**Министерство образования и науки Российской Федерации**
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)**

**Институт инновационных технологий
Факультет информационных технологий
Кафедра информатики и защиты информации**

# «Информационная безопасность»

Курс лекций по дисциплине «Информационная безопасность»
для бакалавров ВлГУ обучающихся по направлению 230700 «Прикладная информатика»
*(шифр направления, название)*

**Владимир – 2014 г.**

# *СОДЕРЖАНИЕ*

# 1. Раздел. Основы информационной безопасности

## Тема 1. Сущность информационной безопасности

С точки зрения информационной безопасности (ИБ) **информация** – данные, представленные в виде, пригодном для хранения, обработки и передачи, и представляющие определенную ценность.

Существуют следующие формы представления информации:

- электронная,
- печатная,
- визуальная,
- аудио-форма.

**Защита информации (ЗИ)** – комплекс мероприятий по обеспечению конфиденциальности, целостности, доступности, учета и неотрекаемости информации.

**Конфиденциальность** – состояние информации, при котором ознакомиться с ней могут только уполномоченные лица.

**Целостность** – состояние информации, при котором изменять её могут только уполномоченные лица.

**Доступность** – возможность получения авторизованного доступа к информации со стороны уполномоченных лиц.

**Учёт** – фиксация и анализ всех действий уполномоченных лиц, выполняемых ими в рамках, контролируемых системой ИБ.

**Неотрекаемость** – предполагает, что отправитель информации не может отречься от факта отправления, а получатель – от факта получения.

Уполномоченными лицами считаются владелец информации и пользователи, получившие право работы с информацией от ее владельца.

**Информационная система (ИС)** – совокупность объектов и субъектов информационного взаимодействия.

Объекты – информационные ресурсы. Субъекты – пользователи или процессы, обрабатывающие информацию.

ИБ – более широкое понятие, чем понятия "защита информации", компьютерная безопасность", "сетевая безопасность", "безопасность данных".

**ИБ** – комплекс мероприятий по защите информации и обеспечению безопасного функционирования ИС

**Информационное пространство** – совокупность информационных систем, взаимодействующих между собой, причем одна часть этих систем может иметь интересы, прямо противоположные интересам другой.

Т.о. ИБ предполагает защиту одних ИС от других.

Для любой ИС характерны следующие понятия:

**Угроза** – возможность реализации несанкционированных действий (НД) в отношении ИС.

**Уязвимость** – незащищенность или ошибка в объекте, которая может привести к возникновению угрозы.

**Атака** – попытка практической реализации угрозы (успешная или нет).

**Ошибка** – непреднамеренное незапланированное действие, совершаемое субъектом, которое представляет или может представлять угрозу ИБ.

**Авария** – неумышленное происшествие с деструктивным воздействием на объект.

**Злоумышленник** – субъект, преследующий корыстные или деструктивные цели, противоречащие целям системы.

## Тема 2. Классификация конфиденциальной информации

Говоря о защите какой-либо информации, следует прежде всего выяснить, к какой категории она относится. Существует следующая классификация тайн по шести категориям:

1. государственная тайна,
2. коммерческая тайна,
3. банковская тайна,
4. профессиональная тайна,
5. служебная тайна,
6. персональные данные.

Последние пять категорий составляют конфиденциальную информацию.

Слово "конфиденциальный" происходит от латинского confidentia - доверие и в современном русском языке означает "доверительный, не подлежащий огласке, секретный. Слово "секрет" заимствовано из французского secret - "тайна". В знаменитом словаре В. Даля также названы аналогичные значения: "конфиденциальная" - "откровенная, по особой доверенности, неоглашаемая, задушевная"; "тайна" - "кто чего не знает, то для него тайна, все сокрытое, неизвестное, неведомое".

Таким образом, точки зрения этимологии можно сделать вывод о равнозначности понятий конфиденциальная информация, тайна и секрет.

Однако понятие тайны в правовой науке не полностью совпадает с понятием конфиденциальной информации, так как тайна означает ещё и правовой режим информации. В соответствии со ст. 2 ФЗ "Об информации ..." и ст. 2 ФЗ "Об участии в международном информационном обмене", конфиденциальная информация - документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации. Но не всегда информация с ограниченным доступом является документированной, например сведения, составляющие личную и семейную тайну, не обязательно зафиксированы на материальном носителе.

При анализе видов конфиденциальной информации возникают большие сложности, связанные с противоречивостью и недостатками отечественного законодательства. Согласно п. 2 ст. 10 ФЗ "Об информации ...", документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную.

Наиболее важными являются сведения, относящиеся к государственной тайне. В Законе "О государственной тайне" дано следующее определение: "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.

В законодательстве предусматривается наличие различного рода сведений, не содержащих гостайну, которые также охраняются законом. Так, охраняется тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, личная и семейная тайна (ст.23 Конституции РФ). Кроме того, сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются (ст.24).

Подлежащую защите информацию можно сгруппировать по следующим основаниям:

1. собственники информации;
2. области (сферы) деятельности, в которых используется информация;
3. лица и организации, на которых возложена защита данной информации.

Ту же информацию, подлежащую защите можно классифицировать по трем признакам:

1. по принадлежности,
2. по степени конфиденциальности (степени ограничения доступа),
3. по содержанию.

По принадлежности владельцами защищаемой информации могут быть:

- органы государственной власти и образуемые ими структуры (государственная тайна, служебная тайна, в определенных случаях коммерческая и банковская тайны);
- юридические лица (коммерческая, банковская служебная, адвокатская, врачебная, аудиторская тайны и т.п.);
- граждане (физические лица) - в отношении личной и семейной тайны, нотариальной, адвокатской, врачебной.

По степени конфиденциальности (степени ограничения доступа) в настоящее время можно классифицировать только информацию, составляющую государственную тайну. Согласно ст.8 Закона РФ "О государственной тайне", устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений:

- "особой важности",
- "совершенно секретно",
- "секретно".

Для остальных видов тайн данное основание классификации пока не разработано, при этом согласно ст. 8 Закона РФ "О государственной тайне", использование названных грифов секретности для засекречивания сведений, не отнесенных к государственной тайне, не допускается.

По содержанию защищаемая информация может быть разделена на политическую, экономическую, военную, научную, технологическую, личную, коммерческую и т.п.

Конфиденциальная информация бывает двух видов: подлежащая обязательной защите и не подлежащая. Обязательность защиты определяется собственником информации, за исключением случаев, предусмотренных законодательством. Так, в Законе говорится, что конфиденциальная информация государственных органов подлежит обязательной защите.

Указом Президента вводится шесть категорий конфиденциальной информации:

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.

Служебная информация

В Гражданском кодексе РФ дается следующее определение служебной информации: "Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности".

В "Положении о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти" (утверждено Постановлением Правительства Российской Федерации № 1233 от 3 ноября 1994г.) вводится понятие служебной информации ограниченного распространения: "несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью".

В государственных структурах еще может быть информация, имеющая политическую или иную ценность. Поскольку к служебной тайне она не относится, ей также необходимо присваивать гриф "для служебного пользования", применяемый в органах исполнительной власти.

# Тема 3. Современная концепция ИБ

Концепция ИБ является методологической основой для формирования и проведения в организации или на предприятии единой политики в области обеспечения ИБ.

Современная КИБ включает в себя следующие разделы:

1. цели и задачи обеспечения ИБ,
2. категории объектов защиты,
3. перечень угроз безопасности,
4. неформальная модель нарушителя,
5. принципы построения и направления работ по созданию и поддержанию СИБ,
6. средства обеспечения ИБ,
7. механизм функционирования СИБ.

**Цели и задачи обеспечения ИБ**

Основная цель обеспечения ИБ – защита субъектов информационных отношений (ИО) от возможного нанесения им материального, физического, морального или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования ИС или НСД к циркулирующей в ней информации и ее незаконного использования.

Субъекты ИО заинтересованы в обеспечении:

- конфиденциальности информации,
- целостности информации,
- своевременного доступа к информации,
- защиты от дезинформации,
- разграничения ответственности за нарушения законных прав (интересов) других субъектов ИО и установленных правил обращения с информацией,
- возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации,
- защиты части информации от незаконного ее тиражирования.

Для достижения основной цели защиты СИБ должна обеспечивать эффективное решение следующих задач:

- защита от вмешательства в процесс функционирования ИС посторонних лиц,
- обеспечение аутентификации субъектов, участвующих в информационном обмене,
- управление доступом уполномоченных лиц к аппаратным, программным и информационным ресурсам ИС,
- регистрация действий пользователей при использовании защищаемых ресурсов,
- контроль и поддержание целостности среды исполнения программ,
- защита от несанкционированной модификации и контроль целостности используемых в ИС программных средств,
- защита ИС от внедрения несанкционированных программ,
- защита конфиденциальной информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи,
- своевременное выявление новых источников угроз безопасности информации,
- создание условий для минимизации и локализации наносимого ущерба и ликвидация последствий нарушения ИБ.

**Категории объектов защиты**

Основными объектами защиты являются:

- информационные ресурсы с ограниченным доступом, представленные в виде документов и массивов информации, независимо от формы и вида их представления;
- процессы обработки, хранения и передачи информации,
- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, системы и средства защиты информации, объекты и помещения, в которых размещены компоненты ИС,
- персонал разработчиков и пользователей ИС и ее обслуживающий персонал.

