Блядский ОЗИ

ТЕМА 1

**1. Информация и информационная безопасность.**

*Кто прочитал, тот здохнет бля(((*

**Информация** (лат. informatio — разъяснение, изложение), первоначально — сведения, передаваемые людьми устным, письменным или другим способом с помощью условных сигналов, технических средств и т.д. С середины 20-го века информация является общенаучным понятием, включающим в себя:

- сведения, передаваемые между людьми;

- сигналы в животном и растительном мире;

- признаки, передаваемые от клетки к клетке, от организма к организму;

- и т.д.

**Защита информации** – комплекс правовых, организационных и технических мероприятий и действий по предотвращению угроз информационной безопасности и устранению их последствий в процессе сбора, хранения, обработки и передачи информации в информационных системах.

**Информационная безопасность –** это одна из характеристик информационной системы, т.е. информационная система на определенный момент времени обладает определенным состоянием (уровнем) защищенности, а защита информации – это процесс, который должен выполняться непрерывно на всем протяжении жизненного цикла информационной системы.

Под **субъектами информационных отношений** понимаются как владельцы, так и пользователи информации и поддерживающей инфраструктуры.

**Информационная угроза** – потенциальная возможность неправомерного или случайного воздействия на объект защиты, приводящая к потере, искажению или разглашению информации.

Политика информационной безопасности (ПИБ) организации или учреждения – совокупность правил, процедур, практических методов, руководящих принципов, документированных управленческих решений, направленных на защиту информации и связанных с ней ресурсов и используемых всеми сотрудниками организации или учреждения в своей деятельности.

**Объект –** пассивный компонент системы, хранящий, перерабатывающий, передающий или принимающий информацию; примеры объектов: страницы, файлы, папки, директории, компьютерные программы, устройства (мониторы, диски, принтеры и т. д.).

**Субъект** – активный компонент системы, который может инициировать поток информации; примеры субъектов: пользователь, процесс либо устройство.

**2. Основные составляющие информационной безопасности.**

**Можно выделить следующие составляющие: обеспечение доступности, целостности и конфиденциальности информационных ресурсов и поддерживающей инфраструктуры.**

**Доступность информации** – свойство системы обеспечивать своевременный беспрепятственный доступ правомочных (авторизованных) субъектов к интересующей их информации или осуществлять своевременный информационный обмен между ними.

**Целостность информации** – свойство информации, характеризующее ее устойчивость к случайному или преднамеренному разрушению или несанкционированному изменению. Целостность можно подразделить на *статическую (*понимаемую как неизменность информационных объектов) и *динамическую* (относящуюся к корректному выполнению сложных действий (транзакций). Средства контроля динамической целостности применяются, в частности, при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений.

**Конфиденциальность информации** – свойство информации быть известной и доступной только правомочным субъектам системы (пользователям, программам, процессам).

**3. Категории и носители информации.**

Неотъемлемой частью любой информационной системы является информация. По характеру ограничений (реализации) конституционных прав и свобод в информационной сфере выделяют **четыре основных вида правовой (регламентированной законами) информации:**

**- информация с ограниченным доступом;**

**- информация без права ограничения;**

**- иная общедоступная информация (например, за деньги);**

**- информация, запрещенная к распространению.**

Информация с ограниченным доступом делится на государственную тайну и конфиденциальную.

К государственной тайне относятся защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ. Владельцем государственной тайны является само государство.

Конфиденциальная информация – документированная информация, правовой режим которой установлен специальными нормами действующего законодательства в области государственной, коммерческой, промышленной и другой общественной деятельности.

Под персональными данными понимается любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных). Несмотря на то, что это информация ограниченного доступа, она является полностью открытой для субъекта персональных данных. Только сам субъект решает вопрос о передаче, обработке и использовании своих персональных данных, а также определяет круг субъектов, которым эти данные могут быть сообщены.

Информация, запрещенная к распространению, определена в многочисленных нормативных документах. В частности: Конституция Республики Беларусь, Уголовный Кодекс Республики Беларусь

**4. Средства защиты информации.**

**I. Формальные средства защиты** – выполняют защитные функции строго по заранее предусмотренной процедуре без участия человека.

Физические средства - механические, электрические, электромеханические, электронные, электронно-механические и тому подобные устройства и системы, которые функционируют автономно от информационных систем, создавая различного рода препятствия на пути дестабилизирующих факторов (замок на двери, жалюзи, забор, экраны).

Аппаратные средства - механические, электрические, электромеханические, электронные, электронно-механические, оптические, лазерные, радиолокационные и тому подобные устройства, встраиваемые в информационных системах или сопрягаемые с ней специально для решения задач защиты информации.

Программные средства - пакеты программ, отдельные программы или их части, используемые для решения задач защиты информации. Программные средства не требуют специальной аппаратуры, однако они ведут к снижению производительности информационных систем, требуют выделения под их нужды определенного объема ресурсов и т.п.

К специфическим средствам защиты информации относятся криптографические методы. В информационных системах криптографические средства защиты информации могут использоваться как для защиты обрабатываемой информации в компонентах системы, так и для защиты информации, передаваемой по каналам связи. Само преобразование информации может осуществляться аппаратными или программными средствами, с помощью механических устройств, вручную и т.д.

**II. Неформальные средства защиты** – регламентируют деятельность человека.

Законодательные средства – законы и другие нормативно-правовые акты, с помощью которых регламентируются правила использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил. Распространяются на всех субъектов информационных отношений.

Организационные средства - организационно-технические и организационно-правовые мероприятия, осуществляемые в течение всего жизненного цикла защищаемой информационной системы (строительство помещений, проектирование информационных систем, монтаж и наладка оборудования, испытания и эксплуатация информационных систем). Другими словами – это средства уровня организации, регламентирующие перечень лиц, оборудования, материалов и т.д., имеющих отношение к информационным системам, а также режимов их работы и использования. К организационным мерам также относят сертификацию информационных систем или их элементов, аттестацию объектов и субъектов на выполнение требований обеспечения безопасности и т.д.

Морально-этические средства - сложившиеся в обществе или в данном коллективе моральные нормы или этические правила, соблюдение которых способствует защите информации, а нарушение приравнивается к несоблюдению правил поведения в обществе или коллективе, ведет к потере престижа и авторитета.

**5. Способы передачи конфиденциальной информации на расстоянии.**

Способов передачи конфиденциальной информации на расстоянии существует множество, среди которых можно выделить три основных направления.

1. Создать абсолютно надежный, недоступный для других канал связи между абонентами.

2. Использовать общедоступный канал связи, но скрыть сам факт передачи информации.

3. Использовать общедоступный канал связи, но передавать по нему нужную информацию в таком преобразованном виде, чтобы восстановить ее мог только адресат.

Проанализируем эти возможности.

1. В настоящий момент для реализации данного механизма защиты используются современные телекоммуникационные каналы связи. Однако следует заметить, что данный подход требует значительных капитальных вложений. При современном уровне развития науки и техники сделать такой канал связи между удаленными абонентами для многократной передачи больших объемов информации практически нереально.

2. Разработкой средств и методов скрытия факта передачи сообщения занимается стеганография. В настоящий момент стеганографические методы в совокупности с криптографическими нашли широкое применение в целях сокрытия и передачи конфиденциальной информации.

3. Разработкой методов преобразования информации с целью ее защиты от несанкционированного прочтения занимается криптография.

**Тема 2 Радужная серия**

´**Радужная серия** (Радужные книги) — серия стандартов информационной безопасности, разработанная и опубликованная в [США](https://ru.wikipedia.org/wiki/%D0%A1%D0%A8%D0%90) в период с 1980 по 1990 гг. Изначально книги были опубликованы [Министерством обороны США](https://ru.wikipedia.org/wiki/%D0%9C%D0%B8%D0%BD%D0%B8%D1%81%D1%82%D0%B5%D1%80%D1%81%D1%82%D0%B2%D0%BE_%D0%BE%D0%B1%D0%BE%D1%80%D0%BE%D0%BD%D1%8B_%D0%A1%D0%A8%D0%90), а затем в [Центре национальной компьютерной безопасности США](https://ru.wikipedia.org/wiki/%D0%A6%D0%B5%D0%BD%D1%82%D1%80_%D0%BD%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B9_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%BE%D0%B9_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8_%D0%A1%D0%A8%D0%90).

´Эти стандарты описывают процесс оценки доверенных систем. Многие из этих стандартов стали основой для Общих критериев оценки защищённости информационных технологий. Книги получили свои названия по цвету обложек. Например, книга [Критерии определения безопасности компьютерных систем](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D1%82%D0%B5%D1%80%D0%B8%D0%B8_%D0%BE%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D1%85_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC) получила название [Оранжевая книга](https://ru.wikipedia.org/wiki/%D0%9E%D1%80%D0%B0%D0%BD%D0%B6%D0%B5%D0%B2%D0%B0%D1%8F_%D0%BA%D0%BD%D0%B8%D0%B3%D0%B0_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)).

**Роль стандартов информационной безопасности**

´С развитием информационных технологий появилась необходимость стандартизации требований в области защиты информации.

´Главная задача стандартов ин­формационной безопасности — создать основу для взаимодей­ствия между производителями, потребителями и специалистам по сертификации.

Оранжевая книга

´Критерии безопасности компьютерных систем» (Trusted Computer System Evaluation Criteria), получившие неформальное название Оранжевая книга, были разработаны Министерством обороны США в 1983 году с целью определения требований безопасности, предъявляемых к аппаратному, программному и специальному обеспечению компьютерных систем, и выра­ботки соответствующей методологии и технологии анализа сте­пени поддержки политики безопасности в компьютерных си­стемах военного назначения.

´Предложенные в этом документе концепции защиты и на­бор функциональных требований послужили основой для фор­мирования всех появившихся впоследствии стандартов безо­пасности

**Классификация требований и критериев Оранжевой книги**

**´В Оранжевой книге предложены три категории требований безопасности — политика безопасности, аудит и корректность, в рамках которых сформулированы шесть базовых требований безопасности.**

**´Первые четыре требования направлены непо­средственно на обеспечение безопасности информации, а два последних — на качество самих средств защиты.**

|  |  |
| --- | --- |
| Политика безопасности | Система должна поддерживать точно определённую полити­ку безопасности. Возможность осуществления субъектами досту­па к объектам должна определяться на основе их идентифика­ции и набора правил управления доступом. Там, где необходимо, должна использоваться политика нормативного управления до­ступом, позволяющая эффективно реализовать разграничение доступа к категорированной информации (информации, отме­ченной грифом секретности: «секретно», «сов. секретно» и т.д.) |
| Метки | С объектами должны быть ассоциированы метки безопас­ности, используемые в качестве атрибутов контроля доступа. Для реализации нормативного управления доступом система должна обеспечивать возможность присваивать каждому объ­екту метку или набор атрибутов, определяющих степень кон­фиденциальности (гриф секретности) объекта и/или режимы доступа к этому объекту |
| Идентификация и аутентификация | **В**се субъекты должны иметь уникальные идентификато­ры. Контроль доступа должен осуществляться на основании результатов идентификации субъекта и объекта доступа, под­тверждения подлинности их идентификаторов (аутентифика­ции) и правил разграничения доступа. Данные, используемые для идентификации и аутентификации, должны быть защище­ны от несанкционированного доступа, модификации и унич­тожения и ассоциированы со всеми активными компонентами компьютерной системы, функционирование которых критич­но с точки зрения безопасности. |
| Регистрация и учет | Для определения степени ответственности пользователей за действия в системе все происходящие в ней события, имею­щие значение с точки зрения безопасности, должны отслежи­ваться и регистрироваться в защищенном протоколе. Система регистрации должна осуществлять анализ общего потока собы­тий и выделять из него только те события, которые оказывают влияние на безопасность для сокращения объема протокола и повышения эффективность его анализа. Протокол событий должен быть надежно защищен от несанкционированного до­ступа, модификации и уничтожения. |
| Контроль корректности функционирования средств за­щиты | Средства защиты должны содержать независимые аппарат­ные и/или программные компоненты, обеспечивающие рабо­тоспособность функций защиты. Это означает, что все средства защиты, обеспечивающие политику безопасности, управление атрибутами и метками безопасности, идентификацию и аутен­тификацию, регистрацию и учёт, должны находиться под кон­тролем средств, проверяющих корректность их функциони­рования. Основной принцип контроля корректности состоит в том, что средства контроля должны быть полностью незави­симы о средств защиты. |
| Непрерывность защиты | Все средства защиты (в т. ч. и реализующие данное требова­ние) должны быть защищены от несанкционированного вме­шательства и/или отключения, причем эта защита должна быть постоянной и непрерывной в любом режиме функционирова­ния системы защиты и компьютерной системы в целом. Данное требование распространяется на весь жизненный цикл компью­терной системы. Кроме того, его выполнение является одним из ключевых аспектов формального доказательства безопас­ности системы. |

**Классы безопасности компьютерных систем**

´Оранжевая книга предусматривает четыре группы критери­ев, которые соответствуют различной степени защищенности: от минимальной (группа D) до формально доказанной (груп­па А). Каждая группа включает один или несколько классов. Группы D и А содержат по одному классу (классы D и А со­ответственно), группа С — классы Cl, С2, а группа В — В1, В2, ВЗ, характеризующиеся различными наборами требова­ний безопасности. Уровень безопасности возрастает при дви­жении от группы D к группе А, а внутри группы — с возраста­нием номера класса.

