ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССОНАЛЬНОГО ОБРАЗОВАНИЯ
«ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ – УЧЕБНО-НАУЧНО-ПРОИЗВОДСТВЕННЫЙ КОМПЛЕКС»
УЧЕБНО-НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В.Т. Еременко

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ И СИСТЕМ

Рекомендовано ФГБОУ ВПО «Госуниверситет-УНПК»
для использования в учебном процессе в качестве учебного пособия
для высшего профессионального образования

Орел 2014

УДК 621.391
ББК 67.401+32.973.2-018.2
Е70

Рецензенты:
кафедра «Системы информационной безопасности»
ФГБОУ ВПО «Брянский государственный технический университет»

д.т.н., профессор кафедры «Информационные системы» ФГБОУ ВПО «Госуниверситет-УНПК» Раков В.И.

Еременко В.Т.
Е70 Основы информационной безопасности сетей и систем: учебное пособие для высшего профессионального образования / В.Т. Еременко – Орел: ФГБОУ ВПО «Госуниверситет - УНПК», 2014. – 207с.

Рассмотрены общие вопросы обеспечения информационной безопасности компьютерных систем, нормативно-правовая база в области защиты информации Российской Федерации, вопросы управления информационной безопасностью, предложены методики защиты информации при межсетевом взаимодействии.

Учебное пособие предназначено для преподавателей и студентов, обучающихся по специальностям, связанным с информационной безопасностью, а также может быть полезно руководителям и сотрудникам службы безопасности и служб защиты информации при обеспечении информационной безопасности информационных систем.

УДК 621.391
ББК 67.401+32.973.2-018.2

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В современных условиях, когда информационные компьютерные системы пронизывают все сферы деятельности предприятия, а с учетом необходимости их связи с Интернет они оказываются открытыми для реализации внутренних и внешних угроз, проблема информационной безопасности становится не менее важной, чем экономическая или физическая безопасность. Несмотря на важность рассматриваемой проблемы для подготовки специалистов по защите информации, отсутствует доступная учебная литература, нет подготовленных специалистов, имеющих практический опыт в области обеспечения информационной безопасности компьютерных систем разного вида.

Предлагаемое учебное пособие написано на основе материала, читаемого студентам по специальностям «Организация и технология защиты информации» и «Комплексное обеспечение информационной безопасности автоматизированных систем» с учетом существующих требований к их подготовке. Общая структура пособия включает следующую последовательность рассматриваемых вопросов:

– рассматривается организационно – правовое обеспечение информационной безопасности.

– рассматриваются основы информационной безопасности вычислительных сетей, основы формирования политики информационной безопасности и разрушающие программные воздействия и методы борьбы с ними;

– анализируются технологии анализа защищенности компьютерных систем;

– приводятся методики защиты информации при межсетевом взаимодействии и даются конкретные рекомендации по использованию VPN для защиты трафика;

Структура учебного пособия ориентирована на практическое использование рассматриваемого материала, во-первых, при изучении лекционного курса, во-вторых, при прохождении производственных практик, в-третьих, при выполнении курсовых и дипломных работ.

1. ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Система нормативно-правовых документов в области информационной безопасности

В настоящее время построение систем информационной безопасности в Российской Федерации базируется на нормативных документах и законодательных актах, охватывающих широкий круг вопросов защиты информации.

В качестве основы нормативно-правового регулирования информационной безопасности в Российской Федерации можно выделить следующие типы документов (рис. 1.1.) [1]:

- законы и подзаконные акты Российской Федерации;
- постановления правительства Российской Федерации;
- руководящие документы ФСТЭК России;
- государственные стандарты России (ГОСТы Р);
- отраслевые стандарты (ОСТы);
- ведомственные приказы и распоряжения;
- лицензии;
- сертификаты.

Законы и подзаконные акты Российской Федерации составляют основу всей нормативно-правовой базы по обеспечению информационной безопасности в нашей стране. Действующие в настоящее время законы России и подзаконные акты направлены на регулирование взаимоотношений различных субъектов, работающих в области обеспечения информационной безопасности, а также являются правовой основой органов, осуществляющих лицензирование различных видов деятельности в области информационной безопасности.

Постановления правительства Российской Федерации вводят перечень органов государственной власти, уполномоченных проводить лицензирование различных видов деятельности, а также регламентируют деятельность органов, осуществляющих сертификацию решений в области информационной безопасности.

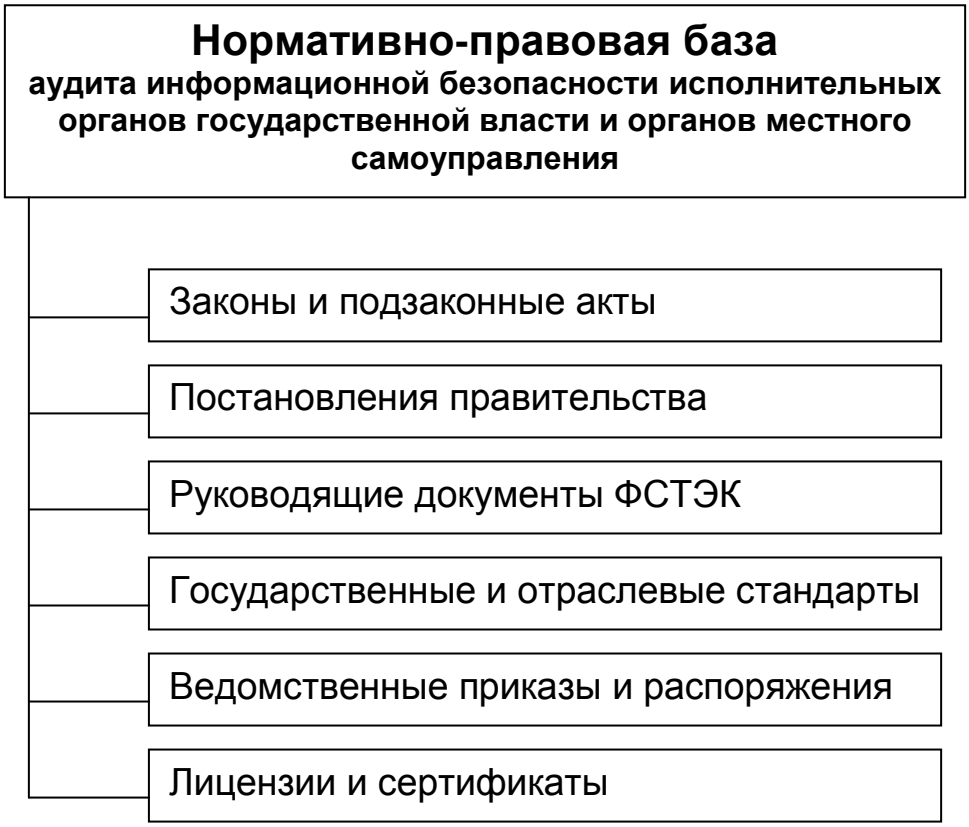

Рис. 1.1. Структура нормативно-правовой базы РФ в сфере ИБ

Руководящие документы Федеральной службы по техническому и экспортному контролю (ФСТЭК) России вводят различные категории и показатели защищенности средств по обеспечению информационной безопасности.

Государственные стандарты России (ГОСТы Р) устанавливают стандарты на различные технологические аспекты обеспечения информационной безопасности, применимые на всей территории Российской Федерации.

Отраслевые стандарты (ОСТы) устанавливают стандарты на различные технологические аспекты обеспечения информационной безопасности, применимые лишь в рамках деятельности какой-либо отрасли, работающей в сфере обеспечения информационной безопасности, на которую распространяется стандарт. Отдельный отраслевой стандарт по обеспечению информационной безопасности имеет, например, Центральный банк Российской Федерации.

Ведомственные приказы и распоряжения составляют основу работы различных ведомств, работающих в сфере информационной безопасности.

Лицензии. По существующим правилам разрабатывать, производить и реализовывать средства защиты информации может только предприятие, имеющее лицензию на эти виды деятельности. Лицензии выдаются на ограниченный срок, если условия для заявленного вида деятельности удовлетворят орган по лицензированию. При этом в течение срока действия лицензии орган по лицензированию следит за неизменностью (не ухудшением) условий заявленного вида деятельности.

Сертификаты. Наличие сертификата у продукта, обеспечивающего информационную безопасность, подтверждает его соответствие определенным требованиям, изложенным в руководящих документах ФСТЭК России, а также отсутствие в продукте недекларированных возможностей.

Нормативные документы, регулирующие вопросы информационной безопасности

Рассмотрим наиболее существенные нормативные документы Российской Федерации в сфере информационной безопасности, которые органы исполнительной власти и органы местного самоуправления должны использовать в процессе защиты информации ограниченного доступа [3, 4].

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [2] регулирует отношения, возникающие:

1) при осуществлении права на поиск, получение, передачу, производство и распространение информации;
2) применении информационных технологий;
3) обеспечении защиты информации.

Положения закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации.

Информация в зависимости от категории доступа к ней подразделяется на ***общедоступную информацию***, а также на

информацию, доступ к которой ограничен федеральными законами России (информация ограниченного доступа). Не может быть ограничен доступ к следующим видам информации:

1) нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;
2) информации о состоянии окружающей среды;
3) информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);
4) информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;
5) иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами. ***Защита информации*** представляет собой принятие правовых, организационных и технических мер, направленных на выполнение следующих требований:

1. Обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
2. Соблюдение конфиденциальности информации ограниченного доступа;
3. Реализация права на доступ к информации.

Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [2] регулирует отношения, связанные с обработкой персональных данных, осуществляемой федеральными

органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами, органами местного самоуправления, не входящими в систему органов местного самоуправления, муниципальными органами, юридическими лицами, физическими лицами с использованием средств автоматизации или без их использования.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Целью закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи» [2] обеспечивает правовые условия использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.

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

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

Электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

– сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки

или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;

− подтверждена подлинность электронной цифровой подписи в электронном документе;

− электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

Федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления, а также организации, участвующие в документообороте с указанными органами, используют для подписания своих электронных документов электронные цифровые подписи уполномоченных лиц указанных органов, организаций.

Сертификаты ключей подписей уполномоченных лиц федеральных органов государственной власти включаются в реестр сертификатов ключей подписей, который ведется уполномоченным федеральным органом исполнительной власти, и выдаются пользователям сертификатов ключей подписей из этого реестра в порядке, установленном настоящим федеральным законом для удостоверяющих центров.

Порядок организации выдачи сертификатов ключей подписей уполномоченных лиц органов государственной власти субъектов Российской Федерации и уполномоченных лиц органов местного самоуправления устанавливается нормативными правовыми актами соответствующих органов.

Доктрина информационной безопасности Российской Федерации [2], утвержденная Президентом Российской Федерации 9 сентября 2000 г., представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации. Доктрина развивает **Концепцию национальной безопасности Российской Федерации** применительно к информационной сфере. Служит основой:

1. Для формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;
2. Подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;

3. Разработки целевых программ обеспечения информационной безопасности Российской Федерации.

Указ Президента Российской Федерации от 6 марта 1997 г. 188 «Об утверждении перечня сведений конфиденциального характера» [4] утверждает следующий перечень сведений:

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;
2. Сведения, составляющие тайну следствия и судопроизводства;
3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);
4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);
5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна);
6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти [4] (утверждено постановлением правительства российской федерации от 3 ноября 1994 г. № 1233) определяет общий порядок обращения с документами и другими материальными носителями информации, содержащими служебную информацию ограниченного распространения, в федеральных органах исполнительной власти, а также на подведомственных им предприятиях, в учреждениях и организациях (далее - организациях). Положение не распространяется на порядок обращения с

документами, содержащими сведения, составляющие государственную тайну.

К служебной информации ограниченного распространения относится несекретная, касающаяся деятельности организаций информация, ограничения на распространение которой диктуются служебной необходимостью.

Не могут быть отнесены к служебной информации ограниченного распространения:

– акты законодательства, устанавливающие правовой статус государственных органов, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

– сведения о чрезвычайных ситуациях, опасных природных явлениях и процессах, экологическая, гидрометеорологическая, гидрогеологическая, демографическая, санитарно-эпидемиологическая и другая информация, необходимая для обеспечения безопасного существования населенных пунктов, граждан и населения в целом, а также производственных объектов;

– описание структуры органа исполнительной власти, его функций, направлений и форм деятельности, а также его адрес;

– порядок рассмотрения и разрешения заявлений, а также обращений граждан и юридических лиц;

– решения по заявлениям и обращениям граждан и юридических лиц, рассмотренным в установленном порядке;

– сведения об исполнении бюджета и использовании других государственных ресурсов, о состоянии экономики и потребностей населения;

– документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах организаций, необходимые для реализации прав, свобод и обязанностей граждан.

Служебная информация ограниченного распространения без санкции соответствующего должностного лица не подлежит разглашению (распространению). руководитель федерального органа исполнительной власти в пределах своей компетенции определяет:

– категории должностных лиц, уполномоченных относить служебную информацию к разряду ограниченного распространения;

– порядок передачи служебной информации ограниченного распространения другим органам и организациям;

− порядок снятия пометки "для служебного пользования" с носителей информации ограниченного распространения;
− организацию защиты служебной информации ограниченного распространения.

Положение о лицензировании деятельности по технической защите конфиденциальной информации [2] (утверждено постановлением правительства российской федерации от 15 августа 2006 г. № 504) определяет порядок лицензирования деятельности по технической защите конфиденциальной информации, осуществляемой юридическими лицами и индивидуальными предпринимателями.

Под технической защитой конфиденциальной информации понимается комплекс мероприятий и (или) услуг по ее защите от несанкционированного доступа, в том числе и по техническим каналам, а также от специальных воздействий на такую информацию с целью ее уничтожения, искажения или блокирования доступа к ней. Лицензирование деятельности по технической защите конфиденциальной информации осуществляет федеральная служба по техническому и экспортному контролю.

1.3. Руководящие и нормативно-методические документы в сфере информационной безопасности

Помимо нормативно-правовых актов, в Российской Федерации используют при обеспечении информационной безопасности ряд руководящих и нормативно-методических документов [2,4].

Положение об аттестации объектов информатизации по требованиям безопасности информации *(Утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.)* устанавливает основные принципы, организационную структуру системы аттестации объектов информатизации по требованиям безопасности информации, порядок проведения аттестации, а также контроля и надзора за аттестацией и эксплуатацией аттестованных объектов информатизации.

Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате

которых посредством специального документа - "Аттестата соответствия" – подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации.

Положение о сертификации средств защиты информации по требованиям безопасности информации *(Утверждено приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 27 октября 1995 г. № 199)* устанавливает организационную структуру системы сертификации средств защиты информации по требованиям безопасности информации, функции субъектов сертификации, порядок сертификации, государственного контроля и надзора, инспекционного контроля за соблюдением правил обязательной сертификации и за сертифицированными средствами защиты информации, общие требования к нормативным и методическим документам по сертификации средств защиты информации.

Под сертификацией средств защиты информации по требованиям безопасности информации понимается деятельность по подтверждению характеристик средств защиты информации требованиям государственных стандартов или иных нормативных документов по защите информации.

В приложениях к положению приведены перечень средств защиты информации, подлежащих сертификации в системе сертификации, формы заявок на проведение сертификации и продление срока действия сертификата, решения по заявке на проведение сертификации (продлению срока действия сертификата), сертификата и лицензии на применение знака соответствия.

Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации *(Утверждена решением Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.)* излагает систему взглядов, основных принципов, которые закладываются в основу проблемы защиты информации от несанкционированного доступа (НСД), являющейся частью общей проблемы безопасности информации.

Концепция предусматривает существование двух относительно самостоятельных и, следовательно, имеющих отличие направлений в

проблеме защиты информации от НСД: направление, связанное со средствами вычислительной техники (СВТ), и направление, связанное с автоматизированными системами (АС).

Отличие двух направлений порождено тем, что СВТ разрабатываются и поставляются на рынок лишь как элементы, из которых в дальнейшем строятся функционально ориентированные АС, и поэтому, не решая прикладных задач, СВТ не содержат пользовательской информации. Помимо пользовательской информации, при создании АС появляются такие отсутствующие при разработке СВТ характеристики АС, как полномочия пользователей, модель нарушителя, технология обработки информации.

НСД определяется как доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения СВТ или АС.

Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. (*Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г.).* Устанавливает термины и определения понятий в области защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Установленные термины обязательны для применения во всех видах документации.

Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. *(утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г).* Устанавливает классификацию средств вычислительной техники по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

Под СВТ понимается совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Устанавливается семь классов защищенности СВТ от НСД к информации. Самый низкий класс – седьмой, самый высокий – первый. Выбор класса защищенности СВТ для автоматизированных систем, создаваемых на базе защищенных СВТ, зависит от грифа секретности обрабатываемой в АС информации, условий эксплуатации и расположения объектов системы.

Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. *(Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.).* Устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов.

Классификация распространяется на все действующие и проектируемые АС учреждений, организаций и предприятий, обрабатывающие конфиденциальную информацию.

Устанавливается девять классов защищенности АС от НСД к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

– наличие в АС информации различного уровня конфиденциальности;
– уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
– режим обработки данных в АС - коллективный или индивидуальный.

Специальные требования и рекомендации по технической защите конфиденциальной информации. (Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282). Устанавливают порядок организации работ, требования и рекомендации по обеспечению технической защиты конфиденциальной информации на территории Российской Федерации и являются основным

руководящим документом в этой области для федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, предприятий, учреждений и организаций независимо от их организационно-правовой формы и формы собственности, должностных лиц и граждан Российской Федерации, взявшим на себя обязательства либо обязанным по статусу исполнять требования правовых документов Российской Федерации по защите информации.

Требования и рекомендации настоящего документа распространяются на защиту:

– конфиденциальной информации – информации с ограниченным доступом, за исключением сведений, отнесенных к государственной тайне и персональным данным, содержащейся в государственных (муниципальных) информационных ресурсах, накопленной за счет государственного (муниципального) бюджета и являющейся собственностью государства (к ней может быть отнесена информация, составляющая служебную тайну и другие виды тайн в соответствии с законодательством Российской Федерации, а также сведения конфиденциального характера в соответствии с "Перечнем сведений конфиденциального характера", утвержденного Указом Президента Российской Федерации от 06.03.97 №188), защита которой осуществляется в интересах государства;

– информации о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющей идентифицировать его личность (персональные данные)

Документ определяет следующие основные вопросы защиты информации:

– организацию работ по защите информации, в том числе при разработке и модернизации объектов информатизации и их систем защиты информации;

– состав и основное содержание организационно-распорядительной, проектной, эксплуатационной и иной документации по защите информации;

– требования и рекомендации по защите речевой информации при осуществлении переговоров, в том числе с использованием технических средств;

– требования и рекомендации по защите информации при ее автоматизированной обработке и передаче с использованием технических средств;

– порядок обеспечения защиты информации при эксплуатации объектов информатизации;
– особенности защиты информации при разработке и эксплуатации автоматизированных систем, использующих различные типы средств вычислительной техники и информационные технологии;
– порядок обеспечения защиты информации при взаимодействии абонентов с информационными сетями общего пользования.

Государственные стандарты Российской Федерации в сфере обеспечения ИБ

Важное место в системе информационной безопасности занимают стандарты России, касающиеся сферы информационной безопасности [1].

ГОСТ Р 50922-96 «Защита информации. Основные термины и определения» устанавливает основные термины и их определения в области защиты информации. Термины, установленные настоящим стандартом, обязательны для применения во всех видах документации и литературы по защите информации. Ниже приведены некоторые термины и их определения.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. Собственником информации может быть государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Защита информации – деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Система защиты информации – совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

Объект защиты – информация или носитель информации или информационный процесс, в отношении которых необходимо

обеспечивать защиту в соответствии с поставленной целью защиты информации.

Категорирование защищаемой информации [объекта защиты] – установление градаций важности защиты защищаемой информации [объекта защиты].

Средство защиты информации – техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации.

Контроль эффективности защиты информации – проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты информации.

ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью» устанавливает рекомендации по управлению информационной безопасностью лицам, ответственным за планирование, реализацию или поддержку решений безопасности в организации. Он предназначен для обеспечения общих основ разработки стандартов безопасности и выбора практических мероприятий по управлению безопасностью в организации, а также в интересах обеспечения доверия в деловых отношениях между организациями. Рекомендации настоящего стандарта следует выбирать и использовать в соответствии с действующим в России законодательством.

Данный стандарт идентичен международному стандарту ИСО/МЭК 17799:2000 «Информационная технология. Практические правила управления информационной безопасностью» (ISO/IEC 17799:2000 "Information technology. Code of practice for security management") и может использоваться в качестве критериев для оценки механизмов безопасности организационного уровня, включая административные, процедурные и физические меры защиты.

Стандарт включает 10 разделов:

1. *Политика безопасности*
   - Документальное оформление
   - Пересмотр и оценка
2. *Организационные меры по обеспечению безопасности*
   - Организация и управление информационной безопасностью
   - Безопасность доступа сторонних организаций

- Условия безопасности в контрактах, заключенных со сторонними организациями

3. *Классификация ресурсов и их контроль*
   - Инвентаризация ресурсов
   - Классификация ресурсов
4. *Безопасность персонала*
   - Безопасность при выборе и работе с персоналом
   - Обучение персонала
   - Реагирование на события, угрозу безопасности
5. *Физическая безопасность*
   - Защищенные области
   - Защита оборудования
6. *Администрирование компьютерных систем и вычислительных сетей*
   - Рабочие процедуры и ответственность
   - Планирование работы систем и их приемка
   - Защита от вредоносного программного обеспечения
   - Обслуживание систем
   - Сетевое администрирование
   - Оперирование с носителями информации и их защита
   - Обмен данными и программами
7. *Управление доступом к системам*
   - Производственные требования к управлению и системам
   - Управление доступом пользователей
   - Обязанности пользователей
   - Управление доступом к сети
   - Управление доступом к компьютерам
   - Управление доступом к приложениям
   - Слежение за доступом к системам и их использование
8. *Разработка и сопровождение информационных систем*
   - Требования к безопасности систем
   - Безопасность в прикладных системах
   - Защита файлов прикладных программ
   - Безопасность в среде разработки и рабочей среде
9. *Планирование бесперебойной работы организации*
   - Вопросы планирования бесперебойной работы организации

- Тестирование планов обеспечения бесперебойной работы организации

10. Соответствие системы основным требованиям

- Выполнение правовых требований
- Проверка безопасности информационных систем
- Аудит систем

В этих разделах содержится описание механизмов безопасности организационного уровня, реализуемых в настоящее время в правительственных и коммерческих организациях во многих странах мира.

Согласно стандарту ключевыми механизмами управления ИБ (средствами контроля) являются следующие:

– документ о политике информационной безопасности;

– распределение обязанностей по обеспечению информационной безопасности;

– обучение и подготовка персонала к поддержанию режима информационной безопасности;

– уведомление о случаях нарушения защиты;

– средства защиты от вирусов;

– планирование бесперебойной работы организации;

– контроль над копированием программного обеспечения, защищенного законом об авторском праве;

– защита документации организации;

– защита данных;

– контроль соответствия политике безопасности.

Данный стандарт должен расцениваться как отправная точка для разработки руководств под конкретные нужды организации. Не все инструкции и мероприятия, приведенные в нем, могут быть применимыми.

ГОСТ ИСО/МЭК 15408-2002 «Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий» предназначен для использования в качестве основы при оценке характеристик безопасности продуктов и систем информационных технологий (ИТ).

Стандарт полностью соответствует международному стандарту ИСО/МЭК 15408-99 «Информационная технология. Методы и

средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» (ISO/IEC 15408:1999 “Information technology. Security techniques. Evaluation criteria for IT security”).

Устанавливая общую базу критериев, стандарт делает результаты оценки безопасности ИТ значимыми для более широкой аудитории. Для потребителей средств и систем защиты информации критерии и методики оценки, предложенные в данном стандарте, играют важную роль в поддержке выбора конкретных программных и программно-аппаратных продуктов для наиболее полного и экономически эффективного выражения своих потребностей.

Стандарт применим к мерам безопасности ИТ, реализуемым аппаратными, программно-аппаратными и программными средствами. Стандарт не содержит критериев оценки безопасности, касающихся административных мер безопасности, специальных физических аспектов ИБ (паразитных излучений и наводок), специфических качеств криптографических алгоритмов.

ГОСТ ИСО/МЭК 15408-2002 состоит из трех основных разделов. В первом постулированы ключевые идеологические и методологические аспекты его применения. Второй содержит общие требования к системам защиты информации и набор параметров, которыми может быть описан каждый тип таких средств. Из этих параметров формируются специальные документы - профили защиты. Они содержат детализированные наборы функциональных требований к средствам защиты различных классов и к процедуре их испытаний. Третий раздел описывает применение так называемых оценочных уровней доверия - наборов требований к разработке, поставке и эксплуатации средств и систем ИБ.

Потенциально сертификация и аттестация по данному стандарту может прийти на смену системе сертификации и аттестации на основе руководящих документов ФСТЭК, однако на данный момент практика использования ГОСТ ИСО/МЭК 15408-2002 недостаточно распространена и условий для обязательного перехода государственных и муниципальных структур на этот стандарт не создано.

ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» устанавливает единые функциональные требования к защите СВТ от НСД к информации; к составу

документации на эти средства, а также номенклатуру показателей защищенности СВТ, описываемых совокупностью требований к защите и определяющих классификацию СВТ по уровню защищенности от НСД к информации.

Требования к защите реализуются в СВТ в виде совокупности программно-технических средств защиты.

Защищенность от НСД к информации при ее обработке СВТ характеризуется тем, что только надлежащим образом уполномоченные лица или процессы, инициированные ими, будут иметь доступ к чтению, записи, созданию или уничтожению информации.

Защищенность обеспечивается тремя группами требований к средствам защиты, реализуемым в СВТ:

– требования к разграничению доступа, предусматривающие то, что СВТ должны поддерживать непротиворечивые, однозначно определенные правила разграничения доступа;

– требования к учету, предусматривающие то, что СВТ должны поддерживать регистрацию событий, имеющих отношение к защищенности информации;

– требования к гарантиям, предусматривающие необходимость наличия в составе СВТ технических и программных механизмов, позволяющих получить гарантии того, что СВТ обеспечивают выполнение требований к разграничению доступа и к учету.

Стандарт следует использовать при разработке технических заданий, при формулировании и проверке требований к защите информации.

2. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

2.1. Особенности обеспечения информационной безопасности в компьютерных сетях

Основной особенностью любой компьютерной вычислительной сети является то, что ее компоненты распределены в пространстве и связь между ними физически осуществляется при помощи сетевых соединений и программно при помощи механизма сообщений. При этом все управляющие сообщения и данные, пересылаемые между объектами распределенной вычислительной системы, передаются по сетевым соединениям в виде пакетов обмена.

Сетевые системы характерны тем, что наряду с локальными угрозами, осуществляемыми в пределах одного компьютера, на них действуют специфические угрозы, обусловленные распределенностью аппаратных и программных средств, а также данных в пространстве. Это так называемые сетевые или удаленные угрозы. Их особенности заключаются в том, что злоумышленник может находиться на большом расстоянии от атакуемого объекта, а объектом нападения является информация, передающаяся по сетевым соединениям. С развитием локальных и глобальных сетей именно удаленные атаки становятся лидирующими как по количеству попыток, так и по успешности их применения, а, значит, обеспечение безопасности вычислительных сетей приобретает первостепенное значение [14].

Удаленная угроза – потенциально возможное информационное разрушающее воздействие на распределенную вычислительную сеть, осуществляемая программно по каналам связи. Это определение охватывает обе особенности сетевых систем – распределенность компьютеров и распределенность информации. Поэтому при рассмотрении вопросов информационной безопасности вычислительных сетей рассматриваются два подвида удаленных угроз – это удаленные угрозы на инфраструктуру и протоколы сети и удаленные угрозы на телекоммуникационные службы.

Цели сетевой безопасности могут меняться в зависимости от ситуации, но основные цели обычно связаны с обеспечением составляющих «информационной безопасности»:

– целостности данных;

– конфиденциальности данных;
– доступности данных.

Целостность данных – одна из основных целей информационной безопасности сетей – предполагает, что данные не были изменены, подменены или уничтожены в процессе их передачи по линиям связи, между узлами вычислительной сети. Целостность данных должна гарантировать их сохранность, как в случае злонамеренных действий, так и случайностей. Обеспечение целостности данных является обычно одной из самых сложных задач сетевой безопасности.

Конфиденциальность данных – вторая главная цель сетевой безопасности. При информационном обмене в вычислительных сетях большое количество информации относится к конфиденциальной, например, личная информация пользователей, учетные записи (имена и пароли), данные о кредитных картах и др.

Доступность данных – третья цель безопасности данных в вычислительных сетях. Функциями вычислительных сетей являются совместный доступ к аппаратным и программным средствам сети и совместный доступ к данным. Нарушение информационной безопасности как раз и связано с невозможностью реализации этих функций.

В локальной сети должны быть доступны: принтеры, серверы, рабочие станции, данные пользователей и др.

В глобальных вычислительных сетях должны быть доступны информационные ресурсы и различные сервисы, например, почтовый сервер, сервер доменных имен, web-сервер и др.

При рассмотрении вопросов, связанных с информационной безопасностью, в современных вычислительных сетях необходимо учитывать следующие факторы:
– глобальную связанность;
– разнородность корпоративных информационных систем;
– распространение технологии «клиент-сервер».

Применительно к системам связи глобальная связанность означает, что речь идет о защите сетей, пользующихся внешними сервисами, основанными на протоколах TCP/IP, и предоставляющих аналогичные сервисы вовне. Весьма вероятно, что внешние сервисы находятся в других странах, поэтому от средств защиты в данном случае требуется следование стандартам, признанным на международном уровне. Национальные границы, законы, стандарты

не должны препятствовать защите потоков данных между клиентами и серверами.

Из факта глобальной связанности вытекает также меньшая эффективность мер физической защиты, общее усложнение проблем, связанных с защитой от несанкционированного доступа, необходимость привлечения для их решения новых программно-технических средств, например, межсетевых экранов.

Разнородность аппаратных и программных платформ требует от изготовителей средств защиты соблюдения определенной технологической дисциплины. Важны не только чисто защитные характеристики, но и возможность встраивания этих систем в современные корпоративные информационные структуры. Если, например, продукт, предназначенный для криптографической защиты, способен функционировать исключительно на платформе Wintel (Windows+Intel), то его практическая применимость вызывает серьезные сомнения.

Корпоративные информационные системы оказываются разнородными еще в одном важном отношении – в разных частях этих систем хранятся и обрабатываются данные разной степени важности и секретности.

Использования технологии «клиент-сервер» с точки зрения информационной безопасности имеет следующие особенности:

– каждый сервис имеет свою трактовку главных аспектов информационной безопасности (доступности, целостности, конфиденциальности);
– каждый сервис имеет свою трактовку понятий субъекта и объекта;
– каждый сервис имеет специфические угрозы;
– каждый сервис нужно по-своему администрировать;
– средства безопасности в каждый сервис нужно встраивать по-особому.

2.2. Сетевые модели передачи данных

Сетевая модель передачи данных – многоуровневая модель, описывающая порядок передачи данных в вычислительной сети, включающая стек протоколов управления передачей данных между узлами вычислительной сети.

Протокол сетевого обмена информацией можно определить как перечень форматов передаваемых блоков данных, а также правил их обработки и соответствующих действий. Иначе говоря, протокол обмена данными – это подробная инструкция о том, какого типа информация передается по сети, в каком порядке обрабатываются данные, а также набор правил обработки этих данных [14].

За время развития вычислительных сетей было предложено и реализовано много протоколов обмена данными, самыми удачными из которых явились семейство протоколов TCP/IP (Transmission Control Protocol / Internet Protocol – протокол управления передачей / межсетевой протокол).

TCP/IP – это набор протоколов, состоящий из следующих компонентов:

– межсетевой протокол (Internet Protocol), обеспечивающий адресацию в сетях (IP-адресацию);

– межсетевой протокол управления сообщениями (Internet Control Message Protocol – ICMP), который обеспечивает низкоуровневую поддержку протокола IP, включая такие функции, как сообщения об ошибках, квитанции, содействие в маршрутизации и т. п.;

– протокол разрешения адресов (Address Resolution Protocol – ARP), выполняющий преобразование логических сетевых адресов в аппаратные, а также обратный ему RARP (Reverse ARP);

– протокол пользовательских датаграмм (User Datagramm Protocol – UDP);

– протокол управления передачей (Transmission Control Protocol – TCP).

Протокол UDP обеспечивает передачу пакетов без проверки доставки, в то время как протокол TCP требует установления виртуального канала и соответственно подтверждения доставки пакета с повтором в случае ошибки.

Этот набор протоколов образует самую распространенную модель сетевого обмена данными, получившую название – TCP/IP. Модель TCP/IP иерархическая (табл. 2.1) и включает четыре уровня.

Прикладной уровень определяет способ общения пользовательских приложений. В системах «клиент-сервер» приложение-клиент должно знать, как посылать запрос, а приложение-сервер должно знать, как ответить на запрос. Этот уровень обеспечивает такие протоколы, как HTTP, FTP, Telnet.

Таблица 2.1

Иерархия модели TCP/IP

Уровень	Название	Функция
4	Прикладной	Приложения пользователей, создание сообщений
3	Транспортный	Доставка данных между программами в сети
2	Сетевой	Адресация и маршрутизация
1	Канальный	Сетевые аппаратные средства и их драйверы

Транспортный уровень позволяет сетевым приложениям получать сообщения по строго определенным каналам с конкретными параметрами.

На **сетевом уровне** определяются адреса включенных в сеть компьютеров, выделяются логические сети и подсети, реализуется маршрутизация между ними.

На **канальном уровне** определяется адресация физических интерфейсов сетевых устройств, например, сетевых плат. К этому уровню относятся программы управления физическими сетевыми устройствами, так называемые драйверы.

В сетях с коммутацией пакетов (модель TCP/IP относится к ним) для передачи по сети сообщение (сформированное на прикладном уровне) разбивается на пакеты или датаграммы. Пакет или датаграмма – это часть сообщения с добавленным заголовком пакета или датаграммы.

На транспортном уровне к полезной информации добавляется заголовок – служебная информация. Для сетевого уровня полезной информацией является уже пакет или датаграмма транспортного уровня. К ним добавляется заголовок сетевого уровня.

Полученный блок данных называется IP-пакетом. Полезной нагрузкой для канального уровня является уже IP-пакет. Здесь перед передачей по каналу к нему добавляются собственный заголовок и еще завершитель. Получившийся блок называется кадром. Он и передается по сети.

Переданный по сети кадр в пункте назначения преобразуется в обратном порядке, проходя по уровням модели снизу-вверх.

2.3. Модель взаимодействия открытых систем OSI/ISO

В конце 80-х годов XX века внимание «компьютерной» общественности было привлечено к разработке Международной организации по стандартизации коммуникационных протоколов (International Standard Organization – ISO). Разработанная ISO спецификация, названная моделью взаимодействия открытых систем (OSI – Open Systems Interconnection), определяла различные уровни взаимодействия систем в сетях с коммутацией пакетов, давала им стандартные имена и указывала, какие функции должен выполнять каждый уровень.

Высказывалось мнение, что эта модель даже потеснит широко распространившийся TCP/IP. Но этого не произошло. Одной из причин этого явилась тщательная проработка протоколов TCP/IP, их функциональность и открытость к наращиванию функциональных возможностей.

Сравнительная схема уровневых моделей протоколов OSI и TCP/IP показана на рис. 2.1.

Модель OSI
Прикладной
Представительный
Сеансовый
Транспортный
Сетевой
Канальный
Физический

МодельTCP/IP
Прикладной
Транспортный
Канальный
Физический

Рис. 2.1. Сравнительная схема протоколов OSI и TCP/IP

В модели OSI средства взаимодействия делятся на семь уровней. Каждый уровень имеет дело с определенным аспектом взаимодействия сетевых устройств.

Физический уровень имеет дело с передачей битов по физическим каналам связи, таким, как коаксиальный кабель, витая пара, оптоволоконный кабель или цифровой территориальный канал. К этому уровню имеют отношение характеристики физических сред передачи данных, такие как полоса пропускания, помехозащищенность и другие.

Задачами **канального уровня** являются проверка доступности среды передачи, реализация механизмов обнаружения и коррекции ошибок. Для этого на канальном уровне биты группируются в наборы, называемые кадрами. Канальный уровень обеспечивает корректность передачи каждого кадра.

Сетевой уровень служит для образования единой транспортной системы, объединяющей несколько сетей, причем эти сети могут использовать различные принципы передачи сообщений между конечными узлами и обладать произвольной структурой связей. Внутри одной сети доставка данных обеспечивается канальным уровнем, а доставкой данных между различными сетями занимается сетевой уровень, который и поддерживает возможность правильного выбора маршрута передачи сообщения.

Сети соединяются между собой специальными устройствами – **маршрутизаторами** – устройствами, которые собирают информацию о топологии межсетевых соединений и пересылают пакеты сетевого уровня в сеть назначения. Чтобы передать сообщение от отправителя, находящегося в одной сети, получателю, находящемуся в другой сети, нужно совершить некоторое количество транзитных передач между сетями.

Транспортный уровень обеспечивает приложениям или верхним уровням стека – прикладному и сеансовому – передачу данных с той степенью надежности, которая им требуется. Модель OSI определяет пять классов сервиса, предоставляемых транспортным уровнем. Эти виды сервиса отличаются качеством предоставляемых услуг: срочностью, возможностью восстановления прерванной связи, наличием средств мультиплексирования нескольких соединений между различными прикладными протоколами через общий транспортный протокол, а главное – способностью к обнаружению и исправлению ошибок передачи, таких как искажение, потеря и дублирование пакетов.

Сеансовый уровень обеспечивает управление диалогом: фиксирует, какая из сторон является активной в настоящий момент, предоставляет средства синхронизации, позволяющие вставлять контрольные точки в длинные передачи, чтобы в случае отказа можно было вернуться назад к последней контрольной точке, а не начинать все сначала.

Представительный уровень имеет дело с формой представления передаваемой по сети информации, не меняя при этом

ее содержания. За счет этого уровня информация, передаваемая прикладным уровнем одной системы, всегда понятна прикладному уровню другой системы. С помощью средств данного уровня протоколы прикладных уровней могут преодолеть синтаксические различия в представлении данных или же различия в кодах символов, например, в кодах ASCII и EBCDIC. На этом уровне может выполняться шифрование и дешифрование данных, благодаря которому секретность обмена данными обеспечивается сразу для всех прикладных служб. Примером такого протокола является протокол Secure Socket Layer (SSL), который обеспечивает секретный обмен сообщениями для протоколов прикладного уровня стека TCP/IP.

Прикладной уровень – это набор разнообразных протоколов, с помощью которых пользователи сети получают доступ к разделяемым ресурсам, таким как файлы, принтеры или Web-страницы, а также организуют совместную работу, например, с помощью протокола электронной почты. Единица данных, которой оперирует прикладной уровень, обычно называется сообщением.

Функции всех уровней модели OSI могут быть отнесены к одной из двух групп: либо к функциям, зависящим от конкретной технической реализации сети, либо к функциям, ориентированным на работу с приложениями.

Три нижних уровня – физический, канальный и сетевой – являются сетезависимыми, то есть протоколы этих уровней тесно связаны с технической реализацией сети и используемым коммуникационным оборудованием.

Три верхних уровня – прикладной, представительный и сеансовый - ориентированы на приложения и мало зависят от технических особенностей построения сети. На протоколы этих уровней не влияют какие бы то ни было изменения в топологии сети, замена оборудования или переход на другую сетевую технологию.