# 2. Раздел. Уязвимости, угрозы, модель нарушителя

## Тема 4. Угрозы ИБ

По источникам появления угрозы подразделяют на:

8. Естественные – вызванные воздействиями на ИС объективных физических процессов или стихийных природных явлений, независящих от человека. Это стихийные бедствия и аварии, сбои и отказы оборудования;
9. Искусственные – это угрозы, вызванные деятельностью человека. Они, исходя из мотивации действий, делятся на:

- непреднамеренные, вызванные ошибками проектирования и разработки компонентов ИС, а также ошибками в действиях персонала в процессе эксплуатации; они бывают только внутренними;
- преднамеренные, вызванные действиями нарушителей; бывают внутренними и внешними.

Основные непреднамеренные угрозы:

1. неумышленные действия, приводящие к отказу системы или разрушению аппаратных, программных, информационных ресурсов (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);
2. неправомерное отключение оборудования или изменение режимов работы устройств и программ;
3. неумышленная порча носителей информации;
4. запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания) или осуществляющих необратимые изменения в системе (форматирование носителей информации, удаление данных и т.п.);
5. нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей);
6. заражение компьютера вирусами;
7. неосторожные действия, приводящие к разглашению конфиденциальной информации;
8. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
9. проектирование архитектуры ИС, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации;
10. игнорирование организационных ограничений (установленных правил) при работе в системе;
11. вход в систему в обход средств защиты (загрузка ОС со сменных магнитных носителей и т.п.);
12. некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;
13. пересылка данных по ошибочному адресу абонента (устройства);
14. ввод ошибочных данных;
15. неумышленное повреждение каналов связи.

Основные преднамеренные угрозы:

1. физическое разрушение ИС (путем взрыва, поджога и т.п.) или вывод из строя отдельных наиболее важных ее элементов (объектов и субъектов);
2. отключение или вывод из строя подсистем обеспечения функционирования ВС (электропитания, охлаждения и вентиляции, линий связи и т.п.);
3. действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т.п.);
4. внедрение агентов в число персонала системы;
5. вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих определенные полномочия;
6. применение подслушивающих устройств, дистанционная фото- и видеосъемка и т.п.;
7. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, отопления и т.п.);
8. перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя;

9. хищение носителей информации;
10. несанкционированное копирование носителей информации;
11. хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);
12. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
13. чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой защиты) или другими пользователями, используя недостатки многозадачных операционных систем и систем программирования;
14. незаконное получение паролей и других реквизитов разграничения доступа (используя халатность пользователей, путем подбора, путем имитации интерфейса системы и т.д.);
15. несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес и т.п.;
16. вскрытие шифров криптозащиты информации;
17. внедрение аппаратных и программных закладок и вирусов;
18. незаконное подключение к линиям связи с использованием пауз в действиях законного пользователя для передачи от его имени ложных сообщений;
19. незаконное подключение к линиям связи с целью подмены законного пользователя путем его отключения после входа в систему и успешной аутентификации.

По отношению к защищаемой информации существуют следующие угрозы:

1. Разглашение – это умышленные или неосторожные действия с конфиденциальной информацией, приведшие к ознакомлению с ней неуполномоченных лиц. Разглашение выражается в сообщении, передаче, предоставлении, пересылке, опубликовании, утере и в других формах обмена информацией.
2. Утечка – это бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена по техническим каналам.
3. Несанкционированный доступ – это преднамеренное овладение конфиденциальной информацией неуполномоченным лицом.

## Тема 5. Неформальная модель нарушителя

Анализ угроз безопасности позволяет построить неформальную модель нарушителя, которая отражает его практические и теоретические возможности, априорные знания, время и место действия и т.п.

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

При разработке модели нарушителя определяются предположения:

- о категориях лиц, к которым может принадлежать нарушитель;
- о мотивах действий нарушителя;
- о квалификации нарушителя и его технической оснащенности;
- о характере возможных действий нарушителей.

Существуют следующие типы нарушителей:

**"Неопытный (невнимательный) пользователь"** – сотрудник организации, который может предпринимать попытки выполнения запрещенных операций, доступа к защищаемым ресурсам организации с превышением своих полномочий, ввода некорректных данных и т.п. действия по ошибке, некомпетентности или халатности без злого умысла и использующий при этом только штатные (доступные ему) аппаратные и программные средства.

**"Любитель"** – сотрудник организации, пытающийся преодолеть систему защиты без корыстных целей и злого умысла, для самоутверждения или из "спортивного интереса". Может использовать различные методы получения дополнительных полномочий доступа к ресурсам (имен, паролей других пользователей), недостатки в построении системы защиты и доступные ему штатные и нештатные программы;

**"Мошенник"** – сотрудник организации, который может предпринимать попытки выполнения незаконных технологических операций, ввода подложных данных и тому подобные действия в корыстных целях, по принуждению или из злого умысла, но использующий при этом только штатные аппаратные и программные средства от своего имени или от имени другого сотрудника.

**"Внешний нарушитель (злоумышленник)"** – постороннее лицо или сотрудник организации, действующий целенаправленно из корыстных интересов, из мести или из любопытства, возможно в сговоре с другими лицами. Он может использовать весь набор радиоэлектронных способов нарушения безопасности информации, методов и средств взлома систем защиты, характерных для сетей общего пользования;

**"Внутренний злоумышленник"** – сотрудник подразделения организации, зарегистрированный как пользователь системы, действующий целенаправленно из корыстных интересов или мести за нанесенную обиду, возможно в сговоре с лицами, не являющимися сотрудниками организации. Он может использовать весь набор методов и средств взлома системы защиты:

- агентурные методы получения реквизитов доступа,
- методы и средства модификации технических средств,
- подключение к каналам передачи данных,
- внедрение программных закладок,
- использование специальных инструментальных и технологических программ.

При этом возможна комбинация воздействий как изнутри, так и извне организации – из сетей общего пользования.

Можно выделить три основных мотива нарушений:

- безответственность,
- самоутверждение,
- корыстный интерес.

Классификация нарушителей может быть проведена по:

- уровню знаний об ИС;
- уровню возможностей (используемым методам и средства);
- времени действия;
- месту действия.

Внутренним нарушителем может быть лицо из следующих категорий персонала организации:

1. зарегистрированные конечные пользователи ИС организации (сотрудники подразделений организации);
2. сотрудники подразделений организации, не допущенные к работе с ИС;
3. персонал, обслуживающий технические средства ИС организации (инженеры, техники);
4. сотрудники отделов разработки и сопровождения ПО (прикладные и системные программисты);

5. технический персонал, обслуживающий здания (уборщики, электрики, сантехники и другие сотрудники, имеющие доступ в здания и помещения, где расположены компоненты ИС);
6. сотрудники службы безопасности организации;
7. руководители различных уровней.
8. Категории лиц, которые могут быть внешними нарушителями:
9. уволенные сотрудники организации;
10. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго-, водо-, теплоснабжения и т.п.);
11. посетители (приглашенные представители организаций, граждане) представители фирм, поставляющих технику, программное обеспечение, услуги и т.п.;
12. члены преступных организаций, сотрудники спецслужб или лица, действующие по их заданию;
13. лица, случайно или умышленно проникшие в ИС организации из внешних (по отношению к организации) сетей телекоммуникации.

Пользователи и обслуживающий персонал из числа сотрудников организации имеют наиболее широкие возможности по осуществлению несанкционированных действий, вследствие наличия у них определенных полномочий по доступу к ресурсам и хорошего знания технологии обработки информации и защитных мер. Действия этой группы лиц напрямую связано с нарушением действующих правил и инструкций.

Уволенные сотрудники могут использовать для достижения целей свои знания о технологии работы, защитных мерах и правах доступа.

Профессиональные хакеры имеют наиболее высокую техническую квалификацию и знания о слабостях программных средств, используемых в ИС. Наибольшую угрозу представляют при взаимодействии с работающими и уволенными сотрудниками организации и криминальными структурами.

Принимаются следующие ограничения и предположения о характере действий возможных нарушителей:

1. работа по подбору кадров не всегда исключает возможность создания коалиций нарушителей, т.е. объединения (сговора) и целенаправленных действий двух и более нарушителей – сотрудников организации;
2. нарушитель скрывает свои несанкционированные действия от других сотрудников организации;
3. несанкционированные действия могут быть следствием ошибок пользователей, администраторов безопасности, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации;
4. в своей противоправной деятельности вероятный нарушитель может использовать любое имеющееся средство перехвата информации, воздействия на информацию и ИС, финансовые средства для подкупа персонала, шантаж и другие средства и методы для достижения стоящих перед ним целей.

## Тема 6. Каналы утечки и НСД к информации

При выявлении каналов утечки и НСД к информации необходимо рассматривать как основные технические средства обработки информации:

- вычислительная техника,
- соединительные линии,
- распределительные и коммутационные устройства,

так и вспомогательные технические средства и системы:

- системы электропитания и заземления,
- телефонной и радиосвязи,
- охранной и пожарной сигнализации,
- электробытовые приборы.

Важное значение имеют вспомогательные средства, выходящие за пределы контролируемой зоны, а также посторонние провода и кабели, к ним не относящиеся, но проходящие через помещения, где установлены ТСОИ, металлические трубы систем отопления, водоснабжения и другие токопроводящие конструкции.

