Министерство образования и науки РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

сборник учебно-методических материалов для направления подготовки
10.03.01 Информационная безопасность

Благовещенск, 2019

Печатается по решению
редакционно-издательского совета
факультета математики и информатики
Амурского государственного
Университета

Составитель: Соловцова Л.А.
МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ: сборник учебно-методических материалов для направления подготовки
10.03.01 Информационная безопасность – Благовещенск: Амурский гос. ун-т, 2019.

Содержание

Краткое изложение лекционного материала.

Тема 1. Введение. Методы и средства защиты информации: информационная безопасность. Основные определения.

Цель лекции. Рассмотреть основные определения и понятия по дисциплине.

План

1. Структура информационной сферы и характеристика ее элементов.
2. Информация как объект правоотношений.
3. Категории информации по условиям доступа к ней и распространения.
4. Конституционные гарантии прав граждан в информационной сфере и механизм их реализации.
5. Понятие информационной безопасности.
6. Субъекты и объекты правоотношений в области информационной безопасности.
7. Система нормативных правовых актов, регулирующих обеспечение информационной безопасности в Российской Федерации
8. Понятие и виды защищаемой информации по законодательству РФ.
9. Перспективы развития законодательства в области информационной безопасности.

Краткое содержание

При определении понятия "информационная сфера" следует учитывать, что в настоящее время не существует такого устоявшегося единого правового понятия. Если рассмотреть понятие "информационная сфера" (среда), под которой в законодательстве понимается "сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации" (Федеральный закон "Об участии в международном информационном обмене"), то оно носит, на наш взгляд, слишком общий характер.

Кроме того, в Законе, например, отсутствует признак хранения информации, названный одним из основных для документа; вместо признаков, указанных в Конституции РФ (ст. 29, п. 4), предложены другие: вместо "производство" - "создание и преобразование", вместо "поиск, получение, передача, распространение" - "потребление", хотя это признаки не одного порядка. Ниже приведено определение, данное в привязке к объектам и их основным признакам.

Информационная сфера - это среда оборота информации (производство - распространение -потребление), при котором субъекты реализуют свои потребности и возможности по отношению к информации.

Основными объектами информационной сферы являются:

1. Информация, в том числе информационные ресурсы - массивы документов, базы и банки данных, все виды архивов, библиотеки, музейные фонды и пр., содержащие данные, сведения и

знания, зафиксированные на соответствующих носителях информации.

2. Информационная инфраструктура, включающая в себя совокупность информационных систем:

а) организационные структуры, обеспечивающие функционирование и развитие информационной сферы, в частности, сбор, обработку, хранение, распространение, поиск и передачу информации.

б) информационно-телекоммуникационные структуры - территориально распределенные государственные и корпоративные компьютерные сети, телекоммуникационные сети и системы специального назначения и общего пользования, сети и каналы передачи данных, средства коммутации и управления информационными потоками;

в) информационные, компьютерные и телекоммуникационные технологии;

г) системы средств массовой информации.

Информация в настоящее время превратилась в общенаучное межотраслевое понятие, так как механизм возникновения и использования информации один и тот же как для технических, так и для социальных систем, в том числе и для сферы геологического изучения и использования недр.

Как объект правовых отношений информация обладает следующими юридически значимыми признаками109.

Прежде всего информация является идеальным компонентом бытия, т. е. благом нематериальным, не сводимым к тем физическим объектам, которые выступают ее носителями (запись на бумаге, магнитная лента и т. п.). Далее, информация есть благо непотребляемое, которое подвергается лишь моральному, но не физическому старению. Важной особенностью информации является возможность ее практически неограниченного тиражирования, распространения и преобразования форм ее фиксации.

А. Б. Венгеров в свое время определил квалифицирующие признаки информации, которые имеют значение и в настоящее время110:

а) самостоятельность по отношению к материальному носителю;

б) возможность многократного использования и неисчерпаемость ресурса;

в) сохранение информации у передающего субъекта;

г) возможность к сохранению, исполнению, агрегированию, синтезу;

д) количественная определенность;

е) системность.

Легальное определение информации содержится в Федеральном законе от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее — Закон об информации)111, в соответствии с которым «информация — сведения (сообщения, данные) независимо от формы их представления». В данном Законе информация признается объектом публичных, гражданских и иных правовых отношений (ст. 5). Информация может свободно использоваться любым лицом и передаваться одним лицом другому липу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения.

Виды информации в зависимости от категории доступа: •

общедоступная информация; •

информация ограниченного доступа (информация, доступ

к которой ограничен федеральными законами).

Субъектом информационных отношений в Законе об

информации признан «обладатель информации» — лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Реализация основных прав и свобод граждан в информационной сфере занимает важное место среди национальных интересов России. Право на поиск, получение и передачу информации (право на доступ к информации или право знать) является определяющим институтом информационного права. Юридический фундамент этого института составляют информационно-правовые нормы Конституции РФ. Основа права на доступ к информации содержится в ст. 29 ч. 4 Конституции РФ: "Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом".

В современной юридической литературе существуют различные мнения на природу права гражданина на информацию. Например, Ю.А. Дмитриев и А.А. Златопольский считают право гражданина на информацию составной частью свободы слова и печати <*>. Существует точка зрения, в соответствии с которой свобода информации - условное обозначен ие группы прав и свобод: свободы слова, мнений, свободы печати и иных средств массовой информации, права на получение информации, свободы распростране-

ния информации <**>. Имеется и противоположное суждение, когда право на доступ к информации рассматривается как отдельное, самостоятельное право в группе других информационных прав и свобод <***>. И действительно, анализируя ст. 29 Конституции РФ, можно сделать вывод, что право гражданина на информацию - все же самостоятельное право, так как в этой статье оно закреплено в части, отдельной от той, где речь идет о гарантии свободы мысли и слова. Кроме того, имеются отдельные нормативные акты, посвященные данному вопросу, например Федеральный закон "Об информации, информатизации и защите информации". Да и сам факт активного формирования такой отрасли российского права, как информационное, доказывает это. Хотя, несомненно, право человека и гражданина на информацию очень тесно связано со свободой слова и печати. Но право на информацию не охватывается полностью свободой слова и печати. Оно выполняет свою роль в удовлетворении определенных интересов субъекта.

Прежде чем говорить об обеспечении безопасности персональных данных, необходимо определить, что же такое *информационная безопасность*. Термин "*информационная безопасность*" может иметь различный смысл и трактовку в зависимости от контекста. В данном курсе под **информационной безопасностью** мы будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести *неприемлемый ущерб субъектам информационных отношений*, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры [1].

ГОСТ "*Защита информации*. Основные термины и определения" вводит понятие **информационной безопасности** как состояние защищенности информации, при котором обеспечены ее *конфиденциальность*, доступность и *целостность*.

- **Конфиденциальность** – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.
- **Целостность** – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;
- **Доступность** – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

Угрозы информационной безопасности – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. **Атакой** называется попытка реализации угрозы, а тот, кто предпринимает такую попытку, - **злоумышленником**. Потенциальные злоумышленники называются *источниками угрозы*.

Угроза является следствием наличия **уязвимых мест или уязвимостей** в информационной системе. Уязвимости могут возникать по разным причинам, например, в результате непреднамеренных ошибок программистов при написании программ.

Угрозы можно классифицировать по нескольким критериям:

- по *свойствам информации* (доступность, целостность, конфиденциальность), против которых угрозы направлены в первую очередь;
- по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, *поддерживающая инфраструктура*);
- по способу осуществления (случайные/преднамеренные, действия природного/техногенного характера);
- по расположению источника угроз (внутри/вне рассматриваемой ИС).

Обеспечение информационной безопасности является сложной задачей, для решения которой требуется *комплексный подход*. Выделяют следующие уровни защиты информации:

1. законодательный – законы, нормативные акты и прочие документы РФ и международного сообщества;

2. административный – комплекс мер, предпринимаемых локально руководством организации;

3. процедурный уровень – меры безопасности, реализуемые людьми;

4. *программно-технический уровень* – непосредственно средства защиты информации.

Законодательный уровень является основой для построения системы защиты информации, так как дает базовые понятия *предметной области* и определяет меру наказания для потенциальных злоумышленников. Этот уровень играет координирующую и направляющую роли и помогает поддерживать в обществе негативное (и карательное) *отношение* к людям, нарушающим информационную *безопасность*.

Объектами обеспечения безопасности, согласно Федеральному закону «О безопасности»от 26.06.2008 N103-ФЗ, являются РФ, субъекты РФ, органы государственной власти и органы местного самоуправления, физические и юридические лица РФ, граждане РФ, общественные организации и объединения, обладающие правами и обязанностями по участию в обеспечении безопасности. К субъектам международного информационного обмена в РФ кроме перечисленных могут относиться, физические и юридические лица иностранных государств, лица без гражданства.

