ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Наступивший новый этап в развитии обмена информацией, который характеризуется интенсивным внедрением современных информационных технологий, широким распространением локальных, корпоративных и глобальных сетей во всех сферах жизни цивилизованного государства, создает новые возможности и качество информационного обмена. В связи с этим проблемы информационной безопасности (ИБ) приобретают первостепенное значение, актуальность и важность которых обусловлена следующими факторами:

- высокие темпы роста парка персональных компьютеров (ПК), применяемых в разных сферах деятельности, и как следствие, резкое расширение круга пользователей, имеющих непосредственный доступ к вычислительным сетям и информационным ресурсам;
- увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью ПК и других средств автоматизации;
- бурное развитие аппаратно-программных средств и технологий, не соответствующих современным требованиям безопасности;
- несоответствие бурного развития средств обработки информации и проработки теории ИБ разработки международных стандартов и правовых норм, обеспечивающих необходимый уровень защиты информации (ЗИ);
- повсеместное распространение сетевых технологий, создание единого информационно-коммуникационного мирового пространства на базе сети Интернет, которая по своей идеологии не обеспечивает достаточного уровня ИБ.

Указанные выше факторы создают определенный спектр угроз ИБ на уровне личности, общества и государства. Средством нейтрализации значительной их части является формирование теории ИБ и методологии защиты информации.

Учебное пособие предназначено для изучения в рамках программы общепрофессиональной дисциплины «Теория информационной безопасности и методология защиты информации» по специальности 090104 «Комплексная защита объектов информатизации» (направление подготовки 090000 «Информационная безопасность»).

Целью курса является формирование профессиональной компетентности на основе системы теоретических и методологических знаний и специальных умений в области информационной безопасности и их использования в профессиональной деятельности будущего специалиста.

В учебном пособии рассматривается основной понятийный аппарат.

ИНФОРММАЦИОННАЯ БЕЗОПАСНОСТЬ

Реалии современного информационного общества показывают, что ни одна сфера жизни цивилизованного государства не может эффективно функционировать без развитой информационной инфраструктуры, широкого применения аппаратно-программных средств и сетевых технологий обработки и обмена информации. По мере возрастания ценности информации, развития и усложнения средств ее обработки и обмена безопасность общества все в большей степени зависит от безопасности используемых информационных технологий (ИТ). Однако, применение информационных технологий немыслимо без повышенного внимания к вопросам обеспечения информационной безопасности (ИБ), а интенсификация процессов обеспечения ИБ – без формирования научно-методологического базиса защиты и рационализации подходов к созданию систем защиты и управлению их функционированием.

Проблемы развития теории и практики обеспечения информационной безопасности

Развитие теории информационной безопасности в настоящее время связано с учетом новых обстоятельств, характерных для современного периода развития информатизации общества. [10].

Во-первых, так как все большую актуальность приобретает не только защита информации, но и защита людей и технических (главным образом, электронных) систем от разрушающего воздействия информации, то формируется задача обеспечения информационной безопасности как органической совокупности задач защиты информации и защиты от информации.

Во-вторых, с самого начала регулярного использования автоматизированных технологий обработки информации актуальность задачи обеспечения требуемого качества информации возрастает, а сама задача усложняется. Следовательно, обеспечение информационной безопасности невозможно без учета задач обеспечения качества информации.

В-третьих, решение задач защиты информации, задач защиты от информации и обеспечения качества информации обусловливает эффективность деятельности объектов. Возникает обобщенное понятие управления информацией, которое объединяет выше обозначенные понятия. В свою очередь, учет задач управления информацией необ-

ходим при формировании, поддержке и использовании концепции информационного обеспечения деятельности объектов.

В-четвертых, серьезное внимание на новом этапе развития теории защиты информации должно быть уделено совершенствованию научно-методологического базиса и инструментальных средств, обеспечивающих решение любых возникающих задач на регулярной основе в органической связи с решением проблем информационной безопасности, информационных технологий, информатизации общества.

Таким, образом, выше изложенное позволяет выделить следующие наиболее острые проблемы развития теории и практики информационной безопасности. Таковыми являются:

- создание теоретических основ и формирование научно-методологического базиса, позволяющих адекватно описывать процессы в условиях значительной неопределенности и непредсказуемости проявления дестабилизирующих факторов (информационных угроз);
- разработка научно-обоснованных нормативно-методических документов по обеспечению по информационной безопасности на базе исследования и классификации угроз информации и выработки стандартов требований к защите;
- стандартизация подходов к созданию систем защиты информации и рационализация схем и структур управления защитой на объектовом, региональном и государственном уровнях.

Решение спектра перечисленных задач имеет большое значение для реализации положений Стратегии национальной безопасности Российской Федерации и Доктрины информационной безопасности.

Основные понятия и определения в области информационной безопасности

Любая область теории и практики базируется на строгом понятийном аппарате. Формирование более полного перечня терминов, их определение и интерпретация с тем, чтобы обеспечивалось однозначное понимание каждого из них, первостепенное значение имеет и для основ информационной безопасности.

Множество понятий и терминов информационной безопасности отражает широкий спектр отличительных существенных свойств, признаков и отношений, присущих данному специфическому виду безопасности. Авторы [1] выделяют три группы терминов теории информационной безопасности. Рассмотрим перечень терминов, входящих в каждую группу.

Термины, определяющие научную основу информационной безопасности

По мнению авторов к этой группе относятся термины, которые используются во многих областях знаний и являются однозначными, семантически унифицированными и стилистически нейтральными. Это: *информация, коммуникация, конфликт, воздействие, угроза, опасность, безопасность, система.*

Термины этой группы отвечают требованиям однозначности и устойчивости, т. е. эти термины однозначно употребляются в одной области знаний и сохраняют свой особый смысл в каждой другой области знаний, а также являются общепризнанными – они употребляются в обиходе. Однако термину «информация» присуще специфическое свойство: в разных областях знаний, и даже в одной области знания он может характеризовать предмет, явление, процесс и их свойства и отношения одновременно.

Термины, определяющие предметную основу информационной безопасности

Ко второй группе относятся термины, обозначающие понятия и их соотношение с другими понятиями в пределах информационной безопасности как специальной сферы или области знаний. К таковым относятся: *информатика, информатизация, информационная система, информационные технологии, информационные процессы, информационный объект, информационный ресурс, информационная инфраструктура, информационная сфера, информационный потенциал*.

Термины, определяющие характер деятельности по обеспечению информационной безопасности

К третьей группе относятся термины, служащие обозначениями характерных для этой сферы предметов, явлений, процессов, их свойств и отношений (в том числе сил, средств и методов их использования при решении задач обеспечения информационной безопасности). Термины этой группы обозначают широкий круг понятий различного уровня: от технического канала утечки информации до информационного противоборства. К ним относятся: *информационное противоборство, информационное превосходство, информационная безопасность, угрозы информационной безопасности, обеспечение информационной безопасности, система обеспечения информационной безопасности, информационная защищенность, безопасность информации, защита информации, объект защиты информации, носитель информации, доступ к информации, доступность информа-*

ции, целостность информации, конфиденциальность информации, несанкционированный доступ к информации, утечка информации, канал утечки информации, канал передачи информации, воздействие на информацию, информационно-психологическое воздействие, информационно-психологическая сфера.

Важной специфической особенностью терминологической системы информационной безопасности является ее тесная связь с правовой лексикой. Это следствие того факта, что информационная безопасность давно перестала быть технической дисциплиной, частью информатики. В связи с этим выработка единообразия в терминологии по проблеме обеспечения информационной безопасности создает предпосылки для целенаправленного развития всех работ по теории информационной безопасности и методологии защиты информации.

Определение информационной безопасности в свете информационных проблем современного общества

Известно, что каждое явление, процесс, объект имеет внутреннее содержание и внешнее выражение. Только сочетание этих составляющих дает полное представление о предмете исследования и возможных направлениях использования его результатов.

Сложность освещения проблемы обеспечения информационной безопасности связана с отсутствием до настоящего времени общепринятого толкования терминов, используемых для описания данной предметной области. В связи с этим для определения понятия информационной безопасности необходимо рассмотреть базовое ключевое понятие «безопасность» [10].

Безопасность как общенаучная категория может быть определена как некоторое состояние рассматриваемой системы, при котором последняя, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних угроз, а с другой – ее функционирование не создает угроз для элементов самой системы и внешней среды. При таком определении мерой безопасности системы являются:

- с точки зрения способности противостоять дестабилизирующему воздействию внешних и внутренних угроз – степень (уровень) сохранения системой своей структуры, технологии и эффективности функционирования при воздействии дестабилизирующих факторов;
- с точки зрения отсутствия угроз для элементов системы и внешней среды – степень (уровень) возможности (или отсутствия возможности) появления таких дестабилизирующих факторов, которые могут представлять угрозу элементам самой системы или внешней среде.

Интерпретация данных формулировок приводит к следующему определению информационной безопасности.

Информационная безопасность – такое состояние рассматриваемой системы, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз, а с другой – ее функционирование не создает информационных угроз для элементов самой системы и внешней среды.

Именно такое понятие информационной безопасности положено в основу Доктрины информационной безопасности и законодательства в сфере обеспечения информационной безопасности Российской Федерации (дословно – «Информационная безопасность – это состояние защищенности жизненно-важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз»).

Ориентиром в направлении поиска путей решения проблем информационной безопасности может служить информация.

Информация как непременный компонент любой организованной системы, с одной стороны, легко уязвима (т.е. весьма доступна для дестабилизирующего воздействия большого числа разноплановых угроз), а с другой – сама может быть источником большого числа разноплановых угроз, как для элементов самой системы, так и для внешней среды. Отсюда, обеспечение информационной безопасности в общей постановке проблемы может быть достигнуто лишь при взаимоувязанном решении трех составляющих проблем:

- защите находящейся в системе информации от дестабилизирующего воздействия внешних и внутренних угроз информации;
- защите элементов системы от дестабилизирующего воздействия внешних и внутренних информационных угроз;
- защите внешней среды от информационных угроз со стороны рассматриваемой системы.

В соответствии с изложенным общая схема обеспечения информационной безопасности может быть представлена так, как показано на рис. 1.

Таким образом, развитие теории информационной безопасности обусловливается основными направлениями развития защиты информации как первой составляющей общей проблемы информационной безопасности, с одной стороны.

С другой, – изучением и разработкой второй составляющей информационной безопасности – защиты от информации (регулярные исследования и разработки на сегодняшний день практически не ведутся).

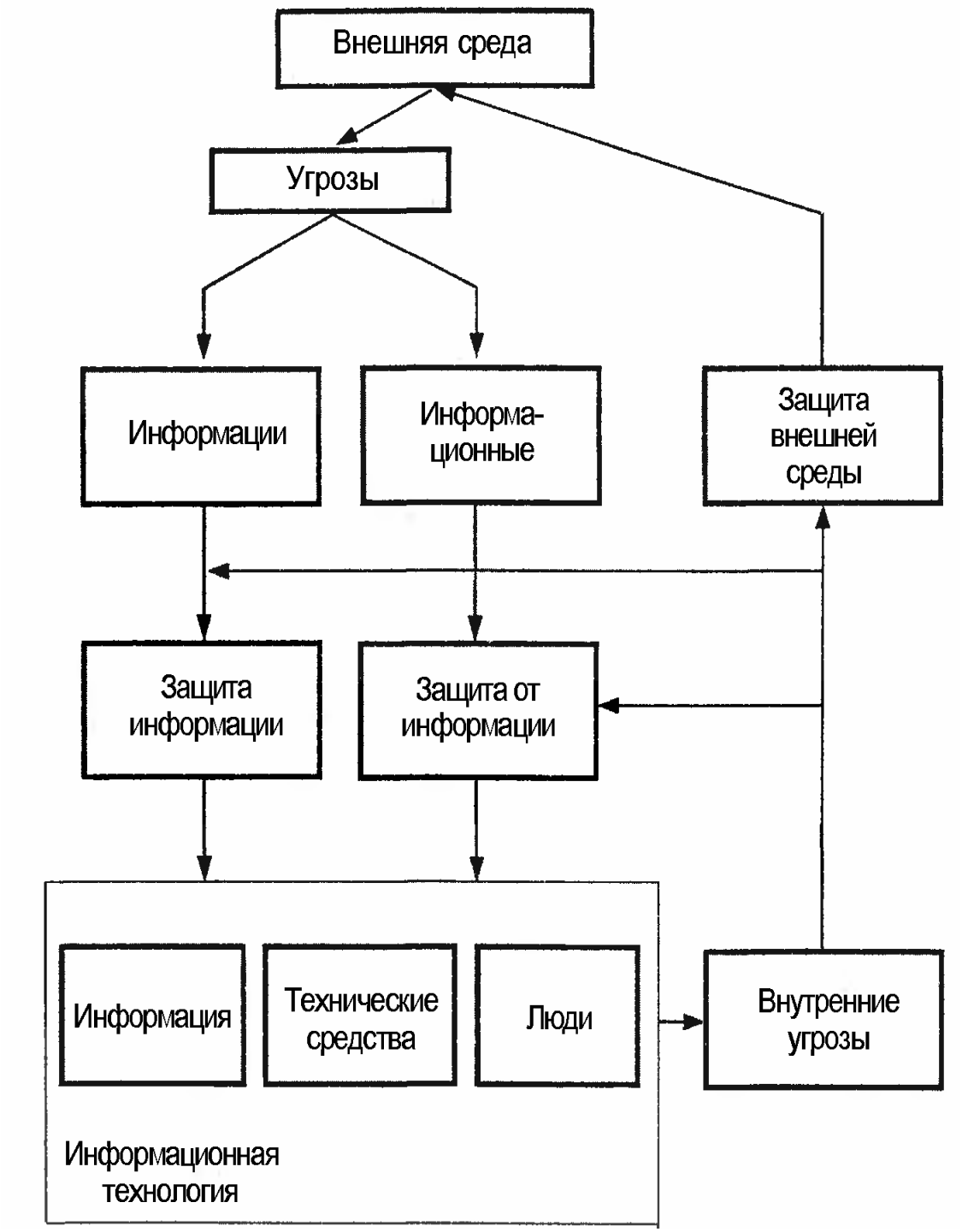

Рис. 1. Общая схема обеспечения информационной безопасности

Вкратце акцентируем внимание на сложность решения второй составляющей проблемы информационной безопасности.

Необходимо отметить, что проблема защиты от информации существенно сложнее проблемы защиты информации в силу многообразности информационных угроз, воздействие которых не всегда очевидно. Предотвращение и нейтрализация таковых требуют как технических решений, так и организационно-правовых и политических на внутригосударственном, межгосударственном и международном уровнях.

В свою очередь, отличительной особенностью проблемы защиты людей от информации, состоит в том, что ее решение будет носить преимущественно гуманитарный характер, в то время как решения по защите от информации технических средств и систем, так же как и по защите информации, носят технический характер и поддаются строгой структуризации.

Основные составляющие информационной безопасности

Информационная безопасность многомерная область деятельности, в которой успех может принести только систематический, комплексный подход.

С методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов.

В обеспечении информационной безопасности нуждаются столь разные субъекты информационных отношений, таких как:

- государство в целом или отдельные органы и организации;
- общественные или коммерческие организации (объединения), предприятия (юридические лица);
- отдельные граждане (физические лица).

Весь спектр интересов субъектов, связанных с использованием информации, можно разделить на следующие категории:

Обеспечение доступности, целостности и конфиденциальности ресурсов информационной среды и поддерживающей инфраструктуры.

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

Поясним понятия доступности, целостности и конфиденциальности.

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

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

Конфиденциальность – это защита от несанкционированного доступа к информации.

В качестве основных информационных ресурсов в дальнейшем будем рассматривать информационные системы и средства коммуникации.

Информационные системы создаются (приобретаются) для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, это, очевидно наносит ущерб всем субъектам информационных отношений. Поэтому, не противопоставляя доступность остальным аспектам, принято выделять ее как важнейший элемент информационной безопасности.

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

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

Значение информационной безопасности для субъектов информационных отношений

Значение каждой из составляющих информационной безопасности для разных категорий субъектов информационных отношений различно.В случае государственных организаций во главу ставится конфиденциальность («пусть лучше все сломается, чем враг узнает хоть один секретный бит»). Далее, для государственных структур осо-

бую значимость принимает целостность информации. Доступность как одна из составляющих ИБ по отношению к двум другим составляющим обладает наименьшим приоритетам.

Для коммерческих организаций ведущую роль играет доступность информации. Особенно ярко это проявляется в разного рода системах управления – производством, транспортном и т.п. Внешне менее драматичные, но также весьма неприятные последствия – и материальные, и моральные – может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей (продажа железнодорожных и авиабилетов, банковские услуги и т.п.). Целостность также важнейший аспект ИБ коммерческих структур. Набор и характеристики комплектующих изделий, ход технологического процесса – все это примеры информации, нарушение целостности которой может оказаться в буквальном смысле смертельным. В то же время конфиденциальность в случае коммерческой информации играет заметно меньшую роль.

Для граждан на первое место можно поставить целостность и доступность информации, обладание которой необходимо для осуществления нормальной жизнедеятельности. Например, участившиеся случаи искажения информации («черного шара») во время выборов. Конфиденциальность здесь не играет ключевой роли, хотя следует отметить, что физические лица на сегодняшний день являются самыми незащищенными субъектами информационных отношений.

Составляющие национальных интересов Российской Федерации в информационной сфере

На современном этапе развития общества возрастает роль информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.

Информационная сфера как системообразующий фактор жизни общества активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности РФ, Национальная безопасность РФ существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать [3, 7, 13, 15, 16].

Стратегия национальной безопасности Российской Федерации до 2020 года

Стратегия национальной безопасности Российской Федерации до 2020 года (Стратегия) разработана в соответствии с поручением главы государства от 4 июня 2008 г. № Пр-1150 межведомственной рабочей группой в рамках Межведомственной комиссии Совета Безопасности Российской Федерации по проблемам стратегического планирования и утверждена Указом Президента Российской Федерации от 12 мая 2009 г. № 537.