Транспортный уровень является промежуточным, он скрывает все детали функционирования нижних уровней от верхних. Это позволяет разрабатывать приложения, не зависящие от технических средств непосредственной транспортировки сообщений.

2.4. Адресация в глобальных сетях

Система адресации в глобальной вычислительной сети основана на протоколе IP, в соответствии с которым каждый узел

вычислительной сети идентифицируется уникальным 32-х битовым двоичным адресом.

Одной из главных проблем построения глобальных сетей является проблема адресации. С одной стороны, постоянное расширение глобальной сети интернет привело к нехватке уникальных адресов для вновь подключаемых узлов. С другой стороны, система адресации в таких сетях должна быть защищена от возможного вмешательства злоумышленников, связанных с подменой адресов и реализацией обходных маршрутов передачи сообщений.

Адресация современного интернета основана на протоколе IP (Internet Protocol), история которого неразрывно связана с транспортным протоколом TCP.

Концепция протокола IP представляет сеть как множество компьютеров (хостов), подключенных к некоторой интерсети. Интерсеть, в свою очередь, рассматривается как совокупность физических сетей, связанных маршрутизаторами. Физические объекты (хосты, маршрутизаторы, подсети) идентифицируются при помощи IP-адресов. Каждый IP-адрес представляет собой 32-битовый идентификатор. Принято записывать IP-адреса в виде 4-х десятичных чисел, разделенных точками.

Для этого 32-х битовый IP-адрес разбивается на четыре группы по 8 бит (1 байт), после чего каждый байт двоичного слова преобразовывается в десятичное число по известным правилам.

Например, IP-адрес:

10010011	10000111	00001110	11100101

преобразовывается указанным способом к виду: 147.135.14.229.

Во времена, когда ARPANET состояла из довольно небольшого числа хостов, все они были перечислены в одном файле (HOSTS.TXT). Этот файл хранился в сетевом информационном центре Станфордского исследовательского института (SRI-NIC – Stanford Research Institute Network Information Center). Каждый администратор сайта посылал в SRI-NIC дополнения и изменения, происшедшие в конфигурации его системы. Периодически администраторы переписывали этот файл в свои системы, где из него генерировали файл /etc/hosts. С ростом ARPANET это стало чрезвычайно затруднительным. С переходом на TCP/IP

совершенствование этого механизма стало необходимостью, поскольку, например, какой-то администратор мог присвоить новой машине имя уже существующей. Решением этой проблемы явилось создание доменов, или локальных полномочий, в которых администратор мог присваивать имена своим машинам и управлять данными адресации в своем домене.

Домен – группа узлов сети (хостов) объединенных общим именем, которое для удобства несет определенную смысловую нагрузку. Например, домен «ru» объединяет узлы на территории России. В более широком смысле под доменом понимается множество машин, которые администрируются и поддерживаются как одно целое. Можно сказать, что все машины локальной сети составляют домен в большей сети, хотя можно и разделить машины локальной сети на несколько доменов. При подключении к интернету домен должен быть поименован в соответствии с соглашением об именах в этой сети. Интернет организован как иерархия доменов.

Домен корневого уровня формируется InterNIC (сетевым информационным центром сети интернет).

Домены верхнего уровня имеют следующие ветви:

edu – образовательные учреждения;

gov – правительственные учреждения;

arpa – ARPANET;

com – коммерческие организации;

mil – военные организации;

int – международные организации;

org – некоммерческие организации;

net – сетевые информационные центры.

Начиная с весны 1997 к ним добавились еще 7 доменов:

firm – фирмы и направления их деятельности;

store – торговые фирмы;

web – объекты, связанные с WWW;

arts – объекты, связанные с культурой и искусством;

rec – развлечения и отдых;

info – информационные услуги;

nom – прочие.

Эти имена соответствуют типам сетей, которые составляют данные домены. Кроме этого, к доменам верхнего уровня относятся домены по географическому признаку, у которых представление названия страны двухбуквенное.

it – Италия;
jp – Япония;
kr – Корея;
nz – Новая Зеландия;
ru – Россия;
se – Швеция;
su – бывший СССР;
tw – Тайвань;
uk – Англия/Ирландия;
us – Соединенные Штаты.

Локальные домены могут состоять из одного хоста или включать не только множество хостов, но и свои поддомены. Имя домена образуется упорядочиванием всех доменов от корневого до текущего, перечисленных справа налево и разделенных точками. Например, в имени romanof.master.edu:

edu – соответствует верхнему уровню,
master – показывает поддомен edu,
romanof – является именем хоста.

Служба доменных имен предназначена для определения соответствия между доменным именем хоста и его реальным IP-адресом и наоборот. По сути, сервер (DNS-сервер), предоставляющий пользователям сети эту услугу, хранит базу данных об этих соответствиях.

История развития сети интернет показывает, что DNS-сервер является объектом атак со стороны злоумышленников, поскольку, выведя из строя этот сервер или изменив данные его базы, можно нарушить работу сети.

2.5. Классификация удаленных угроз в вычислительных сетях

Удаленные угрозы можно классифицировать по следующим признакам.

По характеру воздействия:

- пассивные (класс 1.1);
- активные (класс 1.2).

Пассивным воздействием на распределенную вычислительную систему называется воздействие, которое не оказывает непосредственного влияния на работу системы, но может нарушать

ее политику безопасности. Отсутствие непосредственного влияния на работу сети является причиной практически невозможного обнаружения таких воздействий. Примером пассивного удаленного воздействия может служить прослушивание канала связи.

Под активным воздействием на вычислительную сеть понимается воздействие, оказывающее непосредственное влияние на работу сети (изменение конфигурации, нарушение работоспособности и т.д.) и нарушающее принятую в ней политику безопасности. Почти все типы удаленных угроз являются активными воздействиями, поскольку в результате их осуществления в системе происходят определенные изменения, активные воздействия могут быть обнаружены [14].

По цели воздействия:

– нарушение конфиденциальности информации (класс 2.1);
– нарушение целостности информации (класс 2.2);
– нарушение доступности информации (работоспособности системы) (класс 2.3).

Этот классификационный признак является прямым следствием трех основных типов угроз – раскрытия, целостности и отказа в обслуживании.

Одна из основных целей злоумышленников – получение несанкционированного доступа к информации. Существуют две принципиальные возможности доступа к информации: перехват и искажение. Возможность перехвата информации означает получение к ней доступа, но невозможность ее модификации. Следовательно, перехват информации ведет к нарушению ее конфиденциальности. Имеется несанкционированный доступ к информации без возможности ее искажения. Нарушение конфиденциальности информации является пассивным воздействием.

Возможность искажения информации означает либо полный контроль над информационным потоком между объектами системы, либо возможность передачи сообщений от имени другого объекта. Таким образом, искажение информации ведет к нарушению ее целостности. Это – активное воздействие.

Принципиально другая цель преследуется злоумышленником при реализации угрозы для нарушения работоспособности сети. В этом случае не предполагается получение несанкционированного доступа к информации. Его основная цель – добиться, чтобы узел сети или поддерживаемый им сервис вышел из строя и для всех

остальных объектов сети доступ к ресурсам атакованного объекта был бы невозможен.

По условию начала осуществления воздействия:

– атака по запросу от атакуемого объекта (класс 3.1);

– атака по наступлению ожидаемого события на атакуемом объекте (класс 3.2);

– безусловная атака (класс 3.3).

В первом случае, злоумышленик ожидает передачи от потенциальной цели атаки запроса определенного типа, который и будет условием начала осуществления воздействия. Примером подобных запросов в сети Internet служат DNS-запросы.

Во втором случае, злоумышленник осуществляет постоянное наблюдение за состоянием операционной системы удаленной цели атаки и при возникновении определенного события в этой системе начинает воздействие. Как и в предыдущем случае, инициатором осуществления начала атаки выступает сам атакуемый объект.

Реализация третьего вида атаки не связана ни с какими событиями и реализуется безусловно по отношению к цели атаки, то есть атака осуществляется немедленно.

По наличию обратной связи с атакуемым объектом:

– с обратной связью (класс 4.1);

– без обратной связи (однонаправленная атака) (класс 4.2).

Удаленная атака, осуществляемая при наличии обратной связи с атакуемым объектом, характеризуется тем, что на некоторые запросы, переданные на атакуемый объект, атакующему требуется получить ответ, значит, между атакующим и целью атаки существует обратная связь, которая позволяет атакующему адекватно реагировать на все изменения, происходящие на атакуемом объекте.

Атаки без обратной связи осуществляются передачей на атакуемый объект одиночных запросов, ответы на которые атакующему не нужны. Подобную удаленную атаку можно называть однонаправленной удаленной атакой.

По расположению субъекта атаки относительно атакуемого объекта:

– внутрисегментное (класс 5.1);

– межсегментное (класс 5.2).

С точки зрения удаленной атаки чрезвычайно важно, как по отношению друг к другу располагаются субъект и объект атаки, то есть в одном или в разных сегментах сети они находятся. В случае

внутрисегментной атаки, как следует из названия, субъект и объект атаки находятся в одном сегменте. При межсегментной атаке субъект и объект атаки находятся в разных сегментах.

Данный классификационный признак позволяет судить о так называемой «степени удаленности» атаки.

Важно отметить, что межсегментная удаленная атака представляет гораздо большую опасность, чем внутрисегментная, поскольку в случае межсегментной атаки объект ее и непосредственно атакующий могут находиться на большом расстоянии друг от друга, что может воспрепятствовать мерам по локализации субъекта атаки.

По уровню модели ISO/OSI, на котором осуществляется воздействие:

- физический (класс 6.1);
- канальный (класс 6.2);
- сетевой (класс 6.3);
- транспортный (класс 6.4);
- сеансовый (класс 6.5);
- представительный (класс 6.6);
- прикладной (класс 6.7).
-

2.6. Типовые удаленные атаки и их характеристика

Все распределенные вычислительные сети проектируются на основе одних и тех же принципов и имеют схожие проблемы безопасности.

С учетом этого используется понятие типовой удаленной угрозы (атаки), характерной для любых распределенных вычислительных сетей. Введение этого понятия в совокупности с описанием механизмов реализации типовых удаленных угроз позволяет выработать методику исследования безопасности вычислительных сетей, заключающуюся в последовательной умышленной реализации всех типовых удаленных угроз и наблюдению за поведением системы.

Типовая удаленная атака – это удаленное информационное разрушающее воздействие, программно осуществляемое по каналам связи и характерное для любой распределенной вычислительной сети [14].

Удаленная атака «анализ сетевого трафика»

Основной особенностью распределенной вычислительной сети является распределенность ее объектов в пространстве и связь между ними по физическим линиям связи. При этом все управляющие сообщения и данные, пересылаемые между объектами вычислительной сети, передаются по сетевым соединениям в виде пакетов обмена. Эта особенность привела к появлению специфичного для распределенных вычислительных сетей типового удаленного воздействия, заключающегося в прослушивании канала связи, называемого анализом сетевого трафика.

Анализ сетевого трафика позволяет:

– изучить логику работы распределенной вычислительной сети, что позволяет на практике моделировать и осуществлять другие типовые удаленные атаки;

– перехватить поток данных, которыми обмениваются объекты сети, т.е. получить несанкционированный доступ к информации.

По характеру воздействия анализ сетевого трафика является пассивным воздействием (класс 1.1). Осуществление данной атаки без обратной связи (класс 4.2) ведет к нарушению конфиденциальности информации (класс 2.1) внутри одного сегмента сети (класс 5.1) на канальном уровне OSI (класс 6.2). При этом начало осуществления атаки безусловно по отношению к цели атаки (класс 3.3).

Удаленная атака «подмена доверенного объекта»

Одной из проблем безопасности распределенной ВС является недостаточная идентификация и аутентификация (определение подлинности) удаленных друг от друга объектов. Основная трудность заключается в осуществлении однозначной идентификации сообщений, передаваемых между субъектами и объектами взаимодействия. В том случае, когда в вычислительной сети использует нестойкие алгоритмы идентификации удаленных объектов, то оказывается возможной типовая удаленная атака, заключающаяся в передаче по каналам связи сообщений от имени произвольного объекта или субъекта сети (т.е. подмена объекта или субъекта сети).

Подмена доверенного объекта распределенной вычислительной сети является активным воздействием (класс 1.2), совершаемым с целью нарушения конфиденциальности (класс 2.1) и целостности (класс 2.2) информации, по наступлению на атакуемом объекте определенного события (класс 3.2). Данная удаленная атака может

являться как внутрисегментной (класс 5.1), так и межсегментной (класс 5.2), как с обратной связью (класс 4.1), так и без обратной связи (класс 4.2) с атакуемым объектом и осуществляется на сетевом (класс 6.3) и транспортном (класс 6.4) уровнях модели OSI.

Удаленная атака «ложный объект»

Принципиальная возможность реализации данного вида удаленной атаки в вычислительных сетях также обусловлена недостаточно надежной идентификацией сетевых управляющих устройств (например, маршрутизаторов). Целью данной атаки является внедрение в сеть ложного объекта путем изменения маршрутизации пакетов, передаваемых в сети. Внедрение ложного объекта в распределенную сеть может быть реализовано навязыванием ложного маршрута, проходящего через ложный объект.

Современные глобальные сети представляют собой совокупность сегментов сети, связанных между собой через сетевые узлы. При этом маршрутом называется последовательность узлов сети, по которой данные передаются от источника к приемнику. Каждый маршрутизатор имеет специальную таблицу, называемую таблицей маршрутизации, в которой для каждого адресата указывается оптимальный маршрут. Таблицы маршрутизации существуют не только у маршрутизаторов, но и у любых хостов (узлов) в глобальной сети. Для обеспечения эффективной и оптимальной маршрутизации в распределенных ВС применяются специальные управляющие протоколы, позволяющие маршрутизаторам обмениваться информацией друг с другом.

Реализация данной типовой удаленной атаки заключается в несанкционированном использовании протоколов управления сетью для изменения исходных таблиц маршрутизации. В результате успешного изменения маршрута атакующий получит полный контроль над потоком информации, которой обмениваются объекты сети.

Получив контроль над проходящим потоком информации между объектами, ложный объект сети может применять различные методы воздействия на перехваченную информацию, например:

– перехват потока информации и сохранение ее на ложном объекте (нарушение конфиденциальности);
– модификация информации:
– модификация данных (нарушение целостности),

– модификация исполняемого кода и внедрение разрушающих программных средств – программных вирусов (нарушение доступности, целостности);
– подмена информации (нарушение целостности).

Навязывание ложного маршрута – активное воздействие (класс 1.2), совершаемое с любой из целей из класса 2, безусловно по отношению к цели атаки (класс 3.3). Данная типовая удаленная атака может осуществляться как внутри одного сегмента (класс 5.1), так и межсегментно (класс 5.2), как с обратной связью (класс 4.1), так и без обратной связи с атакуемым объектом (класс 4.2) на транспортном (класс 6.3) и прикладном (класс 6.7) уровне модели OSI.

Удаленная атака «отказ в обслуживании»

Одной из основных задач, возлагаемых на сетевую операционную систему, функционирующую на каждом из объектов распределенной вычислительной сети, является обеспечение надежного удаленного доступа с любого объекта сети к данному объекту. В общем случае в сети каждый субъект системы должен иметь возможность подключиться к любому объекту сети и получить в соответствии со своими правами удаленный доступ к его ресурсам. В зависимости от различных параметров объектов вычислительной сети, основными из которых являются быстродействие ЭВМ, объем оперативной памяти и пропускная способность канала связи – количество одновременно устанавливаемых виртуальных подключений ограничено, соответственно, ограничено и число запросов, обрабатываемых в единицу времени. С этой особенностью работы вычислительных сетей связана типовая удаленная атака «отказ в обслуживании». Реализация этой угрозы возможна, если в вычислительной сети не предусмотрено средств аутентификации (проверки подлинности) адреса отправителя. В такой вычислительной сети возможна передача с одного объекта (атакующего) на другой (атакуемый) бесконечного числа анонимных запросов на подключение от имени других объектов.

Результат применения этой удаленной атаки – нарушение на атакованном объекте работоспособности соответствующей службы предоставления удаленного доступа, то есть невозможность получения удаленного доступа с других объектов вычислительной сети – отказ в обслуживании.

Одна из разновидностей этой типовой удаленной атаки заключается в передаче с одного адреса такого количества запросов

на атакуемый объект, какое позволяет трафик. В этом случае, если в системе не предусмотрены правила, ограничивающие число принимаемых запросов с одного объекта (адреса) в единицу времени, то результатом этой атаки может являться как переполнение очереди запросов и отказа одной из телекоммуникационных служб, так и полная остановка компьютера из-за невозможности системы заниматься ничем другим, кроме обработки запросов.

Еще одной разновидностью атаки «отказ в обслуживании» является передача на атакуемый объект некорректного, специально подобранного запроса, что, при наличии ошибок в удаленной системе, может вызвать зацикливание процедуры обработки запроса, переполнение буфера с последующим зависанием системы.

Типовая удаленная атака «отказ в обслуживании» является активным (класс 1.2) однонаправленным воздействием (класс 4.2), осуществляемым с целью нарушения работоспособности системы (класс 2.3) на транспортном (класс 6.4) и прикладном (класс 6.7) уровнях модели OSI.

2.7. Причины успешной реализации удаленных угроз в вычислительных сетях

Чтобы ликвидировать угрозы (удаленные атаки), осуществляемые по каналам связи, необходимо ликвидировать порождающие их причины. Анализ механизмов реализации типовых удаленных атак позволяет сформулировать причины, по которым данные удаленные атаки оказались возможными.

1. Отсутствие выделенного канала связи между объектами вычислительной сети. Данная причина обусловливает типовую удаленную атаку «анализ сетевого трафика». Такая атака программно возможна только в случае, если атакующий находится в сети с физически широковещательной средой передачи данных (например, Ethernet). Анализ сетевого трафика программными средствами практически невозможен, если у каждого объекта системы существует для связи с любым другим объектом выделенный канал.

2. Недостаточная идентификация объектов и субъектов сети. Эта причина предопределяет такие типовые удаленные атаки как «ложный объект» и «подмена доверенного объекта», а в некоторых случаях и «отказ в обслуживании».

3. Взаимодействие объектов без установления виртуального канала. Объекты распределенных вычислительных сетей могут взаимодействовать двумя способами:

– с использованием виртуального канала;
– без использования виртуального канала.

При создании виртуального канала объекты вычислительной сети обмениваются динамически вырабатываемой ключевой информацией, позволяющей уникально идентифицировать канал, тем самым подтверждается подлинность объектов информационного обмена друг перед другом.

Однако ошибочно считать распределенную вычислительную сеть безопасной, даже если все взаимодействие объектов происходит с созданием виртуального канала. Виртуальный канал является необходимым, но не достаточным условием безопасного взаимодействия. Чрезвычайно важным в данном случае становится выбор алгоритма идентификации при создании виртуального канала.

4. Отсутствие контроля за виртуальными каналами связи между объектами сети может привести к нарушению работоспособности системы путем формирования множества запросов на создание соединения (виртуального канала), в результате чего-либо переполняется число возможных соединений, либо система, занятая обработкой ответов на запросы, вообще перестает функционировать (типовая удаленная атака «отказ в обслуживании»).

5. Отсутствие в распределенных вычислительных сетях возможности контроля за маршрутом сообщений. Если в вычислительных сетях не предусмотрены возможности контроля за маршрутом сообщения, то адрес отправителя сообщения оказывается ничем не подтвержден. Таким образом, в системе будет существовать возможность отправки сообщения от имени любого объекта системы, а именно, путем указания в заголовке сообщения чужого адреса отправителя. Также в таких сетях будет невозможно определить, откуда на самом деле пришло сообщение и выяснить координаты атакующего. Это является причиной успеха таких удаленных угроз, как «подмена доверенного объекта» и «ложный объект сети».

6. Отсутствие в распределенных вычислительных сетях полной информации о ее объектах. В распределенной системе с разветвленной структурой, состоящей из большого числа объектов, может возникнуть ситуация, когда для доступа к определенному объекту системы у субъекта взаимодействия может не оказаться

необходимой информации об интересующем объекте. Обычно такой недостающей информацией об объекте является его адрес. В этом случае осуществляется широковещательный запрос в сеть, на который реагирует искомый узел. Данная ситуация особенно характерна для сети интернет. Пользователь знает доменное имя узла, но для соединения с ним необходим IP-адрес, поэтому при вводе доменного имени операционная система формирует запрос к серверу доменных имен. В ответ DNS-сервер сообщает IP-адрес запрашиваемого узла. В такой схеме существует возможность выдачи ложного ответа на запрос пользователя.

7. Отсутствие в распределенных вычислительных сетях криптозащиты сообщений. Поскольку в вычислительных сетях связь между объектами осуществляется по каналам связи, то всегда существует принципиальная возможность для злоумышленника прослушать канал и получить несанкционированный доступ к информации, которой обмениваются по сети ее абоненты. Если проходящая по каналу информация не зашифрована и атакующий получает доступ к каналу, то удаленная атака «анализ сетевого трафика» является эффективным способом получения информации.

3. СОДЕРЖАНИЕ И ОСНОВНЫЕ ПОНЯТИЯ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

3.1. Содержание и структура понятия компьютерной безопасности

Рассмотрим основные понятия, определяющие такой вид деятельности, как обеспечение компьютерной безопасности.

Основополагающим и наиболее общим, включающим в себя все аспекты теории и практики обеспечения безопасности во всех сферах человеческой деятельности является понятие **безопасности** (Федеральный закон «О безопасности», 1993 г.).

Безопасность – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Одним из направлений обеспечения безопасности является информационная безопасность (Доктрина информационной безопасности Российской Федерации).

Информационная безопасность Российской Федерации – состояние защищенности ее (РФ) национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Аналогично под информационной безопасностью предприятия (учреждения) понимается состояние защищенности информационной сферы предприятия, (учреждения) от внутренних и внешних угроз.

Обеспечение информационной безопасности затрагивает многие сферы деятельности человека и различные формы представления информации на любых ее носителях. Нас в данный момент интересует лишь информация (с точки зрения обеспечения безопасности), связанная со средствами вычислительной техники: хранящаяся на машинных носителях, обрабатываемая с использованием информационных систем или пересылаемая по сетям передачи данных. Таким образом, понятие **компьютерной безопасности** является видовым по отношению к более широкому (родовому) понятию информационной безопасности.

Компьютерная безопасность – состояние защищенности (безопасность) информации в компьютерных системах и безотказность (надежность) функционирования компьютерных систем (КС).

Методологический анализ родового понятия «информационная безопасность» показывает, что ключевыми являются следующие аспекты: информационная сфера (объект), угрозы (внутренние и внешние) и состояние защищенности (предмет объекта) [11, 18].

Следовательно, сфера понятия «компьютерная безопасность» сужается до объекта, именуемого «компьютерной системой», под которой будем понимать человеко-машинную систему, представляющую совокупность электронных технических средств обработки, хранения и представления данных, программного обеспечения (ПО), реализующего информационные технологии, и информации (данных). В результате составляющими компьютерной безопасности выступают безопасность информации (данных), накапливаемых, обрабатываемых в компьютерной системе, и безопасность (безотказность, надежность) функций КС.

С учетом вышеизложенного, структура понятия «Безопасность» показана на рис. 3.1.

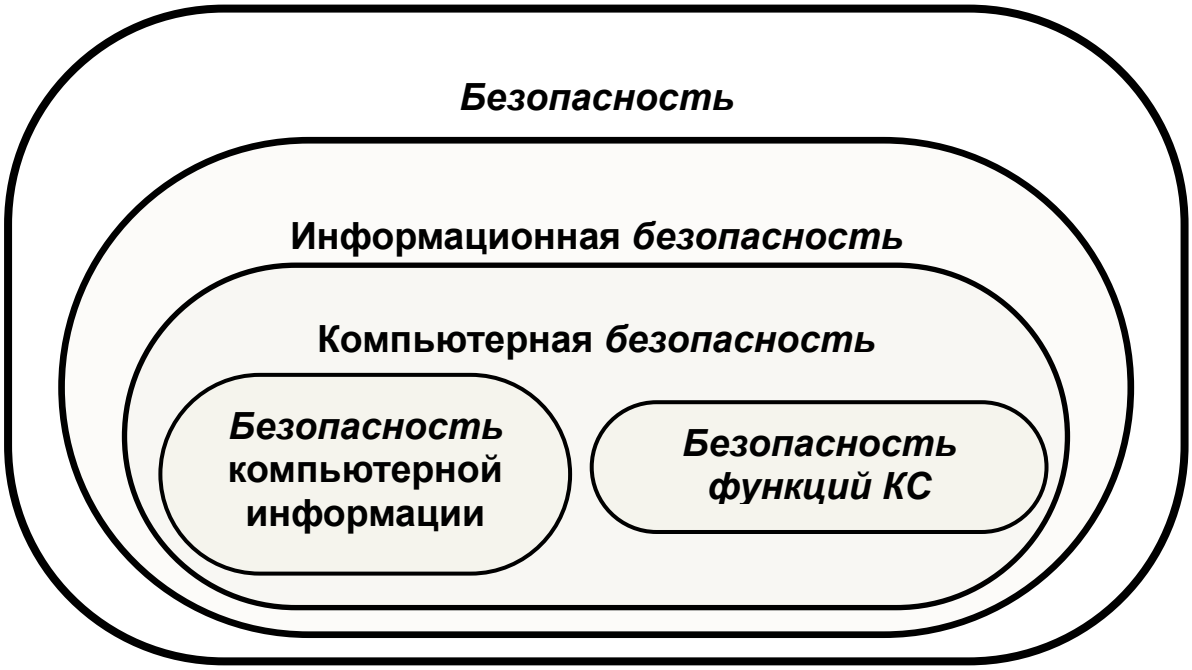

Рис. 3.1. Структура понятия «Безопасность»

Содержательный анализ самого понятия «информация» (сведения (сообщения, данные) независимо от формы их представления), особенностей процессов и технологий ее сбора, обработки, хранения, представления и выдачи показывает, что безотносительно к функционально-содержательной стороне работы с информацией (данными) понятие «безопасность информации» включает три составляющих:

– обеспечение конфиденциальности;
– обеспечение целостности;
– обеспечение доступности.

При этом под конфиденциальностью информации понимается специфическое свойство отдельных категорий (видов) информации, которое субъективно устанавливается ее обладателем, когда ему может быть причинен ущерб от ознакомления с информацией неуполномоченных на то лиц, при условии того, что обладатель принимает меры по организации доступа к информации только уполномоченных лиц. Таким образом, обеспечение безопасности информации в КС означает, включает обеспечение ее конфиденциальности (если характер информации является таковым, т.е. конфиденциальным), заключающееся в обеспечении такого порядка работы с информацией, когда она известна только определенному установленному кругу лиц (пользователей КС).

Под целостностью информации (данных) понимается неискаженность, достоверность, полнота, адекватность и т.д. информации, т.е. такое ее свойство, при котором содержание и структура данных определены и изменяются только уполномоченными лицами и процессами. Таким образом, обеспечение безопасности информации в КС предполагает такой порядок и технологию работы с ней, когда информация изменяется, модифицируется только уполномоченными лицами и в процессах ее передачи, хранения не возникают (устраняются) искажения, ошибки.

И, наконец, под правомерной доступностью информации (данных) понимается такое свойство информации, при котором отсутствуют препятствия доступа к информации и закономерному ее использованию обладателем или уполномоченными лицами. В результате безопасность информации в КС обеспечивается ее сохранностью, способностью к восстановлению при сбоях и разрушениях, а также в отсутствии препятствий работы с ней уполномоченных лиц.

Важно подчеркнуть, что только одновременное обеспечение всех трех составляющих (конфиденциальности, целостности и доступности) дает состояние безопасности информации.

Вторым аспектом компьютерной безопасности, как следует из приведенного выше определения, является безопасность (безотказность, надежность) функций компьютерных систем.

Суть и особенности компьютерных систем, в свою очередь, определяют две составляющие безопасности функций КС:

– обеспечение безотказности реализации функций;
– обеспечение аутентичности реализации функций.

Первая составляющая определяется безотказностью оборудования (технических средств обработки, хранения, передачи и представления информации) и безотказностью программного обеспечения (отсутствие сбоев в работе программного обеспечения).

Вторая составляющая (аутентичность функций) определяется целостностью ПО и целостностью программно-аппаратной конфигурации КС (параметров, настройки, состава ПО и оборудования).

При этом две составляющие компьютерной безопасности являются взаимозависимыми. В частности, при нарушении безопасности информации в КС (нарушении конфиденциальности, целостности и/или доступности данных) в большинстве случаев нарушается безопасность функций КС. Однако обратное в общем случае неверно. Иначе говоря, информация КС может находиться в безопасном состоянии, но в результате сбоев оборудования или ПО, нарушения целостности ПО или целостности программно-аппаратной конфигурации, функции КС не будут реализовываться или будут реализовываться неадекватно.

Следует также отметить, что в силу исторических особенностей развития электронно-вычислительной техники, две составляющие компьютерной безопасности рассматривались и развивались параллельно и достаточно независимо друг от друга, и кроме того, вторая составляющая (безопасность функций) рассматривалась в контексте обеспечения надежности вычислительной техники (оборудования и программного обеспечения). Поэтому, в литературе и в стандартах до настоящего время под компьютерной безопасностью понимается в первую очередь первая ее составляющая – безопасность информации в компьютерной системе.

Мы также в рамках данного пособия будем придерживаться этого подхода, поскольку методы и механизмы обеспечения функций компьютерной системы в контексте безотказности оборудования и программного обеспечения рассматриваются в рамках изучения других дисциплин.

3.2. История развития теории и практики обеспечения компьютерной безопасности

Проблемы и задачи обеспечения безопасности информации, сохранности информационных ресурсов, охраны разного рода тайн возникли и решались задолго до компьютерной эры.

Однако современные компьютерные информационные технологии качественно изменили и обострили проблему безопасности информации. Возможности несанкционированного доступа к информации с целью ее копирования, изменения или мгновенного разрушения информационных ресурсов, хранящихся или использующихся в компьютерной форме, предопределили перевод задач обеспечения безопасности информации из разряда вспомогательных, обеспечивающих, в число основных и приоритетных.

В практическом плане задачи обеспечения безопасности компьютерной информации возникли в 70-х годах в связи с созданием и внедрением автоматизированных информационных систем в процессы информационного обеспечения деятельности крупных и средних предприятий и организаций. Потребовалась теоретическая база, программно-технические решения и механизмы обеспечения безопасности при коллективной обработке общих информационных ресурсов. Именно в то время появились первые работы по политике, методологии и моделям защиты компьютерной информации.

Сформировались три составляющих и, соответственно, три, взаимосвязанных, но различных направления защиты компьютерной информации – обеспечение конфиденциальности информации, обеспечение целостности данных, обеспечение сохранности и работоспособности данных.

Основное внимание исследователей было сосредоточено на проблемах обеспечения конфиденциальности данных, основным ключом к разрешению которых были выбраны позаимствованные из «бумажной» сферы методы ограничения и разграничения доступа. В результате проблема разграничения доступа к данным с той поры и по сей день стала центральным элементом систем безопасности компьютерной информации.

К концу 70-х годов были разработаны исходные модели безопасности компьютерных систем, обеспечивающие те или иные из

трех составляющих безопасности информации, и программно-технические решения построения и функционирования защищенных компьютерных систем, в частности, технологии и протоколы парольной аутентификации, криптографические методы и средства защиты информации и т.д.

Созданные в тот период модели дискреционного и мандатного разграничения доступа послужили методологической основой для разработки первых стандартов безопасности компьютерных систем, в частности, известной «оранжевой книги» (1983 г.).

Модели дискреционного и мандатного доступа явились основой для последующих исследований, повлекших разработку новых подходов к разграничению доступа в 80-е и 90-е годы.

В 90-е годы отечественные исследователи представили доказательный подход к проблеме гарантированности защиты информации в компьютерной системе, а также провели математический анализ ряда задач и решений в теории защиты информации применительно к различным разновидностям компьютерных систем. В сферу исследований были введены новые виды так называемых скрытых каналов утечки информации, основывающихся на использовании статистических характеристик работы компьютерной системы. Была представлена теория разрушающих программных воздействий, составившая теоретическую базу методов и механизмов борьбы с вредоносными программными средствами. На основе положений исходных моделей разграничения доступа была разработана стройная субъектно-объектная модель компьютерной системы, на базе которой сформированы фундаментальные для сферы защиты информации и, в особенности, для процессов разграничения доступа понятия информационных потоков и доступов в компьютерной системе.

Впоследствии была разработана таксонометрия брешей и изъянов в системах защиты компьютерных систем. В практических разработках российских специалистов представлен ряд интересных технических решений по созданию защищенных компьютерных систем, в частности, организационно-иерархическая система разграничения доступа.

Помимо исследований в сфере криптографической защиты информации был проведен анализ решений и механизмов защиты информации в основных разновидностях компьютерных систем, подготовлена целая серия учебных изданий, что позволило

сформировать методическую базу подготовки специалистов в сфере компьютерной безопасности.

Этапы развития концепций обеспечения информационной безопасности приведены в табл. 3.1.

Таблица 3.1

Этапы развития концепций обеспечения ИБ

Этапы развития концепций обеспечения ИБ	Характеристика этапа
1 этап 1960-1970 г.г.	Попытки обеспечить безопасность данных чисто формальными механизмами, содержащими технические и программные средства. Сосредоточение программных средств в рамках операционных систем и систем управления базами данных.
2 этап 1970-1976 г.г.	Дальнейшее развитие формальных механизмов защиты данных. Выделение управляющего компонента защиты данных – ядра безопасности. Развитие неформальных средств защиты. Формирование основ системного подхода к обеспечению безопасности данных.
3 этап 1976-1990 г.г.	Дальнейшее развитие механизмов второго этапа. Формирование взгляда на обеспечение безопасности данных как на непрерывный процесс. Развитие стандартов на средства защиты данных. Усиление тенденции аппаратной реализации средств защиты данных. Формирование вывода о взаимосвязи обеспечения безопасности данных, архитектуры ИС и технологии ее функционирования. Формирование системного подхода к проблеме обеспечения ИБ.
4 этап 1990 г. - по настоящее время	Дальнейшее развитие механизмов третьего этапа. Формирование основ теории обеспечения безопасности данных в ИС. Разработка моделей, методов и алгоритмов управления ИБ.

3.3. Общая характеристика принципов, методов и механизмов обеспечения компьютерной безопасности

На основе анализа теоретических и практических аспектов обеспечения компьютерной безопасности можно выделить ряд общих принципов создания и эксплуатации компьютерных систем, в которых обеспечивается безопасность информации.

Принцип разумной достаточности. Внедрение в архитектуру, в алгоритмы и технологии функционирования КС защитных механизмов, функций и процедур объективно вызывает дополнительные затраты, издержки при создании и эксплуатации, ограничивает, снижает функциональные возможности КС и параметры ее эффективности (быстродействие, ресурсы), вызывает неудобства в работе пользователям КС, налагает на них дополнительные нагрузки и требования. Кроме того, создать абсолютно непреодолимую систему защиты принципиально невозможно; при достаточных времени и средствах можно преодолеть любую защиту. Например, даже средства криптографической защиты не гарантируют абсолютную стойкость, а обеспечивают конфиденциальность информации при использовании для дешифрования современных вычислительных средств в течение приемлемого для защищающейся стороны времени. Поэтому имеет смысл вести речь только о некотором приемлемом уровне безопасности. Важно правильно выбрать тот достаточный уровень зашиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми (задача анализа риска). Поэтому защита должна быть разумно достаточной (на минимально необходимом уровне).

Принцип целенаправленности. Заключается в том, что применяемые меры по устранению, нейтрализации (либо обеспечению снижения потенциального ущерба) должны быть направлены против перечня угроз (опасностей), характерных для конкретной КС в конкретных условиях ее создания и эксплуатации.

Принцип системности. 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. Для обеспечения возможности варьирования уровнем защищенности средства защиты должны

обладать определенной гибкостью. Особенно важно это свойство в тех случаях, когда средства защиты необходимо устанавливать на работающую систему, нарушая процесс ее нормального функционирования. Выбор и реализация защитных механизмов должны производиться с учетом системной сути КС, как организационно-технологической человеко-машинной системы, состоящей из взаимосвязанных, составляющих единое целое функциональных, программных, технических, организационно-технологических подсистем.

Принцип комплексности. В распоряжении специалистов по компьютерной безопасности имеется широкий спектр мер, методов и средств защиты компьютерных систем (современные СВТ, операционные системы, инструментальные и прикладные программные средства, обладающие теми или иными встроенными элементами защиты). Комплексное их использование предполагает согласование разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. При разработке системы безопасности КС необходимо использовать защитные механизмы различной и наиболее целесообразной в конкретных условиях природы – программно-алгоритмических, процедурно-технологических, нормативно-организационных, и на всех стадиях жизненного цикла – на этапах создания, эксплуатации и вывода из строя.

Принцип непрерывности. Защита информации – это не разовое мероприятие и даже не конкретная совокупность уже проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИС (начиная с самых ранних стадий проектирования). Разработка системы защиты 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, внедрения специальных программных и аппаратных «закладок» и других средств преодоления системы защиты после восстановления ее функционирования. Защитные механизмы КС должны функционировать в любых ситуациях, в том числе и внештатных, обеспечивая конфиденциальность, целостность и сохранность (правомерную доступность) информации.

Принцип управляемости. Подсистема безопасности КС должна строиться как система управления – объект управления (угрозы безопасности и процедуры функционирования КС), субъект управления (средства и механизмы защиты), среда функционирования, обратная связь в цикле управления, целевая функция управления (снижение риска от угроз безопасности до требуемого (приемлемого) уровня), контроль эффективности (результативности) функционирования.

Принцип сочетания унификации и оригинальности. С одной стороны, с учетом опыта создания и применения АИС, опыта обеспечения безопасности КС должны применяться максимально проверенные, стандартизированные и унифицированные архитектурные, программно-алгоритмические, организационно-технологические решения. С другой стороны, с учетом динамики и развития информационных технологий, а также средств нападения должны разрабатываться и внедряться новые оригинальные архитектурные, программно-алгоритмические, организационно-технологические решения, обеспечивающие безопасность КС в новых условиях угроз, с минимизацией затрат и издержек, повышением эффективности и параметров функционирования КС, снижением требований к пользователям.

Принцип открытости алгоритмов и механизмов защиты. Суть принципа 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. Но это вовсе не означает, что информация о конкретной системе защиты должна быть общедоступна – необходимо обеспечивать защиту от угрозы раскрытия параметров системы.

Принцип простоты применения средств защиты. 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 непонятных ему операций (ввод нескольких паролей и имен и т.д.).

Организационно-технологический и человеко-машинный характер природы КС определяют обширный набор методов и механизмов обеспечения информационной безопасности.

Сначала можно выделить ряд методов и механизмов, непосредственно обеспечивающих конфиденциальность, целостность и доступность данных, такие как разграничение доступа к данным, контроль и управление информационной структурой данных, контроль и обеспечение ограничений целостности данных, механизмы криптографического скрытия данных (шифрования), механизмы ЭЦП, обеспечивающие целостность данных в процессах их передачи и хранения, а также механизмы контроля и удаления остаточной информации на носителях данных после завершения их обработки и в освобождаемых областях оперативной памяти.

Также важное значение для обеспечения компьютерной безопасности имеют методы и механизмы общесистемного характера, которые можно разделить на общеархитектурные и инфраструктурные с точки зрения программно-технической структуры современных КС.

Основополагающими среди общеархитектурных являются механизмы идентификации и аутентификации, обеспечивающие исходный и обязательный рубеж безопасности в КС, методы и механизмы управления памятью, изоляции процессов и управления транзакциями в клиент-серверных системах.