Совокупность субъектов обеспечения информационной безопасности составляют систему обеспечения информационной безопасности РФ, которая является частью системы обеспечения национальной безопасности страны.

К основным объектам безопасности относятся: личность - ее права и свободы; общество - его материальные и духовные ценности; государство - его конституционный строй, суверенитет и территориальная целостность.

Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации:

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

- свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
- установление ограничений доступа к информации только федеральными законами;
- открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;
- равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;
- обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
- достоверность информации и своевременность ее предоставления;
- неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
- недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Тема 2. Методы и средства защиты информации: информационная безопасность в системе национальной безопасности Российской Федерации. Государственная информационная политика

Цель лекции. Познакомиться с понятием государственной тайны и ее защиты.

План

1. Понятие правового режима защиты государственной тайны.
2. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации.
3. Государственная тайна как особый вид защищаемой информации и ее характерные признаки.
4. Принципы и механизмы отнесения сведений к государственной тайне, их засекречивания и рассекречивания.
5. Органы защиты государственной тайны и их компетенция.
6. Система контроля за состоянием защиты государственной тайны.
7. Юридическая ответственность за нарушения правового режима защиты государственной тайны (уголовная, административная, дисциплинарная).

Краткое содержание

Понятие «государственная тайна» (ГТ) является одним из важнейших в системе защиты государственных секретов в любой стране. От его правильного определения зависит и политика руководства страны по защите секретов.

Определение этого понятия дано в Законе Российской Федерации «О государственной тайне»:

«Государственная тайна - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации».

Данное определение раскрывает главные черты, характеризующие ГТ.

государственной она называется, потому, что защищается государством, и составляющие ее сведения относятся к деятельности государства в жизненно важных для него областях;

в определении подчеркивается недопустимость распространения сведений, составляющих тайну;

ст. 2 названного Закона указывает на нежелательные последствия, к которым может привести такое распространение, а именно - на ущерб безопасности РФ;

в сохранении государственной тайны не менее, чем само государство, заинтересован достаточно широкий круг физических и юридических лиц, а также общество в целом, поскольку согласно ст. 1 Закона Российской Федерации «О безопасности» от 5 марта 1992 г., безопасность представляет собой «состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз».

В соответствии с Конституцией РФ (гл. 2 «Права и свободы человека и гражданина», ст. 29) каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом, а ст. 9^{2} Конвенции Содружества Независимых Государств Конвенция ратифицирована Федеральным законом от 04.11.95 N 163-ФЗ. прямо указывает, что каждый человек имеет право на уважение его личной и семейной жизни, на неприкосновенность жилища и тайну переписки. Не должно быть никакого вмешательства со стороны государственных органов в пользование этим правом, за исключением случаев, когда такое вмешательство предусмотрено законом и которое необходимо в демократическом обществе в интересах государственной и общественной безопасности, общественного порядка, охраны здоровья и нравственности населения или защиты прав и свобод других лиц. Таким образом, для граждан, юридических лиц закреплено право на тайну и защиту, в том числе и такие тайны как: государственная, коммерческая, банковская, тайна усыновления, служебная и другие. На сегодняшний день более

чем в 190 федеральных законах упоминается термин «информация», «защита информации».

Президентом РФ 9 сентября 2000 г. N Пр-1895 утверждена Доктрина[3] информационной безопасности Российской Федерации, которая представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации. Кроме этого Доктрина развивает Концепцию национальной безопасности Российской Федерации применительно к информационной сфере. Доктрина является основой:

- для формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;
- подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;
- разработки целевых программ обеспечения информационной безопасности Российской Федерации.

Информационная сфера как системообразующий фактор жизни общества активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Национальная безопасность Российской Федерации значительно зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Основные составляющие национальных интересов Российской Федерации в информационной сфере:

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

2) информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам;

3) развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов;

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

По своей общей направленности угрозы информационной безопасности Российской Федерации подразделяются на следующие виды:

- угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;
- угрозы информационному обеспечению государственной политики Российской Федерации;
- угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также

обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;

- угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.
- Отнесение сведений к государственной тайне и их засекречивание осуществляются в соответствии с принципами законности, обоснованности и своевременности.

Под законностью отнесения сведений к государственной тайне и их засекречивания понимается соответствие засекречиваемых сведений требованиям законодательства РФ о государственной тайне.

Обоснованность отнесения сведений к государственной тайне заключается в установлении путем экспертной оценки целесообразности их засекречивания, а также вероятных экономических и иных по следствий засекречивания исходя из баланса жизненно важных интересов государства, общества и граждан.

Своевременность отнесения сведений к государственной тайне заключается в установлении ограничений на распространение этих сведений с момента их получения (разработки) или заблаговременно.

Степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности РФ вследствие распространения таких сведений. Устанавливаются **три степени секретности** сведений, составляющих государственную тайну, и для каждой из них — грифы секретности, устанавливаемые на их носителях: **«особой важности», «совершенно секретно» и «секретно».**

Порядок определения размеров ущерба, который может быть нанесен безопасности РФ вследствие распространения сведений, составляю щих государственную тайну, и правила отнесения указанных сведений к той или иной степени секретности устанавливаются Правительством РФ.

Использование перечисленных грифов секретности для засекречивания сведений, не отнесенных к государственной тайне, не допускается.

Отнесение сведений к государственной тайне осуществляется в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью. **Обоснование необходимости** отнесения сведений к государственной тайне возлагается на органы государственной власти, предприятия, учреждения и организации, которыми эти сведения получены (разработаны).

Отнесение сведений к государственной тайне осуществляется руководителями органов государственной власти в соответствии с Перечнем сведений, составляющих государственную тайну, определяемым Федеральным законом «О государственной тайне». Лица, указанные в «Перечне должностных лиц...», несут персональную ответственность за принятые ими решения о целесообразности отнесения конкретных сведений к государственной тайне.

Для осуществления единой государственной политики в области засекречивания сведений межведомственная комиссия по защите государственной тайны формирует по предложениям органов государственной власти и в соответствии с Перечнем сведений, составляющих государственную тайну, **Перечень сведений, отнесенных к государственной тайне.**

В этом Перечне указываются органы государственной власти, наделяемые полномочиями по распоряжению данными сведениями. Указанный Перечень утверждается Президентом РФ, подлежит открытому опубликованию и пересматривается по мере необходимости.

Органы государственной власти, руководители которых наделены полномочиями по отнесению сведений к государственной тайне, разрабатывают развернутые **перечни сведений, подлежащих засекречиванию,** и устанавливают степень их секретности. Перечни утверждаются соответствующими руководителями органов государственной власти.

Основанием для засекречивания сведений, полученных (разработанных) в результате деятельности органов государственной власти, предприятий, учреждений и организаций, является их соответствие действующим в данных органах, на данных предприятиях, в данных учреждениях и организациях перечням сведений, подлежащих засекречиванию. При засекречивании этих сведений их носителям присваивается соответствующий гриф секретности.

На носители сведений, составляющих государственную тайну, наносятся реквизиты, включающие следующие данные:

- о степени секретности содержащихся в носителе сведений;

об органе государственной власти, о предприятии, об учреждении, организации, осуществивших засекречивание носителя;

- о регистрационном номере;

о дате или условии рассекречивания сведений либо о событии, после наступления которого сведения будут рассекречены.

Перечень должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне, утвержден распоряжением Президента РФ от 30 мая 1997 г. № 226-рп (в ред. от 23 июля 1998 г. и от 23 января 1999 г.) // СЗ РФ. 1977. № 22. Ст. 2573.

Перечень сведений, отнесенных к государственной тайне, утвержден Указом Президента РФ от 30 ноября 1995 г. № 1203 (в ред. от 24 января 1998 г. № 61, от 6 июня 2001 г. № 659) //СЗ РФ. 1995. № 49. Ст. 4775; 2001. № 24. Ст. 2418. 372

Тема 3. Оценка уязвимости информации

Цель лекции. Изучить методы оценки уязвимости информации..

План

1. Общая модель процесса уязвимости информации
2. Структурная схема потенциально возможных злоумышленных действий в СОД
3. Общая модель процесса несанкционированного копирования информации
4. Методологические подходы к оценке уязвимости информации

Краткое содержание

Уязвимость информации, т.е. нарушение установленного статуса и требуемого уровня ее защищенности есть событие, возникающее как результат такого стечения обстоятельств, когда в силу каких-то причин используемые в СОД средства защиты не в состоянии оказать достаточного противодействия проявлению угроз нежелательного их воздействия на защищаемую информацию. Модель уязвимости информации в СОД в самом общем виде представлена на рис. 2.6.