Кроме того, каналы утечки информации могут быть связаны с параметрами самих помещений.

Все каналы утечки и НСД разделяют на прямые и косвенные. Под прямыми понимают такие каналы, использование которых требует проникновения в помещения, где расположены компоненты ИС. Для косвенных каналов доступ в помещение не требуется.

По типу основного средства, используемого для реализации угрозы все возможные каналы можно условно разделить на три группы, где средствами являются: человек, программа или аппаратура.

В зависимости от способов перехвата информации, от физической природы сигналов и среды их распространения технические каналы утечки информации можно разделить на:

- электромагнитные,
- электрические,
- параметрические.

Для **электромагнитных** каналов характерными являются побочные излучения:

- ЭМ излучения элементов ТСОИ – носителем информации является электрический ток, сила которого, напряжение, частота или фаза изменяются по закону информационного сигнала (утечка за счет побочного излучения ЭВМ),
- ЭМ излучения на частотах работы высокочастотных генераторов ВТСС – в результате внешних воздействий информационного сигнала возможна непреднамеренная модуляция ВЧ сигналов генераторов бытовой техники.
- ЭМ излучения на частотах самовозбуждения усилителей низкой частоты ТСПИ – это возможно за счет преобразования ООС в паразитные ПОС, что приводит к переводу усилителя из режима усиления в режим автогенерации сигнала, который оказывается промодулированным информационным сигналом (утечка по сети радиосвязи).

Причинами возникновения электрических каналов являются:

- наводки ЭМИ ТСОИ – возникают при излучении элементами ТСОИ информационных сигналов, а также при наличии гальванической связи элементов и посторонних проводников или линий ВТСС (наводки на линии коммуникаций),
- просачивание информационных сигналов в цепи электропитания – возможно при наличии магнитной связи между трансформатором электропитания и трансформаторами ТСОИ,
- просачивание информационных сигналов в цепи заземления – образуется за счет гальванической связи цепей заземления с проводниками выходящими за пределы контролируемой зоны, в том числе с нулевым проводом сети электропитания,
- съем информации с использованием аппаратных закладок, т.е. передатчиков, установленных в ТСОИ, сигналы которых модулируются информационным сигналом и принимаются за пределами контролируемой зоны.

Параметрические каналы утечки информации формируются путем высокочастотного облучения ТСОИ, в результате которого высокочастотный сигнал модулируется информационным.

## Каналы утечки акустической информации

Их можно разделить на:

- воздушные,
- вибрационные,
- электроакустические,
- оптико-электронные,
- параметрические.

В воздушных каналах средой передачи является воздух, для перехвата сигналов используются миниатюрные или направленные микрофоны совместно с диктофонами или передатчиками. Автономные устройства, объединяющие микрофоны и передатчики, называются аудиозакладками. Перехваченная информация может передаваться по радиоканалу, сети электропитания или посторонним проводникам.

В вибрационных (или структурных) каналах средой распространения сигнала являются конструкция здания и коммуникаций. В этом случае для перехвата сигналов используются контактные, электронные (с усилителем) или радиостетоскопы.

Электроакустические каналы образуются за счет преобразований акустических сигналов в электрические двумя способами:

- путем высокочастотного навязывания,
- путем перехвата через ВТСС.

Первый способ используется, например, в устройствах, встраиваемых в телефонный аппарат или подключаемых к телефонной линии и называемых "телефонным ухом". При подаче в линию кодированного сигнала или при дозвоне к контролируемому телефону к линии подключается устройство, передающее разговор на другой телефонный номер.

Второй способ используется тогда, когда ВТСС сами содержат электроакустические преобразователи. Например, датчики пожарной сигнализации и громкоговорители. Используемый в них эффект называют микрофонным.

При облучении лазерным лучом стекол, зеркал, картин и других отражающих поверхностей создается **оптико-электронный** канал утечки информации. Отраженный луч модулируется акустическим сигналом, при демодуляции выделяется речевая информация. Это так называемые "лазерные микрофоны", работающие в инфракрасном диапазоне.

Параметрический канал утечки образуется в результате воздействия акустического поля на элементы высокочастотных генераторов, что приводит к изменениям параметров ВЧ сигнала, например, его модуляции информационным сигналом. Параметрический канал может быть создан и путем высокочастотного облучения помещения, где установлены полуактивные закладные устройства, имеющие элементы, параметры которых изменяются по закону акустического сигнала.

Акустический канал вообще может быть источником утечки не только речевой информации. Например, после статистической обработки звука, возникающего при печатании на клавиатуре можно получить вводимую информацию.

## Перехват информации при передаче по каналу связи

Интерес со стороны злоумышленника к информации, передаваемой на расстояние, вызван тем, что протяженные каналы связи невозможно физически контролировать. В зависимости от вида канала связи технические каналы перехвата информации можно разделить на:

- электромагнитные,
- электрические,
- индукционные.

Электромагнитный канал перехвата используется для прослушивания телефонных разговоров по радиоканалу и спутниковой связи. В этом случае применяются стандартные технические средства.

Электрический канал перехвата информации, передаваемой по кабельным линиям связи, предполагает контактное подключение к этим линиям. Устройства, подключаемые к телефонным линиям связи и содержащие радиопередатчики, называются телефонными закладками.

Но непосредственное электрическое подключение аппаратуры перехвата является компрометирующим признаком и может вызвать изменение характеристик самого канала связи. Т.е. их можно обнаружить техническими средствами. Поэтому чаще используется индукционный канал перехвата, не требующий контактного подключения. Современные индукционные датчики способны снимать информацию с экранированных кабелей.

Единственными надежными методами защиты информации при передаче ее по открытым каналам связи является криптографические и стеганографические методы.

**Утечка видовой информации**

Видовая информация получается техническими средствами в виде изображений объектов путем наблюдения и съемки объекта а также путем копирования документов. В качестве технических средств используются оптические приборы, видео- и телекамеры, приборы ночного видения.

# 3. Раздел. Средства, используемые злоумышленником

## Тема 7. Технические средства добывания информации

Злоумышленник, используя различные каналы утечки и НСД к информации применяет различные технические и программные средства. Технические средства по области применения можно разделить на следующие классы:

1. Радио-микрофоны:
- по типу электропитания (с автономным питанием, с питанием от телефонной сети, с питанием от электросети);
- по управлению (управляемые дистанционно, с функцией включения по голосу);
- по типу способу информации (с постоянной передачей, с накоплением и быстрой передачей информации).

2. Электронные уши:
- проводные микрофоны,
- направленные микрофоны,
- лазерные микрофоны,
- стетоскопы,
- гидроакустические микрофоны.

3. Средства перехвата телефонной связи:
- датчик внутри телефонного аппарата,
- датчик непосредственного подключения к линии,
- индукционный датчик,
- средства перехвата радиосвязи.

4. Средства скрытого наблюдения и поиска:
- оптические,
- фотографические,
- ночного видения,

- определения местоположения.

5. Средства контроля компьютеров и сетей:
- средства контроля монитора,
- средства контроля магистрали сети,
- аппаратные закладки,
- программные закладки,
- компьютерные вирусы.

6. Средства приема, записи и управления:
- приемники для радиозакладок,
- устройства накопления и записи,
- ретрансляторы,
- средства ускоренной передачи,
- устройства дистанционного управления,

## Тема 8. Программные средства добывания информации

Программными средствами добывания информации являются различные вредоносные программы.

**Вредоносная программа** – некоторый программный код (модуль, скрипт, макрос), созданный с целью нарушения ИБ.

Основой реализации программных средств добывания информации является наличие уязвимостей в ПО КС. Уязвимости могут быть вызваны как ошибками в алгоритмах, так и намеренными действиями разработчиков ПО. Во втором случае они представляют собой недокументированные (скрытые) функции программы, которые создаются с целью:
- обеспечения тестирования программы,
- облегчения сборки сложных программных комплексов,
- создания скрытого средства доступа к программе, остающегося и после сборки.

### Программные закладки

**Программная закладка** – вредоносная программа, реализованная как одна из скрытых функций системы. Создается разработчиками системы.

По воздействию программных закладок на информационную систему их подразделяют на три типа:
1. вносят произвольные искажения в коды программ, находящихся в оперативной памяти компьютера,
2. переносят фрагменты информации из одних областей оперативной или внешней памяти компьютера в другие,
3. искажают выводимую на внешние компьютерные устройства или канал связи информацию, полученную в результате работы других программ.

По модели функционирования ПЗ делятся на:
1. программно-аппаратные закладки, ассоциированные с аппаратными средствами компьютера (их средой обитания, как правило, является BIOS),
2. загрузочные закладки, ассоциированные с программами начальной загрузки,
3. драйверные закладки, ассоциированные с драйверами,
4. прикладные закладки, ассоциированные с ППО общего назначения (текстовые редакторы, утилиты, антивирусные мониторы и программные оболочки),

5. исполняемые закладки, ассоциированные с исполняемыми программными модулями, содержащими код этой закладки (чаще всего эти модули представляют собой пакетные файлы),
6. закладки – имитаторы, интерфейс которых совпадает и интерфейсом некоторых служебных программ, требующих ввод конфиденциальной информации (паролей, криптографических ключей, номеров кредитных карточек),
7. замаскированные закладки, которые маскируются под программные средства оптимизации работы компьютера (архиваторы, дефрагментаторы дисков) или под программы игрового и развлекательного назначения.