Методы и механизмы инфраструктурного характера имеют не менее важное значение, в особенности для обеспечения информационной безопасности в распределенных КС – контроль и управление программно-технической конфигурацией КС, управление сеансами работы пользователей, управление доступом пользователей с рабочих станций КС, управление (контроль) сетевыми соединениями в КС, управление инфраструктурой сертификатов

криптоключей, обеспечивающих механизмы шифрования данных и электронно-цифровой подписи.

Обязательными для обеспечения информационной безопасности КС, находящими отражение в стандартах защищенности, имеют методы и механизмы обеспечивающего (профилактирующего) характера, среди которых, в первую очередь следует отметить методы протоколирования и аудита событий, методы и механизмы резервирования и архивирования, журнализации процессов изменения данных. Следует также отметить важность механизмов профилактики носителей данных, их учета и контроля в организационно-технологическом контуре КС. Кроме того, человеко-машинный характер природы КС как особого инструментария деятельности предопределяет существенное значение для обеспечения информационной безопасности нормативно-организационной регламентации эксплуатации КС, процедур обучения, нормативно-административного побуждения и принуждения пользователей по вопросам обеспечения безопасности.

4. ОСНОВЫ ФОРМИРОВАНИЯ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Понятие, цели и задачи политики информационной безопасности

В процессе создания, развития и эксплуатации любой информационной системы возникает проблема обеспечения ее информационной безопасности. Она может решаться разными способами.

Наиболее часто в рамках решения этой задачи приобретаются и устанавливаются отдельные, независимые компоненты системы безопасности. В большинстве случаев ограничиваются межсетевым экраном и пакетом антивирусных программ. Классы этих систем и конкретные спецификации выбираются специалистами, согласно их личному опыту и предпочтениям. При этом, в роли специалистов могут выступать либо сотрудники информационных отделов, либо менеджеры, имеющие к информационным технологиям и их безопасности самое непосредственное отношение. Естественно, что при таком подходе информационная безопасность осуществляется однобоко и не всегда эффективно: для одних систем может существовать чрезмерный контроль, а для других недостаточный или вовсе отсутствующий. Кроме того, такие системы безопасности не масштабируемы, ими сложно управлять, их сложно развивать и адаптировать под изменяющиеся требования управления и бизнеса.

Предпочтительный подход к обеспечению безопасности информационных систем предполагает внедрение определенного процесса управления безопасностью.

Защите подлежит, прежде всего, принимаемая, передаваемая, обрабатываемая и хранимая информация, содержащая [11]:

- сведения, предназначенные для предоставления средствам массовой информации;
- иные сведения, не составляющую служебную тайну;
- сведения, составляющие конфиденциальную, служебную тайну;
- сведения, составляющие коммерческую тайну;
- сведения о частной жизни граждан (персональные данные).

Обеспечение защиты открытой информации осуществляется организационными мерами, средствами сетевого и

телекоммуникационного оборудования, а также стандартными средствами программного обеспечения.

Иногда столь упрощенный подход оправдан, однако, современная лицензионная политика в области безопасности информации определяет наличие у организаций, разрабатывающих средства защиты информации (СЗИ) или оказывающих услуги по защите информации, пакета документов, в которых определены концептуальные и общеорганизационные вопросы информационной безопасности (ИБ). Традиционно в мировой практике такой документ называется политикой безопасности (ПБ) или политикой информационной безопасности (ПИБ) организации.

Политика информационной безопасности должна представлять совокупность требований, правил, положений и принятых решений, определяющих:

– порядок доступа к информационным ресурсам;
– необходимый уровень (класс и категорию) защищенности объектов информатизации;
– организацию защиты информации в целом;
– дополнительные требования по защите отдельных компонент;
– основные направления и способы защиты информации.

Политику информационной безопасности принято трактовать как высокоуровневый и многоуровневый документ, в котором с единых управленческих позиций рассматривается совокупность взглядов, подходов и методов, применяемых в организации при построении корпоративной системы управления информационной безопасностью.

Для лучшего понимания разложим понятие политики информационной безопасности на составляющие:

– политика – это свод формальных правил, которые должны неукоснительно соблюдаться для достижения ее целей,
– безопасность – это обеспечение условий, необходимых как для существования ее объекта, так и для его развития.

Таким образом, политику информационной безопасности можно определить, как свод формальных правил, которые необходимо соблюдать при работе с информацией для обеспечения существования и развития компании.

Политика информационной безопасности направлена на обеспечение:

– конфиденциальности информации, циркулирующей в системе, – субъективно определяемой характеристике информации, указывающей на необходимость введения ограничений на круг субъектов информационных отношений, имеющих доступ к данной информации, и обеспечиваемую способность среды обработки сохранять информацию в тайне от субъектов, не имеющих полномочий на доступ к ней;
– целостности информации и среды её обработки, то есть предотвращение несанкционированной модификации или уничтожения информации, программных средств её обработки;
– доступности информации, то есть способности информационной среды, средств и технологий обработки информации обеспечить санкционированный доступ субъектов к информации, программным и аппаратным средствам.

С точки зрения требований к обеспечению информационной безопасности, обрабатывается информация следующих видов – открытая информация и информация ограниченного распространения [11].

Каждому виду информации соответствуют свои приоритеты в обеспечении информационной безопасности.

Для обеспечения работы пользователей с открытой информацией это целостность и доступность.

Для обеспечения работы пользователей с информацией ограниченного распространения приоритетами являются целостность, конфиденциальность, доступность.

Целью разработки политики информационной безопасности является определение правильного способа использования вычислительных и коммуникационных ресурсов, а также разработка процедур, предотвращающих или реагирующих на нарушения режима безопасности.

Чтобы достичь указанной цели, следует учесть основные направления деятельности организации и стоящие перед ней задачи. Например, на военном заводе и фабрике товаров потребления требования к конфиденциальности существенно разнятся. Разрабатываемая ПИБ должна согласовываться с существующими законами и подзаконными актами. Наконец, если локальная сеть организации не является изолированной, вопросы безопасности следует рассматривать в более широком контексте. Политика должна

освещать проблемы, возникающие на локальном компьютере из-за действий удаленной стороны.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы (ИС) организации. Когда проведен анализ рисков и определена стратегия защиты, составляется программа, реализация которой должна обеспечить информационную безопасность, назначаются ответственные, определяется порядок контроля выполнения программы и т.д.

Высокоуровневая политика безопасности должна периодически пересматриваться (спиральная модель, как показано на рис. 4.1), гарантируя тем самым учет текущих потребностей организации. Документ политики составляют таким образом, чтобы политика была относительно независимой от конкретных технологий, в этом случае документ не потребуется изменять слишком часто.

Рис. 4.1. Спиральная модель разработки и использования ПИБ

4.2. Правовое регулирование ПИБ

Актуальность разработки ПБ возникла с формированием нормативной базы в области ИБ, в первую очередь, – ГОСТ 15408-02,

ГОСТ 15.002-00, ГОСТ Р ИСО/МЭК 17799-2005, являющийся, отечественной редакцией ISO 17799.

Рассмотрим основные российские и зарубежные стандарты более подробно [21].

Согласно **ГОСТ 15408-02 «Критерии оценки безопасности информационных технологий» (КОБИТ)**, ПБ организации – это одно или несколько правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности. ПБ является одним из компонентов среды безопасности, включающей также законы, опыт, специальные навыки, знания и угрозы безопасности, присутствие которых в этой среде установлено или предполагается. Изложение ПБ организации включается в такие документы, как Профиль защиты и Задание по безопасности. В дальнейшем положения ПБ используются при формулировании Целей безопасности для объекта оценки и его среды. Также подчеркивается необходимость наличия механизмов проверки соответствия объекта оценки ПБ.

ГОСТ Р ИСО/МЭК 17799-2005 устанавливает рекомендации по управлению информационной безопасностью. Он предназначен для обеспечения общих основ для разработки стандартов безопасности и выбора практических мероприятий по управлению безопасностью в организации, а также в интересах обеспечения доверия в деловых отношениях между организациями.

ГОСТ 15.002-2000 явно указал требования к документальному определению вопросов ИБ для предприятий, выпускающих оборонную продукцию. Этим стандартом предусматривается обязательная программа обеспечения безопасности как часть политики качества. ПИБ должна включать совокупность процедур, мероприятий и процессов обеспечения безопасности разработки или производства СЗИ.

ISO 17799 состоит из двух частей. Первая – «Практические рекомендации» – определяет и рассматривает следующие аспекты ИБ:

- политика безопасности;
- организация защиты;
- классификация и управление информационными ресурсами;
- управление персоналом;
- физическая безопасность;

– администрирование компьютерных систем и сетей;
– управление доступом к системам;
– разработка и сопровождение систем;
– планирование бесперебойной работы организации;
– проверка системы на соответствие требованиям ИБ.

Вторая часть – «Спецификации системы» – рассматривает те же аспекты с точки зрения сертификации информационной системы на соответствие требованиям стандарта.

Предписываемая документом структура политики информационной безопасности изображена на рисунке 4.2.

Рис. 4.2. Структура ПИБ по ISO 17799

Соответствие законодательству является одним из важнейших аспектов разработки ПБ, зачастую определяющим значительную часть используемых технологий защиты. Классическим примером

для России служат ограничения по легальному использованию криптографических средств.

Важна роль раздела, определяющего ответственность за обеспечение ИБ. Хотя традиционно персональную ответственность за проведение мер по обеспечению ИБ несет руководитель организации, необходимо четкое распределение должностных обязанностей и ответственности между конкретными должностными лицами. Каждый сотрудник должен четко представлять свои обязанности в области защиты информации и ответственность за их невыполнение.

Обучение персонала в области ИБ должно проводиться непрерывно, как в процессе работы, так и в специализированных учебных центрах. Соответствующий раздел ПБ должен содержать обязанности должностных лиц по консультированию и инструктированию пользователей информационной системы, а также порядок прохождения профессиональной переподготовки.

Политика информационной безопасности не является единственным документом, регламентирующим процесс обеспечения ИБ организации. Одновременно с ПБ должны быть разработаны подробные инструкции, относящиеся к конкретным вопросам реализации ПБ. Если сама ПБ является документом статичным, структура и содержание которого определятся общей инфраструктурой организации и подлежит корректировке только в случае ее коренного изменения, то инструкции должны непрерывно обновляться и совершенствоваться по ходу модернизации информационной системы предприятия.

Вопрос обеспечения непрерывности работы организации часто выносится за рамки проблематики ИБ. И напрасно, поскольку при разработке плана обеспечения непрерывности работы организации необходимо полагаться, прежде всего, на анализ рисков безопасности, выполняемый в рамках общего аудита безопасности системы. Ключевой момент обеспечения непрерывности деятельности информационной системы – выделение критических компонентов этой системы и четкая отработка мероприятий по их восстановлению в случае поражения.

Так называемая **«Оранжевая книга»** принята стандартом в 1985 г Министерством обороны США (DOD). Полное название документа «Department of Defense Trusted Computer System Evaluation Criteria».

«Оранжевая книга» предназначается для следующих целей:

1. Предоставить производителям стандарт, устанавливающий, какими средствами безопасности следует оснащать свои новые и планируемые продукты, чтобы поставлять на рынок доступные системы, удовлетворяющие требованиям гарантированной защищенности (имея в виду, прежде всего, защиту от раскрытия данных) для использования при обработке ценной информации;

2. Предоставить DOD метрику для военной приемки и оценки защищенности систем обработки данных, предназначенных для обработки служебной и другой ценной информации;

3. Обеспечить базу для исследования требований к выбору защищенных систем.

Во всех документах DOD, связанных с «Оранжевой книгой», принято единое понимание фразы обеспечение безопасности информации: безопасность = контроль за доступом. Это понимание принимается как аксиома.

Исходя из положений рассмотренных выше стандартов, можно предложить следующую структуру типовой ПИБ организации.

1. Общие положения.
    1.1. Назначение документа.
    1.2. Основания для разработки документа.
    1.3. Основные определения.
2. Идентификация системы.
    2.1. Идентификатор и имя системы.
    2.2. Ответственные подразделения.
    2.3. Режим функционирования системы.
    2.4. Описание и цели системы.
    2.5. Цели и задачи ПБ.
    2.6. Системная среда.
        2.6.1. Физическая организация системы.
        2.6.2. Логическая организация системы.
    2.7. Реализованные сервисы системы.
    2.8. Общие правила, принятые в системе.
    2.9. Общее описание важности информации.
3. Средства управления.
    3.1. Оценка рисков и управление.
    3.2. Экспертиза СЗИ.
    3.3. Правила поведения, должностные обязанности и ответственность.
    3.4. Планирование безопасности.

3.5. Разрешение на ввод компонента в строй.

3.6. Порядок подключения подсетей подразделения к сетям общего пользования.

4. Функциональные средства.

4.1. Защита персонала.

4.2. Управление работой и вводом-выводом.

4.3. Планирование непрерывной работы.

4.4. Средства поддержки программных приложений.

4.5. Средства обеспечения целостности информации.

4.6. Документирование.

4.7. Осведомленность и обучение специалистов.

4.8. Ответные действия в случаях возникновения происшествий.

5. Технические средства.

5.1. Требования к процедурам идентификации и аутентификации.

5.2. Требования к системам контроля и разграничения доступа.

5.3. Требования к системам регистрации сетевых событий.

Конкретный перечень необходимых инструкций определяется используемой аппаратно-программной платформой.

Примерные инструкции по реализации ПИБ могут быть, следующими:

1. Требования к защите портов и служб.
2. Порядок проведения экспертизы СЗИ.
3. Порядок проведения анализа рисков.
4. Использование автоматизированных систем анализа защищенности.
5. Порядок восстановления автоматизированных систем после аварийных ситуаций.

Приведенная структура ПБ, жизнеспособность которой подтверждена неоднократным опытом внедрения, полностью соответствует положениям обоих рассмотренных стандартов.

4.3. Особенности разработки и структура ПИБ

При разработке и проведении политики безопасности в жизнь целесообразно руководствоваться следующими принципами [11]:

1. Невозможность миновать защитные средства;
2. Усиление самого слабого звена;
3. Недопустимость перехода в открытое состояние;

4. Минимизация привилегий;
5. Разделение обязанностей;
6. Многоуровневая защита;
7. Разнообразие защитных средств;
8. Простота и управляемость информационной системы;
9. Обеспечение всеобщей поддержки мер безопасности.

Поясним смысл перечисленных принципов.

1. Принцип невозможности миновать защитные средства означает, что все информационные потоки в защищаемую сеть и из нее должны проходить через СЗИ. Не должно быть скрытых сетевых входов или тестовых линий, идущих в обход экрана.

2. Надежность любой СЗИ определяется самым слабым звеном. Часто таким звеном оказывается не компьютер или программа, а человек, и тогда проблема обеспечения информационной безопасности приобретает нетехнический характер.

3. Принцип недопустимости перехода в открытое состояние означает, что при любых обстоятельствах (в том числе нештатных), СЗИ либо полностью выполняет свои функции, либо должна полностью блокировать доступ.

4. Принцип минимизации привилегий предписывает выделять пользователям и администраторам только те права доступа, которые необходимы им для выполнения служебных обязанностей.

5. Принцип разделения обязанностей предполагает такое распределение ролей и ответственности, при котором один человек не может нарушить критически важный для организации процесс. Это особенно важно для предотвращения злонамеренных или неквалифицированных действий системного администратора.

6. Принцип многоуровневой защиты предписывает не полагаться на один защитный рубеж, каким бы надежным он ни казался. За средствами физической защиты должны следовать программно-технические средства, за идентификацией и аутентификацией – управление доступом и далее – протоколирование и аудит. Такое эшелонированное построение СЗИ позволит, по крайней мере, задержать злоумышленника, а наличие такого рубежа, как протоколирование и аудит, существенно затрудняет незаметное выполнение злоумышленником действий.

7. Принцип разнообразия защитных средств рекомендует организовывать различные по своему характеру оборонительные рубежи, чтобы от потенциального злоумышленника требовалось

овладение разнообразными и, по возможности, несовместимыми между собой навыками преодоления СЗИ.

8. Принцип простоты и управляемости информационной системы в целом и СЗИ в особенности, определяет возможность формального или неформального доказательства корректности реализации механизмов защиты. Только в простой и управляемой системе можно проверить согласованность конфигурации разных компонентов и осуществить централизованное администрирование.

9. Принцип всеобщей поддержки мер безопасности носит нетехнический характер. Рекомендуется с самого начала предусмотреть комплекс мер, направленный на обеспечение лояльности персонала, на постоянное обучение, теоретическое и, главное, практическое.

Как указывалось выше, ПИБ – многоуровневый документ. Политика информационной безопасности верхнего уровня формулирует цели организации в области информационной безопасности в терминах целостности, доступности и конфиденциальности. Если организация отвечает за поддержание критически важных баз данных, на первом плане должна стоять целостность данных. Для организации, занимающейся продажами, важна актуальность информации о предоставляемых услугах и ценах, а также ее доступность максимальному числу потенциальных покупателей. Режимная организация в первую очередь будет заботиться о конфиденциальности информации, т.е. о ее защите от НСД.

На верхнем уровне определяются управление ресурсами безопасности и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем, поддержание контактов с другими организациями, обеспечивающими или контролирующими режим безопасности.

Средний уровень политики безопасности определяет решение вопросов, касающихся отдельных аспектов информационной безопасности, но важных для различных систем, эксплуатируемых организацией. Например, регламентируется порядок доступа в Internet (проблема сочетания свободы получения информации с защитой от внешних угроз), использование домашних компьютеров и т.д.

Нижний уровень политики безопасности относится к конкретным сервисам. Она включает два аспекта – цели и правила их

достижения, поэтому ее порой трудно отделить от вопросов реализации. В отличие от двух верхних уровней, рассматриваемая политика должна быть более детальной.

Главным компонентом политики безопасности организации является базовая политика безопасности.

Базовая политика безопасности устанавливает, как организация обрабатывает информацию, кто может получить к ней доступ и как это можно сделать.

Нисходящий подход, реализуемый базовой политикой безопасности, дает возможность постепенно и последовательно выполнять работу по созданию системы безопасности, не пытаясь сразу выполнить ее целиком. Базовая политика позволяет в любое время ознакомиться с политикой безопасности в полном объеме и выяснить текущее состояние безопасности в организации.

Структура и состав политики безопасности зависит от размера и целей компании. Обычно базовая политика безопасности организации поддерживается набором специализированных политик и процедур безопасности.

Потенциально существуют десятки специализированных политик, которые могут применяться большинством организаций. Некоторые политики предназначаются для каждой организации, другие – специфичны для определенных компьютерных окружений.

Процедуры безопасности являются необходимым и важным дополнением к политикам безопасности. Политики безопасности только описывают, что должно быть защищено и каковы основные правила защиты. Процедуры безопасности определяют, как защитить ресурсы и каковы механизмы исполнения политики, т.е. как реализовывать политики безопасности и представляют собой пошаговые инструкции для выполнения оперативных задач. Часто процедура является тем инструментом, с помощью которого политика преобразуется в реальное действие. Например, политика паролей формулирует правила конструирования паролей, правила о том, как защитить пароль и как часто его заменять. Процедура управления паролями описывает процесс создания новых паролей, их распределения, а также процесс гарантированной смены паролей на критичных устройствах.

Процедуры безопасности детально определяют действия, которые нужно предпринять при реагировании на конкретные

события, обеспечивают быстрое реагирование в критической ситуации.

В руководстве по компьютерной безопасности, разработанном национальным институтом стандартов и технологий США (National Institute of Standards and Technology – NIST), рекомендовано включать в описание политики информационной безопасности следующие разделы [8].

Предмет политики. В разделе должны быть определены цели и причины разработки политики, область ее применения в конкретном фрагменте системы документооборота организации. Должны быть ясно сформулированы задачи, решаемые с использованием информационных систем, которые затрагивает данная политика. При необходимости могут быть сформулированы термины и определения, используемые в остальных разделах.

Описание позиции организации. В этом разделе необходимо ясно описать характер информационных ресурсов организации, перечень допущенных к информационным ресурсам лиц и процессов и порядок получения доступа к информационным ресурсам организации.

Применимость. В разделе может быть уточнен порядок доступа к данным ИС, определены ограничения или технологические цепочки, применяемые при реализации политики безопасности.

Роли и обязанности. В разделе определяются ответственные должностные лица и их обязанности в отношении разработки и внедрения различных элементов политики. Обычно определяются обязанности администратора безопасности данных (отвечает за содержательную сторону предоставления доступа к информационным ресурсам организации), администратора баз данных (определяет техническую реализацию механизмов разграничения доступа), администратора локальной сети, операторов.

Соблюдение политики. В разделе описываются права и обязанности пользователей ИС. Необходимо явное описание и задокументированное знакомство пользователей с перечнем недопустимых действий при осуществлении доступа к информационным ресурсам организации и наказания за нарушения режимных требований. Должна быть ясно определена технология фиксации фактов нарушения политики безопасности и применения административных мер воздействия к нарушителям.

4.4. Автоматизация разработки ПИБ

В настоящее время на рынке отсутствуют системы, которые предоставляли бы исчерпывающие средства для автоматизации всех аспектов разработки ПИБ. Представлены лишь средства для автоматизации нескольких процессов, связанных с разработкой и реализацией ПИБ:

1. Комплекс мероприятий, связанных с проведением анализа рисков.

– учет материальных или информационных ценностей;

– моделирование угроз ИБ системы;

– собственно анализ рисков с использованием того или иного подхода, например, стоимостный анализ рисков.

2. Мероприятия по оценке соответствия мер по обеспечению ИБ системы некоторому эталонному образцу: стандарту, политике безопасности и т.п.

3. Действия, связанные с разработкой разного рода документов, например, отчетов, диаграмм, профилей защиты, заданий по безопасности.

4. Действия, связанные со сбором, хранением и обработкой статистики по событиям безопасности для организации.

Наиболее широко представлены средства для автоматизации анализа рисков, а также для проверки соответствия информационной системы компании положениям того или иного стандарта. Именно на последних системах, с учетом роли, которую они могут сыграть, стоит остановиться подробнее [8, 12].

Система COBRA производства компании C&A Systems Security Ltd – наиболее известный программный продукт, предназначенный для проверки выполнения требований стандарта ISO 17799. Помимо анализа соответствия информационной системы компании положениям стандарта, система обеспечивает также автоматизацию проведения анализа рисков.

Оценка соответствия системы положениям стандарта ISO 17799 производится следующим образом. Пользователю предлагается ответить на ряд вопросов из следующих групп:

1. Классификация активов и управление ими. Под активами в данном случае понимаются материальные и информационные ценности, рассматриваются вопросы их учета и классификации.

2. Планирование непрерывности ведения бизнеса. Рассматриваются вопросы разработки планов непрерывного ведения бизнеса, их тестирования и распределения ответственности.

3. Управление компьютерами и операциями. Выделяется широкий перечень вопросов, связанных с управлением процессами и сервисами безопасности.

4. Соответствие. Рассматриваются вопросы соответствия информационной инфраструктуры различного рода требованиям, инструкциям и рекомендациям.

5. Безопасность персонала. Рассматриваются вопросы распределения ответственности по реализации положений ПБ между сотрудниками, а также порядок приема сотрудников.

6. Физическая безопасность и безопасность среды. Рассматриваются вопросы организации физической защиты на территории предприятия, охраны, контроля физического доступа, энергетической и противопожарной безопасности.

7. Организация безопасности. Рассматриваются вопросы организации службы ИБ на предприятии, в частности, создания форумов по безопасности, а также порядок взаимодействия со сторонними экспертами по безопасности и распределение ролей в ходе реализации мероприятий по защите информации между сотрудниками.

8. Политика безопасности. Вопросы данного раздела преследуют цель определить положение ПБ в системе мер по обеспечению ИБ организации, а также позволяют оценить структуру этого документа и его применяемость на практике.

9. Управление доступом к системе. Рассматриваются вопросы контроля и разграничения доступа, а также категорирования защищаемой информации.

10. Разработка и поддержка системы. Рассматриваются вопросы обеспечения ИБ системы на протяжении всего жизненного цикла. В частности, оцениваются применяемые технологии анализа рисков.

На основании сведений, полученных в ходе выполнения всех вопросников или некоторой их части, COBRA автоматически генерирует отчет, имеющий следующую структуру:

1. Введение. Содержит общую информацию о сгенерированном отчете.

2. Обзор проверки соответствия. В разделе детализируется информация об использованном вопроснике, выделяются использованные модули и категории вопросов.

3. Анализ несоответствий. Раздел содержит исчерпывающий анализ выявленных несоответствий с указанием ссылок на соответствующие разделы стандарта ISO 17799.

4. Требования по улучшению. Приводятся рекомендации по устранению обнаруженных несоответствий.

5. Перечень вопросов и ответов. Раздел содержит перечень вопросов, которые были использованы при построении отчета, и соответствующих ответов.

Программный комплекс КОНДОР (разработчик – компания Digital Security) является русскоязычным аналогом COBRA-подобной системы. Программа также предназначена для оценки соответствия информационной системы положениям стандарта ISO 17799. Концепции этих двух пакетов совершенно аналогичны: на основании ответов на вопросы генерируется отчет.

Вопросы структурированы в следующие разделы:

- политика безопасности;
- организационные меры;
- управление ресурсами;
- безопасность персонала;
- физическая безопасность;
- управление процессами;
- контроль доступа;
- непрерывность бизнеса;
- соответствие системы;
- разработка систем.

Программа **CC Toolbox**, в отличие от рассмотренных ранее систем, ориентированных исключительно на проверку соответствия требованиям стандарта ISO 17799, предполагает использование инструментария КОБИТ и служит для автоматизации разработки формальной политики безопасности.

Система обеспечивает автоматизацию разработки двух типов документов:

- профилей защиты;
- заданий по безопасности.

Порядок работы с CC Toolbox во многом аналогичен продуктам COBRA и КОНДОР. Пользователю предлагается ответить на ряд вопросов, полностью специфицирующих все разделы профиля защиты или задания по безопасности. На основании информации, полученной из анализа ответов на вопросы, генерируется соответствующий документ.

4.5. Действия при нарушении ПИБ

Нарушение может явиться следствием пользовательской небрежности, случайной ошибки, отсутствия должной информации о текущей политике или ее непонимания. Возможно также, что некое лицо или группа лиц сознательно совершают действия, прямо противоречащие утвержденной политике безопасности [24].

Необходимо заранее определить характер действий, предпринимаемых в случае обнаружения нарушений политики, чтобы эти действия были быстрыми и правильными. Следует организовать расследование, чтобы понять, как и почему нарушение стало возможным. После этого нужно внести коррективы в систему защиты. Тип и серьезность корректив зависят от типа случившегося нарушения.

Политику безопасности могут нарушать самые разные лица. Некоторые из них являются своими, местными пользователями, другие нападают извне. Полезно определить сами понятия «свои» и «чужие», исходя из административных, правовых или политических положений. Эти положения очерчивают характер санкций, которые можно применить к нарушителю – от выговора до привлечения к суду. Таким образом, последовательность ответных действий зависит не только от типа нарушения, но и от вида нарушителя; она должна быть продумана задолго до первого инцидента, хотя это и непросто.

Каждое предприятие должно заранее определить набор административных санкций, применяемых к своим сотрудникам, нарушающим политику безопасности сторонней организации. Кроме того, необходимо позаботиться о защите от ответных действий сторонней организации. При выработке политики безопасности следует учесть все юридические положения, применимые к подобным ситуациям.

Политика безопасности предприятия должна содержать процедуры для взаимодействия с внешними организациями, в число

которых входят правоохранительные органы, средства массовой информации. другие организации. В процедурах должно быть определено, кто имеет право на такие контакты и как именно они совершаются.

Необходимо также продумать и написать процедуры, исполняемые в случае обнаружения нарушений режима безопасности. Для всех видов нарушений должны быть заготовлены соответствующие процедуры.

Когда на организацию совершается нападение, грозящее нарушением информационной безопасности, стратегия ответных действий может строиться под влиянием двух противоположных подходов.

Если руководство опасается уязвимости предприятия, оно может предпочесть стратегию «защититься и продолжить». Главной целью подобного подхода является защита информационных ресурсов и максимально быстрое восстановление нормальной работы пользователей. Действиям нарушителя оказывается максимальное противодействие, дальнейший доступ предотвращается, после чего немедленно начинается процесс оценки нанесенных повреждений и восстановления. Возможно, при этом придется выключить компьютерную систему, закрыть доступ в сеть или предпринять иные жесткие меры. Оборотная сторона данной медали состоит в том, что пока злоумышленник не выявлен, он может вновь напасть на эту же или другую организацию прежним или новым способом.

Другой подход, «выследить и осудить», опирается на иные философию и систему целей. Основная цель состоит в том, чтобы позволить злоумышленнику продолжать свои действия, пока организация не сможет установить его личность. Такой подход может использоваться правоохранительными органами. К сожалению, эти органы не смогут освободить организацию от ответственности, если пользователи обратятся в суд с иском по поводу ущерба, нанесенного их программам и данным.

Необходимо заранее взвесить различные возможности при выборе стратегии ответных действий. Стратегия может зависеть от конкретных обстоятельств нападения. Возможен и выбор единой стратегии на все случаи.

Следующий перечень поможет сделать выбор между стратегиями «защититься и продолжить» и «выследить и осудить».

При каких обстоятельствах предпочесть стратегию «защититься и продолжить»:

1. Активы организации недостаточно защищены.
2. Продолжающееся вторжение сопряжено с большим финансовым риском.
3. Нет возможности или намерения осудить злоумышленника.
4. Неизвестен круг пользователей.
5. Пользователи неопытны, а их работа уязвима.
6. Пользователи могут привлечь организацию к суду за нанесенный ущерб.

При каких обстоятельствах предпочесть стратегию «выследить и осудить»:

1. Активы и системы хорошо защищены.
2. Имеются хорошие резервные копии.
3. Угроза активам организации меньше потенциального ущерба от будущих повторных вторжений.
4. Имеет место согласованная атака, повторяющаяся с большой частотой и настойчивостью.
5. Организация «притягивает» злоумышленников и, следовательно, подвергается частым атакам.
6. Организация готова идти на риск, позволяя продолжить вторжение.
7. Действия злоумышленника можно контролировать.
8. Обслуживающий персонал обладает достаточной квалификацией для успешного выслеживания.
9. Руководство организации желает осудить злоумышленника.
10. Системный администратор знает, какого рода информация обеспечит успешное преследование.
11. Имеется тесный контакт с правоохранительными органами.
12. Организация готова к искам собственных пользователей по поводу программ и данных, скомпрометированных во время выслеживания злоумышленника.

4.6. Классификация АС по степени защищенности

Руководящий документ (РД) «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации» устанавливает классификацию СВТ по уровню защищенности от НСД к информации на базе перечня показателей защищенности и

совокупности описывающих их требований [13]. Основой для разработки этого документа явилась «Оранжевая книга». Этот оценочный стандарт устанавливает семь классов защищенности СВТ от НСД к информации.

Устанавливается семь классов защищенности СВТ от НСД к информации. Самый низкий класс седьмой, самый высокий – первый. Классы объединяются в четыре группы, отличающиеся уровнем защиты:

Первая группа содержит только один седьмой класс, к которому относят все СВТ, не удовлетворяющие требованиям более высоких классов;

Вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;

Третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;

Четвертая группа характеризуется верифицированной защитой и содержит только первый класс.

Руководящий документ «АС. Защита от НСД к информации. Классификация АС и требования по защите информации» устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов. К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

– наличие в АС информации различного уровня конфиденциальности;

– уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;

– режим обработки данных в АС – коллективный или индивидуальный.

В документе устанавливаются девять классов защищенности АС от НСД к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы включаются в три группы, отличающиеся особенностями обработки информации в АС.

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

В табл. 4.1 приведены классы защищенности АС и требования для их обеспечения.

Таблица 4.1

Требования к защищенности автоматизированных систем

Подсистемы и требования	**Классы**								
	3Б	**3А**	**2Б**	**2А**	**1Д**	**1Г**	**1В**	**1Б**	**1А**
1. Подсистема управления доступом									
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:									
- в систему	+	+	+	+	+	+	+	+	+
- к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	-	-	-	+	-	+	+	+	+
- к томам, каталогам, файлам, записям, полям записей	-	-	-	+	-	+	+	+	+
1.2. Управление потоками информации	-	-	-	+	-	-	+	+	+
2. Подсистема регистрации и учета									
2.1. Регистрация и учет:									
- входа/выхода субъектов доступа в/из системы (узла сети)	+	+	+	+	+	+	+	+	+
- выдачи печатных (графических) выходных документов	-	+	-	+	-	+	+	+	+
- запуска/завершения программ и процессов (заданий, задач)	-	-	-	+	-	+	+	+	+
- доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	-	-	-	+	-	+	+	+	+
- изменения полномочий субъектов доступа	-	-	-	-	-	-	+	+	+
- создаваемых защищаемых объектов доступа	-	-	-	+	-	-	+	+	+
2.2. Учет носителей информации	+	+	+	+	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	-	+	-	+	-	+	+	+	+

Окончание табл. 4.1.

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

Принятые в таблице обозначения:
"-" нет требований к данному классу;
"+" есть требования к данному классу
"СЗИ НСД" – система защиты информации от несанкционированного доступа.

В таблице систематизированы минимальные требования, которым необходимо следовать, чтобы обеспечить конфиденциальность информации.

РД «СВТ. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации» целесообразно использовать при анализе системы защиты внешнего периметра

корпоративной сети в качестве основных критериев. Данный документ определяет показатели защищенности межсетевых экранов (МЭ). Каждый показатель защищенности представляет собой набор требований безопасности, характеризующих определенную область функционирования МЭ. Всего выделяется пять показателей защищенности:

- управление доступом;
- идентификация и аутентификация;
- регистрация событий и оповещение;
- контроль целостности;
- восстановление работоспособности.

На основании показателей защищенности определяются следующие пять классов защищенности МЭ:

- Простейшие фильтрующие маршрутизаторы – 5 класс;
- Пакетные фильтры сетевого уровня – 4 класс;
- Простейшие МЭ прикладного уровня – 3 класс;
- МЭ базового уровня – 2 класс;
- Продвинутые МЭ – 1 класс.

МЭ первого класса защищенности могут использоваться в АС класса 1А, обрабатывающих информацию «Особой важности». Второму классу защищенности МЭ соответствует класс защищенности АС 1Б, предназначенный для обработки «совершенно секретной» информации и т.п.

В «Оранжевой книге» определены классы систем, распознаваемые при помощи критериев оценки гарантированно защищенных вычислительных систем. Классы представлены в порядке нарастания требований с точки зрения обеспечения безопасности ЭВМ:

1. Класс (D): Минимальная защита
2. Класс (C1): Защита, основанная на разграничении доступа (DAC)
3. Класс (C2): Защита, основанная на управляемом контроле доступом
4. Класс(B1): Мандатная защита, основанная на присваивании меток объектам и субъектам, находящимся под контролем ТСВ
5. Класс (B2): Структурированная защита
6. Класс (B3): Домены безопасности
7. Класс (A1): Верифицированный проект

4.7. Принципы, реализуемые при построении подсистемы информационной безопасности

Подсистема информационной безопасности строится на базе использования следующих основных принципов:

1) законность;
2) экономическая оправданность механизмов защиты
3) системность;
4) комплексность;
5) непрерывность защиты;
6) катастрофоустойчивость;
7) равнопрочность;
8) своевременность;
9) использование существующей базы;
10) использование серийных решений;
11) преемственность и непрерывность совершенствования;
12) преимущественное использование отечественных аппаратно-программных средств защиты;
13) устойчивость функционирования средств защиты при отдельных отказах;
14) масштабируемость подсистемы информационной безопасности;
15) разумная достаточность;
16) рубежность;
17) разделение на подсистемы;
18) персональная ответственность;
19) минимизация полномочий;
20) персонификация при определении порядка доступа к защищаемой информации;
21) взаимодействие и сотрудничество;
22) гибкость системы защиты;
23) открытость алгоритмов и механизмов защиты;
24) простота применения средств защиты;
25) научная обоснованность и техническая реализуемость;
26) максимально возможная степень автоматизации процессов управления безопасностью;
27) специализация и профессионализм;
28) обязательность контроля;
29) этапность;
30) принцип психологической приемлемости.

Рассмотрим указанные принципы подробнее.

Законность

Разработка подсистемы информационной безопасности при доступе к системе осуществляется в соответствии с действующим законодательством в области информации, информатизации и защиты информации, других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с информацией. Принятые меры безопасности информации не должны препятствовать доступу к данным сотрудникам организации в пределах своих полномочий в предусмотренных законодательством случаях к информации конкретных систем.

Экономическая оправданность механизмов защиты

предписывает использование простейшего из всевозможных вариантов проекта, который обеспечивает достижение желаемой цели. Хотя этот принцип относится ко многим аспектам проектирования систем, он наиболее пригоден при разработке механизмов защиты, так как ошибки проектирования и реализации, которые ведут к неконтролируемым способам доступа к данным, могут быть не замечены в ходе нормального использования системы. Строгое соблюдение этого принципа приводит к применению на практике таких методов, как проверка «строка за строкой» программных средств и физическая проверка аппаратных средств, реализующих механизмы защиты.

Системность

Системный подход к построению подсистемы информационной безопасности при доступе к системе предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности информации АС.

При создании подсистемы информационной безопасности учитываются все слабые и наиболее уязвимые места системы обработки информации, 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 строится с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

Комплексность

Комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных её компонентов. Внешняя защита обеспечивается физическими средствами, организационными и правовыми мерами.

Кроме того, комплексный подход к обеспечению безопасности информации подразумевает использование защитных механизмов на всех этапах жизненного цикла системы, от её проектирования и до вывода из эксплуатации, и совместное решение целого спектра вопросов, начиная от физической защиты объектов АС, с применением системы контроля доступа, и оканчивая вопросами поддержки функционирования в критических ситуациях.

Непрерывность защиты

Защита информации – не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла.

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 её функционирования.

Кроме того, организационно-техническое обеспечение должно быть реализовано таким образом, чтобы при внесении любых изменений в структуру, адекватные изменения вносились и в её подсистему защиты.

Катастрофоустойчивость

Означает такое построение и эксплуатацию, при которых вероятность безвозвратной потери информации, обрабатываемой и хранимой, при возможном разрушении, а также при возможном значительном или частичном нанесении физического ущерба зданиям, помещениям, в которых располагается оборудование, и системам жизнеобеспечения, будет минимальна.

Равнопрочность

При создании системы комплексной защиты используется принцип равнопрочности защиты, при котором в системе отсутствуют элементы, снижающие уровень защищенности на отдельных её участках.

Своевременность

Предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач ПИБ и реализацию мер обеспечения безопасности информации по мере развития системы в целом и её подсистемы информационной безопасности, в частности.

Использование существующей базы

Базой для подсистемы информационной безопасности является существующая система, находящаяся в процессе развития. При этом в подсистемы информационной безопасности максимально задействуются штатные механизмы защиты информации, имеющиеся в аппаратных и программных компонентах (на серверах, рабочих станциях, маршрутизаторах, в операционных системах, прикладном программном обеспечении).

Использование серийных решений

В системе комплексной защиты информации максимально используются серийно выпускаемое отечественное и зарубежное оборудование и программное обеспечение, адаптируемое к конкретным условиям эксплуатации и положительно себя зарекомендовавшее.

Преемственность и совершенствование

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования системы и её защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

Преимущественное использование отечественных аппаратно-программных средств защиты

При построении ПИБ предполагается осуществить преимущественное использование отечественных аппаратно-программных средств защиты в рамках реализации единой политики информационной безопасности на объектах.

Устойчивость функционирования средств защиты

При проектировании ПИБ закладываются такие решения, которые бы обеспечили устойчивое функционирование средств защиты и доступ пользователей к ресурсам объектов, в условиях возможных отдельных отказов и сбоев оборудования и активных негативных воздействий на аппаратно-программные средства защиты.