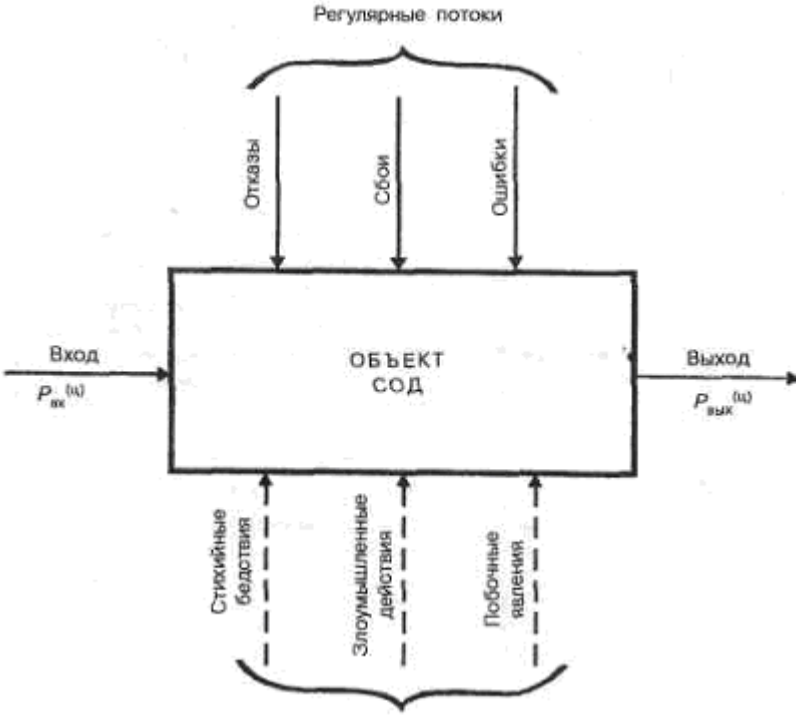


Рис. 2.6. Общая модель процесса уязвимости информации

Приведенная модель детализируется при изучении конкретных видов уязвимости информации: нарушения целостности, несанкционированной модификации, несанкционированного получения, несанкционированного размножения.

При детализации общей модели основное внимание акцентируется на то обстоятельство, что подавляющее большинство нарушений целостности информации осуществляется в процессе ее обработки на различных участках технологических маршрутов. При этом целостность информации в каждом объекте СОД существенно зависит не только от процессов, происходящих на объекте, но и от целостности информации, поступающей на его вход.

Основную опасность представляют случайные дестабилизирующие факторы (отказы, сбои и ошибки компонентов СОД), которые потенциально могут проявиться в любое время, и в этом отношении можно говорить о регулярном потоке этих факторов. Из стихийных бедствий наибольшую опасность представляют пожары, опасность которых в большей или меньшей степени также является постоянной. Опасность побочных явлений практически может быть сведена к нулю путем надлежащего выбора места для помещений СОД и их оборудования. Что касается злоумышленных действий, то они связаны главным образом с несанкционированным доступом к ресурсам СОД. При этом наибольшую опасность представляет занесение вирусов.

С точки зрения несанкционированного получения информации принципиально важным является то обстоятельство, что в современных СОД несанкционированное получение информации возможно не только путем непосредственного доступа к базам данных, но и многими путями, не требующими такого доступа. При этом основную опасность представляют злоумышленные действия людей. Воздействие случайных факторов само по себе не ведет к несанкционированному получение информации, оно лишь способствует появлению; КНПИ, которыми может воспользоваться злоумышленник. Структурированная схема потенциально возможных злоумышленных действий в современных СОД для самого общего случая представлена на рис. 2.7.

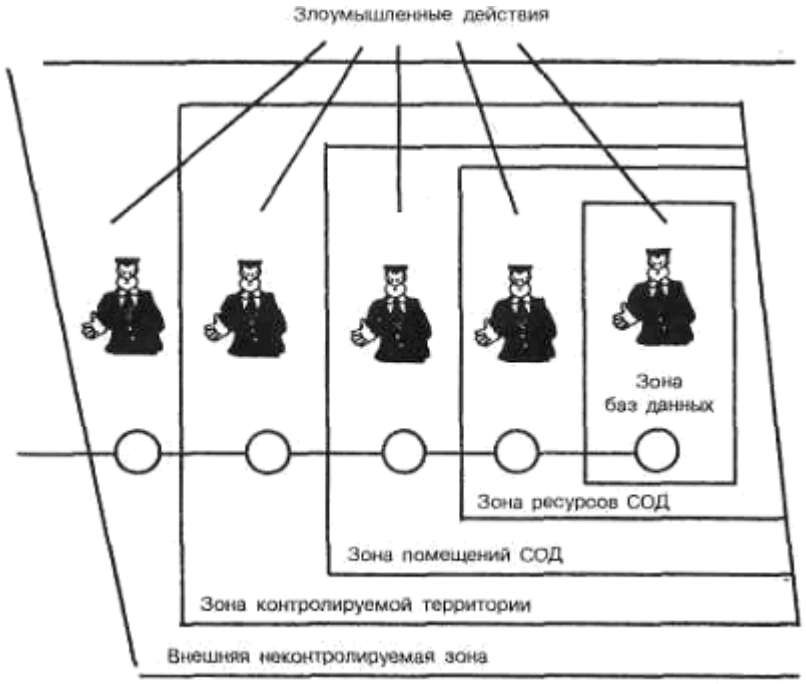


Рис. 2.7. Структурная схема потенциально возможных злоумышленных действий в СОД

Выделенные на рисунке зоны характеризуются следующим образом:

- внешняя неконтролируемая зона — территория вокруг СОД, на которой персоналом и средствами СОД не применяются никакие средства и не осуществляются никакие мероприятия для защиты информации;
- зона контролируемой территории — территория вокруг помещений СОД, которая .непрерывно контролируется персоналом или средствами СОД;
- зона помещений СОД — внутреннее пространство тех помещений, в которых расположены средства системы:
- зона ресурсов СОД — та часть помещений, откуда возможен непосредственный доступ к ресурсам системы;
- зона баз данных — та часть ресурсов системы, с которых возможен непосредственный доступ к защищаемым данным.

Злоумышленные действия с целью несанкционированного получения информации в общем случае возможны в каждой из перечисленных зон. При этом для несанкционированного получения информации необходимо одновременное наступление следующих событий:

- нарушитель должен получить доступ в соответствующую зону;
- во время нахождения нарушителя в зоне в ней должен проявиться (иметь место) соответствующий КНПИ;
- соответствующий КНПИ должен быть доступен нарушителю соответствующей категории;
- в КНПИ в момент доступа к нему нарушителя должна находиться защищаемая информация.

Рассмотрим далее трансформацию общей модели уязвимости с точки зрения несанкционированного копирования информации. Принципиальными особенностями этого процесса являются следующие:

1. любое несанкционированное копирование есть злоумышленное действие;
2. несанкционированное копирование может осуществляться в организациях-разработчиках компонентов СОД, непосредственно в СОД и сторонних организациях, причем последние могут получать носитель, с которого делается попытка снять копию как законным, так и незаконным путем.

Попытки несанкционированного копирования информации у разработчика и в СОД есть один из видов злоумышленных действий с целью несанкционированного ее получения и поэтому имитируются приведенной выше (см. рис. 2.7.) моделью. Если же носитель с защищаемой информацией каким-либо путем (законным или незаконным) попал в стороннюю организацию, то для его несанкционированного копирования могут использоваться любые средства и методы, включая и такие, которые носят характер научных исследований и опытно-конструкторских разработок. Тогда модель процесса размножения в самом общем виде может быть представлена так, как показано на рис. 2.8.

