Международной академии информатизации (Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева)

К43 Киргизова Е.В.Информационная безопасность: учеб. пособие / Е.В. Киргизова, А. В. Рубцов, С.С. Ахтамова – Красноярск: Сибирский федеральный университет, 2018. – 160 с.

Учебное пособие подготовлено с учетом программ дисциплин «Методы и средства защиты информации», «Информационная безопасность и защита информации» для направлений подготовки 44.03.01 «Педагогическое образование» профиль «Информатика», 44.03.05 «Педагогическое образование» профиль «Информатика и экономика» и 09.03.02 – «Информационные системы и технологии» профиль «Информационно-управляющие системы».

В учебном пособии рассмотрены основные теоретические вопросы информационной безопасности и защиты информации: понятия информационной безопасности и защиты информации, структура и содержание угроз защищаемой информации, виды, методы и средства защиты информации, ресурсное обеспечение защиты информации. Учебное пособие предназначено для студентов и преподавателей, занимающихся изучением и преподаванием дисциплин, связанных с информационной безопасностью и средствами ее защиты.

ISBN 978-5-7638-3807-7

УДК 004.4, 004.7
ББК 32.973-018.2

Содержание

Введение

В современном информационном обществе информация превратилась в особый ресурс любой деятельности, следовательно, как и всякий другой ресурс, нуждается в защите, в обеспечении ее сохранности, целостности и безопасности. Развитие информационных технологий, их проникновение во все сферы человеческой деятельности приводит к тому, что проблемы информационной безопасности с каждым годом становятся всё более и более актуальными – и одновременно более сложными. Технологии обработки информации непрерывно совершенствуются, а вместе с ними меняются и практические методы обеспечения информационной безопасности. Действительно, универсальных методов защиты не существует, во многом успех при построении механизмов безопасности для реальной системы будет зависеть от её индивидуальных особенностей, учёт которых плохо подаётся формализации. Поэтому часто информационную безопасность рассматривают как некую совокупность неформальных рекомендаций по построению систем защиты информации того или иного типа. Однако всё обстоит несколько сложнее. За практическими приёмами построения систем защиты лежат общие закономерности, которые не зависят от технических особенностей их реализации. Такие универсальные принципы и делают информационную безопасность самостоятельной научной дисциплиной – и именно им посвящено учебное пособие.

Главная цель настоящего учебного пособия дать обучаемым азы, основы информационной безопасности и защиты информации, определить основные направления развития этой области знаний. В рамках образовательной программы сформировать у них элементы «информационной культуры».

Предлагаемое вниманию читателя учебное пособие посвящено систематическому изложению и анализу современных методов, средств и технологий защиты информации в компьютерных системах и сетях. Авторы старались изложить материал максимально доступно без потери в качестве.

Учебное пособие состоит из двух частей. В первой части рассматриваются общие положения теории информационной безопасности и универсальные подходы к построению систем защиты от основных классов угроз – конфиденциальности, целостности и доступности информации; стандарты информационной безопасности. Во второй части представлен комплекс лабораторных работ, обеспечивающий применение теоретических знаний при выполнении практических заданий.

1. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Основные понятия сферы информационной безопасности. Введение в проблематику вопроса

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

В то время как информационная безопасность - это состояние защищённости информационной среды, защита информации представляет собой деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение этого состояния.

Информационная безопасность организации - целенаправленная деятельность её органов и должностных лиц с использованием разрешённых сил и средств по достижению состояния защищённости информационной среды организации, обеспечивающее её нормальное функционирование и динамичное развитие.

Кортеж защиты информации - это последовательность действий для достижения определённой цели.

Информационная безопасность государства - состояние сохранности информационных ресурсов государства и защищённости законных прав личности и общества в информационной сфере.

В современном социуме информационная сфера имеет две составляющие: информационно-техническую (искусственно созданный человеком мир техники, технологий и т.п.) и информационно-психологическую (естественный мир живой природы, включающий и самого человека). Соответственно, в общем случае информационную безопасность общества (государства) можно представить двумя составными частями: информационно-технической безопасностью и информационно-психологической (психофизической) безопасностью.

Понятие информационной безопасности

Словосочетание «информационная безопасность» в разных контекстах может иметь различный смысл. В Доктрине информационной безопасности Российской Федерации термин «информационная безопасность» используется в широком смысле. Имеется в виду состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

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

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

Под информационной безопасностью мы будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести

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

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

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

Из этого положения можно вывести два важных следствия:

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

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

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

Согласно определению информационной безопасности, она зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электро-, водо- и теплоснабжения, 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 ИБ перед существительным «ущерб» стоит прилагательное «неприемлемый». Очевидно, застраховаться от всех видов ущерба невозможно, тем более невозможно сделать это экономически целесообразным способом, когда стоимость защитных средств и мероприятий не превышает размер ожидаемого ущерба. Значит, с чем-то приходится мириться и защищаться следует только от того, с чем смириться никак нельзя. Иногда таким недопустимым ущербом является нанесение вреда здоровью людей или состоянию окружающей среды, но чаще порог неприемлемости имеет материальное (денежное) выражение, а целью защиты информации становится уменьшение размеров ущерба до допустимых значений.

Основные составляющие информационной безопасности

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

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

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

Поясним понятия доступности, целостности и конфиденциальности.

Доступность – это возможность за приемлемое время получить требуемую информационную услугу. Под целостностью подразумевается актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

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

Информационные системы создаются (приобретаются) для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, это, очевидно, наносит ущерб всем субъектам информационных отношений. Поэтому, не противопоставляя доступность 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, которыми пользуется большое количество людей (продажа железнодорожных и авиабилетов, банковские услуги и т.п.).

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

Целостность оказывается важнейшим аспектом ИБ в тех случаях, когда информация служит «руководством к действию». Рецептура лекарств, предписанные медицинские процедуры, набор и характеристики комплектующих изделий, ход технологического процесса – все это примеры информации, нарушение целостности которой может оказаться в буквальном смысле смертельным. Неприятно и искажение официальной информации, будь то текст закона или страница Web-сервера какой-либо правительственной организации. Конфиденциальность – самый проработанный у нас в стране аспект информационной безопасности. К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем наталкивается в России на серьезные трудности. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные препоны и технические проблемы.

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

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

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

Основные определения и критерии классификации угроз

Угроза - это потенциальная возможность определенным образом нарушить информационную безопасность.

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

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

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

Если речь идет об ошибках вПО, то окно опасности «открывается» с появлением средств использования ошибки и ликвидируется при наложении заплат, ее исправляющих.

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

должно стать известно о средствах использования пробела в защите;

должны быть выпущены соответствующие заплаты;

заплаты должны быть установлены в защищаемой ИС.

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

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

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

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

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

Угрозы можно классифицировать по нескольким критериям:

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

по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);

по способу осуществления (случайные/преднамеренные действия природного/техногенного характера);

по расположению источника угроз (внутри/вне рассматриваемой ИС).

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

Основные угрозы конфиденциальности

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

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

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

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

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

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

Перехват данных - очень серьезная угроза, и если конфиденциальность действительно является критичной, а данные передаются по многим каналам, их защита может оказаться весьма сложной и дорогостоящей. Технические средства перехвата хорошо проработаны, доступны, просты в эксплуатации, а установить их, например на

кабельную сеть, может кто угодно, так что эту угрозу нужно принимать во внимание по отношению не только к внешним, но и к внутренним коммуникациям.

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

Опасной нетехнической угрозой конфиденциальности являются методы морально-психологического воздействия, такие как маскарад - выполнение действий под видом лица, обладающего полномочиями для доступа к данным.

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.

1.2. Исторический аспект информационной безопасности

Учитывая влияние на трансформацию идей информационной безопасности, в развитии средств информационных коммуникаций можно выделить несколько этапов:

I этап - до 1816 года - характеризуется использованием естественно возникавших средств информационных коммуникаций. В этот период основная задача информационной безопасности заключалась в защите сведений о событиях, фактах, имуществе, местонахождении и других данных, имеющих для человека лично или сообщества, к которому он принадлежал, жизненное значение.

II этап - с 1816 года - связан с началом использования искусственно создаваемых технических средств электро- и радиосвязи. Для обеспечения скрытности и помехозащищенности радиосвязи необходимо было использовать опыт первого периода информационной безопасности на более высоком технологическом уровне, а именно применение помехоустойчивого кодирования сообщения (сигнала) с последующим декодированием принятого сообщения (сигнала).

III этап - с 1935 года - связан с появлением радиолокационных и гидроакустических средств. Основным способом обеспечения информационной безопасности в этот период было сочетание организационных и технических мер, направленных на повышение защищенности радиолокационных средств от воздействия на их приемные устройства активными маскирующими и пассивными имитирующими радиоэлектронными помехами.

IV этап - с 1946 года - связан с изобретением и внедрением в практическую деятельность электронно-вычислительных машин (компьютеров). Задачи информационной безопасности решались, в основном, методами и способами ограничения физического доступа к оборудованию средств добывания, переработки и передачи информации.

V этап - с 1965 года - обусловлен созданием и развитием локальных информационно-коммуникационных сетей. Задачи информационной безопасности также решались, в основном, методами и способами физической защиты средств добывания, переработки и передачи информации, объединённых в локальную сеть путём администрирования и управления доступом к сетевым ресурсам.

VI этап - с 1973 года - связан с использованием сверхмобильных коммуникационных устройств с широким спектром задач. Угрозы информационной безопасности стали гораздо серьёзнее. Для обеспечения информационной безопасности в

компьютерных системах с беспроводными сетями передачи данных потребовалась разработка новых критериев безопасности. Образовались сообщества людей - хакеров, ставящих своей целью нанесение ущерба информационной безопасности отдельных пользователей, организаций и целых стран. Информационный ресурс стал важнейшим ресурсом государства, а обеспечение его безопасности - важнейшей и обязательной составляющей национальной безопасности. Формируется информационное право - новая отрасль международной правовой системы.

VII этап - с 1985 года - связан с созданием и развитием глобальных информационно-коммуникационных сетей с использованием космических средств обеспечения. Можно предположить что очередной этап развития информационной безопасности, очевидно, будет связан с широким использованием сверхмобильных коммуникационных устройств с широким спектром задач и глобальным охватом в пространстве и времени, обеспечиваемым космическими информационно-коммуникационными системами. Для решения задач информационной безопасности на этом этапе необходимо создание макросистемы информационной безопасности человечества под эгидой ведущих международных форумов.

Человечество изобрело большое число способов секретного письма, например симпатические чернила, которые исчезают вскоре после написания ими текста или невидимы с самого начала, «растворение» нужной информации в сообщении большего размера с совершенно «посторонним» смыслом, подготовка текста при помощи непонятных знаков.

Криптография возникла именно как практическая дисциплина, изучающая и разрабатывающая способы шифрования сообщений, то есть при передаче сообщений нужно не скрывать сам факт передачи, а сделать сообщение недоступным посторонним. Для этого сообщение должно быть записано так, чтобы с его содержимым не мог ознакомиться никто за исключением самих корреспондентов.

Появление в середине XX столетия первых ЭВМ кардинально изменило ситуацию - практическая криптография сделала в своем развитии огромный скачок и термин «криптография» далеко ушел от своего первоначального значения - «тайнопись», «тайное письмо». Сегодня эта дисциплина объединяет методы защиты информационных взаимодействий совершенно различного характера, опирающиеся на преобразование данных по секретным алгоритмам, включая алгоритмы, использующие секретные параметры. Термин «информационное взаимодействие» или «процесс информационного взаимодействия» здесь обозначает такой процесс взаимодействия двух и более субъектов, основным содержанием которого служит передача и/или обработка информации.

Базовых методов преобразования информации, которыми располагает современная криптография, немного, среди них: шифрование (симметричное и несимметричное); вычисление хэш-функций; генерация электронно-цифровой подписи; генерация последовательности псевдослучайных чисел.

Базовые криптографические методы являются «кирпичами» для создания прикладных систем. На сегодняшний день криптографические методы применяются для идентификации и аутентификации пользователей, защиты каналов передачи данных от навязывания ложных данных, защиты электронных документов от копирования и подделки.

1.3. Стандарты и нормативная база информационной безопасности

Нормативно-методические документы

Методические документы государственных органов России:

- Доктрина информационной безопасности РФ;
- Руководящие документы ФСТЭК (Гостехкомиссии России);
- Приказы ФСБ;

– Стандарты информационной безопасности, из которых выделяют:
– Международные стандарты;
– Государственные (национальные) стандарты РФ;
– Рекомендации по стандартизации;
– Методические указания.
– ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»;
– ГОСТ Р 34.10-94 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма»;
– ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования»;
– ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования».
– Гражданский кодекс Российской Федерации. Часть I, гл. 9, ст. 160. «Письменная форма сделки».
– Законы Российской Федерации в области защиты информации (защиты государственной тайны)
– Закон РФ от 23 сентября 1992 г. N 3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных»;
– Закон РФ от 19 февраля 1993г. N 4524-1 «О федеральных органах правительственной связи и информации (с изменениями от 24 декабря 1993 года, по состоянию на 1 апреля 1994 года)»;
– Закон РФ от 10 июня 1993 года N 5151-1 «О сертификации продуктов и услуг»;
– Закон РФ от 10 июня 1993 года N 5154-1 «О стандартизации»;
– Закон РФ от 01 июля 1993 г. N 5306-1 «О внесении изменений и дополнений в Закон Российской Федерации «О федеральных органах государственной безопасности»;
– Закон РФ от 21 июля 1993 года N 5485-1 «О Государственной тайне»;
– Закон РФ от 20 января 1995 года N 15-ФЗ «О связи»;
– Закон РФ от 20 февраля 1995 г. N 24-ФЗ «Об информации, информатизации и защите информации» (с комментариями)
– Закон РФ от 03 апреля 1995г. N 40-ФЗ «Об органах Федеральной службы безопасности в Российской Федерации»;
– Закон РФ от 4 июля 1996 года N 85-ФЗ «Об участии в международном информационном обмене»
– Указы Президента РФ в области защиты информации (защиты государственной тайны)
– Указ Президента РФ от 7 октября 1993г. N 1607 «О государственной политике в области охраны авторского права и смежных прав»;
– Указ Президента РФ от 31 декабря 1993г. N 2334 «О дополнительных гарантиях прав граждан на информацию»;
– Указ Президента РФ от 20 января 1994г. N 170 «Об основах государственной политики в сфере информатизации»;
– Указ Президента РФ от 3 апреля 1995 г. N 334 «О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации»;
– Указ Президента РФ от 3 июля 1995 г. N 662 «О мерах по формированию общероссийской телекоммуникационной системы и обеспечению прав собственников при хранении ценных бумаг и расчетах на фондовом рынке Российской Федерации»;

– Указ Президента РФ от 30 ноября 1995г. N 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне»;

– Указ Президента РФ от 26 августа 1996г. N 1268 «О контроле за экспортом из Российской Федерации товаров и технологий двойного назначения».

– Список товаров и технологий двойного назначения, экспорт которых контролируется;

– Список товаров и технологий двойного назначения, экспорт которых контролируется (Продолжение);

– Указ Президента РФ от 6 марта 1997 г. N 188 «Об утверждении перечня сведений конфиденциального характера»;

– Указ Президента РФ от 30 мая 1997 года N 226-рп «О перечне должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне».

– Постановления Правительства РФ в области защиты информации (защиты государственной тайны)

– Постановление Правительства РФ от 24 декабря 1994 г. N 1418 «О лицензировании отдельных видов деятельности» (с изменениями от 5 мая, 3 июня, 7 августа,12 октября 1995г.);

– Постановление Правительства РФ от 15 апреля 1995 года N 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и(или) оказанием услуг по защите государственной тайны»;

– Постановление Правительства РФ от 26 июня 1995 г. N 608 «О сертификации средств защиты информации»;

– Постановление Правительства РФ от 04 сентября 1995г. N 870 «Об утверждении правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности».

Защита от несанкционированного доступа к информации. Термины и определения. ГОСТЕХКОМИССИЯ РОССИИ

– Постановление Правительства РФ от 30 апреля 1997 г. N 513 «О внесении дополнения в Положение о лицензировании»

– Нормативные документы в области защиты информации от несанкционированного доступа

Вопросы сертификации и лицензирования

– «О лицензировании и сертификации в области защиты информации», О.А. Беззубцев и А.Н. Ковалев.

– «Проблемы проведения технической экспертизы средств защиты информации и регулирования их ввоза-вывоза», О.А. Беззубцев и А.Н. Ковалев.

– «О порядке лицензирования деятельности» (письмо Президента АРБ С.Е. Егорова и ответ на него Статс-секретаря, первого заместителя ген.директора ФАПСИ В.И. Маркоменко).

– Система сертификации средств криптографической защиты информации.

– Информационные материалы о лицензировании Федеральным агентством правительственной связи и информации при Президенте Российской Федерации отдельных видов деятельности, связанных с сертифицированными ФАПСИ шифровальными средствами, при защите информации по уровню «С».

– Определение шифровальных средств.

– Образец заявления о выдаче лицензии на осуществление деятельности, связанной с конкретными сертифицированными шифровальными средствами в данной сети (системе).

– Требования к заявителю на право установки (инсталляции), эксплуатации сертифицированных ФАПСИ шифровальных средств и предоставления услуг по шифрованию информации при защите информации по уровню «С».

– Требования к заявителю на право реализации шифровальных средств.

– Требования к соискателю лицензии Федерального агентства на право распространения, технического обслуживания и предоставления услуг в области шифрования информации с применением несертифицированных ФАПСИ шифровальных средств иностранного производства.

– Представляемый заявителем перечень сведений, обосновывающих наличие на предприятии условий для установки (инсталляции), эксплуатации сертифицированных ФАПСИ шифровальных средств и предоставления услуг по шифрованию информации при защите информации по уровню «С».

– Положение о государственном лицензировании деятельности в области защиты информации.

Государственные органы РФ, контролирующие деятельность в области защиты информации:

Комитет Государственной думы по безопасности;

Совет безопасности России;

Федеральная служба по техническому и экспортному контролю (ФСТЭК России);

Федеральная служба безопасности Российской Федерации (ФСБ России);

Служба внешней разведки Российской Федерации (СВР России);

Министерство обороны Российской Федерации (Минобороны России);

Министерство внутренних дел Российской Федерации (МВД России);

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор);

Службы, организующие защиту информации на уровне предприятия;

Служба экономической безопасности;

Служба безопасности персонала (Режимный отдел);

Отдел кадров;

Служба информационной безопасности.

Организационно-технические и режимные меры и методы

Для описания технологии защиты информации конкретной информационной системы обычно строится так называемая Политика информационной безопасности, или Политика безопасности рассматриваемой информационной системы.

Политика безопасности (информации в организации) (англ. Organizational security policy) - совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Политика безопасности информационно-телекоммуникационных технологий (англ. ICT security policy) - правила, директивы, сложившаяся практика, которые определяют, как в пределах организации и её информационно-телекоммуникационных технологий управлять, защищать и распределять активы, в том числе критичную информацию.

Для построения Политики информационной безопасности рекомендуется отдельно рассматривать следующие направления защиты информационной системы:

защита объектов информационной системы;

защита процессов, процедур и программ обработки информации;

защита каналов связи;

подавление побочных электромагнитных излучений;

управление системой защиты.

При этом по каждому из перечисленных выше направлений Политика информационной безопасности должна описывать следующие этапы создания средств защиты информации:

определение информационных и технических ресурсов, подлежащих защите;

выявление полного множества потенциально возможных угроз и каналов утечки информации;

проведение оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки;

определение требований к системе защиты;

осуществление выбора средств защиты информации и их характеристик;

внедрение и организация использования выбранных мер, способов и средств защиты;

осуществление контроля целостности и управление системой защиты.

Политика информационной безопасности оформляется в виде документированных требований на информационную систему. Документы обычно разделяют по уровням описания (детализации) процесса защиты.

Документы верхнего уровня Политики информационной безопасности отражают позицию организации к деятельности в области защиты информации, её стремление соответствовать государственным, международным требованиям и стандартам в этой области. Подобные документы могут называться «Концепция ИБ», «Регламент управления ИБ», «Политика ИБ», «Технический стандарт ИБ» и т. п. Область распространения документов верхнего уровня обычно не ограничивается, однако данные документы могут выпускаться и в двух редакциях - для внешнего и внутреннего использования.

К среднему уровню относят документы, касающиеся отдельных аспектов информационной безопасности. Это требования на создание и эксплуатацию средств защиты информации, организацию информационных и бизнес-процессов организации по конкретному направлению защиты информации. Например: безопасность данных, безопасность коммуникаций, использование средств криптографической защиты, контентная фильтрация и т. п. Подобные документы обычно издаются в виде внутренних технических и организационных политик (стандартов) организации. Все документы среднего уровня политики информационной безопасности конфиденциальны.

В политику информационной безопасности нижнего уровня входят регламенты работ, руководства по администрированию, инструкции по эксплуатации отдельных сервисов информационной безопасности.

Программно-технические способы и средства обеспечения информационной безопасности

В литературе предлагается следующая классификация средств защиты информации:

Средства защиты от несанкционированного доступа (НСД).

Средства авторизации.

Мандатное управление доступом.

Избирательное управление доступом.

Управление доступом на основе ролей.

Журналирование (также называется Аудит).

Системы анализа и моделирования информационных потоков (CASE-системы).

Системы мониторинга сетей:

Системы обнаружения и предотвращения вторжений (IDS/IPS).

Системы предотвращения утечек конфиденциальной информации (DLP-системы).

Анализаторы протоколов.

Антивирусные средства.

Межсетевые экраны.

Криптографические средства:

Шифрование.

Цифровая подпись.

Системы резервного копирования.
Системы бесперебойного питания:
Источники бесперебойного питания.
Резервирование нагрузки.
Генераторы напряжения.
Системы аутентификации:
Пароль.
Ключ доступа (физический или электронный).
Сертификат.
Биометрия.
Средства предотвращения взлома корпусов и краж оборудования.
Средства контроля доступа в помещения.
Инструментальные средства анализа систем защиты:
Мониторинговый программный продукт.

Эталоном организации информационной безопасности и защиты информации в организации является серия международных стандартов, включающая стандарты по информационной безопасности опубликованные совместно Международной Организацией по Стандартизации (ISO) и Международной Электротехнической Комиссии (IEC) - ISO/IEC 27000. Серия содержит лучшие практики и рекомендации в области информационной безопасности для создания, развития и поддержания Системы Менеджмента Информационной Безопасности.

1.4. Категории информационной безопасности

Информация с точки зрения информационной безопасности обладает следующими категориями:

конфиденциальность – гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена; нарушение этой категории называется хищением либо раскрытием информации;

целостность – гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений; нарушение этой категории называется фальсификацией сообщения;

аутентичность – гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор; нарушение этой категории также называется фальсификацией, но уже автора сообщения;

апеллируемость – довольно сложная категория, но часто применяемая в электронной коммерции, гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно заявленный человек и не может являться никто другой; отличие этой категории от предыдущей в том, что при подмене автора кто-то другой пытается заявить, что он автор сообщения, а при нарушении апеллируемости – сам автор пытается «откреститься» от своих слов, подписанных им однажды.

В отношении информационных систем применяются иные категории:

– надежность – гарантия того, что система ведет себя в нормальном и внештатном режимах так, как запланировано;

– точность – гарантия точного и полного выполнения всех команд;

– контроль доступа – гарантия того, что различные группы лиц имеют различный доступ к информационным объектам, и эти ограничения доступа постоянно выполняются;

– контролируемость – гарантия того, что в любой момент может быть произведена полноценная проверка любого компонента программного комплекса;

– контроль идентификации – гарантия того, что клиент, подключенный в данный момент к системе, является именно тем, за кого себя выдает;

– устойчивость к умышленным сбоям – гарантия того, что при умышленном внесении ошибок в пределах заранее оговоренных норм система будет вести себя так, как оговорено заранее.

Основные определения и критерии классификации угроз.

Угроза - это потенциальная возможность определенным образом нарушить информационную безопасность.

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

Атака на информацию – это умышленное нарушение правил работы с информацией. На сегодняшний день примерно 90 % всех атак на информацию производят ныне работающие либо уволенные с предприятия сотрудники. При хранении, поддержании и предоставлении доступа к любому информационному объекту его владелец либо уполномоченное им лицо, устанавливает явно либо самоочевидно набор правил по работе с информацией. Умышленное их нарушение классифицируется как информационная атака.

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

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

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

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

1) должно стать известно о средствах использования пробела в защите;
2) должны быть выпущены соответствующие заплаты;
3) заплаты должны быть установлены в защищаемой ИС.

Угрозы можно классифицировать по нескольким критериям:

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

2) по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);

3) по способу осуществления (случайные/преднамеренные действия природного/техногенного характера);

4) по расположению источника угроз (внутри/вне рассматриваемой ИС).

Наиболее распространенные угрозы доступности

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

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

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

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

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

– отказ пользователей;

– внутренний отказ информационной системы;

– отказ поддерживающей инфраструктуры.

Обычно применительно к пользователям рассматриваются следующие угрозы:

– нежелание работать с информационной системой (чаще всего проявляется при необходимости осваивать новые возможности и при расхождении между запросами пользователей и фактическими возможностями и техническими характеристиками);

– невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т.п.);

– невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т.п.).

Основными источниками внутренних отказов являются:

– отступление (случайное или умышленное) от установленных правил эксплуатации;

– выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.);

– ошибки при (пере)конфигурировании системы;

– отказы программного и аппаратного обеспечения;

– разрушение данных;

– разрушение или повреждение аппаратуры.

По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

– нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования;

– разрушение или повреждение помещений;

– невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т.п.).

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

– испортить оборудование;

– встроить логическую бомбу, которая со временем разрушит программы и/или данные;

– удалить данные.

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

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

1.5. Основные виды атак на АС

Атака на компьютерную систему – это действие, предпринятое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости.

Основные виды атак:

1. Вмешательство человека в работу АС. К этому виду относятся организационные средства нарушения безопасности АС (кража носителей информации, несанкционированный доступ (НСД) к устройствам хранения и обработки информации, порча оборудования и т.д.) и осуществление нарушителем НСД к программным компонентам АС (все способы НСД в АС, а также способы получения нарушителем незаконных прав доступа к компонентам АС). Меры, противостоящие таким атакам, носят организационный характер (охрана, режим доступа к АС), а также включают в себя совершенствование систем обнаружения попыток атак (попыток подбора паролей).

2. Аппаратно - техническое вмешательство в работу АС. Т.е. нарушение безопасности и целостности информации вАС с помощью технических средств, например получение информации по электромагнитному излучению устройств АС. Защита от таких угроз, кроме организационных мер, предусматривает соответствующие аппаратные (экранирование излучений аппаратуры) и программные меры (шифрация).

3. Разрушающее воздействие на программные компоненты АС с помощью программных средств (разрушающих программных средств (РПС)). К ним относятся компьютерные вирусы, троянские кони, закладки, «логическая бомба», «часовая мина». Последний вид атак развивается более динамично, используя все последние достижения в области информационных достижений. Остановимся на нем более детально и дадим краткое описания некоторых РПС.

«Логические бомбы» и «часовые мины» - это РПС, которые не выполняют никаких функций до наступления определенного события в системе, после чего «срабатывают», что, как правило, заключается в серьезных нарушениях работы системы, уничтожении информации.

«Троянский конь» - программа, содержащая в себе некоторую разрушающую функцию, которая активизируется при наступлении некоторого условного срабатывания. Обычно такие программы маскируются под какие-нибудь полезные утилиты, игровые программы, картинки или музыку.

Закладки также содержат некоторую функцию, наносящую ущерб АС, но эта функция, наоборот, старается быть как можно незаметнее, т.к. чем дольше программа не будет вызывать подозрений, тем дольше закладка сможет работать.

В качестве примера приведем некоторые функции, реализуемые троянскими конями и закладками:

1. Уничтожение информации. Конкретный выбор объектов и способов уничтожения зависит от фантазии автора такой программы и возможностей ОС.

2. Перехват и передача информации.

3. Целенаправленная модификация кода программы, интересующая нарушителя.

Обычно это программы, реализующие функции безопасности и защиты.

Компьютерный вирус – программа, которая может заражать другие программы, модифицируя их посредством добавления своей, возможно измененной, копии. Способен к саморазмножению, при этом «копии» вируса могут структурно и функционально различаться между собой.

В настоящее время в мире насчитывается более 40 тысяч только зарегистрированных компьютерных вирусов. Все компьютерные вирусы могут быть классифицированы по следующим признакам:

1) по среде обитания;

2) по способу заражения;

3) по степени опасности деструктивных (вредительских) воздействий;

4) по алгоритму функционирования.

По среде обитания вирусы делятся также на:

1) сетевые;

2) файловые;

3) загрузочные;

4) комбинированные.

Средой обитания сетевых вирусов являются элементы компьютерных сетей. Файловые вирусы размещаются в исполняемых файлах. Загрузочные вирусы находятся в загрузочных секторах (областях) внешних запоминающих устройств (boot - секторах). Комбинированные вирусы размещаются в нескольких средах обитания. Примером таких вирусов служат загрузочные файловые вирусы. Эти вирусы могут размещаться как в загрузочных секторах накопителей на магнитных дисках, так и в теле загрузочных файлов.

По способу заражения среды обитания компьютерные вирусы делятся на:

1) резидентные;

2) нерезидентные.

Резидентные вирусы после их активации полностью или частично перемещаются из среды обитания (сеть, загрузочный сектор, файл) в оперативную память ЭВМ. Эти вирусы, используя привилегированные режимы работы, разрешенные только операционной системе, заражают среду обитания и при выполнении определенных условий реализуют деструктивную функцию. Нерезидентные вирусы попадают в оперативную память ЭВМ только на время их активности, в течение которого выполняют вредительскую функцию и функцию заражения. Затем вирусы полностью покидают оперативную память, оставаясь в среде обитания. Если вирус помещает в оперативную память программу, которая не заражает среду обитания, то такой вирус считается нерезидентным.

Арсенал вредительских возможностей вирусов весьма обширен. Деструктивные возможности вирусов зависят от целей и квалификации их создателя, а также от особенностей компьютерных систем.

По степени опасности для информационных ресурсов пользователя компьютерные вирусы делятся на:

1) безвредные вирусы;

2) опасные вирусы;

3) очень опасные вирусы.

Безвредные вирусы создаются авторами, которые не ставят себе цели нанести какой-либо ущерб ресурсам компьютерной системы (АС). Деструктивное воздействие таких вирусов сводиться к выводу на экран монитора невинных картинок, исполнению музыкальных

фрагментов. Но при всей своей безобидности они расходуют ресурсы системы, в какой- то степени снижая эффективность функционирования, могут содержать ошибки, приводящие к нарушению алгоритма работы системы.

К опасным относятся вирусы, которые вызывают существенное снижение эффективности АС, но не приводящие к нарушению целостности и конфиденциальности информации, хранящейся в запоминающих устройствах. В пример можно привести вирусы, вызывающие необходимость повторного выполнения программ, перезагрузки операционной системы.

Очень опасными следует считать вирусы, вызывающие нарушение конфиденциальности, уничтожение, необратимую модификацию информации, а также вирусы, блокирующие доступ к информации, приводящие к отказу аппаратных средств. Одним из основных условий безопасной работы АС является соблюдение ряда правил.

Правило 1: периодически обновляйте вашу антивирусную программу. Антивирусные сканеры способны защищать только от тех компьютерных вирусов, данные

о которых содержатся в антивирусной базе. Конечно, существуют механизмы поиска и неизвестных вирусов (т.е. тех, описаний которых нет в антивирусной базе). Однако это все равно слишком мало для того, чтобы считаться абсолютной защитой.

В связи с этим первоочередную важность приобретает необходимость регулярно обновлять антивирусные базы. Чем чаще будете это делаться, тем более защищенным будет рабочее место. Наиболее оптимальным решением является ежедневная загрузка обновлений, хотя бывают случаи, когда за день появляется сразу несколько обновлений. В связи с этим, рекомендуют настроить внутренний планировщик, присутствующий в большинстве современных антивирусных программ, на автоматическую загрузку обновлений 2 или 3 раза вдень: утром, днем и вечером.

Правило 2: будьте осторожны с файлами в письмах электронной почты.

Вряд ли стоит акцентировать внимание на том, что ни в коем случае нельзя запускать программы, присланные неизвестным лицом. Это правило является общеизвестным и не нуждается в пояснениях.

Другое дело файлы, полученные от знакомых, коллег, друзей. Во-первых, посланные ими программы могут быть инфицированы. Во-вторых, знакомые могут даже и не знать, что сих компьютера несанкционированно отправляются письма: вирус может это делать от чужого имени незаметно для владельца компьютера. Именно таким способом, к примеру, распространялись такие известные вирусы, как LoveLetter, Melissa и многие другие. Они незаметно получали доступ к адресной книге почтовой программы Outlook и рассылали свои копии по найденным адресам электронной почты, сопровождая послания завлекательными комментариями, призывающими запустить вложенный файл.

Не менее важным моментом является кажущаяся безопасность вложенных файлов определенного формата. Думаете, файлы с расширением PIF, GIF, TXT не могут содержать вредоносных программ? Даже в таких «безобидных» программах могут быть замаскированы вирусы.

Правило 3: ограничьте круг пользующихся компьютером.

Идеальным вариантом является ситуация, когда никто, кроме самого владельца, не имеет доступа к компьютеру. Однако если это невозможно, то необходимо четко разграничить права доступа и определить круг разрешенных действий для других лиц. В первую очередь это касается работы с мобильными носителями, Интернет и электронной почтой. В данном случае важно контролировать все источники вирусной опасности и отрезать от них других пользователей.

Правило 4: своевременно устанавливайте «заплатки» установленному ПО.

Многие вирусы используют ―дыры‖ в системах защиты операционных систем и приложений. Антивирусные программы способны защищать от такого типа вредоносных программ, даже если на компьютере не установлена соответствующая –заплатка, закрывающая ―дыру. Несмотря на это, рекомендуется регулярно проверять Web-сайты производителей установленного программного обеспечения и следить за выпуском новых - заплаток. В первую очередь, это правило относится к операционной системе Windows и другим программам корпорации Microsoft. Нет, совсем не потому, что у этой компании самые худшие продукты, а потому, что они наиболее распространены и, соответственно, получают больше всего внимания со стороны создателей вирусов.

Правило 5: обязательно проверяйте мобильные носители информации.

Несмотря на то, что около 85 % всех зарегистрированных случаев заражения компьютерными вирусами приходятся на электронную почту и Интернет, не стоит забывать о таком традиционном способе транспортировки вредоносных кодов, как мобильные носители(дискеты, компакт-диски и т.п.). Перед тем, как начать их использовать на своем компьютере, необходимо тщательно проверить их антивирусной программой. Исключением могут быть разве что диски, предназначенные для форматирования.

Большую опасность представляют собой и столь широко распространенные в России пиратские компакт-диски. К примеру, проверка, проведенная «Лабораторией Касперского» в 2009 году, выявила факт присутствия вирусов на 23 % закупленных носителей. Вывод прост: тщательно проверять даже приобретенные компакт-диски.

Правило 6: будьте осторожны с источниками, заслуживающими доверия.

Никто не застрахован от компьютерных вирусов. Это в равной мере относится к крупным компаниям-производителям программного и аппаратного обеспечения. Нередко случается, что посетителям их сайтов предлагаются зараженные программы. Показательный случай, когда в течение нескольких недель на сайте Microsoft находился документ Word, зараженный макровирусом Concept.

Не менее редки случаи присутствия вирусов на дискетах с драйверами к аппаратному обеспечению, с лицензионным программным обеспечением. Часто случается, что компьютер, переданный на техническое обслуживание в ремонтную мастерскую, возвращается не совсем чистым. Не то чтобы на мониторе был толстый слой пыли, а на клавиатуре паутина (хотя такое тоже случается), а просто на диске заводятся вирусы. Как правило, это происходит из-за того, что ремонтники пользуются одними и теми же дискетами для загрузки программ для тестирования различных узлов компьютера. Таким образом, они очень быстро переносят компьютерную «заразу» с одних компьютеров на другие. Вывод состоит в том, что, получив компьютер из ремонта, не забудьте тщательно проверить его на наличие вирусов.

Все это делает необходимым проверять даже те данные, которые получены из источников, заслуживающих доверия. Вряд ли в данном случае стоит обвинять самих производителей, что они якобы нарочно стараются заразить компьютер: в каждой работе бывают осечки. Просто иногда они касаются и антивирусной безопасности.

Правило 7: сочетайте разные антивирусные технологии.

Не стоит ограничиваться классическим антивирусным сканером, запускаемым по требованию пользователя или при помощи встроенного планировщика событий. Существует ряд других, нередко более эффективных технологий, комбинированное использование которых способно практически гарантировать безопасную работу. К числу таких технологий относятся: во-первых, антивирусный монитор, постоянно присутствующий в памяти компьютера и проверяющий все используемые файлы в масштабе реального времени, в момент доступа к ним; во-вторых, ревизор изменений, который отслеживает все изменения на диске и немедленно сообщает, если в каком-либо из файлов поселился вирус; в-третьих, поведенческий блокиратор, обнаруживающий вирусы не по их уникальному коду, а по последовательности их действий. Сочетание описанных способов борьбы с вирусами является залогом успешной защиты от вредоносных программ.

Правило 8: всегда имейте при себе чистый загрузочный диск.

Часто происходит так, что вирусы лишают компьютеры возможности производить первоначальную загрузку. Иными словами, информация на диске остается в целости и сохранности, но операционная система теряет способность загружаться. Для успешного разрешения подобных проблем необходимо иметь специальную чистую дискету с установленной антивирусной программой. С ее помощью Вы сможете произвести загрузку и восстановить систему.

Правило 9: регулярное резервное копирование.

Это правило поможет сохранить данные не только в случае поражения компьютера каким-либо вирусом, но и в случае, если у компьютера произошла серьезная поломка в аппаратной части. Вряд ли кому-то хочется потерять результаты многолетних наработок вследствие произошедшего сбоя в системе вне зависимости от того, вызвано это вирусами или нет. Именно поэтому рекомендуют регулярно проводить копирование наиболее ценной информации на независимые носители.

Правило 10: не паникуйте.

Вирусы являются такими же программами, как, допустим, калькулятор или записная книжка Windows. Их отличительная черта в том, что вирусы способны размножаться (т.е. создавать свои копии), интегрироваться в другие файлы или загрузочные секторы и производить другие несанкционированные действия. Вирусы создаются самыми обычными людьми, и ничего потустороннего в них нет. Гораздо больший вред сможете принести, если испугаетесь и совершите необдуманные действия, направленные на нейтрализацию вируса. Если работаете в корпоративной сети, немедленно позовите системного администратора. Если же просто домашний пользователь, то свяжитесь с компанией, у которой приобрели антивирусную программу. Дайте возможность профессионалам позаботиться о вашей безопасности.

Существует еще один вид атаки, встречающийся в литературе под названием «атака по социальной психологии» или «Фишинг».

Фишинг (от англ. fishing – рыбная ловля, выуживание) – вид интернет мошенничества с использованием социальной инженерии для получения доступа к конфиденциальной информации пользователей – логинам и паролям.

Основной задачей фишинг-мошенника является получение вашего логина и пароля от определенного сайта с последующим их использованием, т.е это может быть логин и пароль вашего банковского кабинета или номер и пин-код вашей карточки для вывода ваших денег на свой счет. Также довольно часто используют фишинг для доступа к вашим аккаунтам в социальных сетях и т.д. В любом случае, если ваш пароль и логин стал известен мошенникам, последствия для вас будут не приятные.

Сделаем краткий обзор нескольких довольно часто встречающихся методов.

Звонок администратору – злоумышленник выбирает из списка сотрудников того, кто не использовал пароль для входа в течение нескольких дней (отпуск, отгулы, командировка) и кого администратор не знает по голосу. Затем следует звонок с объяснением ситуации о забытом пароле, искренние извинения, просьба зачитать пароль либо сменить его на новый.

Больше чем в половине случаев просьба будет удовлетворена, а факт подмены будет замечен либо с первой неудачной попыткой зарегистрироваться истинного сотрудника, либо по произведенному злоумышленником ущербу.

Почти такая же схема, но в обратную сторону может быть разыграна злоумышленником в адрес сотрудника фирмы – звонок от администратора. В этом случае он представляется уже сотрудником службы информационной безопасности и просит назвать пароль либо из-за произошедшего сбоя в базе данных, либо якобы для подтверждения личности самого сотрудника по какой-либо причине (рассылка особо важных новостей), либо по поводу последнего подключения сотрудника к какому-либо информационному серверу внутри фирмы. Фантазия в этом случае может придумывать самые правдоподобные причины, по которым сотруднику «просто необходимо» вслух назвать пароль. Самое неприятное в этой схеме то, что если причина запроса пароля придумана, что называется, «с умом», то сотрудник повторно позвонит в службу информационной безопасности только через неделю, месяц, если вообще это произойдет. Кроме того, данная схема может быть проведена и без телефонного звонка – по электронной почте, что неоднократно и исполнялось якобы от имени почтовых и Web-серверов в сети Интернет.

В качестве программных профилактических мер используются экранные заставки с паролем, появляющиеся через 5-10 минут отсутствия рабочей активности, автоматическое отключение клиента через такой же промежуток времени.

1.6. Неформальная модель нарушителя в АС

Модель нарушителя - абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа.

Неформальная модель нарушителя отражает его практические и теоретические возможности, априорные знания, время и место действия и т.п. Для достижения своих целей нарушитель должен приложить некоторые усилия, затратить определенные ресурсы. Исследовав причины нарушений, можно либо повлиять на сами эти причины (конечно если это возможно), либо точнее определить требования к системе защиты от данного вида нарушений или преступлений.

В каждом конкретном случае, исходя из конкретной технологии обработки информации, может быть определена модель нарушителя, которая должна быть адекватна реальному нарушителю для данной АС.

В качестве нарушителя рассматривается лицо (субъект), предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства. Злоумышленником будем называть нарушителя, намеренно идущего на нарушение из корыстных побуждений.

При разработке модели нарушителя определяются:

предположения о категориях лиц, к которым может принадлежать нарушитель;

предположения о мотивах действий нарушителя (преследуемых нарушителем целях);

предположения о квалификации нарушителя и его технической оснащенности (об используемых для совершения нарушения методах и средствах);

ограничения и предположения о характере возможных действий нарушителей.

По отношению к АС нарушители могут быть внутренними (из числа персонала системы) или внешними (посторонними лицами). Внутренним нарушителем может быть лицо из следующих категорий персонала:

пользователи (операторы) системы;

персонал, обслуживающий технические средства (инженеры, техники);

сотрудники отделов разработки и сопровождения ПО (прикладные и системные программисты);

технический персонал, обслуживающий здания (уборщики, электрики, сантехники и другие сотрудники, имеющие доступ в здания и помещения, где расположены компоненты АС);

сотрудники службы безопасности АС;

руководители различных уровней должностной иерархии.

Посторонние лица, которые могут быть нарушителями:

клиенты (представители организаций, граждане);

посетители (приглашенные по какому-либо поводу);

представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго-, водо-, теплоснабжения и т.п.);

представители конкурирующих организаций (иностранных спецслужб) или лица, действующие по их заданию;

лица, случайно или умышленно нарушившие пропускной режим (без цели нарушить безопасность АС);

любые лица за пределами контролируемой территории.

Можно выделить три основных мотива нарушений: безответственность, самоутверждение и корыстный интерес.

При нарушениях, вызванных безответственностью, пользователь целенаправленно или случайно производит какие-либо разрушающие действия, не связанные тем не менее

со злым умыслом. В большинстве случаев это следствие некомпетентности или небрежности.

Некоторые пользователи считают получение доступа к системным наборам данных крупным успехом, затевая своего рода игру «пользователь - против системы» ради самоутверждения либо в собственных глазах, либо в глазах коллег.

Нарушение безопасности АС может быть вызвано и корыстным интересом пользователя системы. В этом случае он будет целенаправленно пытаться преодолеть систему защиты для доступа к хранимой, передаваемой и обрабатываемой в АС информации. Даже если АС имеет средства, делающие такое проникновение чрезвычайно сложным, полностью защитить ее от проникновения практически невозможно.

Нарушители классифицируются по уровню знаний, возможностей, предоставляемых им штатными средствами АС и СВТ, по времени действия и по месту действия.

По уровню знаний об АС :

знает функциональные особенности АС, основные закономерности формирования в ней массивов данных и потоков запросов к ним, умеет пользоваться штатными средствами;

обладает высоким уровнем знаний и опытом работы с техническими средствами системы и их обслуживания;

обладает высоким уровнем знаний в области программирования и вычислительной техники, проектирования и эксплуатации автоматизированных информационных систем;

знает структуру, функции и механизм действия средств защиты, их сильные и слабые стороны.

По уровню возможностей (используемым методам и средствам):

применяющий чисто агентурные методы получения сведений;

применяющий пассивные средства (технические средства перехвата без модификации компонентов системы);

использующий только штатные средства и недостатки систем защиты для ее преодоления (несанкционированные действия с использованием разрешенных средств), а также компактные магнитные носители информации, которые могут быть скрытно пронесены через посты охраны;

применяющий методы и средства активного воздействия (модификация и подключение дополнительных технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ).

По времени действия:

в процессе функционирования АС (во время работы компонентов системы);

в период неактивности компонентов системы (в нерабочее время, во время плановых перерывов в ее работе, перерывов для обслуживания и ремонта и т.п.);

как в процессе функционирования АС, так и в период неактивности компонентов системы.

По месту действия:

без доступа на контролируемую территорию организации;

с контролируемой территории без доступа в здания и сооружения;

внутри помещений, но без доступа к техническим средствам АС;

с рабочих мест конечных пользователей (операторов) АС;

с доступом в зону данных (баз данных, архивов и т.п.);

с доступом в зону управления средствами обеспечения безопасности АС.

Могут учитываться следующие ограничения и предположения о характере действий возможных нарушителей:

работа по подбору кадров и специальные мероприятия затрудняют возможность создания коалиций нарушителей, т.е. объединения (сговора) и целенаправленных действий по преодолению подсистемы защиты двух и более нарушителей;

нарушитель, планируя попытки НСД, скрывает свои несанкционированные действия от других сотрудников.

НСД может быть следствием ошибок пользователей, администраторов, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки информации и т.д.

Определение конкретных значений характеристик возможных нарушителей в значительной степени субъективно. Модель нарушителя, построенная с учетом особенностей конкретной предметной области и технологии обработки информации, может быть представлена перечислением нескольких вариантов его облика. Каждый вид нарушителя должен быть охарактеризован значениями характеристик, приведенных выше.

К основным способам НСД относятся:

непосредственное обращение к объектам доступа;

создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;

модификация средств защиты, позволяющая осуществить НСД;

внедрение в технические средства СВТ или АС программных или технических механизмов, нарушающих предполагаемую структуру и функции СВТ или АС и позволяющих осуществить НСД.

Специфика распределенных АС, с точки зрения их уязвимости, связана в основном с наличием интенсивного информационного взаимодействия между территориально разнесенными и разнородными (разнотипными) элементами.

Уязвимыми являются буквально все основные структурно-функциональные элементы распределенных АС: рабочие станции, серверы (Host-машины), межсетевые мосты (шлюзы, центры коммутации), каналы связи.

Защищать компоненты АС необходимо от всех видов воздействий: стихийных бедствий и аварий, сбоев и отказов технических средств, ошибок персонала и пользователей, ошибок в программах и от преднамеренных действий злоумышленников.

Имеется широчайший спектр вариантов путей преднамеренного или случайного несанкционированного доступа к данным и вмешательства в процессы обработки и обмена информацией (в том числе, управляющей согласованным функционированием различных компонентов сети и разграничением ответственности за преобразование и дальнейшую передачу информации).

Правильно построенная (адекватная реальности) модель нарушителя, в которой отражаются его практические и теоретические возможности, априорные знания, время и место действия и т.п. характеристики - важная составляющая успешного проведения анализа риска и определения требований к составу и характеристикам системы защиты.

1.7. Методы и средства обеспечения безопасности процессов переработки информации

Управление доступом включает в себя следующие функции защиты:

идентификация пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);

опознание (установление подлинности) объекта или субъекта по предъявленному им идентификатору;

проверка полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);

разрешение и создание условий работы в пределах установленного регламента;

регистрация (протоколирование) обращений к защищаемым ресурсам;

реагирование (сигнализация, отключение, задержка работ, отказ в запросе) при попытках несанкционированных действий. Маскировка - метод защиты процессов переработки информации путем ее криптографического закрытия. Этот метод защиты широко применяется за рубежом, как при обработке, так и при хранении информации, в том числе на дискетах. При передаче информации по каналам связи большой протяженности этот метод является единственно надежным.

Регламентация - метод защиты процессов переработки информации, создающий такие условия автоматизированной обработки, хранения и передачи защищаемых процессов обработки информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму.

Принуждение - такой метод защиты процессов переработки информации, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемых процессов обработки информации под угрозой материальной, административной или уголовной ответственности.

Побуждение - такой метод защиты процессов переработки информации, который побуждает пользователя и персонал системы не разрушать установленные порядки за счет соблюдения сложившихся моральных и этических норм (как регламентированных, так и неписаных).

Рассмотренные методы обеспечения безопасности процессов переработки информации реализуются на практике за счет применения различных средств защиты, таких как технические, программные, организационные, законодательные и морально-этические.

Средства обеспечения безопасности процессов переработки информации, используемые для создания механизма зашиты, подразделяются на формальные (выполняют защитные функции по заранее предусмотренной процедуре без непосредственного участия человека) и неформальные (определяются целенаправленной деятельностью человека либо регламентируют эту деятельность).

К формальным средствам защиты относятся следующие:

технические, которые реализуются в виде электрических, электромеханических и электронных устройств. Технические средства защиты, в свою очередь, подразделяются на физические и аппаратные. Физические средства защиты реализуются в виде автономных устройств и систем (например, замки на дверях, за которыми размещена аппаратура, решетки на окнах, электронно-механическое оборудование охранной сигнализации. Под аппаратными техническими средствами принято понимать устройства, встраиваемые непосредственно в вычислительную технику, или устройства, которые сопрягаются с подобной аппаратурой по стандартному интерфейсу;

программные, которые представляют собой программное обеспечение, специально предназначенное для выполнения функций защиты процессов обработки информации. К неформальным средствам защиты относятся следующие:

организационные, которые представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации вычислительной техники, аппаратуры телекоммуникаций для обеспечения защиты обработки информации. Организационные мероприятия охватывают все структурные элементы аппаратуры на всех этапах их жизненного цикла (строительство помещений, проектирование компьютерной информационной системы банковской деятельности, монтаж и наладка оборудования, испытания, эксплуатация);

законодательные, которые определяются законодательными актами страны, регламентирующими правила пользования, обработки и передачи информации ограниченного доступа и устанавливающими меры ответственности за нарушение этих правил;

морально-этические, которые реализуются в виде всевозможных норм, сложившихся традиционно или складывающихся по мере распространения вычислительной техники и средств связи в обществе. Эти нормы большей частью не являются обязательными как законодательные меры, однако несоблюдение их обычно ведет к потере авторитета и престижа человека. Наиболее показательным примером таких норм является Кодекс профессионального поведения членов Ассоциаций пользователей ЭВМ США.