Стратегия национальной безопасности Российской Федерации до 2020 года является основным инструментом системы обеспечения национальной безопасности. Она сохраняет преемственность принятых политических установок в области национальной безопасности, в первую очередь Концепции национальной безопасности Российской Федерации, и уточняет государственную политику в области обеспечения национальной безопасности на долгосрочную перспективу, увязанную по целям и задачам с социально-экономическим развитием Российской Федерации. В связи с этим признана утратившей силу прежняя Концепция национальной безопасности Российской Федерации, утвержденная в декабре 1997 г. и модифицированная в январе 2000 г.

Как важнейший документ в системе стратегического планирования, неразрывно связанный с Концепцией долгосрочного социально-экономического развития Российской Федерации на период до 2020 года, Стратегия исходит из фундаментального положения о взаимосвязи и взаимозависимости устойчивого развития государства и обеспечения национальной безопасности.

Особенность Стратегии – ее социальная и социально-политическая направленность, которая состоит в том, что национальная безопасность обеспечивается исходя из принципа «безопасность – через приоритеты устойчивого развития».

Стратегия нацелена на повышение качества государственного управления и призвана скоординировать деятельность органов государственной власти, государственных, корпоративных и общественных организаций по обеспечению безопасности личности, общества и государства от внешних и внутренних угроз в экономической, политической, социальной, международной, духовной, информационной, военной, оборонно-промышленной, экологической сферах, а также в сфере науки и образования. В ней сформулированы главные направления и задачи развития системы обеспечения национальной безопасности России, а также стратегические национальные приоритеты и меры в области внутренней и внешней политики.

Национальные интересы России в информационной сфере заключаются в соблюдении конституционных прав и свобод граждан в области получения информации и пользования ею, в развитии современных телекоммуникационных технологий, в защите государственных информационных ресурсов от несанкционированного доступа.

Важнейшими задачами в области обеспечения информационной безопасности РФ являются:

- реализация конституционных прав и свобод граждан Российской Федерации в сфере информационной деятельности;
- совершенствование и защита отечественной информационной инфраструктуры, интеграция России в мировое информационное пространство;
- противодействие угрозе развязывания противоборства в информационной сфере.

Для этого России потребуется:

- преодолеть технологическое отставание в важнейших областях информатизации, телекоммуникаций и связи, определяющих состояние национальной безопасности;
- разработать и внедрить технологии информационной безопасности в системах государственного и военного управления, в системах управления экологически опасными производствами и критически важными объектами;
- обеспечить условия для гармонизации национальной информационной инфраструктуры с глобальными информационными сетями и системами.

Реализация Стратегии национальной безопасности Российской Федерации до 2020 года призвана стать мобилизующим фактором развития национальной экономики, улучшения качества жизни населения, обеспечения политической стабильности в обществе, укрепления национальной обороны, государственной безопасности и правопорядка, повышения конкурентоспособности и международного престижа РФ.

Доктрина информационной безопасности Российской Федерации

Национальные интересы РФ в информационной сфере и их обеспечение, виды угроз и источники угроз ИБ РФ, а также состояние ИБ РФ и основные задачи и методы по ее обеспечению определены в Доктрине информационной безопасности РФ (Доктрина), утвержденной Указом № 1895 Президента РФ от 9 сентября 2000 года.

Доктрина служит основой для формирования государственной политики в области обеспечения ИБ РФ, подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения ИБ РФ, для разработки целевых программ обеспечения ИБ РФ.

Согласно определению ИБ, прописанному в Доктрине как указывалось выше, интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ и использование информации, на доступ к информации, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества состоят в обеспечении интереса личности в информационной сфере, упрочении демократии, создании правового социального государства, в духовном обновлении России.

Интересы государства заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенности и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развития равноправного и взаимовыгодного международного сотрудничества.

Выделяют четыре основные составляющие национальных интересов РФ в информационной сфере.

1. Соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечения духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

2. Информационное обеспечение государственной политики РФ, связанное до российской и международной общественности достоверной информации о государственной политике РФ, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

3. Развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на миро-

вой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов.

4. Защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

Доктрина также определяет источники угроз информационной безопасности Российской Федерации.

Внешние:

- деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов РФ в информационной сфере;
- стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;
- обострение международной конкуренции за обладание информационными технологиями и ресурсами;
- деятельность международных террористических организаций;
- увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию создания конкурентоспособных российских информационных технологий;
- деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;
- разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

Внутренние:

- критическое состояние отечественных отраслей промышленности;
- неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получение криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;

- недостаточная координация деятельности федеральных органов государственной власти субъектов РФ по формированию и реализации единой государственной политики в области обеспечения информационной безопасности РФ;
- недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;
- неразвитость институтов гражданского общества и недостаточный государственный контроль над развитием информационного рынка России;
- недостаточное финансирование мероприятий по обеспечению информационной безопасности РФ;
- недостаточная экономическая мощь государства;
- снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;
- недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов РФ в информировании общества о своей деятельности, разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развития системы доступа к ним граждан;
- отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти субъектов РФ и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

Доктрина определяет общие методы обеспечения информационной безопасности РФ, которые подразделяются на правовые, организационно-технические и экономические.

К правовым методам относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности РФ.

Организационно-техническими методами обеспечения информационной безопасности РФ являются:

- создание и совершенствование системы обеспечения информационной безопасности РФ;
- усиление правоприменительной деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов РФ, включая предупреждение и пресечение правонарушений в информационной сфере, а также выявление, изобличение и при-

влечение к ответственности лиц, совершивших преступление и другие правонарушения в этой сфере;

- разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышении надежности специального программного обеспечения;
- создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;
- выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата по техническим каналам, применение криптографических средств, защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации;
- сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;
- совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности;
- контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности РФ;
- формирование системы мониторинга показателей и характеристик информационной безопасности РФ в наиболее важных сферах и деятельности общества и государства.

Экономические методы обеспечения включают:

- разработку программ обеспечения информационной безопасности РФ и определение порядка их финансирования;
- совершенствование системы финансирование работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

Информационная безопасность РФ является одной из составляющих национальной безопасности РФ и оказывает влияние на защищенность национальных интересов РФ в различных сферах жизне-

деятельности общества и государства. Угрозы информационной безопасности РФ и методы ее обеспечения являются общими для этих сфер.

В каждой из них имеются свои особенности обеспечения информационной безопасности, связанные со спецификой объектов обеспечения безопасности, степенью их уязвимости и отношения угроз информационной безопасности РФ. В каждой сфере жизнедеятельности общества и государства наряду с общими методами обеспечения информационной безопасности РФ могут использоваться частные методы и формы, обусловленные спецификой факторов, влияющих на состояние информационной безопасности РФ.

Основными составляющими в интенсификации информационных процессов при системно-кибернетическом и социальном подходе к формализации хода общественного развития являются:

- неуклонное возрастание скоростей информационного обмена;
- увеличение объема добываемой и передаваемой информации;
- ускорение процессов обработки информации;
- расширение применения адаптивного управления (с использованием обратных связей);
- расширение наглядного (визуального) представления информации в процессах управления;
- бурный рост технической оснащенности управленческого труда;
- учет особенностей социально-психологических взаимодействий человеческого социума и образований.

Международное сотрудничество в области информационной безопасности: проблемы и перспективы

Высокая сложность и одновременно уязвимость всех систем, на которых базируются национальное, региональные и мировое информационные пространства, а также фундаментальная зависимость от их стабильного функционирования инфраструктур государств приводят к возникновению принципиально новых угроз. Эти угрозы связаны, прежде всего, с потенциальной возможностью использования информационных технологий в целях, несовместимых с задачами поддержания международной стабильности и безопасности, соблюдения принципов отказа от применения силы, невмешательства во внутренние дела государств, уважения прав и свобод человека [11, 12, 13, 15].

В этом плане возникает особая озабоченность в связи с разработкой, применением и распространением новейших видов так называемого гуманного оружия (несмертельных видов оружия и технологий войн), к которым относится информационное, психотронное, экономическое, консциентальное оружие и др.

Значительное внимание уделяется информационному оружию и технологиям ведения информационные войны. Свидетельством тому является тот факт, что в США созданы информационные войска. Сегодня в директивах Министерства обороны США подробно излагается порядок подготовки к информационным войнам. По своей результативности информационное оружие сопоставимо с оружием массового поражения. Спектр действия информационного оружия широк: от нанесения вреда психическому здоровью людей до внесения вирусов в компьютерные сети и уничтожения информации. На суперкомпьютерах моделируются варианты возможных войн в XXI веке с использованием методов и технологии «несмертельного оружия».

Отличие видов и технологий «несмертельного оружия» от обычного военного оружия заключается в том, что оно акцентирует внимание на использовании алгоритмов и технологий, концентрирующих в себе базовые знания и направленных на противника. Информационная война олицетворяет собой войну цивилизаций за выживание в условиях постоянно сокращающихся ресурсов. Информационное оружие поражает сознание человека, разрушает способы и формы идентификации личности по отношению к фиксированным общностям. Оно трансформирует память индивида, создавая личность с заранее заданными параметрами (тип сознания, искусственные потребности, формы самоопределения и т.д.), удовлетворяющими требования агрессора, выводит из строя системы государства-противника и его вооруженных сил.

Можно заключить, что наибольшие потери несут вооруженные силы от применения против них несилового информационного оружия, от воздействия поражающих элементов, действующих на системы управления и психику человека.

В настоящее время осуществляется глобальная информационно-культурная и информационно-идеологическая экспансия Запада по мировым телекоммуникационным сетям (например, Интернет) и через средства массовой информации. Многие страны вынуждены принимать специальные меры для защиты своих граждан, своей культуры, традиций и духовных ценностей от чуждого информационного влияния. Возникает необходимость защиты национальных информационных ресурсов и сохранение конфиденциальности информационного

обмена по мировым открытым сетям, так как на этой почве могут возникать политическая и экономическая конфронтации государств, новые кризисы в международных отношениях. Поэтому информационная безопасность, информационная война и информационное оружие оказались в центре всеобщего внимания.

Информационным оружием называются средства:

- уничтожения, искажения или хищения информационных массивов;
- преодоления систем защиты;
- ограничения допуска законных пользователей;
- дезорганизация работы технических средств, компьютерных систем.

*Атакующим информационным оруж*ием сегодня можно назвать:

- компьютерные вирусы, способные размножаться, внедряться в программы, передаваться по линиям связи, сетям передачи данных, выводить из строя системы управления и т.д.;
- логические бомбы – программные закладные устройства, которые заранее внедряют в информационно-управляющие центры военной или гражданской инфраструктуры, чтобы по сигналу или в установленное время привести их в действие;
- средства подавления информационного обмена в телекоммуникационных сетях, фальсификация информации в каналах государственного и военного управления;
- различного рода ошибки, сознательно вводимые противником в программное обеспечение объекта.

Универсальность, скрытность, многовариантность форм программно-аппаратной реализации, радикальность воздействия, достаточный выбор времени и места применения, экономичность делают информационное оружие чрезвычайно опасным, так как оно легко маскируется под средства защиты (например, интеллектуальной собственности) и даже вести наступательные действия анонимно, без объявления войны.

Нормальная жизнедеятельность общественного организма определяется уровнем развития, качеством функционирования и безопасностью информационной среды. Производство и управление , оборона и связь, транспорт и энергетика, финансы, наука и образование, средства массовой информации – все зависит от интенсивности информационного обмена, полноты, своевременности, достоверности информации. Именно информационная инфраструктура общества – мишень информационного оружия. Но, в первую очередь, новое оружие нацелено на вооруженные силы, предприятия оборонного комплекса,

структуры, ответственные за внешнюю и внутреннюю безопасность страны. Высокая степень структур государственного управления российской экономикой может привести к гибельным последствиям в результате информационной агрессии. Темпы совершенствования информационного оружия превышают темпы развития технологий защиты. Поэтому задача нейтрализации информационного оружия, отражения угрозы его применения должна рассматриваться как приоритетная в обеспечении национальной безопасности страны.

Уничтожение определенных типов сознания предполагает разрушение и переорганизацию общностей, которые конституируют данный тип сознания.

Выделяют пять основных способов поражения и разрушения сознания в консциентальной войне [13]:

- поражение нейромозгового субтрата, снижающее уровень функционирования сознания, которое может происходить под действием химических веществ, длительного отравления воздуха, пищи, радиации;
- понижение уровня организации информационно-коммуникативной среды на основе ее дезинтеграции и примитивизации, в которой функционирует сознание;
- оккультное воздействие на организацию сознания на основе направленной передачи мыслеформ субъекту поражения;
- специальная организация и распространение по каналам коммуникации образов и текстов, которые разрушают работу сознания (психотронное оружие);
- разрушение способов и форм идентификации личности по отношению к фиксированным общностям, приводящее к смене форм самоопределения и деперсонализации.

Воздействие по смене и преобразованию типов иминджидентификаций (глубинного отождествления с той или иной позицией, представленной конкретным образом) и аутентизаций (чувства личной подлинности) осуществляют средства массовой информации, прежде всего, телевидение. Именно в этой области происходят сегодня все основные действия по разрушению российско-русского постсоветского сознания.

Конечная цель использования консциентального оружия - изымание людей из сложившихся форм мегаобщностей. Разрушение народа и превращение его в население происходит за счет того, что никто больше не хочет связывать и соотносить себя с тем полиэтносом, к которому он до этого принадлежал. Разрушение имиджиндентификаций нацелено на разрушение механизмов включение человека в ес-

тественно сложившиеся и существующие общности и замену этих эволюционно-естественно сложившихся общностей одной полностью искусственной – общностью зрителей вокруг телевизора. Не важно, как человек относится к тому, что он видит и слышит с экрана телевизора, важно, чтобы он был постоянным телезрителем. В этом случае на него можно направленно и устойчиво воздействовать. В условиях же формального мира и та называемых локальных войн консциентальная война весьма эффективна.

Таким образом, проблема общемирового противодействия угрозам информационной безопасности усугубляется тем, что до сих пор не выработано общепринятого определения «информационного оружия». Осложняет этот вопрос то обстоятельство, что информационные технологии большей своей частью выступают как технологии невоенного или двойного назначения. Информационные агрессии могут осуществляться с помощью обычных персональных компьютеров с использованием широких технологических возможностей Интернет и примеры тому многочисленны.

Также проблема обеспечения международной информационной безопасности осложняется и тем, что она до сих пор не стала объектом регулирования международного права. В эпоху глобализации, которая затронула и научно-техническую, и информационно-телекоммуникационную сферы, связи между странами становятся все более зависимыми от основанных на информационных технологиях инфраструктур, пересекающих государственные границы. Международный характер угроз информационной агрессии и преступности определяет необходимость взаимодействия как на региональном, так и на глобальном уровне, с тем, чтобы принять согласованные меры для снижения существующих угроз. Ни одному государству не под силу добиться этого в одиночку.

Осознание того факта, что появление и распространение информационного оружия, милитаризация информационных технологий является мощным дестабилизирующим фактором международных отношений, обусловливает функционирование в рамках ООН организации, способной обеспечить решение любой политической проблемы комплексно, при самом широком представительстве и максимальном учете интересов всего мирового сообщества.

Принципиальная позиция Российской Федерации состоит в необходимости жесткого соблюдения принципов неприменения силы, невмешательства во внутренние дела государств, уважения прав и свобод человека и недопущения использования информации и телекоммуникаций в противоречащих Уставу ООН целях.

23 сентября 1998 года в адрес Генерального секретаря ООН было направлено специальное Послание по проблеме международной информационной безопасности Министра иностранных дел Российской Федерации И. С. Иванова. В ходе 53-й сессии Генеральной ассамблеи ООН российской стороной был выдвинут соответствующий проект резолюции под названием «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», консенсусом принятый 4 декабря 1998 года.

Резолюция (документ A/RES/53/70) предлагала государствамчленам ООН продолжить обсуждение вопросов информационной безопасности, дать конкретные определения угроз, предложить свои оценки проблемы, включая разработку международных принципов обеспечения безопасности глобальных информационных систем. О таких оценках страны-члены должны информировать Генерального секретаря ООН, которому поручено представить соответствующий доклад на следующей сессии Генассамблеи ООН. Оценки России были переданы Генсекретарю ООН в мае 1999 года. Доклад Генсекретаря был опубликован 10 августа 1999 года (документ A/54/213) и включал оценки Австралии, Белоруссии, Брунея, Кубы, Омана, Катара, России, Саудовской Аравии, Великобритании и США. Общим для этих оценок стало признание наличия проблемы, однако при этом выявились существенные различия как в расстановке акцентов (военная, правовая, гуманитарная или другие составляющие), так и в методике ее рассмотрения и решения.

Резолюция 53/70 положила начало обсуждению создания совершенно нового международно-правового режима, субъектом которого в перспективе должны стать информация, информационная технология и методы ее использования.

В соответствии с ее рекомендациями Институтом ООН по проблемам разоружения (ЮНИДИР) и Департаментом по вопросам разоружения Секретариата ООН в августе 1999 года в Женеве был организован международный семинар по вопросам международной информационной безопасности. В семинаре приняли участие представители более 50 стран, включая экспертов из наиболее развитых в информационно-технологическом плане государств. Основным итогом семинара стало подтверждение актуальности проблемы информационной безопасности и своевременности постановки этого вопроса в международном плане.

В то же время, в рамках обсуждения обозначились, по крайней мере, два различных подхода к существу проблемы.

Эксперты ряда развитых стран, включая США, исходили из приоритета рассмотрения и разработки мер информационной безопасности применительно к угрозам террористического и криминального характера.

При этом угроза создания информационного оружия и возникновения информационной войны сторонниками такого подхода рассматривалась скорее как теоретическая. Соответственно отпадал и собственно разоруженческий аспект общей проблемы международной информационной безопасности. Дальнейшее обсуждение этой проблематики предлагалось рассредоточить по региональным и тематическим форумам (Европейский Союз, «восьмерка», Организация американских государств, Организация экономического сотрудничества и развития и т. д.), а в рамках ООН перевести из Первого комитета во Второй (экономические вопросы) и Шестой (правовые вопросы).

С другой стороны, приверженцы иного курса (в основном это представители развивающихся стран, России, СИГ, Китая) поддерживали концепцию рассмотрения проблемы международной информационной безопасности в комплексе, с выделением в качестве приоритетной задачи ограничение потенциальной угрозы развязывания информационной войны. При этом подчеркивалась необходимость безотлагательно приступить к обсуждению и практической разработке международно-правовой основы универсального режима международной информационной безопасности. Выдвигалось, в частности, предложение о создании специального международного суда по преступлениям в информационной сфере.