Группа D. Минимальная защита.

´К этому классу относятся все системы, не удовлетворяющие требованиям других классов.

**Группа С. Дискреционная защита**

|  |  |
| --- | --- |
| Класс С1. Дискреционная защита | Системы этого класса удовлетворяют требованиям обеспечения разделения пользо­вателей и информации и включают средства контроля и управ­ления доступом, позволяющие задавать ограничения для инди­видуальных пользователей, что дает им возможность защищать свою приватную информацию от других пользователей. Класс С1 рассчитан на многопользовательские системы, в которых осуществляется совместная обработка данных одного уровня секретности |
| Класс С2. Управление доступом | Системы этого класса осу­ществляют более избирательное управление доступом, чем си­стемы класса С1, с помощью применения средств индивиду­ального контроля за действиями пользователей, регистрацией, учетом событий и выделением ресурсов. |

**Группа В. Мандатная защита**

|  |  |
| --- | --- |
| Класс В1. Защита с применением меток безопасности | Си­стемы класса В1 должны соответствовать всем требованиям, предъявляемым к системам класса С2, и, кроме того, должны поддерживать определенную модель безопасно­сти, маркировку данных и нормативное управление доступом. При экспорте из системы информация должна подвергаться маркировке. Обнаруженные в процессе тестирования недостат­ки должны быть устранены. |
| Класс В2. Структурированная защита | Для соответствия классу В2 ТСВ системы должна поддерживать формально опре­деленную и четко документированную модель безопасности, предусматривающую произвольное и нормативное управление доступом, которое распространяется по сравнению с системами класса В1 на все субъекты. Кроме того, должен осуществлять­ся контроль скрытых каналов утечки информации. В структу­ре ТСВ должны быть выделены элементы, критичные с точ­ки зрения безопасности. Интерфейс ТСВ должен быть четко определен, а ее архитектура и реализация выполнены с учетом возможности проведения тестовых испытаний. По сравнению с классом В1 должны быть усилены средства аутентификации. Управление безопасностью осуществляется администратора­ми системы. Должны быть предусмотрены средства управле­ния конфигурацией. |
| Класс ВЗ. Домены безопасности | Для соответствия этому классу ТСВ системы должна поддерживать монитор взаимодей­ствий, который контролирует все типы доступа субъектов к объ­ектам, который невозможно обойти. Кроме того, ТСВ должна быть структурирована с целью исключения из нее подсистем, не отвечающих за реализацию функций защиты, и достаточно компактна для эффективного тестирования и анализа. В ходе разработки и реализации ТСВ необходимо применение мето­дов и средств, направленных на минимизацию ее сложности. Средства аудита должны включать механизмы оповещения ад­министратора при возникновении событий, имеющих значе­ние для безопасности системы. Требуется наличие средств вос­становления работоспособности системы. |

**Группа А. Верифицированная защита**

|  |  |
| --- | --- |
| **Класс А1. Формальная верификация** | Системы класса А1 функционально эквивалентны системам класса ВЗ, и к ним не предъявляется никаких дополнительных функциональных требований. В отличие от систем класса ВЗ в ходе разработ­ки должны применяться формальные методы верификации, что позволяет с высокой уверенностью получить корректную реализацию функций защиты. Процесс доказательства адек­ватности реализации начинается на ранней стадии разработ­ки с построения формальной модели политики безопасности и спецификаций высокого уровня. Для обеспечения методов ве­рификации системы класса А1 должны содержать более мощ­ные средства управления конфигурацией и защищенную про­цедуру ди**стрибуции.** |

´Согласно «Оранжевой книге» безопасная компьютерная си­стема — это система, поддерживающая управление доступом к обрабатываемой в ней информации таким образом, что толь­ко соответствующие авторизованные пользователи или процес­сы, действующие от их имени, получают возможность читать, писать, создавать и удалять информацию.

´«Критерии безопасности компьютерных систем» Ми­нистерства обороны США представляют собой первую попытку создать единый стандарт безопасности, рассчитанный на разра­ботчиков, потребителей и специалистов по сертификации ком­пьютерных систем. В свое время этот документ явился настоящим прорывом в области безопасности информационных технологий и послужил отправной точкой для многочисленных исследований и разработок.

´Оранжевая книга послужила основой для разработчиков всех остальных стандартов информационной безопасности и до сих пор используется в США в качестве руководящего документа при сертификации компьютерных систем обработки информации.

**Европейские критерии безопасности информационных технологий (ITSEC)**

´Данные критерии были опубли­кованы в июне 1991 года от имени четырех стран: Франции, Германии, Нидерландов и Великобритании.

´Европейские критерии рассматривают следующие задачи средств информационной безопасности:

´защита информации от несанкционированного доступа с целью обеспечение конфиденциальности;

´обеспечение целостности информации посредством за­щиты от ее несанкционированной модификации или уничтожения;

´обеспечение работоспособности систем с помощью противодействия угрозам отказа в обслуживании.

´Европейские критерии безопасности информацион­ных технологий, появившиеся вслед за Оранжевой книгой, ока­зали существенное влияние на стандарты безопасности и ме­тодику сертификации.

Главное достижение этого документа — введение понятия адекватности средств защиты и определение отдельной шка­лы для критериев адекватности. Как уже упоминалось, Евро­пейские критерии придают адекватность средств защиты даже большее значение, чем их функциональности. Этот подход ис­пользуется во многих появившихся позднее стандартах инфор­мационной безопасности.

**Федеральные критерии безопасности информационных технологий США**

´Федеральные критерии безопасности информацион­ных технологий (Federal Criteria for Information Technology Security) разрабатывались как одна из составляющих Амери­канского федерального стандарта по обработке информации (Federal Information Processing Standard), призванного заме­нить Оранжевую книгу. Разработчиками стандарта выступи­ли Национальный институт стандартов и технологий США (Nationa Institute of Standards and Technology) и Агентство на­циональной безопасности США (National Security Agency). (1992)

´Основными объектами применения требований безопасно­сти Федеральных критериев являются

´продукты информационных технологий (Information Technology Products);

´системы обработки информации (Information Тechnology Systems).

´Федеральные критерии безопасности информацион­ных технологий — первый стандарт информационной безопас­ности, в котором определяются три независимые группы тре­бований: функциональные требования к средствам защиты, требования к технологии разработки и к процессу квалифи­кационного анализа. Авторами этого стандарта впервые пред­ложена концепция Профиля защиты — документа, содержа­щего описание всех требований безопасности как к самому ИТ-продукту, так и к процессу его проектирования, разработ­ки, тестирования и квалификационного анализа.

´Разработчики Федеральных критериев отказались от исполь­зуемого в Оранжевой книге подхода к оценки уровня безопас­ности ИТ-продукта на основании обобщенной универсаль­ной шкалы классов безопасности. Вместо этого предлагается независимое ранжирование требований каждой группы, т. е. вместо единой шкалы используется множество частных шкал- критериев, характеризующих обеспечиваемый уровень безо­пасности. Данный подход позволяет разработчикам и пользо­вателям ИТ-продукта выбрать наиболее приемлемое решение и точно определить необходимый и достаточный набор требо­ваний для каждого конкретного ИТ-продукта и среды его экс­плуатации.

´Стандарт рассматривает устранение недостатков существу­ющих средств безопасности как одну из задач защиты наряду с противодействием угрозам безопасности и реализацией мо­дели безопасности.

´Данный стандарт ознаменовал появление нового поколе­ния руководящих документов в области информационной без­опасности, а его основные положения послужили базой для разработки Канадских критериев безопасности компьютер­ных систем и Единых критериев безопасности информацион­ных технологий.

**Единые критерии безопасности информационных технологий**

´Единые критерии безопасности информационных техно­логий (Common Criteria for Information Technology Security Evaluation, далее — Единые критерии) являются результатом совместных усилий авторов Европейских критериев безопас­ности информационных технологий, Федеральных критери­ев безопасности информационных технологий и Канадских критериев безопасности компьютерных систем, направленных на объединение основных положений этих документов и созда­ние Единого международного стандарта безопасности инфор­мационных технологий. Работа над этим самым масштабным в истории стандарте информационной безопасности проектом началась в июне 1993 года с целью преодоления концептуаль­ных и технических различий между указанными документами, их согласования и создания единого международного стандар­та. Версия 2.1 этого стандарта утверждена Международной орга­низацией по стандартизации (ISO) в 1999 г. в качестве Между­народного стандарта информационной безопасности ISO/IEC 15408.

´Требования Единых критериев охватывают практически все аспекты безопасности ИТ-продуктов и техно­логии их создания, а также содержат все исходные материалы, необходимые потребителям и разработчикам для формирова­ния Профилей и Проектов защиты.

´Кроме того, требования Единых критериев являются практи­чески всеобъемлющей энциклопедией информационной безо­пасности, поэтому их можно использовать в качестве справоч­ника по безопасности информационных технологий.

´Данный стандарт ознаменовал собой новый уровень стан­дартизации информационных технологий, подняв его на меж­государственный уровень. За этим проглядывается реальная перспектива создания единого безопасного информационно­го пространства, в котором сертификация безопасности систем обработки информации будет осуществляться на глобальном уровне, что предоставит возможности для интеграции нацио­нальных информационных систем.

**Группа международных стандартов 270000**

´Основное назначение международных стандартов — это соз­дание на межгосударственном уровне единой основы для раз­работки новых и совершенствования действующих систем ка­чества. Сотрудничество в области стандартизации направлено на приведение в соответствие национальной системы стандар­тизации с международной. Международные стандарты не име­ют статуса обязательных для всех стран-участниц. Любая страна мира вправе применять или не применять их. Решение вопроса о применении международного стандарта связано в основном со степенью участия страны в международном разделении труда.

´Международные стандарты принимаются Международ­ной организацией по стандартизации — ИСО (International Organization for Standardization, ISO).

**Законы, среди которых следует отметить:**

´Закон Республики Беларусь 21.06.2008 № 418-З «О регистре населения» (далее – Закон «О регистре населения»);

´Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» (далее – Закон «Об информации»);

´Закон Республики Беларусь от 13 июля 2006 г. № 144-З «О переписи населения» (далее – Закон «О переписи населения»);

´Закон Республики Беларусь от 28 декабря 2009 г. № 113-З «Об электронном документе и электронной цифровой подписи».

**ПРОДОЛЖЕНИЕ ПАРАШИ №2**

**Политика безопасности**

´Политика безопасности - набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. Политика безопасности должна включать в себя анализ возможных угроз и выбор мер противодействия.

´Гарантированность - мера доверия, которая может быть оказана архитектуре и реализации системы. Гарантированность может проистекать как из тестирования, так и из проверки общего замысла и исполнения системы в целом и ее компонентов.

´Механизм подотчетности (протоколирования). Надежная система должна фиксировать все события, касающиеся безопасности. Ведение протоколов должно дополняться аудитом.

´Периметр безопасности - граница надежной вычислительной базы. То, что внутри периметра, считается надежным, а то, что вне - нет.

**Основные элементы политики безопасности**

**´**Согласно "Оранжевой книге", политика безопасности должна включать в себя по крайней мере следующие элементы:

´произвольное управление доступом;

´безопасность повторного использования объектов;

´метки безопасности;

´принудительное управление доступом.

**Произвольное управление доступом**

**´**это метод ограничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит. Произвольность управления состоит в том, что некоторое лицо (обычно владелец объекта) может по своему усмотрению давать другим субъектам или отбирать у них права доступа к объекту.