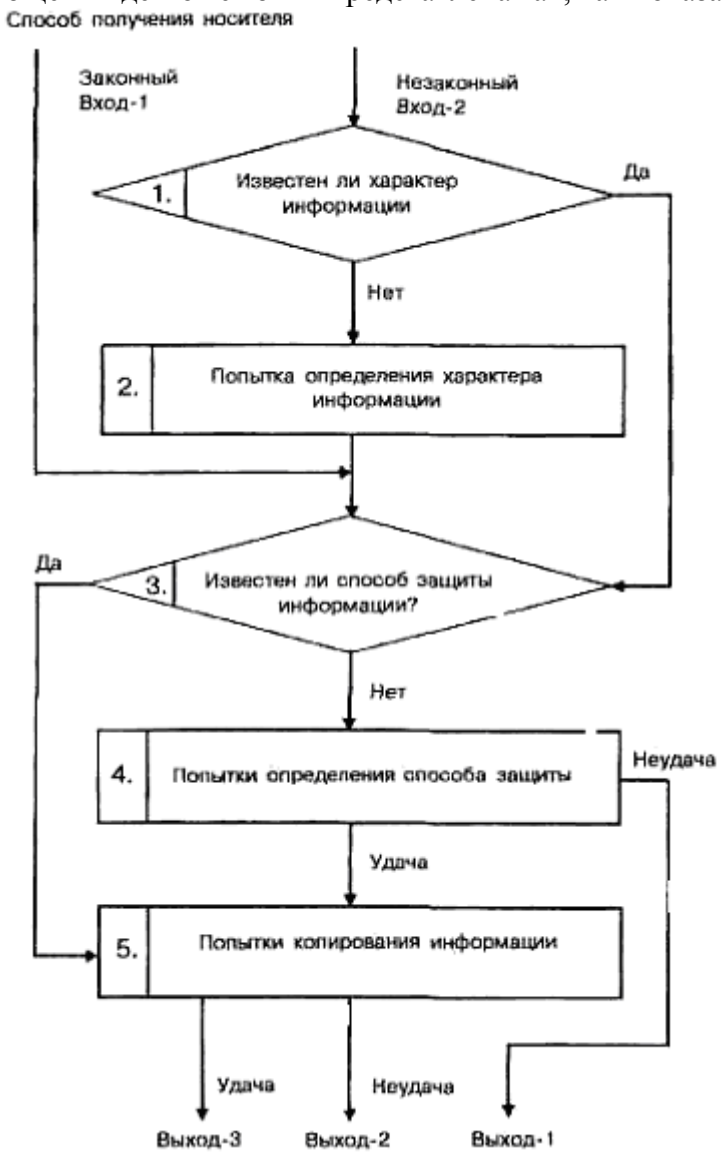


Рис. 2.8. Общая модель процесса несанкционированного копирования информации

Для определения значений показателей уязвимости информации должны быть разработаны методы, соответствующие природе этих показателей и учитывающие все факторы, влияющие на их значение. На основе этих методов должны быть разработаны модели, позволяющие рассчитывать значения любой совокупности необходимых показателей и при любых вариантах архитектурного построения СОД, технологии и условий ее функционирования.

В процессе развития теории и практики защиты информации сформировалось три методологических подхода к оценке уязвимости информации: эмпирический, теоретический и теоретико-эмпирический.

Сущность эмпирического подхода заключается в том, что на основе длительного сбора и обработки данных о реальных проявлениях угроз информации и о размерах того

ущерба, который при этом имел место, чисто эмпирическим путем устанавливаются зависимости между потенциально возможным ущербом и коэффициентами, характеризующими частоту проявления соответствующей угрозы и значения имевшего при ее проявлении размера ущерба. Наиболее характерным примером моделей рассматриваемой разновидности являются модели, разработанные специалистами американской фирмы IBM.

Теоретический подход основывается на знании законов распределения всех случайных величин, характеризующих процессы защиты, и построении на этой основе строгих зависимостей.

Теоретико-эмпирический подход основывается на житейски-естественном представлении процессов негативного воздействия на информацию и выражении этих процессов с использованием основных положений теории вероятностей

Уязвимость информации есть событие, возникающее как результат такого стечения обстоятельств, когда в силу каких-то причин используемые в автоматизированных системах обработки данных средства защиты не в состоянии оказать достаточного противодействия проявлению дестабилизирующих факторам и нежелательного их воздействия на защищаемую информацию.

Данная модель детализируется при изучении конкретных видов уязвимости информации: нарушения физической или логической целостности, несанкционированной модификации, несанкционированного получения, несанкционированного размножения.

При детализации общей модели основное внимание акцентируется на том, что подавляющее большинство нарушений физической целостности информации имеет место в процессе ее обработки на различных участках технологических маршрутов. При этом целостность информации зависит не только от процессов, происходящих на объекте, но и от целостности информации, поступающей на его вход. Основную опасность представляют случайные дестабилизирующие факторы (отказы, сбои и ошибки компонентов автоматизированных систем обработки данных), которые потенциально могут проявиться в любое время, и в этом отношении можно говорить о регулярном потоке этих факторов. Из стихийных бедствий наибольшую опасность представляют пожары, опасность которых в большей или меньшей степени также является постоянной. Опасность побочных явлений практически может быть сведена к нулю путем надлежащего выбора места для помещений автоматизированной системы обработки данных и их оборудования. Что касается злоумышленных действий, то они связаны главным образом с несанкционированным доступом к ресурсам автоматизированной системы обработки данных. При этом наибольшую опасность представляет занесение вирусов.

С точки зрения несанкционированного получения информации принципиально важным является то обстоятельство, что в современных автоматизированных системах обработки данных оно возможно не только путем непосредственного доступа к базам данных, но и многими путями, не требующими такого доступа. При этом основную опасность представляют злоумышленные действия людей. Воздействие случайных факторов непосредственно не ведет к несанкционированному получению информации, оно лишь способствует появлению каналов несанкционированного получения информации, которыми может воспользоваться злоумышленник.

Рассмотрим далее трансформацию общей модели уязвимости с точки зрения несанкционированного размножения информации. Принципиальными особенностями этого процесса являются:

- любое несанкционированное размножение есть злоумышленное действие;
- несанкционированное размножение может осуществляться в организациях-разработчиках компонентов автоматизированной системы обработки данных, непосредственно в автоматизированной системе обработки данных и сторонних организациях, причем последние могут получать носитель, с которого делается попытка снять копию как законным, так и незаконным путем.

Попытки несанкционированного размножения информации у разработчика и в автоматизированной системе обработки данных есть один из видов злоумышленных действий с целью несанкционированного ее получения и поэтому имитируются приведенной моделью. Если же носитель с защищаемой информацией каким-либо путем (законным или незаконным) попал в стороннюю организацию, то для его несанкционированного копирования могут использоваться любые средства и методы, включая и такие, которые носят характер научных исследований и опытно-конструкторских разработок.

В процессе развития теории и практики защиты информации сформировалось три методологических подхода к оценке уязвимости информации: эмпирический, теоретический и теоретико-эмпирический.

Тема 4. Основные теории защиты информации. Модели безопасности

Цель лекции. Рассмотреть основные теории защиты информации и модели безопасности.

План

Основные теории защиты информации.

Модели безопасности

*М*одель управления доступом,

Модель политики безопасности.

Модель дискреционного доступа (DAC).

Модель безопасности белла-ЛаПадулы.

Ролевая модель контроля доступа (RBAC).

Системы разграничения доступа

Краткое содержание

В области защиты информации и компьютерной безопасности в целом наиболее актуальными являются три группы проблем:

1. Нарушение конфиденциальности информации.
2. Нарушение целостности информации.
3. Нарушение работоспособности информационно-вычислительных систем.

Защита информации превращается в важнейшую проблему государственной безопасности, когда речь идет о государственной, дипломатической, военной, промышленной, медицинской, финансовой и другой доверительной, секретной информации. Огромные массивы такой информации хранятся в электронных архивах, обрабатываются в информационных системах и передаются по телекоммуникационным сетям. Основные свойства этой информации - конфиденциальность и целостность, должны поддерживаться законодательно, юридически, а также организационными, техническими и программными методами.

Конфиденциальность информации (от лат. confidentia - доверие) предполагает введение определенных ограничений на круг лиц, имеющих доступ к данной информации. Степень конфиденциальности выражается некоторой установленной характеристикой (особая важность, совершенно секретно, секретно, для служебного пользования, не для печати и т.п.), которая субъективно определяется владельцем информации в зависимости от содержания сведений, которые не подлежат огласке, предназначены ограниченному кругу лиц, являются секретом. Естественно, установленная степень конфиденциальности

информации должна сохраняться при ее обработке в информационных системах и при передаче по телекоммуникационным сетям.

Другим важным свойством информации является ее целостность (integrty). Информация целостна, если она в любой момент времени правильно (адекватно) отражает свою предметную область. Целостность информации в информационных системах обеспечивается своевременным вводом в нее достоверной (верной) информации, подтверждением истинности информации, защитой от искажений и разрушения (стирания).

Несанкционированный доступ к информации лиц, не допущенных к ней, умышленные или неумышленные ошибки операторов, пользователей или программ, неверные изменения информации вследствие сбоев оборудования приводят к нарушению этих важнейших свойств информации и делают ее непригодной и даже опасной. Ее использование может привести к материальному и/или моральному ущербу, поэтому создание системы защиты информации, становится актуальной задачей. Под безопасностью информации (information security) понимают защищенность информации от нежелательного ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

Безопасность информации в информационной системе или телекоммуникационной сети обеспечивается способностью этой системы сохранять конфиденциальность информации при ее вводе, выводе, передаче, обработке и хранении, а также противостоять ее разрушению, хищению или искажению. Безопасность информации обеспечивается путем организации допуска к ней, защиты ее от перехвата, искажения и введения ложной информации. С этой целью применяются физические, технические, аппаратные, программно-аппаратные и программные средства защиты. Последние занимают центральное место в системе обеспечения безопасности информации в информационных системах и телекоммуникационных сетях.

