Информационная безопасность информационных систем. Курс лекций

Лекция 1
Информационная безопасность как определяющий компонент национальной безопасности России

Учебные вопросы:

1. Место информационной безопасности в системе национальной безопасности России: понятие, структура и содержание.
2. Основные руководящие документы, регламентирующие вопросы информационной безопасности.
3. Современные угрозы информационной безопасности в России

Вопрос 1. Место информационной безопасности в системе национальной безопасности России: понятие, структура и содержание

Информатизация социально-политической, экономической и военной деятельности страны и, как следствие, бурное развитие информационных систем сопровождаются существенным ростом посягательств на информацию как со стороны иностранных государств, так и со стороны преступных элементов и граждан, не имеющих доступа к ней. Несомненно, в создавшейся обстановке одной из первоочередных задач, стоящих перед правовым государством, является разрешение глубокого противоречия между реально существующим и необходимым уровнем защищенности информационных потребностей личности, общества и самого государства, обеспечение их ИБ. При этом ***под информационной безопасностью (ИБ) личности, общества, государства и современных***

автоматизированных и телекоммуникационных систем понимается *состояние защищенности информационной среды, соответствующей интересам (потребностям) личности, общества и государства в информационной сфере, при котором обеспечиваются их формирование, использование и возможности развития независимо от наличия внутренних и внешних угроз* .

Информационная безопасность определяется *способностью государства (общества, личности):*

– обеспечить с определенной вероятностью достаточные и защищенные информационные ресурсы и информационные потоки для поддержания своей жизнедеятельности и жизнеспособности, устойчивого функционирования и развития;

– противостоять информационным опасностям и угрозам, негативным информационным воздействиям на индивидуальное и общественное сознание и психику людей, а также на компьютерные сети и другие технические источники информации;

– вырабатывать личностные и групповые навыки и умения безопасного поведения;

– поддерживать постоянную готовность к адекватным мерам в информационном противоборстве, кем бы оно ни было навязано.

Ни одна сфера жизни современного общества не может функционировать без развитой информационной структуры. Национальный информационный ресурс является сегодня одним из главных источников экономической и военной мощи государства. Проникая во все сферы деятельности государства, информация приобретает конкретное политическое, материальное и стоимостное выражение. На этом фоне все более актуальный характер приобретают ***вопросы обеспечения ИБ*** Российской Федерации как неотъемлемого элемента национальной безопасности, а защита информации превращается в одну из приоритетных государственных задач.

В любой стране ИБ придается особое значение. В своем развитии эта задача проходит множество этапов в зависимости от потребностей государства, возможностей, методов и средств добывания сведений (в частности, разведки), правового режима государства и реальных его усилий по обеспечению защиты информации.

Важным этапом становления и совершенствования такой системы в нашей стране явился период 70–80-х гг. С началом 70-х гг. в разведывательной деятельности ведущих стран мира началось широкомасштабное применение технических средств разведки. 80-е гг., ознаменовавшись бурным научно-техническим прогрессом, особенно в военной области, дали новые импульсы в дальнейшем наращивании возможностей технических средств иностранных разведок: до 70 % разведывательной информации добывалось в то время с помощью технических средств.

Сложившаяся обстановка потребовала совершенствования системы мер противоборства иностранным разведкам. Задачей государственной важности и одной из составных частей в общей системе мер по сохранению государственной и служебной тайны стало противодействие техническим разведкам.

К началу 90-х гг. произошли качественные изменения в военно-политической и научно-технической сфере, заставившие во многом пересмотреть государственную политику в области защиты информации в целом.

Во-первых, информационные технологии принципиально изменили объем и важность информации, обращающейся в технических средствах ее передачи и обработки. Во-вторых, в России отошла в прошлое фактическая государственная монополия на информационные ресурсы, в частности получило конституционное закрепление право гражданина искать, получать и распространять информацию. В-третьих, прежний административный механизм управления защитой информации стал неэффективен, в то же время необходимость межведомственной координации в этой сфере объективно возросла. В-четвертых, в связи с усиливающимся включением России в международное разделение труда, укреплением экономических, культурных, гуманитарных контактов с другими государствами многие режимно-ограничительные меры, облегчающие защиту информации, например система

регионов, закрытых для посещения иностранными гражданами, стали неприемлемы.

В сложившихся условиях с учетом рассмотренных угроз ИБ личности, общества и государства важным является рассмотрение проблем и задач обеспечения ИБ являющейся неотъемлемой составной частью обеспечения национальной безопасности любого государства мирового сообщества на новом этапе своего развития – этапе формирования информационного общества. Известными характерными признаками такого общества является явная обусловленность экономического, социального, научного и всего развития страны широким внедрением новых информационных технологий, обеспечивающих эффективную информатизацию общества, которая, в свою очередь, обеспечивает информационную безопасность общества, в том числе обеспечивает его качественной информацией, информационными продуктами, услугами и знаниями, являющимися сегодня важнейшим стратегическим ресурсом страны. Информатизация личности, общества – это важнейшее, стратегическое направление деятельности государства, определяющее стабильное и безопасное социально-экономическое и политическое развитие и приоритеты во всех сферах, в том числе в информационной и видах деятельности в мировом сообществе. Подтверждением этому являются практические шаги ведущих стран мира и России, что подтверждается принятием ими ряда нормативных правовых актов и иных документов:

– 2000 г. – «Окинавская хартия глобального информационного общества» (от имени России подписана Президентом);

– 2000 г. Концепцией национальной безопасности Российской Федерации (утверждена Указом Президента, в ред. от 10.01.2000);

– 2000 г. – Федеральные целевые программы «Развитие единой образовательной информационной среды (2001–2005 годы)», «Электронная Россия»;

– 25 июля 2007 г. – программа «Стратегия развития информационного общества в России» (принята Советом Безопасности Российской Федерации);

– 2002 г. – Федеральная целевая программа «Электронная Россия на 2002–2010 годы» (утверждена Постановлением Правительства России от 28 января 2002 года № 65);

– 2007 г. «Стратегия развития информационного общества в России» (утверждена 25 июля 2007 года Советом Безопасности Российской Федерации) и другие.

Вопрос 2. Основные руководящие документы, регламентирующие вопросы информационной безопасности

Рассматривая Концепцию национальной безопасности России, утвержденную Указом Президента РФ от 17.12.97 № 1300 (в ред. от 10.01.2000), которая отражает названную «Окинавскую хартию глобального информационного общества», можно утверждать, что в ней система национальных интересов России определяется совокупностью следующих основных интересов:

личности – состоят в реальном обеспечении конституционных прав и свобод, личной безопасности, в повышении качества и уровня жизни, в физическом, духовном и интеллектуальном развитии;

– *общества* – включают в себя упрочение демократии, достижение и поддержание общественного согласия, повышение созидательной активности населения и духовное возрождение России;

– *государства* – состоят в защите конституционного строя, суверенитета и территориальной целостности России, в установлении политической, экономической и социальной стабильности, в безусловном исполнении законов и поддержании правопорядка, в развитии международного сотрудничества на основе партнерства.

Концепция определяет национальные интересы России в информационной сфере.

Национальные интересы России обусловливают необходимость сосредоточения усилий общества и государства на решении определенных задач. Такими являются:

– соблюдение конституционных прав и свобод граждан в области получения

информации и обмена ею;

– защита национальных духовных ценностей; – пропаганда национального, культурного наследия, норм морали и общественной нравственности;

– обеспечение права граждан на получение достоверной информации;

– развитие современных телекоммуникационных технологий. Планомерная деятельность государства по реализации этих задач позволит Российской Федерации стать одним из центров мирового развития в XXI в. В то же время недопустимо использование информации для манипулирования массовым сознанием. Необходима защита государственного информационного ресурса от утечки важной политической, экономической, научно-технической и военной информации.

В соответствии с данной Концепцией важнейшими ***задачами обеспечения ИБ*** являются:

– установление необходимого баланса между потребностью в свободном обмене информацией и допустимыми ограничениями ее распространения;

– совершенствование информационной структуры, ускорение развития новых информационных технологий и их широкое распространение, унификация средств поиска, сбора, хранения, обработки и анализа информации с учетом вхождения России в глобальную информационную инфраструктуру;

– разработка соответствующей нормативной правовой базы и координация, при ведущей роли Федерального агентства правительственной связи и информации при Президенте РФ, деятельности федеральных органов государственной власти и других органов, решающих задачи обеспечения ИБ;

– развитие отечественной индустрии телекоммуникационных и информационных средств, их приоритетное по сравнению с зарубежными аналогами распространение на внутреннем рынке;

– защита государственного информационного ресурса, прежде всего в федеральных органах государственной власти и на предприятиях оборонного комплекса.

Доктрина информационной безопасности Российской Федерации от 09.09.2001 № Пр-1895 представляет собой *совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения ИБ Российской Федерации* . Она служит основой:

– для формирования государственной политики в области обеспечения ИБ Российской Федерации;

– подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения ИБ;

– разработки целевых программ обеспечения ИБ Российской Федерации.

По структуре Доктрина состоит из 4 разделов и 11 глав. В первом разделе « ***Информационная безопасность Российской Федерации»*** дается *понятие ИБ, выделяются национальные интересы личности, общества и государства в информационной сфере* . В Доктрине они уточнены более подробно, чем в Концепции национальной безопасности.

Стратегические и текущие задачи внутренней и внешней политики государства по обеспечению ИБ формируются на основе нижеперечисленных интересов в информационной:

– *личности* – заключаются в реализации конституционных прав человека и гражданина на доступ к информации, использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность;

– *общества* – заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России;

– *государства* – заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной

целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

Определяются виды угроз ИБ и их источники. Они также, в отличие от Концепции национальной безопасности, подробно уточнены.

Во втором разделе ***«Методы обеспечения информационной безопасности»*** :

– определяются общие методы обеспечения ИБ Российской Федерации;

– раскрываются особенности обеспечения ИБ Российской Федерации в различных сферах общественной жизни;

– определяется международное сотрудничество в сфере обеспечения ИБ.

В третьем разделе ***«Основные положения государственной политики обеспечения информационной безопасности Российской Федерации»*** содержатся:

– принципы обеспечения государственной политики;

– первоочередные мероприятия по реализации государственной политики обеспечения ИБ Российской Федерации.

Четвертый раздел **« *Организационная основа системы обеспечения информационной безопасности Российской Федерации»*** закрепляет основные функции системы обеспечения ИБ и ее организационную основу.

В Доктрине определены особенности обеспечения информационной безопасности в сфере:

– экономики;

– внутренней и внешней политики;

– науки и техники;

– духовной жизни;

– общегосударственных информационных и телекоммуникационных систем;

– обороны;

– правоохранительной и судебной, а также в условиях чрезвычайных ситуаций.

Это первая попытка законодательного закрепления направлений деятельности государства по обеспечению ИБ. Нет необходимости говорить о значении такого закрепления, потому что оно касается всех сфер деятельности государства и занимает практически приоритетное место в системе национальной безопасности.

Вопрос 3. Современные угрозы информационной безопасности в России

Согласно Закону о безопасности под **угрозой безопасности** понимается *совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства* . Концепция национальной безопасности РФ не дает определения угрозы, но называет некоторые из них в информационной сфере. Так, опасность представляют:

– стремление ряда стран к доминированию в мировом информационном пространстве;

– вытеснение государства с внутреннего и внешнего информационного рынка;

– разработка рядом государств концепции информационных войн;

– нарушение нормального функционирования информационных систем;

– нарушение сохранности информационных ресурсов, получение несанкционированного доступа к ним.

Это так называемые ***внешние угрозы*** , которые обусловлены *конкурентным характером развития межгосударственных и международных отношений* . Соответственно существуют и ***внутренние угрозы*** , связанные во многом с *недостаточным проведением экономических, социально-политических и иных преобразований в сфере* ИБ. Концепция национальной безопасности называет их в качестве предпосылок возникновения угроз. С учетом этих предпосылок, по нашему мнению, к источникам внутренних угроз можно отнести:

– отставание России в сфере информатизации органов государственной власти;

– несовершенство системы организации государственной власти по формированию и реализации единой государственной политики обеспечения ИБ;

– криминализацию общественных отношений, рост организованной преступности;

– увеличение масштабов терроризма;

– обострение межнациональных и осложнение внешних отношений.

Для нейтрализации информационных угроз существует исторически сложившаяся система сохранения государственной тайны, включающая подсистемы:

– криптографической сети конфиденциальной связи;

– противодействия иностранным техническим разведкам;

– обеспечения режима секретности на закрытых государственных объектах.

Наряду с традиционными приоритетами иностранных технических разведок в сферу их интересов все в большей мере вовлекаются вопросы технологий, финансов, торговли, ресурсов, доступ к которым открывается в связи с конверсией, развитием международных интеграционных процессов, широким внедрением компьютерных технологий. Из существующих информационных угроз наиболее актуальными являются угрозы экономической безопасности предприятий и фирм, определяемые недобросовестной конкуренцией, экономическим и промышленным шпионажем. Промышленный шпионаж существовал всегда.

Промышленный шпионаж представляет собой *несанкционированную передачу конфиденциальной технологии, материалов, продукции, информации о них.*

Методы и способы ведения шпионажа остаются неизменными на протяжении многих столетий развития общества и государства. При этом меняются только средства и формы его ведения. К таким методам относятся: подкуп, шантаж, деятельность послов-шпионов, перехват сообщений, представленных на различных носителях (магнитные носители, письма и др.).

Что касается ***анализа полученной информации*** , то все осталось без изменений. Им занимается человек или группа людей, осуществляющих аналитико-синтетическую переработку информации, в том числе с использованием новых информационных технологий.

Развитие техники вплоть до начала XX в. не влияло на средства несанкционированного получения информации: сверлили дырки в стенах и потолках, использовали потайные ходы и полупрозрачные зеркала, устраивались у замочных скважин и под окнами. Появление телеграфа и телефона позволило использовать технические средства получения информации. Гигантское количество сообщений стало перехватываться, влияя на ведение войн и положение на бирже. В 30–40 гг. появились диктофоны, миниатюрные фотоаппараты, различные радиомикрофоны.

Развитие новых информационных технологий позволило осуществлять перехват гигантского количества сообщений, оказывая влияние на все сферы социально-экономического развития общества, в том числе на развитие промышленности.

Анализ результатов исследований угроз информации позволяет утверждать, что одной из основных угроз государственной безопасности Российской Федерации являются попытки западных спецслужб добывать ***конфиденциальные сведения*** , составляющие государственную, промышленную, банковскую и другие виды тайн. Ведущие западные страны продолжают модернизировать и развивать свои разведывательные службы, совершенствовать техническую разведку, наращивать ее возможности.

С учетом рассмотренного содержания понятия угрозы государству, обществу и личности в широком смысле рассмотрим угрозы, непосредственно воздействующие на обрабатываемую конфиденциальную информацию. Система угроз безопасности представляет собой реальные или потенциально возможные действия или условия, приводящие к хищению, искажению, несанкционированному доступу, копированию, модификации, изменению, уничтожению конфиденциальной информации и сведений о

самой системе и, соответственно, к прямым материальным убыткам.

При этом угрозы сохранности информации определяются случайными и преднамеренными разрушающими и искажающими воздействиями внешней среды, надежностью функционирования средств обработки информации, а также преднамеренного корыстного воздействия несанкционированных пользователей, целью которых является хищение, уничтожение, разрушение, модификации и использование обрабатываемой информации. Анализ содержания свойств угроз позволяет предложить следующие варианты их классификации (рис. 1).

Проявление угроз характеризуется рядом закономерностей. Во-первых, незаконным овладением конфиденциальной информацией, ее копированием, модификацией, уничтожением в интересах злоумышленников, с целью нанесения ущерба. Кроме этого, непреднамеренные действия обслуживающего персонала и пользователей также приводят к нанесению определенного ущерба. Во-вторых, основными путями реализации угроз информации и безопасности информации выступают:

– агентурные источники в органах управления и защиты информации;

– вербовка должностных лиц органов управления, организаций, предприятий и т. д.;

– перехват и несанкционированный доступ к информации с использованием технических средств разведки;

– использование преднамеренного программно-математического воздействия;

– подслушивание конфиденциальных переговоров в служебных помещениях, транспорте и других местах их ведения.

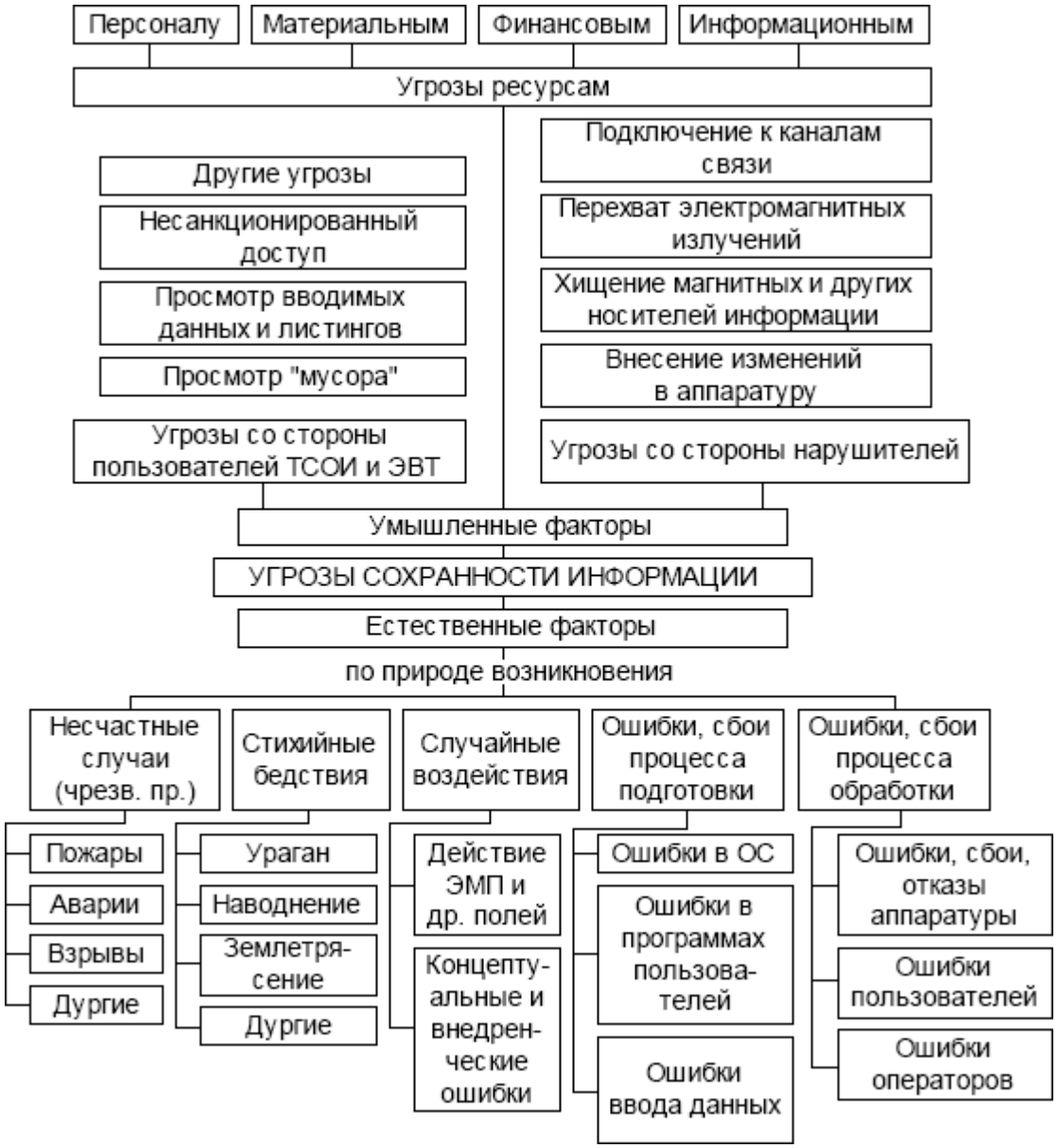

Рис. 1. Классификация угроз безопасности

Основными факторами воздействия угроз, обусловливающими информационные потери и приводящими к различным видам ущерба, возрастание убытков от неправомерных действий, являются:

– несчастные случаи, вызывающие выход из строя оборудования и информационных ресурсов (пожары, взрывы, аварии, удары, столкновения, падения, воздействия химических или физических сред);

– поломки элементов средств обработки информации;

– последствия природных явлений (наводнения, бури, молнии, землетрясения и др.);

– кражи, преднамеренная порча материальных средств;

– аварии и выход из строя аппаратуры, программного обеспечения, баз данных;

– ошибки накопления, хранения, передачи, использования информации;

– ошибки восприятия, чтения, интерпретации содержания информации, соблюдения правил, ошибки как результат неумения, оплошности, наличие помех, сбоев и искажений отдельных элементов и знаков или сообщения;

– ошибки эксплуатации: нарушение защиты, переполнение файлов, ошибки языка управления данными, ошибки при подготовке и вводе информации, ошибки операционной системы, программирования, аппаратные ошибки, ошибки толкования инструкций, пропуск

операций и др.;

– концептуальные ошибки внедрения;

– злонамеренные действия в материальной сфере;

– болтливость, разглашение; – убытки социального характера (уход, увольнение, забастовка и др.).