´Текущее состояние прав доступа при произвольном управлении описывается матрицей, в строках которой перечислены субъекты, а в столбцах - объекты. В клетках, расположенных на пересечении строк и столбцов, записываются способы доступа, допустимые для субъекта по отношению к объекту - например, чтение, запись, выполнение, возможность передачи прав другим субъектам и т.п.

**Безопасность повторного использования объектов**

´важное на практике дополнение средств управления доступом, предохраняющее от случайного или преднамеренного извлечения секретной информации из "мусора". Безопасность повторного использования должна гарантироваться для областей оперативной памяти (в частности, для буферов с образами экрана, расшифрованными паролями и т.п.), для дисковых блоков и носителей в целом.

´Поскольку информация о субъектах также представляет собой объект, необходимо позаботиться о безопасности "повторного использования субъектов". Когда пользователь покидает организацию, следует не только лишить его возможности входа в систему, но и запретить доступ ко всем объектам. В противном случае, новый сотрудник может получить ранее использовавшийся идентификатор а с ним и все права своего предшественника.

**Метки безопасности**

´для реализации принудительного управления доступом с субъектами и объектами. Метка субъекта описывает его благонадежность, метка объекта - степень закрытости содержащейся в нем информации.

´Согласно "Оранжевой книге", метки безопасности состоят из двух частей - уровня секретности и списка категорий. Уровни секретности, поддерживаемые системой, образуют упорядоченное множество, которое может выглядеть, например, так:

´совершенно секретно,

´секретно,

´конфиденциально,

´несекретно.

´Категории образуют неупорядоченный набор. Их назначение - описать предметную область, к которой относятся данные. Механизм категорий позволяет разделить информацию по отсекам, что способствует лучшей защищенности, при этом, субъект не может получить доступ к "чужим" категориям, даже если его уровень благонадежности - "совершенно секретно".

´Главная проблема, которую необходимо решать в связи с метками, это обеспечение их целостности:

´не должно быть непомеченных субъектов и объектов;

´при любых операциях с данными метки должны оставаться правильными.

´Например, печатный документ должен открываться заголовком, содержащим текстовое и/или графическое представление метки безопасности.

´Разделение устройств на многоуровневые и одноуровневые. На многоуровневых устройствах может храниться информация разного уровня секретности. Зная уровень устройства, система может решить, допустимо ли записывать на него информацию с определенной меткой.

**Принудительное управление доступом**

´Основано на сопоставлении меток безопасности субъекта и объекта.

´Субъект может читать информацию из объекта, если уровень секретности субъекта не ниже, чем у объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта. В таком случае говорят, что метка субъекта доминирует над меткой объекта. Смысл сформулированного правила понятен - читать можно только то, что положено.

´ Ни при каких операциях уровень секретности информации не должен понижаться, хотя обратный процесс вполне возможен.

´Принудительное управление доступом реализовано во многих вариантах операционных систем и СУБД, отличающихся повышенными мерами безопасности. Впрочем, в реальной жизни произвольное и принудительное управление доступом сочетается в рамках одной системы, что позволяет использовать сильные стороны обоих подходов.

**Подотчетность**

´Цель подотчетности - в каждый момент времени знать, кто работает в системе и что он делает.

´Средства подотчетности делятся на три категории:

´Идентификация и аутентификация.

´Предоставление надежного пути.

´Анализ регистрационной информации.

**ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИя**

´Каждый пользователь, прежде чем получить право совершать какие-либо действия в системе, должен идентифицировать себя. В свою очередь, система должна проверить подлинность личности пользователя, то есть что он является именно тем, за кого себя выдает.

´Идентификация и аутентификация - первый и важнейший программно-технический рубеж информационной безопасности. Если не составляет проблемы получить доступ к системе под любым именем, то другие механизмы безопасности, например, управление доступом, очевидно, теряют смысл.

**ПРЕДОСТАВЛЕНИЕ НАДЕЖНОГО ПУТИ**

´Надежный путь связывает пользователя непосредственно с надежной вычислительной базой, минуя другие, потенциально опасные компоненты системы. Цель предоставления надежного пути - дать пользователю возможность убедиться в подлинности обслуживающей его системы.

Относительно несложно реализовать надежный путь, если используется неинтеллектуальный терминал - достаточно иметь зарезервированную управляющую последовательность. Если же пользователь общается с интеллектуальным терминалом, персональным компьютером или рабочей станцией, задача обеспечения надежного пути становится чрезвычайно сложной, если вообще разрешимой.

**АНАЛИЗ РЕГИСТРАЦИОННОЙ ИНФОРМАЦИИ**

´Аудит имеет дело с действиями, так или иначе затрагивающими безопасность системы. К числу таких событий, например, относятся:

´Вход в систему (успешный или нет).

´Выход из системы.

´Обращение к удаленной системе.

´Операции с файлами (открыть, закрыть, переименовать, удалить).

´Смена привилегий или иных атрибутов безопасности (режима доступа, уровня благонадежности пользователя и т.п.).

´Протоколирование помогает следить за пользователями и реконструировать прошедшие события. Слежка важна в первую очередь как профилактическое средство. Можно надеяться, что многие воздержатся от нарушений безопасности, зная, что их действия фиксируются.

**Гарантированность**

´Гарантированность - это мера уверенности, с которой можно утверждать, что для проведения в жизнь сформулированной политики безопасности выбран подходящий набор средств, и что каждое из этих средств правильно исполняет отведенную ему роль.

´В "Оранжевой книге" рассматривается два вида гарантированности - операционная и технологическая.

**Операционная гарантированность**

´Операционная гарантированность включает в себя проверку следующих элементов:

´Архитектура системы.

´Целостность системы.

´Анализ тайных каналов передачи информации.

´Надежное администрирование.

´Надежное восстановление после сбоев.

´Операционная гарантированность - это способ убедиться в том, что архитектура системы и ее реализация действительно проводят в жизнь избранную политику безопасности.

´Среди архитектурных решений, предусматриваемых "Оранжевой книгой", упомянем следующие:

´Деление аппаратных и системных функций по уровням привилегированности и контроль обмена информацией между уровнями;

´Защита различных процессов от взаимного влияния;

´Наличие средств управления доступом;

´Структурированность системы, явное выделение надежной вычислительной базы, обеспечение компактности этой базы.

´Следование принципу минимизации привилегий - каждому компоненту дается ровно столько привилегий, сколько необходимо для выполнения им своих функций.

´Сегментация (в частности, сегментация адресного пространства процессов) как средство повышения надежности компонентов.

´Целостность системы в данном контексте означает, что аппаратные и программные компоненты надежной вычислительной базы работают должным образом и что имеется аппаратное и программное обеспечение для периодической проверки целостности.

´Надежное администрирование в трактовке "Оранжевой книги" означает всего лишь, что должны быть логически выделены три роли - системного администратора, системного оператора и администратора безопасности.

´Надежное восстановление после сбоев - вещь необходимая, однако ее реализация может быть сопряжена с серьезными техническими трудностями. Прежде всего, должна быть сохранена целостность информации и, в частности, целостность меток безопасности. В принципе возможна ситуация, когда сбой приходится на момент записи нового файла с совершенно секретной информацией. Если файл окажется с неправильной меткой, информация может быть скомпрометирована.

´Надежное восстановление включает в себя два вида деятельности - подготовку к сбою (отказу) и собственно восстановление. Подготовка к сбою - это и регулярное выполнение резервного копирования, и выработка планов действий в экстренных случаях, и поддержание запаса резервных компонентов. Восстановление связано с перезагрузкой системы и выполнением ремонтных и/или административных процедур.

**Технологическая гарантированность**

**´**Технологическая гарантированность охватывает весь жизненный цикл системы, то есть периоды проектирования, реализации, тестирования, продажи и сопровождения. Все перечисленные действия должны выполняться в соответствии с жесткими стандартами, чтобы обезопаситься от утечки информации и нелегальных "закладок".

´Первое, на что обычно обращают внимание, это тестирование. Тесты должны показать, что защитные механизмы функционируют в соответствии со своим описанием и что не существует очевидных способов обхода или разрушения защиты. Должна быть уверенность, что надежную вычислительную базу нельзя привести в состояние, когда она перестанет обслуживать пользовательские запросы.

**Документация**

´Документация - необходимое условие гарантированной надежности системы и, одновременно, - инструмент проведения политики безопасности. Без документации люди не будут знать, какой политике следовать и что для этого нужно делать.

´Согласно "Оранжевой книге", в комплект документации надежной системы должны входить следующие тома:

´Руководство пользователя по средствам безопасности.

´Руководство администратора по средствам безопасности.

´Тестовая документация.

´Описание архитектуры.

´На практике требуется еще по крайней мере одна книга - письменное изложение политики безопасности данной организации.

**Работы по обеспечению режима ИБ**

´– определение сферы (границ) системы управления информационной безопасностью и конкретизация целей ее создания;

´– оценка рисков;

´– выбор контрмер, обеспечивающих режим ИБ;

´– управление рисками;

´– аудит системы управления ИБ;

´– выработка политики безопасности**.**

´Этап 1. Выбор национальных и международных руководящих документов и стандартов в области ИБ и формулирование на их базе основных требований и положений политики ИБ компании, включая:

´– управление доступом к средствам вычислительной техники (СВТ), программам и данным, а также антивирусную защиту;

´– вопросы резервного копирования;

´– проведение ремонтных и восстановительных работ;

´– информирование об инцидентах в области ИБ и пр.

´Этап 2. Выработка подходов к управлению информационными рисками и принятие решения о выборе уровня защищенности КИС. Уровень защищенности в соответствии с зарубежными стандартами может быть минимальным (базовым) либо повышенным. Этим уровням защищенности соответствует минимальный (базовый) или полный вариант анализа информационных рисков.

´Этап 3. Структуризация контрмер по [защите информации](https://pandia.ru/text/category/zashita_informatcii/) по следующим основным уровням: административному, процедурному, программно-техническому.

´Этап 4. Установление порядка сертификации и аккредитации КИС на соответствие стандартам в сфере ИБ. Назначение периодичности проведения совещаний по тематике ИБ на уровне руководства, в том числе периодического пересмотра положений политики ИБ, а также порядка обучения всех категорий пользователей информационной системы в области ИБ. Известно, что выработка политики безопасности организации – наименее формализованный этап. Однако в последнее время именно здесь сосредоточены усилия многих специалистов по защите информации.

´Этап 5. Определение сферы (границ) системы управления информационной безопасностью и конкретизация целей ее создания. На этом этапе определяются границы системы, для которой должен быть обеспечен режим ИБ. Соответственно, система управления ИБ строится именно в этих границах.

**конец 2 темы пиздеееец**

**ТЕМА 3**

**Криптографические методы защиты информации**

*Криптоанализ* – наука о методах и способах вскрытия шифров и кодов, анализа надежности криптоалгоритмов.

*Криптография* – наука (искусство) о защите информации от прочтения ее посторонними, о методах преобразования (шифрования) информации с целью ее защиты от незаконных пользователей.

В криптографии широко используются следующие преобразования и термины.

´*Перестановка* – нарушение нормального порядка следования единиц информации, например, букв (СЕКРЕТ – ЕТКРСЕ).

´*Замена на основе шифралфавита* – перечень эквивалентов, используемых для преобразования открытого текста в шифрованный. Иногда шифралфавит предусматривает несколько замен одного знака. Например, *С* {16, 21, 35, 72}, т. е. *С* заменяется одним из чисел. Этот выбор называется гомофоном*.* Время от времени в шифралфавит включают символ, который ничего не значит (символ-пустышка).

´*Код* – огромный шифр замены. С одной стороны – тысячи слов, фраз, букв и слогов открытого текста, с другой – заменяющие их кодовые слова или кодовые обозначения.

´*Шифр* – код, основной единицей которого является знак, несколько знаков или битовый блок.

´*Криптограмма* – окончательно обработанное и отосланное сообщение.

´*Расшифровка* (раскодирование) – преобразование шифротекста (кодотекста), при наличии ключа и системы шифрования.

Для построения абсолютно стойкого шифра необходимо уметь получать совершенно случайный ключ.Иначе можно выявить некоторую закономерность в шифрованных сообщениях.

Стойкость шифра – это сложность задачи его вскрытия.

Сложность задачи – минимальная сложность алгоритмов ее решения.

**СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ**

Симметричные системы шифрования, в отличие от асимметричных, используют один и тот же ключ как на этапе зашифрования данных, так и на этапе их расшифрования.