Задачи обеспечения безопасности:

- защита информации в каналах связи и базах данных криптографическими методами;
- подтверждение подлинности объектов данных и пользователей (аутентификация сторон, устанавливающих связь);
- обнаружение нарушений целостности объектов данных;
- обеспечение защиты технических средств и помещений, в которых ведется обработка конфиденциальной информации, от утечки по побочным каналам и от возможно внедренных в них электронных устройств съема информации;
- обеспечение защиты программных продуктов и средств вычислительной техники от внедрения в них программных вирусов и закладок;
- защита от несанкционированных действий по каналу связи от лиц, не допущенных к средствам шифрования, но преследующих цели компрометации секретной информации и дезорганизации работы абонентских пунктов;
- организационно - технические мероприятия, направленные на обеспечение сохранности конфиденциальных данных.

Основную роль в методе формальной разработки системы играет так называемая *модель безопасности (модель управления доступом, модель политики безопасности). Це-*

лью этой модели является выражение сути требований по безопасности к данной системе. Она определяет потоки информации, разрешенные в системе, и правила управления доступом к информации.

Модель позволяет провести анализ свойств системы, но не накладывает ограничений на реализацию тех или иных механизмов защиты. Так как она является формальной, возможно осуществить доказательство различных свойств безопасности системы.

Хорошая модель безопасности обладает свойствами абстрактности, простоты и адекватности моделируемой системе.

Основные понятия, используемые в моделях разграничения доступа, приведены в руководящем документе Государственной технической комиссии при Президенте РФ «Защита от несанкционированного доступа к информации»:

Доступ к информации — ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации

Объект доступа — единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа

Субъект доступа — лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Правила разграничения доступа — совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа

Врамках дискреционной модели контролируется доступ субъектов (пользователей или приложений) к объектам (представляющим собой различные информационные ресурсы: файлы, приложения, устройства вывода и т.д.).

Для каждого объекта существует субъект-владелец,который сам определяет тех, кто имеет доступ к объекту, а также разрешенные операции доступа. Основными операциями доступа являются READ (чтение), WRITE (запись) и EXECUTE (выполнение, имеет смысл только для программ). Таким образом, в модели дискреционного доступа для каждой парысубъект-объектустанавливается набор разрешенных операций доступа.

При запросе доступа к объекту, система ищет субъекта в списке прав доступа объекта и разрешает доступ если субъект присутствует в списке и разрешенный тип доступа включает требуемый тип. Иначе доступ не предоставляется.

Классическая система дискреционного контроля доступа является «закрытой» в том смысле, что изначально объект не доступен никому, и в списке прав доступа описывается набор разрешений. Также существуют «открытые» системы, в которых по умолчанию все имеют полный доступ к объектам, а в списке доступа описывается набор ограничений.

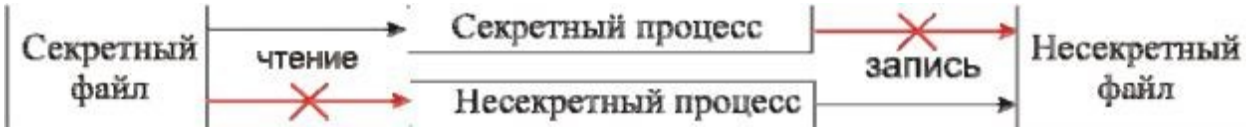
Такая модель реализована в операционных системах Windows (см. рис. 1) и Linux.

В частности, в Linux для каждого файла (все ресурсы в ОС Linux представимы в виде файлов, в том числе устройства ввода-вывода)устанавливаются разрешения доступа для трех категорий субъектов: владелец файла, члены той же группы, что и владелец, и все остальные пользователи. Для каждой из этих категорий устанавливаются права на чтение (r), запись (w) и выполнение (x). Набор прав доступа объекта может быть представлен в виде символьной строки. Например, запись«rwxr-xr--»означает, что владелец файла может делать с ним все, что угодно; члены его группы могут читать и исполнять файл, но не могут записывать, а прочим пользователям доступно только чтение.

Недостаток модели DAC заключается в том, что субъект, имеющий право на чтение информации может передать ее другим субъектам, которые этого права не имеют, без уведомления владельца объекта. Таким образом, нет гарантии, что информация не станет доступна субъектам, не имеющим к ней доступа. Кроме того, не во всех АИС каждому объекту можно назначить владельца (во многих случаях данные принадлежат не отдельным субъектам, а всей системе).

Одна из наиболее известных моделей безопасности — модель Белла-ЛаПадулы(модель мандатного управления доступом). В ней определено множество понятий, связанных с контролем доступа; даются определения субъекта, объекта и операции доступа, а также математический аппарат для их описания. Эта модель в основном известна двумя основными правилами безопасности: одно относится к чтению, а другое – к записи данных.

Пусть в системе имеются данные (файлы) двух видов: *секретные* и*несекретные,* а пользователи этой системы также относятся к двум категориям: с уровнем допуска к несекретным данным (несекретные) и с уровнем допуска к секретным данным (секретные).



1.Свойство простой безопасности: несекретный пользователь (или процесс, запущенный от его имени) не может читать данные из секретного файла.

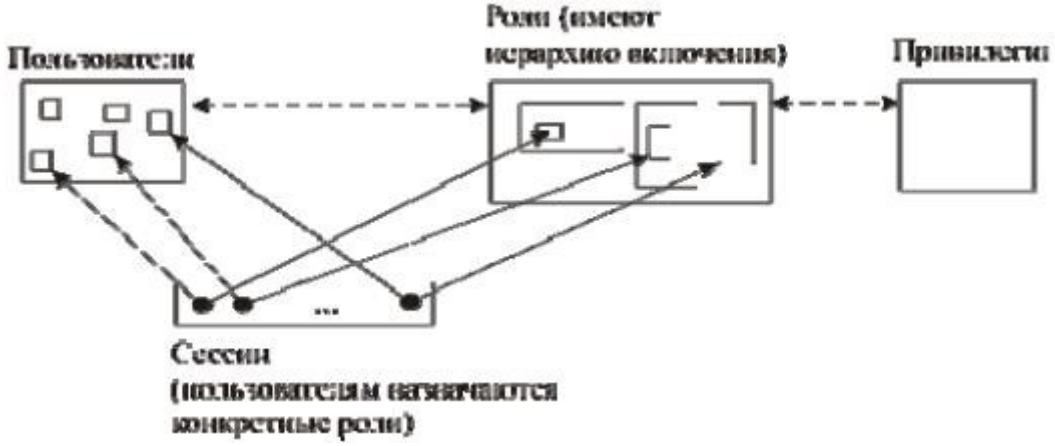
2.-свойство:пользователь с уровнем доступа к секретным данным не может записывать данные в несекретный файл.* Это правило менее очевидно, но не менее важно. Действительно, если пользователь с уровнем доступа к секретным данным скопирует эти данные в обычный файл (по ошибке или злому умыслу), они станут доступны любому «несекретному» пользователю. Кроме того, в системе могут быть установлены ограничения на операции с секретными файлами (например, запрет копировать эти файлы на другой компьютер, отправлять их по электронной почте и т.д.). Второе правило безопасности гарантирует, что эти файлы (или даже просто содержащиеся в них данные) никогда не станут несекретными и не «обойдут» эти ограничения. Таким образом, вирус, например, не сможет похитить конфиденциальные данные. Рассмотренные правила легко распространить на случай, когда в системе необходимо иметь более двух уровней доступа — например, различаются несекретные, конфиденциальные, секретные и совершенно секретные данные. Тогда пользователь с уровнем допуска к секретным данным может читать несекретные, конфиденциальные и секретные документы, а создавать — только секретные и совершенно секретные.

Общее правило звучит так: пользователи могут читать только документы, уровень секретности которых не превышает их допуска, и не могут создавать документы ниже уровня своего допуска.То есть теоретически пользователи могут создавать документы, прочесть которые они не имеют права.

Модель Белла-ЛаПадулыстала первой значительной моделью политики безопасности, применимой для компьютеров, и до сих пор в измененном виде применяется в военной отрасли. Модель полностью формализована математически. Основной упор в модели делается на конфиденциальность, но кроме неё фактически больше ничего не представлено. Кроме того, в модели игнорируется проблема изменения классификации: предполагается, что все сведения относятся к соответствующему уровню секретности, который остается неизменным. Наконец, бывают случаи, когда пользователи должны работать с данными, которые они не имеют права увидеть. «Сведения о том, что самолет несет груз из некоторого количества бомб, возможно, имеют более высокий уровень секретности, чем уровень доступа диспетчера, но диспетчеру тем не менее необходимо знать вес груза.» [1]

3.4. Ролевая модель контроля доступа (RBAC)

Ролевой метод управления доступом контролирует доступ пользователей к информации на основе типов их активностей в системе (ролей). Под *ролью* понимается совокупность действий и обязанностей, связанных с определенным видом деятельности. Примеры ролей: администратор базы данных, менеджер, начальник отдела.