Для реализации мер безопасности используются различные механизмы шифрования (криптографии).

Криптография - это наука об обеспечении секретности или аутентичности (подлинности) передаваемых сообщений.

Сущность криптографических методов заключается в следующем. Готовое к передаче сообщение, будь то данные, речь или изображение того или иного документа, обычно называется открытым, или незащищенным, текстом (сообщением). В процессе передачи по незащищенным каналам связи такое сообщение может быть легко перехвачено или отслежено подслушивающим лицом посредством его умышленных или неумышленных действий. Для предотвращения несанкционированного доступа к этому сообщению оно зашифровывается и тем самым преобразуется в шифрограмму или закрытый текст. Когда же санкционированный пользователь получает сообщение, он дешифрует или раскрывает его посредством обратного преобразования криптофаммы, вследствие чего получается исходный открытый текст.

Методу преобразования в криптографической системе соответствует использование специального алгоритма. Действие такого алгоритма запускается уникальным числом (или битовой последовательностью), обычно называемым шифрующим ключом.

Каждый используемый ключ может производить различные шифрованные сообщения, определяемые только этим ключом. Для большинства систем закрытая схема генератора ключа может представлять собой либо набор инструкций, команд, либо часть (узел) аппаратуры (hardware), либо компьютерную программу (software), либо все это вместе, но в любом случае процесс шифрования/ дешифрования единственным образом определяется выбранным специальным ключом. Поэтому, чтобы обмен зашифрованными сообщениями проходил успешно, как отправителю, так и получателю необходимо знать правильную ключевую установку и хранить ее в тайне.

Следовательно, стойкость любой системы закрытой связи определяется степенью секретности используемого в ней ключа. Тем не менее, этот ключ должен быть известен другим пользователям сети для того, чтобы они могли свободно обмениваться зашифрованными сообщениями. В этом смысле криптографические системы также помогают решить проблему аутентификации (установления подлинности) принятой информации, поскольку подслушивающее лицо, пассивным образом перехватывающее сообщение, будет иметь дело только с зашифрованным текстом. В то же время истинный получатель, приняв эти сообщения, закрытые известным ему и отправителю ключом, будет надежно защищен от возможной дезинформации.

Шифрование может быть симметричным и асимметричным. Симметричное шифрование основывается на использовании одного и того же секретного ключа для шифрования и дешифрования. Асимметричное шифрование характеризуется тем, что для шифрования используется один ключ, являющийся общедоступным, а для дешифрования - другой, являющийся секретным; при этом знание общедоступного ключа не позволяет определить секретный ключ.

Наряду с шифрованием используются и другие механизмы безопасности:

цифровая (электронная) подпись;

контроль доступа;

обеспечение целостности данных;

обеспечение аутентификации;
постановка трафика;
управление маршрутизацией;
арбитраж, или освидетельствование.

Механизмы цифровой подписи основываются на алгоритмах асимметричного шифрования и включают в себя две процедуры: формирование подписи отправителем и ее опознавание (верификацию) получателем. Первая процедура обеспечивает шифрование блока данных либо его дополнение криптографической контрольной суммой, причем в обоих случаях используется секретный ключ отправителя. Вторая процедура основывается на использовании общедоступного ключа, знания которого достаточно для опознавания отправителя Механизмы контроля доступа осуществляют проверку полномочий объектов АИТ (программ и пользователей) на доступ к ресурсам сети. При доступе к ресурсу через соединение контроль выполняется как в точке инициации, так и в промежуточных точках, а также в конечной точке.

Механизмы обеспечения целостности данных применяются как к отдельному блоку, так и к потоку данных. Целостность блока является необходимым, но недостаточным условием целостности потока. Целостность блока обеспечивается выполнением взаимосвязанных процедур шифрования и дешифрования отправителем и получателем. Отправитель дополняет передаваемый блок криптографической суммой, а получатель сравнивает ее с криптографическим значением, соответствующим принятому блоку. Несовпадение свидетельствует об искажении информации в блоке. Однако описанный механизм не позволяет вскрыть подмену блока в целом. Поэтому необходим контроль целостности потока, который реализуется посредством шифрования с использованием ключей, изменяемых в зависимости от предшествующих блоков.

Аутентификация может быть односторонней и взаимной. В первом случае один из взаимодействующих объектов проверяет подлинность другого, тогда как во втором случае проверка является взаимной.

Механизмы постановки трафика, называемые также механизмами заполнения текста, используются для реализации засекречивания потока данных. Они основываются на генерации объектами АИТ фиктивных блоков, их шифровании и организации передачи по каналам сети. Этим нейтрализуется возможность получения информации посредством наблюдения за внешними характеристиками потоков, циркулирующих по каналам связи.

Механизмы управления маршрутизацией обеспечивают выбор маршрутов движения информации по коммуникационной сети таким образом, чтобы исключить передачу секретных сведений по скомпрометированным (небезопасным) физически ненадежным каналам.

Механизмы арбитража, или освидетельствования, обеспечивают подтверждение характеристик данных, передаваемых между объектами АИТ, третьей стороной (арбитром). Для этого вся информация, отправляемая или получаемая объектами, проходит и через арбитра, что позволяет ему впоследствии подтверждать упомянутые характеристики.

В АИТ при организации безопасности данных используется комбинация нескольких механизмов.

1.8. Методы и средства технологий защиты от угроз ИБ

Методы и средства технологий защиты от угроз ИБ подразделяются на три группы:
предотвращение,
парирование;
нейтрализация.

К группе технологий предотвращения угроз ИБ относятся технологии, осуществляющие упреждение и предупреждение от планирования проникновения, организации и реализации защиты объекта при начальном этапе нападения.

К группе технологий парирования угроз ИБ относятся методы и приемы, препятствующие или ограничивающие воздействие на защищенный объект.

К группе технологий нейтрализации угроз ИБ относятся средства устранения и ликвидации угроз, а также либо частичной, либо полной их нейтрализации в случае проникновения или диверсии с объектом.

Организационные и правовые методы защиты процессов переработки информации в КС стоят на первом месте в технологиях предотвращения угроз ИБ. Надо учитывать, что наряду с интенсивным развитием вычислительных средств и систем передачи информации все более актуальной становится проблема обеспечения ее безопасности. Меры безопасности направлены на предотвращение несанкционированного получения информации, физического уничтожения или модификации защищаемых процессов обработки информации.

Сегодня зарождается новая современная технология - технология защиты процессов переработки информации в компьютерных информационных системах и сетях передачи данных.

Классификация правовых и организационных методов и средств предотвращения угроз ИБ.

Законы и нормативные акты исполняются только в том случае, если они подкрепляются организаторской деятельностью соответствующих структур, создаваемых в государстве, ведомствах, учреждениях и организациях. При рассмотрении вопросов безопасности обработки информации такая деятельность относится к организационным методам защиты процессов переработки информации.

Организационные методы защиты процессов переработки информации включают в себя меры, мероприятия и действия, которые должны осуществлять должностные лица в процессе создания и эксплуатации КС для обеспечения заданного уровня безопасности обработки информации.

На организационном уровне решаются следующие задачи обеспечения ИБ в КС:

организация работ по разработке системы защиты процессов переработки информации;

разграничение доступа к ресурсам КС;

планирование мероприятий;

разработка документации;

воспитание и обучение обслуживающего персонала и пользователей;

сертификация средств зашиты обработки информации;

лицензирование деятельности по защите процессов переработки информации;

аттестация объектов защиты;

совершенствование системы защиты процессов переработки информации;

оценка эффективности функционирования системы защиты;

контроль выполнения установленных правил работы в КС.

Государство должно обеспечить в стране защиту процессов переработки информации как в масштабах всего государства, так и на уровне организаций и отдельных граждан. Для решения этой проблемы государство обязано:

выработать государственную политику безопасности в области ИТ;

законодательно определить правовой статус компьютерных систем, информации, систем защиты процессов переработки информации, владельцев и пользователей информации и т.д.;

создать иерархическую структуру государственных органов, вырабатывающих и воплощающих в жизнь политику безопасности ИТ;

создать систему стандартизации, лицензирования и сертификации в области защиты процессов переработки информации; обеспечить приоритетное развитие отечественных защищенных информационных систем;

повысить уровень образования граждан в области ИТ, воспитать у них патриотизм и бдительность;

установить ответственность граждан за нарушения законодательства в области ИТ.

Политика государства РФ в области безопасности ИТ является единой. Вопросы ИБ нашли отражение в «Концепции национальной безопасности Российской Федерации», утвержденной Указом Президента РФ от 17.12.97 № 1300, а затем в Доктрине ИБ РФ. В «Концепции национальной безопасности Российской Федерации» определены важнейшие задачи государства в области ИБ.

Усилия государства направлены на воспитание ответственности у граждан за неукоснительное выполнение правовых норм в области ИБ. Важной задачей государства является также повышение уровня образования граждан в области ИТ. Большая роль в этой работе принадлежит образовательной системе государства, государственным органам управления, средствам массовой информации.

Правовые методы защиты процессов переработки информации основываются на законодательной базе обеспечения информацией, которая определяется социально-экономическими изменениями в обществе, происшедшими в последние годы. Они требовали законодательного регулирования отношений, складывающихся в области ИТ. В связи с этим был принят Федеральный закон «Об информации, информатизации и защите информации» от 25.01.95 № 24-ФЗ.

Другим важным правовым документом, регламентирующим вопросы защиты информации в КС, служит Закон РФ «О государственной тайне» от 21.07.93 № 5485-1. Отношения, связанные с созданием программ и баз данных, регулируются Законами РФ «О правовой охране программ для электронных вычислительных машин и баз данных» от 23.09.92 № 3523-1 и «Об авторском праве и смежных правах» от 09.07.93 № 5352-1.

Очень важным правовым вопросом является установление юридического статуса КС и особенно статуса информации, получаемой с применением КС. Статус информации, или ее правомочность, служит основанием для выполнения (невыполнения) определенных действий. Например, в одних АСУ соответствующее должностное лицо имеет юридическое право принимать решения только на основании информации, полученной из АСУ. В других АСУ для принятия решения необходимо получить подтверждающую информацию по другим каналам. В одной и той же АСУ решение может приниматься как с получением подтверждающей информации, так и без нее.

Правовой статус информации устанавливается с учетом ее стоимости (важности) и степени достоверности, которую способна обеспечить компьютерная система.

Другие законодательные акты (законы РФ, указы и распоряжения Президента РФ, а также организационно-методические и руководящие документы Государственной технической комиссии при Президенте РФ) указывают на организационно-правовую реализацию ИБ путем комплексной защиты информационной деятельности в России.

Организация такой защиты на государственном уровне проводится в соответствии со структурой государственных органов обеспечения ИБ в Российской Федерации.

В министерствах и ведомствах создаются иерархические структуры обеспечения безопасности информации, которые, как правило, совпадают с организационной структурой министерства (ведомства). Называться они могут по-разному, но функции выполняют сходные. Одними из основных задач таких структур являются воспитание патриотизма и бдительности, повышение уровня образования и ответственности граждан в области ИТ.

1.9. Методы предотвращения угроз несанкционированного изменения инфраструктуры КС

Они касаются процессов деформации структурного построения системы. Здесь несанкционированному изменению могут быть подвергнуты алгоритмическая, программная и техническая структуры КС на этапах ее разработки и эксплуатации. На этапе эксплуатации необходимо выделить работы по модернизации КС, представляющие повышенную опасность для ИБ.

Особенностью защиты от несанкционированного изменения структур (НИС) КС является универсальность методов, позволяющих наряду с умышленными воздействиями определять и блокировать непреднамеренные ошибки разработчиков и обслуживающего персонала, а также сбои и отказы аппаратных и программных средств. Обычно НИС КС, выполненные на этапе разработки и при модернизации системы, называют закладками.

Для предотвращения угроз данного класса на различных этапах жизненного цикла КС решаются различные задачи.

Методы и средства предотвращения угроз несанкционированного изменения инфраструктур КС:

выявление и устранение закладок и ошибок в инфраструктуре КС;
привлечение высококвалифицированных специалистов;
применение стандартных блочных иерархических структур;
дублирование разработки КС;
контроль адекватности функционирования устройства,
программы, алгоритма (тестирование);
многослойная фильтрация;
автоматизация процесса разработки КС;
контроль порядка разработки;
сертификация готового продукта (программных и аппаратных средств).

На этапе разработки и при модернизации КС основной задачей признано исключение ошибок и возможности внедрения закладок. На этапе эксплуатации выявляются закладки и ошибки, а также обеспечивается целостность, неизменность структур.

Особые требования предъявляются к квалификации специалистов, занятых разработкой технического задания и алгоритмов, осуществляющих контроль над ходом разработки и привлекаемых к сертификации готовых продуктов.

Принцип многослойной фильтрации предполагает поэтапное выявление ошибок и закладок определенного класса. Например, могут использоваться фильтрующие программные средства для выявления возможных временных, интервальных, частотных и других типов закладок.

Автоматизация процесса разработки существенно снижает возможности внедрения закладок. Это объясняется, прежде всего, наличием большого числа типовых решений, которые исполнитель изменить не может, формализованностью процесса разработки, возможностью в автоматизированного контроля принимаемых решений.

Контроль установленного порядка разработки предполагает регулярный контроль над действиями исполнителей, поэтапный контроль алгоритмов, программ и устройств, приемосдаточные испытания.

1.10. Инженерно-технические методы предотвращения угроз в КС

Современные распределенные корпорации, имеющие подразделения на разных континентах, имеют сложную техническую, инженерную и информационную инфраструктуру. Создание информационной сети такой корпорации и её эффективная защита является чрезвычайно сложной концептуальной и технологической задачей.

Первоначальное решение, характерное для последнего десятилетия прошлого века, использовать для формирования сети телефонные линии быстро привело к нагромождению коммуникаций и к невозможности эффективной защиты. Последующее создание и сопровождение собственных корпоративных сетей для обеспечения информационного обмена данными на базе таких линий связи стало обходиться в миллионы долларов.

Быстрое развитие технологий Интернет, образование, рост и развитие «всемирной паутины» позволили создать достаточно дешевые и надежные коммуникации. Однако техническая надежность связи вовсе не означала безопасности корпоративных сетей, имеющих выходы в Интернет. Общие принципы построения Интернет и его использование как общедоступной сети с публичными сервисами привели к тому, что стало очень трудно обеспечить надежную защиту от проникновения в корпоративные и государственные сети, построенные на базе протоколов TCP/IP и Интернет - приложений - Web, FTP, e-mail и т.д.

Целевое назначение любой корпоративной информационной системы состоит в обеспечении пользователей необходимой информацией в режиме «On Line» и адекватном информационном сопровождении деятельности предприятия.

Базисом КИС является общесистемное программное обеспечение, которое включает операционную систему и программные оболочки, программы общего и прикладного назначения: автоматизированные рабочие места (АРМ) и Web-сервисы общего и специального назначения, СУБД и управление интегрированными вычислительными и мультимедийными приложениями, а также доступом в локальные и внешние сети (рис.1.1).

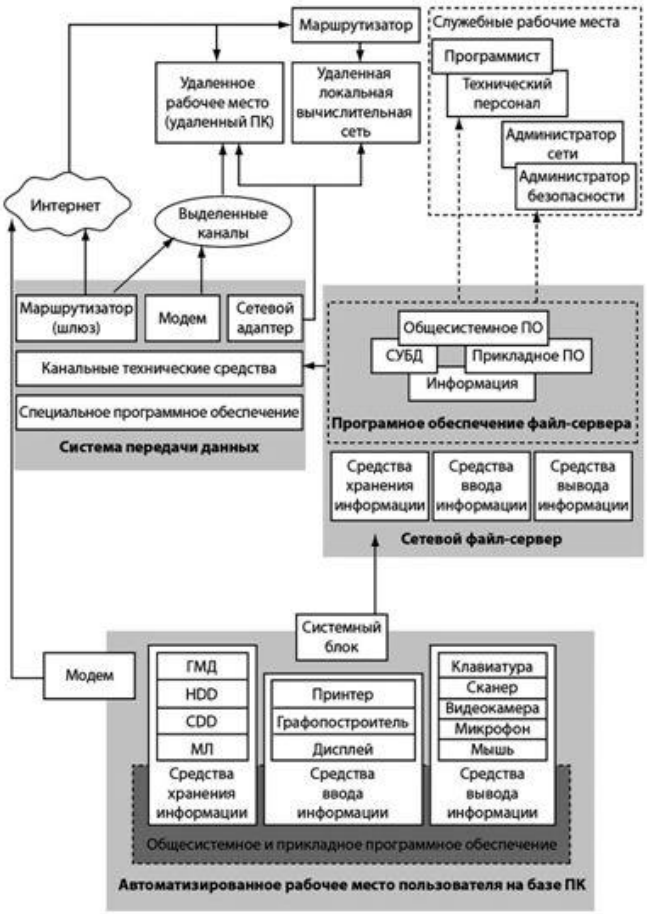

Рис.1.1. Схема корпоративной информационной системы, включающей локальные сети и выход в Интернет

Физически нижний уровень КИС базируется на серверах, рабочих станциях, персональных компьютерах различного назначения и коммуникационных устройствах, а также на программном обеспечении, реализующем работу перечисленных устройств. В связи с этим подсистема ИБ начинается с защиты именно этого программно-аппаратного оборудования. С этой целью можно использовать известные защитные средства операционных систем, антивирусные пакеты, средства и устройства аутентификации пользователя, средства криптографической защиты паролей и данных прикладного уровня. Все эти средства образуют базу для реализации первого уровня технологической модели подсистемы ИБ (рис.1.2).

Рис.1.2. Четырехуровневая технологическая модель подсистемы информационной безопасности

Второй физический уровень КИС - рабочие станции, серверы и персональные компьютеры объединятся в локальные сети, которые организуют внутреннее Интернет-пространство предприятия и могут быть иметь выходы во внешнее Интернет-пространство. В этом случае речь идет о средствах информационной защиты (СЗИ) второго уровня - уровня защиты локальных сетей, который обычно включает:

- средства безопасности сетевых ОС;
- средства аутентификации пользователей (User Authentication Facilities - UAF);
- средства физического и программного разграничения доступа к распределенным и разделяемым информационным ресурсам;
- средства защиты домена локальной сети (Local Area Network Domain - LAND);
- средства промежуточного доступа (Proxy Server) и межсетевые экраны (Firewall);
- средства организации виртуальных локальных подсетей (Virtual Local Area Network - VLAN);
- средства обнаружения атаки и уязвимостей в системе защиты локальных сетей.

Следующий уровень реализации КИС - объединение нескольких локальных сетей географически распределенного предприятия в общую корпоративную Intranet-сеть через открытую сеть на базе современных технологий поддержки и сопровождения таких сетей (Quality of Service - QoS) с использованием открытой среды Интернет в качестве коммутационной среды.

В этом случае на третьем уровне защиты КИС используются технологии защищенных виртуальных сетей (Virtual Private Networks - VPN). VPN-технологии часто интегрируются со средствами первого и второго уровней. Такой защищенный VPN-канал может простираться не только до маршрутизаторов доступа и пограничных Fairwall'лов, но и до серверов и рабочих станций локальной сети.

Четвертый уровень защиты КИС - организация защищенного межкорпоративного обмена в среде электронного бизнеса (eBusiness). Методологической и технологической основой такой защиты являются методы и технологии управления публичными ключами и сертификатами криптографической защиты (Public Key Infrastructure - PKI). Суть этих технологий состоит в реализации двух глобальных функций: генерации и корректном распространении ключей и сертификатов и отслеживании их жизненного цикла. Базой для реализации средств защиты будут электронная цифровая подпись (Electronic Digital Signature - EDS) и VPN-технологии.

Отметим, что два нижних уровня защиты являются достаточно традиционными, так как они предназначены для обеспечения безопасности конкретной физически реализованной КИС. Верхние два уровня относятся к обеспечению безопасности передачи данных и электронного бизнеса, который осуществляется уже не в физическом, а в виртуальном пространстве, при этом VPN-технологии обеспечивают защищенный обмен данными в межкорпоративном пространстве, а PKI-технологии обеспечивают VPN-устройства ключами и сертификатами. В настоящее время на рынке имеется достаточное число технических и программных решений для защиты данных, информации, систем и сетей. Ниже рассмотрены некоторые базовые технологии на примере криптографической защиты данных, технологий межсетевых экранов, защищенных VPN-каналов связи, антивирусных и биометрических методов.

Методы предотвращения угроз шпионажа и диверсий реализуют традиционный подход к обеспечению ИБ объектов. При защите процессов переработки информации в КС от традиционного шпионажа и диверсий используются те же средства и методы защиты, что и для защиты других объектов, на которых не используются КС.

Применение системы охраны объекта основывается на следующих положениях.

Объект, на котором производятся работы с ценной конфиденциальной информацией, имеет, как правило, несколько рубежей защиты:

контролируемая территория;

здание;

помещение;

устройство, носитель информации;

программа;

информационные ресурсы.

От шпионажа и диверсий необходимо защищать первые четыре рубежа и обслуживающий персонал.

Система охраны объекта (СОО) КС создается с целью предотвращения несанкционированного проникновения на территорию и в помещения объекта посторонних лиц, обслуживающего персонала и пользователей.

Состав системы охраны зависит от охраняемого объекта. В общем случае СОО КС должна включать в себя:

инженерные конструкции;

охранную сигнализацию;

средства наблюдения;

подсистему доступа на объект;

дежурную смену охраны.

Организация работ с конфиденциальными информационными ресурсами предусматривает работы с документами. Для предотвращения таких угроз, как хищение документов, носителей информации, атрибутов систем защиты, изучение отходов носителей информации и создание неучтенных копий документов, необходимо определить порядок учета, хранения, выдачи, работы и уничтожения носителей информации. Применяют организационные методы работы с конфиденциальными информационными ресурсами. Обеспечение такой работы в учреждении реализуется путем организации специальных подразделений конфиденциального делопроизводства

либо ввода штатных или нештатных должностей сотрудников. Работа с конфиденциальными информационными ресурсами осуществляется в соответствии с законами РФ и ведомственными инструкциями. В каждой организации должны быть:

разграничены полномочия должностных лиц по допуску их к информационным ресурсам;

определены и оборудованы места хранения «конфиденциальных информационных ресурсов и места работы с ними;

установлен порядок учета, выдачи, работы и сдачи на хранение конфиденциальных информационных ресурсов;

назначены ответственные лица с определением их полномочий и обязанностей;

организован сбор и уничтожение ненужных документов и списанных машинных носителей;

организован контроль над выполнением установленного порядка работы с конфиденциальными ресурсами.

Противодействие наблюдению осуществляется в оптическом и инфракрасном диапазонах.

Наблюдение в оптическом диапазоне злоумышленником, находящимся за пределами объекта с КС, малоэффективно. С расстояния 50 м даже совершенным длиннофокусным фотоаппаратом невозможно прочитать текст с документа или монитора. Так, телеобъектив с фокусным расстоянием 300 мм обеспечивает разрешающую способность лишь 15 х 15 мм. Кроме того, угрозы такого типа легко парируются с помощью:

использования оконных стекол с односторонней проводимостью света;

применения штор и защитного окрашивания стекол;

размещения рабочих столов, мониторов, табло и плакатов таким образом, чтобы они не просматривались через окна или открытые двери.

Для противодействия наблюдению в оптическом диапазоне злоумышленником, находящимся на объекте, необходимо, чтобы:

двери помещений были закрытыми;

расположение столов и мониторов ЭВМ исключало возможность наблюдения документов или выдаваемой информации на соседнем столе или мониторе;

стенды с конфиденциальной информацией имели шторы.

Противодействие наблюдению в инфракрасном диапазоне, как правило, требует применения специальных методов и средств: защитных костюмов, ложных тепловых полей и т.д.

Противодействие подслушиванию осуществляется при помощи методов, которые подразделяются на два класса:

методы защиты речевой информации при передаче ее по каналам связи;

методы защиты от прослушивания акустических сигналов в помещениях.

Речевая информация, передаваемая по каналам связи, защищается от прослушивания (закрывается) с использованием методов аналогового скремблирования и дискретизации речи с последующим шифрованием.

Под скремблированием понимается изменение характеристик речевого сигнала таким образом, что полученный модулированный сигнал, обладая свойствами неразборчивости и неузнаваемости, занимает такую же полосу частот спектра, как и исходный открытый.

Обычно аналоговые скремблеры преобразуют исходный речевой сигнал путем изменения его частотных и временных характеристик.

Применяют следующие способы частотного преобразования сигнала:

частотная инверсия спектра сигнала;

частотная инверсия спектра сигнала со смещением несущей частоты;

разделение полосы частот речевого сигнала на поддиапазоны с последующей перестановкой и инверсией.

Частотная инверсия спектра сигнала заключается в зеркальном отображении спектра С(f) исходного сигнала (рис.1.3,*а*) относительно выбранной частоты Уо спектра. В результате низкие частоты преобразуются в высокие, и наоборот (рис.1.3,*б*).

Такой способ скремблирования обеспечивает невысокий уровень защиты, так как частота легко определяется. Устройства, реализующие такой метод защиты, называют маскираторами.

Частотная инверсия спектра сигнала со смещением несущей частоты обеспечивает более высокую степень защиты.

Способ частотных перестановок заключается в разделении спектра исходного сигнала на поддиапазоны равной ширины (до 10... 15 поддиапазонов) с последующим их перемешиванием в соответствии с некоторым алгоритмом.информации (кадр) перед отправлением запоминается и разбивается на сегменты одинаковой длительности.

Сегменты перемешиваются аналогично частотным перестановкам (рис.1.3). При приеме кадр подвергается обратному преобразованию.

Комбинации временного и частотного скремблирования позволяют значительно повысить степень защиты речевой информации. За это приходится платить существенным повышением сложности скремблеров.

Дискретизация речевой информации с последующим шифрованием обеспечивает наивысшую степень защиты. В процессе дискретизации речевая информация представляется в цифровой форме. В таком виде она преобразуется в соответствии с выбранными алгоритмами шифрования, которые применяются для преобразования данных в КС.

Защита акустических сигналов в помещениях КС является важным направлением противодействия подслушиванию. Существует несколько методов защиты от прослушивания акустических сигналов:

звукоизоляция и звукопоглощение акустического сигнала;

зашумление помещений или твердой среды для маскировки акустических сигналов;

защита от несанкционированной записи речевой информации на диктофон;

обнаружение и изъятие закладных устройств.

Предотвращение угрозы подслушивания с помощью закладных подслушивающих устройств осуществляется методами радиоконтроля помещений, поиска неизлучающих закладок и подавления закладных устройств. Программно-аппаратные средства реализации этих методов подробно описаны.

Защита от злоумышленных действий обслуживающего персонала и пользователей имеет большое значение для функционирования, так как они составляют по статистике 80 % случаев злоумышленных воздействий на информационные ресурсы и совершаются людьми, имеющими непосредственное отношение к эксплуатации КС. Такие действия либо осуществляются под воздействием преступных групп (разведывательных служб), либо побуждаются внутренними причинами (зависть, месть, корысть и т.д.).

Для блокирования угроз такого типа руководство организации с помощью службы безопасности должно выполнять следующие организационные мероприятия:

добывать всеми доступными законными путями информацию о своих сотрудниках, людях или организациях, представляющих потенциальную угрозу информационным ресурсам;

обеспечивать охрану сотрудников;

устанавливать разграничение доступа к защищаемым ресурсам;

контролировать выполнение установленных мер безопасности;

создавать и поддерживать в коллективе здоровый нравственный климат.

Руководство должно владеть по возможности полной информацией об образе жизни своих сотрудников. Основное внимание при этом следует обращать на получение информации о ближайшем окружении, соответствии легальных доходов и расходов, наличии вредных привычек, об отрицательных чертах характера, о состоянии здоровья, степени удовлетворенности профессиональной деятельностью и занимаемой должностью. Для получения такой информации используются сотрудники службы безопасности, психологи, руководящий состав учреждения. С этой же целью осуществляется взаимодействие с органами МВД России и спецслужбами. Сбор информации необходимо вести, не нарушая законы и права личности.

Вне пределов объекта охраняются, как правило, только руководители и сотрудники, которым реально угрожает воздействие злоумышленников.

В организации, работающей с конфиденциальной информацией, обязательно разграничение доступа к информационным ресурсам. В случае предательства или других злоумышленных действий сотрудника ущерб должен быть ограничен рамками его компетенции. Сотрудники учреждения должны знать, что выполнение установленных правил контролируется руководством и службой безопасности.

Далеко не последнюю роль в парировании угроз данного типа играет нравственный климат в коллективе. В идеале каждый сотрудник является патриотом коллектива, дорожит своим местом, его инициатива и отличия ценятся руководством.

1.11. Технологии нижнего уровня защиты информации в локальных сетях: межсетевые экраны

Межсетевой экран (брандмауэр, Firewall) - программно-аппаратная система межсетевой защиты, которая отделяет одну часть сети от другой и реализует набор правил для прохождения данных из одной части в другую. Границей является раздел между локальной корпоративной сетью и внешними Интернет-сетями или различными частями локальной распределенной сети. Экран фильтрует текущий трафик, пропуская одни пакеты информации и отсеивая другие.

Межсетевой экран (МЭ) является одним из основных компонентов защиты сетей. Наряду с Интернет-протоколом межсетевого обмена (Internet Security Protocol - IPSec) МЭ является одним из важнейших средств защиты, осуществляя надежную аутентификацию пользователей и защиту от НСД. Отметим, что большая часть проблем с информационной безопасностью сетей связана с «прародительской» зависимостью коммуникационных решений от ОС UNIX - особенности открытой платформы и среды программирования UNIX сказались на реализации протоколов обмена данными и политики информационной безопасности. Вследствие этого ряд Интернет-служб и совокупность сетевых протоколов (Transmission Control Protocol/Интернет Protocol - TCP/IP) имеет «бреши» в защите.

К числу таких служб и протоколов относятся:

– служба сетевых имен (DomainNameServer-DNS);

– доступ к всемирной паутине WWW;

– программа электронной почты Send Mail;

– служба эмуляции удаленного терминала Telnet;

– простой протокол передачи электронной почты (Simple Mail Transfer Protocol - SMTP);

– протокол передачи файлов (File Transfer Protocol);

– графическая оконная система X Windows.

Настройки МЭ, т.е. решение пропускать или отсеивать пакеты информации, зависят от топологии распределенной сети и принятой политики информационной безопасности. В связи с этим политика реализации межсетевых экранов определяет правила доступа к ресурсам внутренней сети. Эти правила базируются на двух общих принципах - запрещать всё, что не разрешено в явной форме, и разрешать всё, что не

запрещено в явной форме. Использование первого принципа дает меньше возможностей пользователям и охватывает жёстко очерченную область сетевого взаимодействия. Политика, основанная на втором принципе, является более мягкой, но во многих случаях она менее желательна, так как предоставляет пользователям больше возможностей «обойти» МЭ и использовать запрещенные сервисы через нестандартные порты (User Data Protocol - UDP), которые не запрещены политикой безопасности.

Функциональные возможности МЭ охватывают следующие разделы реализации информационной безопасности:

– настройку правил фильтрации;
– администрирование доступа во внутренние сети;
– фильтрацию на сетевом уровне;
– фильтрацию на прикладном уровне;
– средства сетевой аутентификации;
– ведение журналов и учет.

Программно-аппаратные компоненты МЭ можно отнести к одной из трёх категорий: фильтрующие маршрутизаторы, шлюзы сеансового уровня и шлюзы уровня приложений. Эти компоненты МЭ - каждый отдельно и в различных комбинациях - отражают базовые возможности МЭ и отличают их один от другого.

Фильтрующий маршрутизатор (Filter Router - FR) фильтрует IP-пакеты по параметрам полей заголовка пакета: IP-адрес отправителя, IP-адрес адресата, TCP/UDP-порт отправителя и TCP/UDP-порт адресата. Фильтрация направлена на безусловное блокирование соединений с определенными хостами и/или портами - в этом случае реализуется политика первого типа.

Формирование правил фильтрации является достаточно сложным делом, к тому же обычно отсутствуют стандартизированные средства тестирования правил и корректности их исполнения. Возможности FR по реализации эффективной защиты ограничены, так как на сетевом уровне эталонной модели OSI обычно он проверяет только IP-заголовки пакетов. К достоинствам применения FR можно отнести невысокую стоимость, гибкость формирования правил, незначительную задержку при передаче пакетов. Недостатки FR достаточно серьезны, о них следует сказать более подробно:

– отсутствует аутентификация конкретного пользователя;
– указанную выше аутентификацию по IP-адресу можно «обойти» путем замещения информации пользователя информацией злоумышленника, использующего нужный IP-адрес;
– внутренняя сеть «видна» из внешней сети;
– правила фильтрации сложны в описании и верификации, они требуют высокой квалификации администратора и хорошего знания протоколов TCP/UDP;
– нарушение работы ФМ приводит к полной незащищенности всех компьютеров, которые находятся за этим МЭ.

Шлюз сеансового уровня (Session Level Gateway - SLG) - активный транслятор TCP соединения. Шлюз принимает запрос авторизованного клиента на предоставление услуг, проверяет допустимость запрошенного сеанса (Handshaking), устанавливает нужное соединение с адресом назначения внешней сети и формирует статистику по данному сеансу связи. После установления факта, что доверенный клиент и внешний хост являются «законными» (авторизованными) участниками сеанса, шлюз транслирует пакеты в обоих направлениях без фильтрации. При этом часто пункт назначения оговаривается заранее, а источников информации может быть много (соединение «один-ко-многим») - это, например, типичный случай использования внешнего Web-ресурса.

Используя различные порты, можно создавать различные конфигурации соединений, обслуживая одновременно всех пользователей, имеющих право на доступ к ресурсам сети. Существенным недостатком SLG является то, что после установления связи пакеты фильтруются только на сеансовом уровне модели OSI без проверки их

содержимого на уровне прикладных программ. Авторизованный злоумышленник может спокойно транслировать вредоносные программы через такой шлюз. Таким образом, реализация защиты осуществляется, в основном, на уровне квитирования (Handshaking).

Шлюз уровня приложений (ApplicationLayerGateway-ALG). Для компенсации недостатков FR и SLG шлюзов в межсетевые экраны встраивают прикладные программы для фильтрации пакетов при соединениях с такими сервисами, как Telnet и FTP и пр. Эти приложения называются Proxy-службами, а устройство (хост), на котором работает служба, называется шлюзом уровня приложений. Шлюз исключает прямое взаимодействие между авторизованным пользователем и внешним хостом. Зафиксировав сетевой сеанс, шлюз останавливает его и вызывает уполномоченное приложение для реализации запрашиваемой услуги - Telnet, FTP, WWW или E-mail. Внешний пользователь, который хочет получить услугу соединения в Сети, соединяется вначале с ALG, а затем, пройдя предусмотренные политикой безопасности процедуры, получает доступ к нужному внутреннему узлу (хосту). Отметим явные преимущества такой технологии:

– уполномоченные приложения вызывают только те службы, которые прописаны в сфере их действия, исключая все остальные, которые не отвечают требованиям информационной безопасности в контексте запрашиваемой услуги;

– уполномоченные приложения обеспечивают фильтрацию протокола - например, некоторые ALG могут быть настроены на фильтрацию FTP соединения и запрещают при этом выполнение команды <FTP put>, что однозначно не позволяет передавать информацию на анонимный FTP-сервер;

– шлюзы прикладного уровня, как правило, фиксируют в специальном журнале выполняемые сервером действия и в случае необходимости сообщают сетевому администратору о возможных коллизиях и попытках проникновения;

– структура внутренней сети не видна из Интернет-сети, шлюз осуществляет надежную аутентификацию и регистрацию, правила фильтрации просты, так как экран пропускает прикладной трафик, предназначенный только для шлюза прикладного уровня, блокируя весь остальной.

Как показывает практика, защита на уровне приложений позволяет дополнительно осуществлять другие проверки в системе защиты информации, а это снижает опасность «взлома» системы, имеющей «прорехи» в системе безопасности.

Межсетевые экраны можно разделить по следующим основным признакам:

– по исполнению: программный и программно-аппаратный;

– по используемой технологии: контроль состояния протокола (Stateful Inspection Protocol) или с использованием модулей посредников (Proxy Server);

– по функционированию на уровнях эталонной модели OSI (Open System Interconnection): шлюзы экспертного, прикладного, сеансового уровней, пакетный фильтр;

– по схеме подключения: схема единой защиты сети; схема с закрытым и не защищаемым открытым сегментами сети; схема с раздельной защитой закрытого и открытого сегментов сети.

На рис.1.4 показан вариант защиты локальной сети на базе программно-аппаратного решения - межсетевого экрана Cisko 2610 & PIX Firewall 520 компании Cisco Systems. Отличительной особенностью этой модели является специальная ОС реального времени, а высокая производительность реализуется на базе алгоритма адаптивной безопасности (Adaptive Security Algorithm - ASA).

Рис.1.4. Использование комплекса «маршрутизатор-файервол» в системах защиты информации при подключении к Интернету

Приведенное решение имеет несомненные достоинства: высокая производительность и пропускная способность до 4 Гб/с; возможность поддержки до 256 тысяч одновременных сессий; объединение преимуществ пакетного и прикладного шлюзов, простота и надежность в установке и эксплуатации, возможность сертификации в Государственной технической комиссии РФ.

В заключение отметим, что межсетевые экраны, естественно, не решают всех вопросов информационной безопасности распределенных КИС и локальных сетей - существует ряд ограничений на их применение и ряд угроз, от которых МЭ не могут защитить. Отсюда следует, что технологии МЭ следует применять комплексно - с другими технологиями и средствами защиты.

1.12. Концепция защищенных виртуальных частных сетей

При выходе локальной сети в открытое Интернет-пространство возникают угрозы двух основных типов: несанкционированный доступ (НСД) к данным в процессе их передачи по открытой сети и НСД к внутренним ресурсам КИС. Информационная защита при передаче данных по открытым каналам реализуется следующими мерами:

– взаимная аутентификация сторон;

– прямое и обратное криптографическое преобразование данных;

– проверка достоверности и целостности полученных данных.

Организация защиты с использованием технологии виртуальных частных сетей (Virtual Private Network - VPN) подразумевает формирование защищенного «виртуального туннеля» между узлами открытой Сети, доступ в который невозможен потенциальному злоумышленнику. Преимущества этой технологии очевидны: аппаратная реализация довольно проста, нет необходимости создавать или арендовать дорогие выделенные физические сети, можно использовать открытый дешевый Интернет, скорость передачи данных по туннелю такая же, как по выделенному каналу.

В настоящее время существует четыре вида архитектуры организации защиты информации на базе применения технологии VPN.

Локальная сетьVPN (LocalAreaNetwork-VPN). Обеспечивает защиту потоков данных и информации от НСД внутри сети компании, а также информационную безопасность на уровне разграничения доступа, системных и персональных паролей, безопасности функционирования ОС, ведение журнала коллизий, шифрование конфиденциальной информации.

Внутрикорпоративная сеть VPN (Intranet-VPN). Обеспечивает безопасные соединения между внутренними подразделениями распределенной компании.

Для такой сети подразумевается:

– использование мощных криптографических средств шифрования данных;

– обеспечение надежности работы критически важных транзакционных приложений, СУБД, электронной почты, Telnet, FTP;

– скорость и производительность передачи, приема и использования данных;

– гибкость управления средствами подключения новых пользователей и приложений.

Сети VPN с удаленным доступом (Интернет-VPN). Обеспечивает защищенный удаленный доступ удаленных подразделений распределённой компании и мобильных сотрудников и отделов через открытое пространство Интернет (рис1.5).

Такая сеть организует:

– адекватную систему идентификации и аутентификации удалённых и мобильных пользователей;

– эффективную систему управления ресурсами защиты, находящимися в географически распределенной информационной системе.

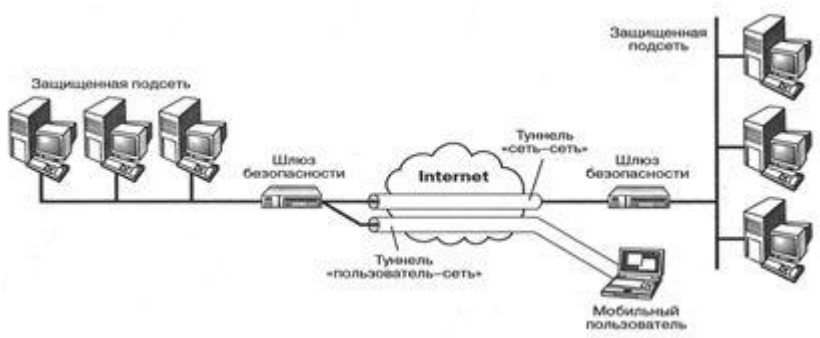

Рис.1.5. Туннельная схема организации VPN сети

Межкорпоративная сеть VPN (Extranet-VPN). Обеспечивает эффективный защищённый обмен информацией с поставщиками, партнёрами, филиалами корпорации в других странах. Такая сеть предусматривает использование стандартизированных и надёжных VPN-продуктов, работающих в открытых гетерогенных средах и обеспечивающих максимальную защищенность конфиденциального трафика, включающего аудио- и видеопотоки информации - конфиденциальные телефонные переговоры и телеконференции с клиентами.

Можно выделить два основных способа технической реализации виртуальных туннелей:

– построение совокупности соединений (Frame Relay или Asynchronous Transfer Mode) между двумя нужными точками единой сетевой инфраструктуры, надежно изолированной от других пользователей механизмом организации встроенных виртуальных каналов;

– построение виртуального IP-туннеля между двумя узлами сети на базе использования технологии туннелирования, когда каждый пакет информации шифруется и «вкладывается» в поле нового пакета специального вида (конверт), который и передается по IP-туннелю - при этом пакет протокола более низкого уровня помещается в поле данных пакета более высокого уровня (рис1.6).

Рис.1.6. Схема пакета, подготовленного к отправке по туннелю

VPN-туннель обладает всеми свойствами защищенной выделенной линии, проходящей через открытое пространство Интернет. Особенность технологии туннелирования состоит в том, что она позволяет зашифровать не только поле данных, а весь исходный пакет, включая заголовки. Это важная деталь, так как из заголовка исходного пакета злоумышленник может извлечь данные о внутренней структуре сети - например, информацию о количестве локальных сетей и узлов и их IP-адресах.

Зашифрованный пакет, называемый SKIP-пакетом, инкапсулируется в другой пакет с открытым заголовком, который транспортируется по соответствующему туннелю (рис.1.7).

При достижении конечной точки туннеля из внешнего пакета извлекается внутренний, расшифровывается, и его заголовок используется для дальнейшей передачи во внутренней сети или подключенному к локальной сети мобильному пользователю. Туннелирование применяется не только для обеспечения конфиденциальности внутреннего пакета данных, но и для его целостности и аутентичности, механизм туннелирования часто применяется в различных протоколах формирования защищенного канала связи. Технология позволяет организовать передачу пакетов одного протокола в логической среде, использующей другой протокол.

Таким образом, можно реализовать взаимодействие нескольких разнотипных сетей, преодолевая несоответствие внешних протоколов и схем адресации.

Рис.1.7. Структура SKIP-пакета

Средства построения защищенной VPN достаточно разнообразны - они могут включать маршрутизаторы с механизмом фильтрации пакетов (Filtering Router), многофункциональные межсетевые экраны (Multifunction Firewall), промежуточные устройства доступа в сеть (Proxy Server), программно-аппаратные шифраторы (Firmware Cryptograph). По технической реализации можно выделить следующие основные виды средств формирования VPN:

– специализированные программные решения, дополняющие стандартную операционную систему функциями VPN;

– программно-аппаратное устройство на базе специализированной ОС реального времени, имеющее два или несколько сетевых интерфейсов и аппаратную криптографическую поддержку;

– средства VPN, встроенные в стандартный маршрутизатор или коммутатор;

– расширение охвата защищаемой зоны канала передачи и приёма данных за счет дополнительных функций межсетевого экрана.

Туннели VPN создаются для различных типов конечных пользователей: это может быть локальная сеть (Local Area Network - LAN) со шлюзом безопасности (Security Gateway) или отдельные компьютеры удаленных или мобильных пользователей с сетевым программным обеспечением для шифрования и аутентификации трафика - клиенты VPN (рис.1.8). Через шлюз безопасности проходит весь трафик для внутренней корпоративной сети. Адрес шлюза VPN указывается как внешний адрес входящего туннелируемого пакета, а расшифрованный внутренний адрес пакета – это адрес конкретного хоста за шлюзом.

Наиболее простым и относительно недорогим способом организации VPN-канала является схема, в соответствии с которой защищенный туннель прокладывается только в открытой сети для транспортировки зашифрованных пакетов. В качестве конечных точек туннеля выступают провайдеры Интернет-сети или пограничные межсетевые экраны (маршрутизаторы) локальной сети. Защищенный туннель формируется компонентами виртуальной сети, функционирующим на узлах, между которыми он создается. В настоящее время активно функционирует рынок VPN-средств. Приведем некоторые примеры популярных и широко используемых решений для каждого класса продуктов.

VPN на базе сетевых операционных систем. Для формирования виртуальных защищённых туннелей в IP сетях сетевая операционная система Windows NT использует протокол PPTP (Point-to-Point Transfer Protocol). Туннелирование информационных пакетов производится инкапсулированием и шифрованием (криптоалгоритм RSA RC4) стандартных блоков данных фиксированного формата (PPP Data Frames) в IP-дейтаграммы, которые и передаются в открытых IP-сетях. Данное решение является недорогим, и его можно эффективно использовать для формирования VPN-каналов внутри локальных сетей, домена Windows NT или для построения Интернет- и Extranet-VPN для небольших компаний малого и среднего бизнеса для защиты не критичных приложений.

VPN на базе маршрутизаторов. В России лидером на рынке VPN-продуктов является компания Cisko Systems. Построение каналов VPN на базе маршрутизаторов Cisko осуществляется средствами ОС версии Cisko IOS 12.x. Для организации туннеля маршрутизаторы Cisko используют протокол L2TP канального уровня эталонной модели OSI, разработанного на базе «фирменных» протоколов Cisko L2F и Microsoft PPTP, и протокол сетевого уровня IPSec, созданного ассоциацией «Проблемная группа проектирования Интернет (Интернет Engineering Task Force - IETF). Эффективно применяется Cisko VPN Client, который предназначен для создания защищенных соединений Point-to Point между удаленными рабочими станциями и маршрутизаторами Cisko - это позволяет построит практически все виды VPN-соединений в сетях.

VPN на базе межсетевых экранов. Эта технология считается наиболее сбалансированной и оптимальной с точки обеспечения комплексной безопасности КИС и её защиты от атак из внешней открытой сети. В России нашел широкое применение программный продукт Check Point Firewall-1/VPN-1 компании Check Point Software Technologies. Это решение позволяет построить глубоко комплексную эшелонированную систему защиты КИС.

В состав продукта входят: Check Point Firewall-1, набор средств для формирования корпоративной виртуальной частной сети Check Point VPN-1, средства обнаружения атак и вторжений Real Secure, средства управления полосой пропускания информационных пакетов Flood Gate, средства VPN-1 Secure Remote, VPN-1 Appliance и VPN-1 Secure Client

для построения Localnet/Intranet/Интернет/Extranet VPN-каналов. Весь набор продуктов Check Point VPN-1 построен на базе открытых стандартов IPSec, имеет развитую систему идентификации и аутентификации пользователей, взаимодействует с внешней системой распределения открытых ключей PKI, поддерживает цетрализованную систему управления и аудита.

На российском рынке можно указать два продукта, получивших достаточно широкую известность, - это криптографический комплекс «Шифратор IP пакетов» производства объединения МО ПН ИЭИ (http://www.security.ru) и ряд программных продуктов ЗАСТАВА компании ЭЛВИС+ (http://www.elvis.ru). Самым быстрорастущим сегментом рынка систем информационной безопасности по исследованиям IDC, Price Waterhouse Cooper и Gartner Group являются системы блокировки корпоративных каналов связи. Быстрее всего растут продажи систем защиты от утечек внутренней информации (Intrusion Detection and Prevention - IDP), которые позволяют контролировать трафик электронной почты и доступ к внешним Интернет-ресурсам.

1.13. Парирование угроз от электромагнитных излучений и наводок

Эти методы, в свою очередь, подразделяются на две группы: пассивные и активные.

Пассивные методы обеспечивают уменьшение уровня опасного сигнала или снижение информативности сигналов. Активные методы направлены на создание помех в каналах побочных электромагнитных излучений и наводок, затрудняющих прием и выделение полезной информации из перехваченных злоумышленником сигналов.

Для блокирования угрозы воздействия на электронные блоки и магнитные запоминающие устройства мощными внешними электромагнитными импульсами и высокочастотными излучениями, приводящими к неисправности электронных блоков и стирающими информацию с магнитных носителей информации, используют экранирование защищаемых средств.

Защита от побочных электромагнитных излучений и наводок осуществляется как пассивными, так и активными методами.

Пассивные методы парирования угроз от электромагнитных излучений и наводок подразделяются на три группы: экранирование; снижение мощности излучений и наводок; снижение информативности сигналов. Экранирование является одним из самых эффективных методов защиты процессов переработки информации от электромагнитных излучений. Под экранированием понимается размещение элементов КС, создающих электрические, магнитные и электромагнитные поля, в пространственно-замкнутых конструкциях. Способы экранирования зависят от особенностей полей, создаваемых элементами КС при протекании в них электрического тока.

Характеристики полей зависят от параметров электрических сигналов в КС. Так, при малых токах и высоких напряжениях в создаваемом поле преобладает электрическая составляющая. Такое поле называется электрическим (электростатическим). Если в проводнике протекает ток большой величины при малых значениях напряжения, то в поле преобладает магнитная составляющая, а поле называется магнитным. Поля, у которых электрическая и магнитная составляющие соизмеримы, называются электромагнитными.

Снижение мощности излучений и наводок и информативности сигналов осуществляется способами защиты от пассивных электромагнитных излучений (ЭМИ) и наводок, объединенных в эту группу, которые реализуются с целью снижения уровня излучения и взаимного влияния элементов КС.

К данной группе относятся следующие методы:

изменение электрических схем;

использование оптических каналов связи;

изменение конструкции;

использование фильтров;

гальваническая развязка в системе питания.

Изменение электрических схем осуществляется для уменьшения мощности побочных излучений. Это достигается за счет использования элементов с меньшим излучением, уменьшения крутизны фронтов сигналов, предотвращения возникновения паразитной генерации, нарушения регулярности повторений информации.