Все эти алгоритмы в той или иной мере строгости обладают следующими основными свойствами:

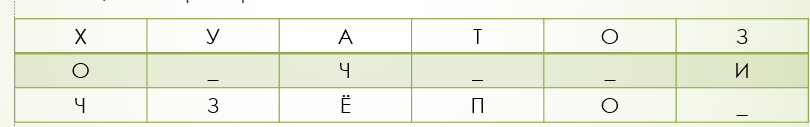
´*рассеивание* (распространение влияния);

´*перемешивание* (исключение статистической взаимосвязи)*.*

**Простая перестановка**

Простая перестановка без ключа — один из самых простых методов шифрования. Сообщение записывается в таблицу по столбцам. После того, как открытый текст записан колонками, для образования шифровки он считывается по строкам. Для использования этого шифра отправителю и получателю нужно договориться об общем ключе в виде размера таблицы.

например, зашифруем фразу «ХОЧУ\_ЗАЧЁТ\_ПО\_ОЗИ", разместим текст в "таблице" - по три строки.



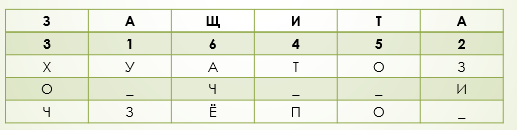
Шифр будет иметь такой вид: ХУАТОЗО\_Ч\_ \_ИЧЗЁПО\_

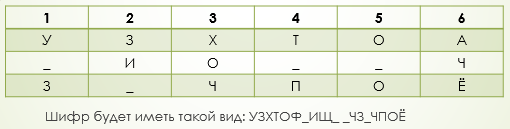
**Одиночная перестановка по ключу**

Более практический метод шифрования, называемый одиночной перестановкой по ключу очень похож на предыдущий. Он отличается лишь тем, что колонки таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы.

Шифровать будем ту же фразу, которую шифровали без ключа

Ключом у нас будет слово ЗАЩИТА





Двойнаяперестановка по ключу

Для дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Этот способ известен под названием двойная перестановка. Для этого размер второй таблицы подбирают так, чтобы длины ее строк и столбцов были другие, чем в первой таблице. Лучше всего, если они будут взаимно простыми. Кроме того, в первой таблице можно переставлять столбцы, а во второй строки. Наконец, можно заполнять таблицу зигзагом, змейкой, по спирали или каким-то другим способом. Такие способы заполнения таблицы если и не усиливают стойкость шифра, то делают процесс шифрования гораздо более занимательным.

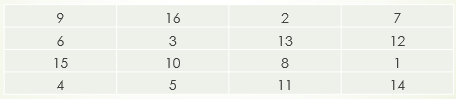
Перестановка «Магический квадрат Дюрера»

Магическими квадратами называются квадратные таблицы со вписанными в их клетки последовательными натуральными числами от 1, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число.

Подобные квадраты широко применялись для вписывания шифруемого текста по приведенной в них нумерации.

Если потом выписать содержимое таблицы по строкам, то получалась шифровка

перестановкой букв.



Например, требуется зашифровать фразу: «**РЕАЛЬНОСТЬ\_БЫТИЯ**». Буквы этой фразы вписываются последовательно в квадрат согласно записанным в них числам: позиция буквы в предложении соответствует порядковому числу



**Стандарты шифрования:**

**Достоинства**

´скорость на 3 порядка выше

´простота реализации (за счёт более простых операций)

´меньшая требуемая длина ключа для сопоставимой стойкости

´изученность (за счёт большего возраста)

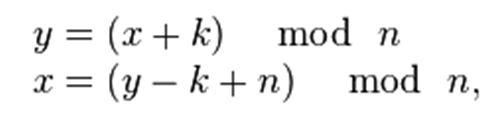
**Недостатки**

´сложность управления ключами в большой сети. Означает квадратичное возрастание числа пар ключей, которые надо генерировать, передавать, хранить и уничтожать в сети. Для сети в 10 абонентов требуется 45 ключей, для 100 уже 4950, для 1000 — 499500 и т. д.

´сложность обмена ключами. Для применения необходимо решить проблему надёжной передачи ключей каждому абоненту, так как нужен секретный канал для передачи каждого ключа обеим сторонам.

**Шифрование с использованием системы Цезаря:**

Это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее.Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами модульной арифметики:



Шифрование с использованием ключа k = 3. Буква «Е» «сдвигается» на три буквы вперёд и становится буквой «З». Твёрдый знак, перемещённый на три буквы вперёд, становится буквой «Э», буква «Я», перемещённая на три буквы вперёд, становится буквой «В», и так далее. :

´Исходный алфавит: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

´Шифрованный: ГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВ

Оригинальный текст: ***ХОЧУ ЗАЧЁТ ПО ОЗИ****.*

Шифрованный текст получается путём замены каждой буквы оригинального текста соответствующей буквой шифрованного алфавита: ***ШСЪЦ ЛГЪИХ ТС СКЛ****.*

**Шифрование с использованием системы Трисемуса:**

Представляет собой усовершенствованный шифр Цезаря, то есть шифр подстановки. По алгоритму шифрования, каждый символ сообщения смещается на символ, отстающий от данного на некоторый шагю Здесь шаг смещения делается переменным, то есть зависящим от каких-либо дополнительных факторов. Например, можно задать закон смещения в виде линейной функции (уравнения зашифрования) позиции шифруемой буквы.Сама функция должна гарантировать целочисленное значение. Прямая функция шифрования должна иметь обратную функцию шифрования, тоже целочисленную.

***Уравнением зашифрования***называется соотношение, описывающее процесс образования зашифрованных данных из открытых данных в результате преобразований, заданных алгоритмом криптографического преобразования.

***Уравнение зашифрования для шифра Тритемиуса*** *имеет следующий вид:*

"L=(m+k)mod N"

*Некоторые варианты вычисления* ***шага смещения k****:*

"k=A∗p+B"*,*

"k=A∗" p^2 "+B∗p+C"*,*

*где p — позиция буквы в сообщении; A, B, C — ключи*

*1.Определяем порядковый номер шифруемой буквы в тексте.*

*2.Определяем код буквы в алфавите.*

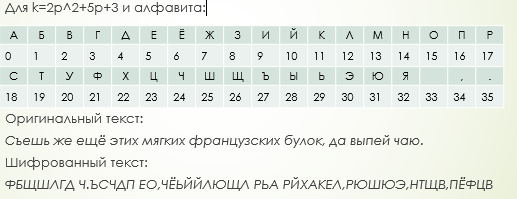
*3.Вычисляем смещение k.*

*4.Находим код зашифрованной буквы, пользуясь нашим уравнением зашифрования."L=(m+k)mod N "*

*Расшифрование "m=(L-k)mod N "*

*5.По коду L восстанавливаем очередную букву криптограммы.*

*6.Повторяем пункты 1..5 до окончания текста шифрограммы*

**

***Шифрование с использованием системы Плейфера:***

*Представляет собой ручную симметричнуютехнику шифрования, в которой впервые использована замена биграмм. Шифр предусматривает шифрование пар символов (биграмм) вместо одиночных символов, как в шифре подстановки*

*Шифр Плейфера использует матрицу 5х5 (для латинского алфавита, для кириллического алфавита необходимо увеличить размер матрицы до 4х8), содержащую ключевое слово или фразу.*

*Для создания матрицы и использования шифра достаточно запомнить ключевое слово и четыре простых правила.*

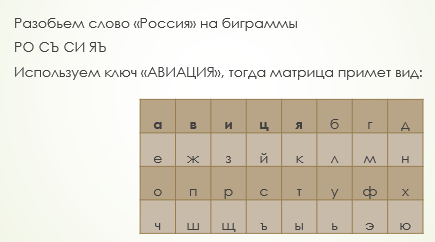
*Чтобы составить ключевую матрицу, в первую очередь нужно заполнить пустые ячейки матрицы буквами ключевого слова (не записывая повторяющиеся символы), потом заполнить оставшиеся ячейки матрицы символами алфавита, не встречающимися в ключевом слове, по порядку.*

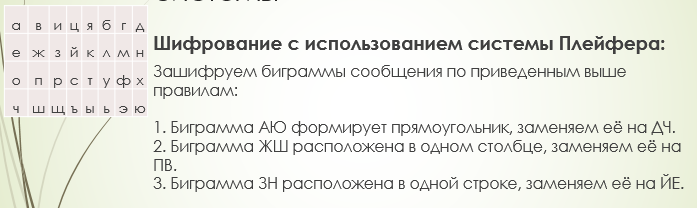
*1.Если два символа биграммы совпадают (или если остался один символ), добавляем после первого символа «Ъ», зашифровываем новую пару символов и продолжаем.*

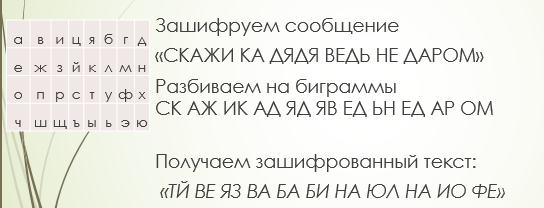
*2.Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки.*

*3.Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящиеся непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца.*

*4.Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника.*

**

**

**

***Шифрование с использованием системы Вижинера:***

*Представляет собой метод полиалфавитного*

*шифрования буквенного текста с использованием ключевого слова.*

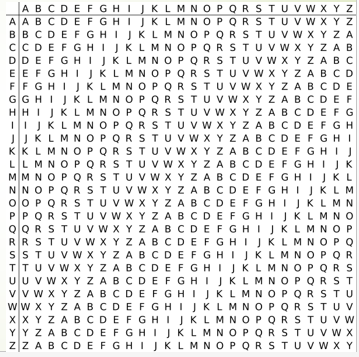
*Этот метод является простой формой многоалфавитной замены.*

*В шифре Цезаря каждая буква алфавита сдвигается на несколько строк; например в шифре Цезаря при сдвиге +3, A стало бы D, B стало бы E и так далее.*

*Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига.*

*Для зашифровывания может использоваться таблица алфавитов, называемая tabula recta или квадрат (таблица) Виженера.*

*Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций.*

**

*Например, предположим, что исходный текст имеет вид: ПОЛУЧИТЬ ЗАЧЁТ*

*Человек, посылающий сообщение, записывает ключевое слово («РАБОТА») циклически до тех пор, пока его длина не будет соответствовать длине исходного текста: РАБОТАРАБОТАР*

*Первый символ исходного текста П зашифрован последовательностью Р, которая является первым символом ключа. Первый символ Я шифрованного текста находится на пересечении строки Р и столбца П в таблице Вижинера. Точно так же для второго символа исходного текста используется второй символ ключа; то есть второй символ шифрованного текста О получается на пересечении строки А и столбца О. Остальная часть исходного текста шифруется подобным способом.*

*Исходный текст: ПОЛУЧИТЬ ЗАЧЁТ*

*Ключ: РАБОТА*

*Зашифрованный текст: ЯОМБЙИВЬ ИОЙЕВ*

*Если буквы A—Z соответствуют числам 0—25, то шифрование Виженера можно записать в виде формулы:*

*C\_i "= (" P\_i " + " K\_i ")mod 26"*

*Расшифровка:*

*P\_i "= (" C\_i " - " K\_i "+26)mod 26"*

***Шифр «двойной квадрат» Уитстона:***

*Пусть имеются две таблицы. В качестве ключей будем использовать два слова «Работа» и «Халява».*

**

*Перед шифрованием исходное сообщение разбивают на биграммы.*

*Каждая биграмма шифруется отдельно.*

*Первую букву биграммы находят в левой таблице, а вторую букву - в правой таблице.*

*Затем мысленно строят прямоугольник так, чтобы буквы биграммы лежали в его противоположных вершинах.*

*Другие две вершины этого прямоугольника дают буквы биграммы шифртекста.*

*Предположим, что шифруется биграмма исходного текста РЮ.*

*Получаем зашифрованную биграмму шифртекста ДШ.*

*Сообщение ПО ЛУ ЧИ ТЬ ЗА ЧЁ ТЪ*

*Шифртекст НП КЦ СМ ЖБ ОМ ЯЬ*

***Ассиметричные системы***

В 1970-х годах появилась новая система шифрования, называемая шифрованием на ассиметричном (открытом) ключе. Она называется ассиметричной, потому что не требует использования идентичных ключей отправителем и получателем шифрованного сообщения. Она является системой с открытым ключом, так как один из ключей не содержится в секрете.

!Система шифрования при которой открытый ключ передаётся по открытому каналу и используется для шифрования сообщения.