Эта первая такого рода представительная встреча экспертов, несомненно, во многом способствовала выполнению рекомендации резолюции 53/70.

На 54-й сессии ГА ООН Россией был предложен обновленный проект резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Проект впервые; указал на угрозы международной информационной безопасности применительно не только к гражданской, но и к военной сферам. 1 декабря 1999 года резолюция (документ A/RES/54/49) консенсусом была принята Генассамблеей. В этом русле, в частности, МИД России по согласованию с заинтересованными ведомствами был подготовлен проект «Принципов, касающихся международной информационной безопасности».

Во исполнение упомянутой резолюции 54-й сессии проект Принципов в мае 2000 года был представлен в Секретариат ООН и

опубликован в докладе Генсекретаря (документ A/55/140) в качестве вклада России в дальнейшее обсуждение темы.

Принципы представляют собой своего рода рабочий вариант кодекса поведения государств в информационном пространстве, создавая для них, по крайней мере, моральные обязательства, и закладывают основу для широких международных переговоров под эгидой ООН и других международных организаций по этой проблематике. Кроме того, Принципы дают необходимые основные понятия по предмету мировой информационной безопасности (МИБ).

Этой деятельности российской стороны по продвижению инициативы МИБ противостояла оппозиция, состоящая, в основном, из США и ряда стран НАТО. В стремлении создать международно-правовой режим МИБ они усматривали угрозу свободе обмена информацией и конкуренции на рынке информационных технологий. Возможность создания информационного оружия и угроза возникновения информационных войн ими принижалась.

Тем не менее, можно констатировать, что, несмотря на противодействие США, международное сообщество осознало сущность и актуальность проблемы МИБ и, в целом, склоняется к необходимости ее дальнейшего рассмотрения и согласованного решения.

В итоге 55-й сессии Генассамблеей 20 ноября 2000 года консенсусом был одобрен новый российский проект резолюции (A/RES/55/28), в котором отмечалось, что целям ограничения угроз в сфере информационной безопасности отвечало бы «изучение соответствующих международных концепций, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем».

Принципиальным отличительным моментом резолюции, принятой консенсусом на 56-й сессии Генассамблеи ООН 29 ноября 2001 года (документ A/RES/56/19), являлось создание в 2004 году специальной группы правительственных экспертов государств-членов ООН для изучения проблемы МИБ, а именно рассмотрения существующих и потенциальных угроз в сфере информационной безопасности и возможных совместных мер по их устранению.

Консенсусно принятая 22 ноября 2002 года ГА ООН резолюция по МИБ (документ A/RES/57/53) указывает на недопустимость использования информационно-телекоммуникационных, технологий и средств в целях оказания негативного воздействия на инфраструктуру государств.

В последнее время, хотя США и продолжают стремиться обеспечить свое доминирование в информационной сфере, относящейся к

области вооружений, и продолжают на первый план выдвигать вопросы информационного терроризма, информационной преступности и обеспечения безопасности компьютерных сетей, в Вашингтоне начало расширяться понимание того, что проблемы противодействия современным формам терроризма непосредственно связаны с вопросами распространения информационного оружия.

В принятой на встрече лидеров стран «восьмерки», состоявшейся в июле 2000 года в Окинаве (Япония), хартии Глобального информационного общества (Окинавская хартия), страны «восьмерки» признали ИКТ в качестве основного фактора, формирующего общество 21 века, и подтвердили свою готовность содействовать переходу к информационному обществу, полной реализации его преимуществ.

Страны выработали и включили в итоговый документ Саммита ключевые направления работы в частности, в области укрепления политики и нормативно-правовой базы по борьбе, со злоупотреблениями, подрывающими целостность информационных сетей. В связи с этим усилия международного сообщества, направленные на развитие глобального информационного общества, должны сопровождаться согласованными действиями по созданию безопасного и свободного от преступности пространства, осуществлению эффективных мер по борьбе с. компьютерной преступностью. Документ предполагает также расширение сотрудничества стран «восьмерки» в рамках Лионской группы по транснациональной организованной преступности. Была поставлена проблема борьбы с попытками несанкционированного доступа и компьютерными вирусами.

Для защиты критических и информационных инфраструктур было решено привлекать представителей промышленности и других негосударственных организаций посредников. Действительно, правительства в одиночку не способны обеспечить безопасность киберпространства. В этой связи особую важность приобретают усилия каждого пользователя киберпространства по содействию обеспечения безопасности в том участке пространства, которым он владеет или пользуется – промышленные предприятия, организации всех секторов экономики, университеты, местные органы власти, а также граждане – пользователи Интернет.

Таким образом, страны «Группы восьми» пошли на закрепление в итоговом документе лишь вопросов целостности информационных сетей и пресечения преступлений в компьютерной сфере, тем самым игнорируя военно-политическую составляющую проблемы МИБ.

Большую роль в объединении мирового сообщества вокруг темы МИБ сыграла прошедшая в г. Марракеш, Марокко с 23.09.02г. по

18.10.02 г. 16-я Полномочная конференция Международного союза электросвязи (МСЭ) – специализированного учреждения ООН, являющегося международной межправительственной организации и занимающегося вопросами развития электросвязи. В соответствии с резолюцией ГА ООН A/RГS/56/183, принятой консенсусом 21 декабря 2001 года, МСЭ играет ведущую управленческую роль исполнительного секретариата ВВУИО и процесса подготовки к Саммиту.

Одним из основных блоков в структуре вклада МСЭ в «Декларацию принципов» и «План действий ВВУИО» составили вопросы доверия и безопасности при использовании информационных технологий. Так использование информационных технологий, в полной мере могут быть реализованы лишь в: случае надежности и безопасности соответствующих технологий и сетей и отказа от их использования в целях, несовместимых с задачами обеспечения международной стабильности и безопасности.

Нашедшие отражение во Вкладе МСЭ формулировки по МИБ в дальнейшем легли в основу соответствующих положений итоговых документов региональных конференций по подготовке к ВВУИО – Общеевропейской конференции (Бухарест, 7-9 ноября 2002 года) и Азиатской конференции (Токио. 13-15 января 2003 года), на которых Россией также активно продвигалась тема МИБ.

Одним из принципов информационного общества, зафиксированных в Бухарестской декларации, стал принцип укрепления доверия и безопасности при использовании ИКТ. Он подразумевает разработку глобальной культуры кибербезопасности, которая должна обеспечиваться путем принятия превентивных мер и поддерживаться всем обществом при сохранении свободы пере дачи информации. Таким образом, это положение фактически повторяет соответствующее положение Окинавской хартии.

Государства -участники конференции в Будапеште, пришили к пониманию того, что «информационные технологии могут использоваться в целях, несовместимых с задачами обеспечения международной стабильности и безопасности, а также негативно воздействовать на целостность инфраструктуры внутри отдельных государств, нарушая их безопасность как в гражданской, так и в военной сфере», …, что необходимо «предотвращать использование информационных ресурсов или технологий в преступных или террористических целях». В основу этих положений легла консенсусная резолюция ГА ООН по МИБ N 56/19.

В декларации зафиксировано, что в целях содействия доверию и безопасности в использовании информационных технологий орга-

ны государственного управления должны способствовать осознанию обществом угроз, связанных с кибербезопасностью, и стремиться укреплять международное сотрудничество в этой сфере.

В Токийской декларации, которую приняли представители 47 стран, 22 международной и 116 неправительственной организаций, а также представители 54 частных компаний, выделены приоритетные области действий в области информационно-коммуникативных технологий. Важное место в их числе занимает вопрос обеспечения безопасности информационных технологий и средств. Признавая принцип справедливого, равного и адекватного доступа к информационным технологиям для всех стран, особое внимание стороны полагают необходимым уделить угрозе потенциального военного использования информационных технологий. Впервые было высказано мнение о том, что эффективное обеспечение информационной безопасности может быть достигнуто не только технологически, для этого потребуются усилия по правовому регулированию вопроса и выработке соответствующих национальных политик.

В соответствии с Доктриной информационной безопасности РФ, основным направлением международного сотрудничества должно стать запрещение разработки, распространения и применения информационного оружия. Сегодня через инициативы России по обеспечению МИБ «красной нитью» проходит идея необходимости совместной выработки международных концепций, направленных на укрепление безопасности Глобального информационного общества.

Предложения РФ по обеспечению МИБ, направленные на противодействие использованию IT- технологий в террористических и экстремистских целях, сводятся к следующему:

- реализация принципа ответственности государств за свои национальные сегменты сети Интернет, в том числе за содержание размещаемой в них информации;
- выработка единых подходов к вопросу прекращения работы Интернет-сайтов террористического и экстремистского характера;
- обмен информацией о признаках, фактах, методах и средствах использования сети Интернет в террористических целях, об устремлениях и деятельности террористических организаций в сфере IT-технологий, а также по вопросам противодействия распространению в Сети сайтов, содержащих инструкции по изготовлению оружия, самодельных взрывных устройств, ядов и т. п.;
- обмен опытом мониторинга открытых информационных ресурсов сети Интернет, поиска и отслеживания содержимого сайтов террористической направленности;

- кроме того, обмен опытом в области правового регулирования и организации деятельности по борьбе с киберпреступностью.

Россия не ослабляет своих усилий на мировой арене, видя конечную цель своей дипломатической работы в создании глобального режима международной информационной безопасности.

Вопросы для самоконтроля

1. Дайте определение понятию информационная безопасность.
2. Перечислите основные составляющие информационной безопасности.
3. Какое значение имеют составляющие информационной безопасности для субъектов информационных отношений?
4. Каковы интересы РФ в информационной сфере?
5. Определите источники угроз информационной безопасности РФ и постройте их классификацию.
6. Перечислите основные методы обеспечения информационной безопасности РФ.
7. Какие основные проблемы международного сотрудничества стоят на повестке дня сегодня?
8. Перечислите основные документы в области международной информационной безопасности.
9. Каково, на ваш взгляд, положение дел в области МИБ сегодня?

Практическая работа

Рассмотрение и анализ Доктрины информационной безопасности Российской Федерации

Необходимо проанализировать Доктрину ИБ РФ и построить схему органов государственной власти и самоуправления, отвечающих за информационную безопасность и определить их функциональные обязанности; определить положения государственной политики в области обеспечения ИБ, выделить первоочередные мероприятия по обеспечению ИБ, дать им оценку.

ОБЩЕЕ СОДЕРЖАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

Понятие и сущность защиты информации

Понятие защита информации тесно связано с понятием информационной безопасности.

Существует множество определений защиты информации из-за широты понятия информация и многозначности понятия информационной безопасности [1- 4, 10, 13, 15].

Так, под **защитой информации** в узком смысле будем понимать совокупность мероприятий и действий, направленных на обеспечение ее (информации) безопасности – конфиденциальности и целостности - в процессе сбора, передачи, обработки и хранения. Это определение подразумевает тождественность понятий защита информации и обеспечение безопасности информации.

Безопасность информации – это свойство (состояние) передаваемой, накапливаемой, обрабатываемой и хранимой информации, характеризующее ее степень защищенности от дестабилизирующего воздействия внешней среды (человека и природы) и внутренних угроз, то есть ее конфиденциальность (секретность, смысловая или информационная скрытность), сигнальная скрытность (энергетическая и структурная) и целостность – устойчивость к разрушающим, имитирующим и искажающим воздействиям и помехам.

Под **защитой информации,** в более широком смысле, понимают комплекс организационных, правовых и технических мер по предотвращению угроз информационной безопасности и устранению их последствий.

Сущность защиты информации состоит в выявлении, устранении или нейтрализации негативных источников, причин и условий воздействия на информацию. Эти источники составляют угрозу безопасности информации. Цели и методы защиты информации отражают ее сущность.

Защита информации направлена:

- на **предупреждение угроз** как превентивных мер по обеспечению информационной безопасности в интересах упреждения возможности их возникновения;
- на **выявление угроз**, которое выражается в систематическом анализе и контроле возможности появления реальных или потенциальных угроз и своевременных мерах по их предупреждению;

- на **обнаружение угроз**, целью которого является определение реальных угроз и конкретных преступных действий;
- на локализацию преступных действий и принятие мер по **ликвидации угрозы** или конкретных преступных действий;
- на **ликвидацию последствий угроз** и преступных действий и восстановление статус-кво.

Предупреждение возможных угроз и противоправных действий может быть обеспечено самыми различными мерами и средствами, начиная от создания климата глубоко осознанного отношения сотрудников к проблеме безопасности и защиты информации до создания глубокой, эшелонированной системы защиты физическими, аппаратными, программными и криптографическими средствами.

Предупреждение угроз возможно и путем получения информации о готовящихся противоправных актах, планируемых хищениях, подготовительных действиях и других элементах преступных деяний.

Выявление имеет целью проведение мероприятий по сбору, накоплению и аналитической обработке сведений о возможной подготовке преступных действий со стороны криминальных структур или конкурентов на рынке производства и сбыта товаров и продукции.

Обнаружение угроз – это действия по определению конкретных угроз и их источников, приносящих тот или иной вид ущерба. К таким: действиям можно отнести обнаружение фактов хищения или мошенничества, а также фактов разглашения конфиденциальной информации или случаев несанкционированного доступа к источникам коммерческих секретов.

Пресечение или локализация угроз – это действия, направленные на устранение действующей угрозы и конкретных преступных действий. Например, пресечение подслушивания конфиденциальных переговоров за счет акустического канала утечки информации по вентиляционным системам.

Ликвидация последствий имеет целью восстановление состояния, предшествовавшего наступлению угрозы. Например, возврат долгов со стороны заемщиков. Это может быть и задержание преступника с украденным имуществом, и восстановление разрушенного здания от подрыва и др.

Все эти способы имеют целью защитить информационные ресурсы от противоправных посягательств и обеспечить:

- предотвращение разглашения и утечки конфиденциальной информации;
- воспрещение несанкционированного доступа к: источникам конфиденциальной информации;

- сохранение целостности, полноты и доступности информации;
- соблюдение конфиденциальности информации;
- обеспечение авторских прав.

Учитывая вышесказанное, **защиту информации** можно определить как совокупность методов, средств и мер, направленных на обеспечение информационной безопасности общества, государства и личности во всех областях их жизненно важных интересов.

Защищаемая информация включает сведения, составляющие государственную, коммерческую, служебную и иные охраняемые законом тайны. Каждый вид защищаемой информации имеет свои особенности в области регламентации, организации и осуществления этой защиты.

Наиболее общими **признаками защиты** любого вида охраняемой **информации** являются следующие:

- защиту информации организует и проводит собственник или владелец информации или уполномоченные им на то лица (юридические или физические);
- защитой информации собственник охраняет свои права на владение и распоряжение информацией, стремится оградить ее от незаконного завладения и использования в ущерб его интересам;
- защита информации осуществляется путем проведения комплекса мер по ограничению доступа к защищаемой информации и созданию условий, исключающих или существенно затрудняющих несанкционированный, незаконный доступ к защищаемой информации и ее носителям.

Таким образом, защита информации – есть комплекс мероприятий, проводимых собственником информации, по ограждению своих прав на владение и распоряжение информацией, созданию условий, ограничивающих ее распространение и исключающих или существенно затрудняющих несанкционированный, незаконный доступ к засекреченной информации и ее носителям.

Защищаемая информация, являющаяся государственной или коммерческой тайной, как и любой другой вид информации, необходима для управленческой, научно-производственной и иной деятельности. В настоящее время перед защитой информации ставятся более широкие задачи, чем обеспечение безопасности информации. Это обусловлено рядом обстоятельств, и в первую очередь тем, что все более широкое распространение в накоплении и обработке защищаемой информации получают ЭВМ, в которых может происходить не только утечка информации, но и ее разрушение, искажение, подделка, блоки-

рование и иные вмешательства в информацию и информационные системы.

Следовательно, под защитой информации следует также понимать обеспечение средств информации, в которых накапливается, обрабатывается и хранится защищаемая информация.

Таким образом, защита информации – это деятельность собственника информации или уполномоченных им лиц по:

- обеспечению своих прав на владение, распоряжение и управление защищаемой информацией;
- предотвращению утечки и утраты информации;
- сохранению полноты, достоверности, целостности защищаемой информации, ее массивов и программ обработки;
- сохранению конфиденциальности или секретности защищаемой информации в соответствии с правилами, установленными законодательными и другими нормативными актами.

Цели защиты информации

Основными целями защиты информации являются [15]:

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

В соответствии с этими целями процесс защиты информации должен обеспечить поддержание целостности и конфиденциальности информации.

Целостность информации тесно связана с понятием надежности как технических, так, и программных средств, реализующих процессы накопления, хранения и обработки информации.

Из анализа угроз безопасности информации, целей и задач ее защиты следует, что достичь максимального (требуемого) уровня защищенности можно только за счет комплексного использования существующих методов и средств защиты. **Комплексность** является одним из принципов, которые должны быть положены в основу разработки как концепции защиты информации, так и конкретных систем защиты.

Цели защиты информации на объектах защиты могут быть достигнуты при проведении работ по следующим направлениям:

- определению охраняемых сведений об объектах защиты;
- выявлению и устранению (ослаблению) демаскирующих признаков, раскрывающих охраняемые сведения;
- оценке возможностей и степени опасности технических средств разведки;
- выявлению возможных технических каналов утечки информации;
- анализу возможностей и опасности несанкционированного доступа к информационным объектам;
- анализу опасности уничтожения или искажения информации с помощью программно-технических воздействий на объекты защиты;
- разработке и реализации организационных, технических, программных и других средств и методов защиты информации от всех возможных угроз;
- созданию комплексной системы защиты;
- организации и проведению контроля состояния и эффективности системы защиты информации;
- обеспечению устойчивого управления процессом функционирования системы защиты информации.

Процесс комплексной защиты информации должен осуществляться непрерывно на всех этапах. Реализация непрерывного процесса защиты информации возможна только на основе систем концептуального подхода и промышленного производства средств защиты, а создание механизмов защиты и обеспечение их надежного функционирования и высокой эффективности может быть осуществлено только специалистами высокой квалификации в области защиты информации.