Перспективным направлением борьбы спобочными ЭМИ является использование оптических каналов связи. Для передачи информации на большие расстояния успешно используются волоконно-оптические кабели. Передачу информации в пределах одного помещения (даже больших размеров) можно осуществлять с помощью беспроводных систем, использующих излучения в инфракрасном диапазоне. Оптические каналы связи не порождают ЭМИ. Они обеспечивают высокую скорость передачи и не подвержены воздействию электромагнитных помех.

Изменение конструкции сводится к изменению взаимного расположения отдельных узлов, блоков, кабелей и сокращению длины шин.

Использование фильтров является одним из основных способов защиты от побочных ЭМИ и наводок. Фильтры устанавливаются как внутри устройств, систем для устранения распространения и возможного усиления наведенных побочных электромагнитных сигналов, так и на выходе из объектов линий связи, сигнализации и электропитания. Фильтры рассчитываются таким образом, чтобы они обеспечивали снижение сигналов в диапазоне побочных наводок до безопасного уровня и не вносили существенных искажений полезного сигнала.

Полностью исключается попадание побочных наведенных сигналов во внешнюю цепь электропитания при наличии генераторов питания, которые обеспечивают гальваническую развязку между первичной и вторичной цепями.

Использование генераторов позволяет также подавать во вторичную цепь электропитание с другими параметрами (по сравнению с первичной цепью). Так, во вторичной цепи может быть изменена частота. Генераторы питания за счет инерционности механической части позволяют сглаживать пульсации напряжения и кратковременные отключения в первичной цепи.

Активные методы парирования угроз от электромагнитных излучений и наводок предполагают применение генераторов шумов, различающихся принципами формирования маскирующих помех. В качестве маскирующих используются случайные помехи с нормальным законом распределения спектральной плотности мгновенных значений амплитуд (гауссовские помехи) и прицельные помехи, представляющие собой случайную последовательность сигналов помехи, идентичных побочным сигналам.

Эффективно применение пространственного и линейного зашумления. Пространственное зашумление осуществляется за счет излучения с помощью антенн электромагнитных сигналов в пространство.

Применяется локальное пространственное зашумление для защиты конкретного элемента КС и объектовое пространственное зашумление для защиты от побочных электромагнитных излучений КС всего объекта. При локальном пространственном зашумлении используются прицельные помехи. Антенна находится рядом с защищаемым элементом КС. Объектовое пространственное зашумление осуществляется, как правило, несколькими генераторами со своими антеннами, что позволяет создавать помехи во всех диапазонах побочных электромагнитных излучений всех излучающих устройств объекта.

Пространственное зашумление должно обеспечивать невозможность выделения побочных излучений на фоне создаваемых помех во всех диапазонах излучения; уровень создаваемых помех не должен превышать санитарных норм и норм по электромагнитной совместимости радиоэлектронной аппаратуры. При использовании линейного зашумления генераторы прицельных помех подключаются к токопроводящим линиям для создания в

них электрических помех, которые не позволяют злоумышленникам выделять наведенные сигналы.

1.14. Криптографические методы предотвращения угроз в КС

Криптография - это совокупность технических, математических, алгоритмических и программных методов преобразования данных (шифрование данных), которая делает их бесполезными для любого пользователя, у которого нет ключа для расшифровки. Криптографические преобразования обеспечивают решение следующих базовых задач защиты - конфиденциальности (невозможности прочитать данные и извлечь полезную информацию) и целостности (невозможность модифицировать данные для изменения смысла или внесения ложной информации).

Технологии криптографии позволяют реализовать следующие процессы информационной защиты:

– идентификация (отождествление) объекта или субъекта сети или информационной системы;

– аутентификация (проверка подлинности) объекта или субъекта сети;

– контроль/разграничение доступа к ресурсам локальной сети или внесетевым сервисам;

– обеспечение и контроль целостности данных.

В соответствии с политиками безопасности используемые в компании технологии криптографии и специализированное программно-аппаратное обеспечение для защиты данных и документов, шифрования файлов и дисков реализуют следующие аспекты информационной защиты:

– шифруемые электронные письма и соединения VPN скрывают передаваемые данные от вирусов и сканеров содержимого;

– шифрование дисков не должно затруднять автоматическое резервное сохранение данных или управление файлами;

– сетевой администратор может не иметь права доступа к защищаемым файлам, содержащим конфиденциальную информацию, если это вызвано производственной необходимостью;

– когда сотрудник покидает предприятие, у его работодателя должна быть возможность доступа к зашифрованным данным, связанным с производственной деятельностью этого сотрудника;

– надежность шифрования и доступа должна быть обеспечена на длительное время;

– если при шифровании применяется метод открытого ключа, то помимо программного обеспечения необходимо построение инфраструктуры управления ключами или сертификатами;

– в случае попытки взлома системы или утечки секретной информации систему можно быстро перенастроить;

– широкое применение шифрования возможно лишь при условии простоты его обслуживания.

Общая схема простой криптосистемы показана на рис.1.9, а на рис.1.10 приведена схема симметричной криптосистемы с закрытым ключом.

Отправитель сообщения генерирует открытый текст сообщения для передачи по незащищенному каналу связи. Для того чтобы передаваемый текст невозможно было прочитать, отправитель преобразует (шифрует) его с помощью алгоритма обратимого преобразования $< \mathrm{E}_k >$, формируя зашифрованный текст (криптограмму) $< \mathrm{C} = \mathrm{E}_k(\mathrm{M}) >$.

Адресат, получив криптограмму, применяет известное ему обратное преобразование $< D = \mathrm{E}_k^{-1} >$ и получает исходный открытый

текст $\mathrm{M} :< D_k(C) = \mathrm{E}_k^{-1}(\mathrm{E}_k(\mathrm{M})) = M >$. Множество преобразований $\mathrm{E}_{\mathrm{к}i}$ образуют семейства криптоалгоритмов $\mathrm{E}_{\mathrm{к}}{}^{N}$. Параметр K, с помощью которого производится преобразование текста сообщения, называется ключом.

Рис.1.9. Общая схема криптосистемы

Такой ключ, по сути, является уникальным параметром - только его владелец (группа владельцев) может использовать этот ключ. Таким образом, криптографическая система по определению - это однопараметрическое семейство $E_k k \in K$ обратимых преобразований $< E_k : M \to C >$ из пространства M сообщений открытого текста в пространство C зашифрованных текстов. Параметр шифрования K (ключ) выбирается из конечного множества {K}, называемого пространством ключей.

Существует два класса криптосистем - симметричные (с одним ключом) и асимметричные (с двумя ключами). Симметричные криптосистемы (рис.1.10) используют один и тот же ключ в процедурах шифрования и расшифровки текста, поэтому такие системы называются системами с секретным закрытым ключом.

Ключ должен быть известен только тем, кто занимается отправкой и получением сообщений. Таким образом, задача обеспечения конфиденциальности сводится к обеспечению конфиденциальности ключа. Передача такого ключа от адресата пользователю может быть выполнена только по защищенному каналу связи (рис.1.10, пунктирная линия), что является существенным недостатком симметричной системы шифрования.

Рис.1.10. Схема симметричной криптосистемы с закрытым ключом

Такой вид шифрования наиболее часто используется в закрытых локальных сетях, в том числе входящих в КИС, для предотвращения НСД в отсутствие владельца ресурса. Таким способом можно шифровать как отдельные тексты и файлы, так и логические и физические диски.

Рис.1.11. Схема асимметричной криптосистемы с открытым ключом

Асимметричные криптосистемы используют различные ключи:

– открытый ключ K_1 используется для шифрования данных и вычисляется по параметрам секретного ключа K_2;

– секретный ключ K_2 используется для расшифровки информации, зашифрованной с помощью парного ему открытого ключа K_1.

Открытый и секретный ключи и K_2 генерируются попарно (рис.1.11), при этом ключ K_2 остается у его владельца и должен быть надежно защищен от НСД. Копии ключа K_1 распространяются среди пользователей сети, с которыми обменивается информацией обладатель секретного ключа K_2. Таким образом, в асимметричной криптосистеме ключ $K1$ свободно передается по открытым каналам связи, а секретный ключ K_2 хранится на месте его генерации.

Система защиты информации называется криптостойкой, если в результате предпринятой злоумышленником атаки на зашифрованное послание невозможно расшифровать перехваченный зашифрованный текст C для получения открытого текста M или зашифровать текст злоумышленника M' для передачи правдоподобного зашифрованного текста C' с искаженными данными.

В настоящее время используется следующий подход реализации криптозащиты - криптосистема, реализующая семейство криптографических преобразований $E_k k \in K$, является открытой системой. Это очень важный принцип криптозащиты, так как защищенность системы не должна зависеть от того, чего нельзя было бы быстро перенастроить в случае необходимости, если произошла утечка секретной информации. Изменение программно-аппаратой части системы защиты информации требует значительных финансовых и временных затрат, а изменение ключей является несложным делом. Именно поэтому стойкость криптосистемы определяется, в основном, секретностью ключа K_2.

Формальные математические методы криптографии были разработаны Клодом Шенноном («Математическая теория криптографии», 1945 г.). Он доказал теорему о существовании и единственности абсолютно стойкого шифра - это такая система шифрования, когда текст однократно зашифровывается с помощью случайного открытого ключа такой же длины.

В 1976 году американские математики У.Диффи и М.Хеллман обосновали методологию асимметричного шифрования с применением открытой однонаправленной функции (это такая функция, когда по её значению нельзя восстановить значение аргумента) и открытой однонаправленной функции с секретом.

В 90-е годы XX века профессор Массачусетского технологического института (MIT, USA) Рональд Ривест разработал метод шифрования с помощью особого класса функций - хэш-функций (Hash Function). Это был алгоритм шифрования MD6 хэширования переменной разрядности. Хэш-функция (дайджест-функция) - это

отображение, на вход которого подается сообщение переменной длины M, а выходом является строка фиксированной длины $h(M)$ - дайджест сообщения (рис.1.12).

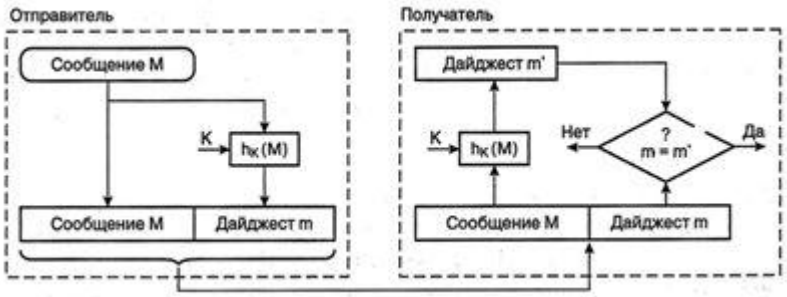

Рис.1.12 Однонаправленной хэш-функции с параметром-ключом

Криптостойкость такого метода шифрования состоит в невозможности подобрать документ M', который обладал бы требуемым значением хэш-функции. Параметры вычисления хэш-функции h – семейство ключей K^N. В настоящее время на этих принципах строятся алгоритмы формирования электронной цифровой подписи (ЭЦП).

Наиболее известные симметричные алгоритмы шифрования в настоящее время – DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm), RC2, RC5, CAST, Blowfish. Асимметричные алгоритмы - RSA (R.Rivest, A.Shamir, L.Adleman), алгоритм Эль Гамаля (ElGamal), криптосистема ECC на эллиптических кривых, алгоритм открытого распределения ключей Диффи-Хеллмана.

Алгоритмы, основанные на применении хэш-функций - MD4 (Message Digest 4), MD5 (Message Digest 5), SHA (Secure Hash Algorithm).

Наиболее известным программным продуктом, распространяемым свободно, является пакет PGP (Pretty Good Privacy). Пакет разработан Филом Циммерманом (Phil Zimmerman) в 1995 году, который использовал упомянутые алгоритмы RSA, IDEA, и MD5. PGP состоит из трёх частей - алгоритма IDEA, сигнатуры и цифровой подписи. PGP использует три ключа - открытый ключ адресата, секретный ключ владельца и сеансовый ключ, генерируемый при помощи RSA и открытого ключа случайным образом при шифровании сообщения (рис.1.13).

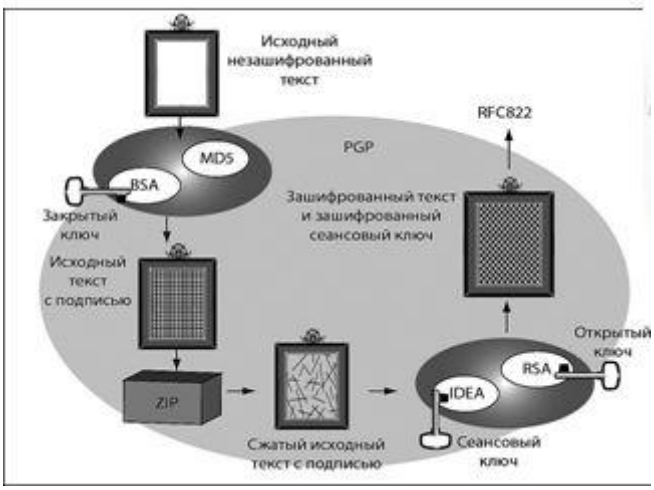

Рис.1.13 Схема формирования защищенного сообщения с помощью пакета PGP

Выбор алгоритма шифрования, кроме обязательного DES, зависит от разработчика. Это создает дополнительное преимущество, так как злоумышленник должен определить,

какой шифр следует вскрыть. Если добавить необходимость подбора ключей, то шансы расшифровки существенно уменьшаются.

Примером простого и эффективного протокола управления криптографическими ключами в сетях является протокол SKIP (Simple Key management for Интернет Protocol), представленный в 1994 году компанией Sun Microsystems (США). Это открытая спецификация, её свободно можно использовать для разработки средств защиты информации в Интернет-сетях. Ряд компаний успешно применяет этот протокол для коммерческих разработок СЗИ: Swiss Institute of Technology (Швейцария), Check Point Software Inc. (США, Израиль), Toshiba (Япония), ЭЛВИС+ (Россия), VPNet (США).

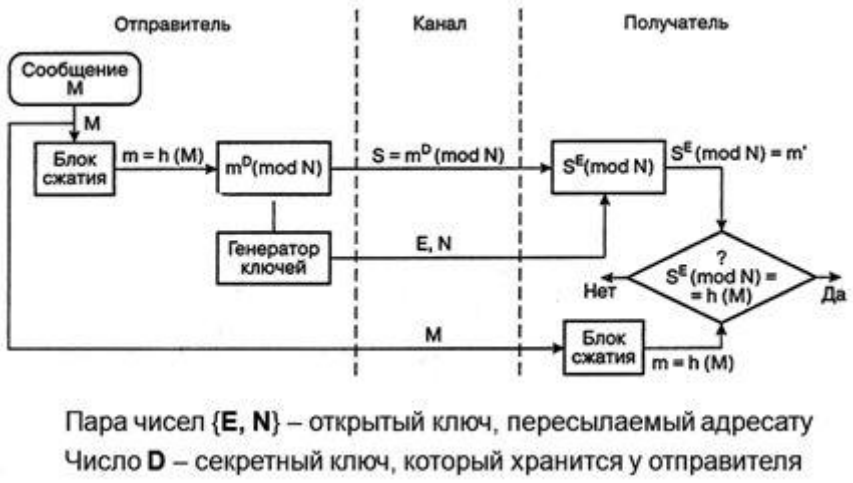

Рис.1.14 Схема формирования ЭЦП

В России установлен единый алгоритм криптографических преобразований данных для систем обработки и передачи данных в сетях, который установлен стандартом ГОСТ 28147-89. Другой российский стандарт - ГОСТ Р 34.11-94 - определяет алгоритм и процедуру вычисления хэш-функций для любых последовательностей двоичных символов, используемых в криптографических методах защиты информации. Отечественный стандарт ГОСТ Р 34.10-94 является стандартом, определяющим алгоритм формирования ЭЦП (рис.1.14).

1. Цикл зашифрования 32-З:

$\boldsymbol{K}_0,\boldsymbol{K}_1,\boldsymbol{K}_2,\boldsymbol{K}_3,\boldsymbol{K}_4,\boldsymbol{K}_5,\boldsymbol{K}_6,\boldsymbol{K}_7,\boldsymbol{K}_0,\boldsymbol{K}_1,\boldsymbol{K}_2,\boldsymbol{K}_3,\boldsymbol{K}_4,\boldsymbol{K}_5,\boldsymbol{K}_6,\boldsymbol{K}_7,\boldsymbol{K}_0,\boldsymbol{K}_1,\boldsymbol{K}_2,\boldsymbol{K}_3,\boldsymbol{K}_4,\boldsymbol{K}_5,\boldsymbol{K}_6,\boldsymbol{K}_7,\boldsymbol{K}_7,\boldsymbol{K}_6,\boldsymbol{K}_5,\boldsymbol{K}_4,\boldsymbol{K}_3,\boldsymbol{K}_2,\boldsymbol{K}_1,\boldsymbol{K}_0.$

2. Цикл расшифрования 32-Р:

$\boldsymbol{K}_0,\boldsymbol{K}_1,\boldsymbol{K}_2,\boldsymbol{K}_3,\boldsymbol{K}_4,\boldsymbol{K}_5,\boldsymbol{K}_6,\boldsymbol{K}_7,\boldsymbol{K}_7,\boldsymbol{K}_6,\boldsymbol{K}_5,\boldsymbol{K}_4,\boldsymbol{K}_3,\boldsymbol{K}_2,\boldsymbol{K}_1,\boldsymbol{K}_0,\boldsymbol{K}_7,\boldsymbol{K}_6,\boldsymbol{K}_5,\boldsymbol{K}_4,\boldsymbol{K}_3,\boldsymbol{K}_2,\boldsymbol{K}_1,\boldsymbol{K}_0,\boldsymbol{K}_7,\boldsymbol{K}_6,\boldsymbol{K}_5,\boldsymbol{K}_4,\boldsymbol{K}_3,\boldsymbol{K}_2,\boldsymbol{K}_1,\boldsymbol{K}_0.$

3. Цикл выработки имитовставки 16-З:

$\boldsymbol{K}_0,\boldsymbol{K}_1,\boldsymbol{K}_2,\boldsymbol{K}_3,\boldsymbol{K}_4,\boldsymbol{K}_5,\boldsymbol{K}_6,\boldsymbol{K}_7,\boldsymbol{K}_0,\boldsymbol{K}_1,\boldsymbol{K}_2,\boldsymbol{K}_3,\boldsymbol{K}_4,\boldsymbol{K}_5,\boldsymbol{K}_6,\boldsymbol{K}_7.$

Каждый из циклов имеет собственное буквенно-цифровое обозначение, соответствующее шаблону «*n-X*», где первый элемент обозначения (*n*), задает число повторений основного шага в цикле, а второй элемент обозначения (*X*), буква, задает порядок зашифрования («З») или расшифрования («Р») в использовании ключевых элементов. Этот порядок нуждается в дополнительном пояснении.

Цикл расшифрования должен быть обратным циклу зашифрования, т.е. последовательное применение этих двух циклов к произвольному блоку должно дать в итоге исходный блок, что отражается следующим соотношением: $\boldsymbol{Ц}_{32\text{-}Р}(\boldsymbol{Ц}_{32\text{-}З}(\boldsymbol{T}))=\boldsymbol{T}$, где $\boldsymbol{T}$ – произвольный 64-битный блок данных, $\boldsymbol{Ц}_{\boldsymbol{X}}(\boldsymbol{T})$ – результат выполнения цикла *X* над блоком данных $\boldsymbol{T}$. Для выполнения этого условия для алгоритмов, подобных ГОСТу, необходимо и достаточно, чтобы порядок использования ключевых элементов соответствующими циклами был взаимно обратным. В справедливости записанного

условия для рассматриваемого случая легко убедиться, сравнив приведенные выше последовательности для циклов 32-З и 32-Р. Из сказанного вытекает одно интересное следствие: свойство цикла быть обратным другому циклу является взаимным, т.е. цикл 32-З является обратным по отношению к циклу 32-Р. Другими словами, зашифрование блока данных теоретически может быть выполнено с помощью цикла расшифрования, в этом случае расшифрование блока данных должно быть выполнено циклом зашифрования. Из двух взаимно обратных циклов любой может быть использован для зашифрования, тогда второй должен быть использован для расшифрования данных, однако стандарт ГОСТ28147-89 закрепляет роли за циклами и не предоставляет пользователю права выбора в этом вопросе.

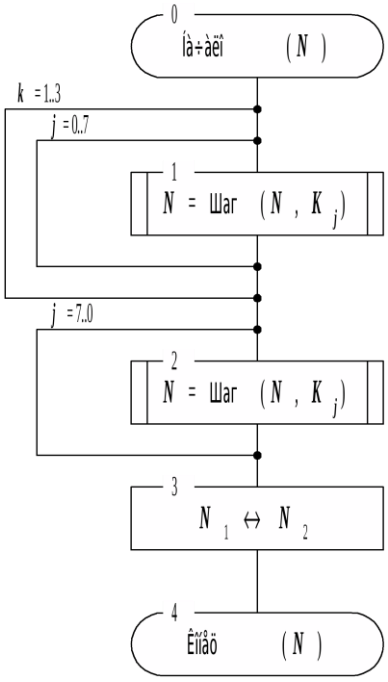

Рис.1.15. Схема цикла зашифрования 32-З

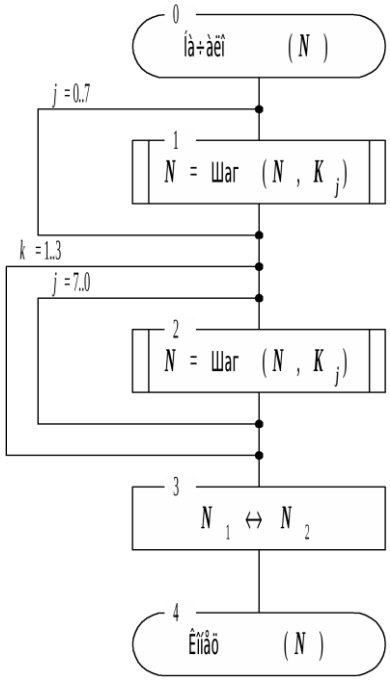

Рис.1.16. Схема цикла расшифрования 32-Р

Цикл выработки имитовставки вдвое короче циклов шифрования, порядок использования ключевых элементов в нем такой же, как в первых 16 шагах цикла зашифрования, в чем нетрудно убедиться, рассмотрев приведенные выше последовательности, поэтому этот порядок в обозначении цикла кодируется той же самой буквой «З».

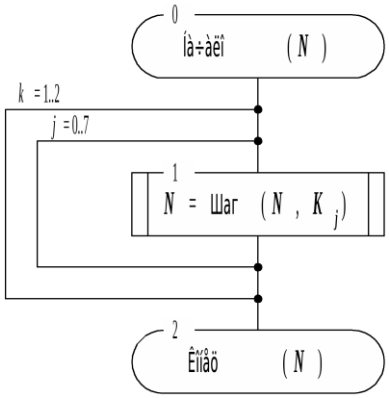

Рис.1.17. Схема цикла выработки имитовставки 16-З

Схемы базовых циклов приведены на рис.1.15-1.17. Каждый из них принимает в качестве аргумента и возвращает в качестве результата 64-битный блок данных, обозначенный на схемах N. Символ Шаг(N,X) обозначает выполнение основного шага криптопреобразования для блока N с использованием ключевого элемента X. Между циклами шифрования и вычисления имитовставки есть еще одно отличие, не упомянутое выше: в конце базовых циклов шифрования старшая и младшая часть блока результата меняются местами, это необходимо для их взаимной обратимости.

По виду воздействия на исходную информацию методы криптографического преобразования информации могут быть разделены на пять групп:

кодирование;

сжатие-расширение;

стенография;

шифрование-дешифрование;

рассечение и разнесение.

Процесс кодирования информации заключается в замене смысловых конструкций исходной информации (слов, предложений) кодами. Кодирование может быть символьным и смысловым. При символьном кодировании в качестве кодов могут использоваться сочетания букв, цифр, букв и цифр. При смысловом кодировании и обратном преобразовании используются специальные таблицы или словари. Кодирование информации целесообразно применять в системах с ограниченным набором смысловых конструкций. Такой вид криптографического преобразования применим, например, в командных линиях АСУ.

Недостатками кодирования конфиденциальной информации является необходимость хранения и распространения кодировочных таблиц, которые необходимо часто менять во избежание раскрытия кодов статистическими методами обработки перехваченных сообщений.

Сжатие-расширение информации может быть отнесено к методам криптографического преобразования информации с определенными оговорками. Целью сжатия является сокращение объема информации. Но сжатая информация не может быть прочитана или использована без обратного преобразования. Учитывая доступность средств сжатия и обратного преобразования, эти методы нельзя рассматривать как надежные средства криптографического преобразования информации. Даже если держать в секрете алгоритмы, то они могут быть сравнительно легко раскрыты статистическими методами обработки информации. Поэтому сжатые файлы конфиденциальной информации подвергаются последующему шифрованию. Для сокращения времени целесообразно совмещать процесс сжатия и шифрования информации.

Процедуры рассечения и разнесения текстов, символов и знаков как элементы сжатия и расширения могут носить смысловой либо механический характер.

В отличие от других методов криптографического преобразования информации методы стенографии позволяют скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации. В компьютерных системах практическое использование стенографии только начинается, но проведенные исследования показывают ее перспективность. В основе всех методов стенографии лежит маскирование закрытой информации среди открытых файлов. Обработка мультимедийных файлов в КС открыла практически неограниченные возможности перед стенографией.

Существует несколько методов скрытой передачи информации. Одним из них является метод внедрения скрытой информации - скрытия файлов при работе в операционной системе MS DOS. За текстовым открытым файлом записывается скрытый двоичный файл, объем которого много меньше текстового файла. В конце текстового файла помещается метка EOF (комбинация клавиш [Control] и [Z]). При обращении к этому текстовому файлу стандартными средствами ОС считывание прекращается по

достижению метки EOF и скрытый файл остается недоступен. Для двоичных файлов никаких меток в конце файла не предусмотрено. Конец такого файла определяется при обработке атрибутов, в которых хранится длина файла в байтах. Доступ к скрытому файлу может быть получен, если файл открыть как двоичный. Скрытый файл может быть зашифрован. Если кто-то случайно обнаружит скрытый файл, то зашифрованная информация будет воспринята как сбой в работе системы.

Графическая и звуковая информация представляется в числовом виде. Так, в графических объектах наименьший элемент изображения может кодироваться одним байтом. В младшие разряды определенных байтов изображения в соответствии с алгоритмом криптографического преобразования помещаются биты скрытого файла. Если правильно подобрать алгоритм преобразования и изображение, на фоне которого помещается скрытый файл, то человеческому глазу практически невозможно отличить полученное изображение от исходного. Очень сложно выявить скрытую информацию и с помощью специальных программ. Наилучшим образом для внедрения скрытой информации подходят изображения местности: фотоснимки со спутников, самолетов и т.д. С помощью средств стеганографии могут маскироваться текст, изображение, речь, цифровая подпись, зашифрованное сообщение. Комплексное использование стеганографии и шифрования многократно повышает сложность решения задачи обнаружения и раскрытия конфиденциальной информации.

Современные методы шифрования должны отвечать следующим требованиям:

способность шифра противостоять криптоанализу (криптостойкость) должна быть такой, чтобы его вскрытие могло быть осуществлено только путем решения задачи полного перебора ключей;

криптостойкость обеспечивается не секретностью алгоритма шифрования, а секретностью ключа;

шифртекст не должен существенно превосходить по объему исходную информацию;

ошибки, возникающие при шифровании, не должны приводить к искажениям и потерям информации;

время шифрования не должно быть большим;

стоимость шифрования должна быть согласована со стоимостью закрываемой информации.

К методам шифрования с симметричными ключами относятся следующие:

методы замены;

методы перестановки;

аналитические методы;

аддитивные методы (гаммирование);

комбинированные методы.

К системам шифрования с открытыми ключами относятся следующие:

система RSA;

система Эль-Гамаля;

криптосистема Мак-Элиса.

1.15. Методы предотвращения угроз несанкционированного доступа в КС

Они являются наиболее практичными и распространенными для пользовательской практики. Для осуществления несанкционированного доступа (НСД) злоумышленник не применяет никаких аппаратных или программных средств, не входящих в состав КС. Он осуществляет доступ, используя:

знания о КС и умения работать с ней;

сведения о системе защиты информации;

сбои, отказы технических и программных средств;

ошибки, небрежность обслуживающего персонала и пользователей.

Методы и средства предотвращения несанкционированного доступа в КС разнообразны.

Для защиты информации от НСД создается система разграничения доступа к информации. Получить несанкционированный доступ к информации при наличии системы разграничения доступа (СРД) можно только при сбоях и отказах КС, а также используя слабые места в комплексной системе защиты информации. Чтобы использовать слабые места в системе защиты, злоумышленник должен о них знать.

Одним из путей добывания информации о недостатках системы защиты является изучение механизмов защиты. Злоумышленник может тестировать систему защиты путем непосредственного контакта с ней. В этом случае велика вероятность обнаружения системой защиты попыток ее тестирования. В результате этого службой безопасности могут быть предприняты дополнительные меры защиты, из которых выделяют:

методы и средства разграничения доступа к информации;

методы и средства защиты от исследования и копирования информации.

Более привлекателен для злоумышленников второй подход. Сначала получается копия программного средства системы защиты или техническое средство защиты, а затем производится исследование в лабораторных условиях. Кроме того, создание неучтенных копий на съемных носителях информации является одним из распространенных и удобных способов хищения информации. Этим способом осуществляется несанкционированное тиражирование программ. Скрытно получить техническое средство защиты для исследования гораздо сложнее, чем программное, и такая угроза блокируется средствами и методами, обеспечивающими целостность технической структуры КС.

Для блокирования несанкционированного исследования и копирования информации КС используется комплекс средств и мер защиты, которые объединяются в систему защиты от исследования и копирования информации (СЗИК).

1.16. Методы и средства предотвращения случайных угроз КС.

Они подразделяются на шесть групп.

Дублирование информации является одним из самых эффективных способов обеспечения целостности информации. Оно обеспечивает защиту информации как от случайных угроз, так и от преднамеренных воздействий.

В зависимости от ценности информации, особенностей построения и режимов функционирования КС могут использоваться различные методы дублирования информации, которые классифицируются по различным признакам.

По времени восстановления информации методы дублирования информации подразделяются на оперативные и неоперативные. К оперативным методам дублирования информации относятся методы, которые позволяют использовать дублирующую информацию в реальном масштабе времени. Это означает, что переход к использованию дублирующей информации осуществляется за время, которое позволяет выполнить запрос на использование информации в режиме реального времени для данной КС. Все методы, не обеспечивающие выполнение этого условия, относятся к неоперативным методам дублирования информации.

По виду копирования методы дублирования информации могут быть:

полного копирования;

зеркального копирования;

частичного копирования;

комбинированного копирования.

При полном копировании дублируются все файлы.

При зеркальном копировании любые изменения основной информации сопровождаются такими же изменениями дублирующей информации. При таком дублировании основная информация и дубль всегда идентичны.

Частичное копирование предполагает создание дублей определенных файлов, например файлов пользователя. Одним из видов частичного копирования, получившим название инкрементного копирования, является метод создания дублей файлов, измененных со времени последнего копирования.

Комбинированное копирование допускает комбинации, например, полного и частичного копирования с различной периодичностью их проведения.

По числу копий методы дублирования информации подразделяются на одноуровневые и многоуровневые.

Как правило, число уровней не превышает трех.

По применяемым для дублирования средствам методы дублирования информации подразделяются на использующие:

дополнительные внешние запоминающие устройства (ВЗУ);

специально выделенные области памяти на несъемных машинных носителях;

съемные носители информации.

По виду дублирующей информации методы дублирования информации подразделяются:

на методы со сжатием информации;

на методы без сжатия информации.

По удаленности носителей основной и дублирующей информации методы дублирования информации подразделяются на методы сосредоточенного и рассредоточенного дублирования.

Для определенности целесообразно считать методами сосредоточенного дублирования информации такие методы, для которых носители с основной и дублирующей информацией находятся в одном помещении. Все другие методы относятся к рассредоточенным.

Повышение надежности КС является одним из эффективных способов предотвращения случайных угроз КС.

Под надежностью понимается свойство системы выполнять возложенные на нее задачи в определенных условиях эксплуатации и установленный период времени. При наступлении отказа компьютерная система не может выполнять все предусмотренные документацией задачи, т.е. переходит из исправного состояния в неисправное. Если при наступлении отказа компьютерная система способна выполнять заданные функции, сохраняя значения основных характеристик в пределах, установленных технической документацией, то она находится в работоспособном состоянии.

С точки зрения обеспечения ИБ необходимо сохранять хотя бы работоспособное состояние КС. Для решения этой задачи необходимо обеспечить высокую надежность функционирования алгоритмов, программ и технических (аппаратных) средств.

Поскольку алгоритмы в КС реализуются за счет выполнения программ или аппаратным способом, то надежность алгоритмов отдельно не рассматривается. В этом случае считается, что надежность КС обеспечивается надежностью программных и аппаратных средств.

Надежность КС достигается на этапах их разработки, производства и эксплуатации.

Для программных средств рассматриваются этапы разработки и эксплуатации. Этап разработки программных средств – определяющий при создании надежных компьютерных систем.

На этом этапе основными направлениями повышения надежности программных средств являются:

корректная постановка задачи на разработку;

использование прогрессивных технологий программирования;

контроль правильности функционирования.

Корректность постановки задачи достигается в результате совместной работы специалистов предметной области и высокопрофессиональных программистов-алгоритмистов.

В настоящее время для повышения качества программных продуктов используются современные технологии программирования (например, CASE-технология). Эти технологии позволяют значительно сократить возможности внесения субъективных ошибок разработчиков. Они характеризуются высокой автоматизацией процесса программирования, использованием стандартных программных модулей, тестированием их совместной работы.

Контроль правильности функционирования алгоритмов и программ осуществляется на каждом этапе разработки и завершается комплексным контролем, охватывающим все решаемые задачи и режимы.

На этапе эксплуатации программные средства дорабатываются, в них устраняются замеченные ошибки, поддерживается целостность программных средств и актуальность данных, используемых этими средствами.

Надежность технических средств (ТС) КС обеспечивается на всех этапах. На этапе разработки выбираются элементная база, технология производства и структурные решения, обеспечивающие максимально достижимую надежность КС в целом.

Велика роль в процессе обеспечения надежности ТС и этапа производства. Главными условиями выпуска надежной продукции являются высокий технологический уровень производства и организация эффективного контроля качества выпускаемых ТС.

Удельный вес этапа эксплуатации ТС в решении проблемы обеспечения надежности КС в последние годы значительно снизился. Для определенных видов вычислительной техники, таких как персональные ЭВМ, уровень требований к процессу технической эксплуатации снизился практически до уровня эксплуатации бытовых приборов. Особенностью нынешнего этапа эксплуатации средств вычислительной техники является сближение эксплуатации технических и программных средств (особенно средств общего программного обеспечения). Тем не менее роль этапа эксплуатации ТС остается достаточно значимой в решении задачи обеспечения надежности КС и, прежде всего, надежности сложных компьютерных систем.

Применение отказоустойчивых КС - важный инструмент для предотвращения случайных угроз. Отказоустойчивость - это свойство КС сохранять работоспособность при отказах отдельных устройств, блоков, схем.

Известны три основных подхода к созданию отказоустойчивых систем:

простое резервирование информации или отдельных блоков;

помехоустойчивое кодирование информации;

создание адаптивных систем.

Любая отказоустойчивая система обладает избыточностью. Одним из наиболее простых и действенных путей создания отказоустойчивых систем является простое резервирование.

Простое резервирование основано на использовании устройств, блоков, узлов, схем, модулей и файлов программ только в качестве резервных. При отказе основного элемента осуществляется переход на использование резервного. Резервирование осуществляется на различных уровнях - на уровнях устройств, блоков, узлов, модулей, файлов и т.д. Резервирование отличается также и глубиной. Для целей резервирования может использоваться один резервный элемент и более. Уровни и глубина резервирования определяют возможность системы предотвратить отказы, а также аппаратные затраты.

Помехоустойчивое кодирование основано на использовании информационной избыточности. Рабочая информация в КС дополняется определенным объемом специальной контрольной информации. Наличие этой контрольной информации (контрольных двоичных разрядов) позволяет путем выполнения определенных действий

над рабочей и контрольной информацией определять ошибки и даже исправлять их. Так как ошибки являются следствием отказов средств КС, то, используя исправляющие коды, можно парировать часть отказов. Исправляющие возможности кодов для конкретного метода помехоустойчивого кодирования зависят от степени избыточности.

Помехоустойчивое кодирование наиболее эффективно при парировании самоустраняющихся отказов, называемых сбоями. Помехоустойчивое кодирование при создании отказоустойчивых систем, как правило, используется в комплексе с другими подходами повышения отказоустойчивости.

Наиболее совершенными системами, устойчивыми к отказам, являются адаптивные системы. В них достигается разумный компромисс между уровнем избыточности, вводимым для обеспечения устойчивости (толерантности) системы к отказам, и эффективностью использования таких систем по назначению.

В адаптивных системах реализуется так называемый принцип элегантной деградации, который предполагает сохранение работоспособного состояния системы при некотором снижении эффективности функционирования в случаях отказов ее элементов.

Оптимизация взаимодействия пользователей и обслуживающего персонала с КС подразумевает применение организационно-социальных методов и средств для предотвращения случайных угроз.

Одним из основных направлений защиты процессов переработки информации в КС от непреднамеренных угроз являются сокращение числа ошибок пользователей и обслуживающего персонала и минимизация последствий этих ошибок. Для достижения этих целей необходимы:

научная организация труда;

воспитание и обучение пользователей и персонала;

анализ и совершенствование процессов взаимодействия системы человек-машина (ЭВМ).

Научная организация труда предполагает:

оборудование рабочих мест;

оптимальный режим труда и отдыха;

дружественный интерфейс (связь, диалог) человека с КС.

Для оптимизации взаимодействия пользователей и обслуживающего персонала используют методы эргономики, оптимального сочетания режима труда и отдыха, современные методы упрощения взаимодействия человека с компьютерной системой в рамках совершенствования диалога, воспитание и обучение пользователей по соблюдению правил ИБ как на уровне государства, так и на уровне предприятия, фирмы, корпорации.

Важной задачей оптимизации взаимодействия человека с КС является также анализ этого процесса и его совершенствование. Анализ должен проводиться на всех жизненных этапах КС и направляться на выявление слабых звеньев. Слабые звенья заменяются или совершенствуются как в процессе разработки новых КС, так и в процессе модернизации существующих.

Минимизация ущерба от аварий и стихийных бедствий является группой методов и средств предотвращения случайных угроз и их последствий в работе КС.

Стихийные бедствия и аварии могут причинить огромный ущерб объектам КС. Предотвратить стихийные бедствия человек пока не в силах, но уменьшить последствия таких явлений во многих случаях удается. Минимизация последствий аварий и стихийных бедствий для объектов КС может быть достигнута путем:

правильного выбора места расположения объекта;

учета возможных аварий и стихийных бедствий при разработке и эксплуатации КС;

организации современного оповещения о возможных стихийных бедствиях;

обучения персонала борьбе со стихийными бедствиями и авариями, методам ликвидации их последствий.

Объекты КС по возможности должны располагаться в тех районах, где не наблюдается таких стихийных бедствий, как наводнения и землетрясения. Объекты необходимо размещать вдалеке от таких опасных объектов, как нефтебазы и нефтеперерабатывающие заводы, склады горючих и взрывчатых веществ, плотин и т.д.

На практике далеко не всегда удается расположить объект вдалеке от опасных предприятий или районов, в которых возможны стихийные бедствия. Поэтому при разработке, создании и эксплуатации объектов КС необходимо предусмотреть специальные меры. В районах возможных землетрясений здания должны быть сейсмостойкими. В районах возможных затоплений основное оборудование целесообразно размещать на верхних этажах зданий. Все объекты должны снабжаться автоматическими системами тушения пожара. На объектах, для которых вероятность стихийных бедствий высока, необходимо осуществлять распределенное дублирование информации и предусмотреть возможность перераспределения функций объектов. На всех объектах должны предусматриваться меры на случай аварии в системах электропитания. Для объектов, работающих с ценной информацией, требуется иметь аварийные источники бесперебойного питания и подвод электроэнергии производить не менее чем от двух независимых линий электропередачи.

Использование источников бесперебойного питания обеспечивает, по крайней мере, завершение вычислительного процесса и сохранение данных на внешних запоминающих устройствах. Для малых КС такие источники способны обеспечить работу в течение нескольких часов.

Потери информационных ресурсов могут быть существенно уменьшены, если обслуживающий персонал будет своевременно предупрежден о надвигающихся природных катаклизмах. В реальных условиях такая информация часто не успевает дойти до исполнителей.

Персонал должен быть обучен действиям в условиях стихийных бедствий и аварий, а также уметь восстанавливать утраченную информацию.

Блокировка ошибочных операций - это методический прием высокоэффективного исключения случайных угроз КС.

Ошибочные операции или действия могут вызываться отказами аппаратных и программных средств, а также ошибками пользователей и обслуживающего персонала. Некоторые ошибочные действия могут привести к нарушениям целостности, доступности и конфиденциальности информации. Ошибочная запись в оперативную память (ОП) и на ВЗУ, нарушение разграничения памяти при мультипрограммных режимах работы ЭВМ, ошибочная выдача информации в канал связи, короткие замыкания и обрыв проводников - вот далеко не полный перечень ошибочных действий, которые представляют реальную угрозу безопасности информации в КС.

Для блокировки ошибочных действий используются технические и аппаратно-программные средства.

1.17. Комплексные организационно-технические методы и средства устранения или нейтрализации угроз

К техническим и аппаратно-программным средствам относятся: применение современных технологий программирования, автоматизированных систем разработки программных средств (ПС), применение комплексных контрольно-испытательных стендов, организация защиты аппаратных средств на этапах разработки, производства и эксплуатации и т.д.

Современные технологии программирования предполагают высокую степень автоматизации процессов создания, отладки и тестирования программ. Применение стандартных модулей позволяет упростить процесс создания программ, поиска ошибок и закладок.

Для разработки программных средств, свободных от ошибок и закладок, необходимо выполнение следующих условий:

использование объектно-ориентированного программирования;

наличие автоматизированной системы разработки программных средств;

применение комплексного контрольно-испытательного стенда;

наличие аппаратных средств для обнаружения закладок;

организация защиты КС.

Одним из перспективных направлений создания программного обеспечения повышенной безопасности является использование объектно-ориентированного программирования, идущего на смену структурному программированию.

Применение объектно-ориентированного программирования (ООП) позволяет разделить фазы описания и фазы реализации абстрактных типов данных. Два выделенных модуля допускают раздельную компиляцию. В модуле описания задаются имена и типы внутренних защищенных и внешних данных, а также перечень процедур (методов) с описанием типов и количества параметров для них. В модуле реализации находятся собственно процедуры, обрабатывающие данные. Такое разделение повышает надежность программирования, так как доступ к внутренним данным возможен только с помощью процедур, перечисленных в модуле описания. Это позволяет определять большую часть ошибок в обработке абстрактного типа данных на этапе компиляции, а не на этапе выполнения. Анализ программных средств на наличие закладок облегчается, так как допустимые действия с абстрактными данными задаются в модуле описания, а не в теле процедур.

Одним из центральных понятий ООП является понятие «класс». С помощью этого понятия осуществляется связывание определенного типа данных с набором процедур и функций, которые могут манипулировать с этим типом данных.

Преимущество ООП заключается также в предоставлении возможности модификации функционирования, добавления новых свойств или уничтожении ненужных элементов, не изменяя того, что уже написано и отлажено. Пользователю достаточно определить объекты, принадлежащие к уже созданным классам, и посылать им сообщения. При этом контроль безопасности программного продукта сводится к анализу модулей описания классов. Если класс из библиотеки классов не удовлетворяет разработчика, то он может создать класс, производный от базового, произвести в нем необходимые изменения и работать с объектами полученного производного класса. Если данные и методы базового класса не должны быть доступны в производных классах, то их следует описать как внутренние.

Автоматизированные системы разработки программных средств - одно из эффективных средств защиты процессов переработки информации не только на этапе разработки, но и при эксплуатации программных продуктов. Особенного эффекта можно добиться в процессах нейтрализации угроз как от закладок, так и от непреднамеренных ошибок персонала.

Автоматизированная система (АС) создается на базе локальной вычислительной сети (ЛВС). В состав ЛВС входят рабочие станции программистов и сервер администратора. Программисты имеют полный доступ только к информации своей ЭВМ и доступ к ЭВМ других программистов в режиме чтения. С рабочего места администратора возможен доступ в режиме чтения к любой ЭВМ разработчиков.

База данных алгоритмов разрабатываемого программного средства находится на сервере администратора и включает в себя архив утвержденных организацией-разработчиком и контролирующей организацией алгоритмов программного средства в виде блок-схем, описания на псевдокоде для их контроля администратором.

На сервере администратора располагается база данных листингов программ разрабатываемого программного средства, включающая в себя архив утвержденных организацией-разработчиком и контролирующей организацией программ для их контроля

администратором с применением программ сравнения листингов и поиска измененных и добавленных участков программ.

На сервере администратора находится также база данных эталонных выполняемых модулей программ разрабатываемого программного средства для их контроля с применением программ поиска изменений в этих модулях.

Программы контроля версий листингов программ и сравнения выполняемых модулей должны быть разработаны организацией, не связанной ни с организацией-разработчиком, ни с контролирующей организацией, и должны контролировать программы любого назначения.

Контроль за безопасностью разработки может осуществляться следующим образом. Администратор в соответствии со своим графиком без уведомления разработчиков считывает в базы данных листинги программ и выполняемые модули. С помощью программ сравнения администратор выявляет и анализирует изменения, которые внесены разработчиком, по сравнению с последним контролем.

По мере разработки выполняемых модулей в базе администратора накапливаются готовые к сдаче заказчику эталонные образцы выполняемых модулей, сохранность которых контролируется администратором.

Применение такой организации работ позволяет администратору выявлять закладки и непреднамеренные ошибки на всех стадиях разработки программного средства. Администратор не может сам внедрить закладку, так как у него нет права на модификацию программ, разрабатываемых программистами.

Одним из наиболее эффективных путей обнаружения закладок и ошибок в разрабатываемых программных средствах является применение комплексного контрольно-испытательного стенда разрабатываемой системы. Он позволяет анализировать программные средства путем подачи многократных входных воздействий на фоне изменяющихся внешних факторов, с помощью которых имитируется воздействие возможных закладок. Таким образом, контрольно-испытательный стенд может рассматриваться как детальная имитационная модель разрабатываемой системы, позволяющая обеспечивать всесторонний анализ функционирования разрабатываемого программного средства в условиях воздействия закладок.

Контрольно-испытательный стенд должен отвечать следующим требованиям:

должен быть построен как открытая система, допускающая модернизацию и наращивание возможностей;

должен обеспечивать адекватность структуры и информационных потоков структуре и информационным потокам реальной системы;

должен удовлетворять взаимозаменяемость программных модулей модели и реальной системы;

должен позволять проводить как автономные испытания модулей, так и всего программного средства в целом.

Контрольно-испытательный стенд может содержать следующие блоки:

модуль системы, который состоит из программных блоков и программных модулей реальной системы;

модуль конфигурации модели системы, осуществляющий регистрацию и динамическое включение программных модулей

реальной системы и блоков программных модулей из соответствующих баз данных;

база данных моделей угроз для накопления и модификации моделей угроз, представленных в формализованном виде;

модуль формирования входных воздействий, учитывающий возможные угрозы, ограничения на входную информацию и результаты тестирования на предыдущем шаге;

модель внешних воздействий, предназначенная для учета воздействий, внешних по отношению к моделируемой системе;

модуль анализа результатов тестирования.

Выполняемые модули программных средств проверяются в процессе сертификации на специальных аппаратно-программных стендах, способных имитировать функционирование испытываемого программного средства на допустимом множестве входных и внешних воздействий. При контроле выполняется операция, обратная транслированию, - дизассемблирование. Для упрощения анализа выполняемых модулей применяются также отладчики, программы-трассировщики, которые позволяют проконтролировать последовательность событий, порядок выполнения команд.

Наличие аппаратных средств для обнаружения закладок на этапе разработки, производства и эксплуатации является эффективным приемом устранения и нейтрализации угроз.

Аппаратные закладки могут внедряться не только в процессе разработки и модернизации, но и в процессе серийного производства, транспортирования и хранения аппаратных средств.

Для защиты от внедрения аппаратных закладок кроме следования общим принципам защиты необходимо обеспечить всестороннюю проверку комплектующих изделий, поступающих к разработчику (производителю) извне.

Комплектующие изделия должны подвергаться тщательному осмотру и испытанию на специальных стендах. Испытания проводятся путем подачи всех возможных входных сигналов во всех допустимых режимах.

Если полный перебор всех комбинаций входных сигналов практически невозможен, то используются вероятностные методы контроля. Чаще всего вероятностное тестирование осуществляется путем получения комбинаций входных сигналов с помощью датчика случайных чисел и подачи этих сигналов на тестируемое и контрольное изделие. В качестве контрольного используется такое же изделие, как и тестируемое, но проверенное на отсутствие закладок, ошибок и отказов. Выходные сигналы обоих изделий сравниваются. Если они не совпадают, то принимается решение о замене тестируемого изделия.

При испытаниях изделий путем подачи детерминированных последовательностей входных сигналов и сравнения выходных сигналов с эталонами часто используются методы сжатия выходных сигналов (данных). Это позволяет сократить объем памяти, необходимый для размещения эталонов выходных сигналов.

Для исследования неразборных конструкций (микросхем, конденсаторов, резисторов, печатных плат и др.) применяются рентгеновские установки. При необходимости осуществляется послойное рентгеновское исследование изделий.

В процессе производства основное внимание уделяется автоматизации технологических процессов и контролю за соблюдением технологической дисциплины. Особо ответственные операции могут производиться под наблюдением должностных лиц с последующим документальным оформлением.

Этапы разработки, производства и модернизации аппаратных средств КС завершаются контролем на наличие конструктивных ошибок, производственного брака и закладок.

Блоки и устройства, успешно прошедшие контроль, хранятся и транспортируются таким образом, чтобы исключалась возможность внедрения закладок.

Организация защиты КС от несанкционированного доступа и изменения ее структур в процессе эксплуатации обеспечивается методологией разграничения доступа к оборудованию.

При эксплуатации КС неизменность аппаратной и программной структур возможна за счет предотвращения несанкционированного доступа к аппаратным и программным средствам, а также за счет организации постоянного контроля за целостностью этих средств.