Информационный ущерб в ряде случаев может быть оценен в зависимости от вида потерь. Это могут быть:

– *потери, связанные с компенсацией или возмещением утраченных, похищенных материальных средств* , которые включают:

• стоимость компенсации возмещения другого косвенно утраченного имущества;

• стоимость ремонтно-восстановительных работ;

• расходы на анализ и исследование причин и величины ущерба;

• другие расходы;

– *дополнительные расходы* на персонал, обслуживающий технические средства обработки конфиденциальной информации, восстановление информации, возобновление работы информационных систем по сбору, хранению, обработке, контролю данных, в том числе расходы:

• на поддержку информационных ресурсов ТСОИ;

• обслуживающий персонал, не связанный с обработкой информации;

• специальные премии, расходы на перевозку и др.;

– *эксплуатационные потери* , связанные с ущербом банковских интересов или финансовыми издержками, потерей клиентов, заказчиков, требующие дополнительных расходов на восстановление: банковского доверия; размеров прибыли; утерянной клиентуры; доходов организации и др.;

• утрата фондов или порча имущества, не подлежащего восстановлению, которые снижают финансовые возможности (деньги, ценные бумаги, денежные переводы и др.);

• расходы и потери, связанные с возмещением морального ущерба, обучением, экспертизой и др.

Анализируя количественные данные потерь, можно сделать вывод о том, что убытки от злонамеренных действий, и особенно от экономического шпионажа, непрерывно возрастают и являются наиболее значимыми. Выводы западных экспертов показывают, что утечка 20 % коммерческой информации в 60 случаях из 100 приводит к банкротству фирмы.

Подводя итоги краткому анализу существующих угроз конфиденциальной информации, можно выделить два направления воздействия угроз, снижающих безопасность информации.

Первое, традиционно сложившееся в рамках защиты конфиденциальных сведений, представляет собой *воздействия* , способствующие несанкционированному доступу к этим сведениям. Второе, сложившееся в рамках широкого понимания проблем ИБ, связано с *использованием* современных технических и организационных систем, а также с участием людей, коллективов людей и общества в целом и их подверженностью внешним, негативным информационным воздействиям.

Так, теоретически доказано, а практикой многократно подтверждено то, что психика и мышление человека подвержены внешним информационным воздействиям и при их надлежащей организации возникает возможность программирования поведения человека. Более того, в последнее время ведутся разработки методов и средств компьютерного проникновения в подсознание, для того чтобы оказывать на него глубокое воздействие. Поэтому актуальной является проблема не только защиты информации, но и защиты от разрушающего воздействия информации, приобретающей международный масштаб и стратегический характер. В силу изменения концепции развития стратегических вооружений, определяющей, что вооруженное решение мировых проблем становится невозможным, все более прочно входит в обиход понятие ***информационной войны*** . Сейчас эффективность наступательных средств информационной войны, информационного оружия

превосходит эффективность систем защиты информации.

Представляют интерес угрозы утраты охраняемых сведений в ходе информационных процессов, участники которых представляют противоположные интересы. Анализ этих угроз позволил выявить ряд их характерных признаков. В большинстве случаев активные действия сторон вполне осознанны и целенаправленны. К таким действиям относятся:

– разглашение конфиденциальной информации ее обладателем;

– утечка информации по различным, главным образом техническим, каналам;

– несанкционированный доступ к конфиденциальной информации различными способами.

Разглашение информации – это *умышленные или неосторожные действия должностных лиц и граждан, которым в установленном порядке были доверены соответствующие сведения по работе, приведшие к оглашению охраняемых сведений, а также передача таких сведений по открытым техническим каналам* . Разглашение выражается в сообщении, передаче, предоставлении, пересылке, опубликовании, при обсуждении, утере и оглашении любыми иными способами конфиденциальной информации лицам и организациям, не имеющим права доступа к охраняемым секретам. Разглашение информации может происходить по многим каналам, в том числе через почтовые отправления, радио, телевидение, печать и т. п. Разглашение возможно в ходе деловых встреч, бесед, при обсуждении совместных работ, в договорах, в письмах и документах, деловых встречах и др. В ходе таких мероприятий партнеры ведут интенсивный обмен информацией. Именно при общении между ними устанавливаются «доверительные» отношения, приводящие к оглашению коммерческих секретов.

Как правило, факторами, способствующими разглашению конфиденциальной информации, являются:

– слабое знание (или незнание) требований по защите конфиденциальной информации;

– ошибочность действий персонала из-за низкой производственной квалификации;

– отсутствие системы контроля за оформлением документов, подготовкой выступлений, рекламы и публикаций;

– злостное, преднамеренное невыполнение требований по защите коммерческой тайны.

Разглашение конфиденциальной информации неизбежно приводит к материальному и моральному ущербу.

Утечку информации в общем виде можно рассматривать как *бесконтрольный и неправомерный выход конфиденциальной информации за пределы организации или круга лиц, которым эта информация была доверена* . При этом природа утечки охраняемой информации характеризуется как обстоятельствами происхождения, так и причинами, условиями возникновения утечки.

Неправомерному овладению конфиденциальной информацией вследствие ***неудовлетворительного управления персоналом*** со стороны должностных лиц, организаций и ведомств способствует наличие следующих обстоятельств:

– склонность сотрудников организации к излишней разговорчивости – 32 %;

– стремление сотрудников зарабатывать деньги любыми способами и любой ценой – 24 %;

– отсутствие в фирме службы безопасности – 14 %; – привычка сотрудников делится друг с другом информацией о своей служебной деятельности – 12 %;

– бесконтрольное использование в фирме информационных систем – 10 %;

– предпосылки возникновения конфликтных ситуаций в коллективе вследствие отсутствия психологической совместимости сотрудников, случайного подбора кадров, отсутствия работы руководителя по сплочению коллектива и др. – 8 %.

Также утечка охраняемой информации обусловлена наличием соответствующих условий, связанных:

– с ***появлением конкурента*** (злоумышленника), который такой информацией интересуется и затрачивает определенные силы и средства для ее приобретения;

– ***несовершенством норм по сохранению коммерческих секретов, а также нарушением этих норм*** , отступлением от правил обращения с соответствующими документами, техническими средствами, образцами продукции и другими материалами, содержащими конфиденциальную информацию;

– разными факторами и обстоятельствами, которые складываются в процессе научной, производственной, рекламной, издательской, информационной и иной деятельности организации и создают предпосылки для ***утечки сведений, составляющих различные виды тайн*** .

К таким факторам и обстоятельствам могут, например, относиться:

– недостаточное знание работниками правил защиты соответствующего вида тайны и непонимание необходимости их тщательного соблюдения;

– утрата удостоверений, пропусков, ключей от режимных помещений, хранилищ, сейфов (металлических шкафов), личных печатей – 12 %;

– пронос без разрешения работников службы безопасности (СБ) на территорию организации кино-, звуко-, фото– и видеозаписывающей, радиопередающей, принимающей и множительно-копировальной аппаратуры личного пользования; недонесение о фактах возможной утечки секретных сведений руководству подразделения и СБ; вынос с предприятия секретных документов и изделий без разрешения руководителя организации или начальника СБ – 4 %;

– неправильное определение грифа секретности документа (изделия) – 3 %;

– несвоевременное направление документов для приобщения к делу с отметками об исполнении и с резолюцией начальника подразделения; оставление открытыми и неопечатанными после окончания работы помещений (спецхранилищ) – 3 %;

– оставление секретных документов на рабочих столах при выходе из помещения, нарушение установленного порядка ознакомления прикомандированных лиц с секретными документами и изделиями, перевозка секретных документов и изделий личным и общественным транспортом и перемещение с ними в места, не связанные с выполнением заданий, – 2 %;

– неправильное оформление секретных документов в печать; несоблюдение порядка отчетности перед СБ за числящиеся за исполнителем документы и изделия при увольнении, перед уходом в отпуск, выездом в командировки; несвоевременное сообщение в кадровую службу об изменениях анкетных и автобиографических данных; ведение переговоров по секретным вопросам по незащищенным линиям связи; выполнение секретных работ на дому; снятие копий с секретных документов или производство выписок из них без письменного разрешения начальника СБ; передача и взятие без расписки секретных документов и изделий – 1 % по каждому случаю.

Причинами неправомерного овладения конфиденциальной информацией могу быть следующие обстоятельства:

– ***использование не аттестованных технических средств*** обработки конфиденциальной информации

– ***слабый контроль за соблюдением правил защиты информации*** правовыми организационными и инженерно-техническими мерами

– ***текучесть кадров*** , в том числе владеющих сведениями, составляющими коммерческую тайну;

– ***нарушения, не попадающие в поле зрения администрации и СБ*** , – это могут быть:

• ознакомление лиц с конфиденциальными документами, изделиями, работами, не входящими в круг их служебных обязанностей;

• направление адресатам конфиденциальных документов, к которым они не имеют отношения;

• подготовка конфиденциальных документов на неучтенных носителях;

• нарушение порядка работы с конфиденциальными документами, изделиями, который не допускает обзор их посторонними лицами;

• несвоевременное сообщение в СБ данных о внеслужебных связях с родственниками, проживающими за границей, с родственниками, выезжающими за границу на постоянное место жительства;

• посещение без разрешения руководства организации посольств, консульств, иностранных частных компаний и фирм;

• установление радиосвязи с радиолюбителями иностранных государств;

• использование конфиденциальных сведений в несекретной служебной переписке, технических заданиях, статьях, докладах и выступлениях;

• преждевременная публикация научных и других работ, которые могут расцениваться на уровне изобретений или открытий или опубликование которых запрещено в установленном порядке;

• сообщение устно или письменно кому бы то ни было, в том числе родственникам, конфиденциальных сведений, если это не вызвано служебной необходимостью;

• сообщение каких-либо сведений о проводимых конфиденциальных работах при обращении по личным вопросам с жалобами, просьбами и предложениями в федеральные государственные органы власти, органы власти субъектов РФ и органы местного самоуправления.

Кроме того, утечке информации способствуют стихийные бедствия, катастрофы, неисправности, отказы, аварии технических средств и оборудования.

Способы **несанкционированного доступа** (НСД) как проблему утечки конфиденциальной информации предлагается рассматривать со следующих позиций. Вопрос обеспечения защиты от НСД связан с проблемой сохранности не только информации как вида интеллектуальной собственности, но физических и юридических лиц, их имущественной собственности и личной безопасности. Известно, что такая деятельность тесно связана с получением, накоплением, хранением, обработкой и использованием разнообразных информационных потоков. Как только информация представляет определенную цену, факт ее получения злоумышленником приносит ему определенный доход, ослабляя тем самым возможности конкурента. Отсюда главная цель противоправных действий – получение информации о составе, состоянии и деятельности объекта конфиденциальной информации для удовлетворения своих информационных потребностей в корыстных целях и внесение изменений в состав информации. Такое действие может привести к дезинформации в определенных сферах деятельности и отражаться, в частности, на учетных данных, результатах решения управленческих задач.

Более опасной угрозой является уничтожение накопленных информационных массивов в документальной или магнитной форме и программных продуктов в среде автоматизированной системы обработки данных. ***Уничтожение*** – это *противоправное действие, направленное на нанесение материального и информационного ущерба конкуренту со стороны злоумышленника* **.**

Таким образом, рассмотренные угрозы в отношении информации, за исключением последней, как правило, нацелены и ведут к получению злоумышленником конфиденциальной информации. Анализ традиционных приемов и методов получения конфиденциальной информации позволил выделить наиболее характерные источники и методы ее получения, которые в общем виде описывают действия субъектов правовых отношений в сфере обеспечения ИБ:

– сбор информации, содержащейся в средствах массовой информации, включая официальные документы;

– использование сведений, распространяемых служащими конкурирующих организаций;

– документы, отчеты консультантов, финансовые отчеты и документы, выставочные экспонаты и проспекты и др.;

– изучение продукции конкурирующих и других организаций, представляющих интерес для соответствующих видов разведки, использование данных, полученных во время

бесед с обслуживающим персоналом;

– замаскированные опросы и "выуживание" информации у служащих организации на научно-технических конгрессах;

– непосредственное наблюдение, осуществляемое скрытно;

– беседы о найме на работу (без намерений приема их на работу);

– наем на работу служащего конкурирующей фирмы или организации для получения требуемой информации;

– подкуп служащего; – подслушивание переговоров, ведущихся в служебных и иных помещениях, перехват телеграфных сообщений, подслушивание телефонных разговоров;

– кража чертежей, документов и т. д.

– шантаж и вымогательство и др.

Рассмотренные источники и методы не является исчерпывающими, однако они позволяют сгруппировать все ***вероятные источники утечки информации*** следующим образом:

– *персонал, имеющий доступ* к конфиденциальной информации;

– *документы* , содержащие эту информацию; – *технические средства и системы обработки информации* , в том числе линии связи, по которым она передается.

Анализ зарубежных публикаций по источникам утечки информации в коммерческих фирмах позволил выявить, что, несмотря на высокий процент каналов, связанных с использованием для добывания сведений технических средств разведки и различных технологических приемов, персонал остается одним из главных причин и одним из источников утечки конфиденциальной информации, что подтверждается примерными следующих процентных соотношений по каналам утечки информации:

– подкуп, шантаж, переманивание служащих, внедрение агентов – 43;

– подслушивание телефонных переговоров – 5;

– кража документов – 10;

– проникновение в ПЭВМ – 18;

– съем информации с каналов "в темную» – 24.

Для раскрытия характеристик правонарушений, совершаемых в информационной сфере, существенное значение имеют характеристики вероятных каналов утечки информации, которые определяются наличием соответствующих источников конфиденциальной информации. Такую классификацию целесообразно рассматривать с учетом того, что обработка конфиденциальной информации осуществляется в организациях, представляющих собой сложные ***системы организационно-технического типа*** , функционирующие в условиях внешних воздействий и внутренних изменений состояния. При этом независимо от рассматриваемых воздействий на конфиденциальную информации и систему ее обработки возникающие каналы утечки информации проявляются через такие правонарушения. Эти каналы можно сгруппировать в рамках рассмотренных трех основных групп вероятных источников утечки информации. Так, первая группа – **персонал, имеющий доступ к конфиденциальной информации** , – представляет собой *людские потоки* и является важнейшей группой возможных каналов утечки информации. По распространенности возможные каналы утечки информации этой группы характеризуются следующими примерными показателями:

– приема и увольнения работников предприятия – 32 %;

– посещения предприятия командированными лицами – 28 %;

– проведения совещаний по секретным вопросам – 15 %;

– ведения секретных работ в рабочих помещениях – 15 %;

– допуска, доступа и обращения с секретной (конфиденциальной) информацией – 14 %;

– выезда специалистов за границу – 10 %;

– организации пропускного и внутриобъектового режима – 8 %;

– прохождения практики студентами – 7 %;

– посещения международных выставок – 7 %;

– обучения на курсах повышения квалификации – 5 %;

– подготовки постановлений и решений, приказов и других документов – 4 %.

Типовые нарушения при приеме и увольнении персонала :

– прием на работу лиц без оформления допуска в установленном порядке;

– доступ персонала к конфиденциальной информации в нарушение установленных требований;

– несвоевременное и неполное ознакомление персонала с требованиями нормативных правовых актов по обеспечению ИБ;

– неудовлетворительные знания нормативных правовых актов;

– увольнение персонала, являющегося носителем конфиденциальной информации.

Характерные нарушения при посещении предприятий командированными лицами :

– допуск командированных лиц с ведома руководителей подразделений к конфиденциальным работам и документам без соответствующего оформления разрешения;

– невыполнение требований инструкций для внутренних объектов по сопровождению прибывших в подразделения командированных лиц;

– отсутствие в предписаниях отметок о действительно выданной информации представителям других предприятий;

– прием командированных лиц с предписаниями, в которых отсутствуют основания командирования (номер и дата хозяйственного договора, ТЗ совместного плана НИОКР и др.);

– не определена степень конфиденциальности материалов, к которым допускается командированное лицо.