Чтобы лучше понять соотношение понятий защиты информации и информационной безопасности, представим их в форме некой схемы (см. рис. 1).

Защита информации выступает некоторым подобием защитной оболочки, которая противостоит дестабилизирующим воздействиям (видам уязвимости информации) и обеспечивает информационную безопасность. Суть же этой оболочки «защиты информации» в том, чтобы обеспечить безопасность самой информации [13, 15, 16].

Концептуальная модель информационной безопасности

Обеспечение информационной безопасности – это комплексная проблема, для решения которой требуется сочетание мер законодательного, административного, процедурного и программно-технического уровней.

Законодательный уровень является важнейшим для обеспечения информационной безопасности.

Разработка и принятие правовых вопросов призваны регулировать вопросы использования информационной структуры и телекоммуникаций, доступа к информации, защиты информации от несанкционированного доступа и утечки по техническим каналам, защиты граждан, общества и государства от ложной информации, защиты информации телекоммуникационных сетей от неправомерных действий, обеспечения техногенной безопасности и ее информационных аспектов.

При формировании законодательства в сфере информационных ресурсов и коммуникаций в самостоятельную отрасль' права – информационное право – законодательство в сфере обеспечения информационной безопасности будет выступать как его подотрасль, а при кодификации в виде Информационного кодекса станет его составной частью.

Принято выделять два направления формирования законодательства. К первому относиться меры, направленные на создание и поддержание в обществе негативного (в том числе карательного) отношения к нарушениям и нарушителям информационной безопасности.

Рис.1. Взаимосвязь понятий информационная безопасность и защита информации

Среди российских законов сюда можно отнести Закон «Об информации, информатизации и защиты информации», соответствующие главы Уголовного кодекса РФ и т.д.

Ко второму можно отнести принятие нормативных документов, способствующих повышению образованности общества в области информационной безопасности, определяющих в разработку и распространение средств обеспечения информационной безопасности. Многообразие нормативных документов представлено международными, национальными, отраслевыми нормативными документами и соответствующими нормативными документами организаций, предприятий и фирм.

Большую работу в этом направлении проводят Международная организация по стандартизации – ISO, Международная электротехническая комиссия - IEC, Международный союз электросвязи – ITU. Кроме того, значительные усилия предпринимают национальные организации по стандартизации ANSI и NIST – в США, DIN в ФРГ, Госстандарт в России и т.д. Активно участвуют в разработках SWIFT – общество всемирных межбанковских финансовых телекоммуникаций, GISA – германское агентство защиты информации и т.д.

Вопросы сертификации и лицензирования средств обеспечения информационной безопасности в России рассматривает Федеральная служба по техническому и экспортному контролю при Президенте РФ.

При проведении работ по стандартизации и сертификации в области обеспечения информационной безопасности учитывают два аспекта: **формальный** – определение критериев, которым должны соответствовать защищенные информационные технологии и **практический** – определение конкретного комплекса мер безопасности применительно к рассматриваемой информационной технологии.

Основными критериями работоспособности концепций и стандартов ИБ в настоящее время считаются следующие

- универсальность – характеристика стандарта, определимая множеством типов вычислительным систем, на которые он ориентирован;
- гибкость – возможность применение стандарта к постоянно развивающимся информационным технологиям;
- гарантируемость – количество и качество предусмотренных стандартом методов и средств подтверждения надежности результатов квалификационного анализа;
- реализуемость – возможность адекватной реализации на практике;

- актуальность – требования и критерии стандарта должны соответствовать постоянно развивающемуся множеству угроз безопасности.

Исходя из подобных критериев оценки, наиболее работоспособным из созданных уже документов считают «Единые общие критерии оценки безопасности информационных технологий», представляющие собой результат совместной работы Международной организации по стандартизации, Национального института стандартов и технологии США, организаций Великобритании, Канады, Германии, Франции и Нидерландов.

Среди стандартов практических аспектов информационной безопасности можно также отметить британский BS 7799 «Практические правила управления информационной безопасностью», в котором обобщен опыт обеспечения режима информационной безопасности в информационных системах различного профиля, и немецкий BSI, который относиться к этапу анализа рисков.

Основой мер **административного уровня,** то есть мер, предпринимаемых руководством организации, является политика безопасности [9, 22].

Под **политикой безопасности** понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политика безопасности определяет стратегию организации в области информационной безопасности, а также ту меру внимания и количество ресурсов, которую руководство считает целесообразным выделить.

Определение политики ИБ должно сводиться к следующим практическим шагам:

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

- управление доступом к средствам вычислительной техники, программа и данным;
- антивирусную защиту;
- вопросы резервного копирования;
- проведение ремонтных и восстановительных работ;
- информирование об инцидентах об области ИБ.

2. Определение подходов к управлению рисками: является ли достаточным базовый уровень защищенности или требуется проводить полный вариант анализа рисков.

3. Структуризация контрмер по уровням.

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

Для построения системы защиты информации необходимо определить границы системы, для которой должен быть обеспечен режим информационной безопасности. Соответственно система управления информационной безопасности (система защиты информации) должна строиться именно в этих границах.

Описание границ системы, для которой должен быть обеспечен режим информационной безопасности, рекомендуется выполнять по следующему плану.

1. Структура организации. Описание существующей структуры и изменений, которые предполагается внести в связи с разработкой или модернизации автоматизированной системы обработки информации.

2. Размещение средств вычислительной техники и поддерживающей инфраструктуры. Модель иерархии средств вычислительной техники.

3. Ресурсы информационной системы, подлежащие защите. Рекомендуется рассмотреть ресурсы автоматизированной системы следующих классов: средства вычислительной техники, данные, системное и прикладное программное обеспечение. Все ресурсы представляют ценность с точки зрения организации. Для их оценки должна быть выбрана система критериев и методология оценок по этим критериям.

4. Технология обработки информации и решаемые задачи. Для решаемых задач должны быть построены модели обработки информации в терминах ресурсов.

В результате должен быть составлен документ, в котором:

- зафиксированы границы и структура системы;
- перечислены ресурсы, подлежащие защите;
- дана система критериев для оценки их ценности.

Минимальным требованиям к режиму информационной безопасности соответствует базовый уровень. Обычной областью использования этого уровня являются типовые проектные решения. Существует ряд стандартов и спецификаций, в которых рассматривается минимальный (типовой) набор наиболее вероятных угроз, таких как вирусы, сбои оборудования, несанкционированный доступ и т.д. Для нейтрализации этих угроз обязательно должны быть приняты контр-

меры вне зависимости от вероятности осуществления угроз и уязвимости ресурсов. Таким образом, характеристики угроз на базовом уровне рассматривать не обязательно.

В случае, когда нарушения информационной безопасности чреваты тяжелыми последствиями, базовый уровень требований к режиму информационной безопасности является недостаточным. Для того, чтобы сформулировать дополнительные требования, необходимо:

- определить ценность ресурсов;
- к стандартному набору добавить список угроз, актуальных для исследуемой информационной системы;
- оценить вероятности угроз;
- определить уровень уязвимости ресурсов.

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

Существуют различные подходы к оценке рисков. Выбор подхода зависит от уровня требований, предъявляемых в организации к режиму информационной безопасности, характера принимаемых во внимание угроз (спектра воздействия угроз) и эффективности потенциальных контрмер.

Процесс оценивая рисков содержит несколько этапов.

1. Идентификация ресурса и оценивание его количественных показателей (определение негативного воздействия).
2. Оценивание угроз.
3. Оценивание уязвимостей.
4. Оценивание существующих и предполагаемых средств обеспечения.
5. Оценивание рисков.

На основании оценивания рисков выбираются средства, обеспечивающие режим ИБ. Ресурсы, значимые для нормальной работы организации и имеющие определенную степень уязвимости, считаются подверженными риску, если по отношению к ним существует какая-либо угроза. При оценивании рисков учитываются потенциальные негативные воздействия от нежелательных происшествий и показатели значимости рассматриваемых уязвимостей и угроз для этих ресурсов.

Риск характеризует опасность, которой может подвергаться система и использующая ее организация. Риск зависит от показателей

ценности ресурсов, вероятности реализации угроз для ресурсов и степени легкости, с которой уязвимости могут быть использованы при существующих или планируемых средствах обеспечения информационной безопасности.

Цель оценивания рисков состоит в определении характеристик рисков для информационной системы и ее ресурсов. На основе таких данных могут быть выбраны необходимые средства управления ИБ.

При оценивании рисков учитывается:

- ценность ресурсов;
- оценка значимости угроз;
- эффективность существующих и планируемых средств защиты.

Показатели ресурсов или потенциальное негативное воздействие на деятельность организации можно определять несколькими способами:

- количественными (например, стоимостные);
- качественными (могут быть построены на использовании таких понятий, как, умеренный или чрезвычайно опасный);
- их комбинацией.

Для того, чтобы конкретизировать определение вероятности реализации угрозы, рассматривается определенный отрезок времени, в течение которого предполагается защитить ресурс. Вероятность того, что угроза реализуется, определяется следующими факторами:

- привлекательность ресурса как показатель при рассмотрении угрозы от умышленного воздействия со стороны человека;
- возможность использования ресурса для получения дохода как показатель при рассмотрении угрозы от умышленного воздействия со стороны человека;
- технические возможности угрозы, используемые при умышленном воздействии со стороны человека;
- вероятность того, что угроза реализуется;
- степень легкости, с которой уязвимость может быть использована.

Вопрос о том, как провести границу между допустимыми и недопустимыми рисками, решается пользователем. Очевидно, что разработка политики безопасности требует учета специфики конкретных организаций.

На основании политики безопасности строится программа безопасности, которая реализуется на процедурном и программно-техническом уровнях уровне.

К **процедурному уровню** относятся меры безопасности, реализуемые людьми.

Можно выделить следующие группы процедурных мер:

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

Управление персоналом заключается в выполнении следующих условий. Во-первых, для каждой должности существовать квалификационные требования по ИБ. Во-вторых, в должностные инструкции должны входить разделы, касающиеся информационной безопасности. В-третьих, каждого работника нужно научить мерам безопасности теоретически и на практике.

Меры физической защиты включают в себя защиту от утечки информации по техническим каналам, инженерные способы защиты и т.д.

Планирование восстановительных работ предполагает:

- слаженность действий персонала во время и после аварии;
- наличие заранее подготовленных резервных производственных площадок;
- официально утвержденную схему переноса на резервные площадки основных информационных ресурсов;
- -схему возвращения к нормальному режиму работы.

Поддержание работоспособности включает в себя создание инфраструктуры, включающий в себя как технические, так и процедурные регуляторы и способной обеспечить любой наперед заданный уровень работоспособности на всем протяжении жизненного цикла информационной системы

Реагирование на нарушение режима безопасности может быть регламентировано в рамках отдельно взятой организации. В настоящее время, осуществляется только мониторинг компьютерных преступлений в национальном масштабе и на мировом уровне.

Основой **программно-технического уровня** являются следующие механизмы безопасности:

- идентификация и аутентификация пользователей;
- управление доступом;
- протоколирование и аудит;
- криптография;
- экранирование;

- обеспечение высокой доступности и т.д.

Важно управлять информационной системой в целом и механизмами безопасности в особенности. Упомянутые меры безопасности должны опираться на общепринятые стандарты, быть устойчивым к сетевым угрозам, учитывать специфику отдельных сервисов.

Вопросы для самоконтроля

1. Проанализируйте различные определения понятия «защита информации» и «информационная безопасность», заполните таблицу.

№ п/п	Определение термина	Ключевые слова	Источник информации

Что общего можно обнаружить во всех определениях? О чем это свидетельствует?

2. Дайте определение понятию защита информации.
3. Что понимается под термином безопасность информации?
4. Что включает в себя защита информации?
5. Какие цели преследует защита информации?
6. Какое место занимается защита информации в информационной безопасности?
7. Какие уровни задействованы в обеспечении информационной безопасности?
8. Что представляет собой политика безопасности организации?
9. Что входит в анализ рисков?
10. Что представляет собой программа безопасности организации?

Практическая работа

Определение целей защиты информации на предприятии регионального уровня

Необходимо проанализировать структуру местного предприятия, рассмотреть виды информации и носители, используемые в его подразделениях. Сформулировать цели защиты информации на данном предприятии. Составить программу информационной безопасности.

ПРЕДМЕТ И ОБЪЕКТ ЗАЩИТЫ ИНФОРМАЦИИ

Предмет защиты информации

Предметом защиты является информация, т.е. сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления.

Информация имеет ряд особенностей:

- она нематериальна;
- информация хранится и передается с помощью материальных носителей;
- любой материальный объект может содержать информацию о самом себе или других объектах.

Нематериальность информации понимается в том смысле, что нельзя измерить ее параметры известными физическими методами и приборами. Информация не имеет массы, энергии и т. п.

Наиболее важным свойством информации является ее ценность. *Ценность информации определяется степенью ее полезности для владельца.*

На сегодняшний день известно много различных попыток формализовать процесс оценки информации, но он до сих пор остается субъективным [4, 13, 15, 23].

Обладание истинной (достоверной) информацией дает ее владельцу определенные преимущества. Истинной или *достоверной информацией является информация, которая с достаточной для владельца (пользователя) точностью отражает объекты и процессы окружающего мира в определенных временных и пространственных рамках.*

Информация, искаженно представляющая действительность (недостоверная информация), может нанести владельцу значительный материальный и моральный ущерб. Если информация искажена умышленно, то ее отзывают дезинформацией.

Законом «Об информации, информатизации и защите информации» гарантируется право собственника информации на ее использование и защиту от доступа к ней других лиц (организаций). Критерием для принятия решения о защиты информации является ценность информации.

Защите подлежит только документированная информация, т.е. информация, зафиксированная на материальном носителе с реквизитами, позволяющими ее идентифицировать.

Собственник вправе ограничивать доступ к информации. Документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне и конфиденциальную.

Государственную тайну могут содержать сведения, принадлежащие государству (государственному учреждению). В соответствии с законом «О государственной тайне» сведениям, представляющим ценность для государства, может быть присвоена одна из трех возможных **уровней** секретности:

- *«секретно»;*
- *«совершенно секретно»;*
- *«особой важности».*

Уровень секретности – это административная или законодательная мера, соответствующая мере ответственности лица за утечки или потерю конкретной конфиденциальной информации, регламентируемой специальным документом, с учетом государственных, военно-стратегических, коммерческих, служебных или частных интересов.

В соответствии с уровнем секретности на носители информации проставляется гриф секретности, т.е. реквизиты, свидетельствующие о степени секретности.

Перечень конфиденциальных сведений утвержден Указом Президента РФ и состоит из:

- персональных данных гражданина;
- сведений, составляющих тайну следствия и судопроизводства;
- служебной тайны, т.е. сведения, доступ к которым ограничен органами государственной власти;
- сведений, связанные с профессиональной деятельностью (врачебная, нотариальная, адвокатская тайны и т.д.);
- сведений о сущности изобретения до момента официальной публикации о них;
- коммерческой тайны.

Коммерческую тайну могут содержать сведения, принадлежащие частному лицу, фирме, корпорации и т. п. Для обозначения ценности конфиденциальной коммерческой информации используются три категории:

- *«коммерческая тайна - строго конфиденциально»;*
- *«коммерческая тайна - конфиденциально»;*
- *«коммерческая тайна».*

Используется и другой подход к градации ценности коммерческой информации:

- *«строго конфиденциально – строгий учет»;*
- *«строго конфиденциально»;*
- *«конфиденциально».*

Необходимо заметить, что суммарное количество не конфиденциальной информации, или статистика несекретных данных, в итоге могут оказаться секретными.

Ценность информации изменяется во времени. Как правило, со временем ценность информации уменьшается. Зависимость ценности информации от времени приближенно определяется в соответствии с выражением [13-15]:

$C(t) = C_0 e^{-2,3t/\tau}$, где C_0 – ценность информации в момент ее возникновения (получения); t – время от момента возникновения информации до момента определения ее стоимости; τ – время от момента возникновения информации до момента ее устаревания.

Время, через которое информация становится устаревшей, меняется в очень широком диапазоне. Так, например, для пилотов реактивных самолетов, автогонщиков информация о положении машин в пространстве устаревает за доли секунд. В то же время информация о законах природы остается актуальной в течение многих веков.

Информация покупается и продается. Ее правомочно рассматривать как товар, имеющий определенную цену. Цена, как ценность информации, связаны с полезностью информации для конкретных людей, организаций, государств. Информация может быть ценной для ее владельца, но бесполезной для других. В этом случае информация не может быть товаром, а, следовательно, она не имеет и цены. Например, сведения о состоянии здоровья обычного гражданина являются ценной информацией для него. Но эта информация, скорее всего, не заинтересует кого-то другого, а, следовательно, не станет товаром, и не будет иметь цены.

Информация может быть получена тремя путями:

- проведением научных исследований;
- покупкой информации;
- противоправным добыванием информации.

Как любой товар, информация имеет себестоимость, которая определяется затратами на ее получение. Себестоимость зависит от выбора путей получения информации и минимизации затрат при добывании необходимых сведений выбранным путем. Информация добывается с целью получения прибыли или преимуществ перед конкурентами, противоборствующими сторонами. Для этого информация:

- продается на рынке;
- внедряется в производство для получения новых технологий и товаров, приносящих прибыль;
- используется в научных исследованиях;
- позволяет принимать оптимальные решения в управлении.

Существует сложность объективной оценки количества информации.

Для измерения количества информации используют следующие подходы.

А. Энтропийный подход.

В теории информации количество информации оценивается мерой уменьшения у получателя неопределенности (энтропии) выбора или ожидания событий после получения информации. Количество информации тем больше, чем ниже вероятность события. Энтропийный подход широко используется при определении количества информации, передаваемой по каналам связи. Выбор при приеме информации осуществляется между символами алфавита в принятом сообщении. Пусть сообщение, принятое по каналу связи, состоит из N символов (без учета связи между символами в сообщении). Тогда количество информации в сообщении может быть подсчитано по формуле Шеннона:

$I = N \sum_{i=1}^{k} P_i log_2 P_i$, где P_i – вероятность появления в сообщении символа, k –количество символов в алфавите языка.