Несанкционированный доступ к аппаратным и программным средствам может быть исключен или существенно затруднен при выполнении следующего комплекса мероприятий:

охрана помещений, в которых находятся аппаратные средства КС;

разграничение доступа к оборудованию;

противодействие несанкционированному подключению оборудования;

защита внутреннего монтажа, средств управления и коммутации от несанкционированного вмешательства;

противодействие внедрению вредительских программ.

Достижение высокого уровня безопасности невозможно без принятия должных организационных мер. С одной стороны, эти меры должны быть направлены на обеспечение правильности функционирования механизмов защиты и выполняться администратором безопасности системы. С другой стороны, руководство организации, эксплуатирующей средства автоматизации, должно регламентировать правила автоматизированной обработки информации, включая и правила ее защиты, а также установить меру ответственности за нарушение этих правил.

1.18. Программа информационной безопасности

Управленческие аспекты разработки и реализации информационной безопасности предполагают наличие совокупности организационных мер в виде развернутой программы, которую целесообразно структурировать по уровням, обычно в соответствии со структурой организации. В большинстве случаев достаточно двух уровней: верхнего (организационно-управленческого), который охватывает всю организацию и корпоративную ИС, и нижнего (или сервисного), который относится к отдельным подсистемам ИС и сервисам.

Программу верхнего уровня формирует и возглавляет лицо, отвечающее за информационную безопасность организации. Эти обязанности, как правило, входят в обязанности руководителя ИТ-подразделения (Chief Information Officer - CIO). Программа должна содержать следующие главные цели:

стратегическое планирование в области развития информационной безопасности;

разработку и исполнение политики в области ИБ;

оценка рисков и управление рисками;

координация деятельности в области информационной безопасности: выбор эффективных средств защиты, их приобретение или разработка, внедрение, эксплуатация, пополнение и распределение ресурсов, обучение персонала;

контроль деятельности в области ИБ.

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

Контроль деятельности в области безопасности имеет двоякую направленность. Во-первых, необходимо гарантировать, что действия организации не противоречат федеральным и региональным законам и нормативным актам. Необходимо постоянно следить за изменениями во внешней среде, приводящие к возможности возникновения угроз. Во-вторых, нужно постоянно отслеживать состояние безопасности внутри организации, реагировать на все случаи нарушений, вырабатывать стратегию развития защитных мер с учетом изменения обстановки во внешней и внутренней средах.

Цель программы нижнего уровня - обеспечить надежную и экономичную защиту информационных подсистем, конкретных сервисов или групп однородных сервисов. На этом уровне решается, какие механизмы защиты использовать, закупаются и устанавливаются технические средства, выполняется повседневное администрирование,

отслеживается состояние слабых мест, проводится первичное обучение персонала и т.п. Обычно за программу нижнего уровня отвечают ответственные менеджеры по обеспечению ИБ, системные администраторы и администраторы сервисов. В плане безопасности важнейшим действием на этом этапе является оценка критичности как самого сервиса, так и информации, которая с его помощью будет обрабатываться. Необходимо сформулировать ответы на следующие вопросы:

Какие данные и информацию будет обслуживать данный сервис?

Каковы возможные последствия нарушения конфиденциальности, целостности и доступности этой информации?

Каковы угрозы, по отношению к которым данные, информация, сервис и пользователь будут наиболее уязвимы?

Существуют ли какие-либо особенности сервиса, требующие принятия специальных мер, например, территориальная распределённость компонентов ИС?

Каковы должны быть характеристики персонала, имеющие отношение к безопасности: компьютерная квалификация, дисциплинированность, благонадежность?

Каковы законодательные положения и корпоративные правила, которым должен удовлетворять сервис?

Результаты оценки критичности являются отправной точкой в составлении спецификаций на приобретение или разработку сервисов. Кроме того, они определяют ту меру внимания, которую служба безопасности организации должна уделять сервису или группе сервисов на всех этапах его жизненного цикла.

Сделаем существенную оговорку. Программа безопасности не является воплощением простого набора технических средств, встроенных в информационную систему, у системы ИБ есть важнейшие «политический» и управленческий аспекты. Программа должна официально приниматься и поддерживаться высшим руководством, у нее должны быть определенные штаты и выделенный бюджет. Без подобной поддержки приказы, распоряжения и «призывы» к исполнению программы останутся пустым звуком.

1.19. Модели ИБ, требования и основные этапы реализации информационной безопасности

Главная цель мер, предпринимаемых на управленческом уровне, - сформировать единую концепцию и программу работ в области информационной безопасности (ИБ) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя текущее состояние системы ИБ.

Практически это можно осуществить, разработав концептуальную, математическую и функциональную модели представления информационной защиты, которая позволяет решать задачи создания, использования, сопровождения, развития и оценки эффективности общей системы ИБ (рис.1.18).

Математическая модель представляет собой формализованное описание сценариев в виде логико-алгоритмической последовательности действий нарушителей и ответных мер. Расчетные количественные значения параметров модели характеризуют функциональные (аналитические, алгоритмические или численные) зависимости, описывающие процессы взаимодействия нарушителей с системой защиты и возможные результаты действий. Именно такой вид модели чаще всего используется для количественных оценок уязвимости объекта, построения алгоритма защиты оценки рисков и эффективности принятых мер (рис.1.18).

Рис.1.18. Содержание модели информационной безопасности

При построении теоретических моделей систем защиты информации (СЗИ) и информационных ресурсов необходимо опираться на следующие важнейшие обстоятельства:

– выбор математически строгих критериев для оценки оптимальности системы защиты информации для данной архитектуры ИС;

– четкая математическая формулировка задачи построения модели СЗИ, учитывающая заданные требования к системе защиты и позволяющая построить СЗИ в соответствии с этими критериями.

Такие модели для разных компаний могут быть разнообразными, но любая из них должна обладать следующими свойствами: универсальность, комплексность, наглядность, простота использования, практическая реализуемость, измеримость с помощью наборов метрик, «самообучаемость» (возможность наращивания знаний), надежное функционирование в условиях высокой неопределенности исходной информации.

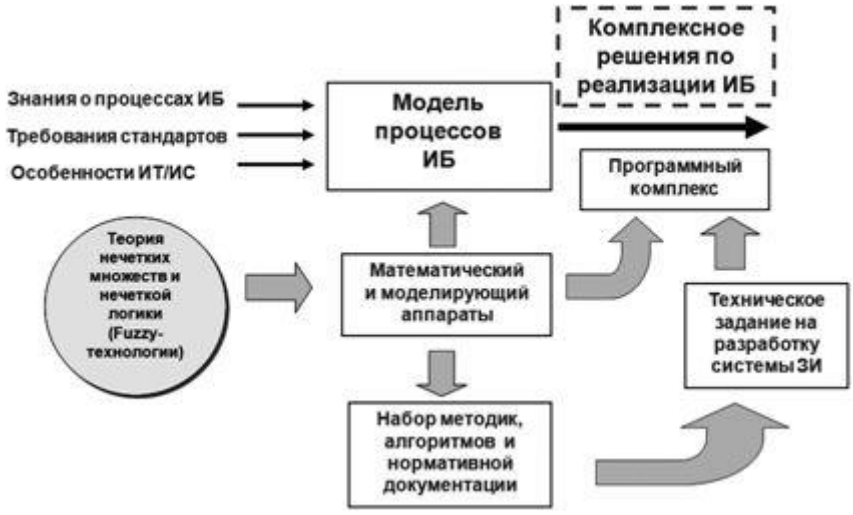

Рис.1.19. Место математической модели в реализации концепции и программы ИБ

Ниже указаны основные этапы построения модели:

– анализ структуры информационно-вычислительной системы и уровня необходимой защиты данных и самой ИС;

– анализ изменяющихся характеристик СЗИ, определяемых динамикой воздействия угроз (адаптивные СЗИ);

– анализ корреляционных зависимостей между различными параметрами СЗИ, являющимися результатом решения конкретных задач по защите информации;

– анализ возможного понижения общего уровня защищенности из-за наличия корреляций;

– определение совокупностей задач защиты для определения контролируемых параметров СЗИ;

– формирование требований и рекомендаций по рациональной организации структуры ИБ.

Для контроля параметров реализуемых моделей СЗИ необходимо формировать системы количественных показателей (метрик), с помощью которых оценивается:

– сложность структуры, поведение и диагностирование нормальной работы СЗИ с учетом обеспечения её устойчивости в условиях быстро изменяющихся условий внешней и внутренней среды;

– нормальное функционирование контролируемых зон СЗИ; определение и оценка направленных угроз, выявление уязвимостей, управление рисками и т.д.

– работоспособность и возможность диагностирования нарушений нормальной работы СЗИ на базе адаптивных моделей.

В настоящее время адаптивные модели с использованием нейронечетких классификаторов чаще всего строятся в терминах теории нечетких множеств (Fuzzy Sets) и нечеткой логики (Fuzzy Logic) по следующей схеме (рис.1.20).

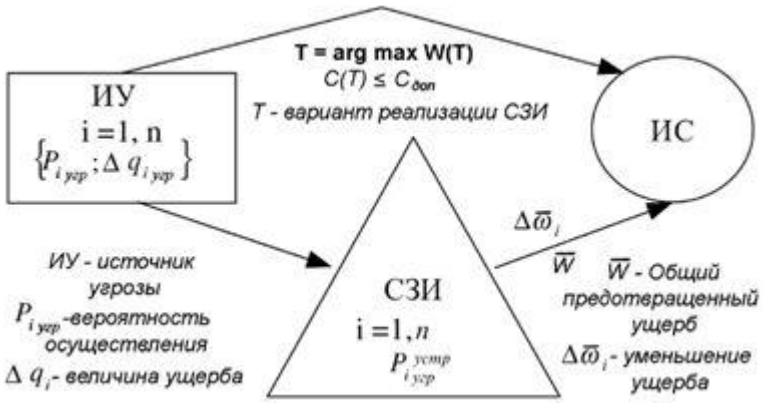

Рис.1.20 . Схема построения модели СЗИ

Адаптивность модели на базе нейронных сетей (НС) позволяет при ограниченных затратах на организацию системы ИБ обеспечить заданный уровень безопасности ИТ-системы за счет быстрой реакции системы на изменение поля угроз. При этом очень важным качеством является возможность накопления и передачи опыта системой ЗИ.

Распределенные поля нейрочетких и нейронечетких сетей аккумулируют знания в процессе развития защищаемой ИТ-системы, производят адаптацию к изменению поля угроз и эти знания могут передаваться в последующие версии ИТ-системы. Так формируется процесс наследования.

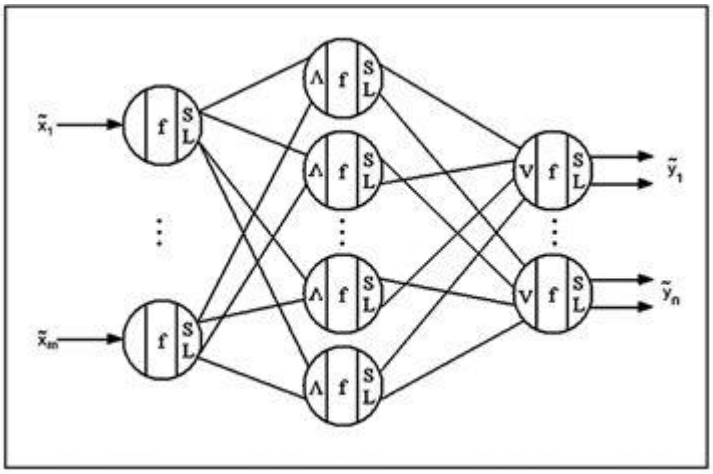

Рис.1.21 Схема нейронечеткого классификатора

На рис.1.21 показана одна из возможных схем такого классификатора. Обозначения здесь следующие: X - вектор угроз, Y - вектор заключений о защищенности системы, F - совокупность формальных нейронов классификатора для выполнения операций композиции над нечеткими заключениями, L и S - нижняя и верхняя границы уровня угроз, V - совокупность весовых коэффициентов, описывающих веса связей между различными взаимодействующими нейронами классификатора.

Обучение нейронечеткого классификатора на наборе $\mathrm{X}\,(i = 1, \ldots, m)$ векторов известных угроз (обучающая выборка) выявляет и позволяет устранить из структуры нейронной сети незначащие связи (слабые неточные заключения в системы нечетких правил, имеющие минимальные веса). Обучение такой НС в виде многослойной структуры с нечеткими связями не требует выполнения сложных математических расчетов, что позволяет снизить трудоемкость решения задачи обучения адаптивной СЗИ (рис.1.22).

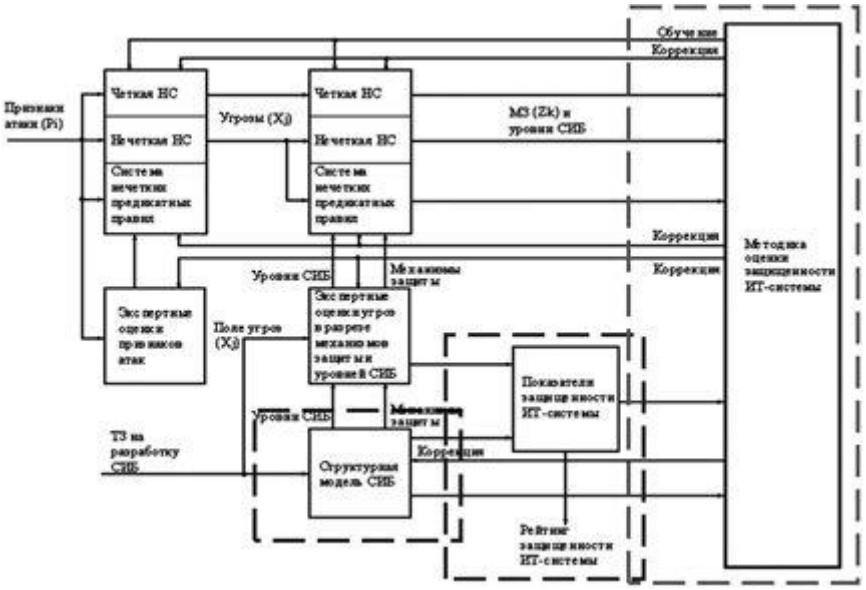

Рис.1.22 Адаптивная модель СЗИ на базе нейронных сетей

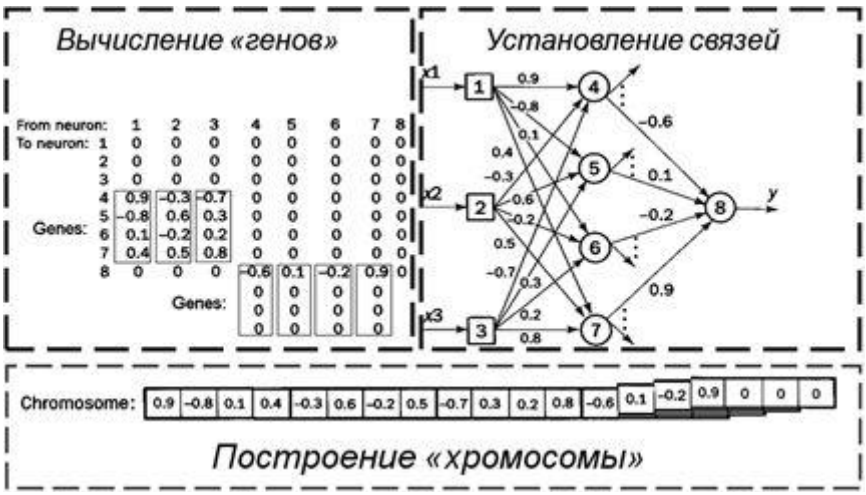

Рис.1.23 Схема работы генетического алгоритма

Минимизацию ошибки в такой адаптивной системе, построенной на базе нейронных сетей, можно эффективно осуществлять с использованием генетических алгоритмов, где в качестве генов хромосомы используются векторы итерационно перевычисляемых весов связей, ассоциированных с входными значениями X (рис.1.23).

Основное назначение функциональной модели СЗИ - практическое обеспечение процесса создания системы ИБ за счет оптимизации принимаемых решений и выбора рационального варианта технической реализации (рис.1.24).

Рис.1.24 Формирование требований к системе информационной безопасности

На рис.1.24 в общем виде представлена модель требований, на основании которых формируются спецификации и организационные меры для приобретения готовых решений или разработки программно-аппаратных средств, реализующих систему информационной защиты

Вне зависимости от размеров организации и специфики ее информационной системы, работы по обеспечению режима ИБ в том или ином виде должны содержать этапы, представленные на рис.1.25. При этом важно не упустить каких-либо существенных аспектов. Это будет гарантировать некоторый минимальный (базовый) уровень ИБ, обязательный для любой информационной технологии или информационной системы.

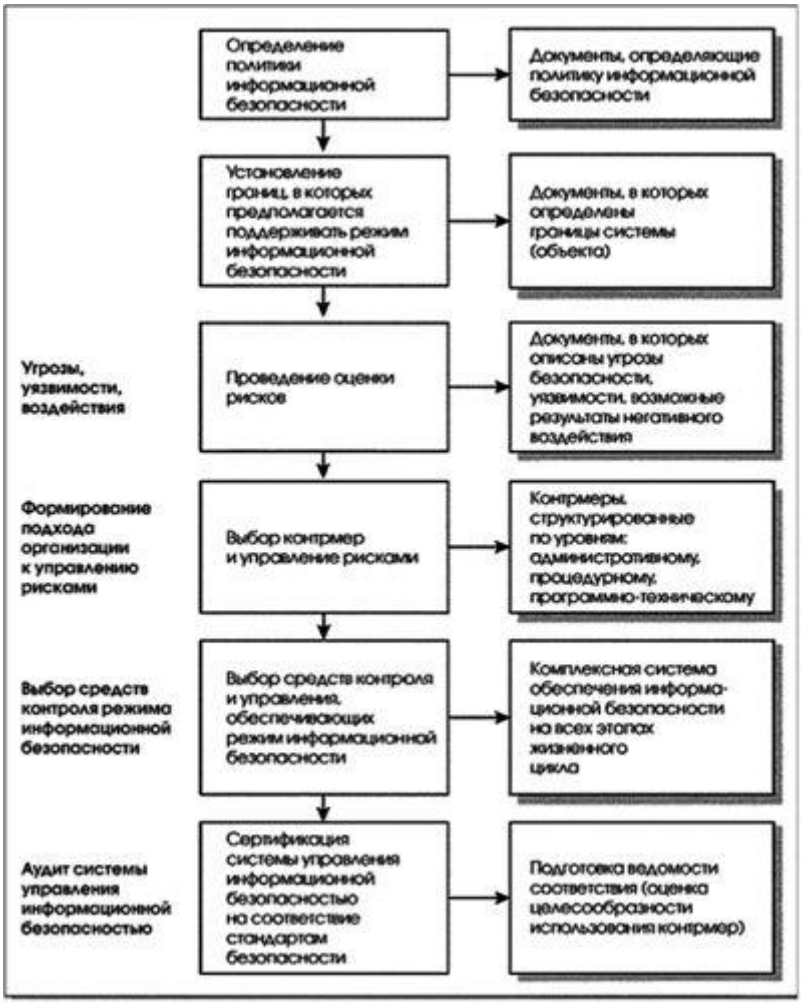

Рис.1.25 Основные этапы обеспечения информационной безопасности

Для обеспечения базового уровня ИБ используется упрощенный подход к анализу рисков, при котором рассматривается стандартный набор наиболее распространенных угроз безопасности без детальной оценки их вероятностей. Для нейтрализации угроз применяется типовой набор контрмер, а вопросы эффективности защиты рассматриваются в отдельных важных случаях.

Подобный подход приемлем, если ценность защищаемых ресурсов с точки зрения организации не является чрезмерно высокой.

Отметим объективные трудности, с которыми можно столкнуться при моделировании системы информационной защиты:

1. Трудность построения формальных моделей СЗИ определяется, в целом, неопределенностью условий функционирования ИС.
2. Постановка задачи обеспечения защиты информации часто оказывается некорректной, поскольку формулируется в условиях непредсказуемости поведения системы защиты в нестандартных и особенно экстремальных ситуациях.
3. В связи с этим задачи обеспечения безопасности вычислительных и информационных систем, как правило, не обладают свойством единственности решения.
4. Эффективность и оптимальность определяются степенью учета ограничений, налагаемых СЗИ для конкретных ситуаций, – в общем случае трудно сформировать модель, пригодную для всех возможных ситуаций, связанных с угрозами.
5. Быстрое развитие информационных технологий заставляет пересматривать концепции и программы информационной защиты, что однозначно приводит к необходимости пересматривать текущие модели СЗИ.

Однако математическое и функциональное моделирование чрезвычайно важно и необходимо. В результате моделирования получаем: оценку возможности реализации различных средств защиты информации в современных системах обработки данных; архитектуру системы защиты, согласованную с архитектурой ИС и информационной инфраструктурой предприятия; количественную оценку качества функционирования СЗИ; оценку экономической и практической эффективности реализуемой модели СЗИ.

1.20. Политика информационной безопасности

Основой программы обеспечения ИБ является многоуровневая политика информационной безопасности, отражающая подход организации к защите своих информационных активов и ресурсов (рис.1.26).

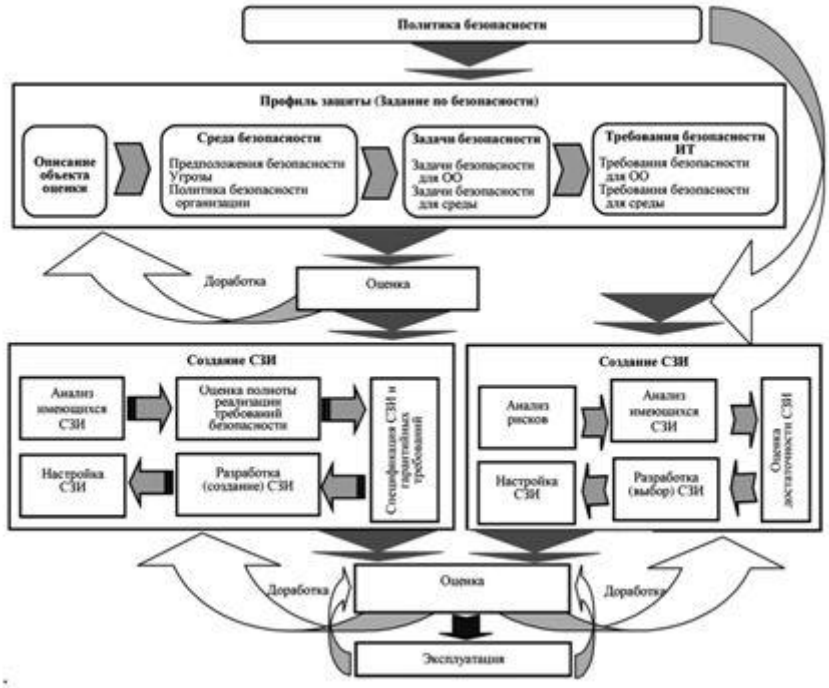

Рис.1.26 Системное содержание политики информационной безопасности

Под политикой информационной безопасности понимается совокупность документированных методологий и управленческих решений, а также распределение ролей и ответственности, направленных на защиту информации, информационных систем и ассоциированных с ними ресурсов.

Политика безопасности является важнейшим звеном в формировании ИБ, поэтому принятие решения о её разработке, внедрении и неукоснительном выполнении всегда принимается высшим руководством организации. Политика разрабатывается на основе концепции и программы информационной безопасности. Как системный документ, политика включает в себя общую (концептуально-программную) часть и совокупность частных политик, относящихся к различным аспектам деятельности компании.

В идеале политика информационной безопасности должна быть реалистичной и выполнимой, а также не приводить к существенному снижению общей производительности бизнес-подразделений компании. Политика безопасности должна содержать основные цели и задачи организации режима информационной безопасности, четко содержать описание области действия, а также указывать на контактные лица и их обязанности.

Вводная часть «Общей политики безопасности» должна быть краткой и понятной, содержать не более двух-четырёх (максимум пяти) страниц текста. При этом важно учитывать, как политика безопасности будет влиять на уже существующие информационные системы компании. Как только политика утверждена, она должны быть предоставлена всем сотрудникам компании для ознакомления. Наконец, политика безопасности должна пересматриваться ежегодно, чтобы отразить текущие изменения в развитии бизнеса компании и в её программно-аппаратном, сетевом и информационном обеспечении.

Формирование, актуализация и совершенствование политики ИБ является многоаспектным циклическим (итерационным) процессом (рис.1.27), реализация которого сводится к следующим практическим шагам.

Рис.1.27 Итерационный процесс разработки и реализации политики ИБ

1. Определение используемых руководящих документов и стандартов в области ИБ, а также основных положений политики ИБ, включая:

– принципы администрирования системы ИБ и управление доступом к вычислительным и телекоммуникационным средствам, программам и информационным ресурсам, а также доступом в помещения, где они располагаются;

– принципы контроля состояния систем защиты информации, способы информирования об инцидентах в области ИБ и выработку корректирующих мер, направленных на устранение угроз;

– принципы использования информационных ресурсов персоналом компании и внешними пользователями;

– антивирусную защиту и защиту против действий хакеров;

– вопросы резервного копирования данных и информации;

– проведение профилактически, ремонтных и восстановительных работ;

– обучение и повышение квалификации персонала.

2. Разработка методологии выявления и оценки угроз и рисков их осуществления, определение подходов к управлению рисками: достаточен ли базовый уровень защищенности или требуется проводить полный вариант анализа рисков.

3. Структуризация контрмер по уровням требований к безопасности.

4. Порядок сертификации на соответствие стандартам в области ИБ.

Должна быть определена периодичность проведения совещаний по тематике ИБ на уровне руководства, включая периодический пересмотр положений политики ИБ, а также порядок обучения всех категорий пользователей информационной системы по вопросам ИБ.

С практической точки зрения политику безопасности целесообразно разделить на три уровня. К верхнему уровню можно отнести решения, затрагивающие организацию в

целом. Они носят общий характер и, как правило, исходят от высшего руководства организации:

– формулировка целей, которые преследует организация в области информационной безопасности, определение общих направлений и средств для достижения этих целей;

– формирование или пересмотр комплексной программы обеспечения информационной безопасности, определение ответственных менеджеров и технических руководителей за реализацию и сопровождение программы;

– обеспечение правовой базы для соблюдения государственных законов и корпоративных правил;

– формулировка общих управленческих решений по тем вопросам реализации программы безопасности, которые должны рассматриваться на уровне организации в целом.

На верхнем уровне политики 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 случаев потерь, повреждений или искажений данных. Для организации, занимающейся продажами, вероятно, важна актуальность информации о предоставляемых услугах и ценах, а также ее доступность максимальному числу потенциальных покупателей. «Режимная» организация в первую очередь заботится о защите от несанкционированного доступа - конфиденциальности.

На верхний уровень выносится управление защитными ресурсами и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем, поддержание контактов 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. В политике должны быть определены обязанности должностных лиц по выработке программы безопасности и по проведению ее в жизнь.

Политика верхнего уровня имеет дело с тремя аспектами законопослушности и исполнительской дисциплины:

– организация должна соблюдать существующие законы, государственные нормативные акты, корпоративные нормативные положения и стандарты;

– следует контролировать все действия направленные на выработку программы безопасности и назначить ответственных лиц на уровне высшего менеджмента за разработку, внедрение и неукоснительное исполнение принятой программы;

– необходимо обеспечить определенную степень исполнительности и послушания персонала, а для этого нужно выработать систему общего и персонального обучения и эффективной мотивации.

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

К среднему уровню можно отнести вопросы, касающиеся отдельных аспектов информационной безопасности, но важные для различных систем, эксплуатируемых организацией. Примеры таких вопросов: широкий доступ в Интернет и сочетание свободы получения информации с защитой от внешних угроз, использование домашних компьютеров, применение пользователями неофициального или несанкционированного 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

обеспечение, которое не было одобрено и/или закуплено и внедрено на уровне организации.

Область применения. Следует специфицировать, где, когда, как, по отношению к кому и чему применяется данный аспект политики безопасности. Например, касается ли организаций-субподрядчиков политика отношения к неофициальному программному обеспечению. Затрагивает ли она работников, пользующихся карманными компьютерами и ноутбуками и вынужденных переносить информацию на производственные машины.

Позиция организации. Продолжая пример с неофициальным программным обеспечением, можно обозначить позиции полного запрета или выработки процедуры приемки и использования подобного обеспечения и т.п. Позиция может быть сформулирована в общем виде, как набор целей, которые преследует организация в данном аспекте. Вообще говоря, содержание документов по политике безопасности, как и перечень таких документов, может быть существенно различным для разных организаций.

Роли, обязанности и ответственность. В документ необходимо включить информацию о должностных лицах, отвечающих за проведение политики безопасности в жизнь. Например, если для использования работником неофициального программного обеспечения нужно официальное разрешение, то должно быть известно, у кого и как его следует получать. Если должны проверяться дискеты, принесенные с других компьютеров, необходимо описать процедуру проверки. Если неофициальное программное обеспечение использовать нельзя, следует знать, кто следит за выполнением данного правила.

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

Точки контакта. Должно быть известно, куда и к каким документам следует обращаться за разъяснениями, помощью и дополнительной информацией. Обычно «точкой контакта» служит должностное лицо и/или доступный раздел соответствующей библиотеки или хранилища.

Политика безопасности нижнего уровня относится к конкретным сервисам. Она включает в себя конкретные цели и задачи, правила и способы их достижения. В отличие от двух верхних уровней рассматриваемая политика должна быть гораздо детальнее. Есть много вещей, специфичных для отдельных сервисов, которые нельзя единым образом регламентировать в рамках всей организации. В то же время эти вещи настолько важны для обеспечения режима безопасности, что решения, относящиеся к ним, должны приниматься на управленческом, а не на техническом уровне. Типичные вопросы, на которые следует дать ответ при следовании политики безопасности нижнего уровня:

– кто имеет право доступа к объектам, поддерживаемым сервисом;
– при каких условиях можно читать и модифицировать данные;
– как организован удаленный доступ к сервису;
– кто имеет право модернизировать сервис и т.д.

При формулировке целей политика нижнего уровня может исходить из соображений целостности, доступности и конфиденциальности, но она не должна останавливаться только на них. Например, если речь идет о системе расчета заработной платы, можно поставить цель, чтобы только работникам бухгалтерии и отдела кадров позволялось вводить и модифицировать информацию. В общем случае цели должны связывать между собой объекты сервиса и осмысленные действия с ними.

Исходя из целей, формулируются правила безопасности, описывающие, кто, что и при каких условиях может делать. Чем детальнее правила, чем более формально они изложены, тем проще поддержать их выполнение программно-техническими мерами и средствами.

Для разработки и внедрения политики ИБ, как правило, создаётся рабочая группа. Формирование такой группы по информационной безопасности актуально, прежде всего, для крупных компаний, в которых процесс изменения информационных технологий

является постоянным, в него вовлечено большое количество людей, поэтому так важно предусмотреть механизм, предоставляющий им возможность постоянного общения. Создание рабочей группы, имеющей свой информационный ресурс (форум) в Интернете, позволяет обеспечить соответствующую координацию комплекса вопросов по обеспечению ИБ и избежать проблем, связанных с недостаточной информированностью всех заинтересованных лиц. Фактически с точки зрения российских реалий такой форум является постоянно действующим органом компании, включающим в свой состав представителей наиболее значимых подразделений компании, а также сотрудников служб информационной, экономической и общей безопасности.

К компетенции этого органа относится разработка динамической модели информационной безопасности, включающей:

– разработку, обсуждение и принятие концепции (политики) информационной безопасности, внесение изменений и принятие новой версии концепции, согласование списков ответственных лиц;

– отслеживание и анализ важных изменений в структуре информационных ресурсов компании на предмет выявления новых угроз информационной безопасности;

– изучение и анализ инцидентов, связанных с безопасностью;

– принятие важных инициатив по усилению мер безопасности.

Рабочая группа является ведущим органом по проведению организационно-режимных процессов и разработке стандартов организации, определяющих режим работы компании в части, касающейся информационной безопасности. Она отвечает за исполнение концепции (политики) информационной безопасности и может быть создана не только в рамках компании, но и в рамках ее крупных структурных подразделений. К компетенции этой рабочей группы относятся следующие вопросы:

– выработка соглашений о разграничении ответственности за обеспечение информационной безопасности внутри компании;

– выработка специальных методик и политик, связанных с информационной безопасностью: анализ рисков, классификация систем и информации по уровням безопасности;

– поддержание в организации «атмосферы» информационной безопасности, в частности, регулярное информирование персонала по этим вопросам;

– обеспечение обязательности учета вопросов информационной безопасности при стратегическом и оперативном планировании;

– обеспечение обратной связи (оценка адекватности принимаемых мер безопасности в существующих системах) и координация внедрения средств обеспечения информационной безопасности в новые системы или сервисы;

– анализ инцидентов в области информационной безопасности, выработка рекомендаций по их предотвращению.

В рабочую группу должны входить специалисты следующих подразделений: представитель высшего менеджмента в лице заместителя генерального директора или технической дирекции (департамента), службы общей безопасности, кадровой службы, служб экономической и информационной безопасности, юридической службы, представители аналитических отделов и служб, а также службы менеджмента качества.

Распределение ответственности за обеспечение безопасности включает необходимость выполнения следующих действий:

– определение ресурсов, имеющих отношение к информационной безопасности по каждой системе;

– назначение для каждого ресурса (или процесса) ответственного сотрудника из числа руководителей. Разграничение ответственности должно быть закреплено документально;

– определение и документальное закрепление для каждого ресурса списка прав доступа (матрицы доступа).

Совершенно очевидно, что реализация политики информационной безопасности вовлекает много специалистов высокого класса и требует существенных затрат. Во всех случаях необходимо найти разумный компромисс, когда за приемлемую цену будет обеспечен приемлемый уровень безопасности, а работники не окажутся чрезмерно ограничены в использовании необходимых информационных ресурсов. Обычно ввиду особой важности данного вопроса наиболее регламентированно и детально задаются права доступа к информационным объектам и устройствам.

Неоднократно отмечено, что сотрудники являются как самым сильным, так одновременно и самым слабым звеном в обеспечении информационной безопасности. Необходимо донести до сотрудников мысль о том, что обеспечение информационной безопасности - обязанность всех без исключения сотрудников. Это достигается путем введения процедуры ознакомления с требованиями политики ИБ и подписания соответствующего документа о том, что сотрудник ознакомлен, ему понятны все требования политики и он обязуется их выполнять.

Политика позволяет ввести требования по поддержанию необходимого уровня безопасности в перечень обязанностей каждого сотрудника. В процессе выполнения ими трудовых обязанностей для сотрудников необходимо периодически проводить ознакомление и обучение вопросам обеспечения информационной безопасности. Критически важным условием для успеха в области обеспечения информационной безопасности компании становится создание в компании атмосферы, благоприятной для создания и поддержания высокого приоритета информационной безопасности. Чем крупнее компания, тем более важной становится информационная поддержка и мотивация сотрудников по вопросам безопасности

1.21. Анализ и управление рисками при реализации информационной безопасности

Одним из важнейших аспектов реализации политики ИБ считается анализ угроз, оценка их достоверности и тяжести вероятных последствий. Реально риск появляется там, где есть вероятность осуществления угрозы, при этом величина риска прямо пропорциональна величине этой вероятности (рис.1.28).

Суть деятельности по управлению рисками состоит в том, чтобы оценить их размер, выработать меры по уменьшению и создать механизм контроля того, что остаточные риски не выходят за приемлемые ограничения. Таким образом, управление рисками включает в себя два вида деятельности: оценка рисков и выбор эффективных и экономичных защитных и регулирующих механизмов. Процесс управления рисками можно подразделить на следующие этапы:

– идентификация активов и ценности ресурсов, нуждающихся в защите;
– выбор анализируемых объектов и степени детальности их рассмотрения;
– анализ угроз и их последствий, определение слабостей в защите;
– классификация рисков, выбор методологии оценки рисков и проведение оценки;
– выбор, реализация и проверка защитных мер;
– оценка остаточного риска.

Рис.1.28 Неопределенность как основа формирования риска

Политика ИБ включает разработку стратегии управления рисками разных классов.

Целесообразно выявлять не только сами угрозы, но и источники их возникновения - это поможет правильно оценить риск и выбрать соответствующие меры нейтрализации. Например, нелегальный вход в систему повышает риск подбора пароля или подключения к сети неавторизованного пользователя или оборудования.

Очевидно, что для противодействия каждому способу нелегального входа нужны свои механизмы безопасности. После идентификации угрозы необходимо оценить вероятность ее осуществления и размер потенциального ущерба.

Оценивая тяжесть ущерба, необходимо иметь в виду не только непосредственные расходы на замену оборудования или восстановление информации, но и более отдаленные, в частности подрыв репутации компании, ослабление её позиций на рынке и т. п.

После проведения идентификации и анализа угроз, их возможных последствий имеется несколько подходов к управлению: оценка риска, уменьшение риска, уклонение от риска, изменение характера риска, принятие риска, выработка корректирующих мероприятий (рис.1.29).

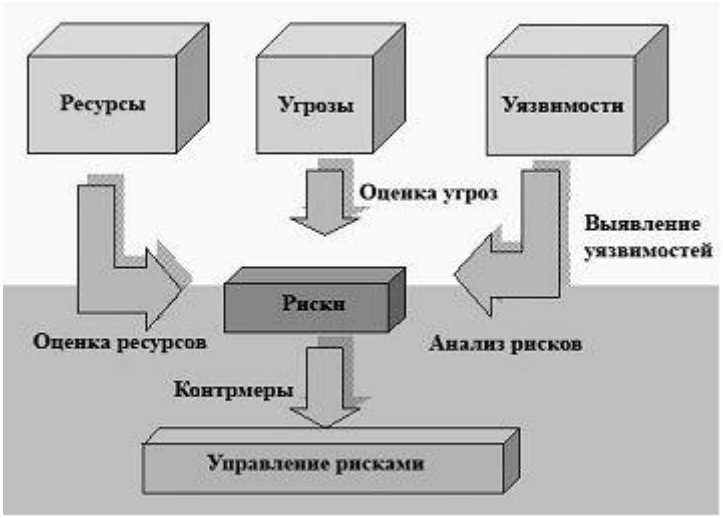

Рис.1.29 Схема управления рисками

При идентификации активов и информационных ресурсов - тех ценностей, которые нужно защитить, - следует учитывать не только компоненты информационной системы, но и поддерживающую инфраструктуру, персонал, а также нематериальные ценности, в том числе текущий рейтинг и репутацию компании. Тем не менее одним из главных

результатов процесса идентификации активов является получение детальной информационной структуры организации и способов ее использования.

Выбор анализируемых объектов и степень детальности их рассмотрения - следующий шаг в оценке рисков. Для небольшой организации допустимо рассматривать всю информационную инфраструктуру, для крупной - следует сосредоточиться на наиболее важных (критичных) сервисах. Если важных сервисов много, то выбираются те из них, риски для которых заведомо велики или неизвестны. Если информационной основой организации является локальная сеть, то в число аппаратных объектов следует включить компьютеры, периферийные устройства, внешние интерфейсы, кабельное хозяйство и активное сетевое оборудование.

К программным объектам следует отнести операционные системы (сетевая, серверные и клиентские), прикладное программное обеспечение, инструментальные средства, программы управления сетью и отдельными подсистемами. Важно зафиксировать, в каких узлах сети хранится программное обеспечение, где и как используется. Третьим видом информационных объектов являются данные, которые хранятся, обрабатываются и передаются по сети. Следует классифицировать данные по типам и степени конфиденциальности, выявить места их хранения и обработки, а также способы доступа к ним. Все это важно для оценки рисков и последствий нарушений информационной безопасности.

Оценка рисков производится на основе накопленных исходных данных и оценки степени определенности угроз. Вполне допустимо применить такой простой метод, как умножение вероятности осуществления угрозы на величину предполагаемого ущерба. 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. По этой шкале можно оценивать приемлемость рисков.

Если какие-либо риски оказались недопустимо высокими, необходимо реализовать дополнительные защитные меры. Для ликвидации или уменьшения слабости, сделавшей опасную угрозу реальной, можно применять несколько механизмов безопасности, отличающихся эффективностью и невысокой стоимостью. Например, если велика вероятность нелегального входа в систему, можно ввести длинные пароли, задействовать программу генерации паролей или закупить интегрированную систему аутентификации на основе интеллектуальных карт. Если имеется вероятность умышленного повреждения серверов различного назначения, что грозит серьезными последствиями, можно ограничить физический доступ персонала в серверные помещения и усилить их охрану.

Технология оценки рисков должна сочетать формальные метрики и формирование реальных количественных показателей для оценки. С их помощью необходимо ответить на два вопроса: приемлемы ли существующие риски, и если нет, то какие защитные средства экономически выгодно использовать.

Рис.1.30. Схема оценки и снижения рисков

Методология снижения рисков. Многие риски можно существенно уменьшить путем использования простых и недорогих контрмер. Например, грамотное (регламентированное) управление доступом снижает риск несанкционированного вторжения. От некоторых классов рисков можно уклониться - вынесение Web-сервера организации за пределы локальной сети позволяет избежать риска несанкционированного доступа в локальную сеть со стороны Web-клиентов. Некоторые риски не могут быть уменьшены до малой величины, однако после реализации стандартного набора контрмер их можно принять, постоянно контролируя остаточную величину риска (рис.1.30).

Оценка стоимости защитных мер должна учитывать не только прямые расходы на закупку оборудования и/или программного обеспечения, но и расходы на внедрение новинки, обучение и переподготовку персонала. Эту стоимость можно выразить в некоторой шкале и затем сопоставить ее с разностью между вычисленным и приемлемым риском. Если по этому показателю средство защиты оказывается экономически выгодным, его можно принять к дальнейшему рассмотрению.

Рис.1.31 Итерационный процесс управления рисками

Контроль остаточных рисков в обязательном порядке включается в текущий контроль системы ИБ. Когда намеченные меры приняты, необходимо проверить их действенность - убедиться, что остаточные риски стали приемлемыми. В случае систематического повышения остаточных рисков необходимо проанализировать допущенные ошибки и немедленно принять корректирующие меры.

Управление рисками является многоступенчатым итерационным процессом (рис.1.31).

Практически все его этапы связаны между собой, и по завершении почти любого из них может выявиться необходимость возврата к предыдущему. Так, при идентификации активов может возникнуть понимание, что выбранные границы анализа следует расширить, а степень детализации - увеличить. Особенно труден первичный анализ, когда многократные возвраты к началу неизбежны. Управление рисками - типичная оптимизационная задача, принципиальная трудность состоит в её грамотной постановке на уровне высшего менеджмента, сочетании оптимальных методик и описания исходных данных (рис.1.32).

Рис.1.32. Формирование деятельности по управлению ИТ-рисками

Методологии «Оценка рисков» (Risk Assessment) и «Управление рисками» (Risk Management) стали неотъемлемой составляющей деятельности в области обеспечения непрерывности бизнеса (Business Continuity) и информационной безопасности (Information Security). Программа реализации ИБ и наборы политик базируются на совокупности системных действий и практических шагов (рис.1.33-рис.1.36).

Рис.1.33 Совокупности системных действий и практических шагов (1)

Рис.1.34. Совокупности системных действий и практических шагов (2)

Рис.1.35. Совокупности системных действий и практических шагов (3)

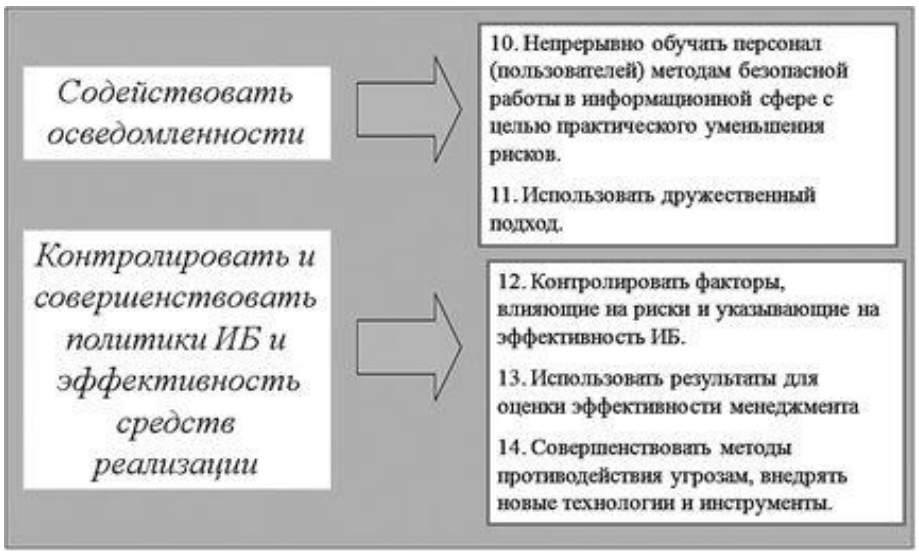

Рис.1.36. Совокупности системных действий и практических шагов (4)

Подготовлено и активно используются более десятка различных международных стандартов и спецификаций, детально регламентирующих процедуры управления информационными рисками: ISO 15408: 1999 («Common Criteria for Information Technology Security Evaluation»), ISO 17799:2002 («Code of Practice for Information Security Management»), NIST 80030, SAS 78/94, COBIT.

Методика и инструментальное средство RA Software Tool основаны на требованиях международных стандартов ISO 17999 и ISO 13335 (части 3 и 4), а также на требованиях руководств Британского национального института стандартов (BSI) - PD 3002 («Руководство по оценке и управлению рисками»), PD 3003 («Оценка готовности компании к аудиту в соответствии с BS 7799»), PD 3005 («Руководство по выбору системы защиты»).

На практике такие методики управления рисками позволяют:

– создавать модели информационных активов компании с точки зрения безопасности;

– классифицировать и оценивать ценности активов;

– составлять списки наиболее значимых угроз и уязвимостей безопасности;

– ранжировать угрозы и уязвимости безопасности;

– оценивать и отрабатывать риски;

– разрабатывать корректирующие меры;

– обосновывать средства и меры контроля рисков;

– оценивать эффективность/стоимость различных вариантов защиты;

– формализовать и автоматизировать процедуры оценивания и управления рисками.

Отработка рисков включает в себя ряд важных этапов, которые в обязательном порядке включаются в плановую работу по обеспечению информационной безопасности (рис.1.37).

Применение соответствующих программных средств позволяет уменьшить трудоемкость проведения анализа рисков и выбора контрмер. В настоящее время разработано более десятка программных продуктов для анализа и управления рисками базового уровня безопасности. Примером достаточно простого средства является программный пакет BSS (Baseline Security Survey, UK).

Программные продукты более высокого класса: CRAMM (компания InsightConsultingLimited, UK), RiskWatch, COBRA (ConsultativeObjectiveandBi-FunctionalRiskAnalysis), BuddySystem. Наиболее популярный из них - CRAMM (Complex Risk Analysis and Management Method), реализующий метод анализа и контроля рисков.

Существенным достоинством метода является возможность проведения детального исследования в сжатые сроки с полным документированием результатов.

Рисунок37. Этапы отработки риска

В основе методов, подобных CRAMM, лежит комплексный подход к оценке рисков, сочетающий количественные и качественные методы анализа. Метод является универсальным и подходит как для больших, так и для мелких организаций как правительственного, так и коммерческого сектора.

К сильным сторонам метода CRAMM относится следующее:

– CRAMM является хорошо структурированным и широко опробованным методом анализа рисков, позволяющим получать реальные практические результаты;

– программный инструментарий CRAMM может использоваться на всех стадиях проведения аудита безопасности ИС;

– в основе программного продукта лежит достаточно объемная база знаний по контрмерам в области информационной безопасности, базирующаяся на рекомендациях стандарта BS 7799;

– гибкость и универсальность метода CRAMM позволяет использовать его для аудита ИС любого уровня сложности и назначения;

– CRAMM можно использовать в качестве инструмента для разработки плана непрерывности бизнеса и политик информационной безопасности организации;

– CRAMM может использоваться в качестве средства документирования механизмов безопасности ИС.

Для коммерческих организаций имеется коммерческий профиль стандартов безопасности (Commercial Profile), для правительственных организаций - правительственный (Government Profile). Правительственный вариант профиля, также позволяет проводить аудит на соответствие требованиям американского стандарта TCSEC («Оранжевая книга»).

2 ПРАКТИЧЕСКАЯ ЧАСТЬ

Лабораторная работа № 1

Средства безопасности Windows. Обеспечение безопасности хранения данных в ОС Windows

Цель:

- познакомиться с особенностями шифрования информации в ОС;
- познакомиться с понятием сертификата ОС Windows;
- научиться шифровать и расшифровывать данные;
- научиться работать с сертификатами ОС;
- изучить технологию теневого копирования данных и возможность создания отказоустойчивых томов для хранения данных;
- Научиться архивировать данные с возможность разграничения доступа к архивам.

I. Шифрование файлов и папок

Поскольку шифрование и дешифрование выполняется автоматически, пользователь может работать с файлом так же, как и до установки его криптозащиты. Например, можно так же открыть текстовый процессор Word, загрузить документ и отредактировать его, как и прежде. Все остальные пользователи, которые попытаются получить доступ к зашифрованному файлу, получат сообщение об ошибке доступа, поскольку они не владеют необходимым личным ключом, позволяющим им расшифровать файл. Следует отметить, что пользователи (в данном случае администраторы) не должны шифровать файлы, находящиеся в системном каталоге, поскольку они необходимы для загрузки системы, в процессе которой ключи пользователя недоступны. Это сделает невозможным дешифрование загрузочных файлов, и система потеряет работоспособность. Проводник предотвращает возможность возникновения такой ситуации, не позволяя шифровать файлы с атрибутом *системный.*

Шифрование информации задается в окне свойств файла или папки:

1. Укажите файл или папку, которую требуется зашифровать, нажмите правую кнопку мыши и выберите в контекстном меню команду Свойства (Properties).

2. В появившемся окне свойств на вкладке Общие (General) нажмите кнопку Другие (Advanced). Появится окно диалога Дополнительные атрибуты (Advanced Attributes) (рисунок 1).

3. В группе Атрибуты сжатия и шифрования (Compress or Encrypt attributes) установите флажок Шифровать содержимое для зашиты данных (Encrypt contents to secure data) и нажмите кнопку ОК.

4. Нажмите кнопку ОК в окне свойств зашифровываемого файла или папки. В появившемся окне диалога укажите режим шифрования.