В ролевой модели с каждым объектом сопоставлен набор разрешенных операций доступа для каждой роли (а не для каждого пользователя). В свою очередь, каждому пользователю сопоставлены роли, которые он может выполнять. В некоторых системах пользователю разрешается выполнять несколько ролей одновременно, в других есть ограничение на одну или несколько не противоречащих друг другу ролей в каждый момент времени.

Для формального определения модели RBAC используются следующие соглашения: *S* = субъект — человек или автоматизированный агент.

R = роль — рабочая функция или название, определяется на уровне авторизации.*P* = разрешения — утверждения режима доступа к ресурсу.

SE = сессия — Соответствие между S, R и/или P.

SA = назначение субъекта (Subject Assignment).*SA* $S \times R$. При этом субъекты назначаются связям ролей и субъектов в отношении «многие ко многим» (один субъект может иметь несколько ролей, а одну роля могут иметь несколько субъектов).

PA = назначение разрешения (Permission Assignment).*PA* $P \times R$. При этом разрешения назначаются связям ролей в отношении «многие ко многим».

RH = частично упорядоченная иерархия ролей (Role Hierarchy).*PH* $R \times R$.

На возможность наследования разрешений от противоположных ролей накладывается ограничительная норма, которая позволяет достичь надлежащего разделения режимов. Например, одному и тому же лицу может быть не позволено создать учетную запись для кого-то,а затем авторизоваться под этой учетной записью. схема ролевой модели контроля доступа (RBAC)

Основные достоинства ролевой модели:

1.Простота администрирования. В отличие от модели DAC нет необходимости прописывать разрешения для каждой пары «объект-пользователь».Вместо этого прописываются разрешения для пар«объект-роль»и определяются роли каждого пользователя. При изменении области ответственности пользователя, у него просто изменяются роли. Иерархия ролей (когда роль наряду со своими собственными привилегиями может наследовать привилегии других ролей) также упрощает процесс администрирования.

Тема 5. Сервисы безопасности

Цель лекции. Рассмотреть основные сервисы безопасности.

План

Понятие сервисов безопасности.

Идентификация/аутентификация.

Разграничение доступа.

Протоколирование/аудит.

Экранирование.

Туннелирование.

Шифрование.

Контроль целостности.

Краткое содержание

Для решения перечисленных задач в ВС создаются специальные механизмы защиты (или сервисы безопасности). Их перечень и содержание для общего случая могут быть представлены следующим образом.

Идентификация/аутентификация. Современные средства идентификации / аутентификации должны удовлетворять двум условиям:

• быть устойчивыми к сетевым угрозам (пассивному и активному прослушиванию сети);

• поддерживать концепцию единого входа в сеть.

Первое требование можно выполнить, используя криптографические методы. В настоящее время общепринятыми являются подходы, основанные на системе Kerberos или службе каталогов с сертификатами в стандарте X.509.

Единый вход в сеть — это, в первую очередь, требование удобства для пользователей. Если в корпоративной сети много информационных сервисов, допускающих независимое обращение, то многократная идентификация/аутентификация становится слишком обременительной.

Дополнительные удобства создает применение биометрических методов аутентификации, основанных на сканировании отпечатков пальцев. Подчеркнем, что и здесь защита от нарушения целостности и перехвата с последующим воспроизведением осуществляется методами криптографии.

Разграничение доступа. Разграничение доступа является самой исследо-ванной областью информационной безопасности.

В настоящее время следует признать устаревшим (или, по крайней мере, не полностью соответствующим действительности) положение о том, что разграничение доступа направлено исключительно на защиту от злоумышленных пользователей. Современные информационные системы характеризуются чрезвычайной сложностью и их внутренние ошибки представляют не меньшую опасность.

Динамичность современной программной среды в сочетании со сложностью отдельных компонентов существенно сужает область применимости самой употребительной — дискреционной модели управления доступом (называемой также моделью с произвольным управлением). При определении допустимости доступа важно не только (и не столько) то, кто обратился к объекту, но и то, какова семантика действия. Без привлечения семантики нельзя выявить троянские программы, противостоять которым произвольное управление доступом не в состоянии.

В последнее время появляются новые модели управления доступом, например модель «песочницы» в Java-технологии.

Активно развиваемое ролевое управление доступом решает не столько проблемы безопасности, сколько улучшает управляемость систем (что, конечно, очень важно). Суть его в том, что между пользователями и их привилегиями помещаются промежуточные сущности — роли. Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему определенные права.

Сложность информационной системы характеризуется, прежде всего, числом имеющихся в ней связей. Поскольку ролей много меньше, чем пользователей и привилегий, их (ролей) использование способствует понижению сложности и, следовательно, улучшению управляемости. Кроме того, на основании ролевой модели можно реализовать такие важные принципы, как разделение обязанностей (невозможность в одиночку скомпрометировать критически важный процесс). Между ролями могут быть определены статические или динамические отношения несовместимости (невозможности одному субъекту по очереди или одновременно активизировать обе роли), что и обеспечивает требуемую защиту.

Для некоторых употребительных сервисов таких, как Web, ролевое управление доступом может быть реализовано относительно просто (в Web-случае — на основе cgi-процедур).

Протоколирование/аудит. Протоколирование и аудит традиционно являлись рубежом обороны, обеспечивающим анализ последствий нарушения информационной безопасности и выявление злоумышленников.

Такой аудит можно назвать пассивным. Довольно очевидным обобщением пассивного аудита для сетевой среды является совместный анализ регистрационных журналов отдельных компонентов на предмет выявления противоречий, что важно в случаях, когда злоумышленнику удалось отключить протоколирование или модифицировать журналы.

В современный арсенал защитных средств несколько лет назад вошел активный аудит, направленный на выявление подозрительных действий в реальном масштабе времени. Активный аудит включает два вида действий:

• выявление нетипичного поведения (пользователей, программ или аппаратуры);

• выявление начала злоумышленной активности.

Нетипичное поведение выявляется статистическими методами, путем сопоставления с предварительно полученными образцами. Начало злоумышленной активности обнаруживается по совпадению с сигнатурами известных атак. За обнаружением следует заранее запрограммированная реакция (как минимум — информирование системного администратора, как максимум — контратака на систему предполагаемого злоумышленника).

Важным элементом современной трактовки протоколирования/аудита является протокол автоматизированного обмена информацией о нарушениях безопасности между корпоративными системами, подключенными к одной внешней сети. В наше время системы не могут считаться изолированными, они не должны жить по. закону «каждый за себя»; угрозам следует противостоять сообща.

Экранирование. Экранирование как сервис безопасности выполняет следующие функции :

• разграничение межсетевого доступа путем фильтрации передаваемых данных;

• преобразование передаваемых данных.

Современные межсетевые экраны (рис. 4.1.) фильтруют данные на основе заранее заданной базы правил, что позволяет, по сравнению с традиционными операционными системами, реализовывать гораздо более гибкую политику безопасности. При комплексной фильтрации, охватывающей сетевой, транспортный и прикладной уровни, в правилах могут фигурировать сетевые адреса, количество переданных данных, операции прикладного уровня, параметры окружения (например, время) и т. п.

Преобразование передаваемых данных может затрагивать как служебные поля пакетов, так и прикладные данные. В первом случае обычно имеется в виду трансляция адресов, помогающая скрыть топологию защищаемой системы. Это уникальное свойство сервиса экранирования, позволяющее скрывать существование некоторых объектов доступа. Преобразование данных может состоять, например, в их шифровании.