Анализ формулы Шеннона показывает, что количество информации в двоичном представлении (в битах или байтах) зависит от двух величин: количества символов в сообщении и частоты появления того или иного символа в сообщениях для используемого алфавита. Этот подход абсолютно не отражает насколько полезна полученная информация, а позволяет определить лишь затраты на передачу сообщения.

Б. Тезаурусный подход.

Этот подход предложен Ю.А. Шрейдером. Он основан на рассмотрении информации как знаний. Согласно этому подходу количество информации, извлекаемое человеком из сообщения, можно оценить степенью изменения его знаний. Структурированные знания, представленные в виде понятий и отношений между ними, называются тезаурусом. Структура тезауруса иерархическая. Понятия и отношения, группируясь, образуют другие, более сложные понятия и отношения.

Знания отдельного человека, организации, государства образуют соответствующие тезаурусы. Тезаурусы организационных структур образуют тезаурусы составляющих их элементов. Так, тезаурус

организации образуют, прежде всего, тезаурусы сотрудников, а также других носителей информации, таких как документы, оборудование, продукция и т.д. Для передачи знаний требуется, чтобы тезаурусы передающего и принимающего элемента пересекались. В противном случае владельцы тезаурусов не поймут друг друга.

Тезаурусы человека и любых организационных структур являются их капиталом. Поэтому владельцы тезаурусов стремятся сохранить и увеличить свой тезаурус. Увеличение тезауруса осуществляется за счет обучения, покупки лицензии, приглашения квалифицированных сотрудников или хищения информации.

В обществе наблюдаются две тенденции: развитие тезаурусов отдельных элементов (людей, организованных структур) и выравнивание тезаурусов элементов общества. Выравнивание тезаурусов происходит как в результате целенаправленной деятельности (например, обучения), так и стихийно. Стихийное выравнивание тезаурусов происходит за счет случайной передачи знаний, в том числе и незаконной передачи.

В. Практический подход.

На практике количество информации измеряют, используя понятие «объем информации». При этом количество информации может измеряться в количестве бит (байт), в количестве страниц текста, длине магнитной ленты с видео- или аудиозаписью и т.п. Однако очевидно, что на одной странице информации может содержаться больше или меньше, по крайней мере, по двум причинам. Во-первых, разные люди могут разместить на странице различное количество сведений об одном и том же объекте, процессе или явлении материального мира. Во-вторых, разные люди могут извлечь из одного и того же текста различное количество полезной, понятной для них информации. Даже один и тот же человек в разные годы жизни получает разное количество информации при чтении книги.

В результате копирования без изменения информационных параметров носителя количество информации не изменяется, а цена снижается. Примером копирования без изменения информационных параметров может служить копирование текста с использованием качественных копировальных устройств. Текст копии, при отсутствии сбоев копировального устройства, будет содержать точно такую же информацию, как и текст оригинала. Но при копировании изображений уже не удастся избежать искажений. Они могут быть только большими или меньшими.

В соответствии с законами рынка, чем больше товара появляется, тем он дешевле. Этот закон полностью справедлив и в отношении

копий информации. Действие этого закона можно проследить на примере пиратского распространения программных продуктов, видеопродукции и т.п.

Информация как объект права собственности

Различные субъекты информационных отношений по отношению к определенной информации могут выступать в качестве (возможно одновременно) [16. 23]:

- источников (поставщиков) информации;
- пользователей (потребителей) информации;
- собственников (владельцев, распорядителей) информации;
- физических и юридических лиц, о которых собирается информация;
- владельцев систем сбора и обработки информации и участников процессов обработки и передачи информации и т.д.

Возникает сложная система взаимоотношений между этими субъектами права собственности.

Информация как объект права собственности копируема за счет материального носителя. Как следствие, информация как объект права собственности легко перемещается перемещаться к другому субъекту права собственности без очевидного (заметного) нарушения права собственности на информации. Перемещение материального объекта к другому субъекту права собственности неизбежно, и, как правило, влечет за собой утрату этого объекта первоначальным субъектом права собственности, т.е. происходит очевидное нарушение его права собственности.

Право собственности включает три полномочия собственника, составляющих содержание (элементы) права собственности: право распоряжения, право владения, права пользования.

Но для необходимости рассмотрения информации как предмета защиты информации, необходимо рассмотреть особенности информации как объекта права собственности.

Субъект права собственности на информацию может передать часть своих прав (распоряжение), не теряя их, другим субъектам, «хранителю», т.е. владельцу материального носителя информации (владение или пользование) или пользователю (пользование и, может быть, владение).

Для информации право распоряжения подразумевает исключительное право определять, кому эта информация может быть предоставлена.

Право владения подразумевает иметь эту информацию в неизменном виде. Право пользования подразумевает право использовать эту информацию в своих интересах.

Таким образом, к информации, кроме субъекта права собственности на эту информацию, могут иметь доступ другие субъекты права собственности, как законно, санкционировано (субъекты права на элементы собственности), так и незаконно, несанкционированно.

Таким образом, цель защиты информации, заключается еще и в защите прав собственности на нее.

Объект защиты информации

Объектом защиты будем рассматривать всю совокупность носителей информации, которая представляет собой комплекс физических, аппаратных, программных и документальных средств [22].

Как правило, в последнее время информация используется, храниться, передается и обрабатывается в различного рода информационных системах (ИС).

Информационная система – это обычно прикладная программная, реже программно-аппаратная подсистема, ориентированная на сбор, хранение, поиск и обработку текстовой и/или фактографической информации.

Материальной основой существования информации в информационных системах, как правило, являются электронные и электронно-механические устройства (подсистемы), а также машинные носители. В качестве машинных носителей информации могут использоваться бумага, магнитные и оптические носители, электронные схемы.

Таким образом, необходимо защищать устройства и подсистемы, а также машинные носители информации.

В различных информационных системах пользователи информационных систем являются обслуживающим персоналом и могут являться источниками и носителями информации.

Поэтому понятие объекта защиты трактуется в более широком смысле. Под объектом защиты понимается не только информационные ресурсы, аппаратные и программные средства, обслуживающий персонал и пользователи, но и помещения, здания, а также прилегающая к зданиям территория.

Вопросы для самоконтроля

1. Определите предмет защиты информации.
2. Сформулируйте основные свойства информации.
3. Дайте определение конфиденциальной информации.
4. Перечислите уровни секретности государственной тайны.
5. Раскройте сущность основных подходов к измерению количества информации.
6. Раскройте сущность информации как объекта права собственности.
7. Раскройте сущность объекта защиты.

Практическая работа

Рассмотрение особенностей объекта защиты информации

Используя данные предыдущей практической работы, рассмотреть особенности каждого типа носителей информации, отметить плюсы и минусы каждого типа, условия хранения и обработки.

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Одним из важнейших аспектов проблемы обеспечения информационной безопасности является определение, анализ и классификация возможных угроз безопасности информации.

Угрозы можно классифицировать по отношению источника угрозы к объекту ИБ (внешние и внутренние), по виду источника угроз (физические, логические, коммуникационные, человеческие), по степени злого умысла (случайные и преднамеренные). Перечень угроз, оценки вероятностей их реализации, а также модель нарушителя служат основой для проведения анализа риска и формулирования требований к системе защиты информации [3, 10, 14, 15].

Под **угрозой безопасности** будем понимать потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности, конфиденциальности или доступности информации.

Все множество угроз можно разделить на два класса:

- случайные или непреднамеренные;
- преднамеренные (см. рис.2).

Случайные угрозы

Угрозы, которые не связаны с преднамеренными действиями злоумышленников и реализуются в случайные моменты времени, называют **случайным** или непреднамеренными.

Реализация угроз этого класса приводит к наибольшим потерям информации (по статистическим данным – до 80% от ущерба, наносимого информационным ресурсам любыми угрозами). При этом могут происходить уничтожение, нарушение целостности и доступности информации. Реже нарушается конфиденциальность информации, однако при этом создаются предпосылки для злоумышленного воздействия на информацию.

Стихийные бедствия и аварии чреваты наиболее разрушительными последствиями для материальных источников хранения информации, т.к. последние подвергаются физическому разрушению, информация утрачивается или доступ к ней становится невозможен.

Сбои и отказы сложных систем неизбежны. В результате нарушается работоспособность технических средств, уничтожаются и искажаются данные и программы. Нарушение работы отдельных узлов и устройств могут также привести к нарушению конфиденциальности

информации. Например, сбои и отказы средств выдачи информации могут привести к несанкционированному доступу к информации путем несанкционированной ее выдачи в канал связи, на печатающее устройство.

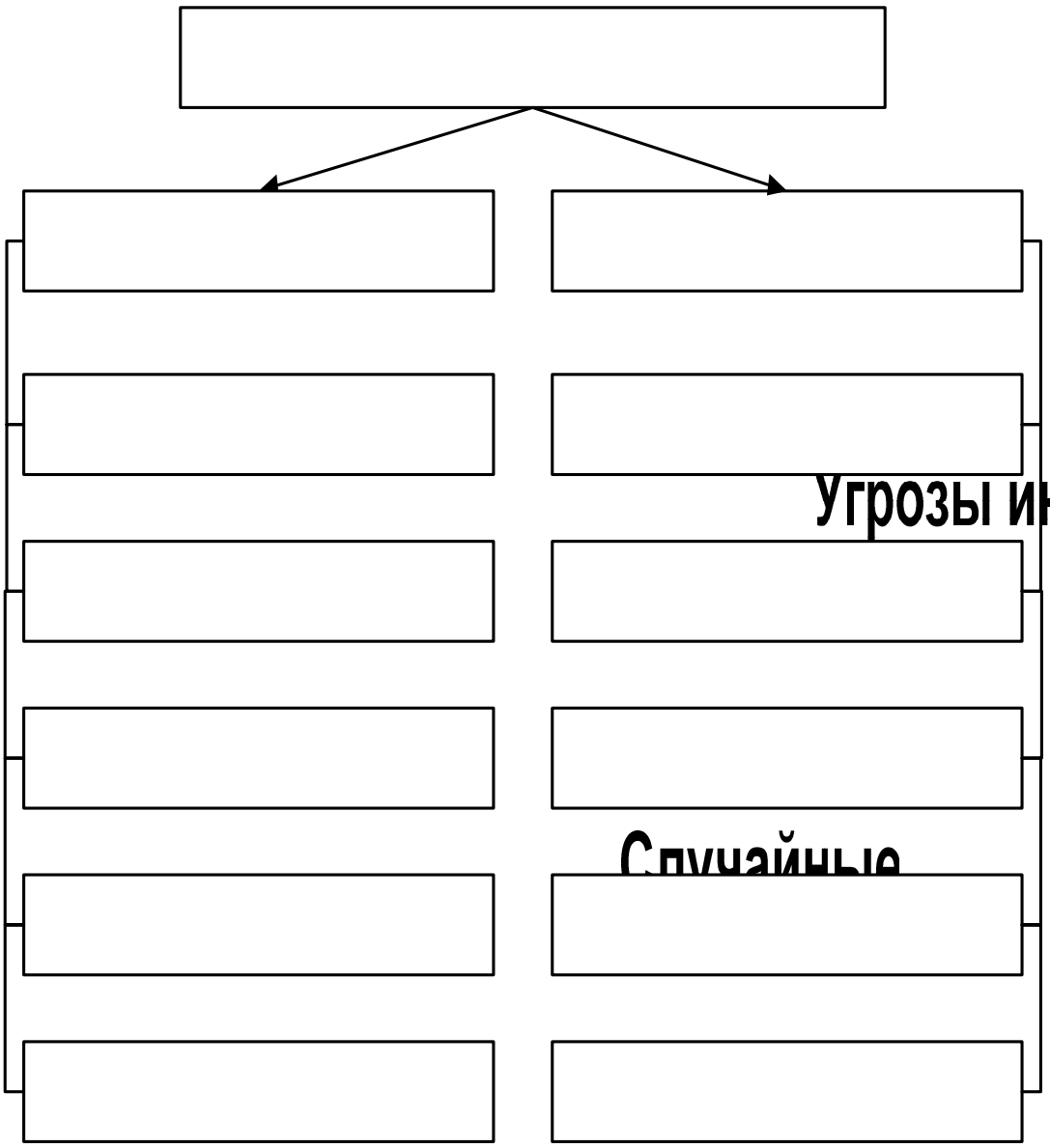

Рис. 2, Угрозы информационной безопасности

Ошибки при разработке информационной системы, алгоритмические и программные ошибки приводят к последствиям, аналогичным последствиям сбоев и отказов технических средств. Кроме того, такие ошибки могут быть использованы злоумышленниками для воздействия на ресурсы информационной системы. Особую опасность представляют ошибки в операционных системах и в программных средствах защиты информации.

Сбои и отказы технических средств

Согласно данным Национального института стандартов и технологий США, 65% случаев нарушения безопасности информации происходит в результате ошибок пользователей и обслуживающего персонала. Некомпетентное, небрежное или невнимательное выполнение функциональных обязанностей сотрудниками приводят к уничтожению, нарушению целостности и конфиденциальности информации, а также компрометации механизмов защиты.

Характеризуя угрозы информации, не связанные с преднамеренными действиями, в целом, следует отметить, что механизм их реализации изучен достаточно хорошо, накоплен значительный опыт противодействия этим угрозам. Современная технология разработки технических и программных средств, эффективная система эксплуатации информационных систем, включающая обязательное резервирование информации, позволяют значительно снизить потери от реализации угроз этого класса.

Преднамеренные угрозы

Второй класс угроз безопасности информации составляют преднамеренно создаваемые угрозы.

Данный класс угроз изучен недостаточно, очень динамичен и постоянно пополняется новыми угрозами. Угрозы этого класса в соответствии с их физической сущностью и механизмами реализации могут быть распределены по пяти группам:

- традиционный или универсальный шпионаж и диверсии;
- несанкционированный доступ к информации;
- электромагнитные излучения и наводки;
- модификация структур информационных систем;
- вредительские программы.

В качестве источников нежелательного воздействия на информационные ресурсы по-прежнему актуальны *методы и средства шпионажа и диверсий,* которые использовались и используются для добывания или уничтожения информации на объектах, не имеющих информационных систем. Эти методы также действенны и эффективны в условиях применения информационных систем. Чаще всего они используются для получения сведений о системе защиты с целью проникновения в информационную систему, а также для хищения и уничтожения информационных ресурсов [23].

К методам шпионажа и диверсий относятся:

- подслушивание;
- визуальное наблюдение;
- хищение документов и машинных носителей информации;

- хищение программ и атрибутов системы защиты;
- подкуп и шантаж сотрудников;
- сбор и анализ отходов машинных носителей информации;
- поджоги;
- взрывы.

Для *подслушивания* злоумышленнику не обязательно проникать на объект. Современные средства позволяют подслушивать разговоры с расстояния нескольких сотен метров. Так, прошла испытания система подслушивания, позволяющая с расстояния 1 км фиксировать разговор в помещении с закрытыми окнами. В городских. условиях дальность действия устройства сокращается до сотен и десятков метров в зависимости от уровня фонового шума. Принцип действия таких устройств основан на анализе отраженного луча лазера от стекла окна помещения, которое колеблется от звуковых волн. Колебания оконных стекол от акустических волн в помещении могут сниматься и передаваться на расстояния с помощью специальных устройств, укрепленных на оконном стекле. Такие устройства преобразуют механические колебания стекол в электрический сигнал с последующей передачей его по радиоканалу. Вне помещений подслушивание ведется с помощью сверхчувствительных направленных микрофонов. Реальное расстояние подслушивания с помощью направленных микрофонов составляет 50-100 метров.

Разговоры в соседних помещениях, за стенами зданий могут контролироваться с помощью стетоскопных микрофонов. Стетоскопы преобразуют акустические колебания в электрические. Такие микрофоны позволяют прослушивать разговоры при толщине стен до 50-100 см. Съем информации может осуществляться также и со стекол, металлоконструкций зданий, труб водоснабжения и отопления.

Аудиоинформация может, быть получена также путем высокочастотного навязывания. Суть этого метода заключается в воздействии высокочастотным электромагнитным полем или электрическими сигналами на элементы, способные модулировать эти поля, или сигналы электрическими или акустическими сигналами с речевой информацией. В качестве таких элементов могут использоваться различные полости с электропроводной поверхностью, представляющей собой высокочастотный контур с распределенными параметрами, которые меняются под действием акустических волн. При совпадении частоты такого контура с частотой высокочастотного навязывания и при наличии воздействия акустических воли на поверхность полости контур переизлучает и модулирует внешнее поле (высокочастотный электрический сигнал). Чаще всего этот метод прослушивания реали-

зуется с помощью телефонной линии. При этом в качестве модулирующего элемента используется телефонный аппарат, на который по телефонным проводам подается высокочастотный электрический сигнал. Нелинейные элементы телефонного аппарата под воздействием речевого сигнала модулируют высокочастотный сигнал. Модулированный высокочастотный сигнал может быть демодулирован в приемнике злоумышленника.

Одним из возможных каналов утечки звуковой информации может быть прослушивание переговоров, ведущихся с помощью средств связи. Контролироваться могут как проводные каналы связи, так и радиоканалы. Прослушивание переговоров по проводным и радиоканалам не требует дорогостоящего оборудования и высокой квалификации злоумышленника.

Дистанционная видеоразведка для получения информации в информационных системах малопригодна и носит, как правило, вспомогательный характер.

Видеоразведка организуемся в основном для выявления работы и расположения механизмов защиты информации. Из информационной системы информация реально может быть получена при истолковании на объекте экранов, табло, плакатов, если имеются прозрачные окна и перечисленные выше средства размещены без учета необходимости противодействовать такой угрозе.

Видеоразведка может вестись с использованием технических средств, таких как оптические приборы, фото-, кино- и телеаппаратура. Многие из этих средств допускают консервацию (запоминание) видеоинформации, а также передачу ее на определенные расстояния.

Еще около семи лет назад в прессе появлялись сообщения о создании в США мобильного микроробота для ведения дистанционной разведки. Пьезокерамический робот размером около 7 см и массой 60 г способен самостоятельно передвигаться со скоростью 30 см/с в течение 45 мин. За это время «микроразведчик» способен преодолеть расстояние в 810 метров, осуществляя транспортировку 28 г полезного груза (для сравнения – коммерческая микровидеокамера весит около 15 г).