Нарушения, связанные с проведением служебных совещаний :

– проведение совещаний без соответствующего разрешения руководителя предприятия или его заместителей;

– допуск на совещание лиц, не имеющих отношения к обсуждаемым вопросам и участие которых не вызывается служебной необходимостью;

– несоблюдение очередности рассмотрения вопросов конфиденциального характера;

– несоблюдение требований режима внутреннего объекта при проведении совещаний;

– фотографирование, демонстрация конфиденциальных изделий, фильмов без согласования с СБ;

– звукозапись выступлений участников совещания на носителе, не учтенном в СБ;

– направление тетрадей (записей) секретного характера в учреждения, которых эти сведения непосредственно не касаются;

– недостаточное знание работниками, участвующими в приеме командированных лиц, требований инструкции о порядке приема командированных лиц (об этом заявили около 45 % опрошенных лиц).

Нарушения при ведении конфиденциальных работ в рабочих помещениях заключаются в отсутствии обеспечения:

– специальных средств защиты конфиденциальной информации, связи, звукозаписи, звукоусиления, переговорных и телевизионных устройств;

– средств изготовления и размножения документов;

– средств пожарной и охранной сигнализации;

– систем электронной часофикации, электрооборудования и других дополнительных технических средств защиты, исключающих утечку информации за счет побочных электромагнитных излучений и наводок.

Такие каналы утечки, как ***доступ и обращение с конфиденциальной информацией*** , образуются за счет расширения круга лиц, имеющих допуск к документам, изделиям, техническим заданиям.

Нарушения в организации пропускного и внутриобъектового режима включают:

– утрату удостоверений, пропусков, ключей от режимных помещений, хранилищ,

сейфов (шкафов), личных печатей – 12 %;

– пронос без разрешения СБ на территорию предприятия кино– и фотоаппаратуры, радиопередающей и принимающей, а также множительно-копировальной аппаратуры личного пользования;

– вынос из предприятия секретных документов и изделий без разрешения;

– оставление незакрытыми и не опечатанными после работы помещений (хранилищ).

Каналы утечки конфиденциальных сведений за счет ***неправильной организации прохождения технологической и преддипломной практики студентов*** проявляются в следующем: студенты и учащиеся вузов и средних специальных учебных заведений после прохождения практики не зачисляются на постоянную работу, где они проходили практику и познакомились со сведениями, составляющими государственную или коммерческую тайну, и другие причины.

Характерные нарушения при решении задач отраслевого и межотраслевого характера :

– включение конфиденциальных сведений в открытые документы с целью упрощения порядка доставки и согласования документов;

– ведение секретных записей в личных блокнотах, записных книжках;

– ознакомление с конфиденциальными работами и сведениями лиц, в круг служебных обязанностей которых они не входят;

– направление адресатам конфиденциальных документов, к которым они не имеют отношения.

Таким образом, проведенный анализ угроз информации позволяет уточнить ее свойства, подлежащие правовой защите. При этом содержание этих свойств будет рассматриваться с учетом положений действующих нормативных актов.

Лекция 2

Угрозы информационной безопасности. Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере. Понятие и виды защищаемой информации.

Учебные вопросы:

1. Информационные ресурсы и конфиденциальность информации.
2. Угрозы конфиденциальной информации организации.
3. Система защиты конфиденциальной информации.

Вопрос 1. Информационные ресурсы и конфиденциальность информации

В соответствии с действующим Федеральным законом «Об информации, информатизации и защите информации» информационные ресурсы предприятия, организации, учреждения, банка, компании и других государственных и негосударственных предпринимательских структур (далее по тексту – фирмы) включают в себя отдельные документы и отдельные массивы документов (дела), документы и комплексы документов в информационных системах (библиотеках, архивах, фондах, банках данных компьютеров и других информационных системах) на любых носителях, в том числе обеспечивающих работу вычислительной и организационной техники.

Информационные ресурсы (информация) являются объектами отношений физических и юридических лиц между собой и с государством. В совокупности они составляют информационные ресурсы России и защищаются законом наряду с другими видами ресурсов. Документирование информации (создание официального документа) является обязательным условием включения информации в информационные ресурсы. Следует учитывать, что документ может быть не только и даже не столько управленческим

(деловым), имеющим в большинстве случаев текстовую, табличную или анкетную форму. Значительно большие объемы наиболее ценных документов представлены в изобразительной форме:

1) конструкторские документы,

2) картографические документы,

3) научно-технические документы,

4) документы на фотографических, магнитных и иных носителях.

По принадлежности к тому или иному виду собственности информационные ресурсы могут быть государственными или негосударственными и как элемент состава имущества находиться в собственности граждан, органов государственной власти, исполнительных органов, органов местного самоуправления, государственных учреждений, организаций и предприятий, общественных объединений, предпринимательских структур.

В соответствии с интересами обеспечения национальной безопасности и степенью ценности для государства, а также правовыми, экономическими и другими интересами предпринимательских структур информационные ресурсы могут быть: а) *открытыми,* т. е. общедоступными, используемыми в работе без специального разрешения, публикуемыми в средствах массовой информации, оглашаемыми на конференциях, в выступлениях и интервью; б) *ограниченного доступа* и использования, т. е. содержащими сведения, составляющие тот или иной вид тайны и подлежащие защите, охране, наблюдению и контролю.

Запрещается относить к информации ограниченного доступа:

• законодательные и другие нормативные акты, устанавливающие правовой статус органов государственной власти, исполнительных органов, органов местного самоуправления, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

• документы, содержащие информацию о чрезвычайных ситуациях, экологическую, метеорологическую, демографическую, санитарно-эпидемиологическую и другую информацию, необходимую для обеспечения безопасного функционирования населенных пунктов, производственных объектов, безопасности граждан и населения в целом;

• документы, содержащие информацию о деятельности органов государственной власти, исполнительных органов и органов местного самоуправления, об использовании бюджетных средств и других государственных и местных ресурсов, о состоянии экономики и потребностях населения, за исключением сведений, относящихся к государственной тайне;

• документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах органов государственной власти, исполнительных органов, органов местного самоуправления, организаций, общественных объединений, представляющие общественный интерес или необходимые для реализации прав, свобод и обязанностей граждан.

Накопители информационных ресурсов называются источниками (обладателями) информации. Они представляют собой пассивные концентраторы этой информации и включают в себя:

• публикации о фирме и ее разработках;

• рекламные издания, выставочные материалы, документацию;

• персонал фирмы и окружающих фирму людей;

• физические поля, волны, излучения, сопровождающие работу вычислительной и другой офисной техники, различных приборов и средств связи.

Источники содержат информацию как открытого, так и ограниченного доступа. Причем информация того и другого рода находится в едином информационном пространстве и разделить ее без тщательного содержательного анализа часто не представляется возможным. Например, систематизированная совокупность открытой информации может в комплексе содержать сведения ограниченного доступа.

Документация как источник информации ограниченного доступа включает:

• документацию, содержащую ценные сведения, ноу-хау;

• комплексы обычной деловой и научно-технической документации, содержащей общеизвестные сведения, организационно-правовые и распорядительные документы;

• рабочие записи сотрудников, их служебные дневники, личные рабочие планы, переписку по производственным вопросам;

• личные архивы сотрудников фирмы. В каждой из указанных групп могут быть:

• документы на традиционных бумажных носителях (листах бумаги, ватмане, фотобумаге и т. п.);

• документы на технических носителях (магнитных, фотопленочных и т. п.);

• электронные документы, банки электронных документов, изображения документов на экране дисплея (видеограммы).

При выполнении управленческих и производственных действий любая информация источника всегда распространяется во внешней среде. Тем самым увеличивается число опасных источников разглашения или утечки информации ограниченного доступа, источников, подлежащих учету и контролю.

Каналы распространения информации носят объективный характер, отличаются активностью и включают в себя:

• деловые, управленческие, торговые, научные и другие коммуникативные регламентированные связи;

• информационные сети;

• естественные технические каналы излучения, создания фона. Канал распространения информации представляет собой путь перемещения сведений из одного источника в другой в санкционированном (разрешенном, законном) режиме или в силу объективных закономерностей. Например: обсуждение важного вопроса на закрытом совещании, запись на бумаге содержания изобретения, переговоры с потенциальным партнером, работа на ЭВМ и т. д.

Следовательно, *информационные ресурсы фирмы представляют собой динамичную категорию, что проявляется прежде всего в процессе документирования информации, объективном возникновении и расширении состава источников и каналов ее распространения.*

Документированные информационные ресурсы, которые используются предпринимателем в бизнесе и управлении фирмой, являются его собственной или частной информацией, представляющей для него значительную ценность. Эта информация составляет интеллектуальную собственность предпринимателя.

Ценность информации может быть стоимостной категорией и характеризовать конкретный размер прибыли при ее использовании или размер убытков при ее утрате. Информация часто становится ценной ввиду ее правового значения для фирмы или развития бизнеса, например: учредительные документы, программы и планы, договоры с партнерами и посредниками и т. д. Ценность может проявляться в ее перспективном научном, техническом или технологическом значении.

Обычно выделяется два вида информации, интеллектуально ценной для предпринимателя:

техническая, технологическая: методы изготовления продукции, программное обеспечение, производственные показатели, химические формулы, рецептуры, результаты испытаний опытных образцов, данные контроля качества и т. п.;

деловая: стоимостные показатели, результаты исследования рынка, списки клиентов, экономические прогнозы, стратегия действий на рынке и т. п.

Ценная информация охраняется нормами права (патентного, авторского, смежных прав и др.), товарным знаком или защищается включением ее в категорию информации, составляющей тайну фирмы.

Процесс выявления и регламентации реального состава ценной информации, составляющей тайну фирмы, является основополагающей частью системы защиты

информации. Состав этих сведений фиксируется в специальном **перечне,** закрепляющем факт отнесения их к защищаемой информации и определяющем период (срок) конфиденциальности (т. е. недоступности для всех) этих сведений, уровень (гриф) их конфиденциальности, список сотрудников фирмы, которым дано право использовать эти сведения в работе. В основе перечня лежит типовой состав защищаемых сведений фирм данного профиля. Перечень является постоянным /рабочим материалом руководства фирмы, служб безопасности и конфиденциальной документации. Он представляет собой классифицированный список типовой и конкретной ценной информации о проводимых работах, производимой продукции, научных и деловых идеях, технологических новшествах. *В перечень включаются действительно Ценные сведения («изюминки») о каждой работе фирмы.* Следует отметить, что нельзя ограничивать доступ к информации, относящейся к новой продукции, но не имеющей ценности.

Дополнительно может составляться **перечень документов,** в которых защищаемая информация отражается (документируется). В перечень включаются также документы, не содержащие указанную информацию, но представляющие ценность для фирмы и подлежащие охране. Часто обычный открытый правовой акт важно сохранить в целостности и безопасности от похитителя или стихийного бедствия. Перечни формируются индивидуально каждой фирмой в соответствии с рекомендациями специальной комиссии и утверждаются первым руководителем фирмы. Эта комиссия регулярно вносит текущие изменения в перечни в соответствии с динамикой выполнения фирмой конкретных работ.

При заключении любого договора (контракта) стороны должны брать на себя взаимные письменные обязательства по защите конфиденциальной информации другой стороны и документов, полученных при переговорах, исполнении условий договора.

Производственная или коммерческая ценность информации, как правило, недолговечна и определяется временем, необходимым конкуренту для выработки той же идеи или ее хищения и воспроизводства, а также временем до патентования, опубликования и перехода в число общеизвестных.

Документированная информация ограниченного доступа всегда принадлежит к одному из видов тайны – государственной или негосударственной. В соответствии с этим документы делятся на секретные и несекретные. Обязательным признаком (критерием принадлежности) секретного документа является наличие в нем сведений, составляющих в соответствии с законодательством государственную тайну. Несекретные документы, включающие сведения, относимые к негосударственной тайне (служебной, коммерческой, банковской, профессиональной, производственной и др.), или содержащие персональные данные граждан, именуются конфиденциальными.

Несмотря на то, что *конфиденциальность* является синонимом секретности, термин широко используется исключительно для обозначения информационных ресурсов ограниченного доступа, не отнесенных к государственной тайне. Конфиденциальность отражает ограничение, которое накладывает собственник информации на доступ к ней других лиц, т. е. собственник устанавливает правовой режим этой информации в соответствии с законом. Вместе с тем в соответствии с постановлением Правительства «О перечне сведений, которые не могут составлять коммерческую тайну» от 05.12.91 к конфиденциальным документам нельзя относить учредительные документы, уставы предпринимательских структур, финансовую документацию, сведения о заработной плате персонала и другую документированную информацию, необходимую правоохранительным и налоговым государственным органам.

Под конфиденциальным (закрытым, защищаемым) документом понимается необходимым образом оформленный носитель документированной информации, содержащий сведения ограниченного доступа или использования, которые составляют интеллектуальную собственность юридического или физического лица. Конфиденциальные документы не следует называть служебными или ставить на них гриф секретности, так как конфиденциальные и секретные документы отражают различные виды тайны.

Конфиденциальные документы включают в себя:

• в государственных структурах – служебную информацию ограниченного распространения, именуемую в чиновничьем обиходе информацией для служебного пользования, т. е. информацией, отнесенной к служебной тайне, а также документы, имеющие рабочий характер и не подлежащие публикации в открытой печати (проекты документов, сопутствующие материалы и др.);

• в предпринимательских структурах и направлениях подобной деятельности – сведения, которые их собственник или владелец в соответствии с законодательством имеет право отнести к коммерческой (предпринимательской) тайне, тайне фирмы, тайне мастерства;

• независимо от принадлежности – любые персональные (личные) данные о гражданах, а также сведения, содержащие профессиональную тайну, технические и технологические новшества (до их патентования), тайну предприятий связи, сферы обслуживания и т. п.

Особенностью конфиденциального документа является то, что он представляет собой одновременно:

• массовый носитель ценной, защищаемой информации;

• основной источник накопления и объективного распространения этой информации, а также ее неправомерного разглашения или утечки;

• обязательный объект защиты.

Конфиденциальность документов всегда имеет значительный разброс по срокам ограничения свободного доступа к ним персонала фирмы (от нескольких часов до значительного числа лет). Следует учитывать, что основная масса конфиденциальных документов после окончания их исполнения или работы с ними теряет свою ценность и конфиденциальность. Например, переписка до заключения контракта может иметь гриф конфиденциальности, но после его подписания этот гриф с письменного разрешения первого руководителя фирмы снимается.

Исполненные документы, сохранившие конфиденциальный характер и ценность для деятельности фирмы, формируются в дела в соответствии с номенклатурой дел. Период нахождения конфиденциальных документов в делах может быть кратковременным или долговременным в зависимости от ценности информации, содержащейся в документах дела. Период конфиденциальности документов определяется по указанному выше перечню конфиденциальных сведений и зависит от специфики деятельности фирмы. Например, производственные, научно-исследовательские фирмы обладают более ценными документами, чем торговые, посреднические и др.

Документы долговременного периода конфиденциальности (программы и планы развития бизнеса, технологическая документация ноу-хау, изобретения и др.) имеют усложненный вариант обработки и хранения, обеспечивающий безопасность информации и ее носителя. Документы кратковременного периода конфиденциальности, имеющие оперативное значение для деятельности фирмы, обрабатываются и хранятся по упрощенной схеме и могут не выделяться из технологической системы обработки открытых документов при наличии в этой системе минимальных защитных, контрольных и аналитических элементов.

Вывод: конфиденциальные документы характеризуются специфическими особенностями, которые отражают их сущность как носителей информации ограниченного доступа и определяют построение системы защиты этой информации.

Вопрос 2. Угрозы конфиденциальной информации организации

Все информационные ресурсы фирмы постоянно подвергаются объективным и субъективным угрозам утраты носителя или ценности информации.

Под угрозой или опасностью утраты информации понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление

неблагоприятных возможностей внешних или внутренних источников угрозы создавать критические ситуации, события, оказывать дестабилизирующее воздействие на защищаемую информацию, документы и базы данных.

Риск угрозы любым (открытым и ограниченного доступа) информационным ресурсам создают стихийные бедствия, экстремальные ситуации, аварии технических средств и линий связи-Другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица. К угрозам, создаваемым этими лицами, относятся: несанкционированное уничтожение документов, ускорение угасания (старения) текста или изображения, подмена или изъятие документов, фальсификация текста или его части и др.

Для информационных ресурсов ограниченного доступа диапазон угроз, предполагающих утрату информации (разглашение, утечку) или утерю носителя, значительно шире в результате того, что к этим документам проявляется повышенный интерес со стороны различного рода злоумышленников. В отличие от объективного распространения утрата информации влечет за собой незаконный переход конфиденциальных сведений, документов к субъекту, не имеющему права владения ими и использования в своих целях.

Под злоумышленником понимается лицо, действующее в интересах конкурента, противника или в личных корыстных интересах (агентов иностранных спецслужб, промышленного и экономического шпионажа, криминальных структур, отдельных преступных элементов, лиц, сотрудничающих со злоумышленником, психически больных лиц и т. п.).

Основной угрозой безопасности информационных ресурсов ограниченного распространения является несанкционированный (незаконный, неразрешенный) доступ злоумышленника или постороннего лица к документированной информации и как результат – овладение информацией и противоправное ее использование или совершение иных действий. Целью и результатом несанкционированного доступа может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, подмена и т. п. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности фирмы (работники коммунальных служб, экстремальной помощи, прохожие и др.), посетители фирмы, работники других организационных структур, а также сотрудники данной фирмы, не обладающие правом доступа в определенные помещения, к конкретному документу, информации, базе данных. Каждое из указанных лиц может быть злоумышленником или его сообщником, агентом, но может и не быть им.

Обязательным условием успешного осуществления попытки несанкционированного доступа к информационным ресурсам ограниченного доступа является *интерес к ним со стороны конкурентов, определенных лиц, служб и организаций.* При отсутствии такого интереса угроза информации не возникает даже в том случае, если создались предпосылки для ознакомления с ней постороннего лица. Основным виновником несанкционированного доступа к информационным ресурсам является, как правило, персонал, работающий с документами, информацией и базами данных. При этом надо иметь в виду, что утрата информации происходит в большинстве случаев не в результате преднамеренных действий, а из-за невнимательности и безответственности персонала.

Следовательно, утрата информационных ресурсов ограниченного доступа может наступить:

• при наличии интереса конкурента, учреждений, фирм или лиц к конкретной информации;

• при возникновении риска угрозы, организованной злоумышленником или при случайно сложившихся обстоятельствах;

• при наличии условий, позволяющих злоумышленнику осуществить необходимые действия и овладеть информацией. Эти условия могут включать:

• отсутствие системной аналитической и контрольной работы по выявлению и

изучению угроз, каналов и степени риска нарушений безопасности информационных ресурсов;

• неэффективную систему защиты информации или отсутствие этой системы;

• непрофессионально организованную технологию обработки и хранения конфиденциальных документов;

• неупорядоченный подбор персонала и текучесть кадров, сложный психологический климат в коллективе;

• отсутствие системы обучения сотрудников правилам защиты информации ограниченного доступа;

• отсутствие контроля со стороны руководства фирмы за соблюдением персоналом требований нормативных документов по работе с информационными ресурсами ограниченного доступа;

• бесконтрольное посещение помещений фирмы посторонними лицами.