Шифрование на открытом ключе использует два различных ключа, составляющих пару, но не идентичных. В шифровании с симметричным ключом каждый ключ является уникальным. Пара ключей открытый/секретный работает сообща: один ключ предназначен для шифрования данных, а другой – для расшифровки, и наоборот. Секретный ключ должен содержаться в секретности в целях безопасности, а открытый ключ может передаваться по небезопасному соединению без угрозы для системы. Следовательно, система шифрования на открытом ключе решает одну из главных проблем старых систем шифрования, заключающуюся в безопасном способе передачи ключа шифрования другой стороне.

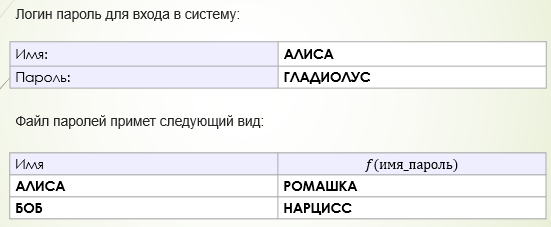
Как правило, открытые ключи используются только для зашифровки данных. Расшифровать их сможет только тот пользователь, чей компьютер содержит соответствующий секретный ключ. Эта система построена на математических принципах, используемых в шифрах с открытыми ключами и обеспечивающих существование одного и только одного уникального секретного ключа, соответствующего уникальному открытому ключу. Следовательно, если выполняется шифрование данных пользователя на общем ключе, можете быть уверены, что только пользователь, владеющий второй, секретной, половиной ключа, сможет их расшифровать.

Основана на идее **односторонней функции,** то есть таких функций f(x), что по известному x довольно просто найти значение f(x), тогда как определение x из f(x) невозможно за разумный срок.

**Лазейка** — это некий секрет, который помогает расшифровать.

Пусть пользователь ***«Алиса»*** придумала пароль ***«гладиолус».*** Функция от пары данных ***«Алиса\_гладиолус»*** будет давать результат **«ромашка».**

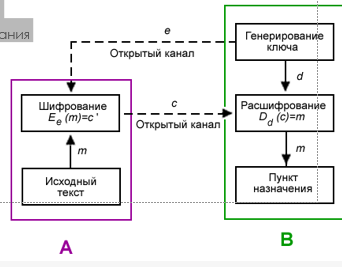
**f"(Алиса\_гладиолус")="ромашка"**



Пусть ***e*** и ***d*** — ключи шифрования и расшифрования соответственно.

E\_e — функция шифрования

D\_d — функция расшифрования



1. Боб выбирает пару (e,d) и шлёт ключ шифрования e (открытый ключ) Алисе по открытому каналу, а ключ расшифрования d (закрытый ключ) защищён и секретен (он не должен передаваться по открытому каналу).
2. Чтобы послать сообщение m Бобу, Алиса применяет функцию шифрования, определённую открытым ключом e: E\_e(m)=c, c — полученный шифротекст
3. Боб расшифровывает шифротекст c, применяя обратное преобразование D\_d, однозначно определённое значением d.

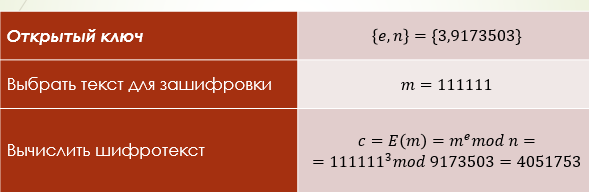
**RSA - аббревиатура от фамилий Rivest, Shamir и Adleman**

Алгоритм шифрования:

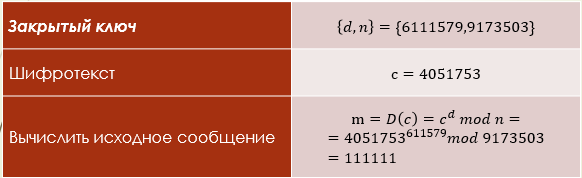
1. Генерация ключей



1. Шифрование:



1. Расшифрование



Алгоритмы криптосистемы с открытым ключом можно использовать:

как самостоятельное средство для защиты передаваемой и хранимой информации,

как средство распределения ключей,

как средство аутентификации пользователей.

Недостатки в сравнении с симметричными системами:

´В алгоритм сложнее внести изменения.

´Хотя сообщения надежно шифруются, но получатель и отправитель самим фактом пересылки шифрованного сообщения «засвечиваются».

´Более длинные ключи.

´Шифрование-расшифрование с использованием пары ключей проходит на два-три порядка медленнее, чем шифрование-расшифрование того же текста симметричным алгоритмом.

´Требуются существенно бо́льшие вычислительные ресурсы, поэтому на практике асимметричные криптосистемы используются в сочетании с другими алгоритмами

**Электронная цифровая подпись**

´Если обратиться к [федеральному закону](http://www.consultant.ru/document/cons_doc_LAW_112701/), то можно найти следующее её определение:

´«Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию»

Электронная подпись предназначена для идентификации лица, подписавшего электронный документ, и является полноценной заменой собственноручной подписи

Словарь терминов:

·*Открытый текст* – данные, подлежащие шифрованию или полученные в результате расшифрования;

·*Шифртекст* – данные, полученные в результате применения шифра к открытому тексту;

·*Шифр* – совокупность обратимых преобразований, зависящая от некоторого параметра (ключа);

·*Ключ* – параметр шифра, определяющий выбор одного преобразования из совокупности;

·*Факторизация* – процесс разложения числа на простые множители;

·*НОД* – наибольший общий делитель;

·Числа a и b называются *взаимно простыми*, если НОД этих чисел равен 1;

·*Функция Эйлера φ(n)* – функция, равная количеству натуральных чисел, меньших n и взаимно простых с ним.

Использование электронной подписи позволяет осуществить:

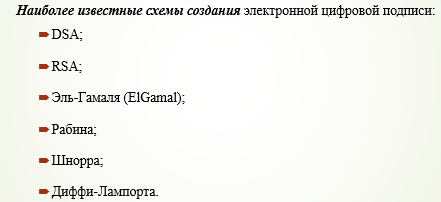
´Контроль целостности передаваемого документа.

´Защиту от изменений (подделки) документа.

´Невозможность отказа от авторства.

´Доказательное подтверждение авторства документа.

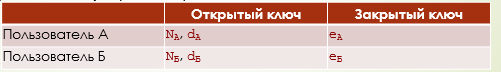


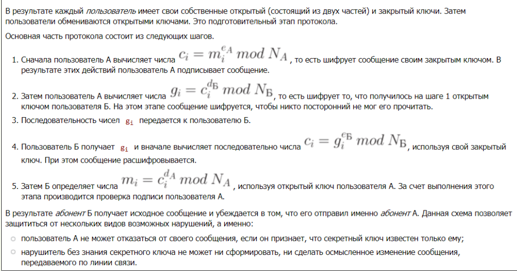
****

**Электронная подпись на основе алгоритма RSA**

´Схема использования алгоритма *RSA* при большом модуле N практически не позволяет злоумышленнику получить закрытый *ключ* и прочитать зашифрованное сообщение. Однако она дает возможность злоумышленнику подменить сообщение от абонента А к абоненту Б, так как *абонент* А шифрует свое сообщение открытым ключом, полученным от Б по открытому каналу связи. А раз *открытый ключ* передается по открытому каналу, любой может получить его и использовать для подмены сообщения. Избежать этого можно, используя более сложные протоколы, например, следующий.

´Пусть, как и раньше, *пользователь* А хочет передать пользователю Б сообщение, состоящее из нескольких блоков mi. Перед началом сеанса связи абоненты генерируют открытые и закрытые ключи, обозначаемые, как указано в следующей таблице:



**

*´Данная схема позволяет избежать многих конфликтных ситуаций. Иногда нет необходимости зашифровывать передаваемое сообщение, но нужно его скрепить электронной подписью. В этом случае из приведенного выше протокола исключаются шаги 2 и 4, то есть текст шифруется закрытым ключом отправителя, и полученная последовательность присоединяется к документу. Получатель с помощью открытого ключа отправителя расшифровывает прикрепленную подпись, которая, по сути, является зашифрованным повторением основного сообщения. Если расшифрованная подпись совпадает с основным текстом, значит, подпись верна.*

*´Существуют и другие варианты применения алгоритма RSA для формирования ЭЦП. Например, можно шифровать (то есть подписывать) открытым ключом не само сообщение, а хеш-код от него.*

*´Возможность применения алгоритма RSA для получения электронной подписи связана с тем, что секретный и открытый ключи в этой системе равноправны. Каждый из ключей, d или e, могут использоваться как для шифрования, так и для расшифрования. Это свойство выполняется не во всех криптосистемах с открытым ключом.*

*´Алгоритм RSA можно использовать также и для обмена ключами.*

***Отметим некоторые недостатки алгоритма цифровой подписи RSA:***

***1.*** *При вычислении ключей для системы цифровой подписи RSA необходимо проверять ряд дополнительных условий. Невыполнение любого из этих условий делает возможным фальсификацию цифровой подписи со стороны того, кто обнаружит такое невыполнение.*

***2.*** *Для обеспечения криптостойкости цифровой подписи RSA по отношению к попыткам фальсификации, например, на уровне алгоритма шифрования DES, необходимо использовать при вычислениях ключей очень большие целые числа, (около 10 в степени 154), что требует относительно больших вычислительных затрат, превышающих на 20-30% вычислительные затраты других алгоритмов цифровой подписи при сохранении того же уровня криптостойкости.*

***3.*** *Цифровая подпись RSА уязвима к так называемой мультипликативной атаке. Иначе говоря, алгоритм цифровой подписи RSA позволяет злоумышленнику без знания секретного ключа сформировать подписи под теми документами, у которых результат хэширования можно вычислить как произведение результатов хэширования уже подписанных документов. Хотя следует заметить, что вероятность реализации такой атаки весьма незначительна.*

*Для работы смарт-карт с цифровыми подписями RSA рекомендуется использование ключей с длиной модуля 1024 бит.*

*´*

**Тема 4**

**Технические каналы утечки информации**

´**Технический канал утечки информации** – совокупность источника конфиденциальной информации, среды распространения и средства технической разведки для перехвата информации.



´Источники конфиденциальной информации:

´– человек;

´– электронная аппаратура;

´– документы (содержание);

´– здания и сооружения (внешний вид).

´Среда распространения конфиденциальной информации:

´– воздушная;

´– твердые вещества (строительные конструкции);

´– электрические цепи.

´Средства технической разведки:

´– визуально-оптические (оптические увеличительные приборы);

´– оптоэлектронные (телевизионные, приборы ночного видения, тепловизоры и т. д.);

´– акустические (закладные устройства, направленные микрофоны, электронные стетоскопы и т. д.);

´– радиоперехвата (перехвата сообщений радио-, сотовой связи и т. д.);

´– фотографические;

´– электронные (для перехвата сигналов в проводных коммуникациях).

´По физическим принципам возникновения каналы утечки информации можно разделить на следующие группы:

´– акустический;

´– материально-вещественный;

´– визуально-оптический;

´– электромагнитный.



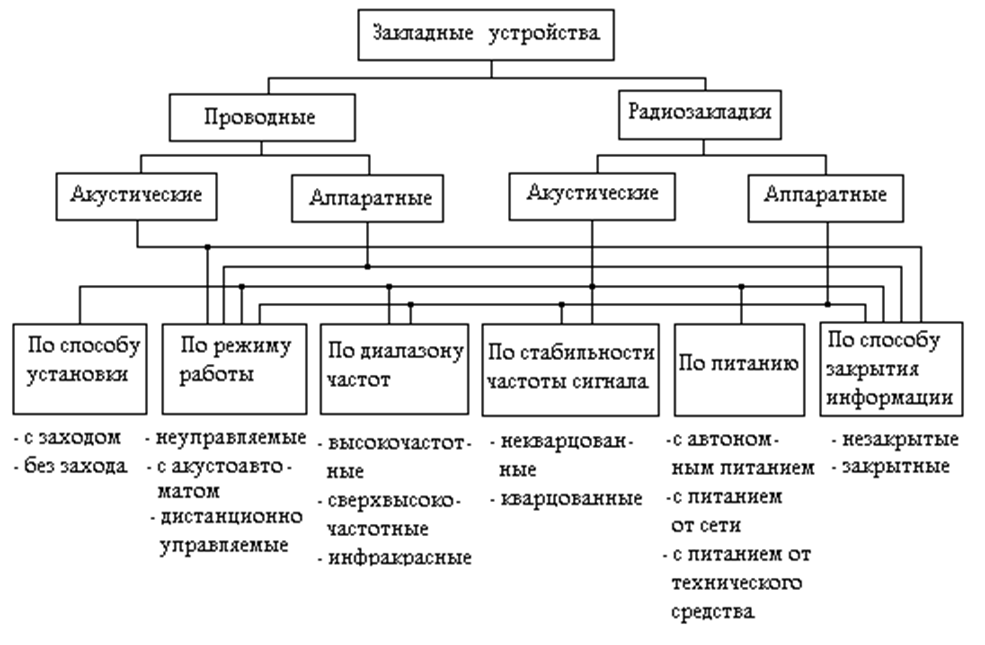
**Акустические каналы утечки информации**

´Голосовой аппарат человека является первичным источником акустических колебаний, которые представляют собой возмущения воздушной среды в виде волн сжатия и растяжения.