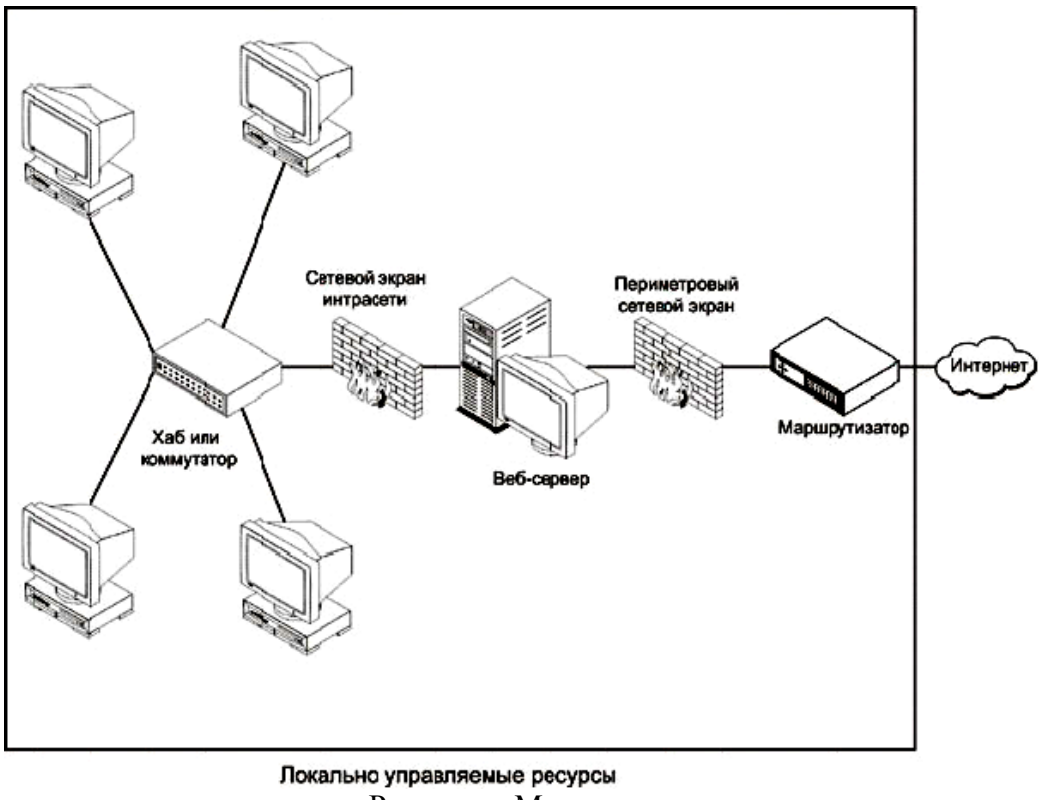


Рисунок – Межсетевые экраны

В процессе фильтрации (точнее, параллельно с ней) может выполняться дополнительный контроль (например, антивирусный). Возможны и дополни-тельные преобразования, наиболее актуальным из которых является исправление заголовков или иной служебной информации, ставшей некорректной после наступления 2000 года.

Применение межсетевого экранирования поставщиками Интернет-услуг в соответствии с рекомендациями разработчиков позволило бы существенно снизить шансы злоумышленников и облегчить их прослеживание.

Данная мера еще раз показывает, как важно рассматривать каждую информационную систему как часть глобальной инфраструктуры и принимать на себя долю ответственности за общую информационную безопасность.

Туннелирование. Его суть состоит в том, чтобы «упаковать» передаваемую порцию данных, вместе со служебными полями, в новый «конверт» . Данный сервис может применяться для нескольких целей:

• осуществление перехода между сетями с разными протоколами (например, IPv4 и IPv6);

• обеспечение конфиденциальности и целостности всей передаваемой порции, включая служебные поля.

Туннелирование может применяться как на сетевом, так и прикладном уровнях. Например, стандартизовано туннелирование для IP и двойное конвертование для почты X.400.

Комбинация туннелирования и шифрования (с необходимой криптографической инфраструктурой) на выделенных шлюзах позволяет реализовать такое важное в современных условиях защитное средство, как виртуальные частные сети. Такие сети, наложенные обычно поверх Интернета, существенно дешевле и гораздо безопаснее, чем действительно собственные сети организации, построенные на выделенных каналах. Коммуникации на всем их протяжении физически защитить невозможно, поэтому лучше изначально исходить из предположения об уязвимости и соответственно обеспечивать защиту. Современные протоколы, направленные на поддержку классов обслуживания, помогут гарантировать для виртуальных частных сетей заданную пропускную способность, вели-

чину задержек и т. п., ликвидируя тем самым единственное на сегодняш-ний день реальное преимущество собственных сетей.

Шифрование. Шифрование — важнейшее средство обеспечения конфиденциальности и одновременно самое конфликтное место информационной безопасности. У компьютерной криптографии две стороны — собственно криптографическая и интерфейсная, позволяющая сопрягаться с другими частями информационной системы. Важно, чтобы были обеспечены достаточное функциональное богатство интерфейсов и их стандартизация. Криптографией, в особенности шифрованием, должны, разумеется, заниматься профессионалы. От них требуется разработка защищенных инвариантных компонентов, которые можно было бы свободно (по крайней мере, с технической точки зрения) встраивать в существующие и перспективные конфигурации.

У современного шифрования есть и внутренние проблемы как техниче-ские, так и нормативные. Из технических наиболее острой является проблема производительности. Программная реализация на универсальных процессорах не является адекватным средством (здесь можно провести аналогию с компрессией видеоизображений). Еще одна техническая задача — разработка широкого спектра продуктов, предназначенных для использования во всех видах компьютерного и сетевого оборудования, — от персональных коммуникаторов до мощных шлюзов (TP-Link).

Контроль целостности. В современных системах контроль целостности должен распространяться не только на отдельные порции данных, аппаратные или программные компоненты.

Он обязан охватывать распределенные конфигурации, защищать от несанкционированной модификации потоки данных.

В настоящее время существует достаточно решений для контроля целостности и с системной, и с сетевой направленностью (обычно контроль выполняется прозрачным для приложений образом как часть общей протокольной активности). Стандартизован программный интерфейс к этому сервису.

Контроль защищенности. Контроль защищенности по сути представляет собой попытку «взлома» информационной системы, осуществляемого силами самой организации или уполномоченными лицами. Идея данного сервиса в том, чтобы обнаружить слабости в защите раньше злоумышленников. В первую очередь, имеются в виду не архитектурные (их ликвидировать сложно), а «оперативные» бреши, появившиеся в результате ошибок администрирования или из-за невнимания к обновлению версий программного обеспечения.

Средства контроля защищенности позволяют накапливать и многократно использовать знания об известных атаках. Очевидна их схожесть с антивирусными средствами; формально последние можно считать их подмножеством. Очевиден и реактивный, запаздывающий характер подобного контроля (он не защищает от новых атак). Следует помнить, что оборона должна быть эшелонированной, так что в качестве одного из рубежей контроль защищенности вполне адекватен. Подавляющее большинство атак носит рутинный характер; они возможны только потому, что известные уязвимости годами остаются неустраненными.

Существуют как коммерческие, так и свободно распространяемые продукты для контроля защищенности. Впрочем, в данном случае важно не просто один раз получить и установить их, но и постоянно обновлять базу данных уязвимостей. Это может оказаться не проще, чем следить за информацией о новых атаках и рекомендуемых способах противодействия.

Обнаружение отказов и оперативное восстановление. Обнаружение отказов и оперативное восстановление относятся к числу сервисов, обеспечивающих высокую доступность (готовность). Его работа опирается на элементы архитектурной безопасности, а именно на существование избыточности в аппаратно-программной конфигурации.

В настоящее время спектр программных и аппаратных средств данного класса можно считать сформировавшимся. На программном уровне соответ-ствующие функции берет на себя программное обеспечение промежуточного слоя. Среди аппаратно-программных продуктов стандартом стали кластерные конфигурации. Восстановление производится действительно оперативно (десятки секунд, в крайнем случае, минуты), прозрачным для приложений образом.

Обнаружение отказов и оперативное восстановление может играть по отношению к другим средствам безопасности роль инфраструктурного сервиса, обеспечивая высокую готовность последних. Это особенно важно для межсетевых экранов, средств поддержки виртуальных частных сетей, серверов аутентификации, нормальное функционирование которых критически важно для корпоративной информационной системы в целом.

Такие комбинированные продукты получают все более широкое распространение

Управление. Управление относится к числу инфраструктурных сервисов, обеспечивающих нормальную работу функционально полезных компонентов и средств безопасности. Сложность современных систем такова, что без правильно организованного управления они постепенно (а иногда и довольно быстро) деградируют как в плане эффективности, так и в плане защищенности.

Особенно важной функцией управления является контроль согласованности конфигураций различных компонентов (имеется в виду семантическая согласованность, относящаяся, например, к наборам правил нескольких межсетевых экранов). Процесс администрирования идет постоянно; требуется, однако, чтобы при этом не нарушалась политика безопасности

Место сервисов безопасности в архитектуре информационных систем. Выше был перечислен десяток сервисов безопасности. Как объединить их для создания эшелонированной обороны, каково их место в общей архитектуре информационных систем?

На внешнем рубеже располагаются средства выявления злоумышленной активности и контроля защищенности. Далее идут межсетевые экраны, защищающие внешние подключения. Они вместе со средствами поддержки виртуальных частных сетей (обычно объединяемых с межсетевыми экранами) образуют периметр безопасности, отделяющий корпоративную систему от внешнего мира.

Сервис активного аудита должен присутствовать во всех критически важных компонентах и, в частности, в защитных.

Это позволит быстро обнаружить атаку, даже если по каким-либо причинам она окажется успешной.

Управление доступом также должно присутствовать на всех сервисах, функционально полезных и инфраструктурных. Доступу должна предшествовать идентификация и аутентификация субъектов.