Методика защиты от ПЗ и других программных средств добывания информации реализуется в трех направлениях:

1. не допустить внедрения ВП в компьютерную систему,
2. выявить ВП,
3. удалить ВП.

Универсальным средством защиты от внедрения ВП является создание **изолированного** компьютера. Компьютер называется изолированным, если выполнены следующие условия:

- в нем установлена система BIOS, не содержащая программных закладок;
- операционная система проверена на наличие в ней закладок;
- достоверно установлена неизменность BIOS и операционной системы для данного сеанса;
- на компьютере не запускалось и не запускается никаких иных программ, кроме уже прошедших проверку на присутствие в них закладок;
- исключен запуск программ, проверенных в каких-либо иных условиях, кроме перечисленных выше, т.е. вне изолированного компьютера.

Для определения степени изолированности компьютера может использоваться модель ступенчатого контроля. Сначала проверяется, нет ли изменений в BIOS. Затем, если все в порядке, считывается загрузочный сектор диска или драйвера операционной системы, которые, в свою очередь, также анализируются на предмет внесения в них несанкционированных изменений. И наконец, с помощью операционной системы запускается драйвер контроля вызовов программ, который следит за тем, чтобы в компьютере запускались только проверенные программы.

Выявление внедренного кода программной закладки заключается в обнаружении признаков его отсутствия в компьютерной системе. Эти признаки можно разделить на следующие два класса:

1. визуальные,
2. обнаруживаемые средствами тестирования и диагностики.

К визуальным признакам относятся ощущения и наблюдения пользователя КС, который отмечает определенные отклонения в ее работе (изменяется состав и длина файлов, старые файлы куда-то пропадают, а вместо них появляются новые, программы начинают работать медленнее, или заканчивают свою работу слишком быстро, или вообще перестают запускаться).

Несмотря на то, что суждение о наличии таких признаков является субъективным, они часто свидетельствуют о наличии неполадок и необходимости проведения дополнительных проверок присутствия программных закладок.

Признаки, выявляемые с помощью средства тестирования и диагностики, характерны для различных видов вредоносных программ. Основные виды признаков:

- несогласованное изменение параметров файлов (размер, дата/время, контрольная сумма),
- наличие подозрительного кода (сигнатуры).

Загрузочные закладки успешно обнаруживаются антивирусными программами. Средства проверки целостности данных на диске позволяют успешно выявлять

изменения, вносимые в файлы. Также используется поиск фрагментов кода программных закладок по характерным для них сигнатурам.

### Клавиатурные шпионы

Клавиатурные шпионы используются злоумышленником для перехвата паролей пользователей операционной системы, а также для определения их прав доступа.

Клавиатурные шпионы можно разделить по способу перехвата паролей на три типа: *имитаторы, фильтры и заместители.*

Для защиты от внедрения клавиатурных шпионов необходимо выполнение следующих условий:

- работа системных процессов ввода паролей должна быть скрыта от программ прикладного уровня,
- недопустимо переключение раскладок клавиатуры во время ввода пароля,
- обслуживание программных модулей, участвующих в работе с паролями пользователей, разрешается только системному администратору.

### Троянские программы

**Троянская программа** – вредоносная программа, выполняющая несанкционированные и недокументированные действия.

Троянская программа состоит из двух частей: серверной и клиентской.

**Серверная часть** – это исполняемый файл, который тем или иным путем внедряется на машину пользователя, и выполняет получаемые от удаленного клиента запросы.

**Клиентская часть** запускается на машине злоумышленника, который, связавшись с серверной частью, может выполнять различные действия: изменение файлов, чтение информации с монитора, контроль вводимых и выводимых данных.

Проникновение на компьютер троянских программ осуществляется через:

- новые программы,
- файлы, прикрепленные к почтовым сообщениям,
- исполнимые файлы с внешними признаками неисполнимых.

Для обнаружения и защиты от троянских программ используются:

- антивирусы,
- межсетевые экраны,
- сканеры уязвимостей.

## Тема 9. Компьютерные вирусы

**Вирус** – вредоносная программа, которая кроме выполнения деструктивных действий может автоматически размножаться (возможно с самомодификацией) и распространяться на новые ИС.

Вирусы можно классифицировать по следующим признакам:

- среда обитания,
- способ заражения,
- воздействие на ресурсы,
- особенности алгоритма.

В зависимости от среды обитания вирусы можно разделить на:

- *Сетевые вирусы* распространяются по компьютерным сетям.
- *Файловые вирусы* внедряются главным образом в исполняемые модули, но могут внедряться и в другие типы файлов.
- *Загрузочные вирусы* внедряются в загрузочный сектор диска.
- *Файлово-загрузочные* вирусы заражают как файлы, так и загрузочные сектора дисков.

По способу заражения вирусы делятся на резидентные и нерезидентные. *Резидентный вирус* при заражении компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т. п.) и внедряется в них.

*Нерезидентные вирусы* не заражают память компьютера и выполняют свои функции только во время выполнения программного модуля, в котором находятся.

По степени воздействия вирусы можно разделить на следующие виды:

- **неопасные,** не мешающие работе компьютера, но уменьшающие объем свободной памяти, выдающие какие-либо графические или звуковые эффекты,
- **опасные** вирусы, которые могут привести к различным нарушениям в работе компьютера,
- **очень опасные**, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

По особенностям алгоритма можно выделить:

**простейшие вирусы**, они изменяют содержимое файлов и секторов диска,

**вирусы-репликаторы** (черви), которые распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии.

**вирусы-невидимки,** (стелс-вирусы), которые перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска,

**полиморфные вирусы**, содержащие алгоритмы шифрования-дешифрования, из-за которых копии одного и того же вируса могут не иметь ни одной повторяющейся цепочки байтов.

## Нерезидентные вирусы

### *COM-вирусы*

Заражение.

Под заражением понимается присоединение вирусом своего кода к файлу. При этом вирус должен так модифицировать файл, чтобы во время его исполнения был выполнен переход на код вируса.

Вирусный код может быть записан в начало, конец или в середину файла. Чтобы был выполнен переход на вирус, зараженная программа модифицируется: изменяются три первых байта программы на команду перехода на код вируса. Исходные байты сохраняются в области данных вируса.

Алгоритм работы.

1. восстановление трех первых байтов программы,
2. поиск подходящего для заражения файла,
3. заражение,
4. выполнение вредоносных действий,
5. передача управления той программе, в которой находится вирус.

Распространение вируса.

1. автор разрабатывает исходный текст вируса,
2. исходный текст компилируется, создается исполняемый файл (запускающая програма),
3. запускающая программа доставляется на машину, которую надо заразить и исполняется на ней.

### *EXE-вирусы*

Заражение.

Как и для COM-программ вирус может быть записан в начало, конец или в середину файла. Чтобы вирус получил управление, должен быть изменен заголовок EXE-файла.

Алгоритм работы.

1. поиск подходящего EXE-файла,
2. сохранение заголовка заражаемого файла,
3. заражение,
4. выполнение вредоносных действий,
5. вычисление корректных значений сегментных регистров для передачи управления зараженной программе,
6. передача управления программе.

Распространение вируса.

Аналогично COM-вирусу.

## Резидентные вирусы

### *COM-вирусы*

Все резидентные программы строятся одинаково и состоят из секции инициализации и резидентной части. Резидентная часть состоит из одной или нескольких подпрограмм-обработчиков прерываний. Секция инициализации изменяет вектора в таблице прерываний так, чтобы они указывали на точки входа подпрограмм резидентной части.

Секция инициализации:

1. получает управление при запуске зараженной программы,
2. проверяется, установлена ли в памяти резидентная часть вируса,
3. если резидентная часть не установлена, то выполняются действия:

- поиск области памяти для размещения резидентной части.
- копируется резидентная часть,
- изменяются вектора прерываний.

Резидентная часть.

1. анализирует вызова прерываний работы с диском,
2. если обнаружен переход по дереву каталогов, то выполняется поиск и заражение подходящего COM-файла,
3. заражение,
4. выполнение вредоносных действий,
5. передача управления той программе, в которой находится вирус.

### *EXE-вирусы*

Аналогично работе резидентного COM-вируса. Выполняется работа с заголовками exe-файлов.

### *Загрузочные вирусы*

Загрузочными называются вирусы, способные заражать загрузочные сектора и загрузочные записи дисков.

Заражение.

Изменение загрузочного сектора или загрузочной записи (добавление своего кода в свободную область).

Алгоритм работы.

При начальной загрузке компьютера с зараженного диска:

1. выполняется копирование зараженной загрузочной области в свободную область памяти,
2. изменяются значения векторов прерываний,
3. фрагмент загрузочной области без кода вируса копируется в память по адресу 0000:7C00h и ему передается управление.

При обращении к новому диску:

4. выполняется проверка на то, заражена ли область начальной загрузки,
5. если нет, то она заражается,
6. заражение,

7. выполнение вредоносных действий,
8. передача управления той программе, в которой находится вирус.

Распространение вируса.

Чтобы вирус заразил новый компьютер достаточно просто попробовать загрузиться с зараженной дискеты, для этого ей совсем не обязательно быть загрузочной.