Масштабируемость подсистемы информационной безопасности

Подсистема информационной безопасности должна удовлетворять требованию масштабируемости, то есть обеспечивать заданный уровень работоспособности и эффективности защиты в условиях динамического развития, роста объема информационных и программных ресурсов объектов.

Разумная достаточность

Предполагает экономическую целесообразность, сопоставимость возможного ущерба от разглашения, утраты, утечки, уничтожения и искажения информации и затрат на организацию её защиты. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать эргономические показатели работы, в которой эта информация передается, обрабатывается и хранится. Излишние меры безопасности, помимо экономической неэффективности, приводят к утомлению и раздражению персонала.

Создать абсолютно непреодолимую систему защиты принципиально невозможно. Пока информация находится в обращении, принимаемые меры могут только снизить вероятность негативных воздействий или ущерб от них, но не исключить их полностью. При достаточном количестве времени и средств возможно преодолеть любую защиту. Поэтому имеет смысл рассматривать некоторый приемлемый уровень обеспечения безопасности, заданный в РД Гостехкомиссии «Автоматизированные системы. Защита от несанкционированного доступа к информации.

Классификация автоматизированных систем и требований по защите информации». Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми (задача анализа риска).

Рубежностъ

Для каждой защищаемой системы используется принцип «рубежности» для построения многоуровневой системы доступа к защищаемой информации (табл. 4.2) Одним из эффективных внешних рубежей защиты системы должны быть СЗИ, реализованные на уровне операционных систем (ОС) в силу того, что ОС – это та часть компьютерной системы, которая управляет использованием всех её ресурсов. Рубеж защиты на прикладном уровне, учитывающий особенности предметной области, представляет собой внутренний рубеж защиты.

Таблица 4.2

Уровни доступа к защищаемой информации

№ уровня защиты	Наименование уровня защиты
Уровень 5	Доступ к передаче информации по каналам связи (ввод ключа шифрования и ЭЦП)
Уровень 4	Доступ к информации в базах данных (ввод пароля в прикладном ПО для доступа к базам данных)
Уровень 3	Доступ к ресурсам (по аутентификации сетевого имени, ввод имени и индивидуального пароля для входа в сеть)
Уровень 2	Доступ к операционной системе рабочей станции (использование встроенных средств операционной системе)
Уровень 1	Система доступа в помещения (к рабочим станциям и оборудованию)
Уровень 0	Система доступа на объект информатизации

Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности информации и системы её обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

Принцип минимизации полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью. Доступ к информации должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

Принцип персонификации при определении порядка доступа к защищаемой информации

Означает, что все полномочия при определении порядка доступа пользователей и администраторов к защищаемой информации должны быть персональными, указаны явно и проверены непосредственно перед предоставлением доступа.

Гибкость системы защиты

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты обладают определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установка средств защиты осуществляется на работающую систему, не нарушая процесса её нормального функционирования. Кроме того, внешние условия и требования с течением времени меняются. В таких ситуациях свойство гибкости системы защиты избавляет владельцев от необходимости принятия кардинальных мер по полной замене средств защиты на новые.

Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что технология систем защиты не должна базироваться на «секретных» алгоритмах. Этот принцип широко используется при проектировании безопасных систем и сетей связи. Высокое качество систем защиты обеспечивается не недостатком знаний у возможных нарушителей, а использованием широко опробованных (как правило, открытых) стандартов и правильной организацией управления ключевой информацией. Использование алгоритмов, основанных на открытых стандартах в области информационной безопасности, повышает степень доверия пользователей к системе защиты и формирует правильную психологическую установку на необходимость внимательности и аккуратности при работе с ключевой информацией. Знание алгоритмов работы системы защиты

не должно давать возможности её преодоления (даже авторам). Это, однако, не означает, что информация о конкретной системе защиты должна быть общедоступна.

Простота применения средств защиты

Механизмы защиты являются интуитивно понятными и простыми в использовании. Применение средств защиты не связывается со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не требует от пользователя выполнения рутинных малопонятных ему операций.

Научная обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты информации реализованы на современном уровне развития науки и техники, обоснованы с точки зрения достижения заданного уровня безопасности информации и соответствуют установленным нормам и требованиям по безопасности информации.

Максимально возможная степень автоматизации процессов управления безопасностью

При проектировании, эксплуатации ПИБ должна быть обеспечена максимально возможная степень автоматизации управления безопасностью информацией, в том числе и при управлении конфигурацией ПИБ.

Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляется профессионально подготовленными специалистами организации (специалистами подразделений технической защиты информации).

Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации на основе используемых систем и средств

защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты осуществляется на основе применения средств оперативного контроля и регистрации и охватывает как несанкционированные, так и санкционированные действия пользователей.

Этапность

Построение подсистемы информационной безопасности осуществляется поэтапно.

Принцип психологической приемлемости

В соответствии с принципом психологической приемлемости работы средств защиты данных взаимодействие людей с системой (и подсистемой защиты) не должно быть сложным. Пользователи должны шаблонно и автоматически применять имеющиеся механизмы защиты. Чрезмерное усложнение механизмов защиты может вызывать их внутреннее неприятие и побуждать к использованию различных форм скрытого саботажа. Осознанное принятие используемых средств и методов обеспечения информационной безопасности и оценка комплекса применяемых мер как необходимых приводит к уменьшению числа ошибок пользователей. В этом случае аномальное поведение потенциального нарушителя становится более заметным и проще устанавливается. Принцип психологической приемлемости является важным при выборе процедур аутентификации и модели управления доступом.

4.8. Особенности политики информационной безопасности распределенных систем

Информационная безопасность распределенных систем традиционно рассматривается в трактовке технической спецификации X.800, появившейся немногим позднее «Оранжевой книги», но весьма полно и глубоко трактующей вопросы информационной безопасности распределенных систем.

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

Выделяют следующие сервисы безопасности и исполняемые ими роли:

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

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

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

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

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

В таблице 4.3 указаны уровни эталонной семиуровневой модели OSI, на которых могут быть реализованы функции безопасности. Отметим, что прикладные процессы, в принципе, могут взять на себя поддержку всех защитных сервисов.

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

– шифрование;
– электронная цифровая подпись;
– механизмы управления доступом. Могут располагаться на любой из участвующих в общении сторон или в промежуточной точке;

Таблица 4.3

Распределение функций безопасности по уровням модели OSI

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

Принятые обозначения:
"+" данный уровень может предоставить функцию безопасности;
"-" данный уровень не подходит для предоставления функции безопасности.

– механизмы контроля целостности данных. В рекомендациях X.800 различаются два аспекта целостности: целостность отдельного сообщения или поля информации и целостность потока сообщений или полей информации. Для проверки целостности потока сообщений (то есть для защиты от кражи, переупорядочивания, дублирования и вставки сообщений) используются порядковые номера, временные штампы, криптографическое связывание или иные аналогичные приемы;

– механизмы аутентификации. Согласно рекомендациям X.800, аутентификация может достигаться за счет использования паролей, личных карточек или иных устройств аналогичного назначения, криптографических методов, устройств измерения и анализа биометрических характеристик;

– механизмы дополнения трафика;

– механизмы управления маршрутизацией. Маршруты могут выбираться статически или динамически. Оконечная система, зафиксировав неоднократные атаки на определенном маршруте, может отказаться от его использования. На выбор маршрута способна повлиять метка безопасности, ассоциированная с передаваемыми данными;

– механизмы нотаризации. Служат для заверения таких коммуникационных характеристик, как целостность, время, личности отправителя и получателей. Заверение обеспечивается надежной третьей стороной, обладающей достаточной информацией. Обычно нотаризация опирается на механизм электронной подписи.

В табл. 4.4 сведены сервисы (функции) и механизмы безопасности. Таблица показывает, какие механизмы (по отдельности или в комбинации с другими) могут использоваться для реализации той или иной функции.

Таблица 4.4

Взаимосвязь функций и механизмов безопасности

Функции	Механизмы							
	Шифрование	Электронная подпись	Управление доступом	Целостность	Аутентификация	Дополнение трафика	Управление маршрутизацией	Нотаризация
Аутентифика-ция партнеров	+	+	-	-	+	-	-	-
Аутентифика-ция источника	+	+	-	-	-	-	-	-
Управление доступом	-	-	+	-	-	-	-	-
Конфиденци-альность	+	-	+	-	-	-	+	-
Избирательная конфиденциа-льность	+	-	-	-	-	-	-	-
Конфиденци-альность трафика	+	-	-	-	-	+	+	-
Целостность соединения	+	-	-	+	-	-	-	-
Целостность вне соединения	+	+	-	+	-	-	-	-
Неотказуе-мость	-	+	-	+	-	-	-	+

Принятые обозначения:
"+" данный уровень может предоставить функцию безопасности;
"-" данный уровень не подходит для предоставления функции безопасности.

Администрирование средств безопасности включает в себя распространение информации, необходимой для работы сервисов и механизмов безопасности, а также сбор и анализ информации об их

функционировании. Примерами могут служить распространение криптографических ключей, установка значений параметров защиты, ведение регистрационного журнала и т.п.

Концептуальной основой администрирования является информационная база управления безопасностью. Эта база может не существовать как единое (распределенное) хранилище, но каждая из оконечных систем должна располагать информацией, необходимой для реализации избранной политики безопасности.

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

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

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

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

Обязанности администратора механизмов безопасности определяются перечнем задействованных механизмов, - типичный перечень которых таков:

– управление ключами (генерация и распределение);
– управление шифрованием (установка и синхронизация криптографических параметров). К управлению шифрованием можно отнести и администрирование механизмов электронной подписи. Управление целостностью, если оно обеспечивается криптографическими средствами, также тяготеет к данному направлению;
– администрирование управления доступом (распределение информации, необходимой для управления – паролей, списков доступа и т.п.);
– управление аутентификацией (распределение информации, необходимой для аутентификации - паролей, ключей и т.п.);

– управление дополнением трафика (выработка и поддержание правил, задающих характеристики дополняющих сообщений – частоту отправки, размер и т.п.);
– управление маршрутизацией (выделение доверенных путей);
– управление нотаризацией (распространение информации о нотариальных службах, администрирование этих служб).

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

4.9. Пример политики информационной безопасности

Политика информационной безопасности

1. Общие положения.

Настоящая Политика регламентирует единый подход в организации (далее по тексту Компания) к защите информации, составляющей коммерческую тайну, и устанавливает режим охраны таких сведений (перечень таких сведений приведен в приложении №1).

Положения Политики распространяются на информацию, составляющую коммерческую тайну Организации, независимо от вида носителя, на котором она зафиксирована.

Информационная безопасность Организации, заключается в неукоснительном соблюдении всеми структурными подразделениями Организации требований и принципов, изложенных в Политике информационной безопасности (далее по тексту Политика).

Информационная безопасность обеспечивается комплексной системой организационно-управленческих, административно-правовых, инженерно-технических и других мер защиты информации, определенных Политикой.

Для более полного отражения в Политике изменений в инфраструктуре Организации и приведению в соответствие с действующим законодательством раз в год Политика подлежит пересмотру.

2. Формирование Перечня сведений, составляющих коммерческую тайну Организации.

Перечень сведений, составляющих коммерческую тайну Организации (далее по тексту Перечень), формируется путем обобщения предложений, поступающих от руководителей

структурных подразделений Организации. Перечень рассматривается и утверждается на Административном совете Организации.

В Перечень включаются сведения, позволяющие Организации при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду, а также сведения, которые имеет действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам.

Сведениям, вошедшим в Перечень, присваивается гриф «Конфиденциально».

Сведения, включенные в Перечень, имеют ограничительный характер на использование (применение). Ограничения, вводимые на использование таких сведений, направлены на защиту интересов Организации, ее клиентов и партнеров.

3. Анализ угроз информационной безопасности Организации и модель действия нарушителя.

Угрозами информационной безопасности Организации являются потенциально возможные действия по отношению к информационным ресурсам, носителям сведений и технологическим ресурсам, связанным с обработкой и хранением сведений, составляющими коммерческую тайну Организации. К таким действиям относятся:

Несанкционированная модификация информации как частичное или полное изменение ее состава и содержания;

Разрушение (уничтожение) информации;

Несанкционированный доступ к сведениям, составляющим коммерческую тайну;

Разглашение информации - это умышленные или неосторожные действия со сведениями, составляющими коммерческую тайну, приведшие к ознакомлению с ними лиц, не имеющими к ним допуска;

Выход из строя оборудования, отвечающего за хранение или обработку сведений, составляющих коммерческую тайну.

4. Модель действия нарушителя информационной безопасности.

При построении модели нарушителя информационной безопасности используется неформальная модель злоумышленника (нарушителя), отражающая причины и мотивы действий, его возможности, априорные знания, преследуемые цели, основные пути

достижения поставленных целей, способы реализации исходящих от него угроз, место и характер действия, возможная тактика.

По отношению к Организации потенциальных нарушителей информационной безопасности условно можно разделить на внутренних и внешних.

К внутренним нарушителям относятся:

– сотрудники Организации, имеющие доступ к охраняемой информации с правами администратора;
– сотрудники организации, имеющие доступ к охраняемой информации на уровне пользователей;
– технический персонал по обслуживанию здания.

К внешним нарушителям относятся:

– клиенты и посетители организации;
– сотрудники органов ведомственного надзора;
– нарушители пропускного режима;
– представители конкурирующих организаций.

Компетентность и техническая подготовка возможных нарушителей может быть самой различной от низкой квалификации до специалистов уровня программистов и системного администратора.

Возможные варианты действия внутренних нарушителей режима информационной безопасности:

– непроизводственная активность сотрудников Организации (пользователей компьютеров), которая может выражаться в нецелевом использовании ресурсов интернет и электронной почты, самостоятельная установка и использование не разрешенного программного обеспечения. Такие действия могут стать причиной и способствовать распространению компьютерных вирусов и других вредоносных программ, что может привести к потере данных на рабочих станциях и серверах Организации, несанкционированному доступу посторонних лиц к конфиденциальной информации;
– вход легального пользователя в компьютерную сеть Организации с реквизитами другого пользователя может использоваться для выполнения запрещенных действий в корпоративной сети Организации или хищению информации;
– установка на компьютер, подключенный к сети Организации, специального программного обеспечения, позволяющего проводить

исследование трафика сети и/или осуществлять атаки на ресурсы сети;

– нерегламентированное использование компьютеров сотрудниками Организации, по роду своей деятельности не имеющими доступа к ресурсам сети;

– несанкционированное копирование конфиденциальной информации;

– уничтожение информации на серверах и рабочих станциях;

– внесение нерегламентированных изменений в данные и программное обеспечение;

– кража носителей конфиденциальной информации;

– кража или вывод из строя оборудования, отвечающего за обработку и хранение конфиденциальной информации.

Возможные варианты действия внешних нарушителей режима информационной безопасности:

– атака на сервисы удаленного доступа и публичные интернет сервисы Организации. Целью может являться захват управления сервисом, получение полномочий администратора, доступ в корпоративную сеть Организации;

– заражение клиентской рабочей станции компьютерным вирусом или другой вредоносной программой через сообщения электронной почты;

– несанкционированное копирование конфиденциальной информации;

– уничтожение информации на серверах и рабочих станциях;

– внесение нерегламентированных изменений в данные и программное обеспечение;

– кража носителей конфиденциальной информации;

– Кража или вывод из строя оборудования, отвечающего за обработку и хранение конфиденциальной информации.

5. Требования к системе защиты информации.

Основной задачей системы информационной безопасности Организации является управление информационными рисками и минимизация их для всех видов потенциальных угроз.

Система защиты информации в Организации строится на следующих принципах:

– непрерывность во времени;

– комплексность;

– целенаправленность;
– универсальность и надежность;
– плановость мероприятий по защите информации;
– адекватность уровню важности защищаемых ресурсов;
– все структурные подразделения организации принимают участие в процессе защиты информации в сфере своей деятельности и в рамках своей компетенции;
– комплексный контроль функционирования системы защиты информации.

Система защиты информации Организации должна обеспечивать:
– персональный допуск сотрудников Организации к работе с конфиденциальной информацией в рамках, необходимых для выполнения своих служебных обязанностей;
– управление информационными потоками;
– возможность аутентификации и идентификации сотрудников Организации, обращающихся к защищаемой информации;
– регулярное создание страховых копий критичных информационных ресурсов Организации;
– регулярное осуществление контроля целостности программного обеспечения;
– регулярное проведение мероприятий по борьбе с компьютерными вирусами и другими вредоносными программами;
– безопасное подключение корпоративной сети Организации к интернету;
– возможность контроля над действиями сотрудников Организации в корпоративной сети;
– объекты информационной системы Организации, подлежащие защите.

Объектами информационной защиты являются носители конфиденциальных сведений, вошедших в Перечень, технологические процессы и оборудование, связанные с обработкой таких сведений.

К защищаемым объектам относятся:
– документы на бумажных носителях, содержащие сведения, вошедшие в Перечень;
– съемные машинные носители информации, на которых в электронном виде хранятся сведения, вошедшие в Перечень;

– рабочие станции и сервера Организации;
– сетевое оборудование (маршрутизаторы, коммутаторы);
– программно-аппаратные средства защиты информации (межсетевые экраны, средства шифрования);
– каналы связи, по которым передаются в электронном виде сведения, вошедшие в Перечень.

6. Подбор персонала и ответственность за нарушение режима информационной безопасности.

Подбор кандидатов и прием на работу в Компанию осуществляется на конкурсной основе. Организация подбора и проведение конкурсов на вакантные должности находится в компетенции менеджера по персоналу.

Кандидаты на работу в Компанию проходят собеседование в Службе безопасности.

При приеме на работу работник подписывает обязательство о неразглашении коммерческой тайны и проходит инструктаж по информационной безопасности у системного администратора.

В письменном трудовом договоре с сотрудником и его должностных обязанностях должны указываться его обязанности по соблюдению режима информационной безопасности.

Руководители структурных подразделений Организации несут персональную ответственность за соблюдение режима информационной безопасности сотрудниками своих подразделений.

Сотрудник несет ответственность за разглашение коммерческой тайны во время трудовых отношений и в течении двух лет после их прекращения в порядке, установленном законодательством.

Разглашение сведений ограниченного распространения и нарушение режима информационной безопасности является чрезвычайным происшествием. По всем фактам проводится служебное расследование комиссией, назначаемой приказом Генерального директора.

Задачи служебного расследования:
– выяснение обстоятельств разглашения коммерческой тайны или потери носителей таких сведений;
– выявление виновных в разглашении сведений, составляющих коммерческую тайну Организации;
– выявление причин и условий, при которых стало возможно разглашение сведений ограниченного распространения или потеря носителей таких сведений;

– принятие действенных мер по недопущению подобных происшествий;

Служебное расследование проводится в минимально короткий срок.

Одновременно с работой комиссии должны проводиться мероприятия по локализации нежелательных последствий из-за разглашения сведений, составляющих коммерческую тайну.

Результаты работы комиссии письменно докладываются Генеральному директору Организации.

7. Доступ сотрудников Организации к сведениям, составляющим Коммерческую тайну.

Допуск сотрудников Организации к сведениям ограниченного распространения осуществляется в соответствии с их должностными инструкциями, в рамках необходимых для выполнения служебных обязанностей на основании заявки, подаваемой руководителем структурного подразделения и утверждаемой Генеральным директором.

Выделение прав и полномочий сотрудникам Организации для работы со сведениями ограниченного распространения в системах электронного документооборота Организации производят администраторы соответствующих информационных систем.

Лица, допущенные к работе со сведениями ограниченного распространения, обязаны:

– знать и строго выполнять требования настоящей Политики и других инструкций, регламентирующих мероприятия режима информационной безопасности;

– немедленно докладывать своему непосредственному начальнику о возможных причинах или фактах утечки конфиденциальной информации;

– знакомиться с конфиденциальными сведениями только в объемах своих служебных обязанностей;

– немедленно сообщать непосредственному начальнику об утрате или недостаче носителей конфиденциальных сведений;

– о попытке посторонних лиц получить доступ к конфиденциальной информации немедленно докладывать руководителю подразделения и начальнику Службы безопасности.

Сотрудникам Организации, допущенным к работе с конфиденциальной информацией, запрещается:

– использовать конфиденциальные сведения в открытой переписке, публичных выступлениях;
– использовать конфиденциальные сведения в личных целях;
– вести обсуждение вопросов безопасности конфиденциального характера в общественных местах;
– выносить с территории Организации носители конфиденциальных сведений без разрешения непосредственного начальника;

8. Работа с документами, содержащими коммерческую тайну.

Делопроизводство и работа с документами, содержащими сведения, вошедшие в Перечень, является составной частью режима информационной безопасности. К разработке таких документов на бумажных носителях следует прибегать лишь в случаях действительной необходимости, когда нет условий для осуществления личного общения, осуществления обмена электронными документами или когда существуют нормативные документы, предписывающие представление документа на бумажном носителе.

Работа сотрудников Организации с конфиденциальными документами должна производиться в служебных помещениях Организации.

По окончании рабочего дня каждый исполнитель обязан проверить наличие находящихся у него конфиденциальных документов.

Конфиденциальные документы печатаются в строго ограниченном количестве экземпляров. Черновики и испорченные экземпляры таких документов должны сразу уничтожаться.

Каждый экземпляр документа, содержащий сведения ограниченного распространения, оформляется следующим образом:
– на первом листе, в правом верхнем углу указывается гриф «Конфиденциально»;
– на последнем листе в левом нижнем углу указывается, фамилия исполнителя и дата изготовления.

Отправка документов с грифом «Конфиденциально» производится с разрешения начальников структурных подразделений Организации.

Уничтожение документов с грифом «Конфиденциально» производится с разрешения начальника структурного подразделения Организации.

Контроль за ведением конфиденциального делопроизводства в подразделениях Организации возлагается на Начальников структурных подразделений.

9. Правила размещения элементов компьютерной сети.

Под элементами компьютерной сети следует понимать следующее оборудование:

Съемные машинные носители, на которых производится запись конфиденциальных сведений;

Рабочие станции и сервера Организации;

Сетевое оборудование (маршрутизаторы, коммутаторы);

Программно-аппаратные средства защиты информации (межсетевые экраны, средства шифрования).

Условия размещения элементов компьютерной сети должны обеспечивать:

Сохранность элементов компьютерной сети;

Исключение возможности несанкционированного доступа посторонних лиц.

Помещения, в которых расположены элементы компьютерной сети, должны удовлетворять следующим требованиям:

Входные двери должны быть оборудованы замками, гарантирующими надежное закрытие помещений в нерабочее время;

Помещения должны быть оборудованы охранной и пожарной сигнализацией, с выводом сигнала тревоги на пульт охраны;

Условия размещения оборудования должны соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности.

Входная дверь серверной оборудуется системой контроля доступа и доводчиком двери. Запасные ключи от серверной хранятся в опечатанном пенале в сейфе у начальника Службы безопасности.

10. Обеспечение режима информационной безопасности при работе с ресурсами интернет и электронной почтой.

Подключение к сети интернет.

Подключение корпоративной сети Организации к сети интернет должно осуществляться только через межсетевой экран.

Весь входящий и исходящий трафик Организации должен проходить через фильтры межсетевого экрана.

Межсетевой экран администрируется локально или удаленно с фиксированного адреса администратора.

В настройке межсетевого экрана должны быть закрыты все не используемые сервисы и протоколы. Необходимо постоянно обновлять программное обеспечение межсетевого экрана, устанавливать все дополнения и обновления. Для межсетевого экрана допускается только один пользователь - администратор, остальные пользователи должны быть удалены или заблокированы.

Серверы с размещенными на них Интернет сервисами должны размещаться в демилитаризованной зоне, созданной межсетевым экраном.

Доступ к FTP должен быть разрешен только изнутри наружу и только определенному кругу пользователей. При необходимости доступа снаружи внутрь должна использоваться усиленная аутентификация.

Доступ пользователей к сети интернет должен осуществляться только через прокси-сервер Организации.

Межсетевой экран и прокси-сервер должны вести детальные системные журналы всех сеансов. Доступ к журналам должны иметь ограниченное число сотрудников Организации.

На Межсетевом экране и/или прокси-сервере должны вестись «Стоп листы» ресурсов интернет сомнительного содержания.

Межсетевой экран или прокси-сервер должен разрешать загрузку только тех программ на ActiveX, Java, Javascript, которые разрешены.

Настройки межсетевого экрана или прокси-сервера должны запрещать загрузку программного обеспечения, кроме ограниченного круга пользователей.

Операционные системы и программное обеспечение интернет серверов Организации должны содержать все исправления, рекомендованные производителем.

Интернет серверы Организации, работающие под UNIX подобными операционными системами, не должны запускаться с правами суперпользователя.

Безопасность WWW сервера Организации.

Все общедоступные WWW-сервера Организации, подключенные к интернету, должны находиться в демилитаризованной зоне либо вне зоны корпоративной сети. Сведения ограниченного распространения не должны размещаться на публичном WWW сервере Организации.

Перед публикацией на WWW сервере Организации информация должна быть просмотрена и утверждена так же, как утверждаются официальные документы Организации.

Все публично доступные WWW сервера Организации должны регулярно тестироваться на предмет корректности ссылок.

Доступ пользователей в сеть интернет.

Веб-браузеры должны быть сконфигурированы так, чтобы выполнялись следующие правила:

– доступ к интернету должен осуществляться только через прокси сервер Организации;

– каждый загружаемый файл должен проверяться на вирусы и троянские программы;

– пользователям без особого разрешения запрещается устанавливать и использовать внешние почтовые серверы и внешние прокси-серверы.

Использование электронной почты.

Электронные документы, содержащие конфиденциальную информацию, не должны отправляться с помощью электронной почты по открытым каналам в не зашифрованном виде.

Пользователи могут использовать только разрешенные администратором сети почтовые программы.

Никто из посетителей Организации или временных сотрудников не имеет права использовать электронную почту Организации.

Почтовые сервера должны быть сконфигурированы так, чтобы отвергать письма, адресованные не домену Организации.

Связь с территориально удаленными подразделениями Организации должна осуществляться только по закрытым каналам связи с использованием средств криптографической защиты информации.

Контроль выполнения мероприятий по информационной безопасности при работе в сети интернет и использованию электронной почты возлагается на администратора компьютерной сети.

11. Обеспечение режима информационной безопасности на рабочих станциях.

На всех рабочих станциях обязателен антивирусный контроль с автоматическим периодическим обновлением антивирусных баз и автоматическим запуском антивирусного монитора.

Использование на рабочих станциях дисковых ресурсов с общим доступом допускается только в исключительных случаях.

Использование на рабочих станциях накопителей со съемными машинными носителями информации и портов USB допускается в исключительных случаях.

Рабочие станции, на жестких дисках которых хранится конфиденциальная информация, защищаются программно-аппаратными комплексами защиты информации от несанкционированного доступа с возможность криптографической защиты хранящейся информации.

Пользователям запрещается:

– входить в компьютерную сеть Организации, используя чужие реквизиты доступа;

– оставлять без присмотра подключенное и не заблокированное рабочее место;

– самостоятельно изменять аппаратную или программную конфигурацию рабочих станций;

– самостоятельно устанавливать на рабочую станцию программное обеспечение;

– разрешать другим лицам работу на компьютере со своими правами доступа;

– запрещается загружать из сети интернет программное обеспечение;

– запрещается отключать антивирусное программное обеспечение, установленное на их рабочих станциях, и изменять его настройки.

Пользователь компьютерной сети Организации обязан:

– соблюдать требования регламентирующих документов;

– использовать персональный компьютер и ресурсы компьютерной сети Организации только для выполнения своих служебных обязанностей;

– сохранять рабочие материалы и документы в электронном виде на специально выделенном каталоге файлового сервера;

– блокировать рабочую станцию при необходимости покинуть рабочее место на непродолжительное время;

– выключать рабочую станцию при уходе с рабочего места на продолжительное время;

Контроль над действиями пользователей компьютерной сети осуществляется по протоколам, формируемыми информационными системами администратором компьютерной сети. Объем контрольных мероприятий и их периодичность указывается в должностных обязанностях соответствующих специалистов и в контрольных функциях соответствующих структурных подразделениях.

12. Применение парольной защиты.

Информация о паролях пользователей является конфиденциальной информацией, предназначенной для идентификации и допуска каждого конкретного пользователя к выделенным ему информационным ресурсам.

Операционные системы рабочих станций, включенных в компьютерную сеть Организации, должны иметь настройки, позволяющие исключить возможность просмотра вводимой парольной информации.

Операционные системы серверов должны быть настроена таким образом, чтобы исключить возможность ознакомления с парольной информацией любого из пользователей, включая Администратора.

Серверы должны быть защищены паролем на загрузку операционной системы и доступа к конфигурации BIOS.

Компьютеры рабочих станций должны быть защищены паролем на доступ к конфигурации BIOS. Компьютеры рабочих станций, на которых хранятся конфиденциальные сведения, должны быть защищены паролем на загрузку операционной системы.

Операционные системы рабочих станций должны быть настроены таким образом, чтобы блокировать паузы неактивности (хранитель экрана) с функцией парольной защиты. Время включения защиты не более 10 минут.

Операционные системы серверов должны блокировать вход в сеть после 3-х кратной ошибки в наборе пароля.

Настройка активного сетевого оборудования Организации (маршрутизаторы, коммутаторы) не должна давать возможности несанкционированной переконфигурации, в связи с чем каждое активное сетевое устройство должно быть защищено уникальным паролем Администратора компьютерной сети.

При уходе сотрудника Организации в отпуск системный администратор, на основании заявки руководителя структурного

подразделения, производит блокировку имени пользователя в информационной системе Организации.

При увольнении сотрудника из Организации системный администратор, на основании обходного листа, производит удаление пользовательского имени в информационной системе Организации.

Период действия паролей составляет 90 суток, после чего они подлежат замене на новые, ранее не применявшиеся.

Администраторам различных информационных систем запрещается использование административного пароля при повседневной деятельности, не связанной с административными функциями. Для этой цели Администраторам должен выделяться пароль с правами пользователя.

Пароли Администраторов и пароли BIOS серверов должны храниться в опечатанных конвертах в сейфе начальника (директора) организации. Каждый пароль хранится в отдельном конверте.

Доступ в компьютерную сеть Организации через общедоступные каналы связи обеспечивается только с применением смарт-карт либо их полнофункциональных аналогов USB брелков eToken.

Любые некорректные действия сотрудников, связанные с доступом в компьютерную сеть, рассматриваются как нарушения режима информационной безопасности и анализируются через процедуру служебного расследования.

Ответственным за настройку серверов и рабочих станций, в соответствии с требованиями настоящей Инструкции, является администратор компьютерной сети.

13. Антивирусная безопасность.

Под компьютерными вирусами, троянскими программами следует понимать программы, которые могут заражать другие программы, изменяя их посредством добавления своей, возможно модифицированной, копии, которая сохраняет способность к дальнейшему размножению (далее по тексту вредоносные программы).

Возможными путями проникновения вредоносных программ в компьютерную сеть Организации являются:

– через сеть интернет, путем загрузки пользователями зараженного программного обеспечения;

– загрузка WWW страниц с активными приложениями, содержащими вредоносный код;

– заражение рабочих станций пользователей через электронную почту;
– распространение вредоносных программ через сеть интернет и электронную почту посредством использования уязвимостей программного обеспечения;
– установка на рабочие станции и сервера Организации зараженного программного обеспечения или электронных документов;

Возможные последствия распространения вредоносных программ в компьютерной сети Организации:
– модификация, потеря данных;
– утечка информации из компьютерной сети Организации;
– нарушение технологических процессов в компьютерной сети Организации.

Выполнение всеми сотрудниками Организации мероприятий, направленных на предотвращение проникновения вредоносных программ в компьютерную сеть Организации, является основой нормального функционирования сети и одним из важнейших условий информационной безопасности.

Весь входящий и исходящий трафик компьютерной сети Организации должен проходить через условия фильтрации межсетевого экрана.

Входящий и исходящий трафик пользователей в сеть интернет должен подвергаться антивирусному контролю.

Все почтовые сервера (как внешние, так и внутренние) должны быть обязательно защищены антивирусным программным обеспечением. Антивирусное программное обеспечение на рабочих станциях и почтовых серверах должно быть от разных производителей, что повышает вероятность успешного обнаружения вредоносных программ на различных этапах.

Внешние почтовые сервера, межсетевой экран должны запрещать прохождение вложенных исполняемых файлов в компьютерную сеть Организации.

На всех серверах компьютерной сети Организации должно быть установлено антивирусное программное обеспечение. На файл-серверах должен быть включен режим проверки в реальном времени.

Все программное обеспечение, устанавливаемое на компьютерах Организации, должно предварительно проходить

антивирусную проверку на специально выделенном компьютере, не имеющем доступа в компьютерную сеть Организации.

На всех рабочих станциях пользователей должно быть установлено антивирусное программное обеспечение, работающее в режиме проверки в реальном времени.

Необходимо обеспечить обновление баз антивирусного программного обеспечения не реже одного раза в сутки.

Правила антивирусной защиты доводятся до всех пользователей компьютерной сети Организации под личную роспись в журнале инструктажа администратором сети.

При передаче программного обеспечения и электронных документов в другие организации или физическим лицам необходимо проводить антивирусный контроль передаваемой информации.

Все факты проникновения вредоносных программ в компьютерную сеть Организации являются нарушением информационной безопасности и подлежат служебному расследованию.

Контроль выполнения антивирусной безопасности пользователями компьютерной сети Организации возлагается на Информационно - технический отдел.

14. Резервное копирование.

Резервное копирование является средством защиты информации, хранящейся в электронном виде, от повреждения либо уничтожения в результате сбоев программного обеспечения, сбоев и неисправностей вычислительной техники, а также в результате физического повреждения (уничтожения) вычислительной техники.

Объектами резервного копирования являются:

– базы данных автоматизированных информационных систем Организации;

– программное обеспечение и данные, расположенные на файл-серверах;

– операционные системы серверов и настройки активного сетевого оборудования (маршрутизаторы, межсетевые экраны);

– критичное программное обеспечение и данные, расположенные на рабочих станциях пользователей.

Схема резервного копирования.

Базы данных автоматизированных информационных систем:

Зеркальные копии создаются на зеркальном жестком диске сервера в режиме реального времени;

Ежедневные копии создаются на съемных машинных носителях информации по окончании рабочего дня. Срок хранения копий одна неделя;

Ежемесячные копии создаются на съемных машинных носителях информации по состоянию на первый рабочий день следующего месяца. Срок хранения копий один год;

Ежеквартальные копии создаются на съемных машинных носителях информации по состоянию на первый рабочий день следующего квартала. Срок хранения копий три года;

Ежегодные копии создаются на съемных машинных носителях информации по состоянию на первый рабочий день следующего года. Срок хранения копий десять лет.

Программное обеспечение и данные, расположенные на файл-серверах:

Зеркальные копии создаются на зеркальном жестком диске сервера в режиме реального времени;

Ежедневные копии на съемных машинных носителях информации по окончании рабочего дня. Срок хранения копий одна неделя.

Операционные системы серверов и настройки активного сетевого оборудования

Резервные копии создаются после первоначальной настройки или внесения изменений в настройку операционных систем серверов, программного обеспечения серверов и сетевого оборудования на съемных машинных носителях, если нет возможности произвести копирование, производится распечатка конфигурационных файлов. Резервные копии хранятся до истечения их актуальности.

Критичное программное обеспечение и данные, расположенные на рабочих станциях пользователей.

Резервные копии создаются по мере необходимости (частота резервного копирования уточняется для каждой рабочей станции) на съемных машинных носителях. Резервные копии хранятся до истечения их актуальности (места хранения резервных копий уточняются для каждой рабочей станции).

Съемные носители информации с архивными копиями учитываются в Журнале учета архивных носителей и хранятся в сейфе начальника Службы безопасности.

Ответственными за проведение резервного копирования являются администраторы соответствующих систем.

15. Обеспечение режима конфиденциальности при проведении совещаний.

Служебные совещания, на которых будут обсуждаться конфиденциальные вопросы, проводятся по решению Генерального директора Организации, его заместителей или начальников структурных подразделений (только если совещание затрагивает вопросы безопасности одного структурного подразделения Организации). Для проведения таких совещаний, при необходимости, назначается ответственное лицо за подготовку и проведение совещания.

Лицо, ответственное за подготовку и проведение совещания, совместно с представителем службы безопасности и соответствующим техническим специалистом осуществляет необходимые организационные и технические мероприятия, обеспечивающие сохранение конфиденциальности обсуждаемых вопросов и исключающие утечку информации во время проведения совещания.

На совещания допускаются лица, имеющие непосредственное отношение к обсуждаемым на них вопросам и участие которых вызвано служебной необходимостью.

Совещания проводятся в помещениях, обеспечивающих сохранение конфиденциальности обсуждаемых вопросов безопасности. Такие помещения до проведения совещания должны быть защищены от технических средств разведки, обследованы соответствующими специалистами с целью обеспечения защиты от утечки информации по техническим каналам и при необходимости - обеспечены охраной.

Руководитель совещания перед его началом обязан проинформировать присутствующих о степени конфиденциальности обсуждаемых вопросов.

5. РАЗРУШАЮЩИЕ ПРОГРАММНЫЕ ВОЗДЕЙСТВИЯ И МЕТОДЫ БОРЬБЫ С НИМИ

5.1. Компьютерные вирусы: понятие, характерные черты и хронология развития

Компьютерные вирусы – одна из главных угроз информационной безопасности. Это связано с масштабностью распространения этого явления и, следовательно, колоссального ущерба, наносимого информационным системам.

Современный компьютерный вирус – это практически незаметный для обычного пользователя «враг», который постоянно совершенствуется, находя все новые и более изощренные способы проникновения на компьютеры пользователей. Необходимость борьбы с компьютерными вирусами обусловлена возможностью нарушения ими всех составляющих информационной безопасности.

Компьютерные вирусы были и остаются одной из наиболее распространенных причин потери информации. Вирусные эпидемии способны блокировать работу организаций, предприятий, а иногда и целых регионов.

В последнее время вирусные эпидемии стали настолько масштабными и угрожающими, что сообщения о них выходят на первое место в мировых новостях.

Термин «компьютерный вирус» появился в середине 80-х годов XX века, на одной из конференций по безопасности информации, проходившей в США.

Трудность, возникающая при попытках сформулировать строгое определение вируса, заключается в том, что практически все отличительные черты вируса (внедрение в другие объекты, скрытность, потенциальная опасность и др.) либо присущи другим программам, которые никакого отношения не имеют к вирусам, либо существуют вирусы, которые не содержат указанных выше отличительных черт (за исключением возможности распространения).

Основная особенность компьютерных вирусов заключается в возможности их самопроизвольного внедрения в различные объекты операционной системы – присуща многим программам, которые не являются вирусами, но именно эта особенность является обязательным (необходимым) свойством компьютерного вируса. К

более полной характеристике современного компьютерного вируса следует добавить способность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети или файлы, системные области компьютера и прочие выполняемые объекты.

Приведем одно из общепринятых определений вируса, содержащееся в ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».

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

Невозможность четкой формулировки определения компьютерного вируса сама по себе не является проблемой. Главная проблема, которая следует из этого, заключается в том, что нет четких (однозначных) признаков, по которым можно отличить различные файлы от «вирусов», что не позволяет в полной мере устранить их влияние.

Несмотря на все усилия разработчиков антивирусного программного обеспечения до сегодняшнего дня нет достаточно надежных антивирусных средств, а значит, противостояние создателей вирусов и их оппонентов будет постоянным.

Хронология развития компьютерных вирусов [14]

Появление первых компьютерных вирусов, способных дописывать себя к файлам, связывают с инцидентом, который произошел в первой половине 70-х годов на системе Univax 1108. Вирус, получивший название «Pervading Animal», дописывал себя к выполняемым файлам, то есть делал практически то же самое, что тысячи современных компьютерных вирусов.