Следует всегда помнить, что факт документирования резко увеличивает риск угрозы информации. Великие мастера прошлого никогда не записывали секреты своего искусства, а передавали их устно сыну, ученику. Поэтому тайна изготовления многих уникальных предметов того времени так и не раскрыта до наших дней.

Угрозы сохранности, целостности и конфиденциальности информационных ресурсов ограниченного доступа практически реализуются через *риск образования канала несанкционированного получения (добывания) кем-то ценной информации и документов.* Этот канал представляет собой совокупность незащищенных или слабо защищенных фирмой направлений возможной утраты конфиденциальной информации, которые злоумышленник использует для получения необходимых сведений, преднамеренного незаконного доступа к защищаемой информации.

Каждая конкретная фирма обладает своим набором каналов несанкционированного доступа к информации, что зависит от множества моментов – профиля деятельности, объемов защищаемой информации, профессионального уровня персонала, местоположения здания и т. п.

Функционирование канала несанкционированного доступа к информации обязательно влечет за собой утрату информации, исчезновение носителя информации.

В том случае, когда речь идет об утрате информации по вине персонала, используется термин «разглашение (огласка) информации». Человек может разглашать информацию устно, письменно, с помощью жестов, мимики, условных сигналов, лично, через посредников, по каналам связи и т. д. Термин «утечка информации», хотя и используется наиболее широко, однако в большей степени относится, по нашему мнению, к утрате информации за счет ее перехвата с помощью технических средств разведки, по техническим каналам.

Утрата информации характеризуется двумя условиями, информация переходит а) непосредственно к заинтересованному лицу – конкуренту, злоумышленнику или б) к случайному, третьему лицу. Под третьим лицом в данном случае понимается любое постороннее лицо, получившее информацию во владение в силу обстоятельств или безответственности персонала, не обладающее правом владения ею и, что очень важно, не заинтересованное в этой информации. Однако от третьего лица информация может легко перейти к злоумышленнику.

Переход информации к третьему лицу представляется достаточно частым явлением, и его можно назвать непреднамеренным, стихийным, хотя при этом факт разглашения информации, нарушения ее безопасности имеет место.

Непреднамеренный переход информации к третьему лицу возникает в результате:

• утери или неправильного уничтожения документа, пакета с документами, дела, конфиденциальных записей;

• игнорирования или умышленного невыполнения сотрудником требований по защите документированной информации;

• излишней разговорчивости сотрудников при отсутствии злоумышленника (с коллегами по работе, родственниками, друзьями, иными лицами в местах общего пользования, транспорте и т. п.);

• работы с документами ограниченного доступа при посторонних лицах, несанкционированной передачи их другому сотруднику;

• использования сведений ограниченного доступа в открытых документации, публикациях, интервью, личных записях, дневниках и т. п.;

• отсутствия маркировки (грифования) информации и документов ограниченного доступа (в том числе документов на технических носителях);

• наличия в документах излишней информации ограниченного доступа;

• самовольного копирования сотрудником документов в служебных или коллекционных целях.

В отличие от третьего лица злоумышленник или его сообщник целенаправленно охотятся за конкретной информацией и преднамеренно, противоправно устанавливают контакт с источником этой информации или преобразуют канал ее объективного распространения в канал ее разглашения или утечки. Такие каналы всегда являются тайной злоумышленника.

Каналы несанкционированного доступа могут быть двух типов: организационные и технические. Обеспечиваются они легальными и нелегальными методами.

Организационные каналы разглашения информации отличаются большим разнообразием видов и основаны на установлении разнообразных, в том числе законных, взаимоотношений злоумышленника с фирмой или ее сотрудником для последующего несанкционированного доступа к интересующей информации.

Основными видами организационных каналов могут быть:

• поступление злоумышленника на работу в фирму, как правило, на техническую или вспомогательную должность (оператором ЭВМ, секретарем, дворником, охранником, шофером и т. п.);

• участие в работе фирмы в качестве партнера, посредника, клиента, использование разнообразных обманных способов;

• поиск злоумышленником сообщника (инициативного помощника), работающего в интересующей его фирме, который становится его соучастником;

• установление злоумышленником доверительных взаимоотношений с сотрудником учреждения, фирмы или посетителем, сотрудником другого учреждения, обладающим интересующими злоумышленника сведениями;

• использование коммуникативных связей фирмы – участие в переговорах, совещаниях, переписке с фирмой и др.;

• использование ошибочных действий персонала или умышленное провоцирование злоумышленником этих действий;

• тайное или по фиктивным документам проникновение в здание фирмы и помещения, криминальный, силовой доступ к информации, т. е. кража документов, дискет, дисков, компьютеров, шантаж и склонение к сотрудничеству отдельных сотрудников, подкуп сотрудников, создание экстремальных ситуаций и т. п.;

• получение нужной информации от третьего (случайного) лица.

Организационные каналы отбираются или формируются злоумышленником индивидуально в соответствии с его профессиональным умением, конкретной ситуацией, и прогнозировать их крайне сложно. Обнаружение организационных каналов требует проведения серьезной поисковой и аналитической работы.

Широкие возможности несанкционированного получения подобных сведений создает техническое обеспечение офисных технологий. Любая управленческая деятельность всегда связана с обсуждением ценной информации в кабинетах или по линиям связи, проведением расчетов и анализа ситуаций на ЭВМ, изготовлением, размножением документов и т. п.

Технические каналы утечки информации возникают при использовании

злоумышленником специальных технических средств промышленного шпионажа, позволяющих получать защищаемую информацию без непосредственного контакта с персоналом фирмы, документами, делами и базами данных.

Технический канал представляет собой физический путь утечки информации от источника или канала объективного распространения информации к злоумышленнику. Канал возникает при анализе злоумышленником физических полей и излучений, появляющихся в процессе работы вычислительной и другой офисной техники, при перехвате информации, имеющей звуковую, зрительную или иную форму отображения. Основными техническими каналами являются: акустический, визуально-оптический, электромагнитный и др. Это каналы прогнозируемые, носят стандартный характер и перекрываются стандартными средствами противодействия. Обычным и профессионально грамотным является творческое сочетание в действиях злоумышленника каналов обоих типов, например установление доверительных отношений с сотрудником фирмы и перехват информации по техническим каналам с помощью этого сотрудника. Вариантов и сочетаний каналов может быть множество. Изобретательность грамотного злоумышленника не знает предела, поэтому риск утраты информации всегда достаточно велик. При эффективной системе защиты информации фирмы злоумышленник разрушает отдельные элементы защиты и формирует необходимый ему канал получения информации.

В целях практической реализации поставленных задач злоумышленник определяет не только каналы несанкционированного доступа к информации фирмы, но и совокупность методов получения этой информации.

Легальные методы входят в содержание понятий «невинного шпионажа» и «разведки в бизнесе», отличаются правовой безопасностью и, как правило, предопределяют возникновение интереса к конкурирующей фирме. В соответствии с этим может появиться необходимость использования каналов несанкционированного доступа к требуемой информации. В основе «невинного шпионажа» лежит кропотливая аналитическая работа специалистов-экспертов над опубликованными и общедоступными материалами конкурирующей фирмы. Одновременно изучается продукция фирмы, рекламные издания, сведения, полученные в процессе официальных и неофициальных бесед и переговоров с сотрудниками фирмы, материалы пресс-конференций, презентаций фирмы и продукции, научных симпозиумов и семинаров, сведения, получаемые из информационных сетей. Легальные методы дают злоумышленнику основную массу интересующей его информации и позволяют определить состав отсутствующих сведений, которые предстоит добыть нелегальными методами.

Нелегальные методы получения ценной информации всегда носят незаконный характер и используются в целях доступа к защищаемой информации, которую невозможно получить легальными методами. В основе нелегального получения информации лежит поиск злоумышленником существующих в фирме и наиболее эффективных в конкретных условиях незащищенных организационных и технических каналов несанкционированного доступа к информации, формирование таких каналов при их отсутствии и реализация плана практического комплексного использования этих каналов.

Нелегальные методы предполагают: воровство, продуманный обман, подслушивание разговоров, подделку идентифицирующих документов, взяточничество, инсценирование или организацию экстремальных ситуаций, использование различных криминальных приемов и т. д. В процессе реализации нелегальных методов часто образуется агентурный канал добывания ценной информации. К нелегальным методам относятся также: перехват информации, объективно распространяемой по техническим каналам, визуальное наблюдение за помещениями фирмы и персоналом, анализ продуктов и объектов, содержащих следы защищаемой информации, анализ архитектурных особенностей объектов защиты, анализ отходов производства, мусора, выносимого из офиса.

В результате эффективного использования каналов несанкционированного доступа к информации ограниченного доступа и разнообразных методов ее добывания злоумышленник

получает:

• подлинник или официальную копию документа (бумажного, машиночитаемого, электронного), содержащего информацию ограниченного доступа;

• несанкционированно сделанную копию этого документа (рукописную или изготовленную с помощью копировального аппарата, фототехники, компьютера и т. п.);

• диктофонную, магнитофонную, видеокассету с записью текста документа, переговоров, совещания;

• письменное или устное изложение за пределами фирмы содержания документа, ознакомление с которым осуществлялось санкционирование или тайно;

• устное изложение текста документа по телефону, переговорному устройству, специальной радиосвязи и т. п.;

• аналог документа, переданного по факсимильной связи или электронной почте;

• речевую или визуальную запись текста документа, выполненную с помощью технических средств разведки (радиозакладок, встроенных микрофонов и видеокамер, микрофотоаппаратов, фотографирования с большого расстояния). Получение ценных документов или информации ограниченного доступа может быть единичным явлением или регулярным процессом, протекающим на протяжении относительно длительного времени.

Вывод: любые информационные ресурсы фирмы являются весьма уязвимой категорией и при интересе, возникшем к ним со стороны злоумышленника, опасность их утраты становится достаточно реальной.

Вопрос 3. Система защиты конфиденциальной информации

Практической реализацией политики (концепции) информационной безопасности фирмы является технологическая система защиты информации. Защита информации представляет собой жестко регламентированный и динамический технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности ценных информационных ресурсов и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности фирмы.

Система защиты информации – рациональная совокупность направлений, методов, средств и мероприятий, снижающих уязвимость информации и препятствующих несанкционированному доступу к информации, ее разглашению или утечке. Главными требованиями к организации эффективного функционирования системы являются: персональная ответственность руководителей и сотрудников за сохранность носителя и конфиденциальность информации, регламентация состава конфиденциальных сведений и документов, подлежащих защите, регламентация порядка доступа персонала к конфиденциальным сведениям и документам, наличие специализированной службы безопасности, обеспечивающей практическую реализацию системы защиты и нормативно-методического обеспечения деятельности этой службы.

Собственники информационных ресурсов, в том числе государственные учреждения, организации и предприятия, самостоятельно определяют (за исключением информации, отнесенной к государственной тайне) необходимую степень защищенности ресурсов и тип системы, способы и средства защиты, исходя из ценности информации. Ценность информации и требуемая надежность ее защиты находятся в прямой зависимости. Важно, что структура системы защиты должна охватывать не только электронные информационные системы, а весь управленческий комплекс фирмы в единстве его реальных функциональных и производственных подразделений, традиционных документационных процессов. Отказаться от бумажных документов и часто рутинной, исторически сложившейся управленческой технологии не всегда представляется возможным, особенно если вопрос стоит о безопасности ценной, конфиденциальной информации.

Основной характеристикой системы является ее комплексность, т. е. наличие в ней

обязательных элементов, охватывающих все направления защиты информации. Соотношение элементов и их содержания обеспечивают индивидуальность построения системы защиты информации конкретной фирмы и гарантируют неповторимость системы, трудность ее преодоления. Конкретную систему защиты можно представить в виде кирпичной стены, состоящей из множества разнообразных элементов (кирпичиков). Элементами системы являются: правовой, организационный, инженерно-технический, программно-аппаратный и криптографический.

Правовой элемент системы защиты информации основывается на нормах информационного права и предполагает юридическое закрепление взаимоотношений фирмы и государства по поводу правомерности использования системы защиты информации, фирмы и персонала по поводу обязанности персонала соблюдать установленные собственником информации ограничительные и технологические меры защитного характера, а также ответственности персонала за нарушение порядка защиты информации. Этот элемент включает:

• наличие в организационных документах фирмы, правилах внутреннего трудового распорядка, контрактах, заключаемых с сотрудниками, в должностных и рабочих инструкциях положений и обязательств по защите конфиденциальной информации;

• формулирование и доведение до сведения всех сотрудников фирмы (в том числе не связанных с конфиденциальной информацией) положения о правовой ответственности за разглашение конфиденциальной информации, несанкционированное уничтожение или фальсификацию документов;

• разъяснение лицам, принимаемым на работу, положения о добровольности принимаемых ими на себя ограничений, связанных с выполнением обязанностей по защите информации.

Организационный элемент системы защиты информации содержит меры управленческого, ограничительного (режимного) и технологического характера, определяющие основы и содержание системы защиты, побуждающие персонал соблюдать правила защиты конфиденциальной информации фирмы. Эти меры связаны с установлением режима конфиденциальности в фирме. Элемент включает в себя регламентацию:

• формирования и организации деятельности службы безопасности и службы конфиденциальной документации (или менеджера по безопасности, или референта первого руководителя), обеспечения деятельности этих служб (сотрудника) нормативно-методическими документами по организации и технологии защиты информации;

• составления и регулярного обновления состава (перечня, списка, матрицы) защищаемой информации фирмы, составления и ведения перечня (описи) защищаемых бумажных, машиночитаемых и электронных документов фирмы;

• разрешительной системы (иерархической схемы) разграничения доступа персонала к защищаемой информации;

• методов отбора персонала для работы с защищаемой информацией, методики обучения и инструктирования сотрудников;

• направлений и методов воспитательной работы с персоналом, контроля соблюдения сотрудниками порядка защиты информации;

• технологии защиты, обработки и хранения бумажных, машиночитаемых и электронных документов фирмы (делопроизводственной, автоматизированной и смешанной технологий); внемашинной технологии защиты электронных документов;

• порядка защиты ценной информации фирмы от случайных или умышленных несанкционированных действий персонала;

• веления всех видов аналитической работы;

• порядка защиты информации при проведении совещаний, заседаний, переговоров, приеме посетителей, работе с представителями рекламных агентств, средств массовой информации;

• оборудования и аттестации помещений и рабочих зон, выделенных для работы с конфиденциальной информацией, лицензирования технических систем и средств защиты информации и охраны, сертификации информационных систем, предназначенных для обработки защищаемой информации;

• пропускного режима на территории, в здании и помещениях фирмы, идентификации персонала и посетителей;

• системы охраны территории, здания, помещений, оборудования, транспорта и персонала фирмы;

• действий персонала в экстремальных ситуациях;

• организационных вопросов приобретения, установки и эксплуатации технических средств защиты информации и охраны;

• организационных вопросов защиты персональных компьютеров, информационных систем, локальных сетей;

• работы по управлению системой защиты информации;

• критериев и порядка проведения оценочных мероприятий по установлению степени эффективности системы защиты информации.

Элемент организационной защиты является стержнем, основной частью рассматриваемой комплексной системы. По мнению большинства специалистов, меры организационной защиты информации составляют 50–60 % в структуре большинства систем защиты информации. Это связано с рядом факторов и также с тем, что важной составной частью организационной защиты информации является подбор, расстановка и обучение персонала, который будет реализовывать на практике систему защиты информации. Сознательность, обученность и ответственность персонала можно с полным правом назвать краеугольным камнем любой даже самой технически совершенной системы защиты информации. Организационные меры защиты отражаются в нормативно-методических документах службы безопасности, службы конфиденциальной документации учреждения или фирмы. В этой связи часто используется единое название двух рассмотренных выше элементов системы защиты – «элемент организационно-правовой защиты информации».

Инженерно-технический элемент системы защиты информации предназначен для пассивного и активного противодействия средствам технической разведки и формирования рубежей охраны территории, здания, помещений и оборудования с помощью комплексов технических средств. При защите информационных систем этот элемент имеет весьма важное значение, хотя стоимость средств технической защиты и охраны велика. Элемент включает в себя:

• сооружения физической (инженерной) защиты от проникновения посторонних лиц на территорию, в здание и помещения (заборы, решетки, стальные двери, кодовые замки, идентификаторы, сейфы и др.);

• средства защиты технических каналов утечки информации, возникающих при работе ЭВМ, средств связи, копировальных аппаратов, принтеров, факсов и других приборов и офисного оборудования, при проведении совещаний, заседаний, беседах с посетителями и сотрудниками, диктовке документов и т. п.;

• средства защиты помещений от визуальных способов технической разведки;

• средства обеспечения охраны территории, здания и помещений (средства наблюдения, оповещения, сигнализирования, информирования и идентификации);

• средства противопожарной охраны;

• средства обнаружения приборов и устройств технической разведки (подслушивающих и передающих устройств, тайно установленной миниатюрной звукозаписывающей и телевизионной аппаратуры и т. п.);

• технические средства контроля, предотвращающие вынос персоналом из помещения специально маркированных предметов, документов, дискет, книг и т. п. *Программно-аппаратный элемент* системы защиты информации предназначен для защиты ценной информации, обрабатываемой и хранящейся в компьютерах, серверах и рабочих

станциях локальных сетей и различных информационных системах. Однако фрагменты этой защиты могут применяться как сопутствующие средства в инженерно-технической и организационной защите. Элемент включает в себя:

• автономные программы, обеспечивающие защиту информации и контроль степени ее защищенности;

• программы защиты информации, работающие в комплексе с программами обработки информации;

• программы защиты информации, работающие в комплексе с техническими (аппаратными) устройствами защиты информации (прерывающими работу ЭВМ при нарушении системы доступа, стирающие данные при несанкционированном входе в базу данных и др.).

Криптографический элемент системы защиты информации предназначен для защиты конфиденциальной информации методами криптографии. Элемент включает:

• регламентацию использования различных криптографических методов в ЭВМ и локальных сетях;

• определение условий и методов криптографирования текста документа при передаче его по незащищенным каналам почтовой, телеграфной, телетайпной, факсимильной и электронной связи;

• регламентацию использования средств криптографирования переговоров по незащищенным каналам телефонной и радиосвязи;

• регламентацию доступа к базам данных, файлам, электронным документам персональными паролями, идентифицирующими командами и другими методами;

• регламентацию доступа персонала в выделенные помещения с помощью идентифицирующих кодов, шифров.

Составные части криптографической защиты, коды, пароли и другие ее атрибуты разрабатываются и меняются специализированной организацией. Применение пользователями собственных систем шифровки не допускается.