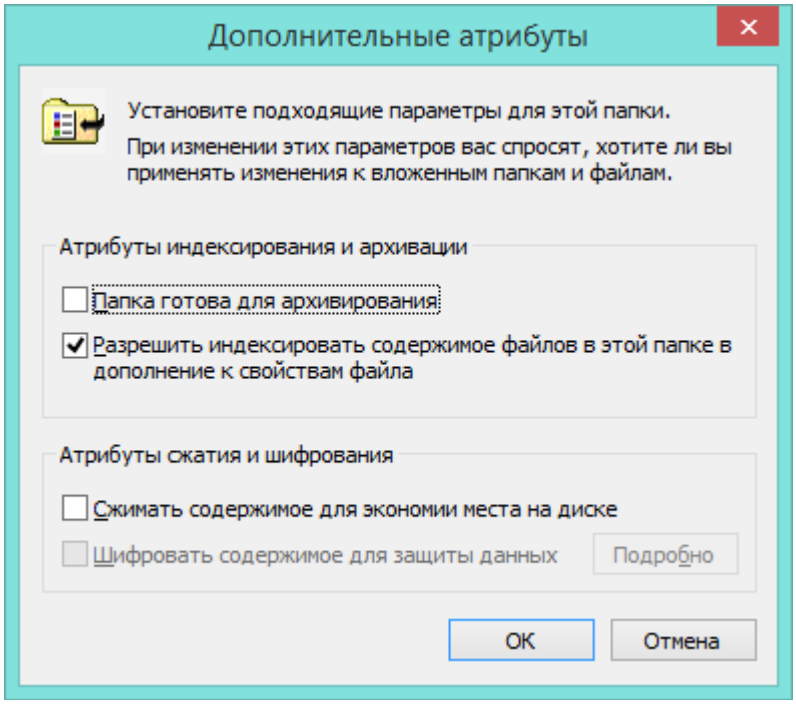

Рис.2.1. Окно диалога Дополнительные атрибуты Advanced Attributes

При шифровании папки можно указать следующие режимы применения нового атрибута:

- Только к этой папке (Apply changes to this folder):
- К этой папке и всем вложенным папкам и файлам (Apply changes to this folder, sub folders and files).

Дешифрование файлов и папок

Чтобы дешифровать файл или папку, на вкладке Общие окна свойств соответствующего объекта нажмите кнопку Другие.

В открывшемся окне диалога в группе Атрибуты сжатия и шифрования сбросьте флажок Шифровать содержимое для защиты данных.

Копирование, перемещение, переименование и уничтожение зашифрованных файлов и папок

Операции копирования, перемещения, переименования и уничтожения зашифрованных файлов и папок выполняются точно так же, как и с незашифрованными объектами. Однако следует помнить, что пункт назначения зашифрованной информации должен поддерживать шифрование. В противном случае при копировании данные будут расшифрованы, и копия будет содержать открытую информацию.

Архивация зашифрованных файлов

Резервную копию зашифрованного файла можно создать с помощью простого копирования его на другой жесткий диск или с использованием утилиты архивации. Однако, как сказано в предыдущем пункте, простое копирование, например, на дискету или оптический диск может привести к тому, что резервная копия будет содержать открытые данные. То есть, если скопировать зашифрованный файл на раздел FAT или на дискету, копия будет не зашифрована и, следовательно, доступна для чтения любому пользователю. Специализированная операция архивации не требует для ее выполнения доступа к открытым ключам пользователя - только к архивируемой информации. Поэтому для обеспечения безопасности конфиденциальных данных при создании резервных копий рекомендуется применять специальные утилиты архивации. В Windows для этих целей предназначена стандартная утилита архивации данных Backup.

Восстановление зашифрованных файлов на другом компьютере

Часто возникает необходимость восстановить зашифрованную информацию не на том компьютере, на котором она была заархивирована. Это можно выполнить с помощью утилиты архивации. Однако необходимо позаботиться о переносе на новый компьютер соответствующего сертификата и личного ключа пользователя с помощью перемещаемого профиля либо вручную.

На любом компьютере, где зарегистрировался пользователь, обладающий перемещаемым профилем, будут применяться одни и те же ключи шифрования. Ручной перенос личного ключа и сертификата выполняется в два этапа: сначала следует создать резервную копию сертификата и личного ключа, а затем восстановить созданную копию на другом компьютере.

Создание резервной копии сертификата состоит из следующих шагов:

Запустите оснастку Сертификаты.

В левом подокне оснастки Сертификаты откройте папку Личные (Personal), а затем папку Сертификаты. В правом подокне появится список ваших сертификатов. Укажите переносимый сертификат и щелкните правой кнопкой мыши. В появившемся контекстном меню выберите команду Все задачи (All Tasks). В ее подменю выберите команду Экспорт (Export). Запустится Мастер экспорта сертификатов (Certificate Export Wizard). Нажмите кнопку Далее.

В следующем окне мастера выберите опцию Да, экспортировать закрытый ключ (Yes, export the private key). Затем нажмите кнопку Далее.

В следующем окне мастера доступен только один формат (PFX), предназначенный для персонального обмена информацией. Нажмите кнопку Далее.

В следующих окнах сообщите пароль, защищающий данные файла *.pfx, а также путь сохранения файла *.pfx; затем нажмите кнопку Далее.

Отобразится список экспортируемых сертификатов и ключей. Нажмите кнопку Готово. Завершите работу мастера экспорта нажатием кнопки ОК в окне диалога, сообщающем об успешном выполнении процедуры экспорта. В результате сертификат и секретный ключ будут экспортированы в файл с расширением pfx, который может быть скопирован на гибкий диск и перенесен на другой компьютер. Для восстановления сертификата из резервной копии перенесите созданный на предыдущем этапе файл с расширением pfx на компьютер, где вы планируете восстанавливать зашифрованные данные.

Запустите оснастку Сертификаты. В окне структуры оснастки Сертификаты откройте папку Личные, затем папку Сертификаты. В правом подокне появится список ваших сертификатов.

Щелкните правой кнопкой мыши на пустом месте правого подокна. В появившемся контекстном меню выберите команду Все задачи. В ее подменю выберите команду Импорт (Import). Запустится Мастер импорта сертификатов (Certificate Import Wizard) Следуйте указаниям мастера - укажите местоположение файла с расширением pfx и сообщите пароль защиты данного файла. Восстановление данных из резервной копии должно быть выполнено в папку Личные.

Для начала операции импорта нажмите кнопки Готово и ОК. После завершения процедуры импорта нажмите кнопку ОК и закройте окно мастера импорта В результате текущий пользователь получит возможность работать с зашифрованными данными на этом компьютере.

Восстановление данных, зашифрованных с помощью неизвестного личного ключа

EFS располагает встроенными средствами восстановления зашифрованных данных в условиях, когда Неизвестен личный ключ пользователя. Технология EFS основана на шифровании с открытым ключом и использует все возможности архитектуры CryptoAPI в Windows. Каждый файл шифруется с помощью случайно сгенерированного ключа,

зависящего от пары открытого (public) и личного, закрытого (private) ключей пользователя. Подобный подход в значительной степени затрудняет осуществление большого набора атак, основанных на криптоанализе. При криптозащите файлов может быть применен любой алгоритм симметричного шифрования. Текущая версия EFS использует алгоритм DESX (расширенный DES) с длиной ключа 56 бит. EFS позволяет осуществлять шифрование и дешифрование файлов, находящихся на удаленных файловых серверах.

Windows позволяет создать необходимые ключи для восстановления зашифрованных данных в описанных ситуациях. Пользователи, которые могут восстанавливать зашифрованные данные в условиях утраты личного ключа, называются агентами восстановления данных. Агенты восстановления данных обладают сертификатом (X509 version 3) на восстановление файлов и личным ключом, с помощью которых выполняется операция восстановления зашифрованных файлов. Используя ключ восстановления, можно получить только сгенерированный случайным образом ключ, с помощью которого был зашифрован конкретный файл. Поэтому агенту восстановления не может случайно стать доступной другая конфиденциальная информация. Средство восстановления данных предназначено для применения в разнообразных конфигурациях вычислительных сред. Параметры процедуры восстановления зашифрованных данных в условиях утраты личного ключа задаются политикой восстановления. Она представляет собой одну из политик открытого ключа. При установке Windows политика восстановления автоматически создается на первом контроллере домена. Администратор домена одновременно является и агентом восстановления. Могут быть добавлены и другие агенты. Это делается с помощью оснастки Групповая политика (Group Policy), в которой нужно раскрыть узел Конфигурация компьютера | Конфигурация Windows | Параметры безопасности | Политики открытого ключа | Агенты восстановления шифрованных данных (Computer Settings | Security Settings I Public Key Policies | Encrypted Data Recovery Agents) и выполнить в контекстном меню команду Добавить (Add) или Создать (Create) (в первом случае выбирается пользователь с имеющимся сертификатом агента восстановления, во втором - запрашивается и устанавливается новый сертификат для текущей учетной записи). Политика восстановления существует и на одиночном компьютере. В этом случае агентом восстановления автоматически становится администратор компьютера.

Политика восстановления, применяемая по умолчанию, создается на каждом компьютере при инсталляции системы. Если компьютер подключается к сети, для него политика восстановления может быть определена также на уровне его домена или подразделения, причем она должна быть установлена до того, как начнет применяться шифрование, и имеет приоритет над политиками восстановления, задаваемыми локальными администраторами.

Существует три «типа» политик восстановления:

1. Политика агентов восстановления. Когда администратор добавляет одного или нескольких агентов восстановления, начинает действовать политика агентов восстановления. Это наиболее широко используемый тип политики.

2. Пустая политика восстановления (empty policy). Когда администратор уничтожает всех агентов восстановления и их сертификаты открытых ключей, начинает действовать пустая политика восстановления. Это значит, что не существует ни одного агента восстановления, и в пределах области действия данной политики пользователи не могут шифровать свои данные. Применение пустой политики восстановления эквивалентно отключению работы EFS.

3. Отсутствие политики восстановления (no policy). Когда администратор удаляет групповую политику восстановления, для восстановления зашифрованных данных в условиях утраты личного ключа используются локальные политики восстановления,

существующие на каждом компьютере, и процессом восстановления управляет локальный администратор компьютера.

Настройка параметров политики восстановления выполняется с помощью оснастки Групповая политика (узел Политики открытых ключей).

II. Работа с сертификатами в ОС Windows

Сертификат - это набор данных специального формата, содержащий сам открытый ключ и всю информацию о нем: кто владелец, адрес электронной почты владельца, когда ключ создан, назначение ключа (подпись или обмен), для какого алгоритма предназначен ключ и т.д.

Сертификат представляет собой набор данных, зашифрованных с помощью цифровой, или электронной, подписи. Информация сертификата подтверждает истинность открытого ключа и владельца соответствующего личного ключа.
В данном разделе описывается использование оснастки Сертификаты консоли MMC для управления сертификатами.

Сертификаты с открытым ключом (public key certificate) представляют собой средство идентификации пользователей в незащищенных сетях (таких как Интернет), а также предоставляют информацию, необходимую для проведения защищенных частных коммуникаций.

Под незащищенными сетями понимаются компьютерные сети, к которым пользователи могут получить доступ без разрешений. Коммуникации в таких сетях открыты для просмотра другими пользователями. Также существует определенная опасность возникновения ложных коммуникаций, когда отправителями сообщений являются ложные пользователи.

Даже частные локальные сети подвержены нападениям взломщиков с целью получения физического доступа к сети. Совершенно защищенные сети практически невозможны. Тем не менее в защищенных сетях большие бреши в системе безопасности возникают крайне редко. Поэтому, поскольку пользователи доверяют друг другу, в таких сетях можно обмениваться данными, не применяя средств безопасности.
В открытых сетях, таких как Интернет, информация может попасть в руки пользователей, намерения которых никому не известны. Информация, не представляющая особой ценности, не нуждается и в безопасности. Однако если информация является ценной или конфиденциальной, необходимо предпринять соответствующие меры безопасности для ее защиты.

Сертификаты можно использовать для решения различных задач безопасности. В их число входят:

Аутентификация (authentication) или проверка подлинности. Проверка того, что объект, с которым вы взаимодействуете, является в действительности авторизованным объектом.

Конфиденциальность (privacy) или секретность. Обеспечение доступа к информации только авторизованным пользователям, даже если любой пользователь сети может перехватить сообщение.

Шифрование (encryption). Обеспечивает доступ к информации только для того пользователя, кому она предназначена.

Цифровые подписи (digital signatures). Обеспечение целостности и подлинности данных.

Для запуска оснастки Сертификаты консоли MMC:

1. В меню Пуск выберите Выполнить В текстовое поле введите mmc и нажмите OK. Запустится окно Консоль консоли MMC.

2. В меню Консоль выберите команду Добавить или удалить оснастку…

3. Для добавления оснастки в текущую консоль нажмите кнопку Добавить...

4. Выберите Сертификаты из списка Оснастка, нажмите кнопку Добавить и затем Закрыть.

5. Для закрытия диалогового окна Добавить/удалить оснастку нажмите кнопку OK.

Каталог Сертификаты теперь добавлен в консоль MMC.

Примечание. Если Вы выполняете данные действия на контроллере домена, то после того, как Вы выберете Сертификаты, появится диалоговое окно, в котором с помощью переключателя необходимо будет указать, какими сертификатами будет управлять данная оснастка: для моей учетной записи , учетной записи службы или учетной записи компьютера. В данном случае выберите моей учетной записи, нажмите Готово и продолжите действия, описанные выше.

6. В меню Консоль выберите команду Сохранить как и введите название «Certificates» в качестве названия файла для этой консоли, после чего нажмите кнопку Сохранить. Для того чтобы впоследствии открыть консоль «Certificates», необходимо в меню Пуск выбрать Программы, перейти в Средства администрирования и выбрать «Certificates» (рис.2.2).

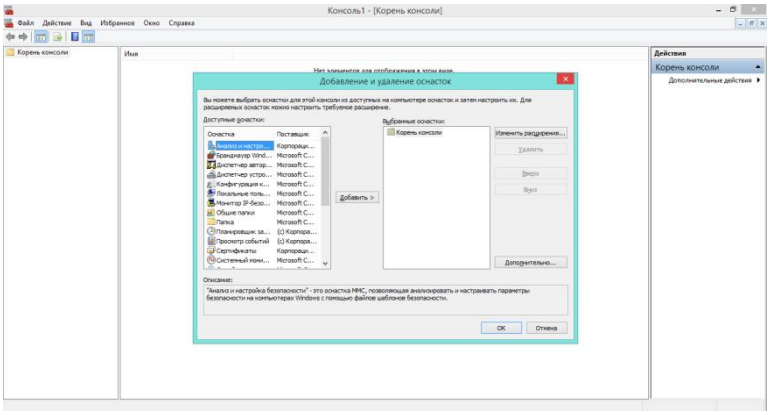

Рис.2.2. Консоль

Для получения сертификата:

В консоли «Certificates» щелкните правой кнопкой мыши по узлу Личные. В контекстном меню выберите пункт Все задачи, а затем Запросить новый сертификат. Запустится Мастер запроса сертификатов. Нажмите кнопку Далее. Выберите шаблон, который необходимо использовать в качестве основы для создания сертификата. В данном случае выберите Пользователь. Нажмите кнопку Далее. Если необходимо, введите понятное имя или описание в соответствующие поля. Нажмите кнопку Далее.

Нажмите кнопку Готово, чтобы отправить запрос сертификата в центр сертификации.

Нажмите кнопку Установить сертификат, чтобы установить сертификат в хранилище сертификатов. Вы также можете просмотреть содержимое сертификата перед его установкой, нажав кнопку Просмотреть сертификат.

Просмотр сертификата

Возможно, Вам понадобится просмотреть Ваши сертификаты в хранилище сертификатов:

Откройте консоль управления сертификатами. В левой области раскройте хранилище сертификатов, в котором содержатся те сертификаты, которые Вам необходимо просмотреть.

Откройте папку Сертификаты, чтобы просмотреть находящиеся в этом хранилище сертификаты.

Щелкните правой кнопкой мыши на сертификате, который Вам необходимо просмотреть, и выберите Открыть (Вы также можете просмотреть сертификат, дважды щелкнув по нему).

Откроется диалоговое окно сертификата, содержащее три вкладки.

- На вкладке Общие представлены общие сведения о сертификате.

- На вкладке Состав отображается содержимое полей сертификата, соответствующего стандарту X.509, а также его расширения и свойства. Вы можете нажать кнопку Свойства... для изменения полей Понятное имя и Описание. Вы также можете указать назначение сертификата.

- На вкладке Путь сертификации отображен путь сертификации, который указывает на источник, из которого был получен сертификат.

Полная информация о сертификате

Экспорт сертификатов

Щелкните правой кнопкой мыши по сертификату/сертификатам, которые Вам необходимо экспортировать.

Из контекстного меню выберите Все задачи и нажмите Экспорт... , чтобы запустить Мастер экспорта сертификатов. Нажмите кнопку Далее.

В случае, если для сертификата, который Вам необходимо экспортировать, в системе существует соответствующий закрытый ключ, Вы можете указать, что его нужно экспортировать вместе с сертификатом.

Примечание. Если Вам необходимо экспортировать закрытый ключ, то единственным возможным форматом сертификата для этой цели будет Файл обмена личной информацией PKCS#12.

Выберите формат экспортируемого файла из предложенных вариантов, как это показано на рис.2.3.

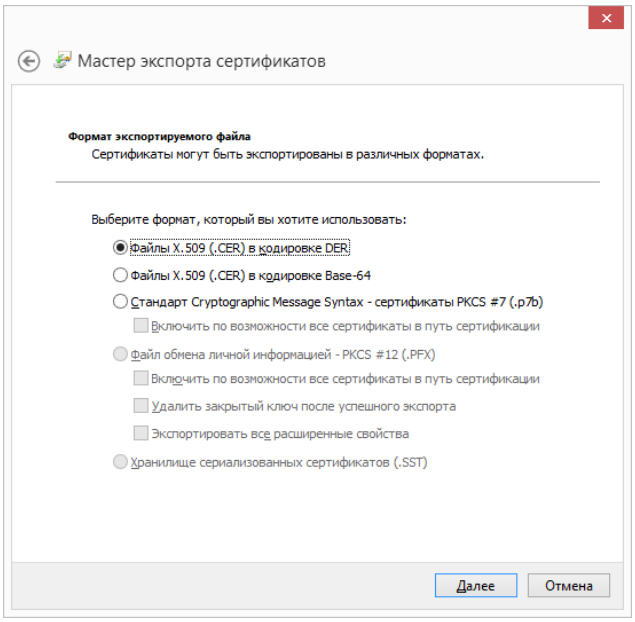

Рис.2.3 Выбор формата экспортируемого файла

Нажмите кнопку Далее. В случае, если Вы выбрали Файл обмена личной информацией - PKCS #12 (*.pfx) (Personal Information Exchange -- PKCS #12 (*.pfx)), будет выдан запрос на ввод пароля. Для экспорта файла введите пароль и нажмите кнопку Далее.

Введите название файла, который Вам необходимо экспортировать, и нажмите кнопку Далее.

Перед завершением работы мастера проверьте все выбранные Вами параметры и нажмите кнопку Готово, чтобы экспортировать файл.

Импорт сертификатов

Вы можете восстановить сертификаты и соответствующие им закрытые ключи из файла:

Щелкните правой кнопкой мыши по хранилищу сертификатов, в которое Вам необходимо импортировать сертификат, и выберите в контекстном меню Установить PFX (Install PFX).

Запустится Мастер импорта сертификатов. Нажмите кнопку Далее. В текстовом поле Имя файла введите название файла сертификата, который Вам необходимо импортировать. Вместо ввода названия Вы можете нажать Обзор (Browse) и выбрать необходимый файл.

Нажмите кнопку Далее. В случае, если импортируемый файл имеет формат Файл обмена личной информацией - PKCS #12 (*.pfx) (Personal Information Exchange-PKCS #12 (*.pfx)), необходимо будет ввести пароль. Введите пароль для импорта файла и нажмите Далее.

На следующем шаге работы мастера необходимо будет указать, куда именно Вам необходимо поместить сертификат. Нажмите Далее.

На последней странице мастера будет выведена сводная информация о файле, который Вам необходимо импортировать. Нажмите кнопку Готово, чтобы импортировать файл. Теперь сертификат/сертификаты готовы к использованию в системе.

Управление сертификатами компьютеров

Оснастку Сертификаты консоли MMC также можно использовать для управления сертификатами компьютеров:

Откройте консоль MMC. Для этого в меню Пуск выберите Выполнить, впишите в текстовом поле mmc.exe и затем нажмите кнопку OK.

В меню Консоль выберите Добавить или удалить оснастку...

Нажмите кнопку Добавить..., чтобы добавить оснастку в текущую консоль.

Выберите Сертификаты и затем нажмите кнопку Добавить.

Переключателем выберите учетной записи компьютера и нажмите кнопку Далее.

Переключателем выберите другим компьютером. Введите название компьютера, которым Вам необходимо управлять (или нажмите кнопку Обзор.., чтобы выбрать его из списка). Нажмите кнопку Готово.

Закройте диалоговое окно Добавить изолированную оснастку и нажмите кнопку OK, чтобы закрыть диалоговое окно Добавить/удалить оснастку. Таким образом, Вы создали консоль, с помощью которой Вы теперь можете управлять сертификатами Вашего компьютера.

В меню Консоль выберите команду Сохранить как... и в текстовом поле Имя файла введите название для этой консоли, затем нажмите Сохранить.

Задание

1. Создайте на диске C:\Темп папку и скопируйте в нее любой файл.

2. Зашифруйте файл вместе с папкой таким образом, чтобы все помещаемые в папку файлы тоже шифровались (если шифрование не удалось, дальнейшие действия с папкой делайте как с зашифрованной).

3. Создайте на рабочем столе папку с вашей фамилией и добавьте в неё резервную копию зашифрованной вами папки (сохраняя шифрование).

4. Установите оснастку Сертификаты.

5. Создайте резервную копию вашего сертификата и поместите ее в вашу папку на рабочем столе.

Из теории информационной безопасности известно, что обеспечение сохранности информации достигается различными решениями: начиная с тиражирования информационных ресурсов (программ и данных) и заканчивая резервированием устройств хранения данных. Поэтому на данной лабораторной рассмотрим интересные и полезные решения, предоставляемые ОС Microsoft Windows в этом диапазоне.

I. Технология теневого копирования данных

Суть данной технологии заключается в создании копий выбранных файлов через определенные промежутки времени. Реализована технология в виде отдельной службы

теневого копирования тома (VSS). Она используется для управления данными на дисках и может взаимодействовать с различными приложениями. Например, в программах резервного копирования, эта служба обеспечивает копирование файлов, занятых во время архивации другими приложениями.

Важной практической функцией технологии теневого копирования является возможность восстановления последних версий случайно удаленных или поврежденных файлов. В ОС Microsoft Windows предоставляется возможность пользователям клиентских компьютеров восстанавливать файлы из теневой копии самостоятельно без вмешательства системных администраторов, что, безусловно, очень удобно с точки зрения экономии времени.

Ограничения теневого копирования томов

Теневые копии файлов на заданных томах доступны только на серверах под управлением ОС Windows. На сервере в каталоге %System-root%\System32\Clients\Twclient\x86\ имеется клиентское ПО для инсталляции на компьютеры под управлением Windows, установив которое пользователи смогут получать доступ к теневым копиям через вкладку «Предыдущие версии» окна свойств файлов теневого том.

Теневое копирование тома не будет работать для точек подключения, когда второй жесткий диск подключается к первому в виде папки. Создавать теневые копии можно только на томах с файловой системой NTFS. Теневое копирование будет выполняться для всех общих папок, хранящихся на этом томе. Возможности выбрать отдельные общие папки на томе, для которых бы создавались теневые копии, нет! Для хранения теневых копий требуется не менее 100 Мб свободного места на выбранном томе. Максимально допустимый значение - 64 теневые копии на один том, независимо от того, сколько свободного места остается в области хранения.

Установка и использование технологии теневого копирования томов

На сервере под управлением ОС Windows желательно разместить общие папки, для которых хотите использовать теневые копии, на отдельном томе. Это убережет от заполнения теневыми копиями дискового пространства и снижения пропускной способности средств ввода-вывода в результате копирования тех общих папок, для которых функция теневого копирования не нужна.

Для активизации создания теневых копий на томе, в окне его свойств перейдите на вкладку «Теневые копии» (рис.2.4). На этой вкладке следует выбрать том, для общих папок которого будут создаваться теневые копии. При большой загрузке файлового сервера целесообразно хранить теневые копии на отдельном томе, который бы размещался на другом жестком диске. Это повысит производительность сервера.

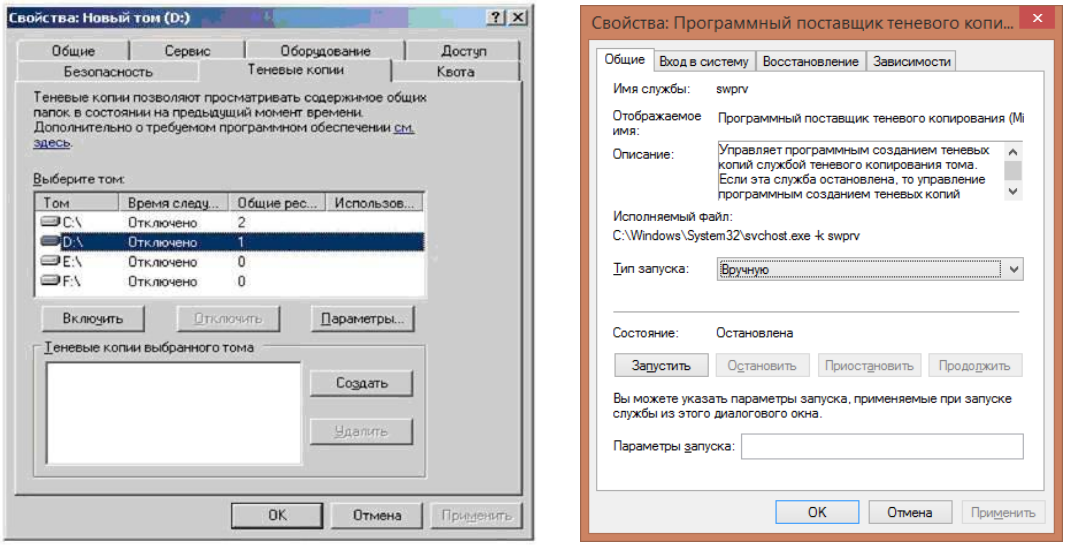

Рис.2.4.Теневое копирование

По умолчанию теневые копии сохраняются на том же диске, где хранятся общие папки. При этом устанавливаются следующие настройки:

- Максимальный размер места для хранения теневых копий равен 10 % от общего пространства диска;
- Автоматически проводить копирование с понедельника по пятницу в 7 утра и в 12 ночи;
- Создается первая теневая копия.

Для изменения настроек теневых копий тома отличных от заданных по умолчанию, выберите нужный том из списка и нажмите кнопку «Параметры» (рис.2.5)

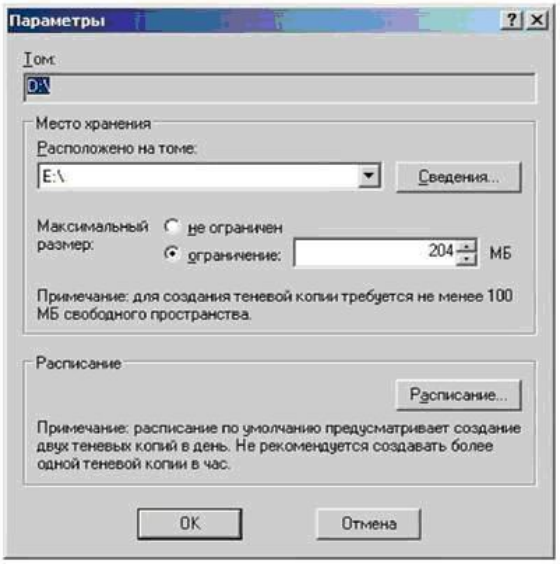

Рис.2.5. Параметры

Если вы решили изменить расписание создания теневых копий, нажмите кнопку «Расписание», появится окно, представленное на рис.2.6, для его настройки.

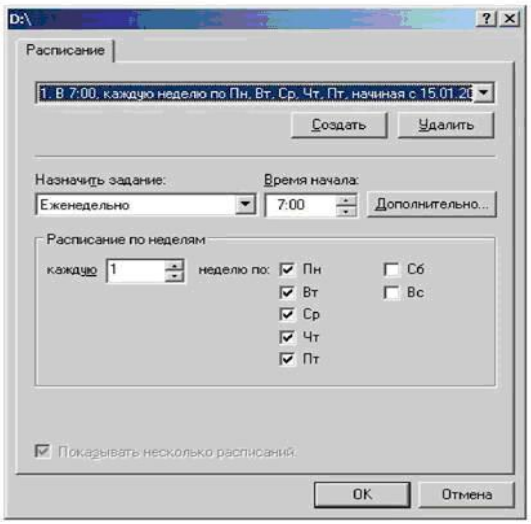

Рис.2.6. Расписание

После выполненных настроек нажмите кнопку «Включить», и начнут создаваться теневые копии общих папок на заданном томе. Теперь, если обратиться через контекстное меню к свойствам файлов, хранящимся в общих папках, появится специальная вкладка

«Предыдущие версии» (рис.2.7). Эта вкладка будет доступна в окне свойств файла, только если вы обратились к общей папке как к сетевому ресурсу (например, UNC-путь).

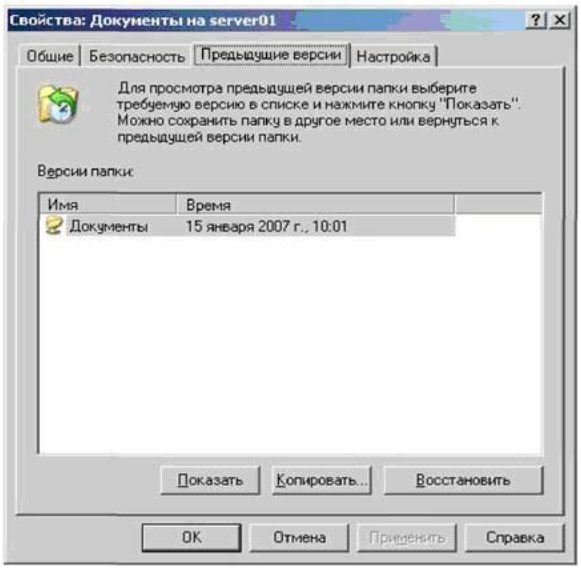

Рис.2.7. Предыдущие версии

Внизу вкладки имеются три кнопки, позволяющие совершать различные действия с копиями файла:

- «Показать» - позволяет просмотреть выбранную копию файла;
- «Копировать» - позволяет копировать выбранную копию файла в новое расположение;
- «Восстановить» - Позволяет восстанавливать выбранную копию файла поверх текущей версии файла.

Далее рассмотрим случай, когда файл был удален и требуется его восстановление из теневой копии. Так как объект файл, на котором можно щелкнуть правой кнопкой мыши, в общей папке в этом случае отсутствует, необходимо обратиться к свойствам папки, где имеется такая же вкладка «Предыдущие версии». Нажав кнопку «Показать», можно просмотреть, какие файлы и папки содержались в ней на выбранный момент времени. Отсюда можно восстановить удаленный файл в любое место, в том числе и в прежнюю папку.

Архивация данных

Под архивацией принято понимать обычное копирование данных на резервный носитель информации, чтобы в случае отказа или повреждения основного устройства хранения можно было быстро восстановить хранившиеся на нем данные. Архивация обеспечивает наивысшую степень отказоустойчивости по сравнению со всеми другими технологиями хранения данных, обеспечивающих отказоустойчивость, такими как теневое копирование, избыточные массивы независимых дисков, кластерные серверы и т.д.

Эффективность применения архивации в сетевой инфраструктуре зависит от правильного выбора специального ПО и планирования. В состав ОС Microsoft Windows входит служебная программа Backup, обеспечивающая основные функции архивации, включая возможности работы по расписанию и взаимодействие со службой теневого копирования тома.

Работа с программой архивирования

Выполнять архивацию всех данных на компьютере почти никогда не требуется, так как при выходе из строя жесткого диска можно достаточно быстро выполнить установку ОС и основного прикладного ПО. Поэтому следует архивировать только создаваемые

пользователями файлы (документы, базы данных и т.п.) и файлы конфигурации приложений. Разумный выбор объектов для резервного копирования сэкономит общее время и ресурсы архивации.

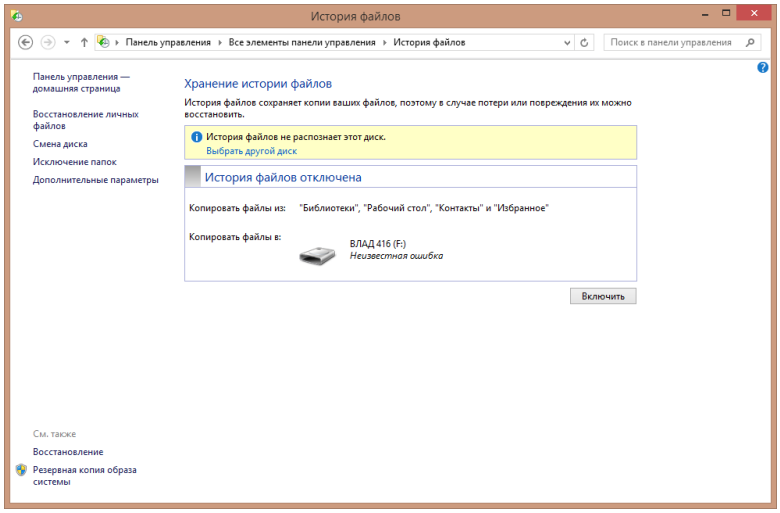

Рис.2.8. Backup

При первом запуске программа архивирования Buckup (Панель управления\Все элементы панели управления\История файлов) запускается в режиме мастера (рис.2.8). На этом занятии работа программы Buckup Windows в режиме мастера изучаться не будет. Нажать ссылку «Расширенный режим», а затем перейти на вкладку «Архивация» (рис.2.9)

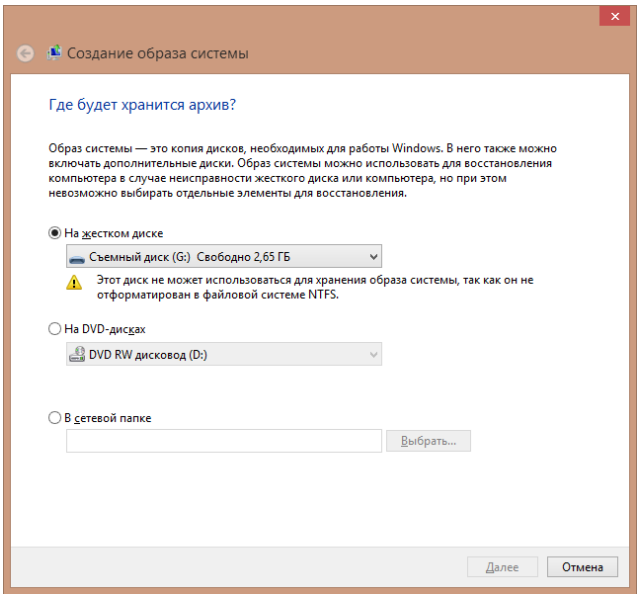

Рис.2.9. Образ системы

На этой вкладке необходимо выбирать файлы и папки, которые должны быть заархивированы. Выбирая определенную папку (диск), Buckup автоматически помечает к архивации все файлы или папки внутри нее. При этом флажок отметки будет синего цвета. Если нужно исключить какие-то файлы или папки из уже отмеченных, щелкните на связанный с ними флажок и снимите пометки о включении. При этом у родительской папки флажок отметки изменит цвет с синего на серый, что означает не стопроцентный выбор содержимого внутри папки. Используя папку «Сетевое окружение», можно включить в процесс архивации данные с других компьютеров сети. Слева в нижней части окна нужно задать имя файла-архива и выбрать место его

сохранения. Файлы-архивы, создаваемые программой Backup, могут быть размещены на любых носителях информации, таких как жесткие диски, записываемые компакт-диски в форматах CD и DVD, накопители на сменных картриджах (Zip, Jaz) и на магнитной ленте. При этом размер файла-архива будет ограничиваться емкостью используемого носителя. Поэтому целесообразно в сетевой инфраструктуре выделить специальный сервер с большим объемом дискового пространства для хранения архивов. После того как заданы носитель и имя архива, выбрать все необходимые файлы и папки

Стратегии архивации

Программа Backup Windows поддерживает пять стандартных типов архивации, которые в действительности представляют собой комбинации фильтров. Для осуществления первых трех типов архивации (табл.2.1)используются атрибуты файлов. Факт изменения файла определяется по установке атрибута «архивный» (бит архива). Во время архивации этот атрибут сбрасывается.

Таблица 2.1

Тип архива	Архивируемые данные	Состояние бита архива
Нормальный	Все выбранные данные, независимо от того, архивировались они ранее	Сбрасывается
Добавочный	Только файлы, модифицированные с момента последней нормальной или добавочной архивации	Сбрасывается
Разностный	Только файлы, модифицированные с момента последней нормальной архивации	Не сбрасывается
Копирующий	Все выбранные файлы	Не используется
Ежедневный	Только файлы, созданные или модифицированные за текущие сутки	Не используется

Представленные типы архивации могут использоваться в различных комбинациях друг с другом, определяющих стратегии архивации (табл.2.2). При выборе стратегии архивации обычно учитывают два критерия - это время, необходимое для архивации и восстановления данных. Во многих организациях стратегии архивации рассчитаны на недельный цикл.

Таблица 2.2 Стратегии архивации

Стратегия архивации	**Необходимое время для архивации**	**Необходимое время для восстановле-ния**	**Описание**
Полная архивация	Максимальное	Минимальное	На практике отдельно полная архивация в еженедельном цикле не используется. Однако при незначительном изменении архивируемых данных на сервере (рабочей станции), она может выполняться один раз в неделю
Полная архивация с последующей добавочной	Максимальное	Минимальное	В понедельник выполняется обычная архивация, со вторника по пятницу – добавочная. Так как каждая из этих архиваций сбрасывает бит архива, то

			ежедневно архивируются только измененные файлы. Если произойдет сбой данных в пятницу, то необходимо будет восстановить обычный архив от понедельника и последовательно каждый добавочный архив со вторника по четверг
Полная архивация с последующей разностной	Промежуточное между стратегиями 1 и 2	Промежуточное между стратегиями 1 и 2	В понедельник выполняется обычная архивация, со вторника по пятницу – разностная. Так как разностная архивация не сбрасывает бит архива, то каждый день ежедневно архивируются все изменения, произошедшие с понедельника. Если произойдет сбой данных в пятницу, то необходимо будет восстановить обычный архив

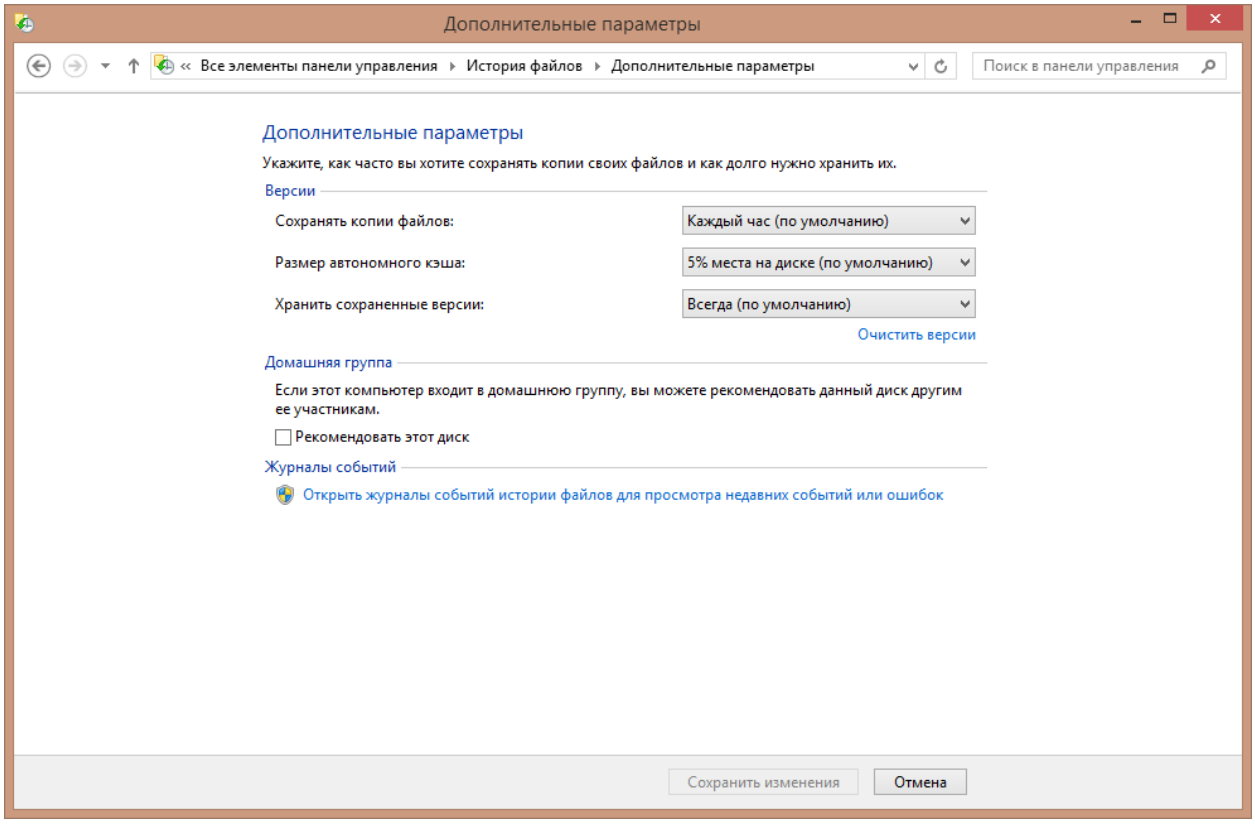

Рис.2.10. Дополнительные параметры

Настроить определенную стратегию архивации можно в дополнительных параметрах архивации (рис.2.10) и в параметрах запланированного задания, которые вызываются нажатием кнопок «Дополнительно» и «Расписание» в окне «Сведения о задании архивации» (рис.2.11).

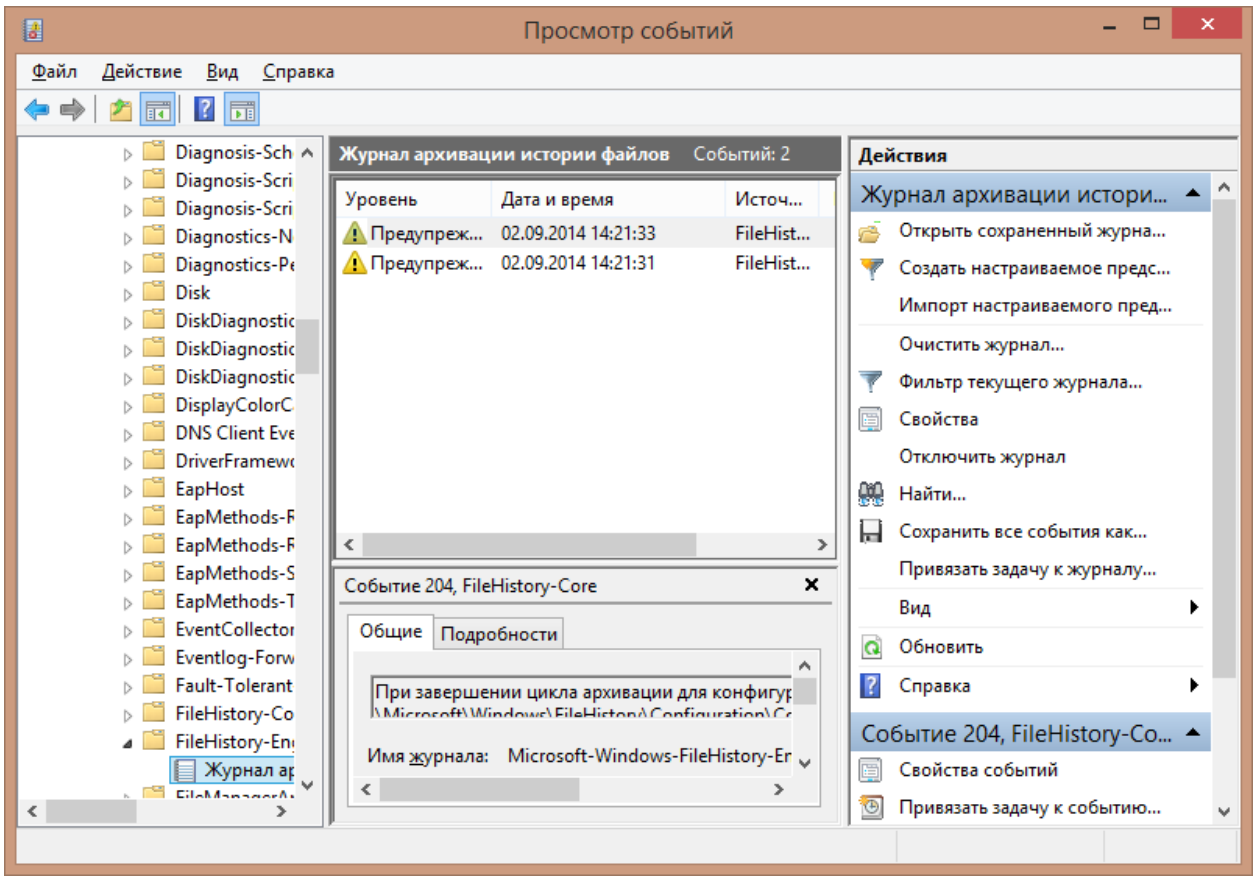

Рис.2.11. Журнал архивации

Восстановление данных

Главная и единственная причина создания резервных копий - это возможность восстановления данных. Успешное восстановление данных возможно, если придерживаться некоторых правил, главные из которых: полное документирование всех мероприятий по архивации, периодическое проведение тестовых восстановлений данных с архивных носителей. В ОС Microsoft Windows восстанавливать папки и файлы из архива могут пользователи, входящие в группу администраторов или операторов архива. Программа Backup Windows позволяет проводить процедуру восстановления данных двумя способами: вручную и с использованием мастера. На данном занятии рассмотрим только первый способ. Настроить параметры и запустить процесс восстановления можно, перейдя на вкладку «Восстановление и управление носителем» в главном окне программы Backup (рис.2.12).

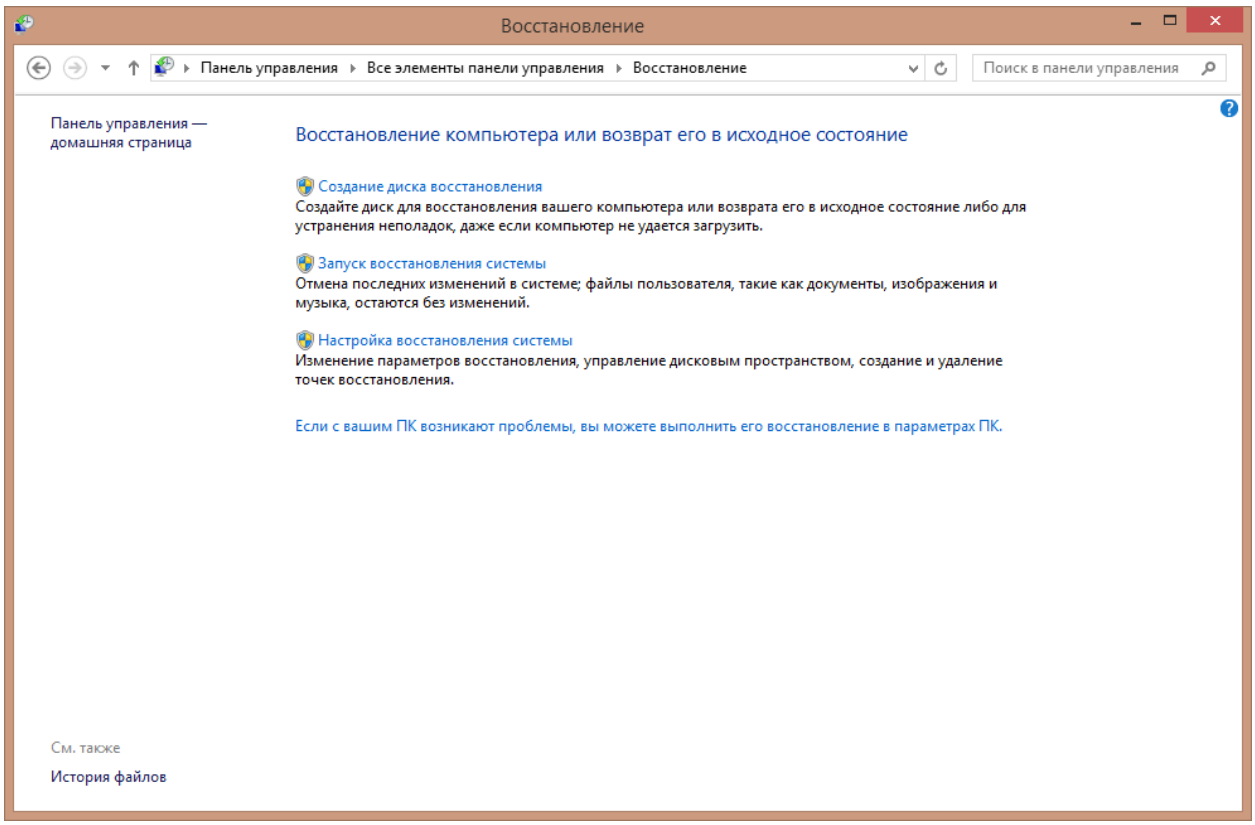

Рис.2.12. Восстановление

На этой вкладке необходимо выбрать носитель, с которого будут восстанавливаться данные. В нижней части окна можно выбрать один из следующих параметров восстановления:

- Исходное размещение - восстановление файлов и папок из архива в то же месторасположение, где они находились до архивации.

- Альтернативное размещение - восстановление файлов и папок из архива в заданную папку. Этот вариант восстановления позволяет со хранить структуру папок архивных данных.

- Одну папку - восстановление файлов и папок из архива в заданную папку без сохранения исходной структуры папок и подпапок. При этом в заданной папке будут восстановлены только файлы.

При выборе вариантов «Альтернативное размещение» или «Одну папку» необходимо задать папку, в которую будет осуществляться восстановление данных из архива. Выбрав все необходимые файлы и папки, можно запустить процесс восстановления, нажать кнопку «Восстановить». Появится диалоговое окно (рис.2.13), где можно либо подтвердить восстановление, нажав кнопку «ОК», либо задать еще дополнительные параметры восстановления, нажав кнопку «Дополнительно».