В то время из-за небольшого распространения компьютеров значимые события, связанные с компьютерными вирусами, происходили один раз в несколько лет. С началом 80-х компьютеры становятся все более и более популярными. Появляется все больше и больше программ, начинают развиваться глобальные сети. Результатом этого является появление большого числа разнообразных «троянских коней» – программ, которые при их

запуске наносят системе какой-либо вред. В 1986 г. произошла первая эпидемия IBM-PC вируса «Brain». Вирус, заражающий 360Кб дискеты, практически мгновенно разошелся по всему миру. Причиной такого «успеха» являлась неготовность компьютерного общества к встрече с таким явлением, как компьютерный вирус.

В 1987 г. произошло событие, которое популяризировало компьютерные вирусы. Код вируса «Vienna» впервые публикуется в книге Ральфа Бюргера «Computer Viruses: A High Tech Desease». Сразу же в 1987 г. появляются несколько вирусов для IBM-PC.

В пятницу 13-го мая 1988-го года сразу несколько фирм и университетов нескольких стран мира столкнулись с вирусом «Jerusalem» – в этот день вирус уничтожал файлы при их запуске. Вместе с несколькими другими вирусами, вирус «Jerusalem» распространился по тысячам компьютеров, оставаясь незамеченным – антивирусные программы еще не были распространены в то время так же широко как сегодня, а многие пользователи и даже профессионалы еще не верили в существование компьютерных вирусов. Не прошло и полгода, как в ноябре повальная эпидемия сетевого вируса Морриса (другое название – Internet Worm) заразила более 6000 компьютерных систем в США и практически парализовала их работу. По причине ошибки в коде вируса он неограниченно рассылал свои копии по другим компьютерам сети и, таким образом, полностью забрал под себя ее ресурсы. Общие убытки от вируса Морриса были оценены в 96 миллионов долларов.

В 1992 году появились первые конструкторы вирусов VCL и PS-MPC, которые увеличили и без того немаленький поток новых вирусов. В конце этого года первый вирус для Windows, заражающий выполняемые файлы этой операционной системы, открыл новую эру в жизни и распространении компьютерных вирусов.

В дальнейшем развитие компьютерных вирусов происходит стремительно и безостановочно. Создатели вирусов становятся все более изощренными, количество антивирусных программ растет, но ни одна из них не защищает в полной мере. В компьютерном обществе появляется синдром компьютерного вируса.

К борьбе с вирусами подключаются правоохранительные органы: летом 1994 года в Великобритании были арестованы автор вируса SMEG и группа вирусописателей, называвшая себя ARCV (Assotiation for Really Cruel Viruses). Некоторое время спустя еще один автор вирусов был арестован в Норвегии.

В августе 1995 г. произошло поворотное событие в истории вирусов и антивирусов: обнаружен первый вирус для Microsoft Word ("Concept"). Начиналось время макровирусов.

В 1998 году появились первые полиморфные Windows32-вирусы-"Win95. HPS" и "Win95. Marburg". Разработчикам антивирусных программ пришлось спешно адаптировать к новым условиям методики детектирования полиморфных вирусов, рассчитанных до того только на DOS-вирусы.

Наиболее заметной в 1998 г. была эпидемия вируса "Win95. CIH". Эпидемию сначала называли массовой, затем глобальной, а затем – повальной. Сообщения о заражении компьютерных сетей и домашних персональных компьютеров исчислялись тысячами. Начало эпидемии зарегистрировано на Тайване, где неизвестный заслал зараженные файлы в местные интернет-конференции.

С середины 90-х годов основным источником вирусов становится глобальная сеть интернет.

С 1999 года макровирусы начинают постепенно терять свое господство. Это связано со многими факторами. Во-первых, пользователи осознали опасность, таящуюся в простых doc- и xls-файлах. Люди стали более внимательными, научились пользоваться стандартными механизмами защиты от макровирусов, встроенными в MS Office.

В 2000 году происходят важные изменения в практике написания вирусов и, соответственно в мировой вирусной войне. Появляется новый тип вредоносных программных кодов – сетевые черви. В это же время появляется вирус «Чернобыль» – исполняемый вирус под Windows, имеющий следующие особенности.

Во-первых, зараженный файл не меняет своего размера по сравнению с первоначальным вариантом. Такой эффект достигается благодаря структуре исполняемых файлов Windows: каждый exe-файл разбит на секции, выровненные по строго определенным границам. В результате между секциями почти всегда образуется небольшой зазор. Хотя такая структура приводит к увеличению места, занимаемого файлом на диске, она же позволяет существенно повысить скорость работы операционной системы с таким файлом. «Чернобыль» либо записывает свое тело в один такой зазор, либо дробит свой код на кусочки и копирует каждый из них в пустое место между границами. В результате антивирусу сложнее определить,

заражен ли файл или нет, и еще сложнее вылечить инфицированный объект.

Во-вторых, «Чернобыль» стал первой программой, умеющей выводить из строя аппаратные средства. Некоторые микросхемы позволяют перезаписывать данные, хранящиеся в их мини ПЗУ. Этим и занимается этот вирус.

2000 год называют годом «Любовных Писем». Вирус «LoveLetter», обнаруженный 5 мая, мгновенно разлетелся по всему миру, поразив десятки миллионов компьютеров практически во всех уголках планеты. Причины этой глобальной эпидемии кроются в чрезвычайно высокой скорости распространения. Вирус рассылал свои копии немедленно после заражения системы по всем адресам электронной почты, найденным в адресной книге почтовой программы Microsoft Outlook. Подобно обнаруженному весной 1999 года вирусу Melissa, LoveLetter это делал, якобы, от имени владельца зараженного компьютера, о чем тот, естественно, даже не догадывался. Немаловажную роль при распространении вируса сыграл и психологический аспект: мало кто сможет удержаться, чтобы не прочитать любовное письмо от своего знакомого. Именно на это была сделана основная ставка в процессе разработки вируса. О масштабах заражения вирусами в самом конце XX века свидетельствует тот факт, что только в мае атаке вируса LoveLetter подверглись более 40 миллионов компьютеров. Уже за первые 5 дней эпидемии вирус нанес мировой экономике убытки в размере 6,7 миллиардов долларов.

С 2000 года сетевые черви начинают преобладать над вирусами других типов. Сегодня, по данным Лаборатории Касперского, на их долю приходится 89,1 % всех заражений. В структуре распространенности сетевых червей традиционно преобладают почтовые, использующие e-mail для доставки на компьютер-жертву.

В 2001 году был обнаружен новый тип вредоносных кодов, способных активно распространяться и работать на зараженных компьютерах без использования файлов – «бестелесные черви». В процессе работы такие вирусы существуют исключительно в системной памяти, а при передаче на другие компьютеры – в виде специальных пакетов данных.

Такой поворот событий поставил сложные задачи перед разработчиками антивирусных пакетов. Традиционные технологии (антивирусный сканер и монитор) проявили неспособность

эффективно противостоять новой угрозе, поскольку их алгоритм борьбы с вредоносными программами основан именно на перехвате файловых операций. Решением проблемы стал специальный антивирусный фильтр, который в фоновом режиме проверяет все поступающие на компьютер пакеты данных и удаляет «бестелесных» червей. Глобальная эпидемия сетевого червя CodeRed, начавшаяся 20 июля 2001 года, подтвердила действенность технологии «бестелесности».

5.2. Классификация компьютерных вирусов

Компьютерные вируса классифицируются по нескольким критериям. Наиболее часто упоминаются и используются классификации по среде «обитания», деструктивным действиям, особенностям алгоритма работы [14]. Структурная схема данных терминов показана на рис. 5.1.

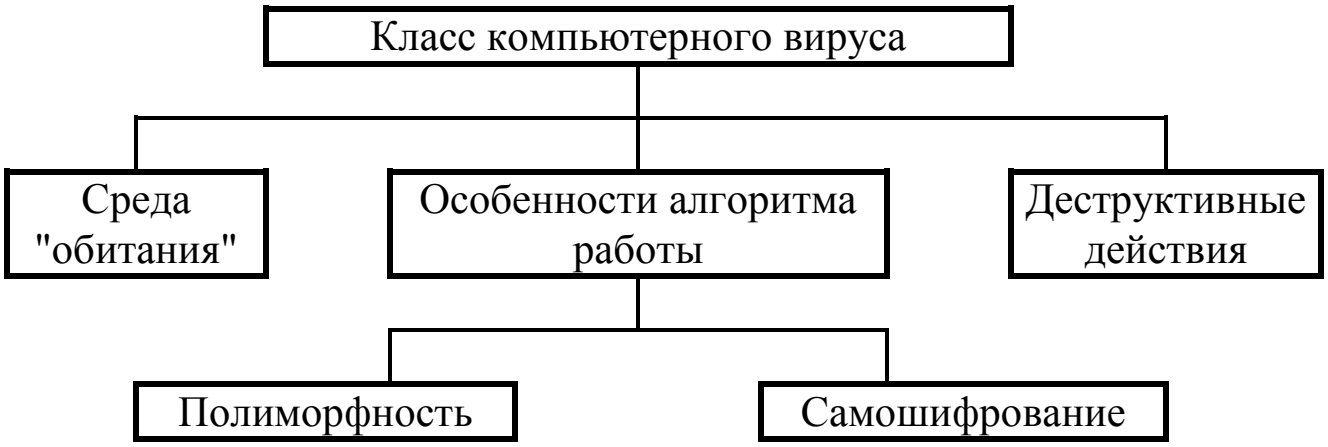

Рис. 5.1. Структурная схема классификации вирусов

По среде «обитания» вирусы делятся на:

- файловые;
- загрузочные;
- макровирусы;
- сетевые.

Файловые вирусы внедряются в выполняемые файлы (наиболее распространенный тип вирусов), либо создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (link-вирусы).

Загрузочные вирусы записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик жесткого диска (Master Boot Record), либо меняют указатель на активный boot-сектор.

Макровирусы заражают файлы-документы и электронные таблицы популярных офисных приложений.

Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

Существует большое количество сочетаний – например, файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные секторы дисков. Другой пример – сетевой макровирус, не только заражающий редактируемые документы, но и рассылающий свои копии по электронной почте.

Заражаемая операционная система является вторым уровнем деления вирусов на классы. Каждый файловый или сетевой вирус заражает файлы какой-либо одной или нескольких операционных систем – DOS, Windows, и т.д. Макровирусы заражают файлы форматов Word, Excel, пакета Office. Загрузочные вирусы также ориентированы на конкретные форматы расположения системных данных в загрузочных секторах дисков.

По особенностям алгоритма работы вирусы делятся на:

- резидентные;
- стелс-вирусы;
- полиморфик-вирусы;
- вирусы, использующие нестандартные приемы.

Резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки операционной системы. Нерезидентные вирусы не заражают память компьютера и сохраняют активность ограниченное время. К резидентным относятся макровирусы, поскольку они постоянно присутствуют в памяти компьютера все время работы зараженного редактора.

Использование *стелс-алгоритмов* позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным стелс-алгоритмом является перехват запросов операционной системы на чтение/запись зараженных объектов. Стелс-вирусы при этом либо

временно лечат их, либо подставляют вместо себя незараженные участки информации. В случае макровирусов наиболее популярный способ – запрет вызовов меню просмотра макросов.

Полиморфик-вирусы – это достаточно труднообнаружимые вирусы, не имеющие сигнатур, т.е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфик-вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

Самошифрование и *полиморфичность* используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру обнаружения вируса.

По деструктивным возможностям вирусы можно разделить на:

- безвредные, никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);
- неопасные, влияние которых ограничивается уменьшением свободной памяти на диске;
- опасные вирусы, которые могут привести к серьезным сбоям в работе компьютера;
- очень опасные, в алгоритм работы которых заведомо заложены процедуры, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера системную информацию, повредить аппаратные средства компьютера.

5.3. Характеристика «вирусоподобных» программ

Под вирусоподобной программой понимают программу, которая сама по себе не является вирусом, однако может использоваться для внедрения, скрытия или создания вируса.

Известны вирусоподобные программы следующих видов:

- «троянские» программы (логические бомбы);
- утилиты скрытого администрирования удаленных компьютеров;
- «intended»-вирусы;
- конструкторы вирусов;
- полиморфик-генераторы.

Рассмотрим названные классы вредоносных программ подробнее.

«Троянские» программы (логические бомбы)

К «троянским» программам относятся программы, наносящие какие-либо разрушительные действия при выполнении определенных заранее заданных условий, например, уничтожение информации на дисках при каждом запуске какой-либо программы или по определенному графику. Большинство «троянских» программ маскируются под какие-либо полезные программы, новые версии популярных утилит или дополнения к ним. Очень часто они рассылаются по электронным конференциям. По сравнению с вирусами «троянские» программы не получают широкого распространения по достаточно простым причинам – они либо уничтожают себя вместе с остальными данными на диске, либо демаскируют свое присутствие и уничтожаются пользователем, пострадавшим от них. К «троянским» программам также относятся так называемые «дропперы» вирусов – зараженные файлы, код которых подправлен таким образом, что антивирусы не определяют присутствие вируса в файле. Например, файл шифруется или упаковывается неизвестным архиватором, что не позволяет антивирусу опознать заражение.

Еще один тип «троянских» программ «злые шутки», которые сообщают о несуществующих опасностях, вынуждая пользователя к активным действиям. Например, к «злым шуткам» относятся программы, пугающие пользователя сообщениями о форматировании диска (хотя на самом деле форматирования не происходит), находят вирусы в незараженных файлах.

Утилиты скрытого администрирования

Утилиты скрытого администрирования являются разновидностью «логических бомб» (троянских программ), которые используются злоумышленниками для удаленного администрирования компьютеров в сети. По своей функциональности они во многом напоминают различные системы администрирования, разрабатываемые и распространяемые различными фирмами-производителями программных продуктов. Единственная особенность этих программ заставляет классифицировать их как вредные «троянские» программы: отсутствие предупреждения об инсталляции и запуске. При запуске такая программа устанавливает себя в систему и затем следит за ней, при этом пользователю не выдается никаких сообщений о действиях программы в системе. Чаще всего ссылка на такую программу отсутствует в списке

активных приложений. В результате пользователь может и не знать о ее присутствии в системе, в то время как его компьютер открыт для удаленного управления.

Внедренные в операционную систему утилиты скрытого управления позволяют делать с компьютером то, что в них заложил их создатель: отсылать файлы, выводить сообщения, стирать информацию, перезагружать компьютер и т.д.

«Intended»-вирусы

К таким вирусам относятся программы, которые, в отличие от обычных вирусов, не могут размножаться из-за ошибок, допущенных автором при их написании. Например, вирус, который при заражении неправильно устанавливает адрес перехватываемого прерывания (в большинстве приводит к "зависанию" компьютера). Появляются «intended»-вирусы чаще всего из-за неумелой перекомпиляции какого-либо уже существующего вируса, либо по причине недостаточного знания языка программирования, либо по причине незнания технических тонкостей операционной системы.

Конструкторы вирусов

К данному виду «вредоносных» программ относятся утилиты, предназначенные для изготовления новых компьютерных вирусов. Известны конструкторы вирусов для DOS, Windows и макровирусов. Они позволяют генерировать исходные тексты вирусов, объектные модули, или непосредственно зараженные файлы. Некоторые конструкторы снабжены стандартным оконным интерфейсом, где при помощи системы меню можно выбрать тип вируса, поражаемые объекты, наличие или отсутствие самошифровки, противодействие отладчику, внутренние текстовые строки, выбрать эффекты, сопровождающие работу вируса и т.п.

Полиморфные генераторы

Полиморфик-генераторы, как и конструкторы вирусов, не являются вирусами в прямом смысле этого слова, поскольку в их алгоритм не закладываются функции размножения. Главной задачей таких программ является шифрование тела вируса и генерация соответствующего расшифровщика. Обычно полиморфные генераторы распространяются в виде файла-архива. Основным файлом в архиве любого генератора является объектный модуль, содержащий этот генератор.

5.4. Антивирусные программы

Одним из наиболее эффективных способов борьбы с вирусами является использование антивирусного программного обеспечения. Антивирусная программа – программа, предназначенная для поиска, обнаружения, классификации и удаления компьютерного вируса и вирусоподобных программ.

Однако, нельзя забывать, что не существует антивирусов, гарантирующих стопроцентную защиту от вирусов, поскольку на любой алгоритм антивируса всегда можно предложить новый алгоритм вируса.

При работе с антивирусными программами встречаются некоторые понятия:

Ложное срабатывание – нахождение вируса в незараженном объекте (файле, секторе или системной памяти).

Пропуск вируса – необнаружение вируса в зараженном объекте.

Сканирование по запросу – поиск вирусов по запросу пользователя. В этом режиме антивирусная программа неактивна до тех пор, пока не будет вызвана пользователем из командной строки, командного файла или программы-расписания.

Сканирование на лету – постоянная проверка на вирусы объектов, к которым происходит обращение. В этом режиме антивирус постоянно активен, он присутствует в памяти «резидентно» и проверяет объекты без команд пользователя

Самыми популярными и эффективными антивирусными программами являются антивирусные сканеры, CRC-сканеры (ревизоры) [14]. Существуют также антивирусы блокировщики и иммунизаторы.

Сканеры.

Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются так называемые «маски». Маской вируса является некоторая постоянная последовательность кода, специфичная для этого конкретного вируса.

Во многих сканерах используются также алгоритмы «эвристического сканирования», т.е. анализ последовательности команд в проверяемом объекте, набор некоторой статистики и

принятие решения для каждого проверяемого объекта. Поскольку эвристическое сканирование является во многом вероятностным методом поиска вирусов, то на него распространяются многие законы теории вероятностей. Например, чем выше процент обнаруживаемых вирусов, тем больше количество ложных срабатываний.

Сканеры также можно разделить на две категории – «универсальные» и «специализированные». Универсальные сканеры рассчитаны на поиск и обезвреживание всех типов вирусов вне зависимости от операционной системы, на работу в которой рассчитан сканер. Специализированные сканеры предназначены для обезвреживания ограниченного числа вирусов или только одного их класса, например, макровирусов.

Сканеры также делятся на «резидентные» (мониторы), производящие сканирование «на лету», и «нерезидентные», обеспечивающие проверку системы только по запросу. Как правило, резидентные сканеры обеспечивают более надежную защиту системы, поскольку они немедленно реагируют на появление вируса, в то время как нерезидентный сканер способен опознать вирус только во время своего очередного запуска.

К достоинствам сканеров всех типов относится их универсальность, к недостаткам – размеры антивирусных баз, которые сканерам приходится хранить и пополнять, и относительно небольшая скорость поиска вирусов.

CRC-сканеры.

Принцип работы CRC-сканеров основан на подсчете CRC-сумм (контрольных сумм) для присутствующих на диске файлов или системных секторов. Эти CRC-суммы затем сохраняются в базе данных антивируса, как и некоторая другая информация: длины файлов, даты их последней модификации и т.д. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом.

CRC-сканеры, использующие «анти-стелс» алгоритмы, реагируют практически на 100% вирусов сразу после появления изменений на компьютере. Характерный недостаток этих антивирусов заключается в невозможности обнаружения вируса с момента его появления и до тех пор, пока не будут произведены

изменения на компьютере. CRC-сканеры не могут определить вирус в новых файлах (в электронной почте, на дискетах, в восстанавливаемых файлах или при распаковке файлов из архива), поскольку в их базах данных отсутствует информация об этих файлах.

Блокировщики.

Антивирусные блокировщики – это резидентные программы, перехватывающие «вирусоопасные» ситуации и сообщающие об этом пользователю. К «вирусоопасным» относятся вызовы на открытие для записи в выполняемые файлы, запись в загрузочный сектор диска и др., которые характерны для вирусов в моменты из размножения.

К достоинствам блокировщиков относится их способность обнаруживать и блокировать вирус на самой ранней стадии его размножения.

Иммунизаторы.

Иммунизаторы делятся на два типа: иммунизаторы, сообщающие о заражении, и иммунизаторы, блокирующие заражение каким-либо типом вируса.

Качество антивирусной программы определяется несколькими факторами. Перечислим их по степени важности:

– надежность и удобство работы – отсутствие «зависаний» антивируса и прочих технических проблем, требующих от пользователя специальной подготовки;

– качество обнаружения вирусов всех распространенных типов, сканирование внутри файлов-документов или таблиц, упакованных и архивированных файлов. отсутствие «ложных срабатываний». возможность лечения зараженных объектов;

– существование версий антивируса под все популярные платформы (dos, windows, linux и т.д.);

– возможность сканирования «на лету»;

– существование серверных версий с возможностью администрирования сети;

– скорость работы.

5.5. Профилактика компьютерных вирусов

Одним из методов борьбы с вирусами является своевременная профилактика. Компьютерная профилактика предполагает соблюдение правил компьютерной гигиены, позволяющих

значительно снизить вероятность заражения вирусом и потери каких-либо данных. Профилактика компьютерных вирусов начинается с выявления путей проникновения.

Рассмотрим основные пути проникновения вирусов в компьютеры пользователей [14, 18]:

- глобальные сети – электронная почта;
- электронные конференции, файл-серверы ftp;
- локальные сети;
- персональные компьютеры «общего пользования»
- пиратское программное обеспечение;
- сервисные службы;

Глобальные сети – электронная почта.

Основным источником вирусов на сегодняшний день является глобальная сеть интернет. По статистике, наибольшее число заражений вирусом происходит при обмене электронными письмами через почтовые серверы e-mail. Пользователь получает электронное письмо с вирусом, который активизируется (как правило, незаметно для пользователя) после просмотра файла-вложения электронного письма.

Локальные сети

Другой путь быстрого заражения – локальные сети. Если не принимать необходимых мер защиты, то зараженная рабочая станция при входе в сеть заражает один или несколько служебных файлов на сервере. Далее пользователи при очередном подключении к сети запускают зараженные файлы с сервера, и вирус получает доступ на компьютеры пользователей.

Персональные компьютеры «общего пользования»

Опасность представляют также компьютеры, установленные в организациях и учебных заведениях, на которых поочередно работают разные люди. Если, например, один из студентов принес на своем флэш-накопителе вирус и заразил какой-либо учебный компьютер, то очередной вирус будет гулять по всему учебному заведению, включая домашние компьютеры студентов и сотрудников.

Пиратское программное обеспечение

Нелегальные копии программного обеспечения являются одной из основных "зон риска". Часто пиратские копии на DVD или CD содержат файлы, зараженные самыми вирусами. Следует помнить,

что низкая стоимость программы может дорого обойтись при потере данных.

Сервисные службы

Достаточно редко, но до сих пор вполне реально заражение компьютера вирусом при его ремонте или профилактическом осмотре в сервисных центрах.

Учитывая возможные пути проникновения вирусов, приведем основные **правила защиты от вирусов.**

1. Перед тем, как запустить файл на выполнение или открыть документ, обязательно следует проверить его на наличие вирусов;
2. Использовать антивирусы для проверки «на лету» всех файлов, загружаемых по сети;
3. Для уменьшения риска заразить файл на сервере администраторам сетей следует использовать стандартные возможности защиты сети, например, ограничение прав пользователей; установку атрибута «только для чтения» и т.д;
4. Регулярно проверять компьютер антивирусными программами (по возможности – не того производителя, чей резидентный сторож установлен на компьютере);
5. Целесообразно запускать для проверки новое программное обеспечение на тестовом компьютере, не подключенном к общей сети или на виртуальной машине;
6. Использовать лицензионное программное обеспечение, приобретенное у официальных продавцов;
7. Дистрибутивы копий программного обеспечения (в том числе – операционной системы) необходимо хранить на защищенных от записи дисках;
8. Пользоваться только хорошо зарекомендовавшими себя источниками программ и прочих файлов;
9. Постоянно обновлять вирусные базы используемого антивируса;
10. Стараться не запускать непроверенные файлы, в том числе полученные из компьютерной сети. Перед запуском новых программ обязательно проверьте их антивирусом;
11. Ограничить круг лиц, допущенных к работе на конкретном компьютере;
12. Пользоваться утилитами проверки целостности информации;
13. Периодически сохранять на внешнем носителе файлы, с которыми ведется работа;

14. При работе с Word или Excel включать защиту от макросов, которая сообщает о присутствии макроса в открываемом документе и предоставляет возможность запретить этот макрос.

6. АДАПТИВНЫЙ ПОДХОД К УПРАВЛЕНИЮ БЕЗОПАСНОСТЬЮ

Под атакой на информационную систему понимают любое действие, выполняемое нарушителем для реализации угрозы путем использования уязвимостей ИС.

Архитектура любой ИС включает в себя четыре уровня.

1. Уровень прикладного программного обеспечения, отвечающий за взаимодействие с пользователем;
2. Уровень системы управления базами данных, отвечающий за хранение и обработку данных ИС;
3. Уровень операционной системы, отвечающий за обслуживание СУБД и прикладного ПО;
4. Уровень сети, отвечающий за взаимодействие узлов ИС.

С целью нарушения безопасности ИС злоумышленник может использовать широкий спектр возможностей на всех четырех уровнях. Например, для получения несанкционированного доступа к информации в СУБД MS SQL Server злоумышленник может [11]:

– перехватить передаваемые по сети данные (уровень сети);
– прочитать файлы БД, обращаясь непосредственно к файловой системе (уровень ОС);
– прочитать нужные данные средствами самой СУБД (уровень СУБД);
– прочитать записи БД при помощи SQL-запросов через программу MS Query, которая позволяет получать доступ к записям СУБД (уровень прикладного ПО).

Рассмотрим этапы осуществления атаки на КИС [13].

Первый, подготовительный, этап заключается в поиске злоумышленником предпосылок для осуществления атаки. На этом этапе злоумышленник ищет уязвимости в системе. На втором, основном этапе – реализации атаки – осуществляется использование найденных уязвимостей. На третьем, заключительном, этапе злоумышленник завершает атаку и старается скрыть следы вторжения. Нельзя забывать, что первый и третий этапы также могут являться атаками. Например, поиск злоумышленником уязвимостей при помощи сканеров безопасности считается атакой.

Большинство существующих механизмов защиты, реализованных в межсетевых экранах, системах разграничения

доступа и т.д. работают только на этапе реализации атаки, то есть защищают от атак, которые находятся уже в стадии осуществления. Комплексная система обеспечения информационной безопасности должна эффективно работать на всех трех этапах осуществления атаки. Наиболее эффективным было бы предупреждение атак путем предотвращения предпосылок вторжения.

Общее снижение уровня защищенности ИС обычно обусловлено несколькими причинами. Во-первых, зачастую не учитывается, что системные администраторы, а иногда и сами пользователи изменяют конфигурацию ИС, в результате чего могут появляться новые уязвимости. Во-вторых, при быстро изменяющихся информационных и сетевых технологиях, появляющемся на рынке новом ПО с одной стороны и отсутствие постоянно проводимого анализа их безопасности и нехватке ресурсов для обеспечения защиты с другой, приводит к тому, что со временем защищенность ИС падает, так как появляются новые неучтенные угрозы и уязвимости системы. И, наконец, в-третьих, администраторы безопасности обычно реагируют только на те риски безопасности, которые им понятны, что может составлять лишь небольшую часть всех рисков, которых может быть существенно больше.

Адаптивный подход к безопасности позволяет контролировать, обнаруживать и реагировать в реальном режиме времени на риски безопасности, используя правильно спроектированные и хорошо управляемые процессы и средства.

Адаптивная безопасность сети включает три основных элемента:

- технологии анализа защищенности;
- технологии обнаружения атак;
- технологии управления рисками.

Оценка риска заключается в выявлении и упорядочивании уязвимостей (по степени серьезности ущерба возможных воздействий), подсистем сети (по степени критичности), угроз (по вероятности их реализации) и т.д. А учитывая постоянные изменения конфигурации сети, процесс оценки риска должен проводиться постоянно. Именно с оценки рисков должно начинаться построение системы защиты ИС.

Анализ защищенности – это поиск уязвимых мест в сети. Сеть состоит из соединений, узлов, хостов, рабочих станций, приложений и БД. Технологии анализа защищенности исследуют сеть, ищут «слабые» места в ней, обобщают эти сведения и выдают

соответствующий отчет. Если система анализа защищенности содержит адаптивный компонент, то устранение найденной уязвимости будет осуществляться автоматически, а не вручную. Технология анализа защищенности позволяет выявить в сети большое число разнообразных проблем:

- «люки» в системах и программы типа «троянский конь»;
- слабые пароли;
- восприимчивость к проникновению из незащищенных систем;
- восприимчивость к атакам типа «отказ в обслуживании»;
- отсутствие необходимых обновлений ОС;
- неправильная настройка элементов ИС и другие.

Обнаружение атак является процессом оценки подозрительных действий, которые происходят в сети, реализующимся путем анализа или журналов регистрации ОС и приложений, или сетевого трафика в реальном времени. Компоненты обнаружения атак, размещенные на узлах или сегментах сети, оценивают различные события и действия, в том числе и действия, использующие известные уязвимости.

Адаптивная составляющая системы адаптивного управления безопасностью отвечает за модификацию процесса анализа защищенности, предоставляя ему самую последнюю информацию о новых уязвимостях. Он также модифицирует составляющую обнаружения атак, дополняя ее последней информацией об атаках. Так, например, в соответствии с принципом адаптивного компонента действует механизм обновления БД антивирусных программ для обнаружения новых вирусов.

Адаптация данных может заключаться в различных формах реагирования, например:

- отправление уведомлений системам сетевого управления или администратору;
- автоматическое завершение сессии с атакующим узлом или пользователем;
- изменение конфигурации межсетевого экрана, маршрутизатора или других сетевых устройств;
- выработка рекомендаций администратору, позволяющих своевременно устранить обнаруженные уязвимости в сетях, приложениях или иных компонентах ИС.

Использование модели адаптивной безопасности сети позволяет контролировать большинство угроз и своевременно, и эффективно на

них реагировать с тем, чтобы не только устранить уязвимости, которые могут привести к реализации угрозы, но и проанализировать условия, способствовавшие появлению уязвимостей. Также модель позволяет уменьшить злоупотребления в сети, повысить осведомленность пользователей, администраторов и руководства о событиях безопасности в сети.

Модель адаптивной безопасности не исключает использование уже используемых механизмов защиты, таких как разграничение доступа, аутентификация и т.д., а расширяет их функциональность за счет дополнения компонентами, отвечающими за анализ защищенности, обнаружение атак и управление рисками.

7. ТЕХНОЛОГИЯ АНАЛИЗА ЗАЩИЩЕННОСТИ

Проблема защищенности информационной системы от угроз безопасности информации неизбежно встает перед руководством организации, сотрудниками службы безопасности и специалистами IT-подразделений. Соответствуют ли используемые инструменты безопасности существующим рискам и можно ли с помощью этой АС обрабатывать информацию ограниченного распространения? Имеются ли в текущей конфигурации АС ошибки, позволяющие злоумышленникам обойти механизмы контроля и защиты? На эти и многие другие вопросы следует дать ответ, прежде чем запустить ИС в эксплуатацию. Стоят эти вопросы и в период работы ИС.

Анализ защищенности АС от угроз безопасности информации – работа сложная. Умение оценивать и управлять рисками, знание типовых угроз и уязвимостей, критериев и подходов к анализу защищенности, владение методами анализа и специализированным инструментарием, знание различных программно-аппаратных платформ, используемых в современных компьютерных сетях, представление о принципах работы разноплановых средств защиты – вот далеко не полный перечень профессиональных качеств, которыми должны обладать специалисты, проводящие работы по анализу защищенности АС [10].

Анализ защищенности автоматической системы обработки информации является основным элементом таких взаимно пересекающихся видов работ, как аттестация, аудит и обследование безопасности АС.

Для проведения анализа защищенности АС требуется учитывать обобщенный существующий опыт проведения работ в этом направлении, требования стандартов в этой области, а также методы анализа и используемый программный инструментарий.

7.1. Понятие защищенности АС

Защищенность является одним из важнейших показателей эффективности функционирования АС, наряду с такими показателями, как надежность, отказоустойчивость, производительность и т.п.

Под защищенностью АС понимают степень соответствия реализованных в ней механизмов защиты информации,

существующим в данной среде функционирования рискам, связанным с осуществлением угроз безопасности информации.

Под угрозами безопасности информации традиционно понимается возможность нарушения таких свойств информации, как конфиденциальность, целостность и доступность.

Количество возможных путей осуществления угроз безопасности в отношении ресурсов АС не поддается точной оценке [11]. В идеале каждый путь осуществления угрозы должен быть перекрыт соответствующим механизмом защиты. Данное условие является первым фактором, определяющим защищенность АС. Вторым фактором является надежность существующих механизмов защиты, характеризующаяся степенью сопротивляемости этих механизмов попыткам их обхода либо преодоления. Третьим фактором является величина ущерба, который может быть нанесен владельцу АС в случае успешного преодоления используемых мер защиты и осуществления угроз безопасности.

На практике получение точных значений приведенных характеристик затруднено, поскольку понятия угрозы, ущерба и сопротивляемости механизма защиты трудно формализуемы. Например, оценку ущерба в результате НСД к информации, составляющей государственную тайну, политического и военного характера точно определить вообще невозможно, а определение вероятности осуществления угрозы не может базироваться на статистическом анализе. Оценка степени сопротивляемости механизмов защиты всегда является субъективной.

7.2. Нормативная база анализа защищенности

Наиболее значимыми нормативными документами в области информационной безопасности, определяющими критерии для оценки защищенности АС, и требования, предъявляемые к механизмам защиты, являются [1, 10, 21]:

1. Общие критерии оценки безопасности информационных технологий (The Common Criteria for Information Technology Security Evaluation/ISO 15408).
2. Практические правила управления информационной безопасностью (Code of practice for Information Security Management/ISO 17799).

Кроме этого, в нашей стране первостепенное значение имеют руководящие документы (РД) Федеральной службы по техническому и экспортному контролю (ранее – Гостехкомиссия) России.

Наиболее полно критерии для оценки механизмов безопасности программно-технического уровня представлены в международном стандарте ISO 15408: Common Criteria for Information Technology Security Evaluation (Общие критерии оценки безопасности информационных технологий), принятом в 1999 году.

Общие критерии оценки безопасности информационных технологий (далее – общие критерии) определяют функциональные требования безопасности и требования к адекватности реализации функций безопасности.

При проведении работ по анализу защищенности АС, а также средств вычислительной техники общие критерии целесообразно использовать в качестве основных критериев, позволяющих оценить уровень защищенности АС с точки зрения полноты реализованных в ней функций безопасности и надежности реализации этих функций.

Хотя применимость общих критериев ограничивается механизмами безопасности программно-технического уровня, в них содержится определенный набор требований к механизмам безопасности организационного уровня и требований по физической защите, которые непосредственно связаны с описываемыми функциями безопасности.

Первая часть общих критериев содержит определение общих понятий, концепции, описание модели и методики проведения оценки безопасности ИТ. В ней вводится понятийный аппарат, и определяются принципы формализации предметной области.

Требования к функциональности средств защиты приводятся во второй части общих критериев и могут быть непосредственно использованы при анализе защищенности для оценки полноты реализованных в АС функций безопасности.

Третья часть общих критериев содержит классы требований гарантированности оценки, включая класс требований по анализу уязвимостей средств и механизмов защиты под названием AVA: Vulnerability Assessment. Данный класс требований определяет методы, которые должны использоваться для предупреждения, выявления и ликвидации следующих типов уязвимостей:

– наличие побочных каналов утечки информации;

– ошибки в конфигурации либо неправильное использование системы, приводящее к переходу в небезопасное состояние;
– недостаточная надежность (стойкость) механизмов безопасности, реализующих соответствующие функции безопасности;
– наличие уязвимостей в средствах защиты информации, дающих возможность пользователям получать несанкционированный доступ к информации в обход существующих механизмов защиты.

Соответствующие требования гарантированности оценки содержатся в следующих четырех семействах требований:

– анализ каналов утечки информации;
– ошибки в конфигурации либо неправильное использование системы, приводящее к переходу системы в небезопасное состояние;
– стойкость функций безопасности, обеспечиваемая их реализацией;
– анализ уязвимостей.

При проведении работ по аудиту безопасности, перечисленные семейства требований могут использоваться в качестве руководства и критериев для анализа уязвимостей АС.

Наиболее полно критерии для оценки механизмов безопасности организационного уровня представлены в международном стандарте ISO 17799: Code of Practice for Information Security Management (Практические правила управления информационной безопасностью), принятом в 2000 году. При этом, ISO 17799 является международной версией британского стандарта BS 7799.

ISO 17799 содержит практические правила по управлению информационной безопасностью и может использоваться в качестве критериев для оценки механизмов безопасности организационного уровня, включая административные, процедурные и физические меры защиты.

Практические правила разбиты на следующие 10 разделов:

1. Политика безопасности;
2. Организация защиты;
3. Классификация ресурсов и их контроль;
4. Безопасность персонала;
5. Физическая безопасность;
6. Администрирование компьютерных систем и вычислительных сетей;
7. Управление доступом;

8. Разработка и сопровождение информационных систем;
9. Планирование бесперебойной работы организации;
10. Контроль выполнения требований политики безопасности.

В этих разделах содержится описание механизмов безопасности организационного уровня, реализуемых в настоящее время в правительственных и коммерческих организациях во многих странах мира.

Десять средств контроля, предлагаемых в ISO 17799, считаются особенно важными (ключевыми). Под средствами контроля здесь понимаются механизмы управления информационной безопасностью организации.

При использовании некоторых из средств контроля, например, шифрования данных, может потребоваться оценка рисков, чтобы определить, нужны ли они и каким образом их следует реализовывать. Для обеспечения более высокого уровня защиты особенно ценных ресурсов или оказания противодействия особенно серьезным угрозам безопасности в ряде случаев могут потребоваться более сильные средства контроля, которые выходят за рамки ISO 17799.

Десять ключевых средств контроля представляют собой либо обязательные требования, либо считаются основными структурными элементами информационной безопасности. Эти средства контроля актуальны для всех организаций и сред функционирования АС и составляют основу системы управления информационной безопасностью. Они служат в качестве основного руководства для организаций, приступающих к созданию и реализации средств управления информационной безопасностью.

Ключевыми являются следующие средства контроля:

1. Документ о политике информационной безопасности;
2. Распределение обязанностей по обеспечению информационной безопасности;
3. Обучение и подготовка персонала к поддержанию режима информационной безопасности;
4. Уведомление о случаях нарушения защиты;
5. Средства защиты от вирусов;
6. Планирование бесперебойной работы организации;
7. Контроль над копированием программного обеспечения, защищенного законом об авторском праве;
8. Защита документации организации;

9. Защита данных;
10. Контроль соответствия политике безопасности.

Процедура аудита безопасности АС включает в себя проверку наличия перечисленных ключевых средств контроля, оценку полноты и правильности их реализации, а также анализ их адекватности рискам, существующим в данной среде функционирования. Составной частью работ по аудиту безопасности АС также является анализ и управление рисками.

В нашей стране при решении задач защиты информации должно обеспечиваться соблюдение следующих Руководящих документов Гостехкомиссии (ФСТЭК) России и других нормативных документов:

– Руководящий документ «Положение по аттестации объектов информатизации по требованиям безопасности информации» (1994 г.);
– Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация АС и требования к защите информации» (1997);
– Руководящий документ «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации» (1992 г.);
– Руководящий документ «Концепция защиты средств вычислительной техники от НСД к информации» (1992 г.);
– Руководящий документ «Защита от НСД к информации. Термины и определения» (1992 г.);
– Руководящий документ «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в АС и СВТ» (1992 г.);
– Руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации» (1997 г.);
– Руководящий документ «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (1999 г.);
– Руководящий документ «Специальные требования и рекомендации по технической защите конфиденциальной информации» (2001г.).