*Windows-вирусы*

Чтобы оставить выполняемый код резидентным в Windows существуют 3 способа:

- зарегистрировать программу, как одно из приложений работающих в данный момент,
- выделить блок памяти при помощи DPMI-вызова и скопировать в него код вируса,
- остаться резидентно как драйвер.

Обращения к файлам выполняется через перехват либо прерывания 21h, либо системных вызовов API.

*Макровирусы*

Макровирусы перехватывают системные вызовы, возникающие при работе с документами и таблицами. Для этого они переопределяют один или несколько системных макросов и функций. При этом даже не требуется делать проверку на наличие этого вируса новый макрос уничтожает старый с таким же именем.

*Стелс-вирусы*

Стелс-вирусы различными способами скрывают факт своего присутствия в системе.

Загрузочные стелс-вирусы используют два способа:

- вирус перехватывает команду чтения зараженного сектора и подставляет вместо него оригинал,
- при запуске любой программы восстанавливается зараженный сектор, а при ее завершении он снова заражается – используется контроль INT 21h.

Большинство файловых стелс-вирусов используют приемы описанные выше. Но при использовании первого способа вирусы становятся громоздки, т.к. приходится обрабатывать много различных событий. Часто вирусы используют часть стелс-функций, например, подменяют размер зараженного файла исходным размером.

*Полиморфные вирусы*

Полиморфные вирусы – это такие вирусы, которые крайне сложно или вообще невозможно обнаружить с использованием вирусных сигнатур (участков кода, характерных для конкретного вируса) из-за того, что код вируса при заражении нового файла изменяется.

Основные способы изменения кода вируса:

- добавление инструкций, не изменяющих алгоритм работы вируса,
- использование взаимозаменяемых инструкций и изменение порядка следования независимых команд,
- перестановка инструкций с добавлением команд перехода,
- перестановка данных с изменением значений смещения в командах чтения-записи.

Полиморфные вирусы могут использовать несколько наборов постоянных алгоритмов шифрования для изменения своего кода при новом заражении. Расшифровка производится самим вирусом уже непосредственно во время выполнения.

### Антивирусные программы

Основные функции антивирусов:

- обнаружение вирусов,
- препятствие работе вирусов,
- удаление вирусов и устранение последствий их работы.

Классы антивирусов:

1. Детекторы (сканеры). Позволяют обнаруживать файлы, зараженные одним из известных вирусов по признаку наличия сигнатуры вируса. Основное преимущество – высокая надежность в обнаружении известных вирусов. Детекторы с функцией доктора позволяют вылечить файл от вируса.
2. Ревизоры. Их работа основывается на сравнении состояния программ и системных областей дисков с сохраненными ранее. Основным признаком того, что эти изменения были сделаны именно вирусом является наличие одинаковых изменений в разных программах. Преимущество – можно обнаружить неизвестные вирусы.
3. Мониторы (фильтры). Располагаются резидентно в оперативной памяти и перехватывают те обращения к операционной системе, которые могут использоваться вирусами, и сообщают о них пользователю. Пользователь может разрешить или запретить выполнение соответствующей операции, а также проверить программу, инициировавшую обращение на наличие вирусов. Преимущество использования – позволяют обнаружить многие вирусы на ранней стадии, когда вирус еще не успел размножиться.
4. Иммунизаторы (вакцины). Модифицируют программы и диски таким образом, что это не отражается на работе программ, вирус, от которого производится вакцинация, считает эти программы или диски уже зараженными.

# 4. Раздел. Методология защиты информации

## Тема 10. Принципы построения и направления работ по созданию СИБ

### Принципы построения СИБ

1. **Принцип системности.** Системный подход предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности.
2. **Принцип комплексности** предполагает согласованное применение разнородных средств при построении целостной СИБ, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.
3. **Принцип непрерывности защиты.** ЗИ – это не разовое мероприятие, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИС, начиная с самых ранних стадий проектирования, а не только на этапе ее эксплуатации.
4. **Принцип разумной достаточности.** Создать абсолютно непреодолимую систему безопасности принципиально невозможно. Важно правильно выбрать

тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми.

5. **Принцип гибкости управления и применения.** Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень безопасности. Данный принцип подразумевает возможность изменения уровня защищенности в зависимости от изменения внешних условий и требований с течением времени.
6. **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 возможность ее преодоления даже разработчику защиты.
7. **Принцип простоты применения защитных мер и средств.** Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе законных пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций.

## Направления работ по созданию СИБ

Разработка СИБ должна проходить в трех параллельных направлениях: методическом, организационном и техническом.

**Методическое направление** предусматривает решение следующих вопросов:

1. разработка методики определения и описания информационных потоков (ИП), т.е. формального и точного описания порядка работы с информацией;
2. определение категорий конфиденциальной информации и разработка классификации информации по этим категориям;
3. создание матрицы конфиденциальности;
4. определение возможных пути разглашения конфиденциальной информации т.е. модели угроз;
5. определение модели нарушителя для каждой угрозы и атаки;
6. определение уровней риска для всей матрицы конфиденциальности, т.е. вероятности реализации каждой атаки и стоимости ущерба при каждой атаке.

В рамках **организационного направления** работ создается совокупность правил (руководящих документов), регламентирующих деятельность сотрудников при обращении с информацией независимо от форм ее представления.

Организационное направление включает в себя:

1. анализ информационной структуры предприятия;
2. разработку регламента обеспечения безопасности;
3. применение методологии при работе с персоналом;
4. работы по уточнению требований к характеристикам защищенности системы;
5. разнесение субъектов и объектов информационных отношений по категориям конфиденциальности;
6. определение допустимых форм их взаимодействий и т.д.

**Регламент обеспечения безопасности** – комплект документов, регламентирующий правила обращения с конфиденциальной информацией (КИ) в зависимости от фазы ее обработки и категории конфиденциальности. В регламенте должен быть определен комплекс методических, административных и технических мер, включающих в себя:

1. создание подразделения, ответственного за обеспечение КИ;
2. определение порядка допуска сотрудников к КИ и обязанностей, ограничений и условий, накладываемых на них;
3. определение сотрудников, допущенных к КИ;

4. классификация КИ и работ с ней по категориям;
5. порядок изменения категории конфиденциальности работ и информации;
6. требования к помещениям, в которых проводятся конфиденциальные работы и обрабатывается КИ, по категориям;
7. требования к конфиденциальному делопроизводству;
8. требования к учету, хранению и обращению с конфиденциальными документами;
9. меры по контролю за обеспечением конфиденциальности работ и информации;
10. план мероприятий по противодействию атаке на КИ;
11. план мероприятий по восстановлению КИ;
12. определение ответственности за разглашение КИ.

В рамках **технического направления** работ создается комплекс технических средств и технологий ЗИ при ее обработке, хранении и передаче, включая криптографические средства. Для этого проводится сбор исходных данных для разработки технических предложений по оснащенности автоматизированной системы обработки, хранения и передачи информации средствами ЗИ, позволяющими реализовать требуемый уровень защищенности.

## Тема 11. Методы и средства обеспечения ИБ

### Методы обеспечения ИБ

1. Управление доступом – метод ЗИ регулированием использования всех ресурсов ИС. Управление доступом включает следующие функции защиты:
   - идентификация пользователей, персонала и ресурсов системы,
   - аутентификация объектов и субъектов,
   - проверка полномочий субъекта на соответствие регламенту безопасности,
   - разрешение и создание условий работы в пределах регламента,
   - регистрация обращений к защищаемым ресурсам,
   - реагирование при попытках несанкционированных действий (отказ в запросе, задержка работы, отключение, сигнализация).
2. Препятствие – метод физического преграждения пути злоумышленнику к ресурсам ИС.
3. Маскировка – методы криптографической и стеганографической защиты.
4. Регламентация – метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму.
5. Принуждение – метод защиты, при использовании которого пользователи и персонал ИС вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.
6. Побуждение – такой метод защиты, который побуждает пользователей и персонал системы не нарушать сложившиеся моральные нормы.

Перечисленные методы ОБ реализуются на практике применением различных средств защиты, которые делятся на два класса:

1. Формальные – выполняющие защитные функции по заранее определенной процедуре без непосредственного участия человека;
2. Неформальные – определяются целенаправленной деятельностью человека либо регламентируют эту деятельность.

**Средства защиты информации:**

1. Технические средства реализуются в виде электрических, электромеханических и электронных устройств. Делятся на аппаратные и физические.
   - Под аппаратными средствами понимают устройства, встраиваемые непосредственно в аппаратуру ИС, или устройства, которые сопрягаются с этой аппаратурой по стандартному интерфейсу (электронные ключи, схемы аппаратного шифрования).
   - Физические средства реализуются в виде автономных устройств и систем (оборудование сигнализации, двери, решетки).
2. Программные средства представляют собой ПО, специально предназначенное для выполнения функций защиты информации. Данные средства составляли основу механизмов защиты на ранних стадиях развития технологий ИБ. Программные средства по функциям делятся на:
   - средства контроля доступа,
   - средства аудита,
   - средства блокирования атак (межсетевые экраны),
   - средства поиска уязвимостей (сканеры безопасности),
   - средства анализа кодов программ,
3. Организационные средства защиты представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые на всех этапах жизненного цикла ИС (строительство помещений, проектирования ИС, монтаж и наладка оборудования, испытания и эксплуатация).
4. Законодательные средства защиты определяются законами и другими документами, регламентирующими правила использования, обработки и передачи КИ и устанавливающими ответственность за нарушение правил.
5. Морально-этические средства защиты реализуются в виде всевозможных норм, которые складываются по мере развития ИТ. Эти нормы не являются обязательными как законы, но их несоблюдение может привести к потере авторитета или престижа человека или организации.