В каждом элементе защиты могут быть реализованы на практике только отдельные составные части в зависимости от поставленных задач защиты в крупных и некрупных фирмах различного профиля, малом бизнесе. Структура системы, состав и содержание элементов, их взаимосвязь зависят от объема и ценности защищаемой информации, характера возникающих угроз безопасности информации, требуемой надежности защиты и стоимости системы. Например, в некрупной фирме с небольшим объемом защищаемой информации можно ограничиться регламентацией технологии обработки и хранения документов, доступа персонала к документам и делам. Можно дополнительно выделить в отдельную группу и маркировать ценные бумажные, машиночитаемые и электронные документы, вести их опись, установить порядок подписания сотрудниками обязательства о неразглашении тайны фирмы, организовывать регулярное обучение и инструктирование сотрудников, вести аналитическую и контрольную работу. Применение простейших методов защиты, как правило, дает значительный эффект.

В крупных производственных и исследовательских фирмах с множеством информационных систем и значительными объемами защищаемых сведений формируется многоуровневая система защиты информации, характеризующаяся иерархическим доступом к информации. Однако эти системы, как и простейшие методы защиты, не должны создавать сотрудникам серьезные неудобства в работе, т. е. они должны быть «прозрачными».

Содержание составных частей элементов, методы и средства защиты информации в рамках любой системы защиты должны регулярно изменяться с целью предотвращения их раскрытия заинтересованным лицом. Конкретная система защиты информации фирмы всегда является строго конфиденциальной, секретной. При практическом использовании системы следует помнить, что лица, проектирующие и модернизирующие систему, контролирующие и анализирующие ее работу не могут быть пользователями этой системы.

Вывод: безопасность информации в современных условиях компьютеризации

информационных процессов имеет принципиальное значение для предотвращения незаконного и часто преступного использования ценных сведений. Задачи обеспечения безопасности информации реализуются комплексной системой защиты информации, которая по своему назначению способна решить множество проблем, возникающих в процессе работы с конфиденциальной информацией и документами. Основным условием безопасности информационных ресурсов ограниченного доступа от различных видов угроз является прежде всего организация в фирме аналитических исследований, построенных на современном научном уровне и позволяющих иметь постоянные сведения об эффективности системы защиты и направлениях ее совершенствования в соответствии с возникающими ситуационными проблемами.

Лекция 3

Общая характеристика способов и средств защиты информации. Криптографические методы защиты информации

Учебные вопросы:

1. Анализ и типизация организационных и программно-аппаратных структур автоматизированных систем предприятия
2. Анализ возможных угроз и их специфика в различных типах АС.
3. Систематизация видов защиты информации

Вопрос 1. Анализ и типизация организационных и программно-аппаратных структур автоматизированных систем предприятия

Под автоматизированной системой (АС) понимается человеко-машинная система, предназначенная для решения определенного круга прикладных задач. Большое многообразие областей применения АС, различия по количественному и качественному составу пользователей и обслуживающего персонала, содержанию и характеру обрабатываемой информации определяют специфичные особенности каждой АС и требуют их классификации с целью выработки общих принципов и универсальных решений по защите информации в каждом классе АС.

Учитывая, что реализация систем защиты информации является дорогостоящей задачей, при проектировании систем защиты каждой АС необходимо учитывать специфику угроз и их последствий с целью обоснования и минимизации затрат на разработку и эксплуатацию средств защиты [1].

Возможно несколько взаимодополняющих подходов к классификации АС по области использования, характеру обрабатываемой информации, программно-аппаратной структуре. В табл.1 приведена классификация АС в зависимости от области их использования и уровня конфиденциальности обрабатываемой информации.

Принадлежность к определенному ведомству характеризует степень глобального ущерба, который, в принципе, может быть нанесен в результате утечки или искажения информации, причем нарушение защиты информации в АС гражданских ведомств, как правило, ведет к экономическим потерям, в то время как в оборонных ведомствах приводит также к угрозе национальной безопасности государства.

Таблица 1. Классификация АС

Вид ведомства	Принадлежность объекта по виду собственности	Специализация функций АС	Уровень конфиденциальности обрабатываемой информации	Шифр АС
1 Гражданские	1 Государственные	1 Планирование, управление, надзор, охрана правопорядка	Государственная, служебная	111
		2 Финансовая деятельность, маркетинг	---------/--------	112
		3 Производство	---------/--------	113
		4 Образование, культура	---------/--------	114
		5 Транспорт, связь, информационное обслуживание	---------/--------	115
		6 Научная и проектная деятельность	Государственная, служебная, личная	116
		7 Обслуживание населения	Служебная, личная	117
	2 Частные	1 Планирование, управление, надзор, охрана правопорядка	Государственная, служебная	121
		2 Финансовая деятельность, маркетинг	---------/--------	122
		3 Производство	---------/--------	123
		4 Образование, культура	---------/--------	124
		5 Транспорт, связь, информационное обслуживание	---------/--------	125
		6 Научная и проектная деятельность	Государственная, служебная, личная	126
		7 Обслуживание населения	Служебная, личная	127
2 Оборонные	1 Государственные	1 Планирование, управление, надзор, охрана безопасности	Государственная, служебная	211
		2 Финансовая деятельность, маркетинг	---------/--------	212
		3 Производство	---------/--------	213
		4 Образование, культура	---------/--------	214
		5 Транспорт, связь, информационное обслуживание	---------/--------	215
		6 Научная и проектная деятельность	Государственная, служебная, личная	216
		7 Обслуживание войск	---------/--------	217
	2 Частные	1 Планирование, управление, надзор, охрана безопасности	Государственная, служебная	221
		2 Финансовая деятельность, маркетинг	---------/--------	222
		3 Производство	---------/--------	223
		4 Образование, культура	---------/--------	224
		5 Транспорт, связь, информационное обслуживание	---------/--------	225
		6 Научная и проектная деятельность	---------/--------	226
		7 Обслуживание войск	---------/--------	227

Разделение объектов по виду собственности определяет, какие интересы превалируют при защите информации в АС: государственные или частные, а специализация функций АС в значительной степени определяет специфику угроз в конкретной АС.

Уровень конфиденциальности обрабатываемой информации соотносит ущерб с конкретным владельцем информации. Следует иметь в виду, что владелец информации, разрешая доступ к информации другим субъектам, определяет уровень конфиденциальности информации, что существенным образом сказывается на реализации системы разграничения доступа в АС.

В любой АС могут использоваться персональные ЭВМ (ПЭВМ), системы коллективного пользования (СКП) и вычислительные сети.

Вопрос 2. Анализ возможных угроз и их специфика в различных типах АС

Событие (или действие), которое может вызвать нарушение функционирования АС, называется угрозой. Возможность нарушения нормальной работы АС зависит от наличия в ней уязвимых мест. Количество и специфика уязвимых мест зависит от вида решаемых задач, характера обрабатываемой информации, аппаратно-программных особенностей АС, наличия средств защиты и их характеристик.

Рассмотрим обобщенный перечень возможных угроз, характерный для любой АС. Условно возможные угрозы можно разделить на три группы в соответствии с основными источниками угроз (табл. 2).

Таблица 2. Классификация угроз АС

Источники возможных угроз		
1. Природные	2. Технические	3. Созданные людьми
1.1 Стихийные бедствия 1.2 Магнитные бури 1.3 Радиоактивное излучение и осадки и т.п.	2.1. Отключения или колебания электропитания и других средств обеспечения 2.2. Отказы и сбои аппаратно-программных средств 2.3. Электромагнитные излучения и наводки 2.4. Утечки через каналы связи (оптические, электрические, звуковые) и т.п.	3.1. Непреднамеренные действи - обслуживающего персонала, - управленческого персонала, - программистов, - пользователей АС архивной сл - службы безопасности 3.2. Преднамеренные действия - обслуживающего персонала, - управленческого персонала, - программистов, - пользователей АС архивной сл - службы безопасности, - несанкционированных пользо (военная разведка, коммер шпионаж, диверсии)

Угрозы первой группы независимы от людей. Угрозы подгруппы 1.1 связаны с прямым физическим воздействием на элементы АС (ураганы, наводнения, пожары и т. п.), вызывают нарушения работы АС и физическое уничтожение носителей информации, средств обработки и передачи данных, обслуживающего персонала. Угрозы подгруппы 1.2 связаны с электромагнитным воздействием на магнитные носители информации, электронные средства обработки и передачи данных, обслуживающий персонал и ведут к отказам и сбоям аппаратуры, искажению или уничтожению информации, ошибкам персонала. Угрозы подгруппы 1.3 аналогичны по последствиям угрозам подгруппы 1.2 и, кроме того, ведут к заболеваниям персонала.

Угрозы второй группы связаны с надежностью технических средств систем обеспечения работы АС. Угрозы подгруппы 2.1 связаны с внезапным временным прекращением работы АС и приводят к потерям информации и управления объектами в управляющих АС. Угрозы подгруппы 2.2 связаны с надежностью работы аппаратно-программных средств и ведут к искажению и потерям информации, нарушениям в управлении объектами. Угрозы подгруппы 2.3 связаны с наличием электромагнитных излучений и наводок, посредством которых осуществляется несанкционированный перенос информации за пределы АС, что приводит к утечке информации. Угрозы подгруппы 2.4 связаны с утечкой информации через легальные каналы связи за счет имеющейся возможности снятия ее специальными датчиками или посредством прямого подключения.

Угрозы третьей группы зависят от присутствия людей, как в АС, так и вне ее. Угрозы подгруппы 3.1 связаны со случайными непреднамеренными действиями пользователей, ошибками операторов, программистов, управленческого персонала, сотрудников архивной службы и службы безопасности и ведут к искажению или уничтожению информации, нарушению выполнения АС своих функций, ошибкам в работе программ и средствах управления безопасностью АС. Угрозы подгруппы 3.2 связаны с преднамеренными действиями людей, направленными на нанесение ущерба АС, получение личных привилегий и доходов. Данная группа угроз является наиболее многочисленной. При этом возможны виды угроз:

– маскировка под законного пользователя;

– проникновение в систему управления безопасностью с целью изменения ее

характеристик;

– организация отказа для пользователей в использовании ресурсов;

– передача информации неверному абоненту;

– злонамеренное разрушение ресурсов АС;

– ввод ложных данных;

– незаконное копирование или кража носителей информации, перехват чужих сообщений;

– порождение правдоподобных сообщений или модификация передаваемых сообщений;

– забастовки, саботаж;

– клевета, мистификация угроз, шантаж;

– искажение программ, внедрение вирусов и троянских коней;

– установка разведывательной аппаратуры.

Рассмотрим специфику угроз по отношению к типам конкретных АС, определенным в таблице 1 (см. графу "Шифр АС").

В подклассе 111 вышеуказанные угрозы приводят к потере управления государством, нарушению баланса отраслей, к крупным экономическим потерям на уровне государства, экономическим преступлениям в особо крупных размерах, нанесению ущерба национальной безопасности, престижу государства.

В подклассе 112 реализация угроз наносит экономический ущерб, как на уровне государства, так и межгосударственных отношений. Экономические потери могут быть также значительными. Особенно опасна утечка информации посредством коммерческого шпионажа, разведки, утечки за счет излучений и средств связи.

В подклассе 113 реализация угроз ведет к срыву выполнения производственных программ предприятий, экономическим потерям.

Особенностью данного подкласса АС является использование информации поставщиков, субподрядчиков, потребителей и т. п. различной ведомственной принадлежности, что повышает сложность и значимость защиты в первую очередь от угроз, созданных людьми.

В подклассе 114 наиболее важна защита информации от искажения и обеспечение авторских прав учреждений. Реализация угроз ведет к экономическим потерям.

В подклассе 115 реализация угроз приводит не только к экономическим потерям, утечке и уничтожению информации, но и связана с безопасностью людей (диспетчерские системы и т. п.). Особое внимание следует уделять обеспечению достоверности информации.

В подклассе 116 реализация угроз может приводить к значительным экономическим потерям. Особое значение имеет защита авторского права. Отличительной особенностью данного подкласса является доступ пользователей к большим объемам информации и различным видам информационно-вычислительных сетей.

В подклассе 117 осуществляется обработка информации, связанной с обслуживанием населения, в том числе и медицинским. Особое значение в данном подклассе АС имеет защита личной тайны.

В подклассе 121 реализация угроз ведет к экономическим потерям. Особое внимание следует уделять защите информации о заказах государственных и оборонных ведомств.

В подклассе 122 особое значение имеет реализация угроз со стороны конкурирующих частных организаций (бирж, банков, страховых организаций, рекламных агентств и т. п.). Возможны экономические потери на уровне частных предприятий, отдельных граждан.

В подклассах 123, 124 особенности реализации угроз аналогичны подклассам 113, 114.

В подклассе 125 реализация угроз ведет к экономическим потерям частных организаций и к угрозе безопасности людей. Особое внимание следует уделить безопасности передачи информации при обслуживании государственных и оборонных организаций.

В подклассе 126 особенности реализации угроз аналогичны подклассу 116.

В подклассе 127 особое внимание следует уделить защите личной информации.

В подклассе 211 реализация угроз впрямую связана с ущербом национальной безопасности государства, нарушением управления вооруженными силами, особое значение имеет временной фактор (средства раннего предупреждения, ПВО, управление стратегическими вооруженными силами, силами быстрого реагирования и т. п.).

Экономический ущерб может быть весьма значителен. Обработка информации связана с данными различной степени конфиденциальности.

В подклассе 212 реализация угроз приводит к экономическим потерям. Особое внимание необходимо уделять защите от коммерческого шпионажа со стороны конкурентов (торговля оружием, системами ПВО, военными технологиями и т. п.).

В подклассе 213 реализация угроз связана с национальной безопасностью, экономическими потерями, приоритетами и авторскими правами. Возможен чрезвычайно широкий спектр угроз. Особое внимание необходимо уделять защите информации в связи с использованием значительного числа субподрядчиков.

В подклассе 214 реализация угроз связана с возможностью разглашения в рамках учебного процесса, например тактико-технических данных военной техники, стратегических и тактических планов и технологий и т. п. Особое внимание следует уделять защите от военной разведки, шпионажа. Возможны экономические потери, нанесение ущерба национальной безопасности.

В подклассах 215–217 особенности реализации угроз аналогичны соответственно подклассам 115–117. Кроме того, возможна утечка информации о дислокации войск и вооружений, что ведет к угрозе национальной безопасности.

В подклассе 221 особенности реализации угроз связаны с выполнением оборонных заказов. Возможны экономические потери, как на государственном, так и частном уровне, нанесение ущерба национальной безопасности, престижу фирмы.

В подклассах 222–227 особенности реализации угроз аналогичны подклассам 212–217 соответственно.

Анализ особенностей реализации угроз безопасности информации показывает невозможность разделения систем зашиты по ведомственному принципу, а необходимость использования компьютерных сетей, баз данных коллективного пользования только усугубляет проблему обеспечения безопасности информации.

Вопрос 3. Систематизация видов защиты информации

В практической деятельности по применению мер и средств защиты информации выделяются следующие самостоятельные направления, определяемые в соответствии со сложившимися отраслевыми структурами и видами информационной собственности [2]:

– защита информации от несанкционированного доступа (НСД);

– защита информации в системах связи; – защита юридической значимости электронных документов;

– защита конфиденциальной информации от утечки по каналам побочных электромагнитных излучений и наводок (ПЭМИН);

– защита информации от компьютерных вирусов и других опасных воздействий по каналам распространения программ;

– защита от несанкционированного копирования и распространения программ и ценной компьютерной информации.

Зашита конфиденциальной и ценной информации от несанкционированного доступа (НСД) и модификации призвана обеспечить решение одной из наиболее важных задач защиты имущественных прав владельцев и пользователей ЭВМ – защиту собственности, воплощенной в обрабатываемой с помощью ЭВМ информации, от всевозможных злоумышленных покушений, которые могут нанести существенный экономический и другой материальный и нематериальный ущерб. К ней примыкает задача защиты государственных секретов, где в качестве собственника информации выступает государство. В части

технической реализации защита от НСД сводится к задаче разграничения функциональных полномочий и доступа к информации, при этом под словом "доступ" следует понимать не только возможность потенциального нарушителя "читать" хранящуюся в компьютере информацию, но и возможность модифицировать ее штатными и нештатными средствами (разграничение функциональных полномочий).

Защита информации в системах связи направлена на предотвращение возможности несанкционированного доступа к конфиденциальной и ценной информации, циркулирующей по каналам связи различных видов. В общем случае должны учитываться все виды угроз, возникающих в каналах и коммутационных узлах систем связи. Однако в своей основе данный вид защиты преследует достижение тех же целей, что и защита от НСД: обеспечение конфиденциальности и целостности информации, готовность систем к обслуживанию.

Наиболее эффективным средством защиты информации в неконтролируемых каналах связи является применение криптографии и специальных связных протоколов. Подробнее вопросы защиты информации в системах связи рассмотрены в Главе 4.

Защита юридической значимости электронных документов оказывается необходимой при использовании вычислительных систем и сетей для обработки, хранения и передачи информационных объектов (сообщений, файлов, баз данных), содержащих в себе приказы, платежные поручения, контракты и другие распорядительные, договорные, финансовые документы. Их общая особенность заключается в том, что в случае возникновения споров (в том числе и судебных) должна быть обеспечена возможность доказательства истинности факта того, что автор действительно фиксировал акт своего волеизъявления в отчуждаемом электронном документе. Проще говоря, получатель должен иметь возможность удостовериться в том, что полученный электронный документ действительно создан конкретным человеком, а не был фальсифицирован каким-либо третьим лицом.

В общем случае незащищенные вычислительные системы не обладают свойством подтверждения подлинности и фиксации авторства электронных документов (ЭД), хранящихся в памяти компьютеров или циркулирующих по каналам вычислительных сетей. Для решения данной проблемы могут использоваться современные криптографические методы проверки подлинности информационных объектов, связанные с применением так называемых "цифровых подписей". Эти методы основаны на включении в ЭД специальных меток, логически неразрывно связанных с его текстом, для порождения которых используется индивидуальный секретный криптографический ключ. При наличии индивидуальных криптографических ключей исключается возможность "подделки" таких меток со стороны других лиц. Цифровая подпись может неопровержимо свидетельствовать об авторстве того или иного конкретного лица, и этот факт может быть легко проверен получателем. С другой стороны, наличие цифровой подписи лишает злоумышленника возможности отказаться впоследствии от авторства, т. е. опровергнуть факт действительного подписания им электронного документа.

Защита информации от утечки по каналам побочных электромагнитных излучений и наводок (ПЭМИН) является важным аспектом защиты конфиденциальной и секретной информации в ЭВМ от несанкционированного доступа со стороны посторонних лиц. Данный вид защиты направлен на предотвращение возможности утечки информативных электромагнитных сигналов за пределы охраняемой территории. При этом предполагается, что внутри охраняемой территории применяются эффективные режимные меры, исключающие возможность бесконтрольного использования специальной аппаратуры перехвата, регистрации и отображения электромагнитных сигналов. Для защиты от ПЭМИН широко применяется экранирование помещений, предназначенных для размещения средств вычислительной техники, а также технические меры, позволяющие снизить интенсивность информативных излучений самого оборудования ЭВМ и связи. В последнее время, определенное распространение получил метод электромагнитной маскировки информативных сигналов за счет применения специальных генераторов-излучателей шумов.