´Перехват информации средствами технической разведки в данном случае может реализовываться за счет применения закладных устройств, устанавливаемых внутри помещения или при помощи направленных микрофонов, путем перехвата акустических сигналов через открытые окна, двери. В данном случае акустическая волна без существенного ослабления попадает в средство технической разведки. Таким образом, образуется **прямой** акустический канал утечки информации.

´**Закладное устройство (ЗУ)** – автономное устройство для перехвата речевой информации, конструктивно объединяющее микрофон и передатчик



´Перехваченная ЗУ речевая информация может передаваться по радиоканалу, сети электропитания, оптическому каналу, телефонной линии, посторонним проводникам, инженерным коммуникациям в ультразвуковом диапазоне частот. Прием информации, передаваемой закладными устройствами, осуществляется, как правило, на специальные приемные устройства, работающие в соответствующем диапазоне длин волн.

´**Направленный микрофон** – электронное устройство, обладающее высокими чувствительностью и помехоустойчивостью за счет его узкой диаграммы направленности

**Виброакустические каналы утечки информации**

´Под действием акустических колебаний в ограждающих строительных конструкциях и инженерных коммуникациях помещения, в котором находится речевой источник, возникают вибрационные колебания. Таким образом, в своем первоначальном состоянии речевой сигнал в помещении присутствует в виде акустических и вибрационных колебаний. В данном случае строительные конструкции выполняют преобразование акустических колебаний в вибрационные и возникает виброакустический (вибрационный) канал утечки информации.



´Перехват информации в виброакустических каналах обеспечивается электронными стетоскопами, выполняющими преобразование механических колебаний строительных конструкций (пол, потолок, стены) в электрические. В качестве преобразователей, подключаемых к электронному стетоскопу, используются акселерометры.

´По виброакустическому каналу также возможен перехват информации с использованием закладных устройств. В основном для передачи информации используется радиоканал, поэтому такие устройства часто называют радиостетоскопами. Возможно использование закладных устройств с передачей информации по инженерным коммуникациям (ультразвуковые колебания).

´Вспомогательные технические средства и системы (ВТСС), кроме указанных элементов, могут содержать непосредственно акустоэлектрические преобразователи. К таким ВТСС относятся некоторые типы датчиков охранной и пожарной сигнализации, громкоговорители ретрансляционной сети и т. д. Эффект акустоэлектрического преобразования в специальной литературе называют «микрофонным эффектом».

´Электромеханический вызывной звонок телефонного аппарата – типичный представитель индуктивного акустоэлектрического преобразователя, микрофонный эффект которого проявляется при положенной микротелефонной трубке

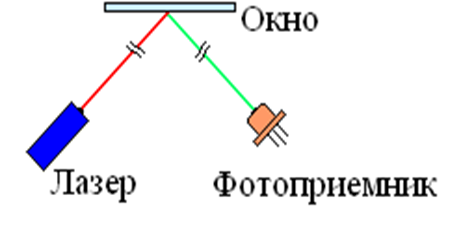
´Структурная схема акустоэлектрического канала утечки информации

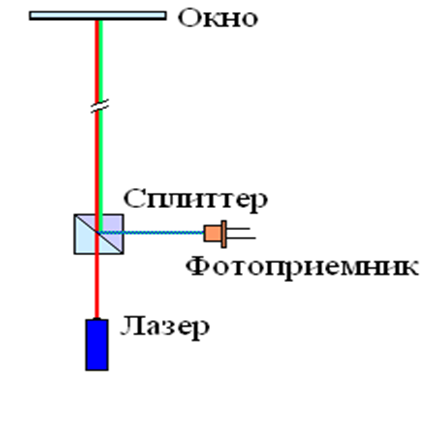


´Структурная схема акустооптического канала утечки информации



´Для перехвата речевой информации по данному каналу используются сложные лазерные системы, которые часто называют «лазерными микрофонами». Работают они, как правило, в ближнем инфракрасном диапазоне длин волн.

´

На рисунке приведен простейший вариант подобной системы: луч лазера падает на стекло окна под некоторым углом (например 45 градусов). На границе стекло–воздух происходит модуляция луча речевыми колебаниями. Отражённый луч принимается фотодетектором, расположенным с другой стороны окна под углом, равным углу падения луча лазера. Такая система требует тщательной юстировки.

´Второй способ, использующий сплиттер (делитель пучка), несколько сложнее, но он позволяет совместить лазер и детектор. Отпадает необходимость в тщательной юстировке системы. Применение сплиттера позволяет свести падающий и отражённый луч в одну точку.

**Материально-вещественный канал утечки информации**

´Утечка информации по материально‑вещественному каналу обусловлена хищением, копированием и ознакомлением с информацией, представленной на бумажном, электронном или каком-либо другом носителе.

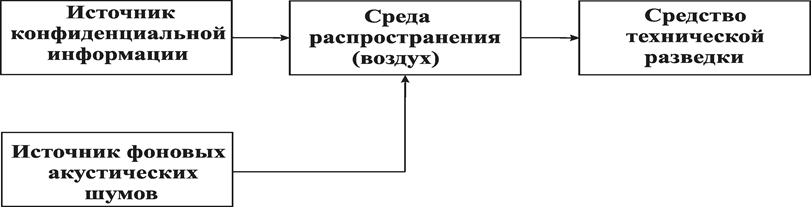
**Электромагнитные каналы утечки информации**

´Физические процессы, происходящие в технических средствах при их функционировании, создают в окружающем пространстве побочные электромагнитные излучения (ПЭМИ), которые в той или иной степени связаны с обрабатываемой информацией (электромагнитный канал).

´Физические явления, лежащие в основе появления этих излучений, имеют различный характер, но тем не менее они могут рассматриваться как непреднамеренная передача конфиденциальной информации по некоторой "побочной системе связи", образованной источником излучения, средой и средством перехвата информации.

´Регистрация средством технической разведки ПЭМИ источника информации (персональный компьютер и др.) распространяющихся через воздушную среду обусловливает возникновение индукционного канала утечки информации.

**´Структурная схема индукционного канала утечки информации**

****

**´Структурная схема электрического канала утечки информации**

****

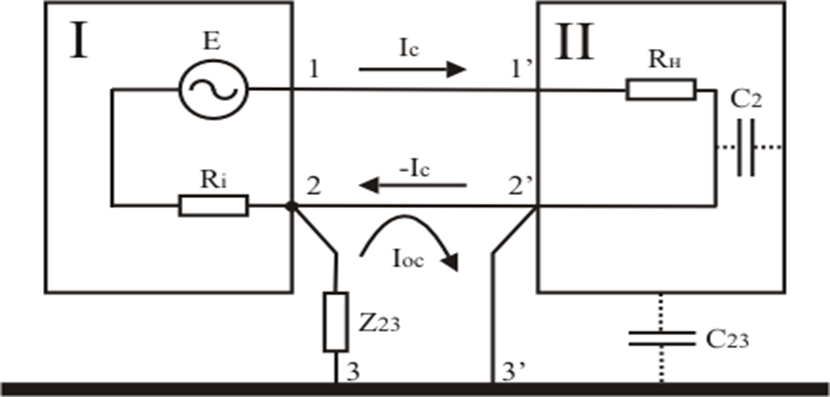
**Утечка информации по цепям заземления**

´Заземлением называется преднамеренное соединение объекта с заземляющим устройством, осуществляемое путем создания системы проводящих поверхностей и электрических соединений, предназначенных для выполнения различных функций.

´Одной из причин попадания опасного (информационного) сигнала в систему заземления является наличие ПЭМИ – носителя информационного сигнала в местах расположения элементов системы. Это ПЭМИ будет наводить в расположенной поблизости системе заземления ток опасного сигнала.

´Проникновение опасного сигнала в цепи заземления может быть связано с образованием так называемых контуров заземления.

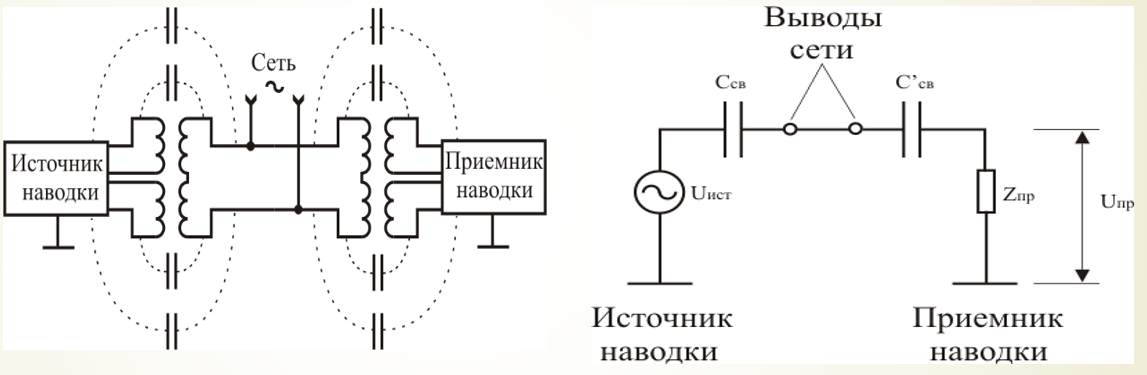
**´Образование контуров заземления между двумя устройствами**

****

**Утечка информации по цепям электропитания**

´Как правило, провода общей сети питания распределяются по различным помещениям, где расположены технические системы, и соединены с различными устройствами. Вследствие этого образуется нежелательная связь между отдельными техническими средствами. Кроме того, провода сети питания являются линейными антеннами, способными излучать или воспринимать электромагнитные поля.

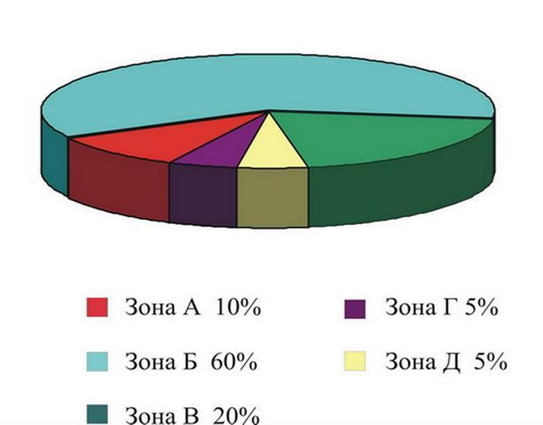
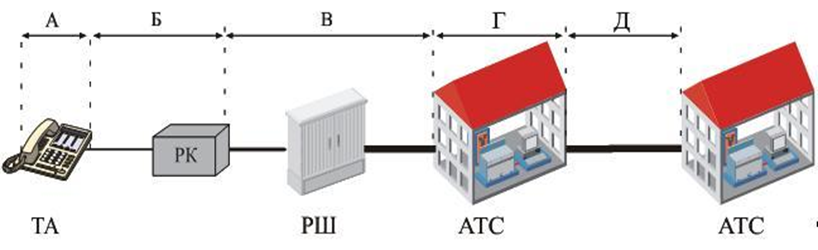
´На практике значительная часть нежелательных наводок между удаленными друг от друга устройствами происходит с участием сети питания. При этом возможны различные ситуации. В случае асимметричной наводки, когда провода сети питания прокладываются вместе и имеют одинаковые емкости относительно источников и приемников наводки, в них наводятся напряжения, одинаковые по величине и по фазе относительно земли и корпуса приборов.