РД Гостехкомиссии России составляют основу нормативной базы в области защиты от НСД к информации в нашей стране. Рассмотрим наиболее значимые из них, определяющие критерии для оценки защищенности АС.

Критерии для оценки механизмов защиты программно-технического уровня, используемые при анализе защищенности АС и СВТ, выражены в РД Гостехкомиссии РФ «АС. Защита от НСД к информации. Классификация АС и требования по защите информации» и «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации».

РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» устанавливает классификацию СВТ по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований. Устанавливается семь классов защищенности СВТ от НСД к информации. Самый низкий класс седьмой, самый высокий – первый. Классы подразделяются на четыре группы, отличающиеся уровнем защиты:

– первая группа содержит только один седьмой класс, к которому относят все СВТ, не удовлетворяющие требованиям более высоких классов;

– вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;

– третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;

– четвертая группа характеризуется верифицированной защитой и содержит только первый класс.

РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов. К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

– наличие в АС информации различного уровня конфиденциальности;

– уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
– режим обработки данных в АС – коллективный или индивидуальный.

Устанавливается девять классов защищенности АС от НСД к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности и конфиденциальности информации и, следовательно, иерархия классов защищенности АС.

При анализе системы защиты внешнего периметра сети в качестве основных критериев целесообразно использовать РД «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». Данный документ определяет показатели защищенности межсетевых экранов (МЭ). Каждый показатель защищенности представляет собой набор требований безопасности, характеризующих определенную область функционирования МЭ. Всего выделяется пять показателей защищенности:

1. Управление доступом;
2. Идентификация и аутентификация;
3. Регистрация событий и оповещение;
4. Контроль целостности;
5. Восстановление работоспособности.

На основании показателей защищенности определяются следующие пять классов защищенности МЭ:

1. Простейшие фильтрующие маршрутизаторы – 5 класс;
2. Пакетные фильтры сетевого уровня – 4 класс;
3. Простейшие МЭ прикладного уровня – 3 класс;
4. МЭ базового уровня – 2 класс;
5. Продвинутые МЭ – 1 класс.

МЭ первого класса защищенности могут использоваться в АС класса 1А, обрабатывающих информацию особой важности. Второму классу защищенности МЭ соответствует класс защищенности АС 1Б, предназначенный для обработки совершенно секретной информации и т.п.

7.3. Методика анализа защищенности

В конкретных ситуациях алгоритмы действий аудиторов могут существенно различаться. Однако существует типовая методика анализа защищенности корпоративной сети, эффективность которой многократно проверена на практике.

Типовая методика предполагает использование следующих методов [1]:

– изучение исходных данных по АС;

– оценка рисков, связанных с осуществлением угроз безопасности в отношении ресурсов АС;

– анализ механизмов безопасности организационного уровня, политики безопасности организации и организационно-распорядительной документации по обеспечению режима информационной безопасности и оценка их соответствия требованиям существующих нормативных документов, а также их адекватности существующим рискам;

– ручной анализ конфигурационных файлов маршрутизаторов, МЭ и прокси-серверов, осуществляющих управление межсетевыми взаимодействиями, почтовых и DNS серверов, а также других критических элементов сетевой инфраструктуры;

– сканирование внешних сетевых адресов ЛВС из сети интернет;

– сканирование ресурсов ЛВС изнутри;

– анализ конфигурации серверов и рабочих станций ЛВС при помощи специализированных программных средств.

Перечисленные методы исследования предполагают использование как активного, так и пассивного тестирования системы защиты [10]. Активное тестирование системы защиты заключается в эмуляции действий потенциального злоумышленника по преодолению механизмов защиты. Пассивное тестирование предполагает анализ конфигурации ОС и приложений по шаблонам с использованием списков проверки. Тестирование может производиться вручную либо с использованием специализированных программных средств.

7.4. Исходные данные по обследуемой АС

В соответствии с требованиями РД Гостехкомиссии при проведении работ по аттестации безопасности АС, включающих в

себя предварительное обследование и анализ защищенности объекта информатизации, заказчиком работ должны быть предоставлены следующие исходные данные [7]:

1. Полное и точное наименование объекта информатизации и его назначение;
2. Характер (научно-техническая, экономическая, производственная, финансовая, военная, политическая) информации и уровень секретности (конфиденциальности) обрабатываемой информации определен (в соответствии с какими перечнями (государственным, отраслевым, ведомственным, предприятия);
3. Организационная структура объекта информатизации;
4. Перечень помещений, состав комплекса технических средств (основных и вспомогательных), входящих в объект информатизации, в которых (на которых) обрабатывается указанная информация;
5. Особенности и схема расположения объекта информатизации с указанием границ контролируемой зоны;
6. Структура программного обеспечения (общесистемного и прикладного), используемого на аттестуемом объекте информатизации и предназначенного для обработки защищаемой информации, используемые протоколы обмена информацией;
7. Общая функциональная схема объекта информатизации, включая схему информационных потоков и режимы обработки защищаемой информации;
8. Наличие и характер взаимодействия с другими объектами информатизации;
9. Состав и структура системы защиты информации на аттестуемом объекте информатизации;
10. Перечень технических и программных средств в защищенном исполнении, средств защиты и контроля, используемых на аттестуемом объекте информатизации и имеющих соответствующий сертификат, предписание на эксплуатацию;
11. Сведения о разработчиках системы защиты информации, наличие у сторонних разработчиков (по отношению к предприятию, на котором расположен аттестуемый объект информатизации) лицензий на проведение подобных работ;
12. Наличие на объекте информатизации (на предприятии, на котором расположен объект информатизации) службы безопасности информации, службы администратора (автоматизированной системы, сети, баз данных);

13. Наличие и основные характеристики физической защиты объекта информатизации (помещений, где обрабатывается защищаемая информация и хранятся информационные носители);
14. Наличие и готовность проектной и эксплуатационной документации на объект информатизации и другие исходные данные по аттестуемому объекту информатизации, влияющие на безопасность информации.

Однако, перечисленных исходных данных часто бывает недостаточно для выполнения работ по анализу защищенности АС, и приведенный в РД Гостехкомиссии список нуждается в расширении и конкретизации. Пункт 14 приведенного списка предполагает предоставление других исходных данных по объекту информатизации, влияющих на безопасность информации. Как раз эти "дополнительные" данные и являются наиболее значимыми для оценки текущего положения дел с обеспечением безопасности АС. Их список включает следующие виды документов:

Дополнительная документация:

1. Нормативно-распорядительная документация по проведению регламентных работ;
2. Нормативно-распорядительная документация по обеспечению политики безопасности;
3. Должностные инструкции для администраторов, инженеров технической поддержки, службы безопасности;
4. Процедуры и планы предотвращения и реагирования на попытки НСД к информационным ресурсам;
5. Схема топологии корпоративной сети с указанием IP-адресов и структурная схема;
6. Данные по структуре информационных ресурсов с указанием степени критичности или конфиденциальности каждого ресурса;
7. Размещение информационных ресурсов в корпоративной сети;
8. Схема организационной структуры пользователей;
9. Схема организационной структуры обслуживающих подразделений;
10. Схемы размещения линий передачи данных;
11. Схемы и характеристики систем электропитания и заземления объектов АС;
12. Данные по используемым системам сетевого управления и мониторинга.

Проектная документация:

1. Функциональные схемы;
2. Описание автоматизированных функций;
3. Описание основных технических решений.

Эксплуатационная документация: Руководства пользователей и администраторов используемых программных и технических средств защиты информации.

7.5. Анализ конфигурации и тестирование средств защиты АС

При анализе конфигурации средств защиты внешнего периметра ЛВС и управления межсетевыми взаимодействиями особое внимание обращается на следующие аспекты, определяемые их конфигурацией [7, 11,12]:

- настройка правил разграничения доступа (правил фильтрации сетевых пакетов) на межсетевых экранах и маршрутизаторах;
- используемые схемы и настройка параметров аутентификации;
- настройка параметров системы регистрации событий;
- использование механизмов, обеспечивающих сокрытие топологии защищаемой сети, включающих в себя трансляцию сетевых адресов, маскарадинг и другие методы;
- настройка механизмов оповещения об атаках и реагирования;
- наличие и работоспособность средств контроля целостности;
- версии используемого программного обеспечения.

Тестирование системы защиты АС проводится для проверки эффективности используемых в ней механизмов защиты, их устойчивости в отношении возможных атак, а также с целью поиска уязвимостей в защите. Традиционно используются два основных метода тестирования:

- тестирование по методу «черного ящика»;
- тестирование по методу «белого ящика».

Тестирование по методу «черного ящика» предполагает отсутствие у тестирующей стороны каких-либо специальных знаний о конфигурации и внутренней структуре объекта испытаний. При этом против объекта испытаний реализуются все известные типы атак, и проверяется устойчивость системы защиты в отношении этих атак. Используемые методы тестирования эмулируют действия потенциальных злоумышленников, пытающихся взломать систему защиты. Основным средством тестирования в данном случае

являются сетевые сканеры, располагающие базами данных известных уязвимостей.

Метод «белого ящика» предполагает составление программы тестирования на основании знаний о структуре и конфигурации объекта испытаний. В ходе тестирования проверяются наличие и работоспособность механизмов безопасности, соответствие состава и конфигурации системы защиты требованиям безопасности и существующим рисками. Выводы о наличие уязвимостей делаются на основании анализа конфигурации используемых средств защиты и системного ПО, а затем проверяются на практике. Основным инструментом анализа в данном случае являются программные агенты средств анализа защищенности системного уровня, рассматриваемые ниже.

7.6. Средства анализа защищенности и параметров защиты

Уровень защищенности компьютерных систем от угроз безопасности определяется многими факторами [10, 18]. При этом одним из определяющих факторов является адекватность конфигурации системного и прикладного ПО, средств защиты информации и активного сетевого оборудования существующим рискам. Перечисленные компоненты АС имеют множество параметров, значения которых оказывают влияние на защищенности системы, что делает их немашинный анализ трудновыполнимой задачей. Поэтому в современных АС для анализа конфигурационных параметров системного и прикладного ПО, технических средств и средств защиты информации зачастую используются специализированные программные средства.

Анализ параметров защиты осуществляется по шаблонам, содержащим списки параметров и их значений, которые должны быть установлены для обеспечения необходимого уровня защищенности. Различные шаблоны определяют конфигурации для различных программно-технических средств.

Относительно коммерческих корпоративных сетей, подключенных к сети интернет, можно говорить о некотором базовом уровне защищенности, который в большинстве случаев можно признать достаточным. Разработка шаблонов (спецификаций) для конфигурации наиболее распространенных системных программных

средств, позволяющих обеспечить базовый уровень защищенности, в настоящее время осуществляется представителями международного сообщества, в котором состоят организации и частные лица, профессионально занимающиеся вопросами информационной безопасности и аудита АС, под эгидой международной организации «Центр Безопасного Интернета».

Разработанные спецификации являются результатом обобщения мирового опыта обеспечения информационной безопасности.

Арсенал программных средств, используемых для анализа защищенности АС, достаточно широк.

Одним из методов автоматизации процессов анализа и контроля защищенности распределенных компьютерных систем является использование технологии интеллектуальных программных агентов. Система защиты строится на архитектуре консоль/менеджер/агент. На каждую из контролируемых систем устанавливается программный агент, который и выполняет соответствующие настройки программного обеспечения и проверяет их правильность, контролирует целостность файлов, своевременность установки пакетов программных коррекций, а также выполняет другие полезные задачи по контролю защищенности АС. Менеджеры являются центральными компонентами подобных систем. Они посылают управляющие команды всем агентам контролируемого ими домена и сохраняют все данные, полученные от агентов в центральной базе данных. Администратор управляет менеджерами при помощи графической консоли, позволяющей выбирать, настраивать и создавать политики безопасности, анализировать изменения состояния системы, осуществлять ранжирование уязвимостей и т.п. Все взаимодействия между агентами, менеджерами и управляющей консолью осуществляются по защищенному клиент-серверному протоколу.

Основным фактором, определяющим защищенность АС от угроз безопасности, является наличие в АС уязвимостей защиты.

Уязвимости защиты могут быть обусловлены как ошибками в конфигурации компонентов АС, так и другими причинами, в число которых входят ошибки и программные закладки в коде ПО, отсутствие механизмов безопасности, их неправильное использование, либо их неадекватность существующим рискам, а также уязвимости, обусловленные человеческим фактором. Наличие

уязвимостей в системе защиты АС, в конечном счете, приводит к успешному осуществлению атак, использующих эти уязвимости.

Для выявления уязвимостей и моделирования их использования злоумышленником применяются сетевые сканеры. Такие системы поиска уязвимостей используют два подхода для определения местонахождения уязвимостей защиты и генерации отчетов о них. Первый подход, «пассивное сканирование», осуществляет проверку настроек (установок) системы, таких как права доступа к файлам, наследование наиболее важных файлов, настройки маршрута (в сети) и т.д. Второй подход, «активное» сканирование [6, 7, 12], на самом деле использует эмулирующие действия потенциальных нарушителей. В основе работы сетевых сканеров лежит база данных, содержащая описание известных уязвимостей ОС, МЭ, маршрутизаторов и сетевых сервисов, а также алгоритмов осуществления попыток вторжения (сценариев атак).

Сетевые сканеры являются наиболее доступными и широко используемыми средствами анализа защищенности. Основной принцип их функционирования заключается в эмуляции действий потенциального злоумышленника по осуществлению сетевых атак. Поиск уязвимостей путем имитации возможных атак является одним из наиболее эффективных способов анализа защищенности АС, который дополняет результаты анализа конфигурации по шаблонам, выполняемый локально с использованием шаблонов (списков проверки). Сканер является необходимым инструментом в арсенале любого администратора либо аудитора безопасности АС.

Современные сканеры способны обнаруживать сотни уязвимостей сетевых ресурсов, предоставляющих те или иные виды сетевых сервисов, и реализуют множество различных сценариев сканирования.

Современный сетевой сканер выполняет четыре основные задачи:

– идентификацию доступных сетевых ресурсов;
– идентификацию доступных сетевых сервисов;
– идентификацию имеющихся уязвимостей сетевых сервисов;
– выдачу рекомендаций по устранению уязвимостей.

В функциональность сетевого сканера не входит выдача рекомендаций по использованию найденных уязвимостей для реализации атак на сетевые ресурсы. Возможности сканера по

анализу уязвимостей ограничены той информацией, которую могут предоставить ему доступные сетевые сервисы.

Для функционирования сетевого сканера необходим только один компьютер, имеющий сетевой доступ к анализируемым системам, поэтому в отличие от продуктов, построенных на технологии программных агентов, нет необходимости устанавливать в каждой анализируемой системе своего агента.

К недостаткам сетевых сканеров можно отнести большие временные затраты, необходимые для сканирования всех сетевых компьютеров из одной системы, и создание большой нагрузки на сеть. Кроме того, бывает трудно отличить сеанс сканирования от действительных попыток осуществления атак, поскольку сетевые сканеры также с успехом используют и злоумышленники.

В настоящее время существует большое количество сканеров, как универсальных, так и специализированных, предназначенных для выявления только определенного класса уязвимостей.

Таким образом, программные средства анализа защищенности условно можно разделить на два класса. Первый класс, к которому принадлежат сетевые сканеры, иногда называют средствами анализа защищенности сетевого уровня. Второй класс, к которому относятся все остальные рассмотренные здесь средства, иногда называют средствами анализа защищенности системного уровня. Данные классы средств имеют свои достоинства и недостатки, а на практике взаимно дополняют друг друга.

Системы анализа защищенности, построенные на интеллектуальных программных агентах, являются потенциально более мощным средством, чем сетевые сканеры. Однако, несмотря на все свои достоинства, использование программных агентов не может заменить сетевого сканирования, поэтому эти средства применяются совместно. Кроме того, сканеры являются более простым, доступным, дешевым и, зачастую, более эффективным средством анализа защищенности.

Обеспечение безопасности компьютерных систем заключается в определении множества возможных угроз, оценке величины связанных с ними рисков, выборе адекватных контрмер, реализации этих контрмер процедурными и программно-техническими средствами и контроле их осуществления. Последний вопрос является, пожалуй, одним из наиболее сложных. Реализация программно-технических мер защиты требует произведения настроек

большого количества параметров ОС, МЭ, СУБД, сетевых сервисов, прикладных программ и активного сетевого оборудования. Когда речь идет о защите отдельного сервера или рабочей станции, то задача хоть и является сложной, но ее решение вполне по силам опытному системному администратору. В этом случае для контроля значений параметров программ, связанных с безопасностью, используются специальные списки проверки. Когда же речь заходит о настройке десятков и сотен сетевых устройств, функционирующих на различных программно-аппаратных платформах, в соответствии с единой политикой безопасности, контроле параметров защиты и мониторинге безопасности в реальном масштабе времени, то без специальных средств автоматизации уже не обойтись. Производители ОС предоставляют специальный инструментарий для контроля целостности и анализа защищенности ОС. Имеется немало свободно распространяемых и широко используемых продуктов, предназначенных для решения подобных задач. Однако эти средства, функционирующие на системном уровне, позволяют обеспечить только некоторый базовый уровень защищенности самой ОС. Для контроля приложений, сетевых сервисов, активного сетевого оборудования в распределенных системах, функционирующих в динамичной агрессивной среде, необходимо использовать специализированный инструментарий, поддерживающий распределенные архитектуры, централизованное управление, различные программно-аппаратные платформы, различные виды приложений, использующий изощренные алгоритмы поиска и устранения уязвимостей, интегрированный с другими средствами защиты и удовлетворяющий многим другим требованиями, предъявляемым к современным продуктам этого класса.

8. МЕТОДИКА ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК

8.1. Классификация компьютерных атак

Эффективную защиту от возможных и потенциально возможных сетевых атак невозможно осуществить без их подробной классификации, которая позволила бы систематизировать и облегчить решение задач по выявлению атак и противодействия им. В настоящее время известно большое количество различных типов классификационных признаков. Сетевые атаки могут быть подразделены на пассивные и активные, внешние и внутренние, умышленные и неумышленные и т.д.

Сначала рассмотрим классификацию, предложенную Питером Меллом в работе «Компьютерные атаки: что это и как им противостоять». В соответствии с этой классификацией все возможные сетевые атаки делятся на следующие типы [6, 43]:

– удаленное проникновение – это тип атак, которые позволяют реализовать удаленное управление компьютером через сеть (например, атаки с использованием программ NetBus или BackOrifice);

– локальное проникновение – это тип атак, которые приводят к получению несанкционированного доступа к узлу, на который они направлены (например, атака с использованием программы GetAdmin);

– удаленный отказ в обслуживании – тип атак, которые позволяют нарушить функционирование системы в рамках глобальной сети (например, атака Teardrop);

– локальный отказ в обслуживании – тип атак, позволяющих нарушить функционирование системы в рамках локальной сети (например, – внедрение и запуск враждебной программы, которая загружает центральный процессор бесконечным циклом, что приводит к невозможности обработки запросов других приложений);

– атаки с использованием сетевых сканеров – это тип атак, основанных на использовании сетевых сканеров – программ, которые анализируют топологию сети и обнаруживают сервисы, доступные для атаки (например, – атака с использованием утилиты nmap);

– атаки с использованием сканеров уязвимостей – тип атак, основанных на использовании сканеров уязвимостей – программ, осуществляющих поиск уязвимостей на узлах сети, которые в

дальнейшем могут быть применены для реализации сетевых атак (например, – атаки с использованием систем SATAN и Shadow Security Scanner);

– атаки с использованием взломщиков паролей – это тип атак, которые основаны на использовании взломщиков паролей – программ, подбирающих пароли пользователей (например, программа LOphtCrack для ОС Windows или программа Crack для ОС Unix);

– атаки с использованием анализаторов протоколов – это тип атак, основанных на использовании анализаторов протоколов – программах, «прослушивающих» сетевой трафик. С их помощью можно автоматизировать поиск в сетевом трафике такой информации, как идентификаторы и пароли пользователей, информацию о кредитных картах и т.д. (например, программы Microsoft Network Monitor, NetXRay компании Network Associates или Lan Explorer).

Приведенная классификация охватывает почти все возможные действия злоумышленника и является достаточно полной с практической точки зрения. Ее недостатком является невозможность определить элементы сети, подверженные воздействию той или иной атаки, а также последствия, к которым может привести успешная реализация атак.

Классификация, предложенная компанией Internet Security Systems, имеет те же самые недостатки и включает пять типов атак:

– сбор информации;
– попытки несанкционированного доступа;
– отказ в обслуживании;
– подозрительная активность;
– системные атаки.

При разработке программных продуктов, предназначенных для защиты сетей, серверов и рабочих станций (таких как Real Secure, System scanner и др.) компания Internet Security Systems использует другие классификационные признаки возможных сетевых атак. Классификация по этим признакам более эффективна с точки зрения защиты от вторжений. Рассмотрим эти признаки.

1. По степени риска – позволяет ранжировать опасность атак по классам:

– высокий – атаки, успешная реализация которых позволяет атакующему немедленно получить доступ к ЭВМ;

– средний – атаки, успешная реализация которых потенциально может дать атакующему доступ к машине;
– низкий – атаки, при успешной реализации которых атакующий может получить сведения, облегчающие ему задачу взлома данной машины.

2. По типу атаки – позволяет судить о том, может ли атака быть осуществлена удаленно, или только локально:
– осуществляемые локально;
– осуществляемые удаленно.

3. По подверженному данной атаке программному обеспечению (например, Microsoft Internet Explorer 6, Microsoft Internet Explorer 10, Adobe Flash Player и т.д.).

4. По характеру действий, используемых в атаке:
– «черные ходы» – атаки, основанные на использовании недокументированных разработчиками возможностях ПО, которые могут привести к выполнению пользователем несанкционированных операций на атакуемом сервере;
– атаки типа «отказ в обслуживании» – атаки, основанные на использовании ошибок, позволяющие атакующему сделать какой-либо сервер недоступным для легитимных пользователей;
– распределенные атаки типа «отказ в обслуживании» – несколько пользователей (программ) посылают большое количество фиктивных запросов на сервер, приводя его в нерабочее состояние;
– потенциально незащищенная операционная система;
– неавторизованный доступ.

Приведенные классификационные признаки также не лишены недостатков. К ним можно отнести невозможность описания цели атаки и ее последствий. Например, классификационный признак «по характеру действий» содержит два класса атак типа «отказ в обслуживании», но не содержит классов, описывающих атак, обеспечивающих злоумышленнику перехват трафика.

Другой подход был применен в классификации, использованной компанией Tenable Network Security в достаточно известном программном продукте Nessus, предназначенном для анализа безопасности серверов. В качестве основного классификационного критерия выбран характер уязвимости, используемой для реализации атаки:
– «черные ходы»;

– ошибки в CGI скриптах;
– атаки типа «отказ в обслуживании»;
– ошибки в программах – FTP-серверах;
– наличие на компьютере сервиса Finger или ошибки в программах, реализующих этот сервис;
– ошибки в реализации межсетевых экранов;
– ошибки, позволяющие пользователю, имеющему терминальный вход на данный сервер, получить права администратора;
– ошибки, позволяющие атакующему удаленно получить права администратора;
– прочие ошибки, не вошедшие в другие категории;
– ошибки в программах – NIS-серверах;
– ошибки в программах – RPC-серверах;
– уязвимости, позволяющие атакующему удаленно получить любой файл с сервера;
– ошибки в программах – SMTP-серверах;
– неиспользуемые сервисы.

Помимо этого, по типу программной среды они подразделяются на уязвимости в операционной системе, уязвимости в определенном сервисе и уязвимости в определенном программном обеспечении.

Положительной чертой данной классификации является наличие класса «прочие ошибки, не вошедшие в другие категории», так как формально к любой атаке, в том числе новой, благодаря этому классу будет применима данная классификация. Однако, данная классификация не охватывает всех существующих сетевых атак. Например, не рассматриваются такие опасные атаки, как атаки типа «отказ в обслуживании», перехват данных и атаки, направленные на сетевое оборудование.

Огромное количество различных сетевых атак и постоянное появление новых атак, не подчиняющихся принятым критериям классификации, приводит к снижению эффективности применения существующих классификаций, поэтому их использование без внесения изменений невозможно.

8.2. Развитие методов обнаружения вторжений

Технология выявления вторжений первоначально возникла благодаря финансовому аудиту мэйнфреймов. Поскольку мэйнфрейм – это вычислительная система высочайшего класса, изначально

ориентированная на бесперебойное исполнение исключительно больших, смешанных рабочих нагрузок при высоком уровне коэффициента использования системы, поддерживающая тысячи одновременно выполняемых операций ввода/вывода, обслуживающая большое число пользователей и обрабатывающая до миллиарда задач в день, то таких компьютеров было очень мало, а стоили они чрезвычайно дорого. Поэтому доступ к их вычислительным мощностям требовал строжайшего контроля, а использование машинного времени – тщательного учета [43].

Первоначально системные администраторы обнаруживали вторжения «вручную», анализируя действия пользователей. Они могли заметить атаку, обратив внимание, например, на то, что пользователь, находящийся в отпуске, локально вошел в систему, или непривычно активен принтер, который крайне редко используется. Достаточно эффективная на начальном этапе, эта форма обнаружения вторжений была вместе с тем сугубо ориентированной на конкретные ситуации и не обладала масштабируемостью.

В конце 70-х годов XX века финансовый аудит был адаптирован к требованиям безопасности. Администраторы получили возможность просматривать системные журналы в поисках аномалий, наличие которых могли бы служить свидетельством некорректного использования ресурсов, например, изменение пользователями файлов без соответствующих полномочий.

Таким образом, на следующем этапе для обнаружения вторжений стали использоваться журналы регистрации, которые системные администраторы просматривали в поисках признаков необычных или злонамеренных действий. В конце 70-х и в начале 80-х годов администраторы, как правило, печатали журналы регистрации на перфорированной бумаге, которая к концу рабочей недели представляла собой кипу высотой в полтора-два метра. Поиск по такому листингу, безусловно, занимал уйму времени. При огромном количестве информации и исключительно ручных методах анализа, администраторы зачастую использовали журналы регистрации в качестве доказательства нарушения защиты уже после того, как оно произошло. Надежда на то, что удастся обнаружить атаку в момент ее проведения, была крайне мала.

По мере того, как дисковая память становилась все дешевле, журналы регистрации стали создавать в электронном виде; появились программные средства для анализа собранных данных. Однако

подобный анализ выполнялся очень медленно и зачастую требовал значительных вычислительных ресурсов, так что, как правило, программы обнаружения вторжений запускались в пакетном режиме, в то время, когда с системой работало мало пользователей, в основном, по ночам. Большинство нарушений защиты по-прежнему выявлялись уже постфактум.

В начале 90-х годов были разработаны системы обнаружения вторжений в реальном времени, которые просматривали записи в журнале регистрации сразу, как только они генерировались. Это позволило обнаруживать атаки и попытки атак в момент их проведения, что, в свою очередь, дало возможность немедленно принимать ответные меры, а, в некоторых случаях, даже предупреждать атаки.

Самые последние проекты, посвященные обнаружению вторжений, сосредоточиваются вокруг создания инструментов, которые могут эффективно развертываться в крупных сетях. Эта задача отнюдь не проста, учитывая все большее внимание, уделяемое вопросам безопасности, бесчисленное количество новых методов организации атак и непрерывные изменения в окружающей вычислительной среде.

8.3. Понятие, назначение и виды систем обнаружения вторжений

Система обнаружения вторжений (СОВ) – программные и программно-аппаратные технические средства, реализующие функции автоматизированного обнаружения в ИС действий, направленных на преднамеренный несанкционированный доступ к информации, а также специальных воздействий на информацию в целях ее добывания, уничтожения, искажения или блокирования.

Современные системы обнаружения вторжений (СОВ, IDS) в соответствии с различными критериями можно отнести к следующим классам [10, 43]:

1. По типу объекта мониторинга:

– сетевые СОВ (обнаружение атак на уровне сети) – «мониторят» сетевой сегмент;

– узловые СОВ (обнаружение атак на уровне хоста) – осуществляют мониторинг активности одного узла в сети;

– обнаружение атак на уровне приложения (часто относят к подвиду узловых СОВ).

2. По архитектуре:

– распределенные СОВ – система состоит из нескольких элементов: разнесенных по сети сенсоров, вычислительного центра, консоли администратора;

– централизованные СОВ – все вычисления совершаются на одной рабочей станции.

3. По технологии анализа:

– без сохранения состояния – каждое событие рассматривается независимо от других;

– с сохранением состояния – информация о предыдущих событиях сохраняется и учитывается при принятии решения.

4. По способу реагирования:

– пассивные СОВ – во время инцидента подается сигнал тревоги и вносится запись в журнал событий;

– активные СОВ – осуществляют активный ответ (сбрасывают соединение, блокируют IP и т.д.).

5. По методу обнаружения атак:

– системы обнаружения злоупотреблений – осуществляют поиск шаблонов известных атак в сетевом трафике или высокоуровневых данных;

– системы обнаружения аномалий – обладают профилем нормальной активности системы и определяют отклонения от него;

– системы обнаружения нарушений в протоколе – следят за корректностью соблюдения протоколов сетевого взаимодействия и фиксируют нарушения.

Рассмотрим перечисленные виды СОВ более подробно.

Сетевые СОВ анализируют сетевой трафик и передают сообщения о возможном нападении на консоль управления.

К их положительным чертам можно отнести:

– могут контролировать большую сеть;

– не влияют на производительность и топологию сети;

– система может быть защищена от нападений на нее саму; ее можно сделать невидимой для нападающих.

Недостатками таких IDS являются:

– высокая ресурсоёмкость; не распознает нападение, начатое при высокой загрузки сети;

– требуют дополнительной настройки и функциональности сетевых устройств;
– не анализируют зашифрованную информацию;
– не могут распознать результат атаки; сообщают о нападении, не анализируя степень проникновения.

Узловые (хостовые) СОВ анализируют активность процессов и пользователей на конкретном сервере, ПК, рабочей станции с высокой степенью детализации и позволяют точно определить злоумышленника.

Их преимущества:
– обнаруживают нападения, пропущенные сетевыми СОВ, так как «имеют представление» о событиях на сервере;
– работают в сети с шифрованием данных, поскольку данные находятся на защищаемом компьютере до их отправки в открытом виде;
– функционируют в коммутируемых сетях.

К недостаткам относятся такие свойства хостовых СОВ:
– должны устанавливаться на каждом компьютере;
– не способны контролировать ситуацию во всей сети;
– трудности в обнаружении атак с отказом в обслуживании;
– могут блокироваться некоторыми DoS-атаками;
– используют ресурсы ПК, снижая эффективность его работы.

СОВ на уровне приложений контролируют события в пределах отдельного приложения и обнаруживают нападения при анализе системных журналов приложения.

Большой запас знаний о приложении позволяют СОВ обеспечивать детальное представление о подозрительной деятельности в приложении.

Преимущества таких систем перед аналогичными:
– очень высокая степень детализации, позволяющая отслеживать деятельность отдельных пользователей;
– способны работать в зашифрованных средах.

Пассивная СОВ при обнаружении нарушения безопасности, записывает информацию о нарушении в лог приложения, и отправляет сигнал на консоль администратору системы.

Пассивная обработка событий является наиболее распространенным типом действий, предпринимаемых при обнаружении вторжения. Причины этого заключаются в том, что пассивные ответные действия более просты для автоматического

применения и обеспечивают меньшую вероятность повреждения легитимного трафика.

В системах могут быть реализованы различные виды пассивных ответных действий.

Предотвращение. Не позволяет пользователям совершать действия, облегчающие атаку, а злоумышленнику – проникнуть в систему.

Игнорирование. Настраивается для атак через несуществующие службы или когда система не чувствительна к данному типу атак.

Ведение журналов. Должно генерироваться максимальное количество информации для обеспечения детального анализа или для помощи в принятии дальнейших мер.

Уведомления. Позволяют СОВ информировать администратора о происшедшем событии, где бы он не находился. В качестве уведомлений могут использоваться, например, мерцающие окна с сообщениями, звуковые сигналы, СМС-сообщения и пр.

Активная СОВ ведет ответные действия на нарушение. В зависимости от настроек, ответные действия могут проводиться автоматически либо по команде оператора.

Активная обработка события позволяет наиболее быстро предпринять возможные меры для снижения уровня вредоносного действия события.

Однако, если недостаточно серьезно отнестись к программированию действий в различных ситуациях и не провести должного тестирования набора правил, активная обработка событий может вызвать повреждение системы или полный отказ в обслуживании легитимных пользователей.

Активными ответными действиями могут служить [15, 20, 43]:

– *прерывание соединений, сеансов или процессов* – самое простое действие из всех возможных ответных действий;

– *определение объекта, подлежащего уничтожению*. Это действие по понятным причинам выполняется после изучения события. Уничтожаемым объектом может стать процесс, сеанс пользователя, сетевое соединение;

– *перенастройка сети*, заключающаяся в перенастройке межсетевого экрана или маршрутизатора выполняется, если произошло несколько попыток несанкционированного доступа с конкретного IP-адреса.

– *обманные действия*. Введение злоумышленника в заблуждение – создание впечатления успешного и необнаруженного проведения атаки. Такой ответ – наиболее сложный вид активной обработки событий.

Технология обнаружения аномального поведения основана на том, что аномальное поведение пользователя (атака или иное враждебное действие) могут проявляться как отклонение от нормального поведения. Примерами аномального поведения могут служить большое число соединений за короткий промежуток времени, высокая загрузка центрального процессора, создание резервной копии в необычное время или с использованием нетрадиционного носителя информации и т.п.

Если однозначно описать профиль нормального поведения пользователя, то любое отклонение от него можно идентифицировать как аномальное поведение. Но аномальное поведение не всегда является атакой. Например, одновременную посылку большого числа запросов от администратора сети система обнаружения атак может идентифицировать как атаку типа «отказ в обслуживании».

При использовании системы с такой технологией возможны два негативных случая:

– обнаружение аномального поведения, которое не является атакой, и отнесение его к классу атак;

– пропуск атаки, которая не подпадает под определение аномального поведения. Этот случай более опасен, чем ложное отнесение аномального поведения к классу атак.

В системах обнаружения аномального поведения для обнаружения аномалии используются несколько методов:

– пороговые значения: наблюдения за объектом выражаются в виде числовых интервалов (количество используемых файлов, число неудачных попыток входа в систему, загрузка центрального процессора и т.п.). Выход за пределы этих интервалов считается аномальным поведением;

– статистические: решение о наличии атаки делается по большому количеству собранных данных;

– параметрические: для выявления атак строится «профиль нормальной системы» на основе шаблонов, которых должен придерживаться объект;

– непараметрические: профиль строится на основе наблюдения за объектом в период обучения;

– другие методы и меры.

При установке и эксплуатации систем обнаружения аномальной деятельности возникают определенные трудности. Так, например, построение профиля объекта – это достаточно трудно формализуемая и затратная по времени задача, требующая большой предварительной работы, высокой квалификации и опыта исполнителя. Кроме того, затруднено определение граничных значений характеристик поведения субъекта для снижения вероятности появления одного из двух вышеназванных крайних негативных случаев.

К достоинствам систем обнаружения аномальной деятельности относят:

– способны обнаруживать новые типы атак, сигнатуры для которых еще не разработаны;

– не нуждаются в обновлении сигнатур и правил обнаружения атак;

– обнаружения аномалий генерируют информацию, которая может быть использована в системах обнаружения злоумышленного поведения.

В качестве их недостатков можно указать:

– требуют длительного и качественного обучения;

– генерируют много ошибок второго рода;

– обычно слишком медленны в работе и требуют большого количества вычислительных ресурсов.

Пока эта технология не получила широкого распространения из-за трудностей с ее практической реализацией. Использование профилей нашло свое практическое применение в системах обнаружения мошенничества, используемых в финансовых структурах или у операторов связи.

Обнаружение злоупотреблений заключается в описании атаки в виде сигнатуры и поиска данной сигнатуры в контролируемом пространстве (сетевом трафике или журнале регистрации). В качестве сигнатуры атаки может выступать шаблон действий или строка символов, характеризующие аномальную деятельность. При этом система может обнаружить все известные атаки. Однако системы данного типа не могут обнаруживать новые, еще неизвестные виды атак.

Подход, реализованный в таких системах, достаточно прост и именно на нем основаны практически все предлагаемые сегодня на рынке системы обнаружения атак.

Несмотря на эффективность и простоту реализации этого метода, проблемы также существуют:

– создание механизма описания сигнатур, т.е. языка описания атак;

– запись атаки для фиксирования всех ее возможные модификации.

Как и другие, эти системы не лишены определенных достоинств и недостатков.

К достоинствам отнесем малое число ложных срабатываний и отсутствие необходимости обучения системы. К недостаткам – возможность обнаружения только известных атак, недостаточная эффективность при работе с большими объемами данных, необходимость регулярного обновления базы данных сигнатур.

К какому бы виду не относилась система обнаружения атак или вторжений, все они основаны на нескольких общих методах. Причем, методы, описанные ниже, не являются взаимоисключающими. Во многих системах используется комбинация нескольких методов.

Анализ журналов регистрации

Это один из самых первых реализованных методов обнаружения атак. Он заключается в анализе журналов регистрации, создаваемых операционной системой, прикладным программным обеспечением, маршрутизаторами и т.д. Записи журнала регистрации анализируются и интерпретируются системой обнаружения атак.

К достоинствам этого метода можно отнести простоту его реализации. Однако из-за этой простоты метод имеет существенные недостатки:

– для достоверного обнаружения подозрительной деятельности необходима регистрация в журналах большого объема данных, что отрицательно сказывается на скорости работы контролируемой информационной системы;

– при анализе журналов регистрации очень трудно обойтись без помощи специалистов, что существенно снижает круг распространения этого метода;

– до настоящего момента нет унифицированного формата хранения журналов;

– анализ осуществляется не в реальном режиме времени, а значит, метод не может быть применен для раннего обнаружения атак в процессе их развития;

– не позволяет обнаружить атаки, направленные на узлы, не использующие журналы регистрации, или для которых не существует соответствующей реализации агента.

Применяют анализ журналов регистрации в дополнение к другим методам обнаружения атак, например, к обнаружению атак «на лету». Использование этого метода позволяет проводить анализ сложившейся ситуации уже после того, как была зафиксирована атака, для того чтобы выработать эффективные меры предотвращения аналогичных атак в будущем.

Анализ «на лету»

Этот метод заключается в мониторинге сетевого трафика в реальном или близком к реальному времени и использовании соответствующих алгоритмов обнаружения.

Этот метод имеет несколько основных преимуществ:

– один агент системы обнаружения атак может просматривать целый сегмент сети с многочисленными хостами и позволяет обнаруживать атаки против всех элементов сети, начиная от атак на маршрутизаторы и заканчивая атаками на прикладные приложения.

– атаки определяются в реальном масштабе времени и нейтрализуются до достижения ими цели;

– невозможность злоумышленнику скрыть следы своей деятельности, что позволяет получить информацию о методе атаки и сведения, которые могут помочь при идентификации злоумышленника;

– обнаружение неудавшихся атак или подозрительной деятельности наиболее важно при оценке и совершенствовании политики безопасности.

Однако системы, использующие указанный метод, имеют и свои недостатки. Такие системы трудно применимы в высокоскоростных сетях со скоростью свыше 100 Мбит/сек, а также неэффективны в коммутируемых сетях и сетях с канальным шифрованием.

Такие методы, как «Использование профилей «нормального» поведения» и «Использование сигнатур атак» были нами рассмотрены выше.

8.4. Структура систем обнаружения вторжений

Как мы знаем, СОВ – это системы, собирающие информацию из различных точек защищаемой компьютерной системы и

анализирующие эту информацию для выявления как попыток нарушения, так и реальных нарушений защиты.