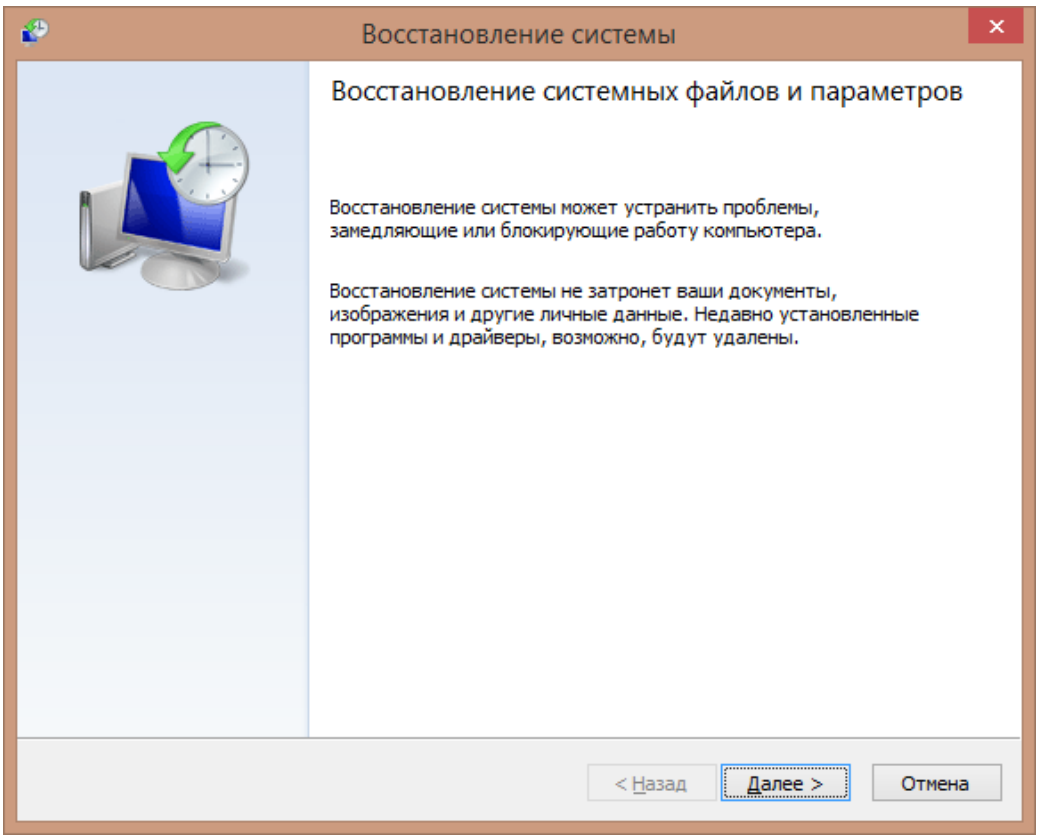

Рис.2.13. Настройка восстановления системы

Процесс восстановления будет отображаться в специальном окне. После его завершения выводится сводная информация об архиве в окне «Ход восстановления» (рис.2.14).

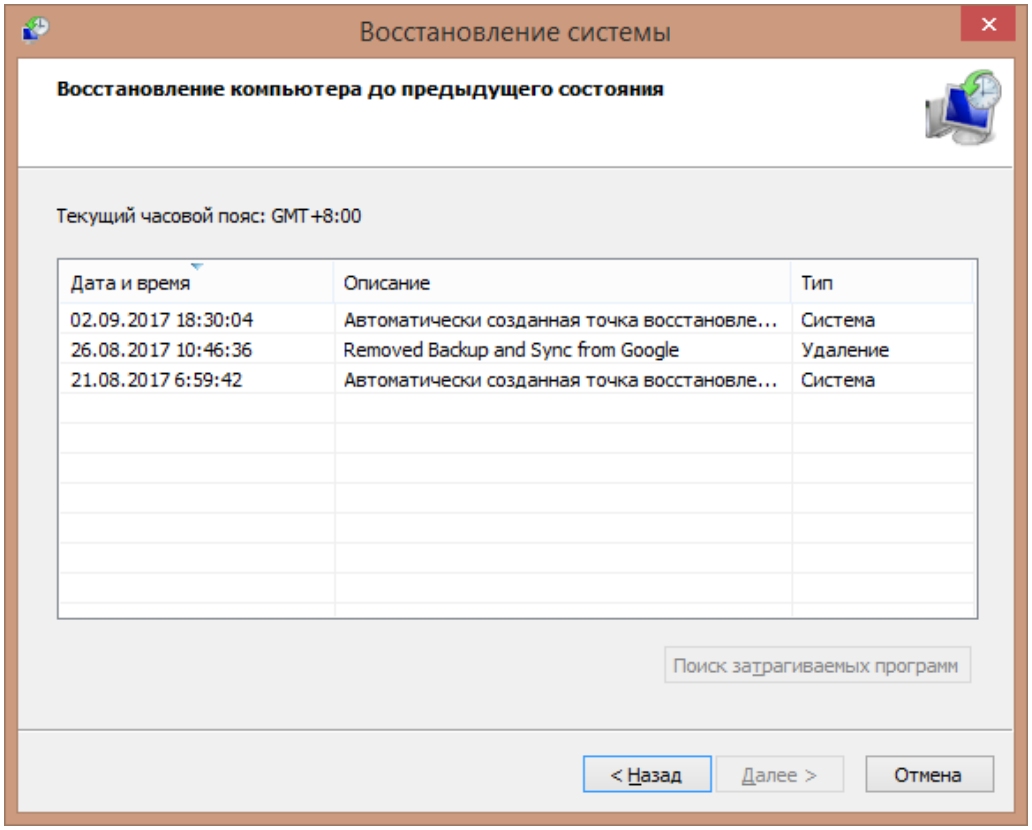

Рис.2.14. Выбор точки восстановления

Если нажать кнопку «Отчет», то можно посмотреть информацию об ошибках и сбоях, произошедших во время процесса восстановления.

Создание отказоустойчивых томов для хранения данных

В ОС Windows возможно создание отказоустойчивых томов RAID-1 (зеркальный том) и RAID-5, которые поддерживаются только на динамических дисках. По умолчанию ОС Microsoft Windows используют традиционное базовое хранение. Для эффективности управления хранением данных базовые диски преобразуют в динамические, на которых можно создавать различные типы томов.

Работа с зеркальными томами

Зеркальный том (RAID 1) состоит из двух одинаковых копий тома, расположенных на разных физических дисках. Данные, записываемые на такой том, записываются одновременно на два диска, поэтому зеркальный том обеспечивает отказоустойчивость. Для более высокой отказоустойчивости рекомендуется использовать диски, подключенные к разным контроллерам, что обеспечит наилучшую производительность и позволит справиться с отказами как контроллера, так и диска.
В ОС Windows для работы с дисками существует специальная оснастка «Управление дисками», которая входит в консоль «Управление компьютером». Для создания зеркального тома необходимо сначала с помощью оснастки «Управление дисками» преобразовать тип хранения с базового в динамическое на двух подключенных физических дисках. После этого щелкните на неразмеченную область в графическом представлении диска и в появившемся контекстном меню выберите команду «Действие» / «Все задачи» / «Создать том». Запустится мастер создания томов, который предложит сначала выбрать тип тома (рис.2.15).

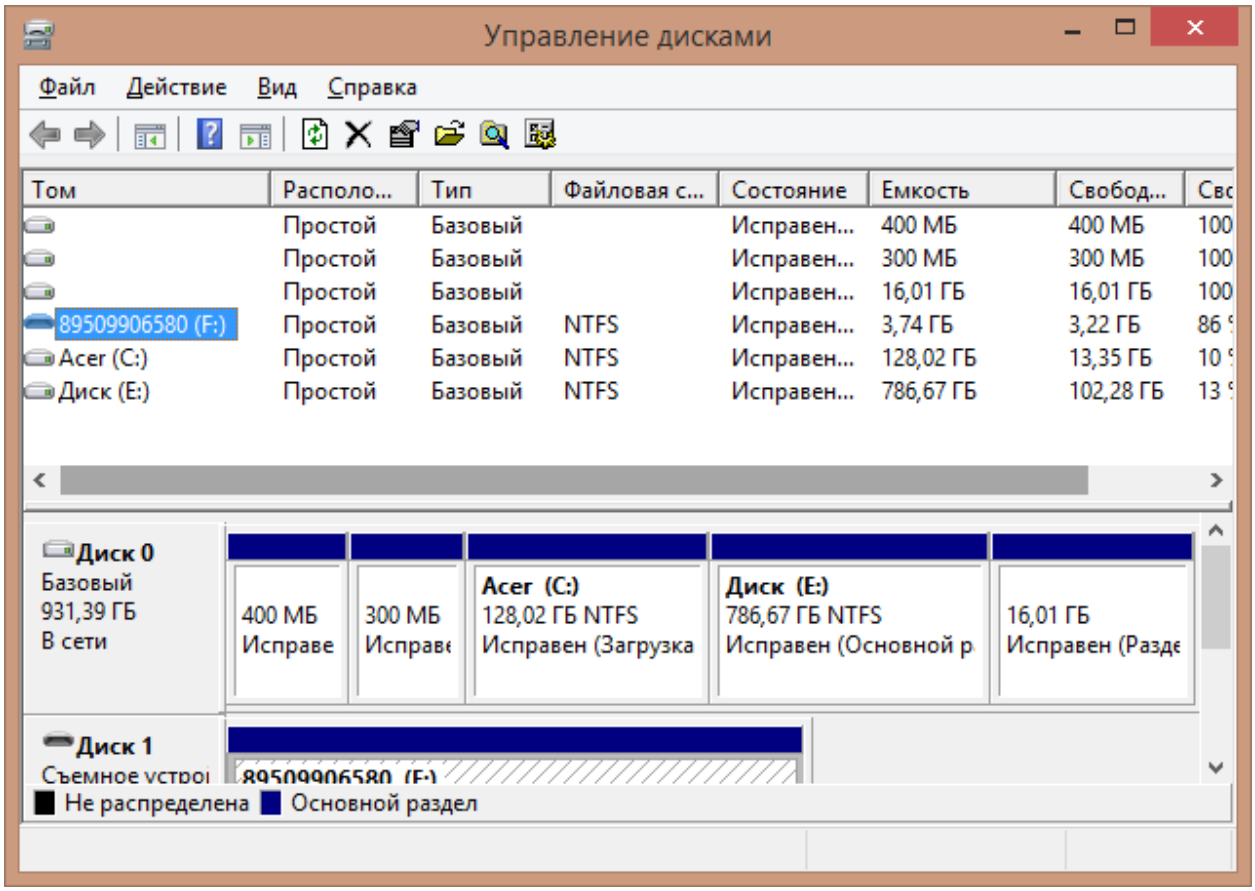

Рис.2.15. Управление дисками

Доступные типы томов зависят от числа установленных дисков на компьютере, содержащих неразмеченные области. Для создания зеркального тома, как было сказано выше, необходимо два динамических диска, имеющих нераспределенное место. Выбрав нужный тип тома, мастер создания томов откроет страницу, показанную на рис.2.16, на которой следует выбрать диски для создания тома.

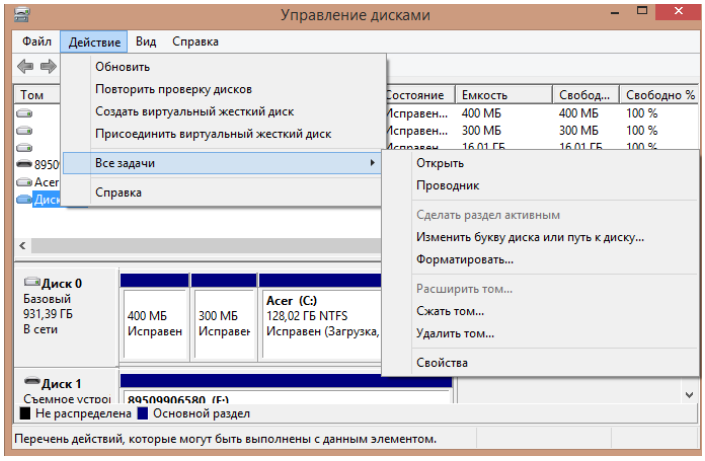

Рис.2.16. Управление дисками

Выбрав диски для создания тома, следует определить еще его размер. Для этого на каждом из дисков необходимо отвести области одинаковых размеров. После выбора дисков для тома укажите в поле «Выберете размер выделяемого пространства (Мб)» максимальный размер области, доступной на каждом из выбранных дисков (он ограничен размером области на диске с минимальным размером свободного места). При изменении размера отведенного места на одном из дисков мастер соответствующим образом изменит размер места, отведенного для нового тома на другом диске. Общий размер зеркального тома равен выделенной области (в Мб), так как диски данного типа тома содержат одинаковые копии данных. После завершения работы «Мастера создания томов» будет создан зеркальный том. Для начала эксплуатации зеркального тома нужно дождаться окончания процессов его форматирования и ресинхронизации (рис.2.18).

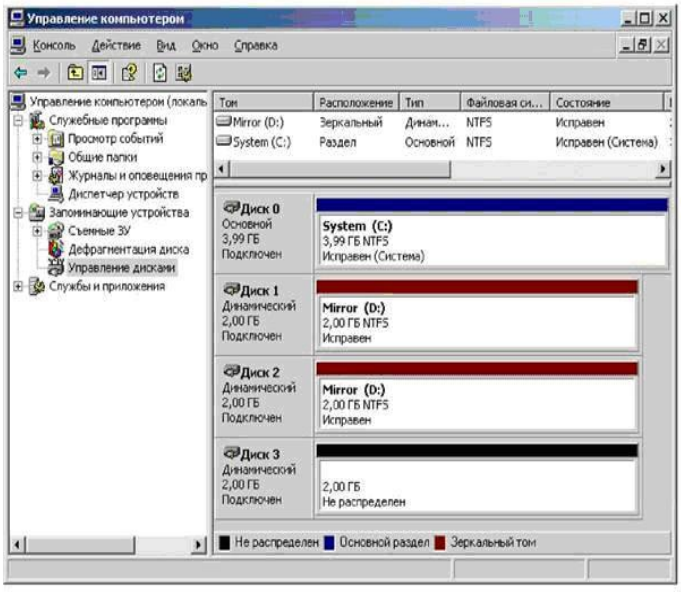

Рис.2.17. Зеркальный том

Процесс восстановления неисправного диска зеркального тома зависит от типа неисправности. Если на диске возникли одиночные ошибки ввода-вывода, оба диска тома перейдут в состояние «Отказавшая избыточность», диск с ошибками находится в состоянии «Автономный» или «Отсутствует» (рисунок 18).

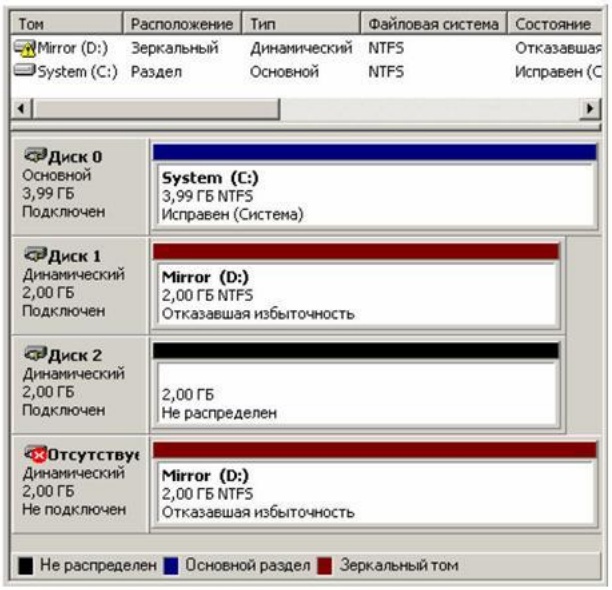

Рис.2.18. Зеркальный том в состоянии Отказавшая избыточность

Устранив источник ошибок ввода-вывода, например плохое соединение кабеля, необходимо выбрать том сбойного диска или сам диск и в контекстном меню указать пункт «Реактивизировать том» или «Реактивизировать диск» соответственно. Повторная активизация переводит диск или том в оперативный режим. Повторная синхронизация зеркального тома выполняется автоматически. Удалить зеркальный том можно тремя способами:

- Удалить том полностью со всеми данными.
- Удалить один из дисков зеркального тома. При этом на одном из дисков остается неразмеченная область, а содержимое зеркального тома сохраняется на другом диске.
- Разделить зеркальный том. При этом остаются два диска с идентичными копиями данных.

В случае выхода из строя одного физического диска зеркального тома можно его заменить, а потом пересоздать зеркальный том. Для этого следует сначала разделить зеркальный том, затем удалить неисправный диск. Второй исправный диск станет простым томом. После замены неисправного диска на сервере щелкните правой кнопкой мыши на оставшемся простом томе от прежнего «зеркала» и при помощи команды «Добавить зеркальный том» создайте новый зеркальный том на основе добавленного диска.

Работа с томами RAID-5

Том RAID-5 состоит как минимум из трех дисков (максимум из 32). По сравнению с зеркальными томами он обеспечивает лучшую производительность операции чтения данных и эффективность использования дискового пространства. В минимальном томе RAID-5 из трех дисков только одна треть дискового пространства используется для обеспечения отказоустойчивости (для хранения данных четности) в отличие от зеркального тома, где этот показатель равен одной второй. Отказоустойчивость зеркальных томов и RAID-5 защищает только от одиночных сбоев одного диска! Создается том RAID-5 аналогично зеркальному через оснастку «Управление дисками», за исключением того, что изначально требуется минимум три свободных диска. При отказе одного из дисков в томе RAID-5 данные все равно будут доступны. Общая

производительность тома снизится, так как при чтении отсутствующие данные будут вычисляться из оставшихся данных и информации о четности. После восстановления или замены отказавшего диска, возможно, придется воспользоваться командой «Повторить сканирование» оснастки «Управление дисками» и реактивировать том на восстановленном диске. При этом система восстановит отсутствующие данные по значениям четности и заново заполнит диск, в результате том восстановит функциональность и отказоустойчивость.

Задания

Задание 1. Выполнение архивации

В этом задании с помощью программы Backup вы выполните полную, а затем добавочную архивацию. Вы также научитесь создавать задания для программы архивации, которые будут выполняться по расписанию.

1. В папке C:\Темп:\Документы создайте три текстовых документа с произвольным содержимым, например Отчет.txt, Планы.txt и Заказы.txt.

2. В проводнике Windows выберите режим просмотра содержимого папки D:\ Документы в виде таблицы (Меню «Вид» / «Таблица»). Обратите внимание, что в столбце «Атрибуты» у всех трех файлов установлен атрибут «архивный» (бит архива обозначается буквой «А»).

3. Выберите «Пуск» / «Программы» / «Стандартные» / «Служебные» / «Архивация данных». Программа Backup Windows первый раз запускается в режиме мастера. На первой странице мастера снимите флажок «Всегда запускать в режиме мастера» и нажмите на ссылку «Расширенный режим». Запустится программа архивации. Перейдите на вкладку «Архивация».

4. В меню «Задание» выберите команду «Создать». Раскройте узел «Мой компьютер», диск C:\, папка «Документы». Установите флажок напротив папки «Документы». Внизу, в поле «Носитель архива или имя файла», введите имя будущего архива, например C : \doc-normal. bkf.

5. Нажмите кнопку «Архивировать». Откроется окно «Сведения о задании архивации». В разделе «Если носитель уже содержит архивы» оставьте переключатель «Дозаписать этот архив к данным носителя».

6. Нажмите кнопку «Дополнительно». Убедитесь, что выбран тип архива «Обычный», и установите флажок «Проверка данных после архивации». Нажмите кнопку «ОК», а затем «Архивировать».

7. Откроется диалоговое окно «Ход архивации», и начнется процесс архивации. По завершении создания архива нажмите кнопку «Отчет» и посмотрите отчет. В нем не должно быть ошибок архивации. Закройте отчет и окно «Ход архивации». Не закрывайте программу Backup Windows.

8. Обратите внимание, что в папке C:\Документы теперь у всех файлов снят атрибут «архивный». Откройте файл Планы. txt и добавьте новую строку с текущей датой. Сохраните и закройте файл. Обратите внимание, что после внесения изменений в файл атрибут «архивный» автоматически устанавливается операционной системой.

9. Вернитесь к программе Backup Windows на вкладку «Архивация». В меню «Задание» выберите команду «Создать».

10. Раскройте узел «Мой компьютер», диск C:\, папка «Документы». Установите флажок напротив папки «Документы».

11. Внизу, в поле «Носитель архива или имя файла», введите имя добавочного архива,например C: \doc-inc.bkf.

12. Нажмите кнопку «Архивировать». Откроется окно «Сведения о задании архивации».

13. Нажмите кнопку «Дополнительно». Выберите тип архива «добавочный» и установите флажок «Проверка данных после архивации». Нажмите кнопку «ОК».

14. Теперь кнопку «Расписание». Появится диалоговое окно, которое предложит вам сохранить заданные параметры перед установкой архивации по расписанию. Нажмите кнопку «Да».

15. Сохраните набор ваших файлов под именем documents. bks.

16. В окне «Указание учетной записи» введите свой пароль и нажмите кнопку «ОК».

17. В появившемся окне «Параметры запланированного задания» введите имя задания - «Ежедневный добавочный архив».

18. Затем нажмите кнопку «Свойства».

19. Откроется окно «Запланированное задание», вкладка «Расписание». В выпадающем списке «Назначить задание» выберите вариант «ежедневно» и установите время начала на три минуты вперед от текущего времени, чтобы увидеть результат выполнения задания. Нажмите кнопку «ОК».

20. Введите повторно свой пароль и нажмите кнопку «ОК».

21. В окне «Параметры запланированного задания» также нажмите «ОК».

22. Перейдите на вкладку «Запланированные задания» программы архивации Backup и убедитесь, что ваше задание «Ежедневный добавочный архив» появилось в расписании (Каждый день, начиная с текущего).

23. Закройте программу Backup. Дождитесь наступления времени установленного вами на запуск задания архивации. Вы увидите, как запустится по расписанию программа Backup. После ее выполнения на диске Е появится добавочный архив doc-inc. bkf.

24. Запустите программу Backup. В меню «Сервис» выберите «Отчет». Появится окно со списком отчетов архивации. Выберите последний и откройте его.

25. Сравните полученный отчет с предыдущим.

26. Закройте все окна программы Backup. Обратите внимание, что в папке С:\Документы опять у всех файлов снят атрибут «архивный».

27. Удалите папку «Документы» со всеми файлами.

Задание 2. Восстановление данных

В этом задании с помощью программы Backup вы восстановите данные, ранее заархивированные.

1. Запустите программу Backup и перейдите на вкладку «Восстановление и управление носителем». В левом окне щелкните на узел «Файлы», чтобы раскрыть его. Выберите архив doc-normal. bkf.

2. Раскройте архив doc-normal .bkf и установите флажок напротив папки «Документы». Восстановим эту папку в ее исходное размещение. По умолчанию задан такой параметр снизу в выпадающем списке «Восстановить файлы в:».

3. Нажмите кнопку «Восстановить». В диалоговом окне «Подтверждение восстановления» нажмите кнопку «ОК».

4. В окне «Проверка расположения архивного файла» также нажмите кнопку «ОК».

5. После завершения восстановления закройте окно «Ход восстановления», нажав кнопку «Закрыть». Не закрывайте программу Backup Windows.

6. Убедитесь, что папка «Документы» со всеми файлами восстановлена в прежнее место на диск С:\. Откройте файл Планы. txt и убедитесь, что он не содержит последнюю строку текста с текущей датой.

7. Вернитесь в программу Backup на вкладку «Восстановление и управление носителем».

8. В левом окне щелкните и раскройте архив doc-inc.bkf и установите флажок напротив папки «Документы», в которой содержится один файл Планы. txt. По

умолчанию программа Backup не заменяет существующие файлы с одинаковым именем. Поэтому необходимо сделать следующую настройку.

9. В меню «Сервис» выберите пункт «Параметры» и перейдите на вкладку «Восстановление». На этой вкладке переключитесь на вариант «Заменять файл на компьютере, только если он старее» и нажмите кнопку «ОК».

10. Нажмите кнопку «Восстановить». В диалоговом окне «Подтверждение восстановления» нажмите кнопку «ОК».

12. Если появится окно «Проверка расположения архивного файла», то также нажмите кнопку «ОК».

13. После завершения восстановления закройте окно «Ход восстановления», нажав кнопку «Закрыть».

14. Закройте программу Backup Windows.

15. Убедитесь, что восстановлена последняя версия файла Планы. txt.

Задание 3. Архивация и восстановление данных при использовании программ архивации данных

В этом упражнении с помощью программы WinRar вы заархивируете данные и защитите архив паролем.

1. Создайте документ на диски С в папке Temp.

2. Загрузите программу - архиватор WinRar.

3. Перейдите в среде архиватора в созданную вами папку.

4. Создайте архив в вашей папке.

5. Перейдите на вкладку Дополнительно в среде архиватора. Выберите Установить пароль, задайте и подтвердите пароль.

6. Проверьте парольную защиту архива.

Оформление отчета

Включить в отчет

1. Номер, тему и цель лабораторной работы.

2. Назначение и основные шаги теневого копирования информации действия при архивации данных с использованием программы Bakup назначение и этапы создания отказоустойчивых томов.

Контрольные вопросы:

1. Технология теневого копирования информации.

2. Что для политики безопасности обеспечивает технология теневого копирования?

3. Какие типы архивов поддерживаются программой Backup Windows?

4. В чем отличие архивирования с использованием программы архивации?

5. Вам необходимо провести резервное копирование файлов с помощью программы Bakup, но при этом вы не хотите изменять состояние бита архива выбранных для архивации файлов. Какой тип архива необходимо выбрать для решения этой задачи?

6. Вам необходимо создать программный RAID на файловом сервере под управлением ОС Windows 2003/XP, чтобы обеспечить отказоустойчивость данных. Пользователи, обращаясь к ресурсам данного файлового сервера чаще выполняют операции чтения, и гораздо реже - записи. Какой при этом тип RAID целесообразно выбрать?

7. Опишите технологию создания отказоустойчивых томов для хранения данных.

8. Назначение шифрования информации.

9. Какие атрибуты шифрования папки можно указать?

10.Почему необходимо чтобы при копировании или перемещении шифрованной папки пункт назначения поддерживал это шифрование?

Лабораторная работа №2

Изучение программных средств защиты от несанкционированного доступа

Цель:

- изучить основные программные средства защиты от несанкционированного доступа;
- определить политику безопасности системы;
- научится применять некоторые средства защиты информации в ОС.

Работа с реестром в Windows

Реестр - база данных операционной системы, содержащая конфигурационные сведения. Физически вся информация реестра разбита на несколько файлов. Реестры Windows 9x и NT частично различаются. В Windows 95/98 реестр содержится в двух файлах **SYSTEM.DAT** и **USER.DAT**, находящиеся в каталоге Windows. В Windows Me был добавлен еще один файл **CLASSES.DAT**. В Windows XP реестр хранится во многих файлах. Основная часть хранится в файлах **sam, security, software, system, default** (все файлы без расширения). По замыслу Microsoft он должен был полностью заменить файлы ini, которые были оставлены только для совместимости со старыми программами, ориентированными на более ранние версии операционной системы. Почему произошел переход от ini файлов к реестру? Дело в том, что на эти файлы накладывается ряд серьезных ограничений и главное то, что предельный размер такого файла составляет 64Кб.

ПРЕДУПРЕЖДЕНИЕ: НИКОГДА не удаляйте или не меняйте информацию в реестре, если Вы не уверены, что это именно то, что нужно. В противном случае некорректное изменение данных может привести к сбоям в работе Windows и, в лучшем случае, информацию придется восстанавливать из резервной копии. Раздел **HKEY_CURRENT_USER** является подразделом раздела HKEY_USERS (HKEY_USERS содержит все активные загруженные профили пользователей компьютера). HKEY_CURRENT_USER является корневым для данных конфигурации пользователя, вошедшего в систему в настоящий момент. Здесь хранятся папки пользователя, параметры рабочего стола, сетевых подключений, принтеров и приложений. Эти сведения сопоставлены с профилем пользователя. Вместо полного имени раздела иногда используется аббревиатура HKCU.

Параметры текущего пользователя делятся на несколько категорий:

AppEvents - содержит пути звуковых файлов, используемых для озвучивания системных событий.

Control Panel - содержит различные данные, которые могут быть изменены в панели управления.

Display - содержит пользовательские установки экрана для текущего пользователя (этот подраздел доступен, только если разрешены пользовательские профили (user profiles)).

InstallLocationsMRU - содержит пути, использованные в процессе последней инсталляции.

Keyboard layout - содержит информацию о раскладке клавиатуры. Текущая раскладка клавиатуры устанавливается с использованием пункта Клавиатура (Keyboard) панели управления.

Network - содержит подразделы, описывающие постоянные и недавно установленные сетевые соединения, а также состояние сети.

RemoteAccess - необязательный подраздел, доступный только в случае, если установлен сервис удалённого доступа.

SOFTWARE - содержит пользовательские настройки приложений. Этот раздел ссылается на раздел HKEY_LOCAL_MACHINE, в котором также хранятся настройки приложений.

Раздел **HKEY_LOCAL_MACHINE** определяет всю информацию, относящуюся к локальному компьютеру, такую как драйверы, установленное программное обеспечение, наименование портов и конфигураций программного обеспечения. Эта информация верна для всех пользователей, подключённых к системе.

Раздел HKEY_LOCAL_MACHINE состоит из нескольких подразделов: Hardware - хранит информацию об устройствах, обнаруженных в компьютере. Все параметры этого раздела хранятся не на жестком диске, а в оперативной памяти. Когда компьютер распознает запуск устройства, он нумерует найденное устройство, исследуя шину и отдельные классы устройств (например, порты или клавиатуру). Security - здесь содержится всевозможная информация, относящаяся к защите. Формат не документирован. Используется для кэширования верительных данных для входа в систему, настроек политики и разделяемых секретных данных сервера. Подраздел Security\SAM содержит копию большинства данных из HKLM\SAM.

Sam - здесь хранятся локальные учетные записи или группы, созданные на компьютере. Раздел скрыт.

Software - вся информация о программах, установленных на компьютере, хранится здесь.

System\CurrentControlSet - последним действием фазы загрузки Windows является обновление реестра, которое должно зафиксировать набор служб и управляющих настроек, применявшийся при последней успешной загрузке. CurrentControlSet всегда указывает на набор управляющих настроек, используемых системой в текущий момент. System\MountedDevices - тома динамических дисков зависят от наличия информации о текущей конфигурации о логических томах на диске. Приложения и оснастки берут эту информацию из службы Logical Volume Manager, которая хранит свой список смонтированных и доступных устройств и подразделе MountedDevices.

Информация о выбранной политике безопасности хранится в следующих ветках реестра Windows XP:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\policies

ВходвWindows

Автоматический вход в Windows

Существует возможность автоматического входа в Windows, минуя экран приветствия. Данный способ не совсем безопасен, так как любой может войти в систему, если не требуется вводить пароль. Для автоматического входа в систему требуется изменить строковый параметр AutoAdminLogon на 1 в разделе HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon

Также необходимо установить строковые значения DefaultUserName и DefaultPassword в этом же разделе, равными имени пользователя и пароля, которые используются для входа в Windows. Возможно, вам также придется установить строковое значение DefaultDomainName, если ваш компьютер используется как домен. Однако вы должны понимать, что при автоматическом входе любой пользователь, получивший доступ к вашем компьютеру, может узнать ваш пароль, который хранится в реестре в открытом виде.

Лимит на число попыток автоматического входа в Windows

Данная настройка является логическим продолжением предыдущей настройки. Можно задать число попыток для автоматического входа в Windows. В этом случае в том же разделе надо создать параметр Dword AutoLogonCount и присвоить ему некоторое значение. Например, если вы присвоите значение 5, то система пять раз автоматически войдет в Windows. Причем при каждом входе данный параметр в реестре будет автоматически уменьшаться на единицу. Когда значение параметра достигнет 0, ключи **AutoLogonCount** и **DefaultPassword** будут удалены из реестра, а параметру **AutoAdminLogo** будет присвоено значение 0.

Регистрационные данные

Если вы нажмете на пункт меню О программе в Проводнике или в других программах, поставляемых с Windows, то увидите, кто обладает правом использования этой копии. Также эти данные можно увидеть в апплете Система Панели управления. Возможно, вам компьютер достался от вашего босса Пупкина, и вы хотели бы изменить регистрационные данные. Для этого нужно изменить строковые параметры RegisteredOwner (Ваше имя) и RegisteredOrganization (название организации) в разделе HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion

Диспетчер задач Windows

Чтобы запретить пользователю возможность запуска **Диспетчера задач Windows**, установите значение параметра типа **DWORD** DisableTaskMgr в разделе HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System равным 1.

Пароль после ждущего режима

Можно настроить систему таким образом, чтобы при включении компьютера после **Ждущего режима** появлялось диалоговое окно с приглашением ввести пароль. Для этого в разделе

HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System\Power создаем параметр типа DWORD Prompt Password On Resume со значением 1.

Автозагрузка

Что скрывается в автозагрузке?

Существует несколько способов прописать программу в автозагрузку. Самый простой - скопировать программу или ярлык в папку Автозагрузка. Но существует другой способ - через реестр. Этим способом часто пользуются вредоносные программы (вирусы, трояны, шпионы)

Сперва откройте раздел

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion.

Найдите там подразделы Run, RunOnce В этих разделах есть строковые ключи (некоторые разделы пустые), отвечающие за запуск программ. Название ключа может быть произвольным, а в качестве значения у них указывается запускаемая программа, если надо, то с параметрами. Обратите внимание на разделы, в названии которых присутствует «Once». Это разделы, в которых прописываются программы, запуск которых надо произвести всего один раз. Например, при установке новых программ некоторые из них прописывают туда ключи, указывающие на какие-нибудь настроечные модули, которые запускаются сразу после перезагрузки компьютера. Такие ключи после своего запуска автоматически удаляются.

Проверьте, что за программы у вас запускаются, все ли они нужны вам при загрузке, и лишнее удалите. Это позволит значительно ускорить загрузку Windows. В разделе HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion есть только два подраздела, отвечающие за автозагрузку: Run и Runonce. Изначально они пустые, так что все записи сделаны другими программами.

Запрет на автозагрузку

Существуют способы наложения запрета на автозагрузку программ через записи в реестре, указанные выше. Используются параметры типа **DWORD**. Все параметры должны храниться в разделе

HKEY_LOCAL_MACHINESoftware\Microsoft\Windows\CurrentVersion\Policies\Explorer

Для запрета запуска программ, прописанных в подразделе Run раздела **LOCAL MACHINE** используется параметр DisableLocalMachineRun со значением 1. В этом случае система игнорирует содержимое списка **Run**, находящегося в **LOCAL MACHINE**. Аналогично действует запрет списка **Run Once** для **LOCAL MACHINE**. За состояние

этой политики отвечает параметр DisableLocalMachineRunOnce. Система игнорирует содержимое **RunOnce** в **LOCAL MACHINE.**

Для запрета списка **Run** раздела **CURRENT USER** используется параметр DisableCurrentUserRun.

Для запрета списка **Run Once** раздела **CURRENT USER** используется параметр DisableCurrentUserRunOnce

Автозапуск CD-ROM

Отключение стандартного автозапуска компакт-дисков

Чтобы отключить автозапуск компакт-диска, устанавливаем значение параметра типа **DWORD** AutoRun, равным 0, в разделе

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CDRom

Запрещение запуска программ

Windows позволяет ограничить доступ к программам, кроме разрешенных в специальном списке.

Для ограничения запускаемых программ надо открыть раздел HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVerson\Policies\Explorer и создать там ключ RestrictRun типа DWORD со значением 0x00000001. Затем тут же надо создать подраздел с аналогичным именем RestrictRun и в нем перечислить список РАЗРЕШЕННЫХ к запуску программ для текущего пользователя. Записи в этом подразделе пронумеровываются, начиная с 1, и содержат строки с путями (необязательно) и именами приложений. Файлы должны быть с расширением. Например, Word.exe, Excel.exe.

Не забудьте указать файл Regedit.exe, иначе Вы сами не сможете больше запустить редактор реестра! Для сброса ограничения на запуск программ надо установить значение ключа RestrictRun в 0.

Запрещение запуска редактора реестра

Вы можете запретить запуск редактор реестра .

Для этого в разделе HKEY_CURRENT_USER\SOFTWARE\Microsoft\ Windows\CurrentVerson\Policies\System нужно добавить ключ типа DWORD DisableRegistryTools со значением 1. Запуск редактора реестра будет запрещен, однако останется возможность вносить изменения с помощью программного обеспечения сторонних разработчиков и с помощью REG-файла

Пароли и безопасность

Рассматриваемые настройки хранятся в ветви

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\ Network

Все ключи имеют тип **DWORD**, если это не обговорено отдельно; значение ключа равное 1 включает данную опцию, 0 выключает, если это не обговорено отдельно

Отмена кэширования пароля

Данная настройка помогает избавиться от проблемы «утаскивания» и дальнейшего взлома ваших сетевых и интернет-паролей. Эти пароли хранятся в файле с расширением PWL. Отключение кэша запрещает запись паролей в этот файл. Следовательно, его «выкрадывание» и дальнейший взлом не приносят никаких результатов. Единственное неудобство - это надобность вводить каждый раз при коннекте в окно DialUp - Password пароль вручную. Но это всё же лучше, чем «подарить» пароль и логин хакеру. Итак, используем параметр типа DisablePwdCaching со значением 1. Находим в каталоге Windows файл (или файлы) с расширением PWL. Удаляем их. Перезагружаемся. Файл паролей хоть и создаётся опять, но он пустой.

Звездочки в паролях

Параметр типа HideSharePwds со значением 1 определяет, показывать ли пароли к расшаренным ресурсам (имеющим общий доступ) открытым текстом или заменять их звездочками.

Запрет перечисления рабочей группы

Для того чтобы запретить перечисление содержимого рабочей группы, надо установить значение ключа NoWorkgroupContents равным 1. Даже при запрете пользователи могут подключаться к компьютерам в своей рабочей группе или домене. Для этого необходимо набрать полное сетевое имя разделенного ресурса в формате UNC, в диалоговых окнах команд «Выполнить» или «Подключить сетевой диск».

Раскладка клавиатуры

Раскладка для окна Приветствие

Если при установки системы вы в качестве основного языка установили русский язык, а пароль обычно используете на английском языке, то при выводе окна **Приветствие** вам каждый раз придется переключаться с русского языка на английский, чтобы ввести пароль. Чтобы по умолчанию система выводила английскую раскладку в этом окне надо открыть раздел HKEY_USERS\.DEFAULT\Keyboard Layout\Preload

И там надо на первую позицию поместить желаемую раскладку - 00000409 (английская раскладка) или 00000419 (русская), т.е. просто поменяйте их местами.

Клавиша Windows

Отключение клавиши Windows

На некоторых современных клавиатурах присутствует клавиша Windows (как правило, логотип-флажок Майкрософт). Некоторым пользователям она мешает при быстрой печати или играх. Чтобы отключить ее, нужно создать новый двоичный параметр Scancode Map со значением **00 00 00 00 00 00 00 00 03 00 00 00 00 00 5B E0 00 00 5C E0 00 00 00 00** в разделе

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\KeyboardLayout

Запрещение горячих клавиш с клавишей Windows

Можно отключить использование комбинацию «горячих» клавиш с клавишей Windows. Для этого создаем параметр типа **DWORD** NoWinKeys со значением 1 в разделе HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Policies\Explorer

Однако после установки этого запрета одиночное нажатие клавиши Windows, которое вызывает меню «Пуск», будет работать.

Длинные и короткие имена файлов

Запрещение длинных имен файлов

Вы можете запретить длинные имена файлов в Windows, заставив тем самым генерировать имена в формате 8.3 (DOS-овский формат). Для этого в разделе HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\FileSystem надо изменить параметр Win31FileSystem, присвоив ему значение 01 (по умолчанию стоит 00). Сделанные изменения вступят в силу после перезагрузки

Установка способа доступа к расширенным ресурсам компьютера из сети (Windows NT/2000/XP)

Раздел: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

Параметр типа DWORD RestrictAnonymous , если значение равно 1 - запрещает анонимным юзерам просматривать удаленно

Учетные записи и расширенные ресурсы. 2 - отказывает любой неявный доступ к системе (в сетевом окружении компьютер не будет виден, однако, доступ к нему можно будет получить, обратившись к нему по его IP).

Запрет сохранения паролей в Dial-Up-соединениях

По умолчанию, в Dial-Up-соединениях введенный пароль сохраняется после успешного соединения, если задействована опция «Сохранять имя пользователя и пароль», расположенная на диалоговом окне для Dial-Up. Это достаточно удобно для

многих пользователей, но если вы занимаетесь проблемой безопасности системы, то можете запретить сохранение этих паролей. В разделе
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters
создайте параметр типа **DWORD** DisableSavePassword со значением 1, который запрещает сохранение паролей в Dial-Up-соединениях. В этом случае опция «Сохранять имя пользователя и пароль» становится недоступной, а сохраненные пароли пропадают.

Задание

1. Запустить программы просмотра и редактирования реестра Windows regedit.exe и regedt32.exe (с помощью команды «Выполнить» главного меню). Ознакомиться со структурой реестра.

1.1. Включить в отчет краткие сведения о содержании основных разделов реестра (HKEY_CURRENT_USER и HKEY_LOCAL_MACHINE).

1.2. Включить в отчет сведения о различиях в функциональных возможностях изученных программ редактирования реестра (если лабораторная работа выполняется в операционной системе Windows).

Примечание: в операционную систему Windows XP Professional включен один редактор реестра, который можно запустить с помощью любого из указанных выше имен.

Защита документов Microsoft

1. Открыть (или создать) произвольный документ в текстовом процессоре Word. Изучить порядок использования паролей для защиты документов в Microsoft Word от чтения и записи и включить в отчет соответствующие сведения. Чтобы защитить документ, следует воспользоваться опциями на закладке **Безопасность (Security)** в диалоговом окне **Параметры (Options)**. В этом диалоговом окне можно установить пароль, который должен быть введен прежде, чем кто-то сможет открыть или изменить документ. Выбор флажка «Рекомендовать доступ только для чтения» (Read-only recommended) позволяет отображать сообщение, которое рекомендует пользователю открывать документ только для чтения. Можно также использовать кнопку «Установить защиту» (Protect Document) на закладке Безопасность (Security), чтобы установить пароли, для ограничения тех, кто может вносить изменения или вводить комментарии.

2. Открыть (или создать) произвольную таблицу Excel. Изучить порядок использования паролей для защиты документов или их частей в табличном процессоре Microsoft Excel от чтения и записи и включить в отчет соответствующие сведения.

Microsoft Excel поддерживает три уровня защиты при сохранении книг. Эти параметры могут использоваться как вместе, так и по отдельности: **Пароль для открытия (Password to open):** для того чтобы открыть книгу, пользователь должен ввести пароль, являющийся кодом, с помощью которого был зашифрован файл. **Пароль для изменения (Password to modify)**: для того чтобы открыть книгу в режиме редактирования, пользователь должен ввести пароль. Не вводя пароль, пользователь может открыть книгу в режиме только для чтения. **Рекомендовать доступ только для чтения (Read-only recommended):** пользователю предлагается открыть документ в режиме только для чтения. Если в диалоговом окне пользователь нажимает кнопку Нет (No), а какой-либо другой метод защиты не используется, книга Excel открывается в режиме редактирования. Для шифрования книг используются различные криптографические методы, которые можно выбрать, нажав кнопку Дополнительно (Advanced) в диалоговом окне Параметры сохранения (Save Options), доступном из меню Файл - Сохранить как - Сервис - Общие параметры (File - Save As - Tools - General Options). Метод шифрования по умолчанию можно также задать с помощью системных политик. В дополнение к защите всей книги Microsoft Excel Вы также можете защитить от несанкционированных изменений отдельные области этой книги.

В некоторой степени можно защитить книгу с помощью следующих параметров, доступных в меню Сервис - Защита (Tools - Protection): Защитить лист (Protect Sheet)/

3. Ознакомиться (на примере папок, созданных на диске с) с порядком разграничения доступа к ресурсам в защищенных версиях операционной системы Windows (с помощью контекстного меню объекта и элементов управления соответствующих диалоговых окон). Если команда «Общий доступ и безопасность» недоступна (при работе в ОС Windows XP Professional), то выключить режим «Использовать простой общий доступ к файлам» на вкладке «Вид» окна свойств папки. Чтобы включить команду «Общий доступ и безопасность», используемую для управления общим доступом к папкам и файлам, необходимо выключить режим «Использовать простой общий доступ к файлам» на вкладке «Вид» окна свойств папки. Общие права доступа задаются во вкладке *Доступ* при просмотре свойств файла. Полный набор прав доступа для конкретного файла (папки) можно просмотреть: Свойства - вкладка *Безопасность* - *Дополнительно* - вкладка *Разрешения* - выбрать пользователя, начать кнопку *Изменить*. Появится окно с полным набором прав доступа. Текущего владельца данного объекта можно определить на вкладке *Владелец* свойств объекта. *Действующие* разрешения можно посмотреть на вкладке Действующие разрешения.

Задание

1. Произвести защиту созданного вами документа Microsoft Word на любом уровне. Завершить работу с Word.

2. Произвести защиту книги и листа документа Microsoft Excel. Завершить работу с Excel.

3. Включить в отчет сведения об особенностях управления доступом к папкам и файлам (общих правах доступа, полном наборе прав доступа, владельце объекта, действующих разрешениях на доступ к объекту для конкретного субъекта).

Изучение политики безопасности системы

I Ознакомиться (с помощью функции Панели управления Администрирование | Управление компьютером) с порядком создания и изменения учетных записей пользователей и групп в защищенных версиях операционной системы Windows. Для этого сделайте следующее:

1. В левой части окна локальных пользователей и групп зайдите в папку **Пользователи (Users)**, чтобы отобразить список текущих пользователей, зарегистрированных на компьютере (рис.2.19).

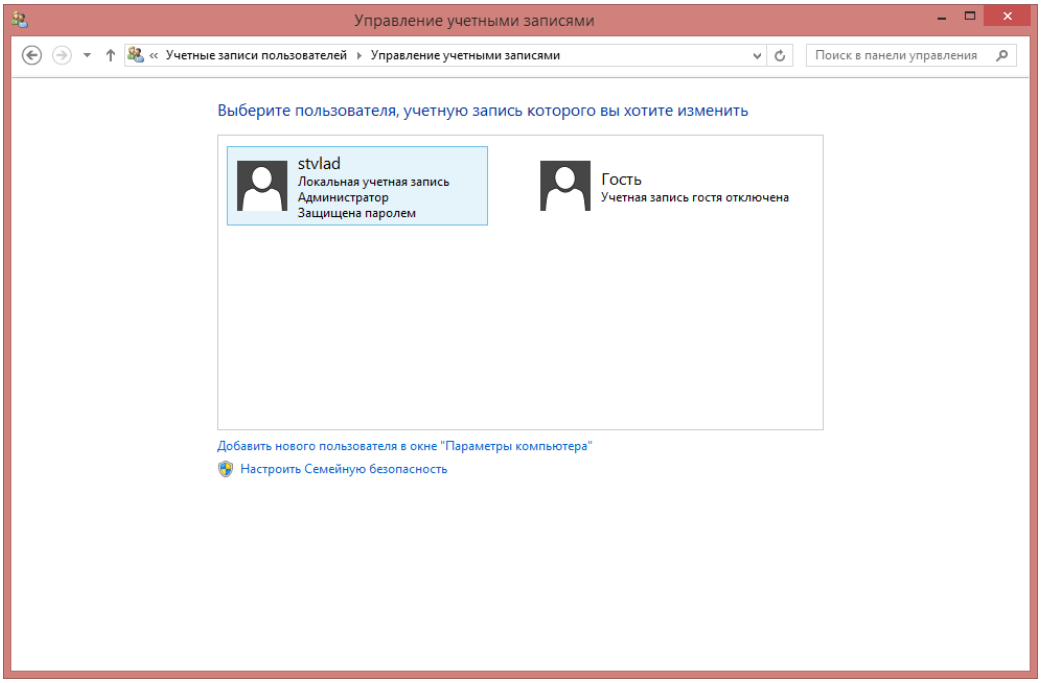

Рис.2.19. Управление учетными записями

2. В меню **Действия (Action**) щелкните на пункте **Новый пользователь (New User**). Откроется окно Н**овый пользователь (New User)** (рис.2.20).

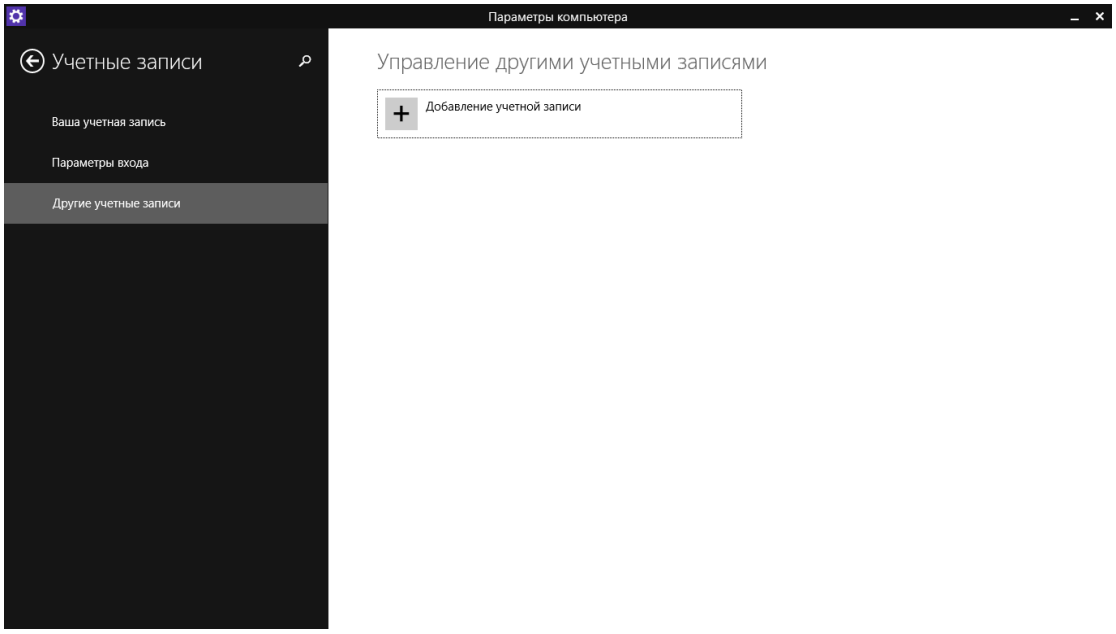

Рис.2.20. Добавление учетной записи

3. В поле ввода **Пользователь (Username)** наберите **Гость.**
4. В поле ввода **Полное имя (Fullname)** наберите **Гость.**
5. В поле ввода **Описание** (**Description)** наберите **Man'sbestfriend.**
6. В поле ввода **Пароль (Password)** наберите **Wooh.**
7. Наберите пароль в окне **Подтверждение пароля (Confirmpassword)**.