В настоящее время имеются следующие тенденции развития средств ОИБ:

1. аппаратная реализация основных функций защиты,
2. создание комплексных средств защиты, выполняющих несколько защитных функций,
3. унификация и стандартизация алгоритмов и технических средств.

# 5. Раздел. Механизмы информационной безопасности

## Тема 12. Идентификация и аутентификация

Существуют следующие концептуальные механизмы ИБ:

1. Идентификация и аутентификация;
2. Контроль и управление доступом;
3. Протоколирование и аудит;
4. Шифрование:
5. Контроль целостности;
6. Экранирование.

Для надежной ЗИ необходима комплексная реализация всех перечисленных механизмов. Некоторые из них могут быть реализованы в более полной мере, другие –

нет. Защита ИС в первую очередь зависит от реализации механизма идентификации и аутентификации

**Идентификатор** – уникальный набор символов, однозначно соответствующий объекту или субъекту в данной системе.

**Идентификация** – распознавание участника процесса информационного взаимодействия (ИВ) перед тем, как к нему будут применены какие-либо аспекты ИБ.

**Пароль** – секретный набор символов, позволяющий подтвердить соответствие субъекта предъявленному им идентификатору.

**Аутентификация** – обеспечение уверенности в том, что участник ИВ идентифицирован верно.

**Профиль** – набор установок и конфигураций для данного субъекта или объекта и определяющий его работу в ИС.

**Авторизация** – формирование профиля прав для конкретного участника ИВ.

Субъект может подтвердить свою подлинность, предъявив по крайней мере одну из следующих сущностей:

- нечто, что он знает (пароль, криптографический ключ и т.п.);
- нечто, чем он владеет (электронный ключ, смарт-карта и т.п.);
- нечто, что есть часть его самого (свои биометрические характеристики).

Аутентификация бывает односторонней (обычно субъект доказывает свою подлинность системе) и двусторонней (взаимной).

Надежная идентификация и аутентификация затруднена по целому ряду причин.

1. В ИС между сторонами может не существовать доверенного маршрута; это значит, что в общем случае данные, переданные субъектом, могут не совпадать с данными, полученными и использованными для проверки подлинности.
2. Почти все аутентификационные сущности можно узнать, украсть или подделать.
3. Имеется противоречие между надежностью аутентификации, с одной стороны, и удобствами субъекта с другой. Так, из соображений безопасности необходимо с определенной частотой просить пользователя повторно вводить аутентификационную информацию.
4. Чем надежнее средство защиты, тем оно дороже.

## Парольная аутентификация

Главное достоинство ***парольной аутентификации*** – простота. Недостаток – это самое слабое средство проверки подлинности.

Основные нарушения при создании и использовании паролей:

- простой пароль,
- использование стандартных значений из какой-либо документации, которые никогда не изменяют,
- запись пароля на тех предметах, где его можно прочитать, подсмотреть и т.д.
- сообщение пароля другому сотруднику.

Меры, позволяющие повысить надежность парольной защиты:

- наложение технических ограничений (длина, использование букв, цифр, знаков);
- управление сроком действия паролей;
- ограничение доступа к файлу паролей;
- ограничение числа неудачных попыток входа в систему;
- обучение пользователей;
- использование программных генераторов паролей, которые основываясь на некоторых правилах, могут порождать сложные, но запоминающиеся пароли,
- одноразовые пароли.

## Одноразовые пароли

Пусть имеется односторонняя функция $f$ (то есть функция, вычислить обратную которой за приемлемое время не представляется возможным). Эта функция известна и пользователю, и серверу аутентификации.

Пусть имеется секретный ключ $K$, известный только пользователю.

На этапе начального администрирования пользователя функция $f$ применяется к ключу $K$ $n$-раз, после чего результат сохраняется на сервере.

После этого процедура проверки подлинности пользователя выглядит следующим образом:

- сервер присылает на пользовательскую систему число ($n$-1);
- пользователь применяет функцию $f$ к секретному ключу $K$ ($n$-1) раз и отправляет результат по сети на сервер аутентификации;
- сервер применяет функцию $f$ к полученному от пользователя значению и сравнивает результат с ранее сохраненной величиной. В случае совпадения подлинность пользователя считается установленной, сервер запоминает новое значение (присланное пользователем) и уменьшает на единицу счетчик ($n$).

Поскольку функция $f$ необратима, перехват пароля и получение доступа к серверу аутентификации, не позволяют узнать секретный ключ $K$ и предсказать следующий одноразовый пароль.

Другой подход к реализации одноразовых паролей состоит в генерации нового пароля через небольшой промежуток времени (например, каждые 60 секунд), для чего могут использоваться программы или smart-карты. Для этого необходимо выполнение условий:

- Сервер аутентификации должен знать алгоритм генерации паролей и ассоциированные с ним параметры;
- Часы клиента и сервера должны быть синхронизированы.

## Аутентификация с использованием токенов

Возможна в следующих вариантах:

1. На запрос системы токен предъявляет ей секретное значение, служащее для подтверждения подлинности. Один раз перехватив этот ответ, злоумышленник может имитировать ответ токена.
2. Токен и система имеют общую, синхронизированную систему генерации одноразовых паролей. На запрос системы токен выдает пароль, действительный для данного промежутка времени. Система генерирует в это время свой вариант пароля, который и сравнивает с полученным.
3. Токен зарегистрирован в системе (она знает его секретный параметр). Для аутентификации она формирует случайную величину, которую токен преобразует с использованием своего параметра. Система выполняет аналогичное преобразование и сравнивает результат с полученным от токена. В этом случае перехват запроса и ответа ничего не дает злоумышленнику. И синхронизация токена и системы не требуется.

Варианты использования токена совместно с паролем:

1. Пароль служит для доступа к токену, который без пароля не действует.
2. Пароль вместе с параметром токена служат основой для выработки одноразовых паролей.
3. Токен генерирует ответ системе на запрос со случайной величиной на основе своего параметра и пароля пользователя.

**Аутентификация с помощью биометрических данных**

Биометрия представляет собой совокупность автоматизированных методов идентификации и аутентификации людей на основе их физиологических и поведенческих характеристик.

К числу физиологических характеристик принадлежат особенности:

- отпечатков пальцев,
- сетчатки и роговицы глаз,
- геометрия руки и лица.

К поведенческим характеристикам относятся:

- динамика подписи,
- стиль работы с клавиатурой.

К характеристикам, включающим физиологию и поведение относят анализ особенностей голоса и распознавание речи.

В общем виде работа с биометрическими данными организована следующим образом. Сначала создается и поддерживается база данных характеристик потенциальных пользователей. Для этого биометрические характеристики пользователя снимаются, обрабатываются, и результат обработки (называемый биометрическим шаблоном) заносится в базу данных. При этом исходные данные, такие как результат сканирования пальца или роговицы, обычно не хранятся.

В дальнейшем для идентификации и одновременно аутентификации пользователя процесс снятия и обработки повторяется, после чего производится поиск в базе данных шаблонов.

В случае успешного поиска личность пользователя и ее подлинность считаются установленными. Для аутентификации достаточно произвести сравнение с одним биометрическим шаблоном, выбранным на основе предварительно введенных данных.

Обычно биометрию применяют вместе с другими аутентификаторами, такими как smart-карты. Иногда биометрическая аутентификация служит для активизации smart-карт, в этом случае биометрический шаблон хранится на той же карте.

Биометрия подвержена тем же угрозам, что и другие методы аутентификации.

1. Биометрический шаблон сравнивается не с результатом первоначальной обработки характеристик пользователя, а с тем, что пришло к месту сравнения.
2. Биометрические методы не более надежны, чем база данных шаблонов.
3. Следует учитывать разницу между применением биометрии на контролируемой территории и в "полевых" условиях.
4. Биометрические данные человека меняются, так что база шаблонов нуждается в сопровождении.
5. Но главная опасность состоит в том, что если биометрические данные окажутся скомпрометированы, придется как минимум производить существенную модернизацию всей системы.

## Тема 13. Управление доступом в ИС

Существует два направления контроля и управления доступом в ИС: физическое и логическое. Физическое управление доступом применяется к техническим и аппаратным средствам ИС, а также к информации, представленной в печатной, визуальной и аудиоформе. Логическое управление доступом – к программным средствам и информации, представленной в электронной форме. Оно реализуется программными средствами.

Логическое управление доступом – это основной механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность объектов и, в

некоторой степени, их доступность (путем запрещения обслуживания неавторизованных пользователей).

В основе управления доступом лежит идентификация и аутентификация.

Если субъект и СИБ территориально разнесены, то с точки зрения безопасности необходимо рассмотреть два аспекта:

- что служит **аутентификатором**;
- как организован (и защищен) обмен данными идентификации и аутентификации.

Имеется совокупность субъектов и набор объектов. Задача логического управления доступом состоит в том, чтобы для каждой пары "субъект-объект" определить множество допустимых операций (зависящее, быть может, от некоторых дополнительных условий) и контролировать выполнение установленного порядка.