Значит, СОВ должна включать следующие основные элементы (рис. 8.1):

– подсистему сбора информации (модуль слежения, сенсор, монитор, зонд), использующуюся для сбора первичной информации о работе защищаемой системы;

– подсистему анализа (ядро, подсистема обнаружения атак), которая осуществляет поиск атак и вторжений в защищаемую систему;

– модуль представления данных (пользовательский интерфейс) – позволяет пользователю СОВ следить за состоянием защищаемой системы.

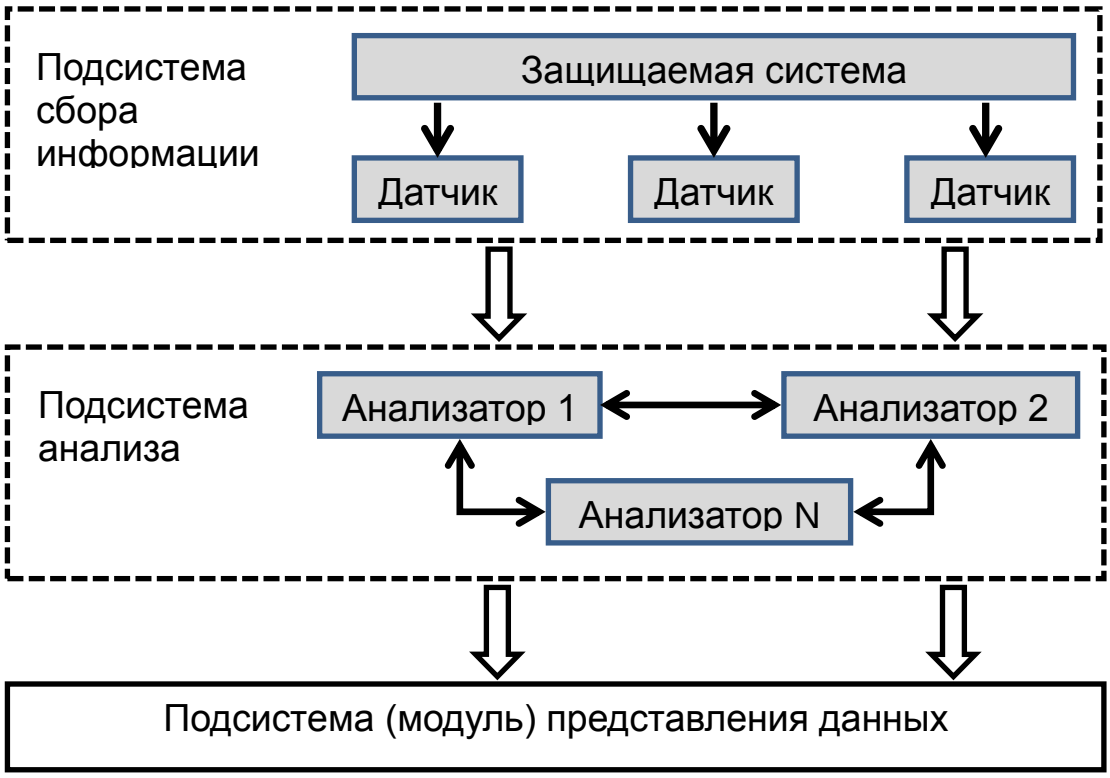

Рис. 8.1. Основные элементы СОВ

Подсистема сбора информации собирает сведения о работе защищаемой системы. Для сбора информации используются автономные модули – датчики, классифицируемые по характеру собираемой информации:

– датчики приложений – собирают данные о работе программного обеспечения защищаемой системы;

– датчики хоста – осуществляют сбор данных о функционировании рабочей станции защищаемой системы;
– датчики сети – обеспечивают сбор данных для оценки сетевого трафика;
– межсетевые датчики – содержат характеристики данных, циркулирующих между сетями.

Система обнаружения вторжений может включать любую комбинацию различных датчиков, становясь при этом более универсальной.

Подсистема анализа структурно состоит из модулей анализа – анализаторов.

Чем больше анализаторов, тем выше эффективность обнаружения. Каждый анализатор выполняет поиск атак или вторжений определенного типа.

Анализатор получает информацию из подсистемы сбора информации или от другого анализатора. Результат работы подсистемы – индикация о состоянии защищаемой системы, а также данные, подтверждающие факт наличия вторжения или атаки.

Подсистема может идентифицировать атаки, принимать решения по вариантам реагирования, сохранять сведения об атаке в хранилище данных и т. д.

Подсистема представления данных необходима для информирования заинтересованных лиц о состоянии защищаемой системы.

В некоторых системах предполагается наличие групп пользователей, каждая из которых контролирует определенные подсистемы защищаемой системы. В таких СОВ применяется разграничение доступа, групповые политики, полномочия и т.д.

Кроме перечисленных выше основных компонентов, СОВ включает и некоторые дополнительные, без которых, тем не менее, адекватная работа IDS не возможна (рис. 8.2).

База знаний содержит профили пользователей и ИС, сигнатуры атак или подозрительные строки, характеризующие несанкционированную деятельность.

Может пополняться производителем СОВ, пользователем системы или компанией, осуществляющей поддержку СОВ.

Хранилище данных обеспечивает хранение данных, собранных в процессе функционирования СОВ.

Подсистема реагирования осуществляет реагирование на обнаруженные атаки и иные контролируемые события.

Подсистема управления компонентами предназначена для управления различными компонентами СОВ (изменение политики безопасности для различных компонентов СОВ, получение информации от этих компонентов.

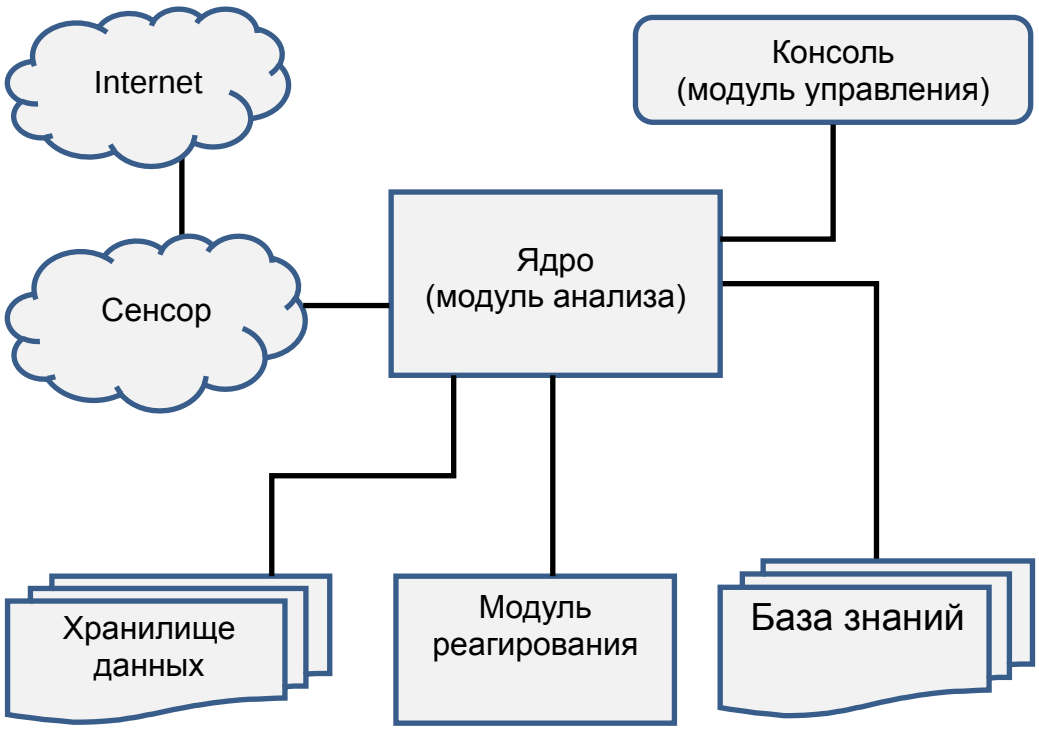

Рис. 8.2. Общая структура СОВ

Эффективность СОВ зависит от применяемых методов анализа:

- статистические методы,
- экспертные системы и нечеткая логика,
- нейронные сети.

Каждый метод обладает рядом достоинств и недостатков.

Сейчас трудно встретить систему, реализующую только один из методов. Методы используются в совокупности.

Статистические методы.

Для всех субъектов ИС определяются профили. Любое отклонение используемого профиля от эталонного считается несанкционированной деятельностью.

Статистические методы универсальны, поскольку для проведения анализа не требуется знания о возможных атаках и используемых ими уязвимостях.

Основные преимущества статистических методов заключаются в использовании известного и зарекомендовавшего себя аппарата математической статистики и адаптации к поведению субъекта.

При использовании статистических методов возникают следующие проблемы:

– не учитывают порядок следования событий (одни и те же события в зависимости от порядка могут быть аномальной или нормальной деятельностью);
– трудно задать пороговые значения отслеживаемых действий, чтобы адекватно идентифицировать аномальную деятельность;
– «статистические» системы могут быть со временем «обучены» нарушителями так, чтобы атакующие действия рассматривались как нормальные;
– «статистические» системы не применимы в тех случаях, когда для пользователя отсутствует шаблон типичного поведения или когда для пользователя типичны несанкционированные действия.

Экспертные системы.

Состоят из набора правил (информация об атаках), которые охватывают знания человека-эксперта. Эти правила могут быть записаны, например, в виде последовательности действий или в виде сигнатуры (характерных признаков) атаки. При выполнении любого из этих правил принимается решение о наличии несанкционированной деятельности.

Чтобы оставаться актуальными, экспертные системы требуют постоянного обновления базы данных.

Главное достоинство экспертных систем заключается в практически полном отсутствии ложных тревог.

Основной недостаток – в невозможности отражения неизвестных (или измененных известных) атак.

Нейронные сети.

Разделение атаки во времени или среди нескольких злоумышленников создает трудности для «статистических» и экспертных систем. Обновления базы данных не дают гарантии корректного выявления атаки.

Нейронные сети преодолевают указанные проблемы.

Нейронная сеть проводит анализ информации и предоставляет возможность оценить, согласуются ли данные с характеристиками, которые она научена распознавать.

Сначала нейросеть обучают правильной идентификации на предварительно подобранной выборке примеров. Обучение нейросети продолжается в процессе работы. Таим образом, такое преимущество нейросети, как обучаемость – способность «изучать» характеристики новых атак позволяет СОВ идентифицировать элементы, которые не похожи на те, что наблюдались в сети прежде.

8.5. Сертификация систем обнаружения вторжений

Для сертификации средств обнаружения вторжений, систем предотвращения утечек данных и т.д. в схеме сертификации средств защиты информации ФСТЭК России существовал определенный порядок проведения испытаний – сертификация подобных продуктов до последнего времени проводилась на соответствие «Техническим условиям», что означало полную неопределенность процесса: поскольку требования к составу функциональных возможностей нигде не были формализованы, то под определение сертифицированного продукта одного и того же типа могли подпасть решения принципиально различных уровней [9].

Такая ситуация требовала пересмотра нормативной базы, поэтому ФСТЭК приняла требования к системам обнаружения вторжений. Этот документ вступил в силу 15 марта 2012 года и имеет пометку «для служебного пользования», однако методические документы «Профили защиты» СОВ, предназначенные для защиты информации, не содержащей сведений, составляющих государственную тайну, доступны на официальном сайте ФСТЭК России.

В документе СОВ рассматривается как один из базовых элементов системы защиты информационной системы. В соответствии с общепринятой практикой выделяются два типа систем обнаружения вторжений: системы обнаружения вторжений уровня сети и системы обнаружения вторжений уровня узла.

Для каждого из типов выделяются 6 классов защиты систем обнаружения вторжений в порядке ужесточения требований от шестого к первому. Каждому классу защиты соответствует определенная категория информационных систем:

– СОВ 6 класса применяются в информационных системах персональных данных 3 и 4 классов;
– СОВ 5 класса применяются в информационных системах персональных данных 2 класса;
– СОВ 4 класса применяются в информационных системах персональных данных 1 класса, информационных системах общего пользования 2 класса, а также в государственных информационных системах, в которых обрабатывается информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну;
– СОВ 3, 2 и 1 классов защиты применяются в информационных системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну.

Наиболее интересной особенностью данного документа является то, что он разработан в соответствии с международной нормативной базой оценки и на основе стандарта ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий». Практически аутентичной копией данного стандарта в редакции 2002 года является руководящий документ Гостехкомиссии России «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Части 1, 2, 3», по которому сегодня проводятся сертификационные испытания.

Испытания системы обнаружения вторжений проводятся на соответствие «Заданию по безопасности», которое представляет собой структурированный и строго формализованный документ, включающий подробное описание функциональных требований безопасности (ФТБ) к объекту оценки и среде его функционирования, а также обеспечивающих мер – требований доверия к безопасности (ТДБ). При разработке «Задания по безопасности» можно использовать типовые наборы требований – «Профили защиты». Испытательная лаборатория и орган по сертификации, в свою очередь, при проведении оценки используют различного рода свидетельства – конструкторскую и проектную документацию на изделие, руководства пользователя и администратора, корпоративные стандарты, руководства и процедуры, требования к которым также могут быть сформулированы в «Задании по безопасности».

Принятый документ в полной мере определяет требования ко всем возможным классам защиты систем обнаружения вторжений, в

частности, в документе сформулированы все функциональные требования и требования доверия, которые должны войти в соответствующие «Профили защиты» – и, в дальнейшем, в «Задания по безопасности» на конкретные изделия.

Состав функциональных требований к системам обнаружения вторжений традиционен, но, помимо возможностей по выявлению, анализу и реагированию на те или иные события, предъявляются еще требования к управлению параметрами СОВ. При этом, часть ФТБ сформулирована в явном виде. Остальные требования разработаны на основе стандартных ФТБ, приведенных во второй части стандарта ГОСТ Р ИСО/МЭК 15408.

Большое значение в документе придается мерам доверия. Так, заявитель должен разработать и реализовать значительное количество технологических процедур, обеспечивающих обновление баз решающих правил системы обнаружения вторжений.

Безусловный интерес вызывает уточнение стандартных (см. часть 3 ГОСТ Р ИСО/МЭК 15408) требований доверия для обеспечения связи с требованиями по контролю отсутствия не декларированных возможностей, изложенными в руководящем документе Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации: Классификация по уровню контроля отсутствия не декларированных возможностей».

Важно отметить, что в документе впервые в отечественной практике в явном виде допускается обновление разработчиком баз решающих правил с предоставлением в испытательную лабораторию подробного отчета обо всех внесенных изменениях и об их возможном влиянии на безопасность системы.

В документе впервые указаны конкретные требования к системам обнаружения вторжений для информационных систем общего пользования, определенных в совместном Приказе ФСБ России и ФСТЭК России №416/489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования».

9. МЕТОДЫ МЕЖСЕТЕВОГО ЭКРАНИРОВАНИЯ

Межсетевой экран (МЭ, брандмауэр, firewall) – это специализированный комплекс межсетевой защиты. МЭ позволяет разделить общую сеть на части и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую. Как правило, эта граница проводится между корпоративной (локальной) сетью предприятия и глобальной сетью Internet.

Обычно МЭ защищают внутреннюю сеть предприятия от «вторжений» из глобальной сети Internet, хотя они могут использоваться и для защиты от «нападений» из корпоративной интрасети, к которой подключена локальная сеть предприятия. Технология МЭ одна из самых первых технологий защиты корпоративных сетей от внешних угроз.

Для большинства организаций установка МЭ является необходимым условием обеспечения безопасности внутренней сети.

9.1. Функции МЭ

Для противодействия несанкционированному доступу МЭ должен располагаться между защищаемой сетью организации, являющейся внутренней, и потенциально враждебной внешней сетью. При этом все взаимодействия между этими сетями должны осуществляться только через МЭ. Организационно МЭ входит в состав защищаемой сети.

МЭ, защищающий несколько узлов внутренней сети, решает задачи [14]:

– ограничение доступа внешних (по отношению к защищаемой сети) пользователей к внутренним ресурсам сети;

– разграничение доступа пользователей защищаемой сети к внешним ресурсам для регулирования доступа к серверам, не требующимся для выполнения служебных обязанностей.

Не существует единой общепризнанной классификации МЭ. Их можно классифицировать по следующим основным признакам.

1. По функционированию на уровнях сетевой модели OSI:

– пакетный фильтр (экранирующий маршрутизатор);

– шлюз сеансового уровня (экранирующий транспорт);

– прикладной шлюз;
– шлюз экспертного уровня.

2. По используемой технологии:
– контроль состояния протокола;
– на основе модулей – посредников.

3. По исполнению:
– аппаратно-программный;
– программный.

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

Фильтрация трафика

Фильтрация информационных потоков состоит в их выборочном, на основе набора предварительно загруженных в МЭ правил, соответствующих принятой политике безопасности, пропускании через экран, возможно, с выполнением некоторых преобразований. Поэтому МЭ можно представлять, как последовательность фильтров, обрабатывающих информационный поток [43].

Каждый из фильтров предназначен для интерпретации отдельных правил фильтрации путем [19]:
– анализа информации по заданным в интерпретируемых правилах критериям, например, по адресам получателя и отправителя или по типу приложения, для которого эта информация предназначена;
– принятия на основе интерпретируемых правил одного из следующих решений:
- не пропустить данные;
- обработать данные от имени получателя и возвратить результат отправителю;
- передать данные на следующий фильтр для продолжения анализа;
- пропустить данные, игнорируя следующие фильтры.

Правила фильтрации могут задавать и дополнительные действия, которые относятся к функциям посредничества, например,

преобразование данных, регистрация событий и др. Именно правила фильтрации определяют перечень условий, по которым осуществляются разрешение или запрещение дальнейшей передачи данных, а также выполнение дополнительных защитных функций.

В качестве критериев анализа информационного потока могут использоваться следующие параметры:

– служебные поля пакетов сообщений, содержащие сетевые адреса, идентификаторы, адреса интерфейсов, номера портов и другие значимые данные;

– непосредственное содержимое пакетов сообщений, проверяемое, например, на наличие компьютерных вирусов;

– внешние характеристики потока информации, например, временные, частотные характеристики, объем данных и т.д.

Используемые критерии анализа зависят от уровней модели OSI, на которых осуществляется фильтрация. В общем случае, чем выше уровень модели OSI, на котором МЭ фильтрует пакеты, тем выше и обеспечиваемый им уровень защиты.

Выполнение функций посредничества

Функции посредничества МЭ выполняет с помощью специальных программ, называемых экранирующими агентами или программами-посредниками. Эти программы являются резидентными и запрещают непосредственную передачу пакетов сообщений между внешней и внутренней сетью.

При необходимости доступа из внутренней сети во внешнюю сеть или наоборот вначале должно быть установлено логическое соединение с программой-посредником, функционирующей на компьютере МЭ. Программа-посредник проверяет допустимость запрошенного межсетевого взаимодействия и при его разрешении сама устанавливает отдельное соединение с требуемым компьютером. Далее обмен информацией между компьютерами внутренней и внешней сети осуществляется через программного посредника, который может выполнять фильтрацию потока сообщений, а также осуществлять другие защитные функции.

МЭ может выполнять функции фильтрации без применения программ-посредников, обеспечивая прозрачное взаимодействие между внутренней и внешней сетью. Также и программные посредники могут и не осуществлять фильтрацию потока сообщений.

В общем случае программы-посредники, блокируя прозрачную передачу потока сообщений, могут выполнять следующие функции:

– проверку подлинности передаваемых данных;
– фильтрацию и преобразование потока сообщений, например, динамический поиск вирусов и прозрачное шифрование информации;
– разграничение доступа к ресурсам внутренней сети;
– разграничение доступа к ресурсам внешней сети;
– кэширование данных, запрашиваемых из внешней сети;
– идентификацию и аутентификацию пользователей;
– трансляцию внутренних сетевых адресов для исходящих пакетов сообщений;
– регистрацию событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и генерацию отчетов.

Способы разграничения доступа к ресурсам внутренней сети практически не отличаются от способов разграничения, поддерживаемых на уровне операционной системы. При разграничении доступа к ресурсам внешней сети чаще всего используется один из следующих подходов [15]:
– разрешение доступа только по заданным адресам во внешней сети;
– фильтрация запросов на основе обновляемых списков недопустимых адресов и блокировка поиска информационных ресурсов по нежелательным ключевым словам;
– накопление и обновление администратором санкционированных информационных ресурсов внешней сети в дисковой памяти МЭ и полный запрет доступа во внешнюю сеть.

С помощью специальных посредников поддерживается также кэширование данных, запрашиваемых из внешней сети. При доступе пользователей внутренней сети к информационным ресурсам внешней сети вся информация накапливается на пространстве жесткого диска МЭ, в этом случае выполняющего роль rгоху-сервера. Поэтому если при очередном запросе нужная информация окажется на rгоху-сервере, то посредник предоставляет ее без обращения к внешней сети, что существенно ускоряет доступ. Администратору следует позаботиться только о периодическом обновлении содержимого rгоху-сервера.

Функция кэширования успешно может использоваться для ограничения доступа к информационным ресурсам внешней сети. В этом случае все санкционированные информационные ресурсы внешней сети накапливаются и обновляются администратором на

рroxy-сервере. Пользователям внутренней сети разрешается доступ только к информационным ресурсам рroxy-сервера, а непосредственный доступ к ресурсам внешней сети запрещается.

Фильтрация и преобразование потока сообщений выполняется посредником на основе заданного набора правил. Здесь следует различать два вида программ-посредников:

– экранирующие агенты, ориентированные на анализ потока сообщений для определенных видов сервиса, например, FTP, HTTP;

– универсальные экранирующие агенты, обрабатывающие весь поток сообщений, например, агенты, ориентированные на поиск и обезвреживание компьютерных вирусов, или прозрачное шифрование данных.

Программный посредник анализирует поступающие к нему пакеты данных и, если какой-либо объект не соответствует заданным критериям, то либо блокирует его дальнейшее продвижение, либо выполняет соответствующие преобразования, например, обезвреживает обнаруженные компьютерные вирусы. При анализе содержимого пакетов важно, чтобы экранирующий агент мог автоматически распаковывать проходящие файлы архивов.

МЭ с посредниками позволяют также организовывать защищенные виртуальные сети VPN, например, безопасно объединять несколько локальных сетей, подключенных к Internet, в одну виртуальную сеть.

9.2. Дополнительные возможности МЭ

Помимо выполнения фильтрации трафика и функций посредничества некоторые МЭ позволяют реализовывать другие, не менее важные функции, выполнение которых направлено на обеспечение защиты ИС [43].

Идентификация и аутентификация пользователей.

Кроме разрешения или запрещения допуска различных приложений в сеть, МЭ могут также выполнять аналогичные действия и для пользователей, которые желают получить доступ к внешним или внутренним ресурсам ИС.

Прежде чем пользователю будет предоставлено право использования какого-либо сервиса, необходимо убедиться, что он действительно тот, за кого себя выдает. Идентификация и аутентификация пользователей являются важными компонентами

концепции МЭ. Авторизация пользователя обычно рассматривается в контексте аутентификации – как только пользователь аутентифицирован, для него определяются разрешенные ему сервисы.

Трансляция сетевых адресов.

Для реализации многих атак злоумышленнику необходимо знать адрес своей жертвы. Чтобы скрыть эти адреса, а также топологию всей сети, МЭ выполняют очень важную функцию – трансляцию внутренних сетевых адресов.

Данная функция реализуется по отношению ко всем пакетам, следующим из внутренней сети во внешнюю. Для этих пакетов выполняется автоматическое преобразование IP-адресов компьютеров-отправителей в один «надежный» IP-адрес.

Трансляция внутренних сетевых адресов может осуществляться двумя способами — динамически и статически. В первом случае адрес выделяется узлу в момент обращения к МЭ. После завершения соединения адрес освобождается и может быть использован любым другим узлом внутренней сети. Во втором случае адрес узла всегда привязывается к одному адресу МЭ, из которого передаются все исходящие пакеты. IP-адрес МЭ становится единственным активным IP-адресом, который попадает во внешнюю сеть. В результате все исходящие из внутренней сети пакеты оказываются отправленными МЭ, что исключает прямой контакт между авторизованной внутренней сетью и являющейся потенциально опасной внешней сетью.

При таком подходе топология внутренней сети скрыта от внешних пользователей, что усложняет задачу несанкционированного доступа. Кроме повышения безопасности трансляция адресов позволяет иметь внутри сети собственную систему адресации, не согласованную с адресацией во внешней сети, например, в сети Internet. Это эффективно решает проблему расширения адресного пространства внутренней сети и дефицита адресов внешней сети.

Администрирование, регистрация событий и генерация отчетов.

Простота и удобство администрирования является одним из ключевых аспектов в создании эффективной и надежной системы защиты. Ошибки при определении правил доступа могут образовать дыру, через которую возможен взлом системы. Поэтому в

большинстве МЭ реализованы сервисные утилиты, облегчающие ввод, удаление, просмотр набора правил. Наличие этих утилит позволяет также производить проверки на синтаксические или логические ошибки при вводе, или редактирования правил. Как правило, утилиты позволяют просматривать информацию, сгруппированную по каким-либо критериям, например, все, что относится к конкретному пользователю или сервису.

Важными функциями МЭ являются регистрация событий, реагирование на задаваемые события, анализ зарегистрированной информации и составление отчетов.

МЭ имеет возможность регистрации всех действий, им фиксируемых. К таким действиям относятся не только пропуск или блокирование сетевых пакетов, но и изменение правил разграничения доступа администратором безопасности и другие действия. Такая регистрация позволяет обращаться к создаваемым журналам по мере необходимости (в случае возникновения инцидента безопасности или сбора доказательств для предоставления их в судебные инстанции или для внутреннего расследования).

Многие МЭ содержат мощную систему регистрации, сбора и анализа статистики. При правильно настроенной системе фиксации сигналов о подозрительных событиях МЭ может дать детальную информацию о том, были ли МЭ или сеть атакованы или зондированы. Статистика использования сети важна в качестве исходных данных при проведении исследований и анализе риска для формулирования требований к сетевому оборудованию и программам.

Учет может вестись по адресам клиента и сервера, идентификаторам пользователей, времени сеансов, времени соединений, количеству переданных/принятых данных, действиям администратора и пользователей.

В качестве обязательной реакции на обнаружение попыток выполнения несанкционированных действий должно быть определено уведомление администратора, т.е. выдача предупредительных сигналов. Любой МЭ, который не способен посылать предупредительные сигналы при обнаружении нападения, нельзя считать эффективным средством межсетевой защиты.

9.3. Варианты исполнения МЭ

Существует два основных варианта исполнения МЭ – программный и программно-аппаратный [19]. В свою очередь программно-аппаратный вариант имеет две разновидности – в виде специализированного устройства и в виде модуля в маршрутизаторе или коммутаторе.

В настоящее время чаще используется программное решение, которое на первый взгляд выглядит более привлекательным [14]. Это связано с тем, что для его применения достаточно, казалось бы, только приобрести программное обеспечение МЭ и установить на любой компьютер, имеющийся в организации. Однако на практике далеко не всегда в организации находится свободный компьютер, удовлетворяющий достаточно высоким требованиям по системным ресурсам. Поэтому одновременно с приобретением ПО, приобретается и компьютер для его установки. Затем следует процесс установки на компьютер операционной системы и ее настройка, что также требует времени. И только после этого устанавливается и настраивается ПО системы обнаружения атак. Нетрудно заметить, что использование обычного персонального компьютера далеко не так просто, как кажется на первый взгляд.

В последние годы значительно возрос интерес к программно-аппаратным решениям, которые постепенно вытесняют «чисто» программные системы. Широкое распространение стали получать специализированные программно-аппаратные решения, называемые security appliance. Программно-аппаратный комплекс межсетевого экранирования обычно состоит из компьютера, а также функционирующих на нем ОС и специального ПО. Используемый компьютер должен быть достаточно мощным и физически защищенным, например, находиться в специально отведенном и охраняемом помещении. Кроме того, он должен иметь средства защиты от загрузки ОС с несанкционированного носителя. Программно-аппаратные комплексы используют специализированные или обычные операционные системы, «урезанные» для выполнения заданных функций и удовлетворяющие ряду требований [19]:

– иметь средства разграничения доступа к ресурсам системы;

– блокировать доступ к компьютерным ресурсам в обход предоставляемого программного интерфейса;

– запрещать привилегированный доступ к своим ресурсам из локальной сети;
– содержать средства мониторинга/аудита любых административных действий.

Достоинства специализированных программно-аппаратных решений:
– простота внедрения в технологию обработки информации. Такие средства поставляются с заранее установленной и настроенной ОС и защитными механизмами;
– простота управления. Данные средства могут управляться с любой рабочей станции Windows или Unix;
– отказоустойчивость и высокая доступность. Исполнение МЭ в виде специализированного программно-аппаратного комплекса позволяет реализовать механизмы обеспечения не только программной, но и аппаратной отказоустойчивости и высокой доступности;
– высокая производительность и надежность. За счет исключения из ОС всех «ненужных» сервисов и подсистем, программно-аппаратный комплекс работает более эффективно;
– специализация на защите. Решение только задач обеспечения сетевой безопасности не приводит к затратам ресурсов на выполнение других функций, например, маршрутизации и т.п.

9.4. Схемы сетевой защиты на базе МЭ

При подключении корпоративной или локальной сети к глобальным сетям необходимы [11]:
– защита корпоративной или локальной сети от удаленного НСД со стороны глобальной сети;
– сокрытие информации о структуре сети и ее компонентов от пользователей глобальной сети;
– разграничение доступа в защищаемую сеть из глобальной сети и из защищаемой сети в глобальную сеть.

Для эффективной защиты межсетевого взаимодействия система МЭ должна быть правильно установлена и сконфигурирована. Данный процесс состоит из формирования политики межсетевого взаимодействия и выбора схемы подключения и настройки параметров функционирования МЭ.

Политика межсетевого взаимодействия является составной частью общей политики безопасности в организации. Она определяет

требования к безопасности информационного обмена организации с внешним миром и должна отражать два аспекта:

- политику доступа к сетевым сервисам;
- политику работы МЭ.

Политика доступа к сетевым сервисам определяет правила предоставления и использования всех возможных сервисов защищаемой компьютерной сети. В рамках данной политики должны быть заданы все сервисы, предоставляемые через МЭ, и допустимые адреса клиентов для каждого сервиса. Кроме того, для пользователей должны быть указаны правила, описывающие, когда, кто, каким сервисом и на каком компьютере может воспользоваться. Задаются также ограничения на методы доступа. Ограничение методов доступа необходимо для того, чтобы пользователи не могли обращаться к «запрещенным» сервисам Internet обходными путями. Правила аутентификации пользователей и компьютеров, а также условия работы пользователей вне локальной сети организации должны быть определены отдельно.

Для того чтобы МЭ успешно защищал ресурсы организации, политика доступа пользователей к сетевым сервисам должна быть реалистичной. Реалистичной считается такая политика, при которой найден баланс между защитой сети организации от известных рисков и необходимым доступом пользователей к сетевым сервисам.

Политика работы МЭ задает базовый принцип управления межсетевым взаимодействием, положенный в основу функционирования МЭ. Может быть выбран один из двух принципов:

- запрещено все, что явно не разрешено;
- разрешено все, что явно не запрещено.

Фактически выбор принципа устанавливает, насколько «подозрительной» или «доверительной» должна быть система защиты. В зависимости от выбора, решение может быть принято, как в пользу безопасности и в ущерб удобству использования сетевых сервисов, так и наоборот.

Основные схемы подключения МЭ

При подключении корпоративной сети к глобальным сетям необходимо разграничить доступ в защищаемую сеть из глобальной сети и из защищаемой сети в глобальную сеть, а также обеспечить защиту подключаемой сети от удаленного НСД со стороны глобальной сети. При этом организация заинтересована в сокрытии

информации о структуре своей сети и ее компонентов от пользователей глобальной сети. Работа с удаленными пользователями требует установления жестких ограничений доступа к информационным ресурсам защищаемой сети.

Часто возникает потребность иметь в составе локальной сети несколько сегментов с разными уровнями защищенности [15]:

– свободно доступные сегменты (например, рекламный WWW-сервер);
– сегмент с ограниченным доступом (например, для доступа сотрудникам организации с удаленных узлов);
– закрытые сегменты (например, финансовая локальная подсеть организации).

Для подключения МЭ могут использоваться различные схемы, которые зависят от условий функционирования защищаемой сети, а также от количества сетевых интерфейсов и других характеристик, используемых МЭ. Широкое распространение получили схемы:

– защиты сети с использованием экранирующего маршрутизатора;
– единой защиты локальной сети;
– с защищаемой закрытой и не защищаемой открытой подсетями;
– с раздельной защитой закрытой и открытой подсетей.

Рассмотрим подробнее схему с защищаемой закрытой и не защищаемой открытой подсетями. Если в составе локальной сети имеются общедоступные открытые серверы, то их целесообразно вынести как открытую подсеть до МЭ. Этот способ обладает высокой защищенностью закрытой части локальной сети, но обеспечивает пониженную безопасность открытых серверов, расположенных до МЭ.

Некоторые МЭ позволяют разместить эти серверы на себе. Однако такое решение не является лучшим с точки зрения безопасности самого МЭ и загрузки компьютера. Схему подключения МЭ с защищаемой закрытой подсетью и не защищаемой открытой подсетью целесообразно использовать лишь при невысоких требованиях по безопасности к открытой подсети.

Если же к безопасности открытых серверов предъявляются повышенные требования, тогда необходимо использовать схему с раздельной защитой закрытой и открытой подсетей.

9.5. Проблемы безопасности МЭ

МЭ не решает всех проблем безопасности сети. Кроме описанных выше достоинств МЭ, существуют ограничения в их использовании и угрозы безопасности, от которых МЭ не могут защитить [43]:

– возможное ограничение пропускной способности. Традиционные МЭ являются потенциально узким местом сети, так как все соединения должны проходить через МЭ и в некоторых случаях изучаться МЭ;

– отсутствие встроенных механизмов защиты от вирусов. Традиционные МЭ не могут защитить от пользователей, загружающих зараженные вирусами программы для ПЭВМ из интернетовских архивов или при передаче таких программ в качестве приложений к письму;

– отсутствие эффективной защиты от получаемого из Internet опасного содержимого. Специфика мобильного кода такова, что он может быть использован как средство для проведения атак. Мобильный код может быть реализован в виде:

- вируса, который вторгается в ИС и уничтожает данные на локальных дисках, постоянно модифицируя свой код и затрудняя тем самым свое обнаружение и удаление;
- агента, перехватывающего пароли, номера кредитных карт и т.п.;
- программы, копирующей конфиденциальные файлы, содержащие деловую и финансовую информацию и пр.;

– МЭ не может защитить от ошибок и некомпетентности администраторов и пользователей;

– традиционные МЭ являются средствами, блокирующими атаки. В большинстве случаев они защищают от атак, которые уже находятся в процессе осуществления. Для организации упреждения атак необходимо использовать средства обнаружения атак и поиска уязвимостей, которые будут своевременно обнаруживать и рекомендовать меры по устранению «слабых мест» в системе защиты.

10. ИСПОЛЬЗОВАНИЕ VPN ДЛЯ ЗАЩИТЫ ТРАФИКА

10.1. Сущность и содержание технологии виртуальных частных сетей

Виртуальная частная сеть (VPN – Virtual Private Network) – технология безопасного подключения к корпоративной сети через Интернет.

В основе концепции построения защищенных виртуальных частных сетей VPN лежит достаточно простая идея: если в глобальной сети есть два узла, которые хотят обменяться информацией, то для обеспечения конфиденциальности и целостности передаваемой по открытым сетям информации между ними необходимо построить виртуальный туннель, доступ к которому должен быть чрезвычайно затруднен всем возможным активным и пассивным внешним наблюдателям. Термин «виртуальный» указывает на то, что соединение между двумя узлами сети не является постоянным и существует только во время прохождения трафика по сети.

Преимущества, получаемые компанией при формировании таких виртуальных туннелей, заключаются, прежде всего, в значительной экономии финансовых средств.

Технология виртуальных частных сетей является одним из эффективных механизмов обеспечения информационной безопасности при передаче данных в распределенных вычислительных сетях.

Виртуальные частные сети являются комбинацией нескольких самостоятельных механизмов безопасности:

– шифрования на выделенных шлюзах (шлюз обеспечивает обмен данными между вычислительными сетями, функционирующими по разным протоколам);
– экранирования (с использованием межсетевых экранов);
– туннелирования.

Сущность технологии VPN заключается в следующем (рис. 10.1) [14]:

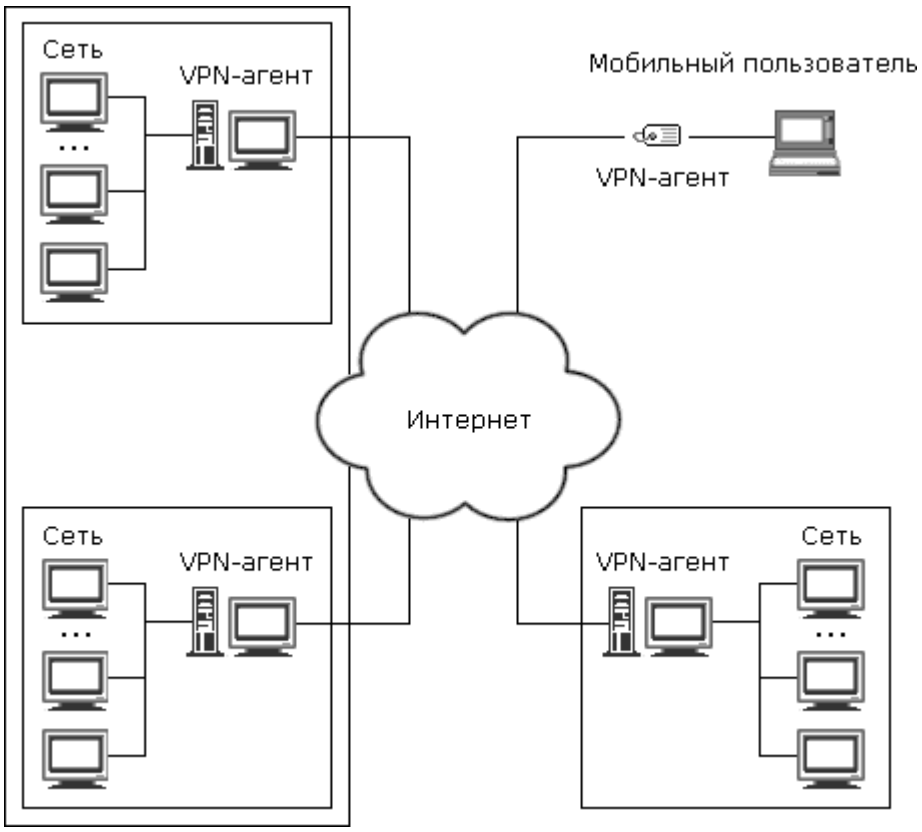

Рис. 10.1. Сущность технологии VPN

На все компьютеры, имеющие выход в Интернет (вместо Интернета может быть и любая другая сеть общего пользования), устанавливается VPN-агенты, которые обрабатывают IP-пакеты, передаваемые по вычислительным сетям.

Перед отправкой IP-пакета VPN-агент выполняет следующие операции:

– анализирует IP-адрес получателя пакета, в зависимости от этого адреса выбирается алгоритм защиты данного пакета. Пакет может игнорироваться, если в настройках VPN-агента такой получатель не значится;

– вычисляет и добавляет в пакет его имитоприставка, обеспечивающая контроль целостности передаваемых данных;

– шифрует пакет (целиком, включая заголовок IP-пакета, содержащий служебную информацию);

– формирует новый заголовок пакета, где вместо адреса получателя указывается адрес его VPN-агента (инкапсуляция пакета).