Для вербовки сотрудников и физического уничтожения объектов информационной системы также не обязательно иметь непосредственный доступ на объект. Злоумышленник, имеющий доступ на объект информационной системы, может использовать любой из методов традиционного шпионажа.

Злоумышленниками, имеющими доступ на объект, могут использоваться миниатюрные средства фотографирования; видео- и ау-

диозаписи. Для аудио- и видеоконтроля помещений и при отсутствии в них злоумышленника могут использоваться закладные устройства или «жучки». Для объектов информационных систем наиболее вероятными являются закладные устройства, обеспечивающие прослушивание помещений. Закладные устройства делятся на проводные и излучающие. Проводные закладные устройства требуют значительного времени на установку и имеют существенный демаскирующий признак провода. Излучающие «закладки» («радиозакладки») быстро устанавливаются, но также имеют демаскирующий признак –излучение в радио или оптическом диапазоне. «Радиозакладки» могут использовать в качестве источника электрические сигналы или акустические сигналы. Примером использования электрических сигналов в качестве источника является применение сигналов внутренней телефонной, громкоговорящей связи. Наибольшее распространение получили акустические «радиозакладки». Они воспринимают акустический сигнал, преобразуют его в электрический и передают в виде радиосигнала на дальность до 8 км. Из применяемых на практике «радиозакладок» подавляющее большинство (около 90%) рассчитаны на работу в диапазоне расстояний 50 – 800 метров.

Для некоторых объектов информационных систем и хранения информации существует угроза вооруженного нападения террористических или диверсионных групп. При этом могут быть применены средства огневого поражения.

Термин несанкционированный доступ к информации (НСДИ) определен как доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств вычислительной техники или автоматизированных систем.

Под правилами разграничения доступа понимается совокупность положений, регламентирующих права доступа лиц или процессов (субъектов доступа) к единицам информации (объектам доступа).

Право доступа к ресурсам информационных систем определяется руководством для каждого сотрудника в соответствии с его функциональными обязанностями. Процессы инициируются в информационных системах в интересах определенных лиц, поэтому и на них накладываются ограничения по доступу к ресурсам.

Выполнение установленных правил разграничения доступа в информационных системах реализуется за счет создания системы разграничения доступа (СРД).

Несанкционированный доступ к информации возможен только с использованием штатных аппаратных и программных средств в следующих случаях:

- отсутствует система, разграничения доступа;
- сбой или отказ в информационной системе;
- ошибочные действия пользователей или обслуживающего персонала информационных систем;
- ошибки в СРД;
- фальсификация полномочий.

Если СРД отсутствует, то злоумышленник, имеющий навыки работы в информационной системе, может получить без ограничений доступ к любой информации. В результате сбоев или отказов средств системы, а также ошибочных действий обслуживающего персонала и пользователей возможны состояния системы, при которых упрощается НСДИ. Злоумышленник может выявить ошибки в СРД и использовать их для НСДИ. Фальсификация полномочий является одним из наиболее вероятных путей (каналов) НСДИ.

Процесс обработки и передачи информации техническими средствами сопровождается электромагнитными излучениями в окружающее пространство и наведением электрических сигналов в линиях связи, сигнализации, заземлении и других проводниках. Они получили названия *побочных электромагнитных излучений и наводок (ПЭМИН). С* помощью специального оборудования сигналы принимаются, выделяются, усиливаются и могут либо просматриваться, либо записываться в запоминающих устройствах. Наибольший уровень электромагнитного излучения присущ работающим устройствам отображения информации на электронно-лучевых трубках. Содержание экрана такого устройства может просматриваться с помощью обычного телевизионного приемника, дополненного несложной схемой, основной функцией которой является синхронизация сигналов. Дальность удовлетворительного приема таких сигналов при использовании дипольной антенны составляет 50 метров. Использование направленной антенны приемника позволяет увеличить зону уверенного приема сигналов до 1 км. Восстановление данных возможно также путем анализа сигналов излучения неэкранированного электрического кабеля на расстоянии до 300 метров. Наведенные в проводниках электрические сигналы могут выделяться и фиксироваться с помощью оборудования, подключаемого к этим проводникам на расстоянии в сотни метров от источника сигналов. Для добывания информации злоумышленник может использовать также «просачивание» информационных сигналов в цепи электропитания технических средств.

«Просачивание» информационных сигналов в цепи электропитания возможно при наличии магнитной связи между выходным трансформатором усилителя и трансформатором выпрямительного

устройства. «Просачивание» также возможно за счет падения напряжения на внутреннем сопротивлении источника питания при прохождении токов усиливаемых информационных сигналов. Если затухание в фильтре выпрямительного устройства недостаточно, то информационные сигналы могут быть обнаружены в цепи питания. Информационный сигнал может быть выделен в цепи питания за счет зависимости значений потребляемого тока в оконечных каскадах усилителей (информационные сигналы) и значений токов в выпрямителях, а значит и в выходных цепях.

Электромагнитные излучения используются злоумышленниками не только для получения информации, но и для ее уничтожения. Электромагнитные импульсы способны уничтожить информацию на магнитных носителях. Мощные электромагнитные и сверхвысокочастотные излучения могут вывести из строя электронные блоки системы. Причем для уничтожения информации на магнитных носителях с расстояния нескольких десятков метров может быть использовано устройство, помещающееся в портфель.

Большую угрозу безопасности информации в информационной системе представляет *несанкционированная модификация алгоритмической, программной и технической структур системы.*

Несанкционированная модификация структур может осуществляться на любом жизненном цикле информационной системы. Несанкционированное изменение структуры системы на этапах разработки и модернизации получило название «закладка». В процессе разработки системы «закладки» внедряются, как правило, в специализированные системы, предназначенные для эксплуатации в какой-либо фирме или государственных учреждениях. В универсальные системы «закладки» внедряются реже, в основном для дискредитации таких систем конкурентом или на государственном уровне, если предполагаются поставки системы во враждебное государство. «Закладки», внедренные на этапе разработки, сложно выявить ввиду высокой квалификации их авторов несложности современных информационных систем.

Алгоритмические, программные и аппаратные «закладки» используются либо для непосредственного вредительского воздействия на информационную систему, либо для обеспечения неконтролируемого входа в систему. Вредительские воздействия «закладок» на систему осуществляются при получении соответствующей команды извне (в основном характерно для аппаратных «закладок») и при наступлении определенных событий в системе. Такими событиями могут быть, переход на определенный режим работы (например, боевой ре-

жим системы управления оружием или режим устранения аварийной ситуации на атомной электростанции т. п.), наступление установленной даты, достижение определенной наработки и т.д.

Программные и аппаратные «закладки» для осуществления неконтролируемого входа в программы, использование привилегированных режимов работы (например, режимов операционной системы), обхода средств защиты информации получили название люки.

Одним из основных источников угроз безопасности информации в КС является использование специальных программ, получивших общее название *вредительские программы.* В зависимости от механизма действия вредительские программы делятся на четыре класса:

- *«логические бомбы»;*
- *«черви»;*
- *«троянские кони»;*
- *«компьютерные вирусы».*

«Логические бомбы». Это программы или их части, постоянно находящиеся в ЭВМ или вычислительных системах и выполняемые только при соблюдении определенных условий. Примерами таких условий могут быть: наступление заданной даты, переход системы в определенный режим работы, наступление некоторых событий установленное число раз и т.п.

«Червями» называются программы, которые выполняются каждый раз при загрузке системы, обладают способностью перемещаться в вычислительных системах или сети и само воспроизводить копии. Лавинообразное размножение программ приводит к перегрузке каналов связи, памяти и, в конечном итоге, к блокировке системы.

«Троянские кони». Это программы, полученные путем явного изменения или добавления команд в пользовательские программы. При последующем выполнении пользовательских программ наряду с заданными функциями выполняются несанкционированные, измененные или какие-то новые функции.

«Компьютерные вирусы». Это небольшие программы, которые после внедрения в ЭВМ самостоятельно распространяются путем создания своих копий, а при выполнении определенных условий оказывают негативное воздействие на информационные системы. Поскольку вирусам присущи свойства всех классов вредительских программ, то в последнее время любые вредительские программы часто называют вирусами.

Модель гипотетического нарушителя информационной безопасности

Для предотвращения возможных угроз необходимо не только обеспечить защиту информации, но и попытаться выявить категории нарушителей и те методы, которые они используют [4, 19].

Нарушитель – это лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

Злоумышленником будем называть нарушителя, намеренно идущего на нарушение из корыстных побуждений.

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

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

При разработке модели нарушителя определяются:

- предположения о категориях лиц, к которым может принадлежать нарушитель;
- предположения о мотивах действий нарушителя (преследуемых нарушителем целях);
- предположения о квалификации нарушителя и его технической оснащенности (об используемых для совершения нарушения методах и средства);
- ограничения и предположения о характере возможных действий нарушителей.

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

- пользователи (операторы) информационной системы;
- персонал, обслуживающий технические средства (инженеры, техники);
- сотрудники отделов разработки и сопровождения программного обеспечения (прикладные и системные программисты);

- технический персонал, обслуживающий здания (уборщики, электрики, сантехники и другие сотрудники, имеющие доступ в здания и помещения, где расположены компоненты информационной системы);
- сотрудники службы безопасности;
- руководители различных уровней должностной иерархии.

Посторонние лица, которые могут быть нарушителями:

- клиенты (представители организаций, граждане);
- посетители (приглашенные по какому-либо поводу);
- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго-, водо-, теплоснабжения и т.п.);
- представители конкурирующих организаций (иностранных спецслужб) или лица, действующие по их заданию;
- лица, случайно или умышленно нарушившие пропускной режим (без цели нарушить безопасность);
- любые лица за пределами контролируемой территории.

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

При нарушениях, вызванных безответственностью, пользователь целенаправленно или случайно производит какие-либо разрушающие действия, не связанные тем не менее со злым умыслом. В большинстве случаев это следствие некомпетентности или небрежности.

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

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

Всех нарушителей можно классифицировать следующим образом.

По уровню знаний об информационной системе:

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

- обладает высоким уровнем знаний и опытом работы с техническими средствами системы и их обслуживания;
- обладает высоким уровнем знаний в области программирования и вычислительной техники, проектирования и эксплуатации автоматизированных информационных систем;
- знает структуру, функции и механизм действия средств защиты, их сильные и слабые стороны.

По уровню возможностей (используемым методам и средствам):

- применяющий чисто агентурные методы получения сведений;
- применяющий пассивные средства (технические средства перехвата без модификации компонентов системы);
- использующий только штатные средства и недостатки систем защиты для ее преодоления (несанкционированные действия с использованием разрешенных средств), а также компактные магнитные носители информации, которые могут быть скрытно пронесены через посты охраны;
- применяющий методы и средства активного воздействия (модификация и подключение дополнительных технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ)

По времени действия:

- в процессе функционирования информационной системы (во время работы компонентов системы);
- в период неактивности компонентов системы (в нерабочее время, во время плановых перерывов в ее работе, перерывов для обслуживания и ремонта и т.п.);
- как в процессе функционирования системы, так и в период неактивности компонентов системы.

По месту действия:

- без доступа на контролируемую территорию организации;
- с контролируемой территории без доступа в здания и сооружения;
- внутри помещений, но без доступа к техническим средствам системы;
- с рабочих мест конечных пользователей (операторов);
- с доступом в зону данных (баз данных, архивов и т.п.);

- с доступом в зону управления средствами обеспечения безопасности.

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

- работа по подбору кадров и специальные мероприятия затрудняют возможность создания коалиций нарушителей, т.е. объединения (сговора) и целенаправленных действий по преодолению подсистемы защиты двух и более нарушителей;
- нарушитель, планируя попытки НСД, скрывает свои несанкционированные действия от других сотрудников;
- НСД может быть следствием ошибок пользователей, администраторов, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки информации и т.д.

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

Вопросы для самоконтроля

1. Составьте классификацию угроз информационной безопасности.
2. Раскройте основные группы классификации.
3. На основании чего строится модель нарушителя информационной безопасности?

Практическая работа

Определение угроз информационной безопасности и анализ рисков на предприятии

Исходя из целей защиты информации и носителей информации, выявленных на предыдущих занятиях, необходимо определить список угроз ИБ, характерных для данного предприятия.

Проанализировать риски, определить степень их допустимости. Составить модели нарушителей информационной безопасности, актуальных для данного предприятия.

СИСТЕМНОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

Как уже говорилось выше, для обеспечения информационной безопасности на основе политики информационной безопасности составляется программа защиты информации.
Программа безопасности имеет своей целью построение системы защиты информации.

Основные принципы построения системы защиты

Защита информации должна основываться на следующих основных принципах [15]:

- системности;
- комплексности; ч
- непрерывности защиты;
- разумной достаточности;
- гибкости управления и применения;
- открытости алгоритмов и механизмов защиты;
- простоты применения защитных мер и средств.

Системный подход к защите информационных ресурсов предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности.

При создании системы защиты необходимо учитывать все слабые, наиболее уязвимые места информационной системы, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и НСД к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

В распоряжении специалистов по безопасности имеется широкий спектр мер, методов и средств защиты.

Комплексно их использование предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонирование. Внешняя защита должна обеспечиваться физическими средствами, организационными и пра-

вовыми мерами. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж обороны.

Защита информации – это не разовое мероприятие и даже не определенная совокупность проведенных мероприятий и установленных средств защиты, а *непрерывный целенаправленный процесс,* предполагающий принятие соответствующих мер на всех этапах жизненного цикла информационной системы, начиная с самых ранних стадий проектирования, а не только на этапе ее эксплуатации.

Разработка системы зашиты должна вестись параллельно с разработкой самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, позволит создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных «закладок» и других средств преодоления системы защиты после восстановления ее функционирования.

Создать абсолютно непреодолимую систему защиты принципиально невозможно. При достаточном количестве времени и средств можно преодолеть любую защиту. Поэтому имеет смысл вести речь только о некотором приемлемом уровне безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть мощности и ресурсов и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми (задача анализа риска).

Часто приходится создавать систему защиты в условиях большой неопределенности. Поэтому принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Естественно, что для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую информационную систему, не нарушая процесса ее нор-

мального функционирования. Кроме того, внешние условия и требования с течением времени меняются. В таких ситуациях свойство гибкости спасает владельцев информационной системы от необходимости принятия кардинальных мер по полной замене средств защиты на новые.

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже автору). Однако, это вовсе не означает, что информация о конкретной системе защиты должна быть общедоступна.

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе законных пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

Методы защиты информации

Для построения системы защиты информации необходимо знать средства и методы защиты информации.

В соответствии с рассмотренными угрозами рассмотрим основные методы защиты информации [8. 13-15, 21].

Минимизация ущерба от аварий и стихийных бедствий

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

- правильного выбора места расположения объекта;
- учета возможных аварий и стихийных бедствий при разработке и эксплуатации системы;
- организации своевременного оповещения о возможных стихийных бедствиях;
- обучение персонала борьбе со стихийными бедствиями и авариями, методам ликвидации их последствий.

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

На практика далеко не всегда удается расположить объект вдалеке от опасных предприятий или районов с возможными стихийными бедствиями. Поэтому при разработке, создании и эксплуатации объектов информационных систем необходимо предусмотреть специальные; меры. В районах с возможными землетрясениями здания должны быть сейсмостойкими. В районах возможных затоплений основное оборудование целесообразно размещать на верхних этажах зданий. Все объекты должны снабжаться автоматическими системами тушения пожара. На объектах, для которых вероятность стихийных бедствий высока, необходимо осуществлять распределенное дублирование информации и предусмотреть возможность перераспределения функций объектов. На всех объектах должны предусматриваться меры на случай аварии в системах электропитания. Для объектов, работающих с ценной информацией, требуется иметь аварийные источники бесперебойного питания и подвод электроэнергии производить не менее чем от двух независимых линий электропередачи. Использование источников бесперебойного питания обеспечивает, по крайней мере, завершение вычислительного процесса и сохранение данных на внешних запоминающих устройствах.

Потери информационных ресурсов могут быть существенно уменьшены, если обслуживающий персонал будет своевременно предупрежден о надвигающихся природных катаклизмах. В реальных условиях такая информация часто не успевает дойти до исполнителей. Поэтому персонал должен быть обучен действиям в условиях стихийных бедствий и аварий, а также уметь восстанавливать утраченную информацию.

Дублирование информации

Для блокирования (парирования) случайных угроз безопасности информации в компьютерных системах должен быть решен целый комплекс задач.

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

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

По времени восстановления информации методы дублирования могут быть разделены на:

- оперативные;
- неоперативные.

К *оперативным* методам относятся методы дублирования информации, которые позволяют использовать дублирующую информацию в реальном масштабе времени. Это означает, что переход к использованию дублирующей информации осуществляется за время, которое позволяет выполнить запрос на использование информации в режиме реального времени для данной системы. Все методы, не обеспечивающие выполнения этого условия, относят к *неоперативным* методам дублирования.

По используемым для целей дублирования средствам методы дублирования можно разделить на методы, использующие:

- дополнительные внешние запоминающие устройства (блоки);
- специально выделенные области памяти на несъемных машинных носителях;
- съемные носители информации.

По числу копий методы дублирования делятся на:

- одноуровневые;
- многоуровневые.

Как правило, число уровней не превышает трех.

По степени пространственной удаленности носителей основной и дублирующей информации методы дублирования могут быть разделены на следующие методы:

- сосредоточенного дублирования;
- рассредоточенного дублирования.

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

В соответствии с процедурой дублирования различают методы:

- полного копирования:
- зеркального копирования;
- частичного копирования;
- комбинированного копирования.

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

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

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

Наконец, по виду дублирующей информации методы дублирования разделяются на:

- методы со сжатием информации;
- методы без сжатия информации.

Повышение надежности информационной системы

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

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

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

Надежность системы достигается на этапах:

- разработки;
- производства;
- эксплуатации.

Для программных средств рассматриваются этапы разработки и эксплуатации. Этап разработки программных средств является определяющим при создании надежных информационных систем.

На этом этапе основными направлениями повышения надежности программных средств являются:

- корректная постановка задачи на разработку;
- использование прогрессивных технологий программирования;
- контроль правильности функционирования.