Отношение "субъекты-объекты" можно представить в виде **матрицы доступа**, в строках которой перечислены субъекты, в столбцах – объекты, а в клетках, расположенных на пересечении строк и столбцов, записаны дополнительные условия (например, время и место действия) и разрешенные виды доступа. Фрагмент матрицы может выглядеть, например, так:

| | Файл | Программа | Линия связи | Реляционная таблица |
|---|---|---|---|---|
| Пользователь 1 | ORW с консоли | E | RW с 8:00 до 17:00 | |
| Пользователь 2 | | | | A |

"O" – обозначает разрешение на передачу прав доступа другим пользователям,
"R" – чтение,
"W" – запись,
"E" – выполнение,
"A" – добавление информации

Тема логического управления доступом – одна из сложнейших в области информационной безопасности. Понятие объекта (а тем более видов доступа) меняется от сервиса к сервису. Для операционной системы к объектам относятся файлы, устройства и процессы.

Применительно к файлам и устройствам обычно рассматриваются права на чтение, запись, выполнение (для программных файлов), иногда на удаление и добавление. Отдельным правом может быть возможность передачи полномочий доступа другим субъектам (так называемое право владения). Процессы можно создавать и уничтожать. Современные операционные системы могут поддерживать и другие объекты.

Для систем управления реляционными базами данных объект – это база данных, таблица, процедура. К таблицам применимы операции поиска, добавления, модификации и удаления данных, у других объектов иные виды доступа.

Разнообразие объектов и применимых к ним операций приводит к децентрализации логического управления доступом. Каждый сервис должен сам решать, позволить ли конкретному субъекту ту или иную операцию. Хотя это согласуется с современным объектно-ориентированным подходом, но приводит к значительным трудностям.

1. Ко многим объектам можно получить доступ с помощью разных сервисов. Так, до реляционных таблиц можно добраться не только средствами СУБД, но и путем непосредственного чтения файлов.
2. При экспорте/импорте данных информация о правах доступа, как правило, теряется (на новом сервисе она не имеет смысла).

Существует три подхода к логическому управлению доступом:

1. Произвольное управление,
2. Принудительное управление.
3. Ролевое управление.

В случае произвольного управления матрица доступа хранится в виде списков, то есть для каждого объекта поддерживается список "допущенных" субъектов вместе с их правами. Большинство операционных систем и систем управления базами данных реализуют именно произвольное управление доступом. Основное достоинство произвольного управления – возможность для каждой пары "субъект-объект" независимо задавать права доступа. Но у произвольного управления есть ряд недостатков.

- Доверенными должны быть многие пользователи, а не только системные операторы или администраторы.
- Права доступа существуют отдельно от данных. Ничто не мешает пользователю, имеющему доступ к секретной информации, записать ее в доступный всем файл или заменить полезную утилиту вредоносной программой.

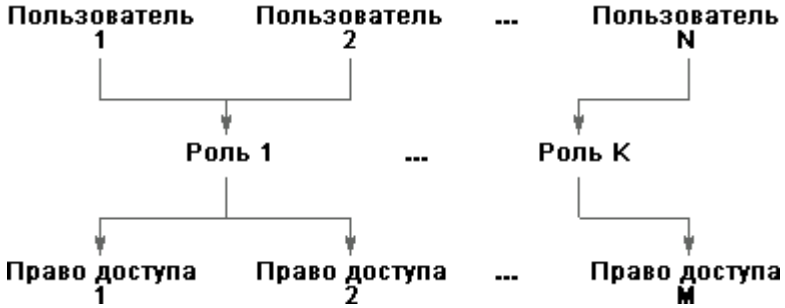
В случае принудительного управления матрицу не хранят в явном виде, а каждый раз вычисляют содержимое соответствующих клеток. Для этого с каждым субъектом и каждым объектом ассоциируются метки безопасности. Управление доступом основано на сопоставлении меток безопасности субъекта и объекта. Субъект может читать информацию из объекта при одновременном выполнении следующих двух условий:

- уровень секретности субъекта не ниже, чем у объекта,
- все категории действий, перечисленные в метке безопасности объекта, присутствуют в метке субъекта.

**Ролевое управление доступом**

При большом количестве пользователей первые два вида управления доступом становятся крайне сложными для администрирования. Число связей в них пропорционально произведению количества пользователей на количество объектов.

Суть ролевого управления доступом в том, что между пользователями и их привилегиями появляются промежуточные сущности – роли. Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему определенные права.




Ролевой доступ нейтрален по отношению к конкретным видам прав и способам их проверки; он использует объектно-ориентированный подход т.о. позволяет сделать подсистему управления доступа управляемой при сколь угодно большом числе пользователей, за счет установления между ролями связей, аналогичных наследованию в объектно-ориентированных системах.

Ролей значительно меньше, чем пользователей. В результате число администрируемых связей становится пропорциональным сумме (а не произведению) количества пользователей и объектов.

Ролевое управление доступом оперирует следующими основными понятиями:

- пользователь;
- сеанс работы пользователя;
- роль (определяется в соответствии с организационной структурой);
- объект;
- операция (зависит от объекта);

- право доступа (разрешение выполнять определенные операции над определенными объектами).

Роли как бы именуют отношения "многие ко многим" между пользователями и правами. Роли могут быть приписаны многие пользователи; один пользователь может быть приписан нескольким ролям. Во время сеанса работы пользователя активизируется подмножество ролей, которым он приписан, т.о. он становится обладателем объединения прав, приписанных активным ролям.

Одновременно пользователь может открыть несколько сеансов.

Между ролями может быть определено отношение наследования. Если роль $R_2$ является наследницей $R_1$, то все права $R_1$ приписываются $R_2$, а все пользователи $R_2$ приписываются $R_1$. Наследование ролей соответствует наследованию классов в объектно-ориентированном программировании, только правам доступа соответствуют методы классов, а пользователям – объекты (экземпляры) классов.

Можно представить себе формирование иерархии ролей, начиная с минимума прав (и максимума пользователей), приписываемых роли "сотрудник", с постепенным уточнением состава пользователей и добавлением прав (роли "системный администратор", "бухгалтер" и т.п.), вплоть до роли "руководитель". Но руководителю не предоставляются неограниченные права; как и другим ролям. Каждой роли целесообразно разрешить только то, что необходимо для выполнения служебных обязанностей.


Для реализации ролевого управления также вводится понятие разделения обязанностей, в двух видах: статическом и динамическом.

Статическое разделение обязанностей налагает ограничения на приписывание пользователей ролям. Принадлежность к одной роли запрещает приписывание пользователя определенному множеству других ролей.

Динамическое разделение обязанностей отличается от статического только тем, что рассматриваются роли, одновременно активные (в том числе, в разных сеансах) для данного пользователя. Например, один пользователь может играть роль и кассира, и контролера, но не одновременно; чтобы стать контролером, он должен сначала закрыть кассу. Тем самым реализуется так называемое временное ограничение доверия.

Администрирование ролевого управления доступом предусматривает реализацию трех категорий функций:

- Административные функции:
  - создать/удалить роль или пользователя,
  - приписать пользователя или право роли или ликвидировать существующую ассоциацию,
  - создать/удалить отношение наследования между существующими ролями,
  - создать/удалить ограничения для разделения обязанностей.
- Функции управления:
  - открыть сеанс работы пользователя;
  - активировать новую роль,
  - деактивировать роль,
  - проверить правомерность доступа.
- Информационные функции:
  - получение списка пользователей, приписанных роли,

- получение списка ролей, с которыми ассоциирован пользователь,
- получение информации о правах, приписанных роли,
- о правах заданного пользователя,
- об активных в данный момент ролях и правах,
- об операциях, которые пользователь может совершить над объектом,
- о статическом/динамическом разделении обязанностей.

## Тема 14. Протоколирование и аудит

Под **протоколированием** понимается сбор и накопление информации о событиях, происходящих в ИС. **Аудит** – это анализ накопленной информации, проводимый в реальном времени или периодически. Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.

Реализация протоколирования и аудита решает следующие задачи:

1. обеспечение подотчетности пользователей и администраторов; является сдерживающим средством;
2. обеспечение возможности реконструкции последовательности событий – позволяет выявить слабости в защите сервисов, найти виновника вторжения, оценить масштабы причиненного ущерба и вернуться к нормальной работе;
3. обнаружение попыток нарушений информационной безопасности;
4. предоставление информации для выявления и анализа проблем.

Для реализации эффективного протоколирование требуется определиться с тем, какие события регистрировать и с какой степенью детализации. Слишком обширное или подробное протоколирование не только снижает производительность работы ИС (что отрицательно сказывается на доступности), но и затрудняет аудит, то есть не увеличивает, а уменьшает информационную безопасность.

Основные события, безусловно требующие протоколирования:

- попытка входа в систему (успешная или нет);
- выход из системы;
- обращение к удаленной системе;
- операции с файлами (открыть, закрыть, переименовать, удалить);
- смена привилегий или иных атрибутов безопасности.

При протоколировании события рекомендуется записывать, по крайней мере, следующую информацию:

- дата и время события;
- уникальный идентификатор пользователя – инициатора действия;
- тип события;
- результат действия (успех или неудача);
- источник запроса (например, имя терминала);
- имена затронутых объектов (например, открываемых или удаляемых файлов);
- описание изменений, внесенных в базы данных защиты (например, новая метка безопасности объекта).