Убедитесь, что напротив пунктов **Потребовать смену пароля при следующем входе в систему (Usermustchangepasswordatnextlogon)** и **Отключить учетную запись (Accountisdisabled)** не стоит галочек. После этого щелкните на кнопке **Создать (Create).**

8. Щелкните на **Закрыть (Close)**, чтобы вернуться в окно **Локальные пользователи и группы (LocalUsersandGroups)**. Гость был добавлен в список пользователей. Щелкните дважды по пользователю Гость в правой части окна **Локальные пользователи и группы (LocalUsersandGroups)**. Откроется диалоговое окно свойств пользователя (рис.2.21).

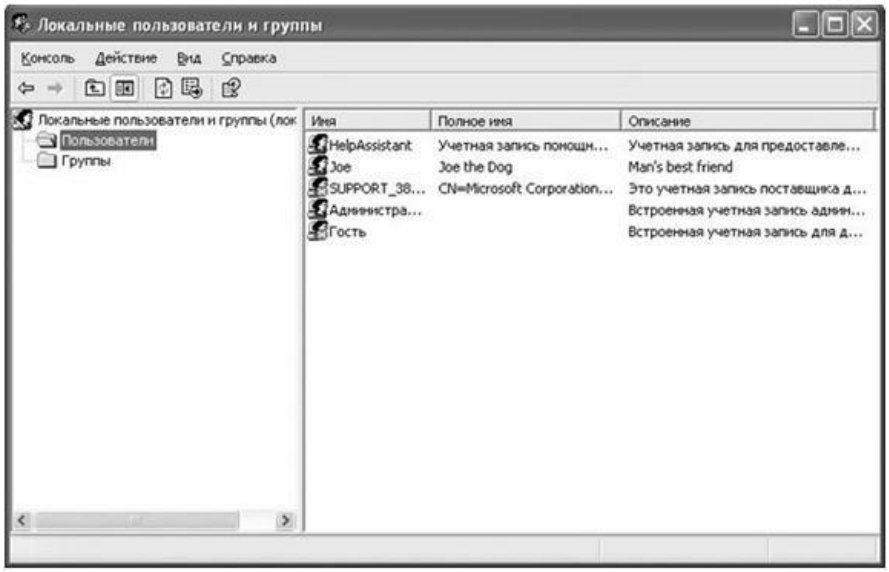

Рис.2.21. Изменение учетной записи

9. Выберите вкладку **Членство в группах (Memberof)**. На данный момент Joe принадлежит к группе **Пользователи (Users)**, которая является группой по умолчанию для новых пользователей.

10. Щелкните на **Отмена (Cancel)**, чтобы закрыть диалоговое окно свойств пользователя «Joe». Чтобы переместить пользователя в другую группу, откройте папку **Группы (Groups)**. В левой части окна **Локальные пользователи и группы (LocalUsersandGroups)** отобразится список доступных групп (рис.2.22).

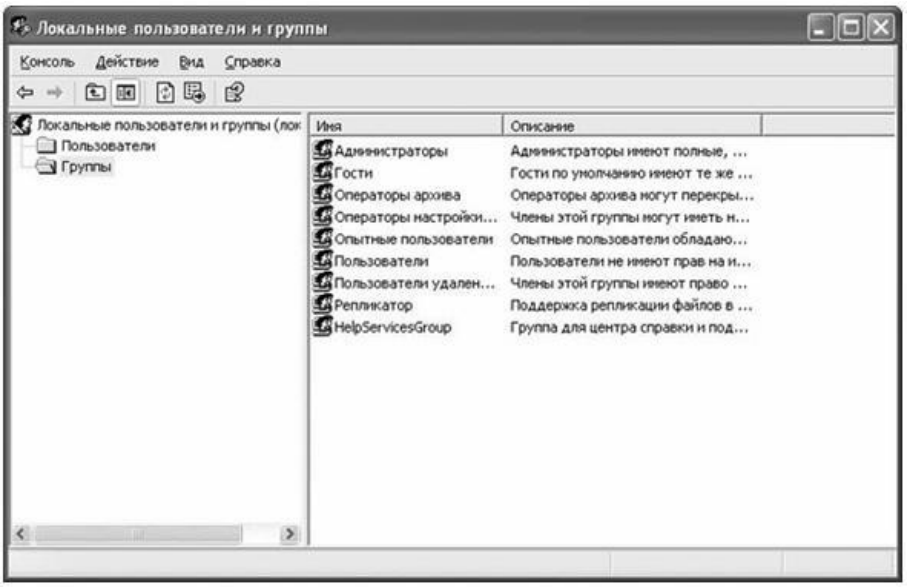

Рис.2.22. Изменение учетной записи

11. В правой части окна **Локальные пользователи и группы (LocalUsersandGroups)** дважды щелкните на пункте **Опытные пользователи (PowerUsers)**, чтобы открыть диалоговое окно свойств группы привилегированных пользователей. Щелкните на **Добавить (Add).**

12. Если вы подсоединены к сетевому домену, щелкните на кнопке **Размещение (Location)**, выберите имя вашего компьютера, а затем щелкните на OK.

13. В поле ввода **Введите имена выбираемых объектов (Entertheobjectnametoselect)** наберите Joe, а затем щелкните на **Проверить имена (Checknames).**

14. Щелкните на **OK**, чтобы добавить Joe в группу привилегированных пользователей, а затем щелкните на OK, чтобы закрыть диалоговое окно привилегированных пользователей (рис.2.23).

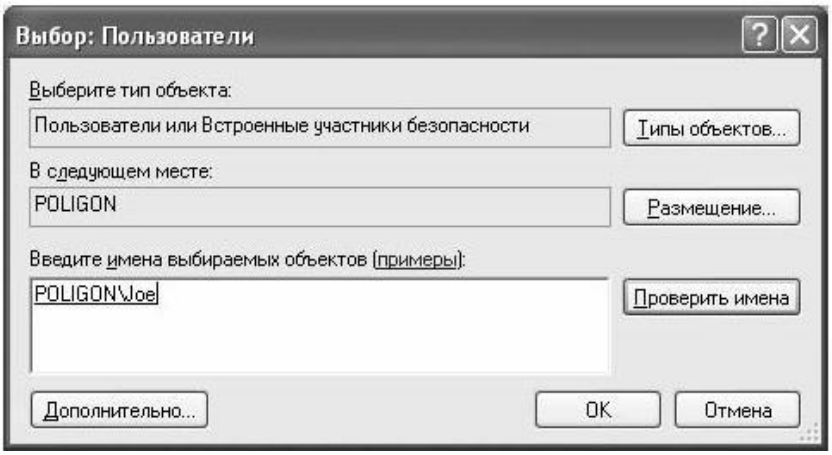

Рис.2.23. Изменение имени

II. Ознакомиться (с помощью функции Панели управления Администрирование | Локальная политика безопасности | Локальные политики | Назначение прав пользователя) с порядком назначения прав пользователям и группам.

Открыть объект Локальные параметры безопасности. В дереве консоли выбрать узел Назначение прав пользователей. В области сведений дважды щелкнуть право пользователя, которое требуется изменить. В окне Свойства: Право_пользователя нажать кнопку Добавить. Добавить пользователя или группу, а затем нажать кнопку ОК (рис.2.24).

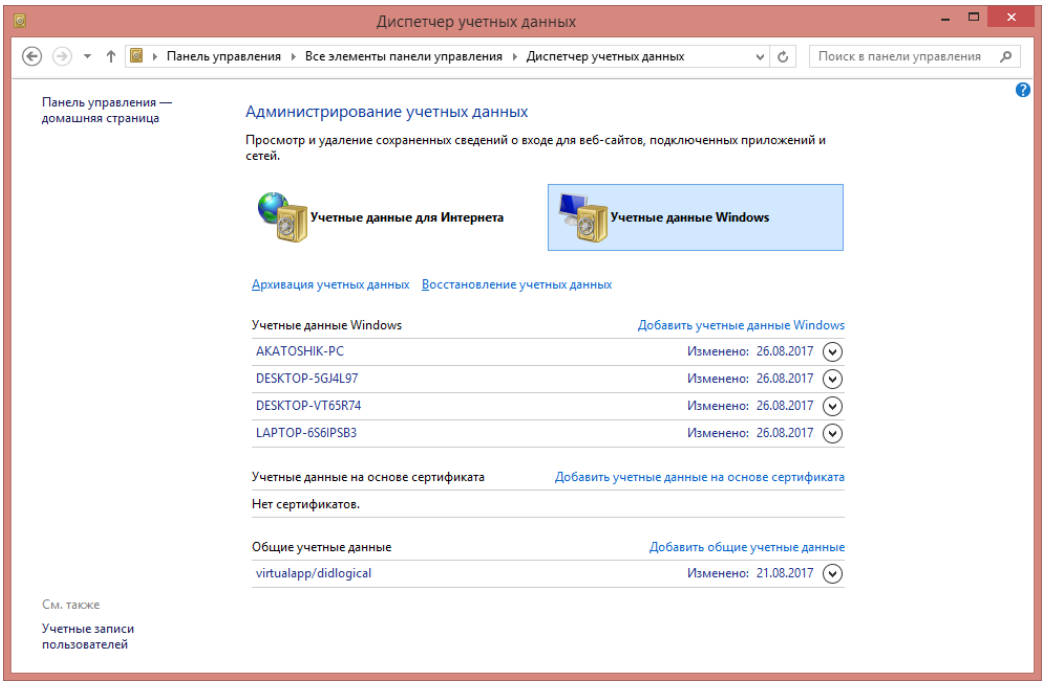

Рис.2.24. Администрирование

III. Ознакомиться (с помощью функции Панели управления Администрирование | Локальная политика безопасности | Локальные политики | Политика аудита) с порядком организации аудита доступа к файлам для определенных пользователей.

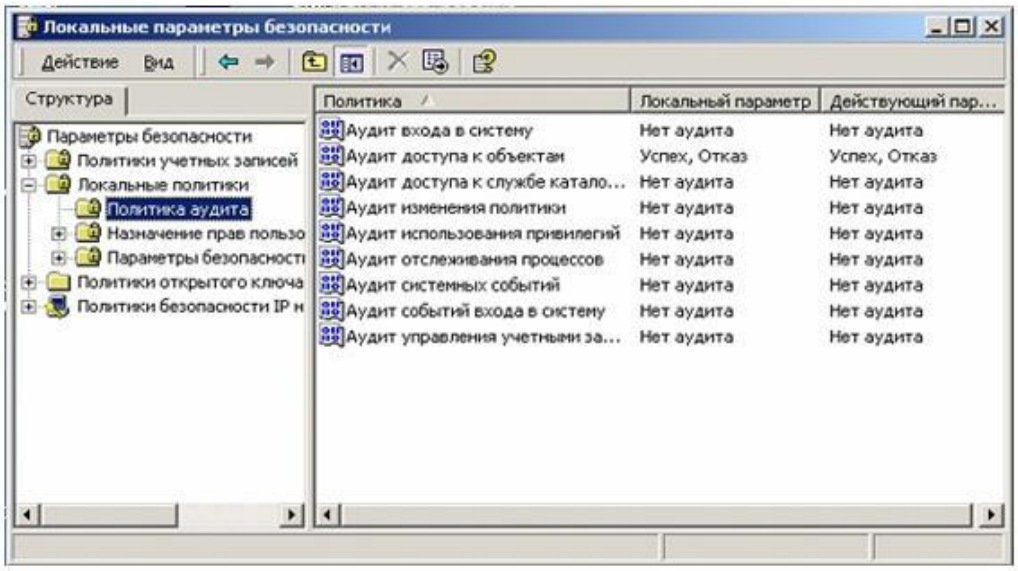

Рис.2.25. Безопасность

1. Включить в список проверки нужную совокупность событий, например, аудит доступа к объектам.

2. С помощью программы WindowsExplorer выбрать файл для аудита. Вызвать панель фиксации событий, которые связаны с файлом, подлежащим аудиту. Для этого при помощи мыши в контекстном меню открыть окно «Свойства», выбрать вкладку «Безопасность» (рис.2.25), затем, нажав кнопку «Дополнительно», выбрать «Аудит» (рис.2.26). Затем с помощью кнопки «Добавить» выбрать пользователя, действия которого подлежат аудиту, и перечень событий, подлежащих аудиту

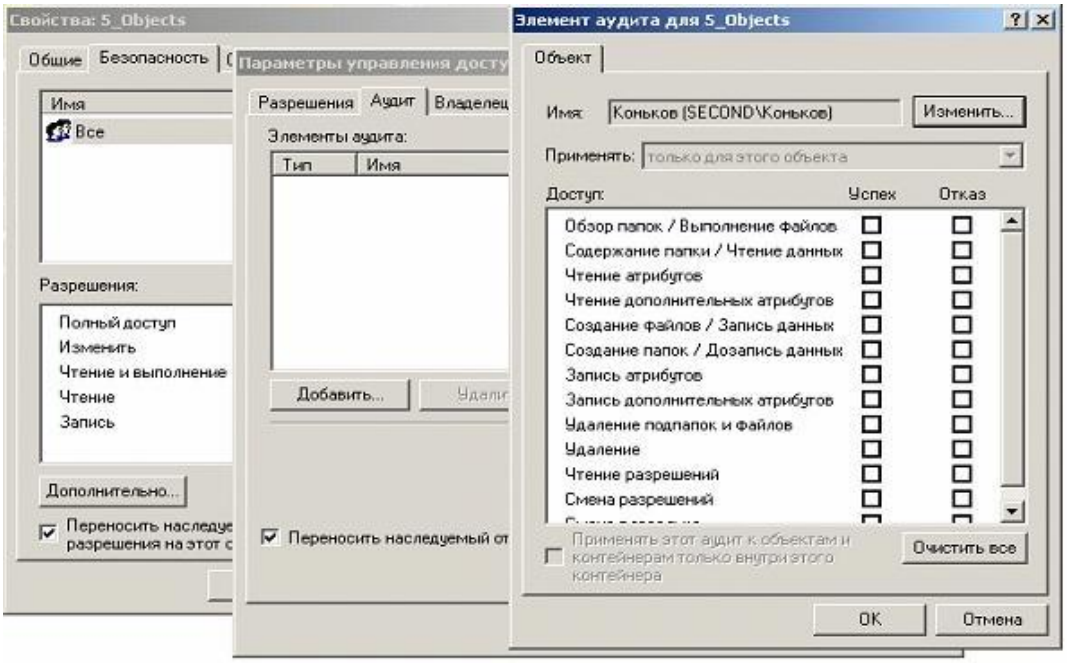

Рис.2.26. Аудит

3. В случае успеха попробовать осуществить обращение к данному файлу. Все оговоренные действия в отношении файла должны найти отражение в журнале событий безопасности. Для просмотра журнала событий нужно выбрать окно «Просмотр событий» через иконку «Администрирование» панели управления.

4. В случае отказа проверить наличие у пользователя (в том числе и у администратора), от имени которого производится эксперимент, привилегии «Создание журналов безопасности» и, в случае ее отсутствия, назначить ее пользователю с помощью консоли «Назначение прав пользователям».

IV. Ознакомиться (с помощью функции Панели управления Администрирование | Локальная политика безопасности | Политики учетных записей | Политика паролей) с порядком определения параметров безопасности для парольной аутентификации.

В этом разделе мы можем изменить такие параметры паролей, как: максимальный и минимальный сроки действия паролей, минимальная длина пароля, включить или отключить такие требования, как неповторяемость паролей у разных пользователей и соответствие пароля требованиям сложности.

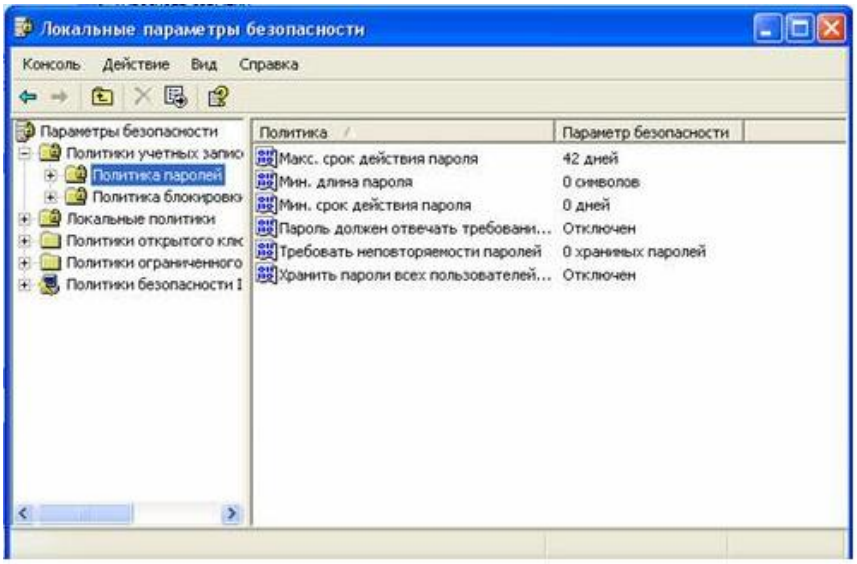

Рис.2.27. Параметры безопасности

V. Ознакомиться (с помощью функции Панели управления Администрирование | Локальная политика безопасности | Политики учетных записей | Политика блокировки учетных записей) с порядком определения параметров безопасности для политики блокировки учетных записей.

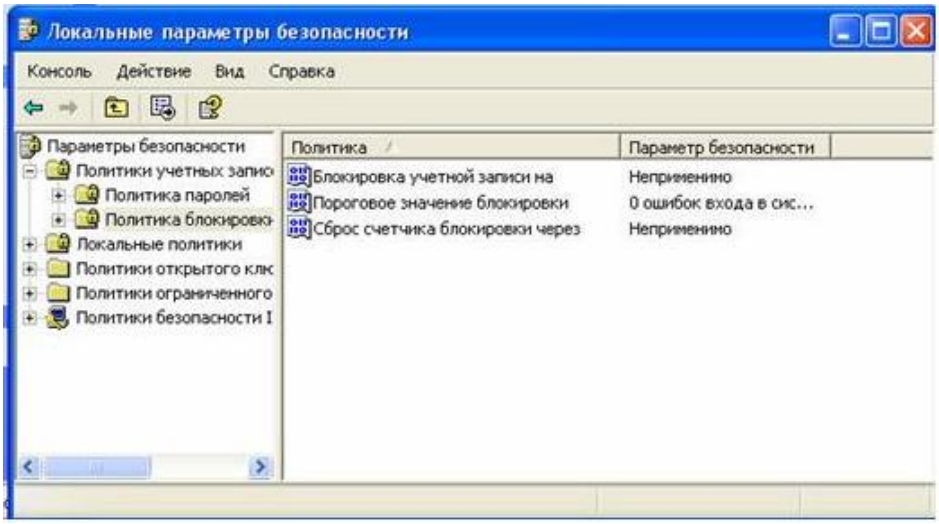

Рис.2.28. блокировка учетных записей

В этом разделе мы можем задать политику блокировки учётных записей. Существуют три параметра:

Пороговое значение блокировки - определяет количество ошибочных входов в систему, после которых учётная запись блокируется (от 1 до 999 попыток). Блокировка учётной записи на (количество времени) - определяет время, на которое блокируется учётная запись (от 1 до 99999 минут). Сброс счётчика блокировки через - определяет время, через которое сбросится счётчик блокировки (от 1 до 99999 минут). По умолчанию не определен, так как этот параметр имеет смысл только при указании параметра Пороговое значение блокировки.

VI. Ознакомиться (с помощью функции Панели управления Администрирование | Просмотр событий | Безопасность) с порядком определения всех событий, происходящих в системе и нарушающих политику безопасности (фиксируются данные, учтенные с помощью статического и сигнатурного метода).

Оформление отчета

Включить в отчет:

номер, тему;

сведения о содержании основных разделов реестра;

сведения о локальной политики парольной защиты, политики блокировки учетных записей пользователя и правилах их создания, о назначенных правах пользователей и т.д. порядок действий для защиты документов Microsoft.

Контрольные вопросы

1. Какой из изученных в лабораторной работе редакторов реестра предоставляет функции по разграничению доступа к разделам реестра и как использовать эти функции?

3. Как с помощью программы restrick.exe ограничить доступ пользователей к дисковым устройствам?

4. Как ограничить доступ пользователей к функциям Панели управления с помощью программы restrick.exe?

5. Доступ к каким функциям Панели управления может быть ограничен с помощью программы restrick.exe?

6. В чем недостаточность средств ограничения прав пользователей, предоставляемых программой restrick.exe?

7. Как может быть заблокирована рабочая станция на период временного отсутствия пользователя? Укажите несколько вариантов.

8. Какой из способов блокирования рабочей станции на период временного отсутствия пользователя является наиболее безопасным и почему?

9. Как устанавливается защита от чтения документов Microsoft Word и таблиц Microsoft Excel?

10. Что происходит с документом Microsoft Office после установки защиты от чтения с помощью паролей?

Лабораторная работа №3

Шифр Цезаря. Шифр Гронсфельда. Шифры перестановки (маршрутное шифрование)

Цель:

- изучить алгоритмы шифрования;
- реализовать алгоритмы шифрования на одном из языков программирования высокого уровня.

Шифр Цезаря (шифр сдвига, код Цезаря или сдвиг Цезаря). Один из самых известных и в то же время простых шифров (рис.2.29). Относится к шифрам моноалфавитной замены (каждой букве исходного текста ставится в соответствие единственная буква зашифрованного текста). В данном шифре каждая буква в слове или тексте заменяется другой, которая находится на некоторое постоянное число позицией левее или правее от неё в алфавите. Для расшифровки нужно только знать сдвиг (или ключ) в шифре. Например, если ключ k=3, то формула у нас получится такая: x=y-3. Здесь x – номер исходного (шифруемого) символа в алфавите, y – номер символа шифрованного текста в алфавите.

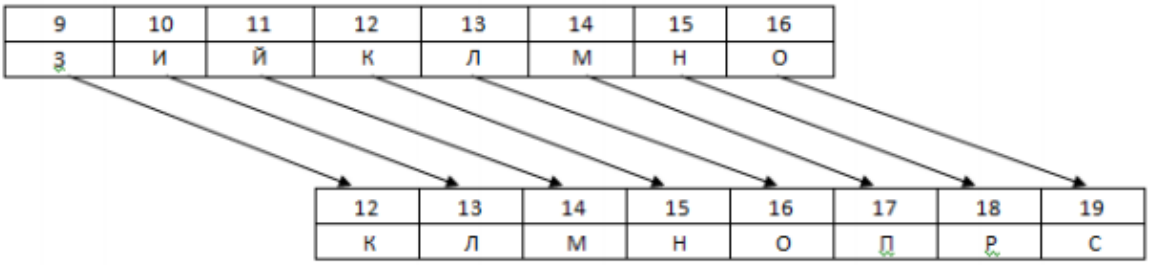

Рис.2.29. Шифр Цезаря

Пример:
Исходное слово: Наука.
Ключ (сдвиг) 4.
Шифрованное слово: Сдчод.

Существуют различные вариации этого шифра, например: ROT1, ROT13. ROT образовано от английского слово rotate, что в данном случае означает «сдвинуть». То есть сдвинуть на 1 позицию, сдвинуть на 13 позиций.

Шифр Гронсфельда

Этот шифр сложной замены, называемый шифром Гронсфельда, представляет собой модификацию шифра Цезаря числовым ключом. Для этого под буквами исходного сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифртекст получают примерно, как в шифре Цезаря, но не отсчитывают по алфавиту третью букву (как это делается в шифре Цезаря), а выбирают ту букву, которая смещена по алфавиту на соответствующую цифру ключа. Например, применяя в качестве ключа группу из четырех начальных цифр числа e (основания натуральных логарифмов), а именно 2718, получаем для исходного сообщения ВОСТОЧНЫЙ ЭКСПРЕСС следующий шифртекст:

Сообщение		В	О	С	Т	О	Ч	Н	Ы	Й		Э	К	С	П	Р	Е	С	С
Ключ		2	7	1	8	2	7	1	8	2		7	1	8	2	7	1	8	2
Шифртекст		Д	Х	Т	Ь	Р	Ю	О	Г	Л		Д	Л	Щ	С	Ч	Ж	Щ	У

Чтобы зашифровать первую букву сообщения В, используя первую цифру ключа 2, нужно отсчитать вторую по порядку букву от В; в алфавите получается первая буква шифртекста Д.

В	Г	Д
	1	2

Следует отметить, что шифр Гронсфельда вскрывается относительно легко, если учесть, что в числовом ключе каждая цифра имеет только десять значений, а значит, имеется лишь десять вариантов прочтения каждой буквы шифртекста. С другой стороны, шифр Гронсфельда допускает дальнейшие модификации, улучшающие его стойкость, в частности двойное шифрование разными числовыми ключами.

Шифры перестановки (маршрутное шифрование)

При таком способе шифрования изменяется только порядок следования символов в исходном тексте, но не изменяются сами символы. Существует несколько разновидностей шифров перестановки. Приведу некоторые из них. Шифр Сцитала. Использовался еще во времена Древней Спарты. Для шифровки использовался жезл («Сцитала») – цилиндр, на который наматывалась узкая пергаментная лента. На этой ленте вдоль оси цилиндра записывался шифруемый текст. Чтобы прочитать зашифрованный текст, использовались цилиндры такого же диаметра.

Шифр вертикальной перестановки. Для шифрования используется прямоугольник, в него вписывается текст (слева направо). Каждый столбец прямоугольника нумеруется, и затем буквы по вертикали (сверху вниз) выписываются согласно нумерации (ключу).

Пример: Исходный текст: «шифр вертикальной перестановки».

Ключ у нас пусть будет 3, 2, 5, 1, 4.

3	2	5	1	4
ш	и	ф	р	в
е	р	т	и	к
а	л	ь	н	о
й	п	е	р	е
с	т	а	н	о
в	к	и	-	-

Выпишем последовательно буквы из каждого столбца согласно ключу.

У нас получится вот такой зашифрованный текст:

Ринрн-ирлптк-шеайсв-вкоео-фтьеаи

Задание

Реализовать все рассмотренные шифры программно.

Оформление отчета

Включить в отчет

номер, тему лабораторной работы;

листинги программ алгоритмов шифрования.

Контрольные вопросы

1. Основные понятия криптографии и криптоанализа.
2. Понятие симметричной криптосистемы.
3. Шифры перестановки.
4. Шифры замены.
5. Основные характеристики открытых сообщений.

Лабораторная работа № 4

Реализация дискреционной модели политики безопасности

***Цель работы*:** ознакомиться с проблемами реализации политик безопасности в компьютерных системах на примере дискреционной модели.

Теоретические сведения

Под политикой безопасности понимают набор норм, правил и практических приемов, регулирующих управление, защиту и распределение ценной информации. Политика безопасности задает механизмы управления доступа к объекту, определяет как разрешенные, так и запрещенные доступы.

Политика безопасности реализуется посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты. Для конкретной организации политика безопасности должна носить индивидуальный характер и зависеть от конкретной технологии обработки информации и используемых программных и технических средств.

Политика безопасности определяется способом управления доступом, который задаёт порядок доступа к объектам системы. Различают два основных вида политики безопасности: избирательную и полномочную.

Избирательная политика безопасности основана на избирательном способе управления доступом. Избирательное (или дискреционное) управление доступом характеризуется заданным администратором множеством разрешенных отношений доступа (например, в виде троек объект – субъект – тип доступа). Обычно для описания

свойств избирательного управления доступом применяют математическую модель на основе матрицы доступа.

Матрица доступа представляет собой матрицу, в которой столбец соответствует объекту системы, а строка – субъекту. На пересечении столбца и строки матрицы указывается тип разрешенного доступа субъекта к объекту. Обычно выделяют такие типы доступа субъекта к объекту, как «доступ на чтение», «доступ на запись», «доступ на исполнение» и т.п. Матрица доступа является самым простым подходом к моделированию систем управления доступом. Однако она служит основой для сложных моделей, более адекватно описывающих реальные автоматизированные системы обработки информации (АСОИ).

Избирательная политика безопасности широко применяется в АСОИ коммерческого сектора, так как её реализация соответствует требованиям коммерческих организаций по разграничению доступа и подотчетности, а также имеет приемлемую стоимость.

Полномочная политика безопасности основана на полномочном (мандатном) способе управления доступом. Полномочное (или мандатное) управление доступом характеризуется совокупностью правил предоставления доступа, определенных на множестве атрибутов безопасности субъектов и объектов, например, в зависимости от метки конфиденциальности информации и уровня допуска пользователя. Полномочное управление доступом подразумевает следующее:

1) все субъекты и объекты системы однозначно идентифицированы;

2) каждому объекту системы присвоена метка конфиденциальности информации, определяющая ценность содержащейся в нем информации;

3) каждому субъекту системы присвоен определенный уровень допуска, определяющий максимальное значение метки конфиденциальности информации объектов, к которым субъект имеет доступ.

Чем важнее объект, тем выше его метка конфиденциальности. Поэтому наиболее защищенными оказываются объекты с наиболее высокими значениями метки конфиденциальности.

Основное назначение полномочной политики безопасности – регулирование доступа субъектов системы к объектам с различными уровнями конфиденциальности, предотвращение утечки информации с верхних уровней должностной иерархии на нижние, а также блокирование возможных проникновений с нижних уровней на верхние.

При выборе и реализации политики безопасности в компьютерной системе, как правило, работают следующие шаги:

1. В информационную структуру вносится структура ценностей (определяется ценность информации) и проводится анализ угроз и рисков для информации и информационного обмена.

2. Определяются правила использования для любого информационного процесса, права доступа к элементам информации с учетом данной оценки ценностей.

Реализация политики безопасности должна быть четко продумана. Результатом ошибочного или бездумного определения правил политики безопасности, как правило, является разрушение ценности информации без нарушения политики.

Дискреционная политика безопасности

Пусть O – множество объектов, U – множество пользователей, S – множество действий пользователей над объектами. Тогда дискреционная политика определяет отображение $O \rightarrow U$ (объектов на пользователей-субъектов). В соответствии с данным отображением каждый объект $O_j \in O$ объявляется собственностью соответствующего пользователя $U_k \in U$, который может выполнять над ними определенную совокупность действий $S_i \in S$, в которую могут входить несколько элементарных действий (чтение, запись, модификация и т.д.). Пользователь, являющийся собственником объекта, иногда

имеет право передавать часть или все права другим пользователям (обладание администраторскими правами).

Указанные права доступа пользователей-субъектов к объектам компьютерной системы записываются в виде так называемой матрицы доступа. На пересечении *i*-й строки и *j*-го столбца данной матрицы располагается элемент S_{ij} – множество разрешенных действий *j*-го пользователя над *i*-м объектом.

Пример. Пусть имеем множество из трёх пользователей {Администратор, Гость, Пользователь_1} и множество из четырёх объектов {Файл_1, Файл_2, CD-RW, Дисковод}. Множество возможных действий включает следующие: {Чтение, Запись, Передача прав другому пользователю}. Действие «Полные права» разрешает выполнение всех трёх действий, действие «Запрет» запрещает выполнение всех перечисленных действий. В данном случае матрица доступа, описывающая дискреционную политику безопасности, может выглядеть следующим образом (табл.2.3).

Таблица 2.3. Пример матрицы доступа

Объект / Субъект	Файл_1	Файл_2	CD-RW	Дисковод
1. Администратор	Полные права	Полные права	Полные права	Полные права
2. Гость	Запрет	Чтение	Чтение	Запрет
3. Пользователь_1	Чтение, передача прав	Чтение, запись	Полные права	Запрет

Например, Пользователь_1 имеет права на чтение и запись в Файл_2. Передавать же свои права другому пользователю он не может.

Пользователь, обладающий правами передачи своих прав доступа к объекту другому пользователю, может сделать это. При этом пользователь, передающий права, может указать непосредственно, какие из своих прав он передает другому.

Например, если Пользователь_1 передает право доступа к Файлу_1 на чтение пользователю Гость, то у пользователя Гость появляется право чтения из Файла_1.

Задание на лабораторную работу

Пусть множество *S* возможных операций над объектами компьютерной системы задано следующим образом: *S* = {«Доступ на чтение», «Доступ на запись», «Передача прав»}.

1. Получить данные о количестве пользователей и объектов компьютерной системы из табл.2.4, соответственно варианту.

2. Реализовать программный модуль, создающий матрицу доступа пользователей к объектам компьютерной системы. Реализация данного модуля подразумевает следующее:

2.1. Необходимо выбрать идентификаторы пользователей, которые будут использоваться при их входе в компьютерную систему (по одному идентификатору для каждого пользователя, количество пользователей указано для варианта). Например, множество из трёх идентификаторов пользователей {Ivan, Sergey, Boris}. Один из данных идентификаторов должен соответствовать администратору компьютерной системы (пользователю, обладающему полными правами доступа ко всем объектам).

2.2. Реализовать программное заполнение матрицы доступа, содержащей количество пользователей и объектов, соответственно Вашему варианту.

2.2.1. При заполнении матрицы доступа необходимо учитывать, что один из пользователей должен являться администратором системы (допустим, Ivan). Для него права доступа ко всем объектам должны быть выставлены как полные.

2.2.2. Права остальных пользователей для доступа к объектам компьютерной системы должны заполняться случайным образом с помощью датчика случайных чисел. При заполнении матрицы доступа необходимо учитывать, что пользователь может иметь

несколько прав доступа к некоторому объекту компьютерной системы, иметь полные права либо совсем не иметь прав.

2.2.3. Реализовать программный модуль, демонстрирующий работу в дискреционной модели политики безопасности.

3. Данный модуль должен выполнять следующие функции:

3.1. При запуске модуля должен запрашиваться идентификатор пользователя (проводится идентификация пользователя), при успешной идентификации пользователя должен осуществляться вход в систему, при неуспешной – выводиться соответствующее сообщение.

3.2. При входе в систему после успешной идентификации пользователя на экране должен распечатываться список всех объектов системы с указанием перечня всех доступных прав доступа идентифицированного пользователя к данным объектам. Вывод можно осуществить, например, следующим образом:

```
User: Boris
Идентификация прошла успешно, добро пожаловать в систему
Перечень Ваших прав:
Объект1:     Чтение
Объект2:     Запрет
Объект3:     Чтение, Запись
Объект4:     Полные права
Жду ваших указаний >
```

3.3. После вывода на экран перечня прав доступа пользователя к объектам компьютерной системы необходимо организовать ожидание указаний пользователя на осуществление действий над объектами в компьютерной системе. После получения команды от пользователя на экран необходимо вывести сообщение об успешности либо неуспешности операции. При выполнении операции передачи прав (grant) должна модифицироваться матрица доступа. Программа должна поддерживать операцию выхода из системы (quit), после которой запрашивается идентификатор пользователя. Диалог можно организовать, например, так:

```
Жду ваших указаний >read
Над каким объектом производится операция? 1
Операция прошла успешно
Жду ваших указаний > write
Над каким объектом производится операция? 2
Отказ в выполнении операции. У Вас нет прав для ее осуществления
Жду ваших указаний >grant
Право на какой объект передается? 3
Отказ в выполнении операции. У Вас нет прав для ее осуществления
Жду ваших указаний >grant
Право на какой объект передается? 4
Какое право передается? read
Какому пользователю передается право? Ivan
Операция прошла успешно
Жду ваших указаний > quit
Работа пользователя Boris завершена. До свидания.
User:
```

4. Выполнить тестирование разработанной программы, продемонстрировав реализованную модель дискреционной политики безопасности.

5. Оформить отчет по лабораторной работе.

Таблица 2.4. Варианты заданий

Вариант	Количество субъектов доступа (пользователей)	Количество объектов доступа
1	3	3
2	4	4
3	5	4
4	6	5

5	7	6
6	8	3
7	9	4
8	10	4
9	3	5
10	4	6
11	5	3
12	6	4
13	7	4
14	8	5
15	9	6
16	10	3
17	3	4
18	4	4
19	5	5
20	6	6
21	7	3
22	8	4
23	9	4
24	10	5
25	3	6
26	4	3
27	5	4
28	6	4
29	6	5
30	8	6

Контрольные вопросы

1. Что понимается под политикой безопасности в компьютерной системе?
2. В чем заключается модель дискреционной политики безопасности в компьютерной системе?
3. Что понимается под матрицей доступа в дискреционной политике безопасности? Что хранится в данной матрице?
4. Какие действия производятся над матрицей доступа в том случае, когда один субъект передает другому субъекту свои права доступа к объекту компьютерной системы?

Лабораторная работа № 5

Количественная оценка стойкости парольной защиты

Цель работы: реализация простейшего генератора паролей, обладающего требуемой стойкостью к взлому.

Теоретические сведения

Подсистемы идентификации и аутентификации пользователя играют важную роль в системах защиты информации.

Стойкость подсистемы идентификации и аутентификации пользователя в системе защиты информации (СЗИ) во многом определяет устойчивость к взлому самой СЗИ. Данная стойкость определяется гарантией того, что злоумышленник не сможет пройти аутентификацию, присвоив чужой идентификатор или украв его.

Парольные системы идентификации/аутентификации являются одними из основных и наиболее распространенных в СЗИ методами пользовательской

аутентификации. В данном случае информацией, аутентифицирующей пользователя, выступает некоторый секретный пароль, известный только легальному пользователю.

Парольная аутентификация пользователя, как правило, передний край обороны СЗИ. В связи с этим модуль аутентификации по паролю наиболее часто подвергается атакам со стороны злоумышленника. Цель последнего в данном случае – подобрать аутентифицирующую информацию (пароль) легального пользователя.

Методы парольной аутентификации пользователя наиболее просты и при несоблюдении определенных требований к выбору пароля достаточно уязвимы.

Основными минимальными требованиями к выбору пароля и к подсистеме парольной аутентификации пользователя являются следующие.

К паролю:

1) минимальная длина пароля должна быть не менее 6 символов;

2) пароль должен состоять из различных групп символов (малые и большие латинские буквы, цифры, специальные символы ‘(’, ‘)’, ‘#’ и т.д.);

3) в качестве пароля не должны использоваться реальные слова, имена, фамилии и т.д.

К подсистеме парольной аутентификации:

1) администратор СЗИ должен устанавливать максимальный срок действия пароля, после чего пароль следует сменить;

2) в подсистеме парольной аутентификации необходимо установить ограничение числа попыток ввода пароля (как правило, не более трёх);

3) в подсистеме парольной аутентификации требуется установить временную задержку в случае ввода неправильного пароля.

Как правило, для генерирования паролей в СЗИ, удовлетворяющих перечисленным требованиям к паролям, используются программы – автоматические генераторы паролей пользователей.

При выполнении перечисленных требований к паролям и к подсистеме парольной аутентификации единственно возможным методом взлома данной подсистемы злоумышленником является прямой перебор паролей (brute forcing). В данном случае оценка стойкости парольной защиты осуществляется следующим образом.

Количественная оценка стойкости парольной защиты

Пусть A – мощность алфавита паролей (количество символов, которые могут быть использованы при составлении пароля: если пароль состоит только из малых английских букв, то $A = 26$), L – длина пароля, $S = A^L$ – число всевозможных паролей длины L, которые можно составить из символов алфавита A, V – скорость перебора паролей злоумышленником, T – максимальный срок действия пароля.

Тогда вероятность P подбора пароля злоумышленником в течение срока его действия V определяется по формуле

$$P = (V \cdot T) / S = (V \cdot T) / A^L.$$

Эту формулу можно использовать в обратную сторону для решения следующей задачи.

Задача. Определить минимальные мощность алфавита паролей A и длину паролей L, обеспечивающих вероятность подбора пароля злоумышленником не более заданной P, при скорости подбора паролей V, максимальном сроке действия пароля T.

Данная задача имеет неоднозначное решение. При исходных данных V, T, P однозначно можно определить лишь нижнюю границу S^* числа всевозможных паролей. Целочисленное значение нижней границы вычисляется по формуле

$$S^* = [V \cdot P / T], \quad (1)$$

где [] – целая часть числа, взятая с округлением вверх.

После определения нижней границы S^* необходимо выбрать такие A и L для формирования $S = A^L$, чтобы выполнялось следующее неравенство:

$$S^* \leq S = A^L. \quad (2)$$

При выборе S, удовлетворяющего неравенству (2), вероятность подбора пароля злоумышленника (при заданных V и T) будет меньше, чем заданная P.

Следует отметить, что при осуществлении вычислений по формулам (1) и (2) величины должны быть приведены к одним размерностям.

Пример. Исходные данные: $P = 10^{-6}$, T = 7 дней = 1 неделя, V = 10 (паролей / минуту) = 10 · 60·24·7 = 100800 паролей в неделю. Тогда, $S^* = [(10800 \cdot 1) / 10^{-6}] = = 108 \cdot 10^8$.

Условию $S^* \le A^L$ удовлетворяют, например, такие комбинации A и L, как A = 26, L = 8 (пароль состоит из восьми малых символов английского алфавита), A = 36, L = 6 (пароль состоит из шести символов, среди которых могут быть малые латинские буквы и произвольные цифры).

Задание на лабораторную работу

1. В табл.2.5 найти для указанного варианта значения характеристик P, V, T.

2. Вычислить по формуле (1) нижнюю границу S^* для заданныхP, V, T.

3. Выбрать некоторый алфавит с мощностью A и получить минимальную длину пароля L, при котором выполняется условие (2).

4. Реализовать программу для генерации паролей пользователей. Программа должна формировать случайную последовательность символов длины L, при этом должен использоваться алфавит из A символов.

5. Оформить отчет по лабораторной работе.

Коды символов:

1. Коды английских символов :«A» = 65, …, «Z» = 90, «a» = 97,…, «z» = 122.

2. Коды цифр :«0» = 48, «9» = 57.

3. «!» = 33, «“« = 34, «#» = 35, «$» = 36, «%» = 37, «&» = 38, «‘« = 39.

4. Коды русских символов :«А» – 128, … «Я» – 159, «а» – 160,…, «п» – 175, «р» – 224,…, «я» – 239.

Таблица 2.5. Варианты заданий

Вариант	P	V	T
1	10^{-4}	15 паролей/мин	2 недели
2	10^{-5}	3 паролей/мин	10 дней
3	10^{-6}	10 паролей/мин	5 дней
4	10^{-7}	11 паролей/мин	6 дней
5	10^{-4}	100 паролей/день	12 дней
6	10^{-5}	10 паролей/день	1 месяц
7	10^{-6}	20 паролей/мин	3 недели
8	10^{-7}	15 паролей/мин	20 дней
9	10^{-4}	3 паролей/мин	15 дней
10	10^{-5}	10 паролей/мин	1 неделя
11	10^{-6}	11 паролей/мин	2 недели
12	10^{-7}	100 паролей/день	10 дней
13	10^{-4}	10 паролей/день	5 дней
14	10^{-5}	20 паролей/мин	6 дней
15	10^{-6}	15 паролей/мин	12 дней
16	10^{-7}	3 паролей/мин	1 месяц
17	10^{-4}	10 паролей/мин	3 недели
18	10^{-5}	11 паролей/мин	20 дней
19	10^{-6}	100 паролей/день	15 дней
20	10^{-7}	10 паролей/день	1 неделя
21	10^{-4}	20 паролей/мин	2 недели
22	10^{-5}	15 паролей/мин	10 дней

23	10^{-6}	3 паролей/мин	5 дней
24	10^{-7}	10 паролей/мин	6 дней
25	10^{-4}	11 паролей/мин	12 дней
26	10^{-5}	100 паролей/день	1 месяц
27	10^{-6}	10 паролей/день	3 недели
28	10^{-7}	20 паролей/мин	20 дней
29	10^{-4}	15 паролей/мин	15 дней
30	10^{-5}	3 паролей/мин	1 неделя

Контрольные вопросы

1. Чем определяется стойкость подсистемы идентификации и аутентификации?
2. Перечислить минимальные требования к выбору пароля.
3. Перечислить минимальные требования к подсистеме парольной аутентификации.
4. Как определить вероятность подбора пароля злоумышленником в течение срока его действия?
5. Выбором каких параметров можно повлиять на уменьшение вероятности подбора пароля злоумышленником при заданной скорости подбора пароля злоумышленником и заданном сроке действия пароля?

Лабораторная работа №6

Асимметричные алгоритмы шифрования данных

Цель работы: освоить методику работы асимметричных алгоритмов шифрования, где существует два ключа – один для шифрования, другой для дешифрования.

Теоретические сведения

Алгоритм RSA разработан в 1977 г. Роном Ривестом, Ади Шамиром и Леном Адлеманом и опубликован в 1978 г. С тех пор алгоритм Rivest-Shamir-Adleman (RSA) широко применяется практически во всех приложениях, использующих криптографию с открытым ключом.

Алгоритм RSA:

1. Вычисление ключей

Важным моментом в этом криптоалгоритме является создание пары ключей: открытого и закрытого. Для алгоритма RSA этап создания ключей состоит из следующих операций:

1.1. Выбираются два простых различных числа p и q. Вычисляется их произведение $n = p \cdot q$, называемое модулем. Под простым числом будем понимать такое число, которое делится только на 1 и на само себя. Взаимно простыми числами будем называть такие числа, которые не имеют ни одного общего делителя, кроме единицы.

1.2. Вычисляется функция Эйлера $\Phi(n) = (p - 1) \cdot (q - 1)$.

1.3. Выбирается произвольное число e ($e<n$), такое, что $1 < e < \Phi(n)$ и не имеет общих делителей, кроме 1 (взаимно простое) с числом $(p - 1) \cdot (q - 1)$.

1.4. Вычисляется d методом Евклида таким образом, что $(e \cdot d - 1)$ делится на $(p - 1) \cdot (q - 1)$.

1.5. Два числа (e, n) публикуются как открытый ключ.

1.6. Число d хранится в секрете – закрытый ключ есть пара (d, n), который позволит читать все послания, зашифрованные с помощью пары чисел (e, n).

2. Шифрование

Шифрование с помощью пары чисел производится следующим образом:

2.1. Отправитель разбивает своё сообщение M на блоки m_i. Значение $m_i < n$, поэтому длина блока m_i в битах не больше $k = [\log_2(n)]$ бит, где квадратные скобки обозначают взятие целой части от дробного числа.

Например, если $n = 21$, то максимальная длина блока $k = [\log_2(21)] = [4.39\ldots] = = 4$ бита.

2.2. Подобный блок может быть интерпретирован как число из диапазона $(0; 2^k - 1)$. Для каждого такого числа m_i вычисляется выражение (c_i – зашифрованное сообщение): $c_i = ((m_i)^e) \bmod n$.

Необходимо добавлять нулевые биты слева в двоичное представление блока c_i до размера $k = [\log_2(n)]$ бит.

3. Дешифрование

Чтобы получить открытый текст, необходимо каждый блок дешифровать отдельно: $m_i = ((c_i)^d) \bmod n$.

Пример

Выбрать два простых числа: $p = 7$, $q = 17$. Вычислить $n = p \cdot q = 7 \cdot 17 = 119$. Вычислить $\Phi(n) = (p - 1) \cdot (q - 1) = 96$.

Выбрать e так, чтобы e было взаимно простым с $\Phi(n) = 96$ и меньше, чем $\Phi(n)$: $e = 5$.

Определить d так, чтобы $d \cdot e \equiv 1 \bmod 96$ и $d < 96$, $d = 77$, так как

$77 \cdot 5 = 385 = 4 \cdot 96 + 1$.

Результирующие ключи открытый {5, 119} и закрытый ключ {77, 119}.

Например, требуется зашифровать сообщение $M = 19$: $19^5 = 66 \pmod{119}$,

$C = = 66$. Для дешифрования вычисляется $66^{77} \pmod{119} = 19$.

Варианты заданий

1. Разработать консольное приложение для шифрования/дешифрования произвольных файлов с помощью алгоритма RSA.
2. Разработать визуальное приложение для шифрования/дешифрования изображений.
3. Разработать визуальное приложение для шифрования/дешифрования произвольных файлов.
4. Разработать клиент-серверное приложение для защищённой передачи файлов по сети.
5. Разработать клиент-серверное приложение для защищённого обмена сообщениями по сети.
6. Разработать визуальное приложение для шифрования/дешифрования чисел.
7. Разработать консольное приложение для генерации ключей.
8. Реализовать программу для шифрования / дешифрования текстов, работающую по алгоритму RSA. Программа должна уметь работать с текстом произвольной длины.

Контрольные вопросы

1. Дайте определение алгоритма с открытым ключом.
2. Сколько этапов содержит алгоритм RSA?
3. В чем заключается вычисление ключей алгоритма RSA?
4. Как происходит шифрование в алгоритме RSA?
5. Как происходит дешифрование в алгоритме RSA?

Лабораторная работа №7

Защита от копирования. Привязка к аппаратному обеспечению. Использование реестра

***Цель работы*:** ознакомиться с возможностями «привязки» к характеристикам компьютера.

Теоретические сведения

В качестве анализируемых характеристик компьютера могут использоваться следующие:

1. Информация об используемой операционной системе.
2. Имя пользователя.
3. Имя компьютера.
4. Наличие звуковой карты.
5. Наличие подключенных принтера, сканера и т.д.
6. Дата создания BIOS.
7. Серийный номер диска.
8. Характеристики процессора.

Для получения подобных характеристик в операционной системе Windows используются API-функции и информация из реестра.

API-функции

API сокращенно Application Programming Interface (интерфейс прикладного программирования). API – набор функций, которые операционная система предоставляет программисту. API обеспечивает относительно простой путь для программистов для использования полных функциональных возможностей аппаратных средств или операционной системы.

32-разрядные версии Windows обычно используют один и тот же набор функций API, хотя имеются некоторые различия между платформами.

Почти все функции, которые составляют Windows API, находятся внутри DLL (Dynamic Link Library). Эти dll-файлы находятся в системной папке Windows. Существует свыше 1000 функций API, которые условно делятся на четыре основные категории:

1) работа с приложениями – запуск и закрытие приложений, обработка команд меню, перемещения и изменения размера окон;

2) графика – создание изображений;

3) системная информация – определение текущего диска, объема памяти, имя текущего пользователя и т.д.

4) работа с реестром – манипуляции с реестром Windows.

Реестр Windows

Реестр – база данных операционной системы, содержащая конфигурационные сведения. По замыслу Microsoft реестр должен был полностью заменить файлы ini, которые были оставлены только для совместимости со старыми программами, ориентированными на более ранние версии операционной системы.

Переход от ini файлов к реестру произошел по той причине, что на эти файлы накладывается ряд серьезных ограничений, и главное из них состоит в том, что предельный размер такого файла составляет 64 Кб.

Предупреждение: никогда не удаляйте или не меняйте информацию в реестре, если Вы не уверены, что это именно то, что нужно. В противном случае некорректное изменение данных может привести к сбоям в работе Windows и, в лучшем случае, информацию придется восстанавливать из резервной копии.