В некоторых ответственных случаях может быть необходима дополнительная проверка

средств вычислительной техники на предмет возможного выявления специальных закладных устройств промышленного шпионажа (по своему назначению аналогичных известным телефонным "жучкам"), которые могут быть внедрены туда недобросовестным конкурентом с целью ретрансляции или записи информативных излучений компьютера, а также речевых и других несущих уязвимую информацию сигналов.

Защита информации от компьютерных вирусов и других опасных воздействий по каналам распространения программ приобрела за последнее время особую актуальность. Масштабы реальных проявлений "вирусных эпидемий" оцениваются сотнями тысяч случаев "заражения" персональных компьютеров во всех странах, в том числе и в России. Хотя некоторые из вирусных программ оказываются вполне безвредными, многие из них имеют разрушительный характер, как показан, например, случай с вирусом 5COKE5, буквально опустошившим тысячи персональных компьютеров в США. Особенно опасны вирусы для компьютеров, входящих в состав однородных вычислительных сетей.

Некоторые особенности современных вычислительных систем создают благоприятные условия для распространения вирусов, К ним, в частности, относятся: необходимость совместного использования программного обеспечения, многими пользователями, трудность ограничения в использовании программ, ненадежность существующих механизмов защиты и разграничения доступа к информации в отношении противодействия вирусу.

Как правило, рассматриваются два направления в методах защиты от вирусов: применение "иммуностойких" программных средств, защищенных от возможности несанкционированной модификации (разграничение доступа, методы самоконтроля и самовосстановления); применение специальных программ-анализаторов, осуществляющих постоянный контроль возникновения "аномалий" в деятельности прикладных программ, периодическую проверку наличия других возможных следов вирусной активности (например, обнаружение нарушений целостности программного обеспечения), а также "входной" контроль новых программ перед их использованием (по характерным признакам наличия в их теле вирусных образований). Так как первое направление трудно поддается практической реализации, то в большинстве случаев реальные антивирусные средства базируются на втором подходе.

Защита от несанкционированного копирования и распространения программ и ценной компьютерной информации является самостоятельным видом защиты имущественных прав, ориентированным на проблему охраны интеллектуальной собственности, воплощенной в виде программ ЭВМ и ценных баз данных. Лица, занимающиеся "программным пиратством" и извлекающие в обход требований авторского права доход от перепродажи программ без соответствующих отчислений в пользу автора, наносят тем самым большой вред нормальному развитию рыночных экономических механизмов в области разработки отечественного программного обеспечения.

Защита от несанкционированного копирования и распространения программ обычно осуществляется с помощью специальных программных средств, подвергающих защищаемые программы предварительной обработке (вставка парольной защиты, проверок по обращению к устройствам хранения ключа и ключевым дискетам, блокировка отладочных прерываний, проверка рабочей ЭВМ по ее уникальным характеристикам и т. п.), которая приводит исполнимый код защищаемой программы в состояние, препятствующее его выполнению на "чужих" машинах. В некоторых случаях для повышения защищенности применяются дополнительные аппаратные блоки (ключи), подключаемые к разъему принтера или к системной шине ПЭВМ, а также производится шифрование файлов, содержащих исполнимый код программы.

Общим свойством средств защиты программ от несанкционированного копирования является ограниченная стойкость такой защиты, так как в конечном случае исполнимый код программы поступает на выполнение в центральный процессор в открытом виде и может быть прослежен с помощью аппаратных отладчиков. Однако это обстоятельство не снижает потребительские свойства средств защиты до нуля, так как основной целью их применения

является в максимальной степени затруднить, хотя бы временно, возможность массового тиражирования новых изданий программных средств до появления последующих изданий.

Лекция 3
Основные направления обеспечения информационной безопасности компьютерных сетей учебных заведений

Учебные вопросы:
1. Состояние вопросов обеспечения информационной безопасности.
2. Угрозы и уязвимости КСУЗ.
3. Этапы построения БКСУЗ.
4. Направление исследований

Введение

В настоящее время противоречие между требованиями к защите ресурсов компьютерных сетей учебных заведений (КСУЗ) и ростом компьютерных преступлений определяет одну из важных задач – построение интегрированной системы безопасности КСУЗ. Данная проблема включает в себя комплексное решение задач определения нормативно-правовой базы, формирование концепции безопасности, разработку мероприятий, планов и процедур по безопасной работе, проектирование, реализацию и сопровождение технических средств защиты информации в процессе обучения. Несмотря на видимую схожесть задач защиты корпоративных сетей и компьютерных сетей вузов, задача по обеспечению безопасности вузовских сетей не получила окончательного решения и, в рамках динамичности развития процесса безопасности информационных технологий, находится в процессе постановки.

Кроме общих проблем внедрения технологий безопасности для вузовских сетей можно отметить две специфические:

– отсутствие единой технической политики информационной безопасности (ИБ) в области образования, в том числе унифицированных вузовских технологий;

– в вузах, как известно, сосредоточены наиболее вероятные потенциальные нарушители безопасности компьютерных систем.

Решение задач ИБ осложняется: текучестью кадров, разнородностью специалистов, большим количеством пользователей, отсутствием больших финансовых ресурсов, часто, недооценкой вопросов физической защиты и обработкой условно (декларировано) открытой информации.

В данной работе рассмотрены проблемные вопросы и общие направления построения интегрированной системы безопасности КСУЗ.

Вопрос 1. Состояние вопросов обеспечения информационной безопасности

В настоящее время вопросы ИБ в вузах стали принимать все более актуальное значение. Следует вспомнить, что проблема компьютерных правонарушений зародилась именно в вузах (например, вирус Морриса). По оценкам МВД число компьютерных преступлений за предыдущий год в России возросло в 4 раза. Анализ сообщений в Интернет относительно уголовных правонарушений по статьям компьютерных преступлений показал, что фактически все они были совершены студентами. Кроме того, множество инцидентов находятся на грани компьютерных преступлений. Помимо сетевых атак, в последнее время возникло такое явление, как информационное противостояние студентов в Интернет, например: ведение неофициальных сайтов вузов (mgtu.ru), выкладывание компрамата на преподавателей, «реферативная» поддержка и т. д.

В настоящее можно насчитать около двух десятком вузов, где активно ведутся работы в области ИБ и создали подготовку по специальностям ИБ. Пять вузов имеют действительные лицензии Гостехкомиссии России на преподавание спецкурсов, а также разработку средств защиты информации. Однако в большинстве вузов вопросам всестороннему обеспечению ИБ уделяют недостаточное внимание. Представленный в Интернет обзор по ИТ-технологиям в вузах (http://www.cnews.ru/education) позволяет сделать вывод, что их внедрение находится на самом раннем этапе развития.

Вопрос 2. Угрозы и уязвимости КСУЗ

Под КСУЗ понимается совокупность рабочих станций и устройств, использующих общие сетевые ресурсы и сетевые услуги в интересах учебной деятельности. Следует отметить, что современные КСУЗ являются чрезвычайно неоднородными по своей сути. Однако их можно разделить на:

– большие объединенные гетерогенные TCP/IP-сети вуза, поддерживаемые на уровне технологий различными западными компаниями (например, Learning Space), в таких вузах как, правило имеются соответствующие учебные центры;

– ЛВС или объединение ЛВС с выходом в Интернет;

– изолированные от Интернет ЛВС и АРМ.

Под безопасностью КСУЗ понимается свойство системы быть защищенной от угроз целостности, доступности и конфиденциальности сетевых ресурсов. Под угрозой обычно понимается некоторое потенциальное событие (нарушение), реализация которого способно привести к снижению степени безопасности ресурсов КСУЗ. Преднамеренную реализацию в сетевой среде угроз ИБ принято называть атакой на ресурсы сетей. При этом известны классификации угроз ИБ на внутренние и внешние, преднамеренные и случайные, реализационные и эксплуатационные и др… К наиболее актуальным сейчас угрозам относят наличие уязвимостей (дефектов безопасности) в программных ресурсах, на базе которых реализуется до 98 % сетевых атак и 99 % вирусных эпидемий. Очевидно, что для КСУЗ наиболее типовыми являются внутренние угрозы.

Вопрос 3. Этапы построения БКСУЗ

Задача построения интегрированной системы безопасности КСУЗ в общем случае включает 3 уровня:

1. Определение законодательно-правовой базы;
2. Разработку организационных документов, мер и процедур;
3. Разработку, внедрение, сопровождение подсистем и средств защиты информационно-программных ресурсов.

Определение законодательно-правовой базы

Пакет правовых документов в области ИБ, главным образом, включает: Уголовный кодекс РФ, Гражданский кодекс РФ, ФЗ «О правовой охране программ для электронных вычислительных машин и баз данных», ФЗ «О сертификации продуктов и услуг», ФЗ "О

Государственной тайне", ФЗ "Об информации, информатизации и защите информации", ФЗ "Об электронной цифровой подписи", Указ Президента РФ "Об утверждении перечня сведений конфиденциального характера". В целом законодательная база учебной деятельности касается определения необходимости лицензий на деятельность в сфере ИБ, использования сертифицированных средств, соблюдения соответствующих требований УК РФ и ФЗ РФ. Следует заметить, что в связи с реформой системы лицензирования несколько упрощены требования некоторым видам деятельности и услугам в области ИБ.

К нормативным документам в области ИБ относят РД Гостехкомиссии РФ и следующие стандарты:

– ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования;

– ГОСТ 45.127-99. Система обеспечения информационной безопасности Взаимоувязанной сети связи РФ. Термины и определения;

– ГОСТ 51583-2000. Порядок создания АС в защищенном исполнении. Общие положения;

– ГОСТ Р 34.10–94. ИТ. Криптографическая защита информации. Процедуры выработки и проверки электронной подписи на базе асимметричного криптографического алгоритма;

– ГОСТ Р 34.11–94. ИТ. Криптографическая защита информации. Функция хэширования;

– ГОСТ Р 50739-95. СВТ. Защита от НСД к информации;

– ГОСТ Р 50922-96. ЗИ. Основные термины и определения; – ГОСТ Р 51188-98. Испытания ПС на наличие компьютерных вирусов;

– ГОСТ Р 51275-99 ЗИ. Объект информатизации. Факторы, воздействующие на информацию;

– ГОСТ Р 51624-00. ЗИ. АС в защищенном исполнении. Общие требования;

– ГОСТ Р ИСО/МЭК 15409-2001. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ;

– ГОСТ Р ИСО 7498-2-99. ИТ. ВОС. Базовая эталонная модель. Часть 2. Архитектура защиты информации;

– ГОСТ Р ИСО/МЭК 9594-8-98. ИТ. ВОС. Справочник. Часть 8. Основы аутентификации;

– ГОСТ Р ИСО/МЭК 9594-9-95. ИТ. ВОС. Справочник. Часть 9. Дублирование. ГОСТ Р ИСО/МЭК 15408-2001. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ.

Особое внимание представляет международный ГОСТ 15408, планируемый на смену РД Гостехкомиссии РФ. ГОСТ 15408 предназначен для анализа и оценки безопасности и качества ИТ и СЗИ. ГОСТ определяет типовые требования к функциям безопасности (девять классов, 76 семейств, 184 компонента и 380 элементов), требования доверия безопасности – семь классов, 25 семейств, 72 компонента, и 9 уровней гарантии. Типовой алгоритм оценки ИБ по ГОСТу представлен на рис. 1.

Организационные меры

Организационные меры в общем случае включают:

1. Проведение аудита ИБ КСУЗ и экспертиза вуза по требованиям безопасности;

2. Определение политики и процедур безопасности;

3. Рекомендации по настройке сетей и систем.

Организационно-техническими документами здесь являются: – стандарт ISO 17799 (BS 7799) по аудиту информационной безопасности и частично стандарты РФ по аккредитации, ИБ, качеству;

– политика (положение) безопасности, реестр анализа риска, планы защиты и восстановления;

– руководства по настройке, детальные инструкции, как-то: Stepbystep (cert.org),

инструкции Stiv Substen (www.trustedsystem.com) и др.

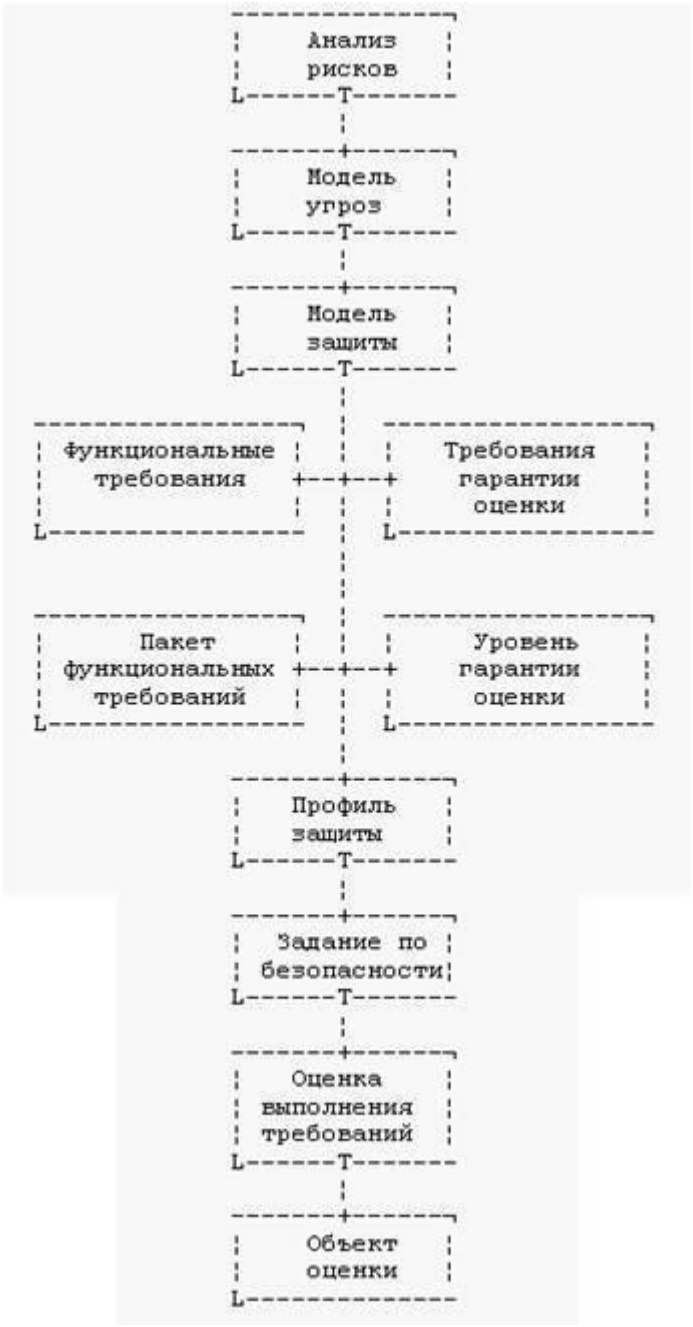

Рис. 1. Типовой алгоритм оценки ИБ

В первой части документов особо выделяют международный стандарт ISO 17799, к сожалению не имеющего аналога в РФ. Указанный стандарт определяет типовые решения по: классификации и управлению ресурсами, безопасности персонала (в т. ч. обучению), физической безопасности, управлению коммуникациями и процессами, контролю доступа, разработке и технической поддержке вычислительных систем, управлению непрерывностью бизнеса, соответствию системы основным требованиям нормативных документов.

Таблица 1. Разработка политики безопасности

№	Мероприятия	Уровень	Документ
1	Разработка политики безопасности	Управления (администрирования)	Политика безопасности (security policy)
2	Проведение анализа рисков		Реестр рисков (risk report)
3	Планирование обеспечения информационной безопасности	Управления (планирования)	План защиты (security plan)
4	Планирование действий в чрезвычайных ситуациях		План обеспечения непрерывной работы и восстановления функционирования ИС (contingency and recovery plan)

Наиболее применительным является подход, определенный в ISO 17799 – CRAMM. Данный подход включает: определение ценности ресурсов (1-10 баллов), оценка угроз (36 классов), уязвимостей, уровней риска (1–5, 1–3, 1–7 баллов), Поиск адекватных контрмер, рекомендаций и примеров (300, 1000, 900).

Таблица 2.
Основные документы

Политика безопасности	План защиты	План обеспечения непрерывной работы и восстановления	
		Меры реагирования на нарушения	Восстановительные раб
1.Основные положения информационной безопасности. 2.Область применения. 3.Цели и задачи обеспечения информационной безопасности. 4.Распределение ролей и ответственности. 5. Общие обязанности.	1.Общие положения, отражающие политику безопасности. 2.Текущее состояние системы и ее уязвимость. 3.Рекомендации по реализации системы защиты. 4.Ответственность персонала. 5.Порядок ввода в действие средств защиты. 6.Порядок пересмотра средств защиты.	1.Основные положения. 2.Оценка инцидента. 3.Оповещение. 4.Ответные меры. 5.Правовой аспект. 6.Регистрационная документация.	1.Оперативный ресмотр полити 2.Устранение бостей. 3.Усвоение уро 4.Совершенств ние политики процедур.

В основе планов по ИБ лежат описание процедур безопасности: проверка системы и средств безопасности, управление паролями, управление счетами, поддержка пользователей, сопровождение программного обеспечения, конфигурационное управление, резервное

копирование, управление носителями, документирование.

Технические вопросы

При решении технических вопросов принято разделять систему безопасности КСУЗ на подсистемы. Это связано с классами актуальных угроз, сложившийся рынок средств и технологий ИБ и требования нормативных документов – Руководящих документов Гостехкомиссии РФ по защите информации от НСД АС, СВТ, МЭ и ГОСТ Р ИСО/МЭК 15408 (ИТ. Методы и средства ОБИ. Критерии оценки безопасности ИТ).

Выделяют основные подсистемы, криптографические, защиты распределенных ресурсов, а также защиты инфраструктуры.

Основными подсистемам являются:

1. Идентификация и аутентификация;
2. Разграничение доступа;
3. Протоколирование и аудит;
4. Обеспечение целостности данных;
5. Защита от разрушающих программных средств.

Криптографические подсистемы разделяют на:

6. Шифрование;
7. Обеспечения целостности данных;
8. Криптографическая аутентификация и инфраструктура;

Подсистемы безопасности распределенных систем:

9. Межсетевое экранирование;
10. Виртуальные частные сети;
11. Анализ защищенности;
12. Предупреждение об НСД.