Создание отказоустойчивых информационных систем

Отказоустойчивость – это свойство информационной системы сохранять работоспособность при отказах отдельных устройств, блоков, схем.

Известны три основных подхода к созданию отказоустойчивых систем:

- простое резервирование;
- помехоустойчивое кодирование информации;
- создание адаптивных систем.

Любая отказоустойчивая система обладает избыточностью. Одним из наиболее простых и действенных путей создания отказоустойчивых систем является **простое резервирование.** Простое резервирование основано на использовании устройств, блоков, узлов, схем только в качестве резервных. При отказе основного элемента осуществляется переход на использование резервного. Резервирование осуществляется на различных уровнях: на уровне устройств, на уровне блоков, узлов и т. д. Резервирование отличается также и глубиной. Для целей резервирования могут использоваться один резервный элемент и более. Уровни и глубина резервирования определяют возможности системы парировать отказы, а также аппаратные затраты. Такие системы должны иметь несложные аппаратно-программные средства контроля работоспособности элементов и средства перехода на использование, при необходимости, резервных элементов. Примером резервирования может служить использование «зеркальных» накопителей на жестких магнитных дисках. Недостатком простого резервирования является непроизводительное использование средств, которые применяются только для повышения отказоустойчивости.

Помехоустойчивое кодирование основано на использовании информационной избыточности. Рабочая информация в информационной системе дополняется определенным объемом специальной контрольной информации. Наличие этой контрольной информации (кон-

трольных двоичных разрядов) позволяет путем выполнения определенных действий над рабочей и контрольной информацией определять ошибки и даже исправлять их. Так как ошибки являются следствием отказов средств системы, то, используя исправляющие коды, можно парировать часть отказов.

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

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

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

Оптимизация взаимодействия пользователей и обслуживающего персонала

Одним из основных направлений защиты информации в информационных системах от непреднамеренных угроз являются сокращение числа ошибок пользователей и обслуживающего персонала, а также минимизация последствий этих ошибок. Для достижения этих целей необходимы:

- научная организация труда;
- воспитание и обучение пользователей и персонала;
- анализ и совершенствование процессов взаимодействия человека с системой.
- научная организация труда предполагает:
- оборудование рабочих мест;
- оптимальный режим труда и отдыха;
- дружественный интерфейс (связь, диалог) человека с системой.

Рабочее место пользователя или специалиста из числа обслуживающего персонала должно быть оборудовано в соответствии с рекомендациями эргономики. Освещение рабочего места; температурно-влажностный режим; расположение табло, индикаторов, клавиш и тумблеров управления; размеры и цвет элементов оборудования, по-

мещения; положение пользователя (специалиста) относительно оборудования; использование защитных средств – все это должно обеспечивать максимальную производительность человека в течение рабочего дня. Одновременно сводится к минимум утомляемость работника и отрицательное воздействие на его здоровье неблагоприятных факторов производственного процесса.

Одним из центральных вопросов обеспечения безопасности информации от всех классов угроз (в том числе и от преднамеренных) является вопрос воспитания и обучения обслуживающего персонала, а также пользователей корпоративных информационных систем.

У обслуживающего персонала и пользователей системы необходимо воспитывать такие качества как патриотизм (на уровне государства и на уровне корпорации), ответственность, аккуратность и др. Чувство патриотизма воспитывается у граждан страны за счет целенаправленной политики государства и реального положения дел в стране. Успешная политика государства внутри страны и на международной арене способствует воспитанию у граждан патриотизма, гордости за свое отечество. Не меньшее значение, особенно для негосударственных учреждений, имеет воспитание корпоративного патриотизма. В коллективе, где ценится трудолюбие, уважительное отношение друг к другу, поощряется аккуратность, инициатива и творчество, у работника практически не бывает внутренних мотивов нанесения вреда своему учреждению. Важной задачей руководства является также подбор и расстановка кадров с учетом их деловых и человеческих качеств.

Наряду с воспитанием специалистов большое значение в деле обеспечения безопасности информации имеет и обучение работников. Дальновидный руководитель не должен жалеть средств на обучение персонала. Обучение может быть организовано на различных уровнях. Прежде всего, руководство должно всемерно поощрять стремление работников к самостоятельному обучению. Важно обучать наиболее способных, трудолюбивых работников в учебных заведениях, возможно и за счет учреждения.

Методы и средства защиты информации от традиционного шпионажа и диверсий

Для защиты объектов информационных ресурсов от угроз данного класса должны быть решены следующие задачи [15, 21, 23]:

- создание системы охраны объекта;
- организация работ с конфиденциальными информационными ресурсами на объекте;

- противодействие наблюдению;
- противодействие подслушиванию;
- защита от злоумышленных действий персонала.

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

- контролируемая территория;
- здание:
- помещение;
- устройство, носитель информации;
- программа;
- информационные ресурсы.

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

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

Состав системы охраны зависит от охраняемого объекта. В общем случае СОО должна включать следующие компоненты:

- инженерные конструкции;
- охранная сигнализация:
- средства наблюдения:
- подсистема доступа на объект:
- дежурная смена охраны.

Инженерные конструкции служат для создания механических препятствий на пути злоумышленников. Они создаются по периметру контролируемой зоны. Инженерными конструкциями оборудуются также здания и помещения объектов. По периметру контролируемой территории используются бетонные или кирпичные заборы, решетки или сеточные конструкции. Для повышения защитных свойств заграждений поверх заборов укрепляется колючая проволока, острые стержни, армированная колючая лента. Последняя изготавливается путем армирования колючей ленты стальной оцинкованной проволокой диаметром 2,5 мм. Армированная колючая лента часто используется в виде спирали диаметром 500-955 мм. Для затруднения проникновения злоумышленника на контролируемую территорию могут использоваться малозаметные препятствия. Примером малозаметных препятствий может служить металлическая сеть из тонкой проволоки. Такая сеть располагается вдоль забора на ширину до 10 метров. Она исключает быстрое перемещение злоумышленника.

В здания и помещения злоумышленники пытаются проникнуть, как правило, через двери или окна. Поэтому с помощью инженерных конструкций укрепляют, прежде всего, это слабое звено в защите объектов. Надежность двери зависит от механической прочности самой двери и от надежности замков. Требования к механической прочности и способности противостоять несанкционированному открыванию предъявляются к замку.

Вместо механических замков все чаще используются кодовые замки. Самыми распространенными среди них (называемых обычно сейфовыми замками) являются дисковые кодовые замки с числом комбинаций кода ключа в пределах 10^6-10^7.

Наивысшую стойкость имеют электронные замки, построенные с применением микросхем. На базе электронных замков строятся автоматизированные системы контроля доступа в помещения. В каждый замок вводятся номера микросхем, владельцы которых допущены в соответствующее помещение. Может также задаваться индивидуальный временной интервал, в течение которого возможен доступ в помещение. Все замки могут объединяться в единую автоматизированную систему, центральной частью которой является ПЭВМ.

По статистике 85% случаев проникновения на объекты происходит через оконные проемы. Эти данные говорят о необходимости инженерного укрепления окон, которое осуществляется двумя путями:

- установка оконных решеток;
- применение стекол, устойчивых к механическому воздействию.

Охранная сигнализация служит для обнаружения попыток несанкционированного проникновения на охраняемый объект.

Системы охранной сигнализации должны отвечать следующим требованием:

- охват контролируемой зоны по всему периметру;
- высокая чувствительность к действиям злоумышленника;
- надежная работа в любых погодных и временных условиях;
- устойчивость к естественным помехам;
- быстрота и точность определения места нарушения;
- возможность централизованного контроля событий.

Охранная система представляет собой систему датчиков (извещателей), объединенных шлейфом сигнализации для подачи сигналов на приемно-контрольное устройство, которое выдает сигнал тревоги на оповещатель.

Датчик (извещатель) представляет собой устройство, формирующее электрический сигнал тревоги при воздействии на датчик или на создаваемое им поле внешних сил или объектов.

Шлейф сигнализации образует электрическую цепь для передачи сигнала тревоги от датчика к приемно-контрольному устройству.

Приемно-контрольное устройство служит для приема сигналов от датчике в, их обработки и регистрации, а также для выдачи сигналов в оповещатель.

Оповещатель выдает световые и звуковые сигналы дежурному охраннику.

По принципу обнаружения злоумышленников датчики делятся на:

- контактные;
- акустические;
- оптико-электронные;
- микроволновые;
- вибрационные;
- емкостные;
- телевизионные.

Организация непрерывного наблюдения или видеоконтроля за объектом является одной из основных составляющих системы охраны объекта. В современных условиях функция наблюдения за объектом реализуется с помощью систем замкнутого телевидения. Их называют также телевизионными системами видеоконтроля (ТСВ).

Телевизионная система видеоконтроля обеспечивает:

- автоматизированное видеонаблюдение за рубежами защиты;
- контроль за действиями персонала организации;
- видеозапись действий злоумышленников;
- режим видеоохраны.

В режиме видеоохраны ТСВ выполняет функции охранной сигнализации. Оператор ТСВ оповещается о движении в зоне наблюдения. В общем случае телевизионная система видеоконтроля включает следующие устройства:

- передающие телевизионные камеры;
- мониторы;
- устройство обработки и коммутации видеоинформации (УОКВ);
- устройства регистрации информации (УРИ).

Доступ на объекты производится на контрольно-пропускных пунктах (КПП), проходных, через контролируемый вход в здания и

помещения. На КПП и проходных дежурят контролеры из состава дежурной смены охраны. Вход в здания и помещения может контролироваться только техническими средствами. Проходные, КПП, входы в здания и помещения оборудуются средствами автоматизации и контроля доступа.

Одной из основных задач, решаемых при организации допуска на объект, является идентификация и аутентификация лиц, допускаемых на объект. Их называют субъектами доступа.

Под **идентификацией** понимается присвоение субъектам доступа идентификаторов и (или) сравнение предъявляемых идентификаторов с перечнем присвоенных идентификаторов, владельцы (носители) которых допущены на объект.

Аутентификация означает проверку принадлежности, субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

Различают два способа идентификации людей: атрибутивный и биометрический. *Атрибутивный способ* предполагает выдачу субъекту доступа либо уникального предмета, либо пароля (кода), либо предмета, содержащего код.

Предметами, идентифицирующими субъект доступа, могут быть пропуска, жетоны или ключи от входных дверей (крышек устройств), а также различного вида карточки.

Все атрибутивные идентификаторы обладают одним существенным недостатком. Идентификационный признак слабо или совсем не связан с личностью предъявителя.

Этого недостатка лишены методы биометрической идентификации. Они основаны на использовании индивидуальных биологических особенностей человека.

Для *биометрической идентификации* человека используются:

- папиллярные узоры пальцев;
- узоры сетчатки глаз;
- форма кисти руки;
- особенности речи;
- форма и размеры лица.
- динамика подписи;
- ритм работы на клавиатуре;
- запах тела;
- термические характеристики тела.

Основным достоинством биометрических методов идентификации является очень высокая вероятность обнаружения попыток несанкционированного доступа. Но этим методам присущи два недос-

татка. Даже в лучших системах вероятность ошибочного отказа в доступе субъекту, имеющему право на доступ, составляет 0,01. Затраты на обеспечение биометрических методов доступа, как правило, превосходят затраты на организацию атрибутивных методов доступа.

Для повышения надежности аутентификации используются несколько идентификаторов.

Подсистема доступа на объект выполняет также функции регистрации субъектов доступа и управления доступом.

Состав дежурной смены, его экипировка, место размещения определяется статусом охраняемого объекта. Используя охранную сигнализацию, системы наблюдения и автоматизации доступа, дежурная смена охраны обеспечивает только санкционированный доступ на объект и в охраняемые помещения. Дежурная смена может находиться на объекте постоянно или прибывать на объект при получении сигналов тревоги от систем сигнализации и наблюдения.

Наблюдение в оптическом диапазоне злоумышленником, находящимся за пределами объекта, малоэффективно. С расстояния 50 м даже совершенным длиннофокусным фотоаппаратом невозможно прочитать текст с документа или монитора. Кроме того, угрозы такого типа легко парируются с помощью:

- использования оконных стекол с односторонней проводимостью света;
- применения штор и защитного окрашивания стекол;
- размещения рабочих столов, мониторов, табло и плакатов таким образом, чтобы они не просматривались через окна или открытые двери.

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

- двери помещений были закрытыми;
- расположение столов и мониторов ЭВМ исключало возможность наблюдения документов или выдаваемой информации на соседнем столе или мониторе;
- стенды с конфиденциальной информацией имели шторы.

Методы борьбы с подслушиванием можно разделить на два класса. Таковыми являются:

- методы защиты речевой информации при передаче ее по каналам связи.
- методы защиты от прослушивания акустических сигналов в помещениях.

Речевая информация, передаваемая по каналам связи, защищается от прослушивания (закрывается) с использованием методов ана-

логового скремблирования и дискретизации речи с последующим шифрованием.

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

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

Применяются несколько *способов частотного преобразования* сигнала:

- частотная инверсия спектра сигнала;
- частотная инверсия спектра сигнала со смещением несущей частоты;
- разделение полосы частот речевого сигнала на поддиапазоны с последующей перестановкой и инверсией.

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

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

- звукоизоляция и звукопоглощение акустического сигнала;
- зашумление помещений или твердой среды для маскировки акустических сигналов;
- защита от несанкционированной записи речевой информации на диктофон;
- обнаружение и изъятие закладных устройств.

Вместе с тем, основными мероприятиями при защите от подслушивания и записи конфиденциальных переговоров выступают организационные, организационно-технические и технические меры [21].

Организационные меры предусматривают проведение архитектурно-планировочных, пространственных и режимных мероприятий.

Архитектурно-планировочные мероприятия основываются на предъявлении и реализации определенных требований на этапе проектирования защищаемых помещений или в период их реконструкции с

целью исключения или ослабления неконтролируемого распространения звуковых полей.

Пространственные мероприятия увязываются с предписанным выбором расположения выделенных для защиты помещений в пространственном плане и их оборудовании необходимыми для акустической безопасности элементами.

Режимные мероприятия предусматривают строгий контроль пребывания в охранной зоне сотрудников и посетителей.

Организационно-технические меры предполагают проведение мероприятий двух видов – пассивных (обеспечение звукоизоляции) и звукопоглощения) и активных (обеспечение звукоподавления), а также их комбинации.

Проведение *пассивных* мероприятий направлено на уменьшение величины акустического сигнала в местах предполагаемого расположения технических средств злоумышленника до уровня, гарантирующего невозможность перехвата такого сигнала.

Активные способы защиты, основанные на звукоподавлении, позволяют увеличить шумы на частоте приема информативного сигнала до значения, обеспечивающего гарантированное нарушение акустического канала утечки информации.

Технические меры включают в себя проведение мероприятий с привлечением специальных средств защиты конфиденциальных переговоров.

К специальным средствам и системам противодействия подслушиванию и записи относятся: средства и системы для обнаружения электромагнитных полей моторов, обеспечивающих продвижение записывающего носителя; программно-аппаратные комплексы для обнаружения диктофонов с флэш-памятью; устройства подавления диктофонов (высокочастотный генератор, генератор мощных ультразвуковых групп сигналов); системы противодействия мобильным телефонам как подслушивающим устройствам.Для защиты акустической информации от несанкционированной записи необходимо обнаружить работу записывающего устройства и принять эффективные меры противодействия его использованию (обнаружитель, блокиратор).

Методы и средства защиты от электромагнитных излучений и наводок

Все методы защиты от электромагнитных излучений и наводок можно разделить на **пассивные и активные.**

Пассивные методы обеспечивают уменьшение уровня опасного сигнала или снижение информативности сигналов.

Активные методы защиты направлены на создание помех в каналах побочных электромагнитных излучений и наводок, затрудняющих прием и выделение полезной информации из перехваченных злоумышленником сигналов.

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

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

Пассивные методы защиты от ПЭМИН могут быть разбиты на три группы:

- экранирование;
- снижение мощности излучений и наводок;
- снижение информативности сигналов.

Экранирование является одним из самых эффективных методов защиты от электромагнитных излучений. Под *экранированием* понимается размещение элементов информационной системы, создающих электрические, магнитные и электромагнитные поля, в пространственно замкнутых конструкциях. Способы экранирования зависят от особенностей полей, создаваемых элементами системы при протекании в них электрического тока.

В зависимости от типа создаваемого электромагнитного поля различают следующие виды экранирования:

- экранирование электрического поля;
- экранирование магнитного поля;
- экранирование электромагнитного поля.

К группе, обеспечивающей снижение мощности излучений и наводок, относятся следующие методы:

- изменение электрических схем;
- использование оптических каналов связи;
- изменение конструкции;
- использование фильтров;
- гальваническая развязка в системе питания.

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

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

Изменения конструкции сводятся к изменению взаимного расположения отдельных узлов, блоков, кабелей, сокращению длины шин.

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

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

Снижение информативности сигналов ПЭМИН, затрудняющее их использование при перехвате, осуществляется так:

- специальные схемные решения;
- кодирование информации.

В качестве примеров специальных схемных решений можно привести такие, как замена последовательного кода параллельным, увеличение разрядности параллельных кодов, изменение очередности развертки строк на мониторе и т. п. Эти меры затрудняют процесс получения информации из перехваченного злоумышленником сигнала.

Для предотвращения утечки информации может использоваться кодирование информации, в том числе и криптографическое преобразование.

Активные методы защиты от ПЭМИН предполагают применение генераторов шумов, различающихся принципами формирования маскирующих помех. В качестве маскирующих используются случайные помехи с нормальным законом распределения спектральной плотности мгновенных значений амплитуд (гауссовские помехи) и

прицельные помехи, представляющие собой случайную последовательность сигналов помехи, идентичных побочным сигналам.

Используется пространственное и линейное зашумление. *Пространственное зашумление* осуществляется за счет излучения с помощью антенн электромагнитных сигналов в пространство. Применяется *локальное пространственное зашумление* для защиты конкретного элемента системы и *объектовое пространственное зашумление* для защиты от побочных электромагнитных излучений всего объекта. При *локальном пространственном зашумлении* используются прицельные помехи. Антенна находится рядом с защищаемым элементом. *Объектовое пространственное зашумление* осуществляется, как правило, несколькими генераторами со своими антеннами, что позволяет создавать помехи во всех диапазонах побочных электромагнитных излучений всех излучающих устройств объекта.