В отношении определенной категории пользователей и событий может применяться выборочное протоколирование.

Характерная особенность протоколирования и аудита – зависимость от других средств безопасности. Идентификация и аутентификация служат отправной точкой подотчетности пользователей, логическое управление доступом защищает конфиденциальность и целостность *регистрационной информации*.

Реализация протоколирования и аудита в распределенной разнородной системе является сложной задачей по крайней мере по двум причинам:

1. некоторые компоненты, важные для безопасности (например, маршрутизаторы), могут не обладать своими ресурсами протоколирования, значит их нужно экранировать другими элементами, которые могут реализовать функции протоколирования,
2. необходимо увязывать между собой события в разных элементах системы.

# Тема 15. Шифрование

**Шифрование** – преобразование информации в форму, при которой невозможно или существенно затруднено извлечение из неё осмысленных данных без ключа.

**Дешифрование** – восстановление с помощью ключа исходной информации.

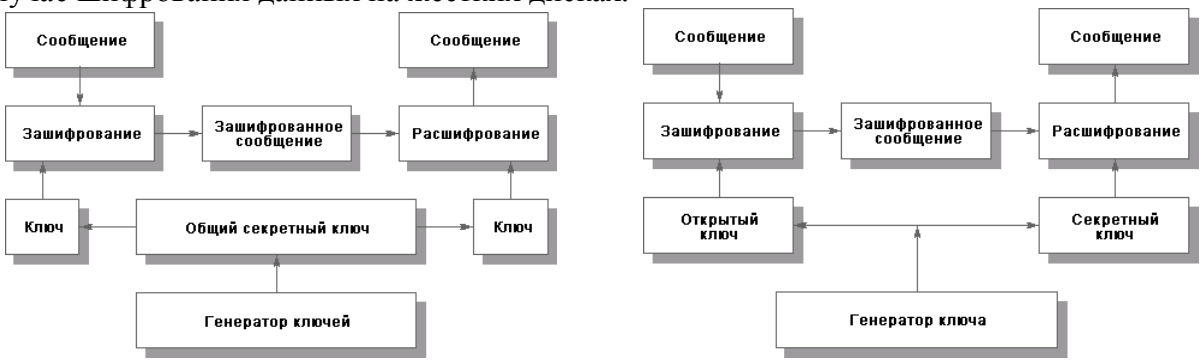
**Расшифрование** – восстановление без помощи ключа исходной информации.

Различают два метода шифрования: симметричный и асимметричный.

**Ключ** – набор данных, определяющий параметры алгоритмов шифрования и дешифрования.

В симметричном шифровании один ключ используется и для шифрования, и для дешифрования данных. Если данные должны быть переданы от одного субъекта ИС к другому, то этот ключ должен быть известен и отправителю и получателю сообщения. Ключ должен быть сформирован одним из участников обмена данными и передан другому. Это приводит к появлению проблемы надежной передачи ключа. Кроме проблемы передачи ключа еще одним недостатком симметричного шифрования является то, что получатель сообщения не может доказать, что это сообщение пришло от конкретного отправителя, поскольку точно такое же сообщение он мог сгенерировать сам.

Данных проблем не возникает, если передачи данных как таковой нет. Например в случае шифрования данных на жестких дисках.




В асимметричном методе используются два ключа. Один из них, открытый, применяется для шифрования, другой, секретный, – для дешифрования. Оба ключа являются взаимосвязанными и должны быть сформированы получателем сообщения. Открытый ключ передается отправителю сообщения. Знание открытого ключа не дает возможности дешифровать сообщение.

Существенным недостатком асимметричных методов шифрования является их низкое быстродействие (асимметричные методы на 3 – 4 порядка медленнее), поэтому данные методы приходится сочетать с симметричными.

Для решения задачи эффективного шифрования с передачей секретного ключа, использованного отправителем, сообщение сначала симметрично шифруют случайным ключом, затем этот ключ шифруют открытым ключом получателя, после чего сообщение и зашифрованный ключ отправляют получателю.


# Тема 16. Контроль целостности

В основе контроля целостности лежат два понятия:

- хэш-функция;
- электронная цифровая подпись (ЭЦП).

**Хэш-функция** – это труднообратимое преобразование данных, реализуемое, как правило, средствами симметричного шифрования со связыванием блоков. Результат шифрования последнего блока (зависящий от всех предыдущих) и служит результатом хэш-функции.

Пусть имеются данные, целостность которых нужно проверить, хэш-функция и ранее вычисленный результат ее применения к исходным данным (так называемый *дайджест*). Обозначим хэш-функцию через H, исходные данные – через T, проверяемые данные – через T'. Контроль целостности данных сводится к проверке равенства h(T') = h(T). Если оно выполнено, считается, что T' = T.

Совпадение дайджестов для различных данных называется коллизией. В принципе, коллизии, конечно, возможны, поскольку мощность множества дайджестов меньше, чем мощность множества хэшируемых данных, однако то, что H есть функция односторонняя, означает, что за приемлемое время специально организовать коллизию невозможно.

Электронная цифровая подпись защищает целостность сообщения и удостоверяет личность отправителя, то есть защищает целостность источника данных и служит основой неотказуемости.

Для выработки и проверки ЭЦП необходимо выполнение следующего условия:

E’(D(T)) = D’(E(T)) = T

где T – зашифрованное сообщение,

D – результат шифрования T секретным ключом,

E – результат шифрования T открытым ключом,

D’ – результат дешифрования T с помощью секретного ключа,

E’ – результат дешифрования T с помощью открытого ключа.

Использование асимметричного шифрования имеет существенный недостаток. Злоумышленник может, выдавая себя за другого пользователя, сформировать пару ключей (открытый и закрытый), опубликовать открытый ключ и получать сообщения, адресованные этому пользователю. Для устранения этого недостатка применяются цифровые сертификаты.

Цифровой сертификат состоит из открытого ключа владельца сертификата и его идентификационных данных. Все это подписано цифровой подписью надежной третьей стороны, которая называется центром сертификации (ЦС).

Пользователь некоторым защищенным образом доставляет в ЦС свой открытый ключ и подтверждает свою подлинность. ЦС формирует сертификат. Получив сертификат пользователь публикует его. Если открытый ключ пользователя нужен другому

пользователю для передачи сообщений, то он может убедиться в подлинности сертификата, проверив ЭЦП.

Цифровой сертификат состоит из следующих элементов:

1. порядковый номер сертификата (целое число, уникальное для каждого сертификата);
2. идентификатор алгоритма создания электронной подписи;
3. имя ЦС;
4. срок действия сертификата (дата начала действия и дата окончания);
5. имя владельца сертификата;
6. открытые ключи владельца сертификата (ключей может быть несколько);
7. идентификаторы алгоритмов, ассоциированных с открытыми ключами владельца сертификата;
8. электронная подпись – хэш-код всех предыдущих полей, зашифрованный секретным ключом ЦС.

Для формирования ЭЦП выполняются следующие действия:

1. выполняется хэш-преобразование сообщения T – H(T),
2. результат преобразования шифруется секретным ключом ЦС – D(H(T)).

Для проверки ЭЦП:

1. с помощью открытого ключа дешифруется подпись E’(D(H(T)))=H(T),
2. выполняется хэш-преобразование сообщения T’ – H(T’),
3. проверяется равенство H(T)=H(T’).

## Тема 17. Экранирование

**Экран** – это средство разграничения доступа клиентов из одного множества информационных систем к серверам из другого множества посредством контроля информационные потоков между двумя множествами систем Контроль потоков состоит в их фильтрации и выполнении некоторых преобразований.

Бороться с угрозами, присущими сетевой среде, средствами универсальных операционных систем не представляется возможным по следующим причинам:

- Универсальная ОС всегда содержит, помимо явных ошибок, особенности, которые могут быть использованы для нелегального получения привилегий. Современная технология программирования не позволяет сделать столь большие программы безопасными.
- Администратор, имеющий дело со сложной системой, не в состоянии учесть все последствия производимых изменений.
- В универсальной многопользовательской системе уязвимости постоянно создаются самими пользователями (слабые пароли, неудачно установленные права доступа, оставленный без присмотра терминал).

Экран можно представить как последовательность фильтров. Каждый из фильтров, проанализировав данные, может пропустить или не пропустить их, преобразовать, передать часть данных на следующий фильтр или обработать данные от имени адресата и возвратить результат отправителю.

Помимо функций разграничения доступа, экраны осуществляют протоколирование обмена информацией.

Обычно экран не является симметричным, для него определены понятия "внутри" и "снаружи". Задача экранирования формулируется как защита внутренней области от потенциально враждебной внешней.

Экранирование помогает поддерживать доступность сервисов внутренней области, уменьшая или вообще ликвидируя внешние воздействия, уменьшая уязвимость внутренних сервисов безопасности.

Экранирование дает возможность контролировать также информационные потоки, направленные во внешнюю область для поддержания конфиденциальности в ИС организации.

Экранирование может использоваться как сервис безопасности не только в сетевой, но и в любой другой среде, где происходит обмен сообщениями. Пример – разграничение доступа к объектам в объектно-ориентированных программных системах, когда для активизации методов объектов выполняется передача сообщений.

Экранирование может быть частичным, защищающим определенные информационные сервисы, например, электронную почту.