Безопасность инфраструктуры и физическая безопасность:

13. Защита от несанкционированного копирования программ;
14. Гарантированное хранение и восстановление данных;
15. Безопасность электропитания;
16. Безопасность кабельной системы и др.

Отметим принципиальные особенности указанных подсистем.

Подсистема идентификации и аутентификации предназначена для именования ресурсов и проверки подлинности субъектов сети. Около 80 % инцидентов в сети связано с уязвимостью указанной подсистемы. В настоящее время подсистему подразделяют на одноразовые/многоразовые параольные системы, системы, основанные на использовании уникальных устройств (карточек), биометрические устройства.

Основной подсистемой ИБ принято считать систему разграничения доступом. В настоящее время выделяют дискретный и мандатный принципы разграничения доступом, как основные, и различные их расширения: изолированная программная среда, контроль потоков, ролевое управление и др. Следует помнить, что в сетях, обрабатывающих информацию, составляющую гостайну, должен быть реализован мандатный принцип разграничения доступом.

Подсистема протоколирования является важнейшей в КСУЗ. Помимо технического предназначения, она представляет моральное ограничение – нарушители должны знать, что их действия будут зафиксированы. Выделяют встроенные системы протоколирования, системы аудита и активного аудита.

Основной системой обеспечения управления доступом на уровне сети является подсистема межсетевого экранирования. Принципиальным компонентом защиты АРМ является сочетание персонального МЭ с антивирусными средствами и средствами контроля целостности.

Среди антивирусных средств и средств контроля целостности традиционно выделяют продукты Лаб. Каперского и ДиалогНауки, считающимися одними из лучших в мире (в

классе АРМ.ЛВС).

Одной из актуальных подсистем ИБ выделяют подсистему отслеживания уязвимостей (bug-tracking). Как указывалось, подавляющее большинство атак основаны на опубликованных уязвимостях. Учитывая любознательность современных учащихся, указанная подсистема безопасности является одной из решающих в обеспечении ИБ КСУЗ. В настоящее время выделяется общедоступных БД по уязвимостям:

– Common Vulnerabilities & Exposures dictionary (cve.mitre.org/cve)
– CERT Vulnerability Notes Database (cert.org)
– SecurityFocus (securityfocus.com)
– ISS X-Force Threat and Vulnerability Database (iis.net/force)
– Computer Incident Advisor Capability (cias.com)
– Microsoft
– SecurityLab (РФ).

Принципиальной особенность вузовской сети должно быть наличие средств анализа защищенности и обнаружения атак. К сожалению, коммерческие продукты порою недоступны для закупки вузами. Поэтому, для построения безопасной КСУЗ приходится использовать бесплатные или условно бесплатные версии.

Кроме названных подсистем, в вузовских сетях отдельно выделяют задачи защиты отдельных сервисов. К таким сервисам, видимо можно отнести, защиту эл. почты, web-серверов, дистанционных курсов.

При организации дистанционного обучения в сети Интернет могут быть реализованы подсистемы VPN и, в перспективе, PKI.

Одним из новых подсистем ИБ относят системы эмулирование (Honey pot), включающие мониторы портов (Port monitors), эмуляторы служб (Deception systems), эмуляторы систем (Full systems).

Вопрос 4. Направление исследований

В нормативно-правовой сфере:

1. Определение базовых требований правовых документов применительно к построению КСУЗ;

В организационной сфере:

1. Определение общих требований стандарта ISO 15408 применительно к типовым КСУЗ;
2. Общие принципы формирования политики безопасности КСУЗ;
3. Разработка алгоритма, рекомендации и средства автоматизации проведения анализа риска КСУЗ;
4. Разработка общих принципов построения планов защиты и восстановления КСУЗ, определение процедур обеспечения безопасности;
5. Разработка типовых рекомендаций по настройке и конфигурированию КСУЗ на базе ОС линии Windows и Linux, имеющих доступ к сети Интернет (на базе технологий, используемых нарушителями);

В технической сфере:

1. Проведение аналитического обзора современных средств защиты информации и выдачу рекомендаций по их использованию.
2. Разработка прототипа защищенной КСЗИ.

Лекция 4
Защита информации от компьютерных вирусов и других опасных

воздействий по каналам распространения программных средств

Учебные вопросы:

1. Юридические и организационные меры защиты.

2. Программно-аппаратные методы и средства защиты.

3. Защита программ и ценных баз данных от несанкционированного копирования и распространения.

Вопрос 1. Юридические и организационные меры защиты

Юридические средства защиты сводятся, в основном, к административной и уголовной ответственности за умышленное создание и распространение вируса или «троянских коней» с целью нанесения ущерба Трудность их применения состоит: в доказательстве авторства умышленности создания таких программ. Так как автора «троянского коня» найти легче, то юридическое преследование их авторов проще юридического преследования авторов вирусов, но и здесь встреча большие трудности.

Отметим некоторые законы, применяемые в США, Великобритании, Германии и Франции для борьбы с компьютерными преступлениями, под действие которых подпадают многие распространители вирусов и "троянских коней":

– Закон о поддельных средствах доступа, компьютерном мошенничестве и злоупотреблении (США);

– Федеральный закон о частной тайне (США):

– Закон о предупреждении экономических преступлений (Германия);

– Закон об авторском праве (Германия);

– Федеральный закон о защите данных (Германия);

– Закон об авторском праве (Великобритания);

– Закон о защите данных (Великобритания);

– Закон об обработке данных, о файлах данных и личных свободах (Франция).

Соответствующие статьи введены в уголовные кодексы ряда стран.

Вышеперечисленные законы позволяют вести достаточно эффективную борьбу с изготовителями вирусов и "троянских коней".

Все организации, где, так или иначе, имеет место проблема вирусов, можно разделить на две группы: разрабатывающие и эксплуатирующие программное обеспечение. В случае смешанных организаций для успешной борьбы с вирусами и "троянскими конями" необходимо стремиться разделить функции подразделений, занимающихся разработкой и эксплуатацией. В свою очередь, вирус или троянский конь может поступать извне или создаваться внутри подразделения.

В подразделениях, связанных с эксплуатацией (использованием) программного обеспечения, можно и необходимо применять более жесткие административные и организационные меры по сравнению с разрабатывающими подразделениями. Это чаше всего оказывается возможным, так как в эксплуатирующих подразделениях собственная разработка программного обеспечения обычно не проводится, и новые программы они получают от разработчиков. С другой стороны, наличие вируса или "троянского коня" в эксплуатируемой системе зачастую приводит к гораздо более тяжелым последствиям, так как здесь обрабатывается реальная информация.

Рассмотрим способы проникновения вируса или "троянского коня" в эксплуатируемую систему:

1) поступают вместе с программным обеспечением, предназначенным для последующего использования в работе. Вероятность такого проникновения вирусов и "троянского коня" можно свести практически к нулю, если разработать правильные процедуры приема программ к эксплуатации и контроля за внесением изменений и появлением новых версий. Процедура приемки должна быть достаточно продолжительной и

всесторонней, в нее должны быть включены специальные операции по провоцированию известных вирусов и "троянских коней";

2) приносятся персоналом с программами, не относящимися к эксплуатируемой системе. Вероятность такого проникновения можно уменьшить путем запрета на приобретение и запуск программ, исключая те, которые прошли специальную процедуру проверки. К сожалению, этот запрет не всегда выполняется. Возможен частичный запрет на использование посторонних программ на определенном оборудовании;

3) преднамеренно создаются обслуживающим персоналом. Вероятность создания вируса или "троянского коня" можно существенно уменьшить, если с достаточным вниманием относиться к контролю за деятельностью персонала вычислительных центров, разработчиков программного обеспечения и конечных пользователей. Одним из наиболее важных условий, способствующих снижению мотивации в создании вирусов и "троянских коней" внутри организации, является хороший моральный климат и правильная кадровая политика, а также справедливая оплата выполняемых работ в соответствии с их качеством и количеством.

Источник вируса легко выявляется, если в эксплуатируемой системе производится разграничение доступа пользователей к привилегированным функциям и оборудованию, присутствуют надежные средства регистрации процессов всего технологического цикла, включая регистра внутримашинных процессов. Особенно важными являются разграничения доступа в вычислительных сетях.

Для быстрого устранения последствий заражения в каждой организации должны иметься копии используемого программного обеспечения. Надежная связь со специалистами из разрабатывающего подразделения из собственной группы позволит быстро разобраться в экстремаль ситуации и выработать подходящие средства для ее устранения.

Для разрабатывающих подразделений, по сравнению эксплуатирующими, характер применения административных организационных мер должен быть другим, поскольку чрезмерное администрирование приводит к существенному снижению темпов качества разработки программных систем. При существующей ситуации программисты-разработчики постоянно сталкиваются с вирусами и "троянскими конями" из-за копирования друг у друга общесистемного программного обеспечения. Такое копирование является в большинстве случаев единственным способом повышения эффективности программиста.

Возможны два пути проникновения вируса или "троянского кон разрабатывающие подразделения:

– вместе с программным обеспечением, скопированным у других программистов;

– преднамеренное создание вируса программистом. Поскольку принципиально невозможно исключить появление вирусов в разрабатывающих подразделениях, административные и организационные меры должны быть направлены на снижение вероятности их появления. Все они регламентируют работу с поступающим программным обеспечением, которое должно проходить через этап предварительного контроля. На этом этапе осуществляется:

– карантин на вновь поступающие программные средства с провоцирования появления возможного вируса или "троянского коня";

– контроль программных средств на известные типы вирусов.

Этап предварительного контроля может быть не оформлен о организационно, но должен присутствовать обязательно, и может проходить на рабочем месте каждого программиста.

Большинство антивирусных программ просты в использовании. Минимальный их комплект должен находиться на каждом компьютере. Если регулярно происходят крупные поставки программного обеспечения, то выделяется компьютер, специально предназначенный для проверки вновь поступающих программ.

Из состава квалифицированных программистов создается "антивирусная" группа, ответственная за планирование и реализацию соответствующих мероприятий. При оценке

работы этой группы следует в большей степени учитывать общий ущерб, нанесенный программам, чем число успешно ликвидированных вирусов и "троянских коней" (по аналогии с оценкой труда пожарных).

В разрабатывающих подразделениях рекомендуется применять следующие меры, снижающие вероятность появления и распространения вирусов и "троянских коней":

– разграничение доступа программистов к оборудованию, в том числе к сетевому. На ЭВМ коллективного пользования желательно разделить между пользователями совместно используемые ресурсы. Например, разбить винчестер на логические диски, а если такой возможности нет, то каждому из пользователей необходимо завести свой каталог и только в нем вести работы. По окончании работы каждый оператор обязан очистить оперативную память и совместно используемые участки диска от своих программ и данных;

– запрет на использование некоторых видов программ, никогда не применяемых для работы (например, игровых). Эта мера, против которой теоретически никто не возражает, практически нигде не выполняется;

– наличие достаточного числа резервных копий программного обеспечения. После окончания проверки программное обеспечение должно быть скопировано, защищено от записи и помещено в соответствующий фонд;

– наличие у каждого программиста средств, необходимых для диагностики и борьбы с вирусами и "троянскими конями";

– проведение семинаров с целью обучения методам борьбы с вирусами и "троянскими конями".

Возможно создание вируса или "троянского коня" внутри разрабатывающего подразделения. Контроль над этим процессом затруднен, так как любой программист, достигнув определенной квалификации, в состоянии сделать это. Как и в эксплуатирующих подразделениях, основные средства, направленные против создания вирусов и "троянских коней" в данном случае – хороший моральный климат в коллективе и оплата, соответствующая проделанной работе. Необходимо создавать и поддерживать в коллективе общественное мнение, осуждающее создание и запуск вирусов и "троянских коней".

Вопрос 2. Программно-аппаратные методы и средства защиты

В современных персональных ЭВМ реализован принцип разделения программных и аппаратных средств. Поэтому программные вирусы и «троянские кони» не могут эффективно влиять на аппаратуру, исключением случаев, когда разработчику вируса удается:

– подобрать частоту обращения к устройствам ЭВМ, имеющим движущиеся части (диски, печать), близкую к резонансной;

– усилить яркость части экрана для прожигания люминофора;

– зациклить программу так, чтобы она использовала минимальное число оборудования (например, одну микросхему) с целью его разогрева и вывода из строя.

Такие способы воздействия на аппаратуру являются маловероятными, и поэтому аппаратные средства могут стать верным помощником в борьбе с вирусами и "троянскими конями".

Вирус или "троянский конь" может портить информацию, содержащуюся в КМОП (CMOS) памяти компьютеров и влияющую загрузку операционной системы. Эта память питается от батареи, информация сохраняется при выключении питания. В случае обнаружения такого эффекта необходимо произвести повторную начальную установку параметров компьютера с помощью процедуры SETUP. Эта процедура значительно упростится, если параметры будут записаны заранее.

Перечислим некоторые из аппаратных методов защиты:

– блокировка возможности записи путем заклеивания (закрывания) отверстия защиты записи дискеты. При отсутствии наклеек можно использовать любую липкую ленту или

просто закрывать отверстие достаточно длинной бумажкой, вставляя ее вместе с дискетой в прорезь дисковода. Данный способ прост и надежен, но имеет ограниченное применение. Ограниченность объясняется следующими причинами: большинство программных систем работают с винчестером, а не с гибкими дисками, системы, работающие с гибкими дисками, часто сами осуществляют запись на дискету;

– физическая блокировка ключом клавиатуры ЭВМ – этот метод похож на способ разграничения доступа административными мерами. Как и все запретительные меры, лишь частично разрешает проблему. Применим в сочетании с другими методами;

– форматирование диска и перезагрузка операционной системы с восстановлением программ с незараженных копий. Недостатками этого метода являются потеря файлов, у которых нет незараженных копий, и значительные потери времени. При наличии копий и времени – это самый надежный способ борьбы с вирусами, но если повреждение информации произошло от невыявленных вирусов или "троянских коней", которые хранятся в копиях программ, то и такая радикальная мера может не привести к успеху.

Следующие способы основаны на аппаратной поддержке операционной системы и ее контролирующих средств:

– запрет или регистрация попыток записи в файлы операционной системы и в области памяти, занятые системной информацией;

– установление приоритета в обработке программ, составляющих операционную систему и антивирусных средств, иерея программами пользователей:

– разделение областей памяти, в которых работают программы, невозможность записи в чужую область памяти:

– выделение некоторых возможностей ЭВМ, которые могут быть реализованы только программами операционной системы.

К сожалению, аппаратная поддержка контролирующих средств отсутствует в персональных ЭВМ, совместимых с IBM PC, что создает хорошие предпосылки для распространения вирусов и действия "троянских коней".

Некоторые западные фирмы приступили к созданию противовирусных компьютеров, у которых есть специальная аппаратная поддержка против вирусов и "троянских коней".

По сообщению журнала "Computer age" (январь 1989 г.) фирма “American Computer Security Industries” (г. Нэшвилл, штат Теннеси, США) представила первый надежно защищенный противовирусный компьютер, названный "Immune system" ("Иммунная система"). Это персональный компьютер на базе процессора i-80286, работающий в операционной системе MS-DOS. Этот компьютер обладает иммунитетом от вирусной атаки, а также полным набором средств, предохраняющих его и хранящиеся в нем данные от любого внешнего или внутреннего вмешательства.

Фирма "Zeus" поставляет дополнительную плату Immunetec PC (цена 295 дол.) для установки в компьютерах, совместимых с IBM PC. С помощью этой платы, в процессе загрузки операционной системы проверяются MBR, Boot-сектор и системные файлы. Плата совместима с сетями Nowel, 3COM, Token Ringи позволяет предотвращать загрузку и устанавливать уровень доступа.

Фирма "Micronyx" поставляет дополнительную плату Trispan (цена 895 дол.). С помощью платы производится контроль зараженности системных файлов, контроль доступа, шифрование данных и регистрация попы обращения к данным. Плата может использоваться в сетях.

Фирма "БИС" (г. Донецк) выпускает плату Port Watch Card, которая вместе с программой IWP предупреждает об опасных действиях с портами контроллеров жестких и гибких дисков, а также о записи в память CMOS.

В настоящее время на рынке имеется довольно большое число специальных антивирусных программных средств. На Западе создано и предлагается большое число программных средств антивирусного направления, однако их рынок характеризуется определенной спецификой. Крупные фирмы-производители программного обеспечения

(такие, как "Microsoft", "Lotus" и "Ashton-Tate") явно отсутствуют на рынке. Большинство программ защиты от вирусов разработаны небольшими компаниями или частными лицами.

На отечественном рынке также нет недостатка в антивирусных средствах. Ряд из них имеет хорошую репутацию, пользуется популярностью у потребителей. В большинстве случаев эти средства также разработаны индивидуально или небольшими группами программистов.

Рассмотрим требования, которым должны отвечать антивирусные средства зашиты:

– вхождение в состав операционной системы;

– способность самоконтроля, так как они работают в более "агрессивной" среде, по сравнению с программами других типов.

Приведем некоторые рекомендации, которые необходимо учитывать при создании антивирусных средств. Антивирусные программы должны:

– проводить самотестирование в момент загрузки программы, так как после этого дискета с исходным модулем может быть извлечена из накопителя;

– учитывать возможность уменьшения размеров программы после заражения из-за упаковки вирусом части программного кода;

– выявлять замаскированное вирусом изменение длины программы, если оно проводится стандартными средствами. Следует контролировать размер программы различными способами и дополнительно определять значения некоторых байт программного модуля;

– учитывать возможность шифрования вирусом собственного "тела" и части зараженной программы;

– выявлять возможность нестандартного расположения вируса относительно заражаемой программы;

– определять наличие в теле вируса изменяющихся кодов.

Операционная система MS DOS не создает серьезных препятствий для существования вирусов. Полностью совместимые с ней операционные системы DR DOS и HI DOS несколько более вирусоустойчивы, но и они "прозрачны" для большинства вирусов. Повышенная вирусоустойчивость возникает из-за изменения внутреннего содержания этих операционных систем при сохранении пользовательского интерфейса. Вирусы, использующие нестандартные способы обращения к операционной системе, могут не работать на ее аналогах.

В операционной системе OS/2 введены средства регламентации при доступе к файлам и изменены внутренние характеристики. Это должно сдерживать распространение вирусов в этой среде, пока не появятся их модификации, учитывающие изменения. Но в этой сложной и относительно новой операционной системе могут содержаться ошибки и непредусмотренные возможности, которые могут быть использованы разработчиками вирусов.

Определенное внимание привлекает к себе проблема своевременного обнаружения и ликвидации компьютерных вирусов. Как и в медицине, гораздо проще предупредить заражение компьютера, чем "лечить" его. В связи с этим получили широкое распространение специальные программы диагностики наличия вирусов в прикладном программном обеспечении – так называемые вирус – детекторы, определяющие факт присутствия вирусов по характерным признакам (фрагменты кода), специфическим для каждого типа вируса. Для этого в программе вирус – детектора содержится набор образцов – сигнатур конкретных вирусов, и только такие вирусы сможет находить данный вирус-детектор. При появлении новых типов, а иногда и новых версий вирусов необходимо выпускать и новые версии вирус – детекторов, "обученные" распознаванию новых вирусов.