Реестр имеет следующую структуру:

1) HKEY_CLASSES_ROOT. В этом разделе содержится информация о зарегистрированных в Windows типах файлов, что позволяет открывать их по двойному щелчку мыши, а также информация для OLE и операций drag-and-drop;

2) HKEY_CURRENT_USER. Здесь содержатся настройки оболочки пользователя (например, Рабочего стола, меню «Пуск», ...), вошедшего в Windows. Они дублируют содержимое подраздела HKEY_USER\name, где name – имя пользователя, вошедшего в Windows. Если на компьютере работает один пользователь и используется обычный вход в Windows, то значения раздела берутся из подраздела HKEY_USERS\.DEFAULT;

3) HKEY_LOCAL_MACHINE. Этот раздел содержит информацию, относящуюся к компьютеру: драйверы, установленное программное обеспечение и его настройки;

4) HKEY_USERS. Содержит настройки оболочки Windows для всех пользователей. Как было сказано выше, именно из этого раздела информация копируется в раздел

HKEY_CURRENT_USER. Все изменения в HKCU (сокращенное название раздела HKEY_CURRENT_USER) автоматически переносятся в HKU;

5) HKEY_CURRENT_CONFIG. В этом разделе содержится информация о конфигурации устройств Plug&Play и сведения о конфигурации компьютера с переменным составом аппаратных средств;

6) HKEY_DYN_DATA. Здесь хранятся динамические данные о состоянии различных устройств, установленных на компьютере пользователя. Именно сведения этой ветви отображаются в окне «Свойства: Система» на вкладке «Устройства», вызываемого из Панели управления. Данные этого раздела изменяются самой операционной системой, так что редактировать что-либо вручную не рекомендуется.

Примеры процедур и функций, определяющих параметры компьютера

Определение версии операционной системы

```
BOOL DisplaySystemVersion()
{
OSVERSIONINFOEXosvi;
BOOLbOsVersionInfoEx;
ZeroMemory(&osvi, sizeof(OSVERSIONINFOEX));
osvi.dwOSVersionInfoSize = sizeof(OSVERSIONINFOEX);
if( !(bOsVersionInfoEx = GetVersionEx ((OSVERSIONINFO *) &osvi)) )
{
osvi.dwOSVersionInfoSize = sizeof (OSVERSIONINFO);
if (! GetVersionEx ( (OSVERSIONINFO *) &osvi) )
returnFALSE;
}

switch (osvi.dwPlatformId)
{
      case VER_PLATFORM_WIN32_NT:
         if ( osvi.dwMajorVersion <= 4 )
            printf(«Microsoft Windows NT «);
         if ( osvi.dwMajorVersion == 5 && osvi.dwMinorVersion == 0 )
            printf («Microsoft Windows 2000 «);
         if( bOsVersionInfoEx )
         {
            if ( osvi.wProductType == VER_NT_WORKSTATION )
            {
               if ( osvi.dwMajorVersion == 5 && osvi.dwMinorVersion == 1
)
                  printf («Microsoft Windows XP «);

               if( osvi.wSuiteMask & VER_SUITE_PERSONAL )
                  printf ( «Home Edition « );
               else
                  printf ( «Professional « );
            }
            else if ( osvi.wProductType == VER_NT_SERVER )
            {
               if ( osvi.dwMajorVersion == 5 && osvi.dwMinorVersion == 2
)
                  printf («Microsoft Windows .NET «);

               if( osvi.wSuiteMask & VER_SUITE_DATACENTER )
                  printf ( «DataCenter Server « );
               else if( osvi.wSuiteMask & VER_SUITE_ENTERPRISE )
                  if( osvi.dwMajorVersion == 4 )
                     printf («Advanced Server « );
                  else
                     printf ( «Enterprise Server « );
               else if ( osvi.wSuiteMask == VER_SUITE_BLADE )
                  printf ( «Web Server « );
               else
```

```
                        printf ( «Server « );
                    }
                }
                else
                {
                    HKEY hKey;
                    char szProductType[BUFSIZE];
                    DWORD dwBufLen=BUFSIZE;
                    LONG lRet;
                    lRet = RegOpenKeyEx( HKEY_LOCAL_MACHINE,
    «SYSTEM\\CurrentControlSet\\Control\\ProductOptions»,
                       0, KEY_QUERY_VALUE, &hKey );
                    if( lRet != ERROR_SUCCESS )
                        return FALSE;
                    lRet = RegQueryValueEx( hKey, «ProductType», NULL, NULL,
                       (LPBYTE) szProductType, &dwBufLen);
                    if( (lRet != ERROR_SUCCESS) || (dwBufLen > BUFSIZE) )
                        return FALSE;
                    RegCloseKey( hKey );
                    if ( lstrcmpi( «WINNT», szProductType) == 0 )
                       printf( «Professional « );
                    if ( lstrcmpi( «LANMANNT», szProductType) == 0 )
                       printf( «Server « );
                    if ( lstrcmpi( «SERVERNT», szProductType) == 0 )
                       printf( «Advanced Server « );
                }
                if ( osvi.dwMajorVersion <= 4 )
                {
                    printf («version %d.%d %s (Build %d)\n»,
                       osvi.dwMajorVersion,
                       osvi.dwMinorVersion,
                       osvi.szCSDVersion,
                       osvi.dwBuildNumber & 0xFFFF);
                }
                else
                {
                    printf («%s (Build %d)\n»,
                       osvi.szCSDVersion,
                       osvi.dwBuildNumber & 0xFFFF);
                }
                break;
            case VER_PLATFORM_WIN32_WINDOWS:
                if (osvi.dwMajorVersion == 4 && osvi.dwMinorVersion == 0)
                {
                    printf («Microsoft Windows 95 «);
                    if ( osvi.szCSDVersion[1] == 'C' || osvi.szCSDVersion[1] ==
'B' )
                       printf(«OSR2 « );
                }
                if (osvi.dwMajorVersion == 4 && osvi.dwMinorVersion == 10)
                {
                    printf («Microsoft Windows 98 «);
                    if ( osvi.szCSDVersion[1] == 'A' )
                       printf(«SE « );
                }
                if (osvi.dwMajorVersion == 4 && osvi.dwMinorVersion == 90)
                {
                    printf («Microsoft Windows Millennium Edition «);
    }
    break;
       }
       return TRUE;
    }
```

Определение серийного номера раздела диска

```
TCHARszVolName[256];
DWORDdwNum;
DWORDdwMaxComSize;
DWORDdwFlags;
TCHARszFS[256];
BOOLbRes;
bRes = GetVolumeInformation ( «c:\\», szVolName, sizeof(szVolName),
&dwNum, &dwMaxComSize, &dwFlags, szFS, sizeof(szFS));
```

Определение имени компьютера

```
constintWSVer = 0x101;
WSADATAwsaData;
charBuf[128];
if (WSAStartup(WSVer, &wsaData) == 0)
{
gethostname(&Buf[0], 128);
MessageBox(0, Buf,0,0);
WSACleanup;
}
```

Определение имени пользователя

```
charbuffer[UNLEN+1];
DWORD size;
size=sizeof(buffer);
GetUserName(buffer,&size);
```

Определениеверсии BIOS

```
LPSTR GetSystemBiosVersion()
{
  HKEY hKey;
  LONG Res1, Res2;
  DWORD cData=255;
  TCHAR SystemBiosVersion[255]={'\0'};

Res1=RegOpenKeyEx(HKEY_LOCAL_MACHINE,»HARDWARE\\DESCRIPTION\\System»,NULL,
KEY_QUERY_VALUE, &hKey);
   if(Res1==ERROR_SUCCESS)
     {

  Res2=RegQueryValueEx(hKey,»SystemBiosVersion»,NULL,NULL,…
     (LPBYTE)SystemBiosVersion,&cData);
      if(Res2==ERROR_SUCCESS)
        {
          for (const char* p = SystemBiosVersion; *p; p += strlen(p)+1)
            {
              printf(«%s\n», p);
            }

        return SystemBiosVersion;
        }
     else
       {
           MessageBox(NULL,»RegQueryValueEx:
SystemBiosVesion»,»ERROR»,MB_OK);
           return NULL;
       }
     }
  else
     {
      MessageBox(NULL,»RegOpenKeyEx: SystemBiosVersion»,»ERROR»,MB_OK);
return NULL;
     }
  RegCloseKey(hKey);
}
```

Определение частоты процессора (способ №1)

```
doubleCPUSpeed(void)
  {
DWORDdwTimerHi, dwTimerLo;
asm
     {
DW 0x310F
movdwTimerLo, EAX
movdwTimerHi, EDX
}
Sleep (500);
asm
     {
DW 0x310F
subEAX, dwTimerLo
subEDX, dwTimerHi
movdwTimerLo, EAX
movdwTimerHi, EDX
}
returndwTimerLo/(1000.0*500);
  }
```

Задание на лабораторную работу

Разработать программу, реализующую привязку к компьютеру, используя совокупность характеристик согласно варианту задания (табл.2.6). Добиться того, чтобы программа не запускалась на другом компьютере**.**

Таблица 2.6. Варианты заданий

№ варианта	Характеристики
1	Серийный номер раздела жесткого диска, MAC-адрес сетевой карты
2	Информация из реестра, тактовая частота процессора
3	Версия операционной системы, MAC-адрес сетевой карты
4	Имя пользователя, серийный номер раздела жесткого диска
5	Название компьютера, информация из реестра
6	Версия БИОС, имя пользователя
7	Серийный номер раздела жесткого диска, имя пользователя
8	Имя пользователя, тактовая частота процессора
9	MAC-адрес сетевой карты, тактовая частота процессора

Контрольные вопросы

1. Что понимается под «привязкой» к компьютеру?
2. Какие характеристики обычно используются для идентификации компьютера?
3. Перечислите основные API-функции для определения индивидуальных характеристик компьютера.
4. Что представляет собой реестр Windows?
5. Какую структуру имеет реестр?

Лабораторная работа №8

Защита баз данных на примере MS ACCESS

Цель: изучение способов защиты информации в БД на примере СУБД MS Access.

Теоретическая часть

Защита баз данных

Система безопасности БД должна обеспечивать физическую целостность БД и защиту от несанкционированного вторжения с целью чтения содержимого и изменения данных.

Защита БД производится на двух уровнях:

- на уровне пароля;
- на уровне пользователя (защита учетных записей пользователей и идентифицированных объектов).

Для защиты БД Access использует файл рабочих групп system.mdw (рабочая группа - это группа пользователей, которые совместно используют ресурсы сети), к которому БД на рабочих станциях подключаются по умолчанию. Файл рабочих групп содержит учётные записи пользователей и групп, а также пароли пользователей. Учётным записям могут быть предоставлены права на доступ к БД и её объектам, при этом сами разрешения на доступ хранятся в БД.

Для обеспечения защиты БД Access необходимо создать рабочую группу, используя файл - администратор рабочих групп wrkgadm.exe. При создании уникальной рабочей группы задается имя пользователя, название организации и код рабочей группы. Файл рабочей группы MS Access содержит следующие встроенные учётные записи:

1. Admins - стандартная учётная запись пользователя. Данные записи одинаковы для всех экземпляров Ms Access.
2. Admin - учётная запись группы администратора - является уникальной в каждом файле рабочей группы.
3. Users - содержит учётные записи пользователей.

Для создания файла рабочих групп необходимо выйти из Access и в папке system или system32 в каталоге windows найти файл рабочей группы и создать новую рабочую группу (может быть до 20 цифровых или буквенных обозначений).

Группа Admins может содержать произвольное число пользователей, но владелец объекта всегда один (владельцем объекта может быть учётная запись, которая создавала объект или которой были переданы права на его использование). Так как чтение записи Admin возможно для всех рабочих групп и данные учётные записи являются одинаковыми, то пользователя ADMIN необходимо удалить из группы администраторов, для чего следует создать новую учётную запись администратора и задать пароль на его учётные записи и на учетные записи владельца.

Разграничение прав доступа пользователей

Разрешения к доступу называются явными, если они принадлежат или присвоены учётной записи пользователя. Разрешения будут неявными, если они присвоены учётной записи группы, при этом пользователь, включённый в группу получает все её разрешения. ТИПЫ РАЗРЕШЕНИЙ НА ДОСТУП К БД (табл.2.7).

Таблица 2.7. Разграничение прав

Разрешения	Разрешенные действия	Объекты БД
Открытие и запуск	Открытие БД, формы или отчета	БД, формы, отчеты, макросы
Монопольный доступ	Монопольное открытие БД	БД
Чтение макета	Просмотр объектов в режиме конструктора	Таблицы запросы, формы, отчеты, макросы и модули
Изменение макетов	Просмотр и изменение макетов, удаление	Таблицы, запросы, формы, отчеты, макросы и модули
Разрешения администратора	Установка пароля в БД	Предоставление прав доступа другим пользователям
Чтение данных	Просмотр данных	Таблицы и запросы
Обновление данных	Просмотр и изменение данных без удаления и вставки	Таблицы и запросы
Вставка данных	Просмотр и вставка данных без удаления и изменения	Таблицы, запросы
Удаление	Просмотр	Таблицы

Полномочия пользователя определяются по минимальным разрешениям доступа. Изменить разрешения для пользователей могут члены группы Admins, владелец объекта и пользователь, получивший на этот объект разрешения администратора. При подключении к БД пользователи получают права групп, которым они принадлежат.

Задание

1. Создать новую базу данных и создать в ней следующие объекты:

- таблицу Заказы;
- запрос Сведения о заказах;
- форму Заказы клиентов.

Заполнить таблицу несколькими записями.

2. Определить два уровня доступа к БД:

- на уровне пароля;
- на уровне пользователя (защита учетных записей пользователей и идентифицированных объектов).

Защита на уровне пароля

Для установки пароля нам понадобится открыть базу в так называемом монопольном, однопользовательском режиме. Дело в том, что возможность установки пароля при одновременной работе нескольких пользователей приводила бы к ошибкам, поэтому MS Access не предоставляет ее. Запускаем программу, в главном меню переходим «Файл \ Открыть», переходим в нужную директорию, выделяем файл, из выпадающего списка значений кнопки «Открыть» выбираем «Монопольно» (рис.2.29).

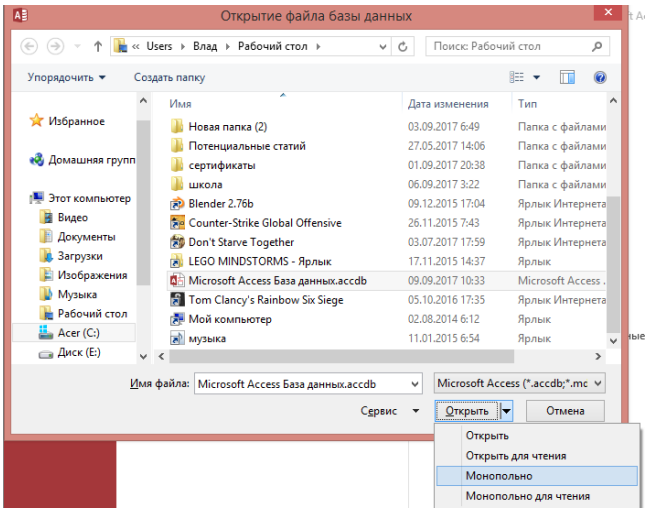

Рис.2.29. Монопольно

Появляется окно базы данных. В главном меню переходим «Сервис \ Защита \ Задать пароль базы данных», в окне «Задание пароля базы данных» вводим пароль «12345» и подтверждаем его (рис.2.30).

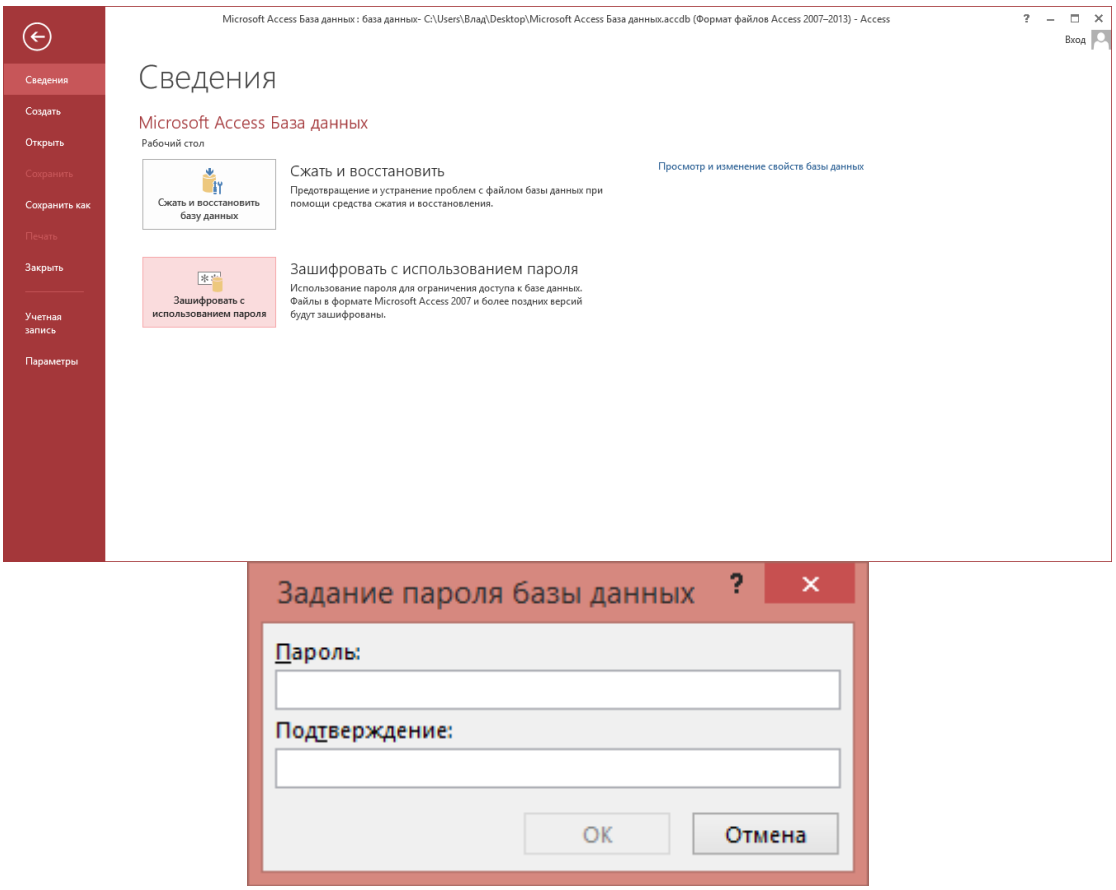

Рис.2.30. Задание пароля

Теперь всякий раз при открытии этого файла на любом компьютере нужно будет вводить указанный пароль. Для изменения пароля нам потребуется удалить существующий и затем задать новый. Снова открываем базу в монопольном режиме, в главном меню переходим «Сервис \ Защита \ Удалить пароль базы данных». В появившемся окне вводим текущий пароль, после нажатия кнопки «OK» он будет удален. Для ввода нового значения опять переходим к пункту меню «Задать пароль базы данных», на этот раз введем более сложный пароль «q1w2e3r4t5y6u7i8o9p0». Рекомендации по выбору пароля:

- не желательно в качестве пароля использовать такие данные, как ваше имя, дата рождения и т.д.;

- не стоит выбирать короткий пароль, так как он может быть подобран при помощи специальных программ за достаточно короткое время;

- не желательна комбинация букв и цифр, так как это затрудняет подбор пароля и делает бесполезной атаку по словарю.

Защита на уровне пользователя

1. Защита с помощью мастера

Microsoft Access предоставляет средства распределенного доступа к базе данных. С одним файлом могут одновременно работать большое количество пользователей, обладающих разными правами: одни могут только просматривать таблицы, другие - только вносить новые данные, и лишь администраторы базы обладают полным доступом. Когда мы устанавливаем пакет Microsoft Office на локальный компьютер и, ни о чем не задумываясь, начинаем создавать свою базу в программе Access, мы по умолчанию выступаем в роли администратора. Поставим теперь задачу: разделить доступ для двух пользователей - один сможет только просматривать данные (читать), другой по-прежнему будет обладать полным доступом. Скопируйте созданный вами файл и переименуйте его как «BDwithUsers.mdb». Открываем базу, в главном меню программы переходим «Сервис

\ Защита \ Мастер». Появляется мастер защиты, в первом шаге которого доступен единственный переключатель «Создать файл рабочей группы» (рис.2.31).

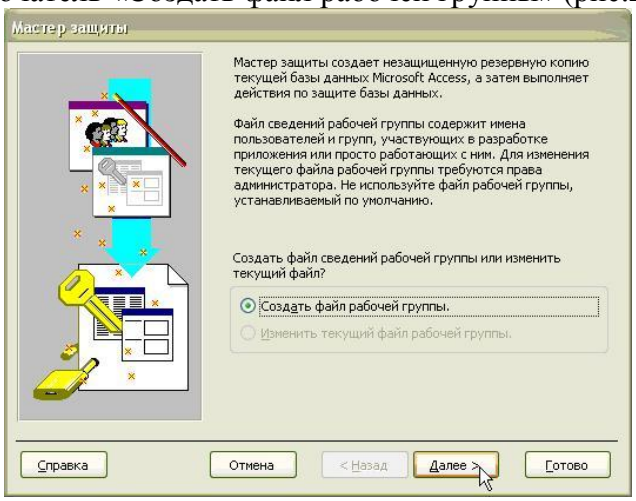

Рис.2.31. Первый шаг мастера защиты

Файл рабочей группы представляет собой своеобразный электронный ключ, в котором будут храниться созданные настройки. Он имеет расширение *.mdw. В следующем шаге мастера нажимаем кнопку «Обзор» - по умолчанию мы оказываемся в той же директории, где расположен исходный файл базы данных BDwithUsers.mdb, вводим название создаваемого файла BDWorkFile.mdw. Нажимаем кнопку «Выбрать», возвращаясь в окно мастера. Устанавливаем переключатель на значение «Использовать файл рабочей группы по умолчанию». На другие параметры - «Код рабочей группы», «Ваше имя», «Организация» - можно не обращать внимания. Нажимаем кнопку «Далее» (рис.2.32).

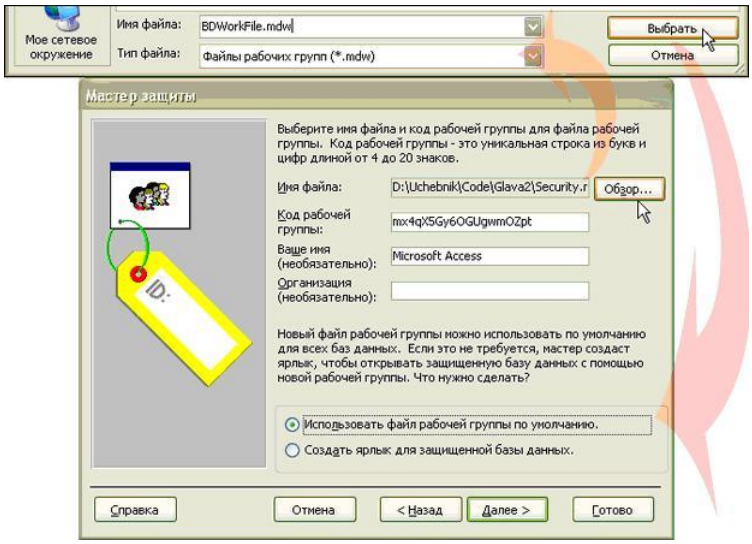

Рис.2.32. Определение файла рабочей группы BDWorkFile.mdw

Теперь предстоит определить, какие объекты базы данных защищены. Оставляем все таблицы и нажимаем кнопку «Далее» (рис.2.33).

Рис.2.33. Определение объектов базы данных, которые будут защищены

Мы добрались до самих рабочих групп. Программа Microsoft Access предлагает несколько рабочих групп, в каждой из которых может быть большое число пользователей. К примеру, пять пользователей могут обладать полными правами, десять - быть разработчиками проекта и еще пять - обладать правами на обновление данных. Код группы также можно не запоминать. Мы выбираем группу «Только чтение», отмечая ее галочкой, нажимаем кнопку «Далее» (рис.2.34).

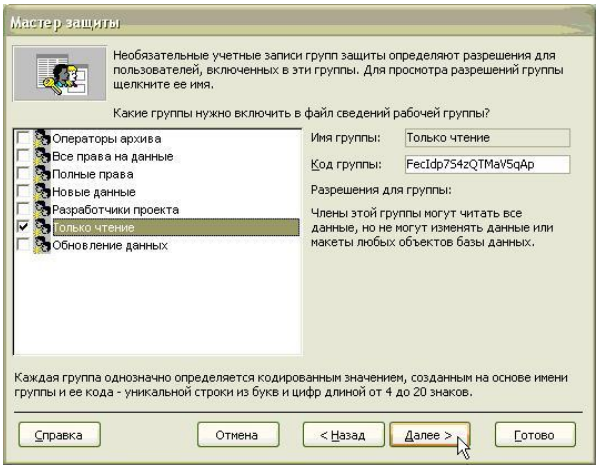

Рис.2.34. Выбор рабочей группы

Теперь требуется определить права группы Users. Это группа в любом случае будет входить в файл BDWorkFile.mdw; по умолчанию пользователи, входящие в нее, могут работать с базой данных без всякого пароля. Предоставление каких-либо прав этой группе означает предоставление этих же прав любому пользователю. Поэтому из соображений безопасности Microsoft Access предлагает вариант по умолчанию. Изменение этого варианта означает встраивание «черного» входа в файл рабочей группы. Мы оставляем предложенное значение и нажимаем кнопку «Далее» (рис.2.35).

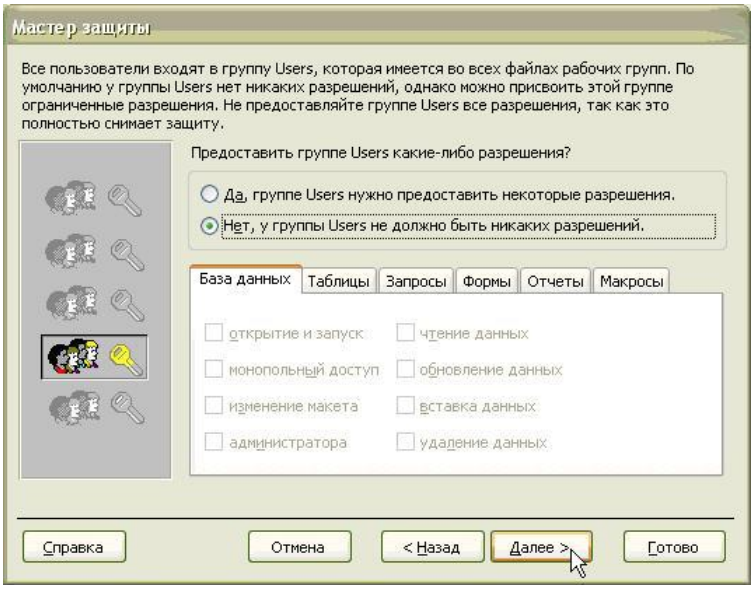

Рис.2.35. Определение разрешений группы Users

В следующем шаге мастера следует определить пользователей и пароли. Именно эти сведения для каждого пользователя будут постоянно использоваться в работе с приложением, поэтому на них следует обратить внимание. В поле «Пользователь:» вводим «Adonetuser», задаем этому пользователю пароль «12345», нажимаем кнопку «Добавить пользователя в список». Поля «Пользователь» и «Пароль» очищаются, а в списке, расположенном в левой части формы, появляется новая запись. Нажимаем кнопку «Далее» (рис.2.36).

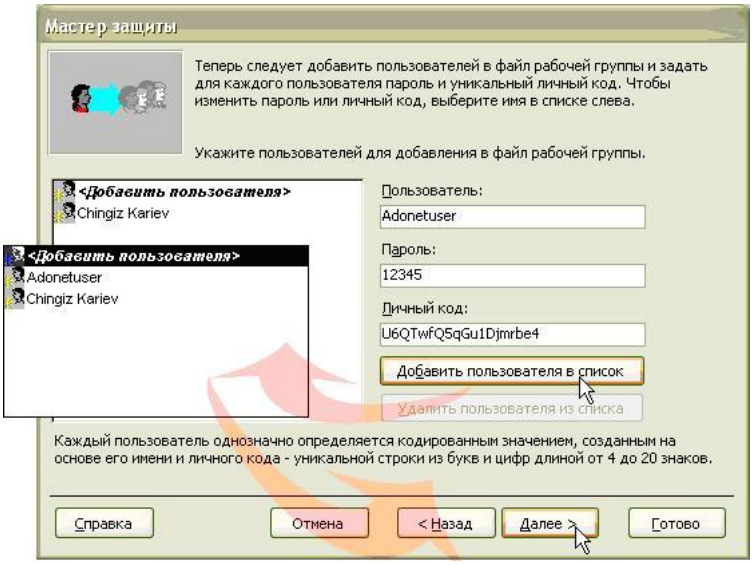

Рис.2.36. Добавление пользователя «Adonetuser»

Итак, теперь у нас уже есть рабочая группа - «Только чтение», и теперь появился пользователь «Adonetuser». Из выпадающего списка «Группа или пользователь» следует выбрать «Adonetuser» и отметить галочкой группу «Только чтение». При выборе второго пользователя из выпадающего списка - здесь «Chingiz Kariev», - можно заметить, что он входит в группу Admins (рис.2.37). Это очень важный момент: должен быть хотя бы один пользователь-администратор, входящий в эту группу, в противном случае после завершения работы мастера мы не сможем добавлять новых пользователей и изменять права существующих!

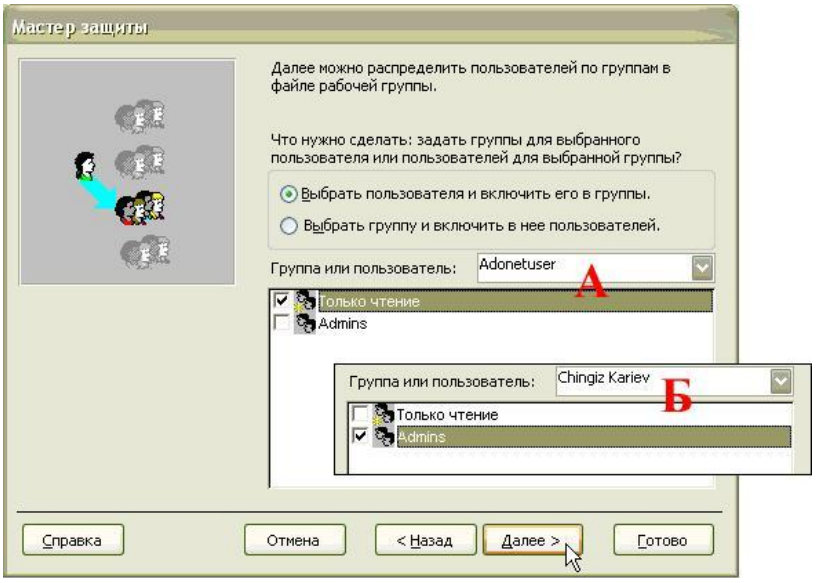

Рис.2.37. Распределение пользователей в рабочие группы: А - включение пользователя «Adonetuser» в группу «Только чтение», Б - вхождение пользователя «Chingiz Kariev» в группу «Admins» по умолчанию

В последнем шаге мастера создается резервная копия базы данных (рис.2.38). Она располагается в той же самой директории, где и основная. Несмотря на свое расширение - *.bak (backup), это, по сути, обычный файл базы данных Microsoft Access.

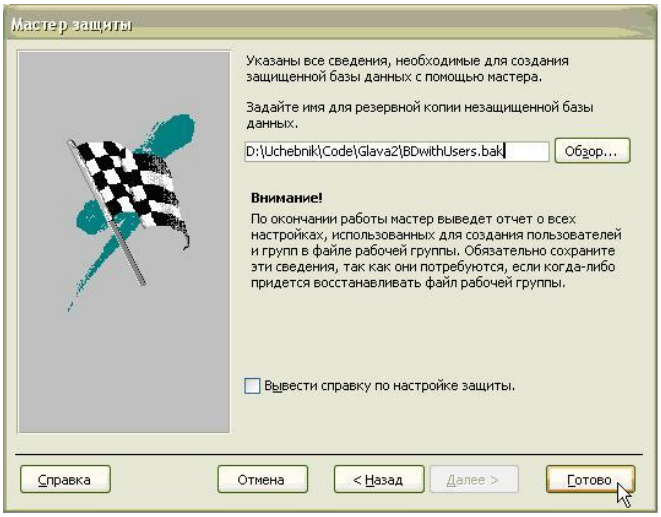

Рис.2.38. Создание резервной копии базы данных

При нажатии на кнопку «Готово» появляется отчет, создаваемый мастером защиты. Он включает в себя перечень всех сведений, которые в дальнейшем могут понадобиться для восстановления доступа к базе:

Отчет мастера защиты

Данный отчет содержит все сведения, необходимые для воссоздания файла рабочей группы и восстановления доступа к защищенной базе данных в случае повреждения.

Незащищенная база данных:

D:\Uchebnik\Code\Glava2\BDwithUsers.bak

Защищенная база данных:

D:\Uchebnik\Code\Glava2\BDwithUsers.mdb

Файл рабочей группы:

D:\Uchebnik\Code\Glava2\BDWorkFile.mdw
Пользователь:
Microsoft Access
Организация:
Код рабочей группы:
mx4qX5Gy6OGUgwmOZpt
Защищенные объекты:
Таблицы:
Информация о туристах
Оплата
Путевки
Сезоны
Туристы
Туры
<Новые таблицы и запросы>
Запросы:
<Новые таблицы и запросы>
Формы:
<Новые формы>
Отчеты:
<Новые отчеты>
Макросы:
<Новые макросы>
База данных:
Пароль VBE не установлен
Группы:
Имя: Только чтение
Кодгруппы: FecIdp7S4zQTMaV5qAp
Users:
Adonetuser
Имя: Admins
Код группы: <Созданные ранее>
Users:
Chingiz Kariev
Имя: Users
Код группы: <Созданные ранее>
Users:
ChingizKariev
Adonetuser
Пользователи:
Имя: ChingizKariev
Личныйкод: ifXdiQ2D2GaQvBhly
Пароль:
Группы:
Admins
Имя: Adonetuser
Личныйкод: U6QTwfQ5qGu1Djmrbe4
Пароль: 12345
Группы:
Только чтение
Имя: admin
Личный код: <Созданные ранее>

Пароль: S0nxw3IDds5rO

Группы:

Users

Отчет мастера защиты Дата работы г.

Желательно последовать совету мастера и сохранить эти сведения в надежном месте. Итак, в результате всех проделанных действий в рабочем каталоге появились три файла - BDwithUsers.bak, BDwithUsers.mdb и BDWorkFile.mdw (рис.2.39).

Рис.2.39. Файлы, полученные в результате работы мастера

Файл BDwithUsers.bak тоже лучше сохранить в надежном месте, поскольку он представляет собой незащищенную копию базы данных.

Запускаем файл BDWorkFile.mdw - появляется окно, в котором следует ввести имя пользователя «Adonetuser» и пароль «12345» (рис.2.40).

Рис.2.40. Аутентификация пользователя «Adonetuser»

Открывается окно базы данных, в котором имеющиеся таблицы доступны только для чтения. Выходим из приложения и запускаем его снова. Введем на этот раз имя администратора базы - «Chingiz Kariev», без пароля (рис.2.41).

Рис.2.41. Аутентификация пользователя «Chingiz Kariev»

На этот раз база данных открывается с полным доступом, более того, выбрав пункт главного меню «Сервис \ Защита \ Мастер_», можно редактировать уже существующий файл рабочей группы, добавляя, например, новых пользователей (рис.2.42).

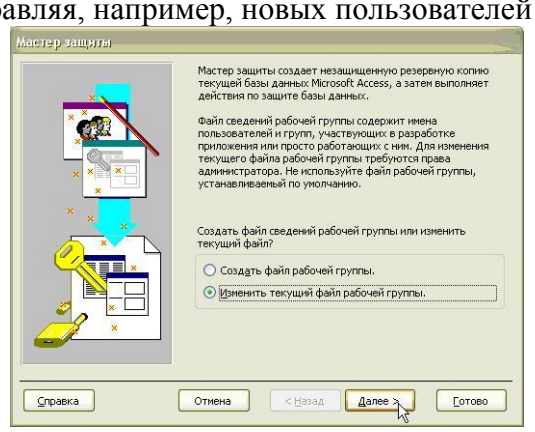

Рис.2.42. Первый шаг мастера. Изменение файла BDWorkFile.mdw рабочей группы

Примечание: При создании файла рабочей группы BDWorkFile.mdw мы определили его дальнейшее использование по умолчанию. Это означает, что вся дальнейшая работа с программой Microsoft Access на данном компьютере будет производиться от имени этого файла и определенных в нем пользователей. Без наличия соответствующих прав будет невозможно создать даже новую базу данных. Для возврата к файлу рабочей группы, принятому по умолчанию, проделываем следующие действия:

1) включаем режим отображения скрытых файлов и папок;

2) открываем базу данных BDwithUsers.mdb от имени администратора (здесь - от имени пользователя «Chingiz Kariev»);

3) в главном меню программы переходим «Сервис \ Защита \ Администратор рабочих групп» ;

4) появляется окно «Администратор рабочих групп», в котором отображается связь с текущим файлом BDWorkFile.mdw. Нажимаем кнопку «Связь» для смены рабочего файла (рис.2.43).

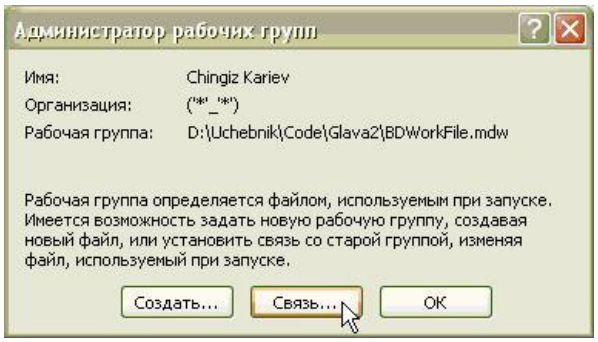

Рис.2.43. Окно «Администратор рабочих групп»

5) в появившемся окне «Файл рабочей группы» нажимаем кнопку «Обзор».

Переходим в директорию C:\Documents and Settings\ Имя пользователя (здесь - Chingiz Kariev)\Application Data\ Microsoft\Access и выбираем файл System.mdw. Это файл рабочей группы, который программа использует с момента своей установки. Нажимаем кнопку «Открыть». В окне «Файл рабочей группы» нажимаем «OK». Появляется уведомление «Успешное присоединения файла рабочей группы» (рис.2.44).

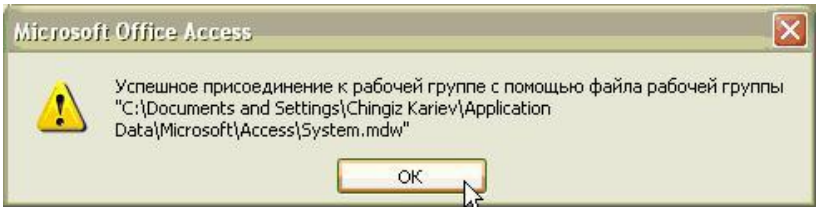

Рис.2.44. Уведомление присоединения файла рабочей группы

6) нажимаем кнопку «OK» - теперь в окне «Администратор рабочих групп» отображается связь с файлом по умолчанию «System.mdw». Нажимаем «OK» для завершения (рис.2.45).

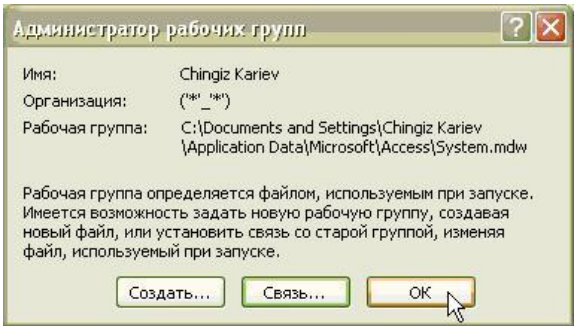

Рис.2.45. Связь с файлом System.mdw в окне «Администратор рабочих групп»

В результате проделанных операций мы вернулись к файлу рабочей группы, принятому по умолчанию. Теперь при создании новых баз данных снова будем работать от имени администратора «Admin». Однако мы не сможем открыть базу данных BDwithUsers.mdb, использующую другой файл рабочей группы (рис.2.46).

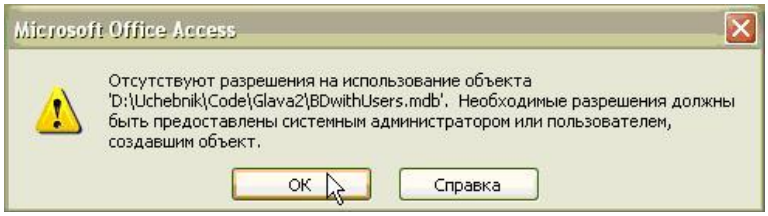

Рис.2.46. Попытка открыть базу данных BDwithUsers.mdb

Для открытия базы данных нам снова нужно будет связаться со своеобразным электронным ключом - файлом BDWorkFile.mdw. Сделайте это самостоятельно. Для распространения подготовленной базы данных на компьютеры пользователей вам потребуется скопировать сам файл базы данных и файл рабочей группы, а затем связать их.

Изменим пароль администратора «Chingiz Kariev» базы BDwithUsers.mdb. Открываем от имени этого пользователя базу данных, в главном меню переходим «Сервис \ Защита \ Пользователи и группы_». В появившемся окне «Пользователи и группы» из выпадающего списка «Имя» выбираем этого пользователя, переходим на вкладку «Изменение пароля». Оставляя пустым поле «Текущий пароль», вводим и подтверждаем пароль «a1s2d3f4g5h6j7k8l9z0» (рис.2.47).

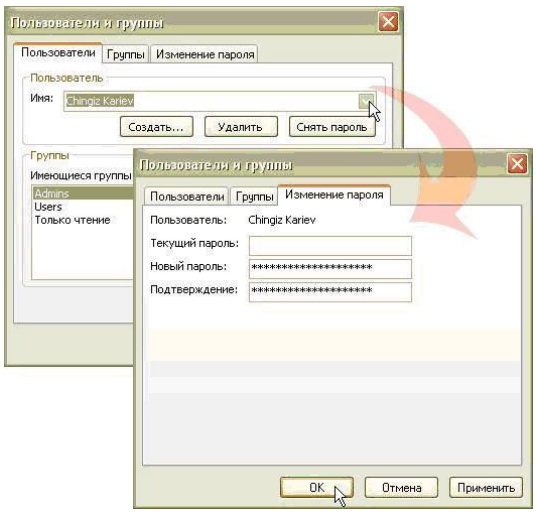

Рис.2.47. Изменение пароля администратора базы данных

Аналогично, открывая базу от имени пользователя «Adonetuser», можно изменить его пароль.

Может показаться, что вся эта продуманная система разделения пользователей предоставляет надежную безопасность создаваемым приложениям. Но это не так - вся информация по-прежнему хранятся в незашифрованном виде в файле рабочей группы. Достаточно получить к этому файлу доступ - а для работы самой базы данных это необходимое условие, - чтобы получить все сведения о пользователях и их паролях. Утилита Access Password позволяет считывать все данные (рис.2.48).

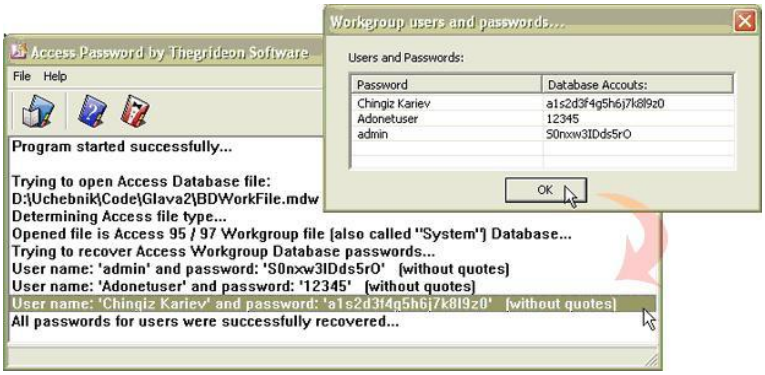

Рис.2.48. Вскрытие учетных записей пользователей MS Access

С помощью утилиты просмотрим также содержимое файла System.mdw. Здесь мы видим всего одного пользователя «admin» с пустым паролем, обладающего правами администратора (рис.2.49).

Рис.2.49. Просмотра файла System.mdw

Именно от этого пользователя по умолчанию мы начинаем работать с MS Access после установки пакета Microsoft Office.

2. Создание групп пользователей вручную

1. Создать новую уникальную рабочую группу.

2. Создать новую учетную запись администратора. Подключиться к новой рабочей группе; открыть любую БД; в меню - сервис выбрать защиту и пользователей группы; создать нового пользователя, ввести имя и код учетной записи (это не пароль); в списке имеющейся группы выбрать: Admins - добавить.

3. Удалить из группы администраторов пользователя Admin.

4. Выйти из Access и войти новым пользователем в Access; обязательно ввести пароль на данную учетную запись.

5. Создать заново БД, которую хотим защитить.

6. Выполнить импорт объектов из исходной БД в БД, созданную на предыдущем шаге.

7. Выполнить распределение прав на необходимые объекты.

8. Порядок выполнения и результаты работы Запустите БД, которую необходимо защитить. В пункте меню Сервис выберите ***Защита/Пользователи и группы*** (рис.2.50).

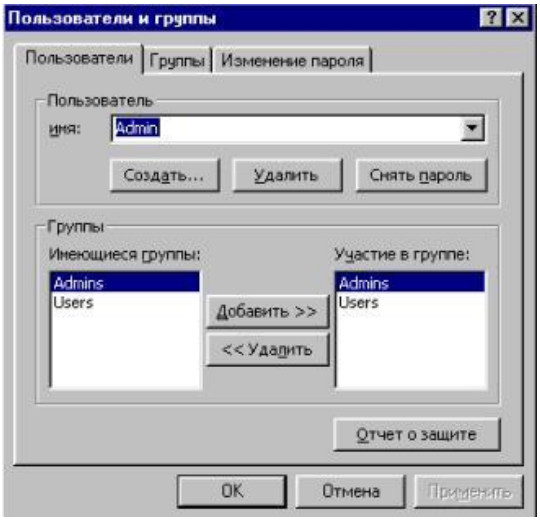

Рис.2.50. Окно свойств пользователей и групп

Нажмите кнопку Создать... и введите имя нового пользователя, например user1, укажите его код. По умолчанию запись войдет в группу Users. Повторите эти действия для всех пользователей, которые будут работать с БД.

Перейдите в вкладку Изменение пароля. Задайте пароль администратора, после чего при каждом запуске Access будет появляться окно, предлагающее ввести имя пользователя и пароль (рис.2.51).

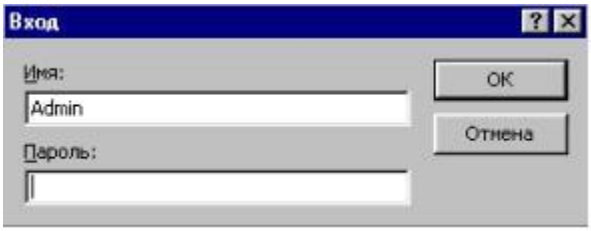

Рис.2.51. Запрос имени и пароля пользователя

В пункте меню ***Сервис*** выберите ***Защита/Разрешения***. Выберите защищаемый объект, например Таблица1. Задайте разрешения для группы *Users,* а затем и для каждого из пользователей.

Вот и все, остается каждому пользователю самому ввести свой пароль. Для этого необходимо зайти в БД под своим имением и выполнить действия как при создании пароля Администратора (рис.2.52).

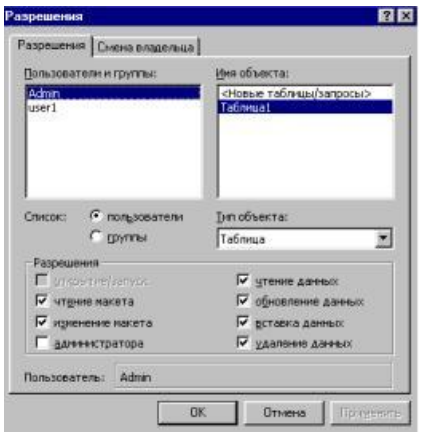

Рис.2.52. Окно определения прав доступа для каждого пользователя

Оформление отчета

Включить в отчет

номер и тема лабораторной работы;

проделанные действия;

напечатать или экспортировать отчет мастера защиты и сохранить его в надежном месте.

Контрольные вопросы

1. Способы защиты информации в БД Access.
2. Группы и пользователи БД Access . Файл рабочей группы.
3. Этапы создания рабочей группы с помощью мастера.
4. Порядок изменения пароля пользователя или группы.
5. Для чего создается связь защищенной на уровне пользователя базы данных с файлом рабочей группы (электронным ключом)?
6. К каким файлам БД относятся расширения *.mdw, *.bak, *.mdb?
7. Объекты БД Access и права доступа к объектам. Понятие владельца объекта.
8. Алгоритм защиты БД Access.

Библиографический список

1. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — М.: КноРус, 2013. — 136 с.
2. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. — Рн/Д: Феникс, 2010. — 324 с.
3. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. — Ст. Оскол: ТНТ, 2010. — 384 с.
4. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. — М.: ЮНИТИ-ДАНА, 2013. — 239 с.
5. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт. Монография. / Л.Л. Ефимова, С.А. Кочерга. — М.: ЮНИТИ, 2013. — 239 с.
6. Запечников, С.В. Информационная безопасность открытых систем: В 2 тт. Т.1. Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г Милославская. — М.: ГЛТ, 2006. — 536 с.
7. Запечников, С.В. Информационная безопасность открытых систем: В 2 тт. Т.2. Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. — М.: ГЛТ, 2008. — 558 с.
8. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. — М.: ГЛТ, 2004. — 280 с.
9. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. — М.: Форум, 2012. — 432 с.
10. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. — М.: АРТА, 2012. — 296 с.
11. Семененко, В.А. Информационная безопасность: Учебное пособие / В.А. Семененко. — М.: МГИУ, 2010. — 277 с.
12. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. — М.: Гелиос АРВ, 2010. — 336 с.
13. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. — М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. — 416 с.
14. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. — М.: ДМК, 2014. — 702 с.
15. Ярочкин, В.И. Информационная безопасность: Учебник для вузов / В.И. Ярочкин. — М.: Акад. Проект, 2008. — 544 с.
16. Ярочкин, В.И. Информационная безопасность. 5-е изд. / В.И. Ярочкин. — М.: Академический проект, 2008. — 544 с.

Учебное издание

Киргизова Елена Викторовна, Рубцов Александр Владимирович, Ахтамова Светлана Станиславовна

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебное пособие

Редактор …
Компьютерная верстка …

Пример смотреть на обороте распечатанного экземпляра