Пространственное зашумление должно обеспечивать невозможность выделения побочных излучений на фоне создаваемых помех во всех диапазонах излучения и, вместе с тем, уровень создаваемых помех не должен превышать санитарных норм и норм по электромагнитной совместимости радиоэлектронной аппаратуры.

При использовании *линейного зашумления* генераторы прицельных помех подключаются к токопроводящим линиям для создания в них электрических помех, которые не позволяют злоумышленникам выделять наведенные сигналы.

Защита информации от несанкционированного доступа

Для осуществления НСДИ злоумышленник может не применять никаких аппаратных или программных средств. Он осуществляет НСДИ, используя [14, 15, 23]:

- знания о информационной системе и умения работать с ней;
- сведения о системе защиты информации;
- сбои, отказы технических и программных средств;
- ошибки, небрежность обслуживающего персонала и пользователей.

Для защиты информации от НСД создается система разграничения доступа к информации. Получить несанкционированный доступ к информации при наличии системы разграничения доступа (СРД) возможно только при сбоях и отказах системы, а также используя слабые места в комплексной системе защиты информации.

Для блокирования несанкционированного исследования и копирования информации используется комплекс средств и мер защиты,

которые объединяются в систему защиты от исследования и копирования информации (СЗИК).

Таким образом, СРД и СЗИК могут рассматриваться как подсистемы системы защиты от НСДИ.

Исходной информацией для создания СРД является решение владельца (администратора) системы в допуске пользователей к определенным информационным ресурсам. Так как информация в системе хранится, обрабатывается и передается файлами (частями файлов), то доступ к информации регламентируется на уровне файлов (объектов доступа). Сложнее организуется доступ в базе данных, в которых он может регламентироваться к отдельным ее частям по определенным правилам. При определении полномочий доступа администратор устанавливает операции, которые разрешено выполнять пользователю (субъекту доступа).

Различают следующие операции с файлами:

- чтение;
- запись;
- выполнение программ.

Операция записи в файл имеет две модификации.

Субъекту доступа может быть дано право осуществлять запись с изменением содержимого файла. Другая организация доступа предполагает разрешение только дописывания в файл, без изменения старого содержимого,

В информационных системах нашли применение два подхода к организации разграничения доступа:

- матричный;
- полномочный (мандатный).

Матричное управление доступом предполагает использование матриц доступа. Матрица доступа представляет собой таблицу, в которой объекту доступа соответствует столбец, а субъекту доступа – строка. На пересечении столбцов и строк записываются операции, которые допускается выполнять субъекту доступа с объектом доступа. Матричное управление доступом позволяет с максимальной детализацией установить права субъекта доступа по выполнению разрешенных операций над объектами доступа. Такой подход нагляден и легко реализуем. Однако в реальных системах из-за большого количества субъектов и объектов доступа матрица доступа достигает таких размеров, при которых сложно поддерживать ее в адекватном состоянии.

Полномочный или *мандатный* метод базируется на многоуровневой модели защиты. Документу присваивается уровень конфиденциальности (гриф секретности), а также могут присваиваться метки,

отражающие категории конфиденциальности (секретности) документа. Таким образом, конфиденциальный документ имеет гриф конфиденциальности (конфиденциально, строго конфиденциально, секретно, совершенно секретно и т. д.) и может иметь одну или несколько меток, которые уточняют категории лиц, допущенных к этому документу («для руководящего состава», «для инженерно-технического состава» и т. д.). Субъектам доступа устанавливается уровень допуска, определяющего максимальный для данного субъекта уровень конфиденциальности документа, к которому разрешается допуск. Субъекту доступа устанавливаются также категории, которые связаны с метками документа.

Правило разграничения доступа заключается в следующем: лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа равен или выше уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа, содержатся все категории, определенные для данного документа.

Правило разграничения доступа заключается в следующем: лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа равен или выше уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа, содержатся все категории, определенные для данного документа.

Система разграничения доступа к информации должна содержать четыре функциональных блока:

- блок идентификации и аутентификации субъектов доступа;
- диспетчер доступа;
- блок криптографического преобразования информации при ее хранении и передаче;
- блок очистки памяти.

Идентификация и аутентификация субъектов осуществляется в момент их доступа к устройствам, в том числе и дистанционного доступа.

Диспетчер доступа реализуется в виде аппаратно-программных механизмов и обеспечивает необходимую дисциплину разграничения доступа субъектов к объектам доступа (в том числе и к аппаратным блокам, узлам, устройствам). Диспетчер доступа разграничивает доступ к внутренним ресурсам системы субъектов, уже получивших доступ к этим системам (см. рис.3). Необходимость использования диспетчера доступа возникает только в многопользовательских информационных системах.

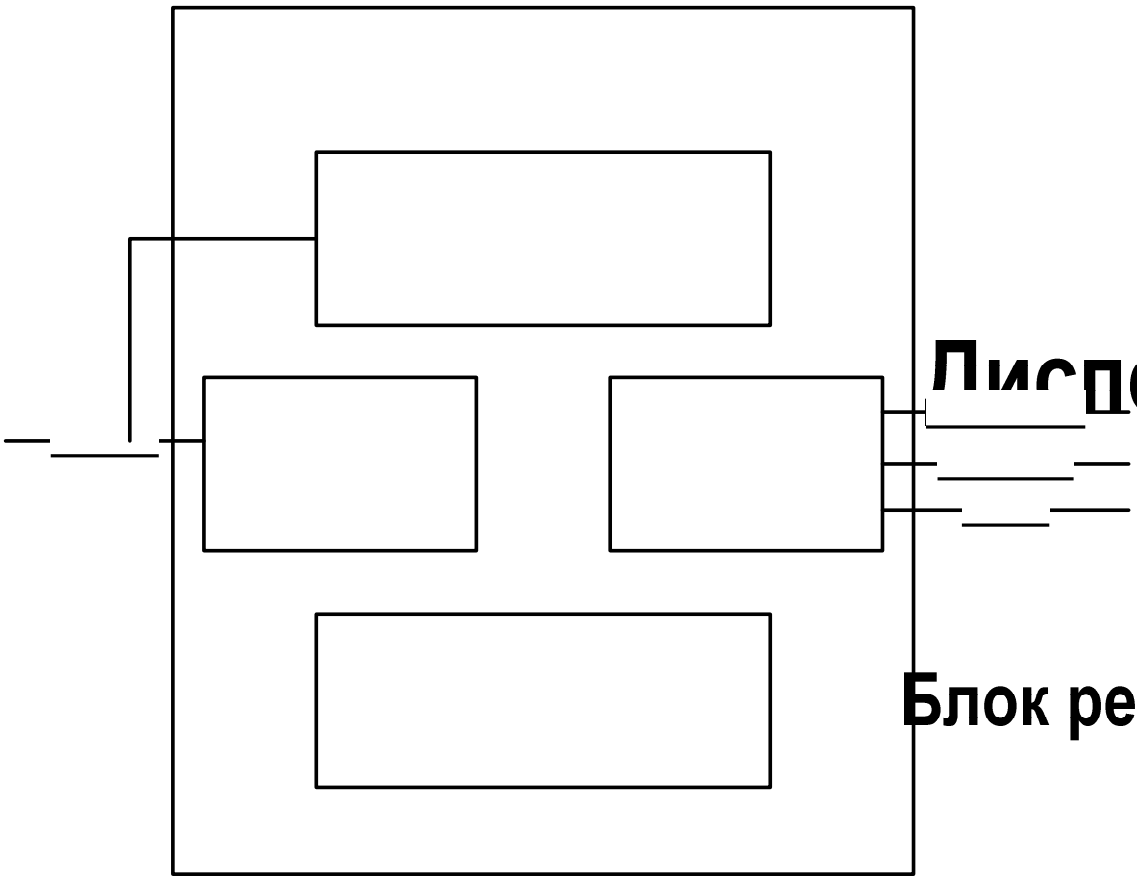

Рис. 3. Условная схема диспетчера доступа

Запрос на доступ *i-го* субъекта к *j-му* объекту поступает в блок управления базой полномочий и характеристик доступа и в блок регистрации событий. Полномочия субъекта и характеристики объекта доступа анализируются в блоке принятия решения, который выдает сигнал разрешения выполнения запроса, либо сигнал отказа в допуске. Если число попыток субъекта допуска получить доступ к запрещенным для него объектам превысит определенную границу (обычно 3 раза), то блок принятия решения на основании данных блока регистрации выдает сигнал администратору системы безопасности. Администратор может блокировать работу субъекта, нарушающего правила доступа в системе, и выяснить причину нарушений. Кроме преднамеренных попыток НСДИ диспетчер фиксирует нарушения правил разграничения, явившихся следствием отказов, сбоев аппаратных и программных средств, а также вызванных ошибками персонала и пользователей.

Модели защиты информации

Одной из первых моделей была опубликованная в 1977 модель Биба (BiBa). Согласно ей все субъекты и объекты предварительно разделяются по нескольким уровням доступа, а затем на их взаимодействия накладываются следующие ограничения:

- субъект не может вызывать на исполнение субъекты с более низким уровнем доступа;
- субъект не может модифицировать объекты с более высоким уровнем доступа.

Модель Гогена-Мезигера (Goguen-Meseguer), представленная ими в 1982 году, основана на теории автоматов. Согласно ей система может при каждом действии переходить из одного разрешенного состояния только в несколько других. Субъекты и объекты в данной модели защиты разбиваются на группы – домены, и переход системы из одного состояния в другое выполняется только в соответствии с так называемой таблицей разрешений, в которой указано какие операции может выполнять субъект, скажем, из домена C над объектом из домена D. В данной модели при переходе системы из одного разрешенного состояния в другое используются транзакции, что обеспечивает общую целостность системы.

Сазерлендская (от англ. Sutherland) модель защиты, опубликованная в 1986 году, делает акцент на взаимодействии субъектов и потоков информации. Так же как и в предыдущей модели, здесь используется машина состояний со множеством разрешенных комбинаций состояний и некоторым набором начальных позиций. В данной модели исследуется поведение множественных композиций функций перехода из одного состояния в другое.

Важную роль в теории защиты информации играет модель защиты Кларка-Вильсона (Clark-Wilson), опубликованная в 1987 году и модифицированная в 1989. Основана данная модель на повсеместном использовании транзакций и тщательном оформлении прав доступа субъектов к объектам. Но в данной модели впервые исследована защищенность третьей стороны в данной проблеме – стороны, поддерживающей всю систему безопасности. Эту роль в информационных системах обычно играет программа-супервизор. Кроме того, в модели Кларка-Вильсона транзакции впервые были построены по методу верификации, то есть идентификация субъекта производилась не только перед выполнением команды от него, но и повторно после выполнения. Это позволило снять проблему подмены автора в момент между его идентификацией и собственно командой. Модель Кларка-

Вильсона считается одной из самых совершенных в отношении поддержания целостности информационных систем.

Криптографические методы защиты информации

Криптография является методологической основой современных систем обеспечения безопасности информации, занимается поиском и исследованием математических методов преобразования информации. Сфера интересов криптоанализа – исследование возможности расшифровывания информации без знания ключей.

Под **криптографической защитой информации** понимается такое преобразование исходной информации, в результате которого она становится недоступной для ознакомления и использования лицами, не имеющими на это полномочий [15, 22].

Известны различные подходы к классификации методов криптографического преобразования информации. По виду воздействия на исходную информацию методы криптографического преобразования информации могут быть разделены на четыре группы: 1) шифрование; 2) стеганография; 3) кодирование; 4) сжатие.

Процесс **шифрования** заключается в проведении обратимых математических, логических, комбинаторных и других преобразований исходной информации, в результате которых зашифрованная информация представляет собой хаотический набор букв, цифр, других символов и двоичных кодов.

Для шифрования информации используются алгоритм преобразования и ключ. Как правило, алгоритм для определенного метода шифрования является неизменным. Исходными данными для алгоритма шифрования служат информация, подлежащая шифрованию, и ключ шифрования. Ключ содержит управляющую информацию, которая определяет выбор преобразования на определенных шагах алгоритма и величины операндов, используемые при реализации алгоритма шифрования. Преобразование шифрования может быть симметричным (с одним ключом) или ассиметричным (с двумя ключами) относительно преобразования расшифрования.

В отличие от других методов криптографического преобразования информации, методы **стеганографии** позволяют скрыть не толькосмысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации.

Содержанием процесса кодирования информации является замена смысловых конструкций исходной информации (слов, предложений) кодами. При кодировании и обратном преобразовании используются специальные таблицы или словари.

Сжатие информации может быть отнесено к методам криптографического преобразования информации с определенными оговорками. Целью сжатия является сокращение объема информации. В то же время сжатая информация не может быть прочитана или использована без обратного преобразования.

Даже если держать в секрете алгоритмы, то они могут быть сравнительно легко раскрыты статистическими методами обработки. Поэтому сжатые файлы конфиденциальной информации подвергаются последующему шифрованию. Для сокращения времени целесообразно совмещать процесс сжатия и шифрования информации.

Вопросы для самоконтроля

1. Сформулируйте основные принципы построения системы защиты информации.
2. Перечислите основные модели защиты информации и их особенности.
3. В чем заключается сущность методов защиты от случайных угроз?
4. Дайте определение понятиям идентификации и аутентификации.
5. Перечистите основные виды аутентификации.
6. В чем заключается повышение надежности и отказоустойчивости информационных систем?
7. Какую роль играет подготовленность персонала в построении системы защиты информации?
8. Какие методы и средства используются для организации противодействия традиционным методам шпионажа и диверсий?
9. Раскройте особенность построения защиты от несанкционированного доступа
10. Какие методы защиты информации относятся к криптографическим?

Практическая работа

Построение концепции безопасности предприятия

Определите, комплекс практических мероприятий, направленных на обеспечение информационной безопасности предприятия. Составьте программу информационной безопасности предприятия.

ВЫВОДЫ

Таковы основные положения информационной безопасности, методы и средства ее обеспечения. Безусловно, в данном пособии раскрыты не все методы защиты информации (их число постоянно расширяется и пополняется) или отражены неполно – более глубоко они изучаются в других учебных курсах. Однако, базовые положения, определения и методы отображены в данном учебном пособии.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. Азамов О. В. Информационная безопасность [Текст] / О. В. Азамов, К. Ю. Будылин, Е. Г. Бунев, С. А. Сакун, Д. Н. Шакин (Электронный ресурс) – http://www.naukaxxi.ru/materials/41/.
2. Байбурин В.Б., Введение в защиту информации.[Текст] / В.Б. Байбурин, М.Б. Бровкина и др.– М.: ФОРУМ: ИНФРА, 2004. – 128 с.
3. Гатчин Ю.А. Основы информационной безопасности [Текст]: учебное пособие/ Ю.А. Гатчин, Е.В. Климова. – СПб.: СПбГУ ИТМО, 2009. – 84с.
4. Гатчин Ю.А. Основы информационной безопасности компьютерных систем и защиты государственной тайны [Текст]: учебное пособие / Ю.А. Гатчин, Е.В. Климова, А.А. Ожиганов. – СПб.: СПбГУ ИТМО, 2001. – 60 с.
5. ГОСТ Р 50922-96. Защита информации. Основные термины и определения. [Текст].
6. Гринберг А.С. Защита информационных ресурсов государственного управления [Текст] / А.С. Гринберг, Н.Н. Горбачев, А.А. Тепляков. – М.: ЮНИТИ, 2003. – 327 с.
7. Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 года № Пр-1895. [Текст].
8. Завгородний В.И. Комплексная защита в компьютерных системах [Текст] / В.И. Завгородний. – М.: Логос, 2001. – 264 с.
9. Конев И.Р. Информационная безопасность предприятия [Текст] / И.Р. Конев, А.В. Беляев. – СПб.: БХВ-Петербург, 2003. – 752 с.
10. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации [Текст]. Учебное пособие для вузов / А.А Малюк. – М.: Горячая линия – Телеком, 2004. – 280 с.
11. Международная информационная безопасность: проблемы и перспективы [Текст] (Электронный ресурс) – http://www.mid.ru/ns-vnpop.nsf/.
12. Международная информационная безопасность: проблемы и перспективы // «Электросвязь», №8, 2008. – С. 2-4.
13. Мельников В. П. Информационная безопасность и защита информации [Текст]: учебное пособие для студентов высших учебных заведений / В.П. Мельников, С.А. Клейменов, .М.Петраков; под. ред. С.А.Клейменова. – М.: Издательский центр «Академия», 2009. – 336 с.

14. Мельников В. П. Защита информации в компьютерных системах [Текст] / В.П. Мельников. – М.: Финансы и статистика, 1997. – 368 с.
15. Павлухин Д.В. Теория информационной безопасности и методология защиты информации [Текст]: Учебно-методическое пособие / Д.В. Павлухин. – Тамбов: Изд-во ТГУ им. Г.Р. Державина, 2005. – 104 с.
16. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: Учебное пособие [Текст] / Ю.А. Родичев. – СПб.: Питер, 2008. – 272с.
17. Стратегия развития информационного общества в Российской Федерации от 7 февраля 2008 г. N Пр-212 [Текст].
18. Стратегии национальной безопасности Российской Федерации до 2020 года от 12 мая 2009 года N 537 [Текст].
19. Садердиниов А.А., Информационная безопасность предприятия [Текст] / А.А. Садердиниов, В.А. Трайнев, А.А. Федулов. – М.: Дашков и К, 2004. – 336 с.
20. Тарасюк М.В. Защищенные информационные технологии: Проектирование и применение [Текст] / М.В. Тарасюк. – М.: СОЛОН-Пресс, 2004. – 192 с.
21. Теоретические основы защиты информации от утечки по акустическим каналам [Текст]: учебное пособие / Ю.А. Гатчин, А.П. Карпик, К.О. Ткачев, К.Н. Чиков, В.Б. Шлишевский. – Новосибирск: СГГА, 2008. – 194 с.
22. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей [Текст]: учебное пособие / В.Ф. Шаньгин. – М.: ИД «ФОРУМ»: ИНФРА-М, 2009. – 416 с.
23. Ярочкин В.И. Информационная безопасность [Текст]: Учебник для вузов / В.И. Ярочкин – М.: Академический проект, 2008. – 544 с.