Очевидно, что задача создания универсальной программы вирус – детектора, которая бы определяла наличие любых вирусов в программных файлах типов COM или EXE, практически неразрешима. Наиболее целесообразным путем обнаружения вирусов в программных средствах было бы, по-видимому, создание псевдоуниверсального комплекса

тестирования пакетов программных продуктов.

Комплекс проверки на вирус должен включать в себя три компонента:

– программу поиска вируса по его сигнатуре;

– программу выделения сигнатуры вируса на основе сравнения незараженного командного процессора с зараженным;

– банк сигнатур вирусов, созданный другой программой экстрактором.

Механизм обнаружения прост: программа поиска вируса по его сигнатуре перебирает все образцы сигнатур в банке вирусов. Для каждого вируса осуществляется сканирование всех программных файлов (операция поиск подстроки по заданному контексту – сигнатуре). Если при этом операция поиска окажется успешной и заданный контекст будет обнаружен в каком-нибудь программном файле, то можно с уверенностью сказать, что тестируемая программа заражена вирусом, сигнатура которого обнаружена. Задача обнаружения вируса решается в настоящее время загрузкой в оперативную память ПЭВМ резидентных программ, контролирующих обращение к системным функциям операционной системы:

– обращение к магнитным дискам (как с помощью диспетчера операционной системы, реализующего и поддерживающего файловую систему, так и на уровне базовой системы ввода-вывода);

– попытки оставить в оперативной памяти ПЭВМ программу, имеющую статус резидентной.

В процессе функционирования ПЭВМ резидентная программа "надсмотрщик" будет отслеживать указанные выше критические ситуации и перед их возникновением информировать пользователя о предстоящей попытке какой бы то ни было программы совершить указанные действия. Кроме того, программа "надсмотрщик" сделает запрос пользователю о разрешении выполнения действия или о блокировке системы. Резидентная программа протоколирует свои действия с той целью, чтобы при анализе деятельности вычислительной среды системным программистом на предмет обнаружения в ней наличия вируса была под рукой вся необходимая информация ("трассировка") о поведении и событиях в вычислительной среде.

В общем случае, существуют следующие основные способы автоматического поиска вирусов: детекторы, вакцины, фаги.

Программы-детекторы – это специальные программы, предназначенные для просмотра всех возможных мест нахождения вирусов (файлы ОС, основная память, возможно даже пустое в данный момент пространство диска) и сигнализировать об их наличии или отсутствии.

Программы-вакцины – это программы, "вшиваемые" в тело защищаемой программы (дописывающиеся к ее коду), либо резидентно оставляемые в оперативной памяти с целью обнаружения присутствия вируса по признакам аномального поведения (попытки записи в определенные области памяти и т. п.) и, возможно, обезвреживания его.

Программы-фаги – детекторы, дополненные специальными функциями по обезвреживанию данного вируса (удаление его из файлов ОС, оперативной памяти и т. п.).

Следует отметить, что, пользуясь вакцинами, необходимо быть осторожными. Вакцина тем качественнее, чем более точно она имитирует вирус. Но из этого следует, что многие антивирусные программы будут принимать эта вакцины за настоящие вирусы. Возможно, что некоторые фаги попытаются даже обезвредить эти вакцины (в представлении фагов эти вакцины – настоящие вирусы), что, скорее всего, приведет к порче ОС.

Вопрос 3. Защита программ и ценных баз данных от несанкционированного копирования и распространения

По оценкам экспертов в первом десятилетии XXI века только в США общая стоимость нелегально тиражируемых программных средств ежегодно составляла около 3 миллиардов долларов, а общее число нелегально изготовленных копий ПО составляло 45–52 % всех

используемых программных средств. При этом особенно широкое распространение получило незаконное копирование программ для персональных ЭВМ. В частности, ущерб от экспортных недопоставок ПО для ПЭВМ в другие страны и от недополучения лицензионных платежей из-за рубежа за использование ПО только в 2007 г. оценивался в США соответственно в 705 и 235 миллионов долларов.

Выполнить простейшую операцию, достаточную для несанкционированного копирования программного средства на персональной ЭВМ, способен сегодня каждый пользователь.

Процесс нелегального распространения ПО получил развитие и в нашей стране. Это объясняется не только массовым применением вычислительной техники и умением большинства пользователей работать с командой СОРУ, но и более фундаментальными обстоятельствами и факторами:

– новизной законодательства по авторскому праву на программные средства и фактическим отсутствием юридической практики по вопросам защиты прав авторов программной продукции;

– наличием в прошлом многолетней практики нелегального заимствования иностранного программного обеспечения, во многом опиравшейся на определенную государственную поддержку;

– неразвитостью и низкой культурой рыночных отношений в нашей стране.

Можно выделить юридические, экономические и технические меры защиты программного обеспечения от несанкционированного копирования (НСК).

К юридическим средствам охраны ПО относятся различные правовые акты, оговаривающие вопросы зашиты ПО, а также более общие правовые нормы, которые могут применяться для этой цели. Хотя юридическая охрана прав на ПО в технически развитых странах осуществляется различными способами, в основном для этого применяются законы об охране авторских прав, об охране коммерческой тайны, о торговой марке и о патентной защите.

Авторское право . Заявление авторских прав на ПО применяется в качестве наиболее общего способа защиты ПО. Обладание авторским правом на ПО относит практически все операции по манипулированию этим ПО (продажа, применение, развитие) в исключительное ведение владельца.

Вместе с тем применение Закона об авторских правах для защиты ПО сталкивается с некоторыми проблемами, в частности с проблемой создания ПО в рамках служебного задания.

Другой проблемой применения этого Закона для защиты ПО является вопрос о границах действия охраны прав на ПО – охраняется ли алгоритм, текст и структура программы или внешний способ организации взаимодействия с пользователем.

Патентная защита . Несмотря на возможность зашиты ПО с помощью патентов, очень немногие фирмы-производители ПО прибегают к патентованию программ, как способу защиты своих интересов.

На практике громоздкая процедура оформления и получения патента зачастую затягивается на столь длительный срок (более года), что многие программные продукты могут морально устареть раньше, чем на них может быть оформлен патент. Кроме того, патент на ПО действует меньший период времени по сравнению с авторскими правами.

Коммерческая тайна . Согласно Закону о коммерческой тайне под коммерческой тайной понимается некоторая информация либо формула, не являющаяся общеизвестной. В отношении ПО Закон о коммерческой тайне может применяться для защиты программ, разрабатываемых под конкретные требования клиента.

Торговая марка . Торговая марка представляет собой фирменный знак продуцента ПО, применяемый для идентификации программы при ее сбыте, официально защищаемый от копирования. Регистрация торговой марки полезна в случае возрастания спроса на какой-либо программный продукт – если название популярной программы не было

зарегистрировано в качестве торговой марки, оно может быть использовано конкурентами для привлечения покупателей. Закон о торговой марке во многих случаях проще для применения, чем другие способы защиты ПО, т. к. гораздо легче доказать незаконное использование чужой торговой марки, чем доказать копирование.

В Российской Федерации в конце прошлого столетия происходили весьма важные процессы в области становления законодательства по охране программного обеспечения и ценной компьютерной информации. С этой целью приняты законы "О правовой охране программ для электронных вычислительных машин и баз данных" и "О правовой охране топологии интегральных микросхем", что знаменует новый этап в решении проблемы защиты интеллектуальной собственности в нашей стране. Теперь, после появления законодательной базы защиты ПО, основная проблема переходит в плоскость прецедентного накопления юридической практики и внедрения соответствующих административных процедур.

Экономические меры защиты ПО, проводимые фирмами-изготовителями программного обеспечения, предусматривают действенное стимулирование легального приобретения программных средств. Такое стимулирование проводится в настоящее время только для зарегистрированных пользователей, которые совершили легальное приобретение программных средств, и позволяет значительно экономить средства при использовании программ, а иногда даже делает невыгодным их нелегальное копирование.

Возможно, использование следующих мер стимулирования зарегистрированных пользователей:

– периодическая поставка дополнительной документации, специальных журналов и т. п.;

– регулярное сообщение об изменениях и обнаруженных ошибках;

– проведение семинаров и курсов по обучению пользователей программных средств;

– возможность получения оперативной консультации; – предоставление скидки при покупке следующей версии. В настоящее время отечественные предприятия-поставщики ПО активно осваивают вышеуказанные меры стимулирования легального приобретения программной продукции.

Технические меры защиты от несанкционированного копирования программ тесно увязаны с вопросами защиты информации от несанкционированного доступа (НСД). Хотя несанкционированный доступ не всегда направлен на копирование информации, большинство методов защиты от НСД можно применять и для защиты от НСК. Однако в проблеме защиты от НСК имеются свои, специфические методы, описанию которых и посвящена данная глава.

Отметим важную особенность – реализация средств защиты от ИСК существенно облегчается при наличии привилегированных режимов функционирования процессов в операционной системе.

Механизм защиты программного обеспечения, как показывает опыт работы в данной области, может включать следующие блоки:

– защиты от наблюдения;

– установки характеристик среды;

– сравнения характеристик среды;

– ответной реакции.

Блок защиты от наблюдения (БЗОН) представляет собой комплекс программных средств, ориентированных на исследование защищенного программного продукта. Главная функция БЗОН заключается в том, чтобы обеспечить надежную защиту от профессиональных любителей "раздевать" чужие программы, т. е. снимать защиту с пакетов программ. Ниже изложены некоторые способы, которые направлены на выявление и ликвидацию непредусмотренных внешних воздействий на защищаемую программу, характерных для средств снятия защиты.

Для снятия защиты используется комбинация двух основных методов нападения:

статического и динамического .

Статические методы предусматривают анализ текстов защищенных программ. Динамические методы осуществляют слежение за выполнением программы с помощью специальных средств. Обработка результатов слежения может быть частично или полностью автоматизирована.

Среди мер противодействия статическим методам нападения следует упомянуть следующие:

– модификация и шифрование программного кода (типичные способы внесения особенностей в программную среду);

– включение в тело программы переходов по динамически изменяемым адресам и прерываниям, а также самогенерирующихся команд (например, команд, полученных с помощью сложения и вычитания);

– скрытый переход, когда вместо команды безусловного перехода ЗМР используется команда возврата из подпрограммы КЕТ (предварительно в стек записывается адрес перехода, который в процессе работы программы модифицируется непосредственно в стеке);

– включение в тело программы, если ее размер недостаточно велик, так называемой "пустышки", т. е. модуля, к которому имитируется, но не осуществляется передача управления. Этот модуль может содержать большое количество команд, не имеющих никакого отношения к логике работы программы. Но "ненужность" этих команд не должна быть очевидна потенциальному нарушителю;

– изменение начала защищаемой программы таким образом, чтобы стандартный дизассемблер не смог ее правильно восстановить.

Среди мер противодействия динамическим методам нападения следует отметить следующие:

– периодический подсчет в процессе выполнения программы контрольной суммы области оперативной памяти, занимаемой образом задачи, что позволяет своевременно обнаружить изменения, вносимые в загрузочный модуль при попытке ее "раздеть";

– проверка количества свободной памяти и сравнения с тем объемом, к которому "приучена" задача. Это действие позволяет застраховаться от явной слежки за программой с помощью резидентных модулей;

– проверка содержимого незадействованных для решения защищаемой программы областей памяти, которые не попадают под общее распределение оперативной памяти, доступной для программиста, что позволяет добиться "монопольного" режима работы программы;

– проверка содержимого векторов прерываний (особенно с кодами 13h и 21h) на наличие тех значений, к которым "приучена" задача. Иногда полезным бывает сравнение первых команд операционной системы, отрабатывающих эти прерывания, с теми командами, которые там должны быть (вместе с предварительной очисткой оперативной памяти проверка векторов прерываний и их принудительное восстановление позволяет избавиться от большинства присутствующих в памяти резидентных программ);

– переустановка векторов прерываний

– содержимое некоторых векторов прерываний копируется в область свободных векторов, соответственно изменяются и обращения к прерываниям. При этом слежение за известными векторами не даст нарушителю желаемого результата (например, первыми исполняемыми командами программы копируется содержимое вектора с кодом 21h в вектор с кодом 60h, а вместо команд int21h в программе везде записывается команда int60h, в результате в тексте программы не обнаружится ни одной команды работы с прерыванием 21h (обращение к функциям DOS);

– постоянное чередование команд разрешения и запрещения прерывания, что затрудняет установку отладчиком контрольных точек;

– контроль времени выполнения отдельных частей программы, что позволяет выявить "остановы" в теле исполняемого модуля.

Блок установки характеристик среды (БУХС) отвечает за первоначальное "знакомство" защищаемой программы с окружающей средой. Инициатором "знакомства" может выступать как сама защищаемая программа, так и специальный "Установщик". Последний заносит в тело защищаемого файла снятые им характеристики программно-аппаратной среды или, наоборот, подгоняет окружающую среду, например DOS, под защищаемую программу, если она изначально не способна функционировать в нормальном окружении.

Среди основных характеристик, на которые может ориентироваться "привыкающая" программа, исполняются особенности аппаратной среды ЭВМ; программной среды; психофизиологических характеристик оператора ЭВМ.

Если среда недостаточно индивидуальна, ее можно дополнить специальными "индивидуализирующими" признаками.

К особенностям аппаратной среды относятся:

– конфигурация конкретной ПЭВМ (наличие логических дисков, тип видеоадаптера – EGA, CGA или VGA, объем оперативной памяти и т. п.);

– контрольная сумма и дата создания микропрограмм базовой системы ввода-вывода (BIOS);

– измеряемые программой динамические характеристики различных компонентов компьютера и их соотношение между собой (основной проблемой при использовании динамических характеристик является их зависимость от температуры, продолжительности работы и других меняющихся условий, что делает затруднительным получение достаточно стабильных характеристик, индивидуальных для каждого устройства);

– специальная модификация BIOS путем перепрограммирования соответствующих ПЗУ;

– подключение специальных устройств (логических микросхем, дополнительных ПЗУ, подключаемых к ЭВМ через параллельный или последовательный интерфейс и т. п.);

– создание специальных "дефектов" на предъявляемых носителях данных, например на "ключевых" дискетах. Недостаток данного способа заключается в том, что совсем несложно сделать резидентную программу, которая будет перехватывать все обращения к устройству и возвращать в защищенный пакет все те коды завершения, которые тот рассчитывает получить. Этот недостаток можно ликвидировать, если обращения к внешнему устройству адресовать напрямую, а не через DOS.

К особенностям программной среды относятся:

– место физического размещения защищаемого файла на магнитном диске;

– порядок физического размещения файлов защищаемого программного средства на магнитном диске (при этом учитывается не только место физического размещения, но и положение файлов относительно друг друга);

– наличие на ПЭВМ "привычных" для пакета драйверов, таблиц, файлов; простой для реализации, но столь же простой для снятия защиты способ;

– наличие заданной последовательности вызовов определенных программ перед запуском защищаемого пакета;

– специально модифицированные программы операционной системы;

– проверка наличия уникальной даты, например даты инициализации диска;

– нестандартные способы организации данных на магнитных носителях;

– размещение в теле программы в зашифрованном виде данных, которые бы однозначно идентифицировали автора программы и пользователя, которому она официально продана. В качестве таких данных часто используется строка "© ФИО Дата" и системный номер программы; наличие таких данных позволят впоследствии применять юридические средства защиты.

Блок сравнения характеристик среды (БСХС) является одним из самых уязвимых мест защиты. Можно детально не разбираться с логикой защиты, а немного "подправить" результат сравнения, и защита будет снята. Иногда этот блок отсутствует и его выполняет человек (например, в некоторых системах с шифрованием информации сравнение

производится человеком на этапе ее использования).

БСХС может иметь следующие варианты реализации:

– реализация множества операторов сравнения наличных параметров с ожидаемыми;

– генерация исполняемых команд в зависимости от результатов работы защитного механизма (например, в первом байте хранится исходная ключевая контрольная сумма BIOS, во второй байт в процессе выполнения записывается подсчитанная контрольная сумма в процессе выполнения задачи; суть блока сравнения – вычесть из первого байта значение второго байта, а полученный результат добавить к каждой ячейке оперативной памяти в области DOS; ясно, что если суммы не совпадут, то, вряд ли DOS продолжит функционирование);

– выполнение ряда арифметических операций над данными в зависимости от результатов работы защитного механизма.

Блок ответной реакции (БОР) реализует ответные действия программы при обнаружении ею попытки анализа и взлома защитных механизмов. Такими действиями могут быть:

– саморазрушение программы или частичное уменьшение числа выполняемых ею функции;

– необратимая перестройка окружающей среды нот свои потребности, что приводит к невозможности работать на данной ПЭВМ с любыми другими пакетами, кроме данного;

– разрушение окружающей среды, в том числе запуск в профаммную среду вирусов и создание в ней "троянских коней".

– различные способы "издевательства" над пользователем, например замедление реакции программы, подача различных звуковых сигналов в случайные моменты времени, вывод посторонних изображений, добавление комментариев к вводимой и выводимой информации и тому подобное.

Блок ответной реакции может заметно демаскировать систему защиты. С целью снижения демаскирующего эффекта применяются идеи кратности ответной реакции (только после определенного числа запусков) и отложенности возмездия (ответная реакция происходит через определенное время или при срабатывании фрагмента программы, далеко отстоящего от блока сравнения характеристик среды).

Идеи постепенности ответной реакции и частичной деградации исполняемой программы перед полным прекращением работоспособности имеют в плане защиты некоторые плюсы:

– пользователь несанкционированной копии не сразу замечает факт наличия реакции системы защиты;

– желание вскрывать защиту может не появиться, так как используемая программа воспринимается как просто плохо отлаженная;

– может пропасть желание использовать программу из-за страха получить какую-нибудь неизвестную реакцию.

Отрицательным моментом является возникновение антирекламы, поскольку ответная реакция может быть воспринята как свойство самого продукта в незащищенном виде.

Эффект ответной реакции может быть усилен, если она соответствующим образом описана в документации. Возможно описание не всех ответных воздействий или некоторое их преувеличение.

Следует упомянуть о демонстрационных версиях программ, распространяемых с целью рекламы. Представляется, что способ их создания путем установки переключателя в блоке ответной реакции, реализующего частичную потерю программой своих функций, вряд ли может быть признан удачным. Такая демонстрационная версия может быть легко превращена нарушителем в рабочую. Демонстрационная версия должна быть специальной программой, у которой недопустимые функции отсутствуют физически. Кроме того, должны отсутствовать все защитные механизмы, и даже намеки на них.