В результате этого обмен данными между двумя локальными сетями снаружи представляется как обмен между двумя компьютерами, на которых установлены VPN-агенты. Всякая

полезная для внешней атаки информация, например, внутренние IP-адреса сети, в этом случае недоступна.

При получении IP-пакета выполняются обратные действия:

– из заголовка пакета извлекается информация о VPN-агенте отправителя пакета, если такой отправитель не входит в число разрешенных, то пакет отбрасывается;

– согласно настройкам выбираются криптографические алгоритмы и ключи, после чего пакет расшифровывается и проверяется его целостность (пакеты с нарушенной целостностью также отбрасываются);

– после всех обратных преобразований пакет в его исходном виде отправляется настоящему адресату по локальной сети.

Все перечисленные операции выполняются автоматически, работа VPN-агентов является незаметной для пользователей. Сложной является только настройка VPN-агентов, которая может быть выполнена только очень опытным пользователем. VPN-агент может находиться непосредственно на защищаемом компьютере (что особенно полезно для мобильных пользователей). В этом случае он защищает обмен данными только одного компьютера, на котором он установлен.

Для передачи данных VPN-агенты создают виртуальные каналы между защищаемыми локальными сетями или компьютерами (такой канал называется «туннелем», а технология его создания называется «**туннелированием**»). Вся информация передается по туннелю в зашифрованном виде.

Одной из обязательных функций VPN-агентов является фильтрация пакетов. Фильтрация пакетов реализуется в соответствии с настройками VPN-агента, совокупность которых образует политику безопасности виртуальной частной сети. Для повышения защищенности виртуальных частных сетей на концах туннелей целесообразно располагать межсетевые экраны.

Классификация VPN

Наиболее часто используются три признака классификации VPN [43]:

– рабочий уровень модели OSI;

– конфигурация структурно-технического решения;

– способ технической реализации.

Классификация VPN по рабочему уровню ЭМВОС

Для технологий безопасной передачи данных по незащищенной сети применяют обобщенное название – защищенный канал.

Защищенный канал можно построить с помощью системных средств, реализованных на разных уровнях эталонной модели взаимодействия открытых систем (ЭМВОС, OSI).

От выбранного уровня OSI во многом зависит функциональность реализуемой VPN и ее совместимость с приложениями ИС, а также с другими средствами защиты. По признаку рабочего уровня модели OSI различают следующие группы VPN:

– VPN второго (канального) уровня;
– VPN третьего (сетевого) уровня;
– VPN пятого (сеансового) уровня.

VPN строятся на достаточно низких уровнях модели OSI. Причина этого в том, что чем ниже в стеке реализованы средства защищенного канала, тем проще их сделать прозрачными для приложений и прикладных протоколов. Однако здесь возникает другая проблема – зависимость протокола защиты от конкретной сетевой технологии.

Если для защиты данных используется протокол одного из верхних уровней (прикладного или представительного), то такой способ защиты не зависит от того, какие сети (IP или IPX, Ethernet или ATM) применяются для транспортировки данных, что можно считать несомненным достоинством. С другой стороны, приложение при этом становится зависимым от конкретного протокола защиты, то есть для приложений подобный протокол не является прозрачным.

Защищенному каналу на прикладном уровне свойствен еще один недостаток – ограниченная область действия.

Протокол защищает только вполне определенную сетевую службу – файловую, гипертекстовую или почтовую. Поэтому для каждой службы необходимо разрабатывать соответствующую защищенную версию протокола.

На верхних уровнях модели OSI существует жесткая связь между используемым стеком протоколов и приложением.

10.2 Классификация VPN по архитектуре технического решения

По архитектуре технического решения принято выделять три основных вида виртуальных частных сетей:

- VPN с удаленным доступом;
- внутрикорпоративные VPN;
- межкорпоративные VPN.

Виртуальные частные сети с удаленным доступом предназначены для обеспечения защищенного удаленного доступа к корпоративным информационным ресурсам мобильным и/или удаленным сотрудникам компании.

Внутрикорпоративные VPN предназначены для обеспечения защищенного взаимодействия между подразделениями внутри предприятия или между группой предприятий, объединенных корпоративными сетями связи, включая выделенные линии.

Межкорпоративные VPN обеспечивают сотрудникам предприятия защищенный обмен информацией со стратегическими партнерами по бизнесу, поставщиками, крупными заказчиками, пользователями, клиентами и т.д. Они обеспечивает прямой доступ из сети одной компании к сети другой, тем самым способствуя повышению надежности связи, поддерживаемой в ходе делового сотрудничества. В межкорпоративных сетях большое значение придается контролю доступа посредством межсетевых экранов и аутентификации пользователей.

Классификация VPN по способу технической реализации

По способу технической реализации различают:

- VPN на основе сетевой операционной системы;
- VPN на основе межсетевых экранов;
- VPN на основе маршрутизаторов;
- VPN на основе программных решений;
- VPN на основе специализированных аппаратных средств со встроенными шифропроцессорами.

VPN на основе сетевой ОС

Реализацию VPN на основе сетевой ОС можно рассмотреть на примере операционной системы Windows. Для создания VPN компания Microsoft предлагает протокол PPTP, интегрированный в сетевую операционную систему Windows. Такое решение выглядит привлекательно для организаций, использующих Windows в качестве

корпоративной ОС. В сетях VPN, основанных на Windows, используется база данных клиентов, хранящаяся в контроллере PDC.

Для шифрования применяется нестандартный фирменный протокол Point-to-Point Encryption с 40-битовым ключом, получаемым при установлении соединения.

В качестве достоинства приведенной схемы следует отметить, что стоимость решения на основе сетевой ОС значительно ниже стоимости других решений.

Несовершенство такой системы – недостаточная защищенность протокола PPTP.

VPN на основе маршрутизаторов

Данный способ построения VPN предполагает применение маршрутизаторов для создания защищенных каналов. Поскольку вся информация, исходящая из локальной сети, проходит через маршрутизатор, то вполне естественно возложить на него и задачи шифрования.

VPN на основе межсетевых экранов

Межсетевые экраны большинства производителей содержат функции туннелирования и шифрования данных. К программному обеспечению собственно межсетевого экрана добавляется модуль шифрования.

К недостаткам этого метода относятся высокая стоимость решения в пересчете на одно рабочее место и зависимость производительности от аппаратного обеспечения, на котором работает межсетевой экран. При использовании межсетевых экранов на базе ПК надо помнить, что подобный вариант подходит только для небольших сетей с ограниченным объемом передаваемой информации.

VPN на основе программного обеспечения

Для построения сетей VPN также применяются программные решения. При реализации подобных схем используется специализированное ПО, работающее на выделенном компьютере и в большинстве случаев выполняющее функции proxy-сервера. Компьютер с таким программным обеспечением может быть расположен за межсетевым экраном,

VPN на основе специализированных аппаратных средств со встроенными шифропроцессорами

Вариант построения VPN на специализированных аппаратных средствах может быть использован в сетях, требующих высокой

производительности. Недостаток подобного решения – его высокая стоимость.

10.3. Технические и экономические преимущества внедрения технологий VPN

Технология VPN позволяет эффективно решать задачи, связанные с циркуляцией конфиденциальной информации по каналам связи. Она обеспечивает связь между сетями, а также между удаленным пользователем и корпоративной сетью с помощью защищенного канала (туннеля), «проложенного» в общедоступной сети Internet.

Таким образом, на современном этапе развития, в условиях, когда филиалы одного и того же предприятия находятся на значительном удалении друг от друга, потребность в оперативном и надежном обмене информацией стала наиболее острой. Использование дорогих высокопропускных каналов связи не всегда оказывается целесообразным и экономически выгодным. Развитие же средств связи, особенно недорогих и наиболее доступных (например, Internet), приводит к тому, что их практическое использование, особенно предприятиями, становится все более массовым. В этих условиях становится заманчивым их использование для передачи ценной корпоративной информации, убытки от потери или искажения которой могут пагубно сказаться на деятельности компании. Поэтому использование защищенных виртуальных частных сетей VPN с учетом всех их достоинств становится все более актуальным и жизненно необходимым. Концепция таких сетей позволяет организовывать столь необходимый обмен информацией внутри компании и с клиентами при наилучшем сочетании производительности, оперативности, защищенности и стоимости.

ЗАКЛЮЧЕНИЕ

Содержание предлагаемого учебного пособия «Основы информационной безопасности сетей и систем» отражает основные направления деятельности по обеспечению защиты информации в компьютерных системах различных видов. Одна из главных задач, которая стояла перед авторами, наряду с изложением общих теоретических основ, дать необходимые конкретные рекомендации для проведения работ по обеспечению информационной безопасности компьютерных систем.

В результате проведения работ по защите информации в компьютерных системах предоставляются следующие возможности:

1. **Руководителям организаций** обеспечить формирование единой политики и концепции безопасности организации по защите информации; объективно и независимо оценить текущий уровень информационной безопасности данных, имеющихся в организации.

2. **Начальникам отделов информатизации и отделов безопасности организации** сформировать требования по защите информации, обрабатываемой в организации, выработать и обосновать необходимые меры организационного характера, такие как меры по защите информации от утечки по техническим каналам, определить перечень необходимых работ по обеспечению информационной безопасности, разработать пакет документов, связанных с обработкой и хранением информации ограниченного доступа.

3. **Системным, сетевым администраторам и администраторам безопасности организаций и предприятий** объективно оценить безопасность всех основных компонентов и сервисов систем обработки, хранения и передачи информации ограниченного доступа, выбрать при необходимости технические средства её защиты.

4. **Сотрудникам и работникам организаций и предприятий** определить свои основные функциональные обязанности и, что особенно важно, зоны ответственности, в том числе финансовой, за надлежащее использование информационных ресурсов и состояние политики безопасности предприятия.

СПИСОК ИСПОЛЬЗОВАННОЙ И РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. Аверченков, В.И. Аудит информационной безопасности: учеб. пособие/В.И. Аверченков. – Брянск: БГТУ, 2005. – 269 с.
2. Аверченков, В.И. Организационная защита информации: учеб. пособие/В.И. Аверченков, М.Ю. Рытов – Брянск: БГТУ, 2005. – 184с.
3. Аверченков, В.И. Системы защиты информации в ведущих зарубежных странах: учеб. пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. – Брянск: БГТУ, 2007. – 225 с
4. Аверченков, В.И., Служба защиты информации: организация и управление: учеб. пособие / В.И. Аверченков, М.Ю. Рытов. – Брянск: БГТУ, 2005. – 186с.
5. Аграновский А.В., Хади Р.А. Новый подход к защите информации – системы обнаружения компьютерных угроз / Jet Info, 2007 г., №4.
6. Азарченков, А.А, Информатика: Основы защиты информации в компьютерных системах [Текст] + [Электронный ресурс]: учеб. пособие / А.А. Азарченков, М.Л. Гулак, С.Н. Зимин. – Брянск: БГТУ, 2014. –69с
7. Астаханов А. Актуальные вопросы выявления сетевых атак.
8. Астахов А. Анализ защищенности корпоративных автоматизированных систем // Jet Info. Информационный бюллетень, №7 (110), 2002г.
9. Астахов И. Разработка эффективных политик информационной безопасности // Директор информационной службы №01, 2004.
10. Барабанов А., Марков А., Цирлов В. Сертификация систем обнаружения вторжений «Открытые системы», № 03, 2012.
11. Биячуев Т.А. / под ред. Л.Г. Осовецкого. Безопасность корпоративных сетей. – СПб: СПб ГУ ИТМО, 2004. –161 с.
12. Гайдамакин Н.А. Теоретические основы компьютерной безопасности: Учебное пособие. –Екатеринбург, Изд-во Урал. ун-та. 2008.
13. Галатенко А.В. Активный аудит. //JetInfo N8, 1999.

14. Галатенко В.А. Основы информационной безопасности. М.: ИНТУИТ.РУ. – 2006.

15. Галатенко В.А. Основы информационной безопасности: Курс лекций. –М.: ИНТУИТ.ру, 2003. –280 с.

16. Грязнов Е., Панасенко С. Безопасность локальных сетей – Электрон. журнал "Мир и безопасность" №2, 2003. – Режим доступа к журн.: www.daily.sec.ru.

17. Гулак, М.Л. Основы компьютерной безопасности [Текст] + [Электронный ресурс]: учебное пособие/ М.Л. Гулак, М.Ю. Рытов – Брянск: БГТУ, 2013. – 216 с.

18. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности – М.: Радио и связь -2000.

19. Завгородний В.И. Комплексная защита информации в компьютерных системах. М.: «Логос» – 2001.

20. Загинайлов Ю.Н. Комплексная система защиты информации на предприятии: учебно-методическое пособие / Ю.Н. Загинайлов и др., –Алт.гос.техн.ун-т им. И.И. Ползунова. –Барнаул: АлтГТУ. –2010. –287с.

21. Зима В. М., Молдовян А. А., Молдовян Н. А. Безопасность глобальных сетевых технологий. СПб.: БХВ-Петербург, 2001.

22. Зима В.М., Котухов М.М., Ломако А.Г. и др. Разработка систем информационно-компьютерной безопасности. –СПб: ВКА им. А.Ф. Можайского, 2003. –327 с.

23. Карпов Е.А., Котенко И.В., Котухов М.М. и др. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем и информационно-вычислительных сетей / Под редакцией И.В. Котенко. – СПб.: ВУС, 2000.

24. Касперский Е. Компьютерные вирусы в MS-DOS. – М.: Эдель, 1992.

25. Касперский Е. Компьютерные вирусы, 2003. – Электронная энциклопедия. – Режим доступа к энциклопедии: www.viruslist.com/viruslistbooks.html.

26. Конеев И. Политики информационной безопасности // Директор информационной службы №11, 2007.

27. Костров Д. Системы обнаружения атак, URL: www.ByteMag.ru

28. Лукацкий А. Мир атак многообразен, URL: www.Sec.ru

29. Лукацкий А. Обнаружение атак своими силами, URL: www.Sec.ru

30. Лукацкий А. Обнаружение атак. СПб.: БХВ-Петербург, 2003.

31. Лукацкий А. Системы обнаружения атак, URL: www.Sec.ru

32. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. М.: «Горячая Линия – Телеком» – 2001.

33. Медведовский И.Д. Программные средства проверки и создания политики безопасности. –SecurityLab, 2004.

34. Милославская Н.Г., Толстой А.И. Интрасети: обнаружение вторжений. М.: ЮНИТИ-ДАНА, 2001.

35. Новиков Ю.В., Кондратенко С. В. Локальные сети: архитектура, алгоритмы, проектирование. – М.: ЭКОМ, 2001.

36. Олифер В.Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы. – СПб: Питер, 2000.

37. Политика безопасности при работе в Интернет: Техническое руководство / Б. Гутман, Р. Бэгвилл; Пер. с англ. Казенова В.Н. –NIST Special Publication 800-12.

38. Симонов С. Аудит безопасности ИС. – Info Jet, 1999. -№ 9. -24 с.

39. Спортак М., Паппас Ф. Компьютерные сети и сетевые технологии. – М.: ТИД "ДС", 2002.

40. Таили Э. Безопасность персонального компьютера. - Мн.: ООО «Попурри», 1997. - 480 с.

41. Таназ М. Анализ сигнатур или анализ протоколов, что лучше? URL: www.SecurityLab.ru

42. Тихонов А. Системы обнаружения вторжений, URL: www.Isoft.com.ru

43. Управление информационной безопасностью: Практические правила –Info Jet, приложение, 1999.

44. Фролов А. В., Фролов Г. В. Осторожно: компьютерные вирусы. – М.: ДИАЛОГ-МИФИ, 1996.

45. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. –М.: ИД «ФОРУМ»: ИНФРА-М, 2008. –416 с.

46. Щербаков А.Ю. Введение в теорию и практику компьютерной безопасности. – М.: Издательство Молгачева С.В., 2001.

47. Curry D., Kirkpatrick S., Longstaff T. Руководство по информационной безопасности предприятия. Site Security Handbook, RFC 1244.

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

49. ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».

50. Комментарии к Российскому стандарту ГОСТ Р ИСО/МЭК 15408-2002 «Критерии оценки безопасности информационных технологий» / Долинин М.Ю., Кобзарь М.Т., Лыков В.А. и др. –М.: ФГУП «ЦНИИАТОМИН-ФОРМ», 2003. –38с.

51. Руководящий документ. Безопасность информационных технологий –Руководство по разработке профилей защиты и заданий по безопасности. –М.: Гостехкомиссия России, 2003.

52. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. –М.: Гостехкомиссия России, 2002. –Части 1, 2, 3.

53. www.jetinfo.ru.

54. www.ISACA.ru.

55. Политика информационной безопасности. Информационный ресурс: http://www.sgqconsulting.ru/3-8-7-1-information-security-policies.htm

56. http://www.practice-group.com/content/view/10849/

ГЛОССАРИЙ

Автоматизированная информационная система, АИС [Automated information system (AIS)] – совокупность программных и аппаратных средств, предназначенных для создания, передачи, обработки, распространения, хранения и/или управления данными и информацией и производства вычислений.

Автоматизированная система (АС) – комплекс программных и технических средств, предназначенных для автоматизации различных процессов, связанных с деятельности человека. При этом человек является звеном системы.

Авторизация [Authorization] (1) – предоставление доступа пользователю, программе или процессу.

Авторизация [Authorization] (2) – предоставление определенных полномочий лицу (группе лиц) на выполнение некоторых действий в системе обработки данных.

Авторизация данных [Data authorization] – определение и установление степени приватности данных в базе данных.

Авторизация программы [Program authorization] – установление ограничения на доступ к системной или пользовательской программе со стороны других программ и пользователей.

Администратор базы данных [Data administrator] (1) – специальное должностное лицо (группа лиц), имеющий(ие) полное представление о базе данных и отвечающее за ее ведение, использование и развитие. Входит в состав администрации банка данных.

Администратор базы данных [Data administrator] (2) – лицо, имеющее полное представление о данных, используемых в учреждении (на предприятии), и отвечающее за хранение, обновление и организацию их использования.

Администратор доступа [Access administrator] – одно из должностных лиц в составе администрации банка данных, отвечающее за организацию доступа пользователей к базам данных.

Администратор защиты [Security administrator] – субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.

Администратор системы (системный администратор) [Systemadministrator] – лицо, отвечающее за эксплуатацию системы и поддержание ее в работоспособном состоянии

Администратор службы безопасности – человек (или группа людей), имеющий(ие) полное представление об одной или нескольких системах обеспечения безопасности и контролирующий(ие) проектирование и их использование.

Администратор СОВ – уполномоченный пользователь, ответственный за установку, администрирование и эксплуатацию ОО (СОВ).

Администрация банка данных [Databank administratoin] – группа лиц (подразделение), отвечающих за эксплуатацию банка данных: ведение баз данных, организацию коллективного доступа к ним пользователей и развитие системы.

Администрация системы [System administration] – пользователь сети, деятельность которого связана с управлением системами.

Активная угроза [Active threat] – угроза преднамеренного несанкционированного изменения состояния системы.

Активное скрытие [active hiding] – способ технической защиты информации, Активное содержимое – WWW-страницы, которые содержат ссылки на программы, что загружаются и выполняются автоматически WWW-браузерами.

Анализ риска [Risk analysis] (1) – процесс изучения характеристик и слабых сторон системы, проводимый с использованием вероятностных расчетов, с целью определения ожидаемого ущерба в случае возникновения неблагоприятных событий. Задача анализа риска состоит в определении степени приемлемости того или иного риска в работе системы.

Анализ риска [Risk analysis] (2) – процесс определения угроз безопасности системы и отдельным ее компонентам, определения их характеристик и потенциального ущерба, а также разработка контрмер.

Анализ трафика (рабочей нагрузки) линии связи [Traffic analysis] – исследование наблюдаемых потоков данных, проходящих между пунктами посети связи (наличие, отсутствие, объем, направление, частота).

Анализатор СОВ – программный или программно-технический компонент СОВ, предназначенный для сбора информации от сенсоров (датчиков) СОВ, ее итогового анализа на предмет обнаружения вторжения (атаки) на контролируемую ИС.

Аппаратная защита [Hardware security] – использование аппаратных средств, например, регистров границ или замков и ключей для защиты данных в ЭВМ.

Аппаратное средство защиты информации – специальное защитное устройство или приспособление, входящее в комплект технического средства обработки информации.

Аппаратные средства защиты – механические, электромеханические, электронные, оптические, лазерные, радио, радиотехнические, радиолокационные и другие устройства, системы и сооружения, предназначенные для защиты информации от несанкционированного доступа, копирования, кражи или модификации.

Апплеты – небольшие приложения, написанные на различных языках программирования, которые автоматически загружаются и выполняются WWW-браузерами, поддерживающими апплеты

Атрибут [Attribute] – 1) Признак, описатель данных, содержащий одну из характеристик данного: имя, тип, длину, количество, форму представления, систему счисления. 2) Поименованное свойство одного или нескольких объектов.

Атрибут файла [File attribute] – характеристика, определяющая файл: имя, размер, организация (тип), метод доступа, длина записи, тип записи и др.

База решающих правил – составная часть СОВ, содержащая информацию о вторжениях (сигнатуры), на основе которой СОВ принимает решение о наличии вторжения (атаки).

Безопасная операционная система [Secure operating system] – операционная система, эффективно управляющая аппаратными и программными средствами с целью обеспечения уровня защиты, соответствующего содержанию данных и ресурсов, контролируемых этой системой.

Безопасное состояние [secure state] – условие, при выполнении которого ни один субъект не может получить доступ ни к какому объекту иначе как на основе проверки имеющихся у него полномочий.

Безопасность [Safety (security)] (1) – свойство системы противостоять внешним или внутренним дестабилизирующим факторам, следствием воздействия которых могут быть нежелательные ее состояния или поведение.

Безопасность [Safety (security)] (2) – состояние, в котором файлы данных и программы не могут быть использованы, просмотрены и модифицированы неавторизованными лицами (включая персонал системы), компьютерами или программами. Безопасность обеспечивается путем создания вокруг компьютера и оборудования защищенной зоны, в которой работает только авторизованный персонал, а также использования специального программного обеспечения и встроенных в операционные процедуры механизмов защиты.

Безопасность автоматизированной информационной системы [Automated information system security] – совокупность мер управления и контроля, защищающая APIS от отказа в обслуживании и несанкционированного (умышленного или случайного) раскрытия, модификации или разрушения АИС и данных.

Безопасность данных [Data security] (1) – защита данных от несанкционированной (случайной или намеренной) модификации, разрушения или раскрытия.

Безопасность данных [Data security] (2) – свойство компьютерной системы противостоять попыткам несанкционированного доступа к обрабатываемой и хранимой информации. Безопасность достигается применением аппаратных, программных и криптографических методов и средств защиты, а также комплексом организационных мероприятий. Одним из показателей безопасности является безопасное время.

Безопасность информации [Information security] (1) – состояние информации, при котором исключаются случайные или преднамеренные несанкционированные воздействия на информацию или несанкционированное ее получение.

Безопасность информации [Information security] (2) – состояние уровня защищенности информации при ее обработке техническими средствами, обеспечивающее сохранение таких ее качественных характеристик (свойств) как секретность /конфиденциальность/, целостность и доступность.

Безопасность информации [Information security] (3) – состояние защищенности информации, обрабатываемой средствами вычислительной техники, или автоматизированной системы от внутренних или внешних угроз.

Безопасность информации в ИС – защищенность информации и оборудования ИС от факторов, представляющих угрозу для:

конфиденциальности (обеспечение санкционированного доступа); целостности; доступности.

Безопасность информационная – способность системы противостоять случайным или преднамеренным, внутренним или внешним информационным воздействиям, следствием которых могут быть ее нежелательное состояние или поведение.

Безопасность информационной сети [Network security] – меры, предохраняющие информационную сеть от несанкционированного доступа, случайного или преднамеренного вмешательства в нормальные действия или попыток разрушения ее компонентов.

Безопасность информационной системы [Information system security] – свойство информационной системы противостоять попыткам несанкционированного доступа. Совокупность элементов, необходимых для обеспечения адекватной защиты компьютерной системы; включает аппаратные и/или программные функции, характеристики и средства; операционные и учетные процедуры, средства управления доступом на центральном компьютере, удаленных компьютерах и телекоммуникационных средствах; административные мероприятия, физические конструкции и устройства; управление персоналом и коммуникациями.

Безопасность компьютерных систем [Computer security] – свойство компьютерных систем противостоять попыткам несанкционированного доступа к обрабатываемой и хранимой информации, вводу информации, приводящей к деструктивным действиям, и навязыванию ложной информации.

Безопасность связи [Communication security] – свойство систем связи противостоять попыткам несанкционированного доступа к обрабатываемой и хранимой информации, вводу информации, приводящей к деструктивным действиям, навязыванию ложной информации.

Блокировка доступа – запрещение доступа к ограниченному участку памяти, например, дорожке диска, вследствие обнаруженных на этом участке дефектов. Выполняется программными или аппаратными средствами.

Брандмауэр (1) – метод защиты сети от угроз безопасности, исходящих от других систем и сетей, с помощью централизации доступа к сети и контроля за ним аппаратно-программными средствами.

Брандмауэр (2) – является защитным барьером, состоящим из нескольких компонентов (например, маршрутизатора или шлюза, на котором работает программное обеспечение брандмауэра). Брандмауэр конфигурируется в соответствии с принятой в организации политикой контроля доступа к внутренней сети. Все входящие и исходящие пакеты должны проходить через брандмауэр, который пропускает только авторизованные пакеты.

Брандмауэр с фильтрацией пакетов [packet-filtering firewall] – является маршрутизатором или компьютером, на котором работает программное обеспечение, сконфигурированное таким образом, чтобы отбраковывать определенные виды входящих и исходящих пакетов. Фильтрация пакетов осуществляется на основе информации, содержащейся в TCP- и IP- заголовках пакетов (адреса отправителя и получателя, их номера портов и др.).

Брандмауэр экспертного уровня [stateful inspecthion firewall] – проверяет содержимое принимаемых пакетов на трех уровнях модели OSI – сетевом, сеансовом и прикладном. Для выполнения этой задачи используются специальные алгоритмы фильтрации пакетов, с помощью которых каждый пакет сравнивается с известным шаблоном авторизованных пакетов.

Брешь безопасности [security flaw] – ошибка при назначении полномочий или упущение при разработке, реализации или управлении средствами защиты системы, которые могут привести к преодолению защиты.

Ведение базы данных [Database maintenance] – деятельность, направленная на обновление и восстановление базы данных, а также на перестройку ее структуры) (ДСТУ 2874).

Вспомогательные технические средства и системы (ВТСС) – технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, устанавливаемые совместно с ОТСС или в выделенных помещениях. К ним относятся: различного рода телефонные средства и системы; средства и системы передачи данных в системе радиосвязи; средства и системы охранной и пожарной сигнализации; средства и системы оповещения и сигнализации; контрольно-измерительная аппаратура; средства и системы кондиционирования; средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения (абонентские громкоговорители,

системы радиовещания, телевизоры и радиоприемники и т.д.); средства электронной оргтехники.

Вставка [Insertion] – операция добавления к множеству (массиву, списку, файлу) нового элемента.

Вставка в программу (заплата) [Patch] – изменение в программе, которое важно внести наиболее удобным и быстрым способом, обращая меньше внимания на защиту данных ради временного восстановления работоспособности программы с целью последующего ее исправления. Часто на этапе тестирования незначительные ошибки исправляются с помощью заплат, что бы без долгих задержек продолжить тестирование, не компилируя программу каждый раз повторно. Впоследствии все необходимые изменения вносятся в исходный текст программы, которая затем компилируется повторно только один раз.

Вторжение (атака) – действие, целью которого является осуществление несанкционированного доступа к информационным ресурсам.

Вызов [Call (calling)] – действие по активизации машинной программы,

Вычислительная сеть (сеть ЭВМ) [Network] – система взаимосвязанных между собой ЭВМ, а также технического и программного обеспечения для их взаимодействия.

Государственная тайна – сведения, охраняемые государством, разглашение которых может оказать отрицательное воздействие на качественное состояние военно-экономического потенциала страны или повлечь другие тяжкие последствия для ее обороноспособности, государственной безопасности, экономических и политических интересов. К государственной тайне относится секретная информация с грифами "особой важности" и "совершенно секретно".

Данные СОВ – данные, собранные или созданные СОВ в результате выполнения своих функций.

Датчик (сенсор) СОВ – программный или программно-технический компонент СОВ, предназначенный для сбора и первичного анализа информации (данных) о событиях в контролируемой ИС, а также – передачи этой информации (данных) анализатору СОВ.

Двудомный шлюз [Dual-homed gateway] – компьютер, на котором работает программное обеспечение брандмауэра и который имеет две сетевые интерфейсные платы: одна подключена к

внутренней сети, а другая – к внешней. Шлюз передает информацию из одной сети в другую, исключая прямое взаимодействие между ними. Шлюзы сеансового и прикладного уровня относятся к двудомным шлюзам.

Демон [Daemon] – программа, которая контролирует работу другой программы и время от времени прерывает ее работу, не разрушая саму программу (чаще всего это программа управления периферийными устройствами).

Доверительность [Trusted funcionality] – свойство соответствия безопасности некоторым критериям.

Домен безопасности [Secyrity domain] – ограниченная группа объектов и субъектов безопасности, к которым применяется одна методика безопасности со стороны одного и того же администратора безопасности.

Дыра [Loophole] – в вычислительной технике недоработки, ошибки в программном обеспечении или аппаратуре, позволяющие обойти процессы управления доступом.

Задание по безопасности – совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного ОО.

Защищенность – в вычислительной технике способность системы противостоять несанкционированному доступу к программам и данным (безопасность, секретность), а также их случайному искажению или разрушению (целостность).

Защищенные средства [protected facilities] – основные и вспомогательные технические средства, в которых предусмотрено предотвращение осуществления угроз информации.

Защищенные средства вычислительной техники (защищенные автоматизированные системы) [Trusted computer system] – средство вычислительной техники (автоматизированная система), в котором реализован комплекс средств защиты.

Информация (для процесса обработки данных) [information (in data processing)] – любые знания о предметах, фактах, понятиях и т.д. проблемной области, которыми обмениваются пользователи системы обработки данных.

Категория безопасности информации – уровень безопасности информации, определяемый установленными нормами в зависимости от важности (ценности) информации.

Категория защиты информации – качественный показатель, отражающий степень важности защиты информации в выбранной шкале ценностей.

Контроль средств защиты [Security audit] – инспекция системных записей и работы персонала с целью проверки функционирования систем защиты, их соответствия принятой стратегии требованиям эксплуатации, а также выработки соответствующих рекомендаций.

Нештатная ситуация – ситуация, возникающая в процессе работы вычислительной системы, но не предусмотренная программной документацией.

Обмен данными [Data commuunication] – процедура приема и передачи данных, включая кодирование, декодирование буферизацию и проверку.

Объект вычислительной техники (ВТ) – стационарный или подвижный объект, который представляет собой комплекс средств вычислительной техники, предназначенный для выполнения определенных функций обработки информации к объектам вычислительной техники относятся автоматизированные системы (АС), автоматизированные рабочие места (АРМ) информационно-вычислительные центры (ИВЦ) и другие комплексы средств вычислительной техники. К объектам вычислительной техники могут быть отнесены также отдельные средства вычислительной техники, выполняющие самостоятельные функции обработки информации.

Объект защиты – обобщающий термин для всех форм существования информации, требующих защиты от технических разведок. По своему составу объекты защиты могут быть единичными и групповыми.

Объект оценки – подлежащая сертификации (оценке) СОВ уровня сети с руководствами по эксплуатации.

Основные технические средства и системы (ОТСС) – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной (секретной) информации. К ОТСС могут относиться средства и системы информатизации (средства вычислительной техники, автоматизированные системы различного уровня и назначения на базе средств вычислительной техники, в том числе информационно-вычислительные комплексы, сети и системы, средства и системы связи и передачи данных), технические средства

приема, передачи и обработки информации (телефонии, звукозаписи, звукоусиления, звуковоспроизведения переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической видео-, смысловой и буквенно-цифровой информации) используемые для обработки конфиденциальной (секретной) информации.

Оценка риска [Risk assessment] – количественная или качественная оценка повреждения, которое может произойти, если вычислительная система не защищена от определенных угроз. Количественная оценка риска может рассчитываться на основе финансовых потерь, которые могут иметь место, если каждая конкретная угроза будет приводить в действие любой из возможных механизмов уязвимости системы.

Подстановка трафика [Traffic padding] – установление поддельных соединений, генерация фальшивых блоков данных и (или) отдельных фальшивых данных внутри блоков данных.

Политика безопасности ОО – совокупность правил, регулирующих управление, защиту и распределение информационных ресурсов, контролируемых ОО.

Протокол [Protocol] (1) – согласованная процедура передачи данных между различными объектами вычислительной системы; обычно употребляется в сочетании ISO protocol протокол Международной организации по стандартизации.

Протокол [Protocol] (2) – набор правил и форматов, семантических и синтаксических, позволяющих различным компонентам системы обмениваться информацией (например, узлам сети).

Протокол Gopher – разработан для того, чтобы позволить пользователю передавать текстовые и двоичные файлы между компьютерами в сети.

Протокол Telnet – используется для терминального (возможно удаленного) подключения к хосту.

Протокол безопасной передачи данных [SSL] – разработан Netscape Communications, Inc. Этот протокол использует межконцевое шифрование трафика на прикладном уровне.

Протокол передачи гипертекста [HTTP] – базовый протокол WWW, использующийся для передачи гипертекстовых документов.

Протокол передачи файлов [FTP] – используется для передачи файлов по сети.

Профиль защиты – совокупность требований безопасности для СОВ уровня сети.

Путь проникновения [Penetration route] – последовательность не санкционированных действий пользователя при его проникновении в защищенную вычислительную систему.

Сервер-посредник [Proxy server] – брандмауэр, в котором для преобразования IP-адресов всех авторизованных клиентов в IP-адреса, ассоциированные с брандмауэром, используется процесс, называемый трансляцией адресов (address translation).

Сигнатура – характерные признаки вторжения (атаки), используемые для его (ее) обнаружения.

Сигнатура [Signature] – уникальная характеристика системы, которая может быть проверена. Примером сигнатуры может служить признак диска, используемый в качестве идентификационной метки диска-оригинала; этот признак не должен копироваться программным способом.

Система обнаружения вторжений (СОВ) – программное или программно-техническое средство, реализующие функции автоматизированного обнаружения (блокирования) действий в информационной системе, направленных на преднамеренный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней.

Средства вычислительной техники – электронные вычислительные машины и комплексы, персональные электронные вычислительные машины, в том числе программные средства, периферийное оборудование, устройства телеобработки данных.

Средства информатизации – средства вычислительной техники и связи, оргтехники, предназначенные для сбора, накопления, хранения, поиска, обработки данных и выдачи информации потребителю.

Стратегия защиты [Security policy] – формальное определение критериев, особенно оперативных, которыми следует руководствоваться при обеспечении защиты системы от известных угроз.

Техническое средство защиты информации – техническое средство, предназначенное для устранения или ослабления

демаскирующих признаков объекта, создания ложных (имитирующих) признаков, а также для создания помех техническим средством доступа информации.

Техническое средство обработки информации (ТСОИ) – техническое средство, предназначенное для приема, хранения, поиска, преобразования, отображения и/или передачи информации по каналам связи. К ТСОИ относятся средства вычислительной техники, средства и системы связи средства записи, усиления и воспроизведения звука, переговорные и телевизионные устройства, средства изготовления и размножения документов, кинопроекционная аппаратура и другие технические средства, связанные с приемом, накоплением, хранением, поиском, преобразованием, отображением и/или передачей информации по каналам связи.

Угроза безопасности информации – потенциальная возможность нарушения основных качественных характеристик (свойств) информации при ее обработке техническими средствами: секретности /конфиденциальности/, целостности, доступности.

Угроза безопасности информации – совокупность условий и факторов, определяющих потенциальную или реально существующую опасность нарушения безопасности информации.

Угроза информации [information treat] – утечка или возможность на рушения целостности информации.

Уровень безопасности [security level] – комбинация иерархической классификации (уровень доступа) и неиерархической категории, представляющих уровень критичности информации.

Уязвимость [Vulnerability] (1) – свойство системы, которое может привести к нарушению ее защиты при наличии угрозы. Уязвимость может возникать случайно из-за неадекватного проектирования или неполной отладки или может быть результатом злого умысла.

Уязвимость [Vulnerability] (2) – слабость в системных средствах защиты, вызванная ошибками или слабостями в процедурах, проекте, реализации, внутреннем контроле системы, которая может быть использована для нарушения системной политики безопасности.

Уязвимые места – слабые места ЛВС, которые могут использоваться угрозой для своей реализации. Например, неавторизованный доступ (угроза) к ЛВС может быть осуществлен посторонним человеком, угадавшим очевидный пароль.

Использовавшимся при этом уязвимым местом является плохой выбор пароля, сделанный пользователем. Уменьшение или ограничение уязвимых мест ЛВС может снизить или вообще устранить риск от угроз ЛВС. Например, средство, которое может помочь пользователям выбрать надежный пароль, сможет снизить вероятность того, что пользователи будут использовать слабые пароли и этим уменьшить угрозу несанкционированного доступа к ЛВС.

Функции безопасности ОО – совокупность всех функций безопасности ОО, направленных на осуществление политики безопасности объекта оценки (ПБО).

Хакер [Hacker] – пользователь, который пытается вносить изменения в системное программное обеспечение, зачастую не имея на это право. Хакером можно назвать программиста, который создает более или менее полезные вспомогательные программы, обычно плохо документированные и иногда вызывающие нежелательные побочные результаты.

Хост-бастион [Batiston host] – компьютер-шлюз, на котором работает программное обеспечение брандмауэра и который устанавливается между внутренней и внешней сетями. Хост-бастионами являются шлюзы сеансового и прикладного уровня, а также брандмауэры экспертного уровня.

Шлюз прикладного уровня [Application-level gateway] – исключает прямое взаимодействие между авторизованным клиентом и внешним хостом. Шлюз фильтрует все входящие и исходящие пакеты на прикладном уровне модели OSI. Связанные с приложениями программы-посредники перенаправляют через шлюз информацию, генерируемую конкретными сервисами TCP/IP.

Шлюз сеансового уровня [Circuit-level gateway] – исключает прямое взаимодействие между авторизованным клиентом и внешним хостом. Он принимает запрос доверенного клиента на определенные услуги и, после проверки допустимости запрошенного сеанса, устанавливает соединение с внешним хостом. После этого шлюз просто копирует пакеты в обоих направлениях, не осуществляя их фильтрации.

Эффективность защиты информации [information techmical protection efficiency] (1) – степень соответствия достигнутого уровня защищенности информации поставленной цели.

Эффективность защиты информации [information techmical protection efficiency] (2) – показатель, характеризующий уровень технической защиты информации.

Ядро безопасности [security kernel] – программные и аппаратные элементы ДВБ (TCB), реализующие концепцию монитора ссылок. Они должны разделять все попытки доступа субъектов к объектам, быть защищенным от модификации и проверены на корректное выполнение своих функций.

Ядро защиты [Security kernel] – технические, программные и микропрограммные элементы комплекса средств защиты, реализующие концепцию диспетчера доступа.

Учебное издание

Еременко Владимир Тарасович

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ И СИСТЕМ

Учебное пособие

Редактор
Технический редактор

Федеральное государственное бюджетное образовательное
Учреждение высшего профессионального образования
«Государственный университет – учебно-научно-
производственный комплекс»

Подписано к печати Формат 60х90 1/16
Усл. печ. л. Тираж экз.
Заказ №

Отпечатано с готового оригинал-макета