´Действительная (а) и эквивалентная (б) схемы нежелательной асимметричной связи двух устройств

**Перехват информации в телефонных каналах связи**

´Телефонную систему связи можно представить в виде нескольких условных зон. К зоне «А» относится телефонный аппарат (ТА) абонента. Сигнал с аппарата по телефонному проводу попадает в распределительную коробку (РК) (зона «Б») и оттуда в магистральный кабель (зона «В»). После коммутации на автоматической телефонной станции (АТС) (зона «Г») сигнал распространяется по многоканальным кабелям (зона “Д”) до следующей автоматической телефонной станции (АТС). В каждой зоне имеются свои особенности по перехвату информации, но принципы, на которых построена техника несанкционированного подключения, практически не отличается.



´Наиболее опасными зонами, с точки зрения вероятности применения подслушивающих устройств, считаются зоны «А», «Б» и «В»

´Непосредственное подключение к линии – это самый простой и распространенный способ подслушивания телефонных разговоров. Для негосударственных организаций, занимающихся промышленным шпионажем, реально доступным местом подключения для перехвата информации являются зоны «А», «Б», «В». Подключение может быть:

´– контактным;

´– бесконтактным.

**Высокочастотное навязывание**

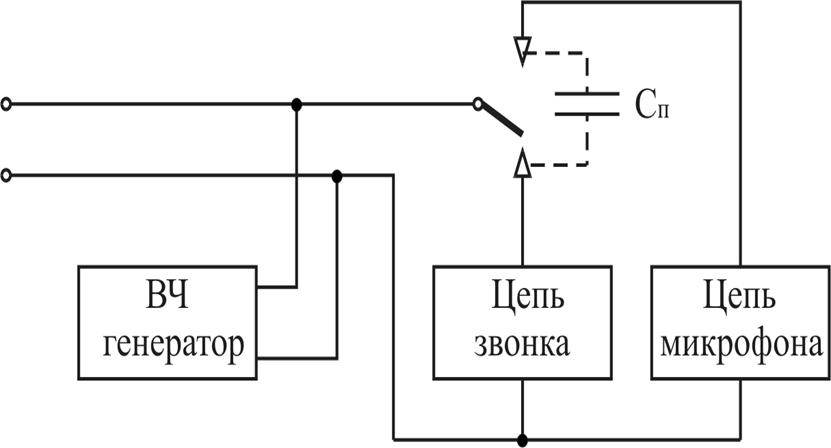
´**Высокочастотное навязывание** - это воздействие на технические средства высокочастотных сигналов.

´В настоящее время используются два способа высокочастотного навязывания:

´1. Посредством контактного введения высокочастотного сигнала в электрические цепи, имеющие функциональные или паразитные связи с техническим средством.

´2. Путем излучения высокочастотного электромагнитного поля. Возможность утечки информации при использовании высокочастотного навязывания связана с наличием в цепях технических средств нелинейных или параметрических элементов. Навязываемые высокочастотные колебания воздействуют на эти элементы одновременно с низкочастотными сигналами, возникающими при работе этих средств и содержащими конфиденциальные сведения.

´Принцип реализации высокочастотного навязывания в телефонном аппарате



´Излучение высокочастотных колебаний, промодулированных опасным сигналом, в свободное пространство осуществляется с помощью случайной антенны – телефонного провода. Промодулированный высокочастотный сигнал распространяется также в телефонной абонентской линии за пределы контролируемой территории. Следовательно, прием высокочастотных колебаний можно осуществлять либо путем подключения приемного устройства к телефонной линии, либо по полю.

**Пассивные и активные методы защиты информации от утечки по техническим каналам**

**´Пассивные методы защиты информации –** предназначены для предотвращения или существенного затруднения перехвата информации по техническим каналам за счет снижения соотношения сигнал/шум на входе средства технической разведки путем уменьшения уровня сигнала.

**´**К пассивным техническим средствам защиты относятся экранирующие устройства и сооружения, маски различного назначения, разделительные устройства в сетях электроснабжения, защитные фильтры и т. д. Цель пассивного способа – максимально ослабить сигнал от источника информативного сигнала, например, за счет отделки стен звукопоглощающими материалами или экранирования технических средств.

Пассивные методы защиты информации направлены на:

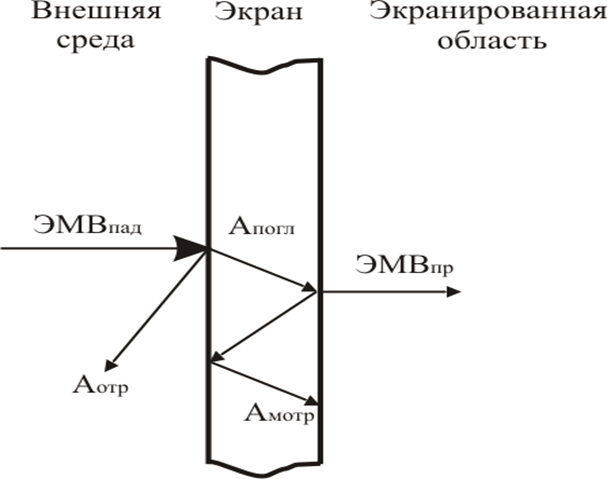
**´**• ослабление побочных электромагнитных излучений (информационных сигналов) ТСПИ на границе контролируемой зоны до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов;

**´**• ослабление наводок побочных электромагнитных излучений (информационных сигналов) ТСПИ в посторонних проводниках и соединительных линиях ВТСС, выходящих за пределы контролируемой зоны, до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов;

**´**+• исключение (ослабление) просачивания информационных сигналов ТСПИ в цепи электропитания, выходящие за пределы контролируемой зоны, до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов.

**Экранирование электромагнитных полей**

´Экранирование электромагнитного поля металлическим экраном

****

´Экранирование электромагнитных полей

На границе раздела двух сред (воздух–металл и металл–воздух) волна претерпевает отражение и преломление, а в толще экрана происходит частичное поглощение энергии электромагнитного поля.

Общая эффективность экранирования определяется суммой потерь за счет затухания энергии в толще материала *Апогл*, отражения энергии от границ раздела внешняя среда–металл и металл–экранируемая область *Аотр* и многократных внутренних отражений в стенках экрана *Амотр*:

*А = Апогл + Аотр + Амотр*

´Защита информации от утечки по электромагнитному каналу может быть обеспечена за счет снижения уровней побочных электромагнитных излучений средств обработки информации при размещении их в экранированных помещениях, а также экранировании непосредственно таких средств.

**Конструкции экранов электромагнитного излучения**

´Защита информации от утечки по электромагнитному каналу может быть обеспечена за счет снижения уровней ПЭМИ средств обработки информации при размещении их в экранированных помещениях, а также экранировании непосредственно таких средств.

´Для изготовления экранов ЭМИ применяются различные материалы, объединяемые в единую конструкцию.

´Выбор материала экрана проводится исходя из обеспечения требуемой эффективности экранирования в заданном диапазоне частот при определенных ограничениях. Эти ограничения связаны с массогабаритными характерными экрана, его влиянием на экранируемый объект, с механической прочностью и устойчивостью экрана против коррозии, с технологичностью его конструкции и т. д.

**Классификация конструкций экранов электромагнитного излучения**

****

**Фильтрация**

´В системах и средствах информатизации и связи фильтрация может осуществляться в:

´– высокочастотных тактах передающих и приемных устройств для подавления нежелательных излучений – носителей опасных сигналов – и исключения возможности их нежелательного приема;

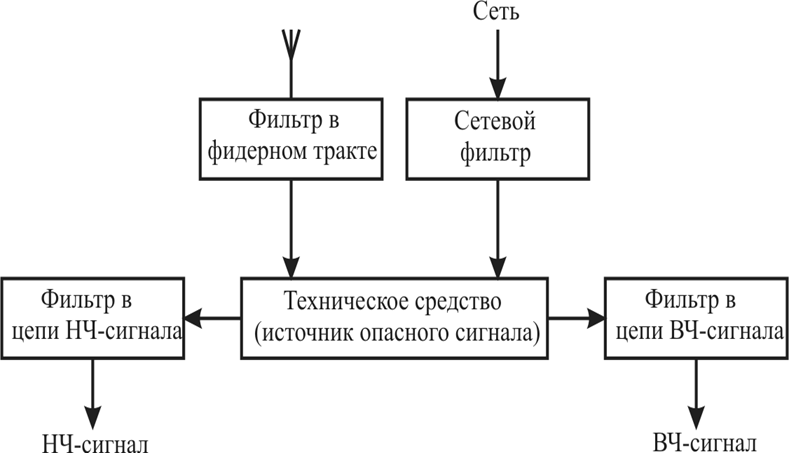
´– различных сигнальных цепях технических средств для устранения нежелательных связей между устройствами и исключения прохождения сигналов, отличающихся по спектральному составу от полезных сигналов;

´– цепях электропитания, управления, контроля, коммутации технических средств для исключения прохождения опасных сигналов по этим цепям;

´– проводных и кабельных соединительных линиях для защиты от наводок;

´– цепях пожарной и охранной сигнализации для исключения прохождения опасных сигналов и воздействия навязываемых высокочастотных колебаний.

Обобщенная схема фильтрации



**Основные требования, предъявляемые к защитным фильтрам, заключаются в следующем:**

´– величины рабочих напряжения и тока фильтра должны соответствовать величинам напряжения и тока цепи, в которой фильтр установлен;

´– эффективность ослабления нежелательных сигналов должна быть не меньше заданной в защищаемом диапазоне частот;

´– ослабление полезного сигнала в полосе прозрачности фильтра должно быть незначительным, не влияющим на качество функционирования системы;

´– габариты и масса фильтров должны быть, по возможности, минимальными;

´– фильтры должны обеспечивать функционирование при определенных условиях эксплуатации (температура, влажность, давление, удары, вибрация и т. д.);

´– конструкции фильтров должны соответствовать требованиям техники безопасности.

**К фильтрам цепей питания наряду с общими предъявляются следующие дополнительные требования:**

´– затухание, вносимое такими фильтрами в цепи постоянного тока или переменного тока основной частоты, должно быть незначительным (например 0,2 дБ и менее) и иметь большое значение (более 60 дБ) в полосе подавления, которая в зависимости от конкретных условий может быть достаточно широкой (до 1010 Гц);

´– сетевые фильтры должны эффективно работать при больших проходящих токах, высоких напряжениях и высоких уровнях мощности рабочих и подавляемых электромагнитных колебаний;

´– ограничения, накладываемые на допустимые уровни нелинейных искажений формы напряжения питания при максимальной нагрузке, должны быть достаточно жесткими (например уровни гармонических составляющих напряжения питания с частотами выше 10 кГц должны быть на 80 дБ ниже уровня основной гармоники).

**Заземление технических средств**

**´Основные требования, предъявляемые к системе заземления, заключаются в следующем:**

**´**– система заземления должна включать общий заземлитель, заземляющий кабель, шины и провода, соединяющие заземлитель с объектом;

´– сопротивления заземляющих проводников, а также земляных шин должны быть незначительными;

´– каждый заземляемый элемент должен быть присоединен к заземлителю или к заземляющей магистрали при помощи отдельного ответвления.

´Последовательное включение в заземляющий проводник нескольких заземляемых элементов запрещается;

´– в системе заземления должны, по возможности, отсутствовать замкнутые контуры, образованные соединениями или нежелательными связями между сигнальными цепями и корпусами устройств, между корпусами устройств и землей;

´– следует избегать использования общих проводников в системах экранирующих заземлений, защитных заземлений и сигнальных цепей;

´– качество электрических соединений в системе заземления должно обеспечивать минимальное сопротивление контакта, надежность и механическую прочность контакта в условиях климатических воздействий и механических нагрузок;

´– контактные соединения должны исключать возможность образования оксидных пленок на контактирующих поверхностях и связанных с этими пленками нелинейных явлений;

´– контактные соединения должны исключать возможность образования гальванических пар для предотвращения коррозии в цепях заземления;

´– запрещается использовать в качестве заземляющего устройства нулевые фазы электросетей, металлоконструкции зданий, трубы систем отопления, водоснабжения, канализации и т. д.

**Звукоизоляция помещений**

´Защита речевой информации от утечки по акустическим каналам может быть реализована за счет создания защищенных методом звукоизоляции помещений.

´Выделение акустического сигнала на фоне естественных шумов происходит при определенных соотношениях сигнал/шум. Производя звукоизоляцию, добиваются его снижения до предела, затрудняющего (исключающего) возможность выделения речевых сигналов, проникающих за пределы контролируемой зоны по акустическому или виброакустическому (ограждающие конструкции, трубопроводы) каналам.