Криптографические средства целесообразно выносить на специальные шлюзы, где им может быть обеспечено квалифицированное администрирова-ние. Масштабы пользовательской криптографии следует минимизировать .

Наконец, последний рубеж образуют средства пассивного аудита, помогающие оценить последствия нарушения безопасности, найти виновного, выяснить, почему успех атаки стал возможным.

Расположение средств обеспечения высокой доступности определяется критичностью соответствующих сервисов или их компонентов. Для обеспече-ния доступности (непрерывности функционирования) могут применяться следующие защитные меры:

• внесение в конфигурацию той или иной формы избыточности (резервное оборудование, запасные каналы связи и т. п.). Это элемент архитектурной безопасности, рассматриваемой в следующем разделе;

• наличие средств обнаружения отказов. Если требуется постоянная высокая готовность, необходим специализированный сервис. В остальных случаях достаточно протоколирования/аудита в квазиреальном времени;

• наличие средств реконфигурирования для восстановления, изоляции и/или замены компонентов, отказавших или подвергшихся атаке на доступ-ность. Это или специализированная функция, или одна из функций управления;

• рассредоточенность сетевого управления, отсутствие единой точки отказа. Это, как и следующий пункт, — элементы архитектурной безопасности;

• выделение подсетей и изоляция групп пользователей друг от друга. Данная мера ограничивает зону поражения при возможных нарушениях информационной безопасности.

Каждый компонент, вообще говоря, не обязан поддерживать все перечисленные выше сервисы безопасности. Важно, чтобы он обладал программными и/или протокольными интерфейсами для получения недостающих сервисов от других компонентов и чтобы не существовало возможности обхода основных и дополнительных защитных средств.

Методические указания к лабораторным занятиям

Лабораторная работа №1

Оценка уязвимости информации

Цель работы: Получить навыки оценки уязвимости информации.

Задание

1. Используя Microsoft Visio построить общая модель процесса уязвимости информации для образовательного учреждения.
2. Используя Microsoft Visio построить общая модель процесса уязвимости информации для медицинского учреждения
3. Используя Microsoft Visio построить общая модель процесса уязвимости информации для транспортного предприятия

Контрольные вопросы

1. Что такое уязвимость информации?
2. Какие злоумышленные действия характерны для СОД?
3. Назвать виды уязвимости информации.
4. Привести примеры уязвимости информационной безопасности.
5. Что такое уязвимость нулевого дня?
6. По каким признакам выполняется классификация уязвимостей безопасностей?
7. Какие уязвимости относятся к субъективным уязвимостям?
8. Как выполняется идентификация уязвимостей?
9. Какой математический аппарат используется для описания и расчета уязвимостей?
10. Что такое уровень уязвимости и как он оценивается?

Лабораторная работа №2

Разработка модели безопасности

Цель работы: Получить практические умения разработки модели безопасности.

Задание

1. Программно реализовать автомат, построенный на основе модели Харрисона-Руззо-Ульмана.
2. Программно реализовать модель решетки.
3. Программно реализовать конечный автомат.

Контрольные вопросы

1. Какие основные виды политики безопасности известны?
2. В чем суть дискреционной политики безопасности?
3. Какими условиями определяется мандатная политика безопасности?
4. Чем отличается политика безопасности информационных потоков от политики ролевого разграничения доступа?
5. Какова цель реализации политики изолированной программной среды?

6. Что такое матрица доступов?
7. Перечислить классические угрозы безопасности?
8. Как описываются информационные потоки по времени и по памяти?
9. Какие математические понятия используются в моделях безопасности?
10. Какая задача является алгоритмически разрешимой?

Лабораторная работа №3

Разработка и использование сервисов безопасности

Цель работы: Получить навыки разработки и использования сервисов безопасности.

Задание

1. Программно реализовать сервис идентификации аутентификации.
2. Написать программу для реализации сервиса разграничение доступа.
3. Написать программу для реализации сервиса ролевого управления.
4. Написать программу для реализации сервиса протоколирования и аудита.

Контрольные вопросы

1. Перечислить сервисы безопасности.
2. Каким условиям должны удовлетворять современные средства идентификации аутентификации?
3. Что такое разграничение доступа?
4. В чем суть ролевого управления?
5. Почему протоколирование и аудит относят к пассивным сервисам безопасности?
6. Какие функции выполняет экранирование как сервис безопасности?
7. Для каких целей используется туннелирование?
8. Что такое шифрование, криптография?
9. Какие существуют виды конфиденциальности?
10. Что такое стандарт X.800?

Методические указания к практическим занятиям;

Практическое занятие №1

Методы и средства защиты информации: информационная безопасность. Основные определения

Цель занятия. Изучение основных понятий и определений, связанных с дисциплиной..

Задание

1. Сформулировать основные понятия и определения известные из других дисциплин.
2. Выполнить классификацию методов защиты информации.
3. Построить глоссарий по теме

Контрольные вопросы

1. Что такое информационная безопасность?
2. Перечислить виды угроз.
3. Назвать методы защиты информации?
4. Раскрыть понятие компьютерное преступление.
5. Что такое конфиденциальность информации?
6. Что такое целостность данных?
7. Что такое доступность данных?
8. В каком случае информация считается защищенной?
9. Назвать источники информации, требующие защиты?
10. Что относится к способам получения доступа к информации?

Практическое занятие №2

Методы и средства защиты информации: информационная безопасность в системе национальной безопасности Российской Федерации. Государственная информационная политика

Цель занятия. Изучение вопросов государственной информационной политики.

Задание

1. Государственная информационная политика: содержание и основные концептуальные подходы.
2. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации..
3. Выполнить анализ эволюции государственной информационной политики в России.
4. Построить иерархию органов защиты государственной тайны.

Контрольные вопросы

1. Что такое государственная тайна?
2. Каковы принципы отнесения сведений к государственной тайне?
3. Что представляет собой механизм засекречивания и рассекречивания?
4. Какие государственные органы относятся к органам защиты государственной тайны?
5. Что представляет собой система контроля за состоянием защиты государственной тайны?

6. Какая юридическая ответственность предусмотрена за нарушения правового режима защиты государственной тайны?

7. Что такое носители сведений, составляющих государственную тайну?

8. Какие бывают грифы секретности?

9. Сколько лет действует гриф секретности?

10. Привести пример информации, относящейся к государственной тайне.

Практическое занятие №3

Оценка уязвимости информации

Цель занятия. Научиться выполнять оценку уязвимости информации для различных предметных областей.

Задание

1. Используя методологию IDEF0 построить модель процесса уязвимости информации для образовательного учреждения.

2. Построить структурная схема потенциально возможных злоумышленных действий в СОД для транспортного предприятия.

Контрольные вопросы

1. Что такое уязвимость информации?
2. Какие злоумышленные действия характерны для СОД?
3. Назвать виды уязвимости информации.
4. Привести примеры уязвимости информационной безопасности.
5. Что такое уязвимость нулевого дня?
6. По каким признакам выполняется классификация уязвимостей безопасностей?
7. Какие уязвимости относятся к субъективным уязвимостям?
8. Как выполняется идентификация уязвимостей?
9. Какой математический аппарат используется для описания и расчета уязвимостей?
10. Что такое уровень уязвимости и как он оценивается?

Практическое занятие №4

Основные теории защиты информации. Модели безопасности

Цель занятия. Научиться строить модели безопасности для различных предметных областей.

Задание

1. Выполнить анализ основных видов моделей безопасности.

2. Решение ситуационных задач в группах по составлению неформальных политик безопасности для заданной автоматизированной системе.

Контрольные вопросы

1. Какие основные виды политики безопасности известны?
2. В чем суть дискреционной политики безопасности?
3. Какими условиями определяется мандатная политика безопасности?
4. Чем отличается политика безопасности информационных потоков от политики ролевого разграничения доступа?
5. Какова цель реализации политики изолированной программной среды?
6. Что такое матрица доступов?
7. Перечислить классические угрозы безопасности?

8. Как описываются информационные потоки по времени и по памяти?
9. Какие математические понятия используются в моделях безопасности?
10. Какая задача является алгоритмически разрешимой?

Практическое занятие №5
Сервисы безопасности

Цель занятия. Изучить основные сервисы безопасности компьютерной системы.

Задание

1. Выполнить сравнительный анализ сервисов безопасности компьютерной системы.

2. Предложить набор сервисов для заданной информационной системы.

Контрольные вопросы

1. Перечислить сервисы безопасности.
2. Каким условиям должны удовлетворять современные средства идентификации аутентификации?
3. Что такое разграничение доступа?
4. В чем суть ролевого управления?
5. Почему протоколирование и аудит относят к пассивным сервисам безопасности?
6. Какие функции выполняет экранирование как сервис безопасности?
7. Для каких целей используется туннелирование?
8. Что такое шифрование, криптография?
9. Какие существуют виды конфиденциальности?
10. Что такое стандарт X.800?