´При выборе ограждающих конструкций выделенных помещений в процессе проектирования необходимо руководствоваться следующими правилами:

´– в качестве перекрытий рекомендуется использовать акустически неоднородные конструкции;

´– в качестве полов целесообразно использовать конструкции на упругом основании или конструкции, установленные на виброизоляторы;

´– потолки целесообразно выполнять подвесными, звукопоглощающими со звукоизолирующим слоем;

´– в качестве стен и перегородок предпочтительно использование многослойных акустически неоднородных конструкций с упругими прокладками (резина, пробка, ДВП, МВП и т. п.).

**Прохождение волн через препятствия осуществляется различными путями:**

´– через поры, окна, щели, двери и т. д. (путем воздушного переноса);

´– через материал стен, по трубам тепло-, водо- и газоснабжения и т. д. за счет их продольных колебаний (путем материального переноса);

– через материал стен и перегородок помещения за счет их поперечных колебаний (путем мембранного переноса

´Звукоизоляция помещений обеспечивается за счет использования звукопоглощающих материалов – имеющих сквозную пористость и относительно высокий коэффициент звукопоглощения (более 0,2) и обладающих динамическим модулем упругости не более 150 кгс/см2.

´По форме звукопоглощающие материалы разделяют на штучные (блоки, плиты), рулонные (маты, полосовые прокладки, холсты), рыхлые и сыпучие (вата минеральная, стеклянная, керамзит, шлак).

´По величине относительного сжатия (жесткости) звукопоглощающие и звукоизоляционные строительные материалы подразделяются на мягкие, полужесткие и твердые.

**Активные методы ЗИ от утечки по техническим каналам**

**´Активные методы ЗИ** – предназначены для предотвращения или существенного затруднения перехвата информации по техническим каналам за счет снижения соотношения сигнал/шум на входе средства технической разведки путем уменьшения уровня шума.

**´Активное техническое средство защиты** – устройство, обеспечивающее создание маскирующих активных помех (или имитирующих их) для средств технической разведки или нарушающие нормальное функционирование средств негласного съема информации. Активные способы предупреждения утечки информации можно подразделить на обнаружение и нейтрализацию этих устройств.

**Активные методы защиты информации направлены на:**

´Создание маскирующих пространственных электромагнитных помех с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения средством разведки информационного сигнала ТСПИ;

´Создание маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях ВТСС с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения средством разведки информационного сигнала ТСПИ.

**Акустическая маскировка**

Мероприятия акустической маскировки позволяют обеспечить:

´– неузнаваемость голоса диктора;

´– существенное снижение разборчивости речи диктора;

´– скрыть факт передачи речевой информации.

**Электромагнитная маскировка**

´Активные маскирующие помехи (шумовые).

´ Реализуется с помощью систем активной защиты. Такие системы подразделяются на системы линейного и пространственного зашумления.

**Обнаружение закладных устройств**

´Для повышения скрытности работы мощность передатчика ЗУ делается небольшой, но достаточной для перехвата высокочувствительным приемником с небольшого расстояния (20…400 м).

´Микрофоны делают как встроенными, так и выносными. Они бывают двух типов: акустическими или вибрационными.

**Наиболее информативными признаками проводной микрофонной системы являются:**

´– тонкий провод неизвестного назначения, подключенный к малогабаритному микрофону (часто закамуфлированному и скрытно установленному) и выходящий в другое помещение;

´– наличие в линии (проводе) неизвестного назначения постоянного (в несколько вольт) напряжения и низкочастотного информационного сигнала.

**Демаскирующие признаки автономных некамуфлированных акустических закладок:**

´признаки внешнего вида – малогабаритный предмет неизвестного назначения;

´одно или несколько отверстий малого диаметра в корпусе;

´наличие автономных источников питания;

´наличие полупроводниковых элементов, выявляемых при облучении обследуемого устройства нелинейным радиолокатором;

´наличие в устройстве проводников или других деталей, определяемых при просвечивании его рентгеновскими лучами.

´Некоторые камуфлированные ЗУ не отличаются от оригиналов даже при тщательном внешнем осмотре. Их можно обнаружить только при просвечивании предметов рентгеновскими лучами.

**Методы поиска закладных устройств:**

´специальное обследование выделенных помещений;

´поиск ЗУ с использованием технических средств;

´измерение параметров линий электропитания, телефонных линий связи и т. д.;

´проведение тестового «прозвона» всех телефонных аппаратов, установленных в проверяемом помещении, с контролем (на слух) прохождения всех вызывных сигналов автоматических телефонных станций.

**Технические средства обнаружения закладных устройств**

´*Индикаторы электромагнитных излучений.*

´Порог устанавливается так, чтобы индикатор не реагировал на внешние излучения (фон). В результате подслушивающее устройство обнаруживается только в тех точках помещения, где уровень его поля превосходит фоновый на 15…20 дБ

´*Индикаторы-частотомеры*. Отличаются от индикаторов электромагнитных излучений встроенным счетчиком – частотомером, который измеряет частоту радиосигнала, превысившего установленный порог, и помогает оператору идентифицировать сигнал подслушивающего устройства.

´*Нелинейные локаторы.* Используются для физического обнаружения и определения местоположения скрытно размещенных электронных устройств, которые могут находиться в выключенном состоянии

´*Сканирующие радиоприемники*. Современные сканеры могут автоматически перестраиваться в диапазоне до нескольких ГГц и обнаруживать сигналы с различными видами модуляции

´*Тепловизоры*. Техническое средство, обеспечивающее преобразование электромагнитного излучения (теплового), излучаемого различными объектами в видимое изображение

´*Компьютерные комплексы контроля помещений и зданий* (радиомониторинга). Представляют собой аппаратно-программные системы на базе стандартных узлов компьютера и недорогого сканера, которые оснащаются дополнительной аппаратурой и программами

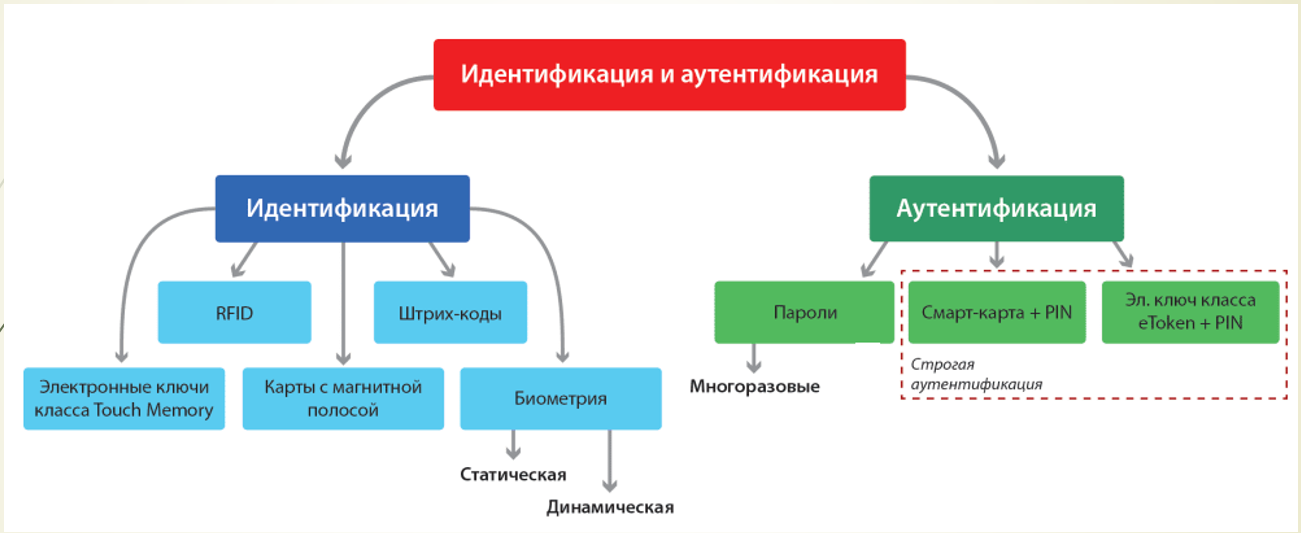
**Тема 5**

**Идентификация и аутентификация субъектов**

**´Идентификация –** процедура распознавания субъекта по его идентификатору.

**´Аутентификация –** процедура проверки подлинности субъекта, позволяющая достоверно убедиться в том, что субъект, предъявивший свой идентификатор, на самом деле является именно тем субъектом, идентификатор которого он использует.

**´Авторизация –** процедура предоставления субъекту определенных прав доступа к ресурсам системы после прохождения им процедуры аутентификации.

****

**Электронные ключи, iButton**

´Наиболее распространенный тип электронных ключей

´Как правило имеют 64 битную ПЗУ

´Количество кодовых комбинаций более 280 трлн.

´Устройства контактной памяти используются:

Øв системах управления доступом персонала

Øв системах электронных платежей

Øдля автоматической идентификации изделий (товаров) и объектов

´Электронные ключи Touch Memory – одна из разновидностей электронных идентификаторов, широко применяемых во всем мире. *По внешнему виду данный тип электронного ключа напоминает плоскую батарейку, толстую пуговицу или таблетку.*

´Второе название электронных ключей данного семейства – ключи iButton, что означает Information Button (“таблетка” с информацией). Данное название пришло на смену Touch Memory в начале 1997 года. Под этим названием электронные ключи Touch Memory выпускаются по сегодняшний день.

´Функционал, потребности программного обеспечения, количество встроенной памяти увеличиваются вместе с ростом номера модели – от DS1990 (не содержит памяти, идентификация по ID номеру, используется в домофонах), до DS1996; В модели DS1996 имеется встроенный календарь.

**Электронные ключи, Dongle**

´Аппаратное средство, предназначенное для защиты ПО и защиты от несанкционированного доступа к данным

´Могут иметь различные форм-факторы, но чаще всего они подключаются к компьютеру через USB. Также встречаются с LPT- или PCMCIA-интерфейсами.

**Технология RFID**

**´ (Radio Frequency Identification — радиочастотная идентификация) –** это технология, основанная на использовании радиочастотного электромагнитного излучения.

**´RFID-метка –** миниатюрное запоминающее устройство, которое состоит из микрочипа, хранящего информацию, и антенны, с помощью которой метка эти данные передает и получает.

´В памяти RFID-метки хранится ее собственный уникальный номер и пользовательская информация. Когда метка попадает в зону регистрации, эта информация принимается считывателем, специальным прибором, способным читать и записывать информацию в метках.

**Классификация RFID-меток**

**´1. По питанию:**

**´Активные —** используют для передачи данных энергию встроенного элемента питания (зона чтения до 100 метров);

**´Пассивные —** используют энергию, излучаемую считывателем (дальность до 8 метров).

**´2. По видам памяти:**

**´"RO" (Read Only) —** данные записываются только один раз, сразу при изготовлении. Такие метки пригодны только для идентификации. Никакую новую информацию в них записать нельзя, и их практически невозможно подделать;

**´"WORM” (Write Once Read Many) —** кроме уникального идентификатора такие метки содержат блок однократно записываемой памяти, которую в дальнейшем можно многократно читать;

**´"RW" (Read and Write) —** такие метки содержат идентификатор и блок памяти для чтения/записи информации. Данные в них могут быть перезаписаны большое число раз.

**´3. По использованию:**

´Самоклеющиеся бумажные или лавсановые метки;

´Стандартные пластиковые карты;

´Дисковые метки (в том числе с центральным отверстием для закрепления на палете);

´Различные виды брелоков;

´Специальное исполнение для жестких условий эксплуатации.

**NFC**

**´NFC (Near Field Communication) —** технология беспроводной высокочастотной связи малого радиуса действия (до 10 см), позволяющая осуществлять бесконтактный обмен данными между устройствами, расположенными на небольших расстояниях.

´Технология NFC базируется на RFID (Radio Frequency IDentification, радиочастотная идентификация).

´Три наиболее популярных варианта использования NFC технологии в мобильных телефонах:

´эмуляция карт — телефон эмулирует карту, например пропуск или платежную карту;

´режим считывания — телефон считывает пассивную метку (Tag), например для интерактивной рекламы;

´режим P2P — два телефона связываются и обмениваются информацией.

**Карты с магнитной полосой**

´Карты с магнитной полосой. В данном типе карты информация заносится на магнитную полосу. Карты с магнитной полосой бывают трёх форматов: ID-1, ID-2, ID-3. Магнитная полоса содержит 3 дорожки, на которые в закодированном виде записывают номер карты, срок ее действия, фамилию держателя карты и тому подобные данные. Объем записанной информации около 100 байт.

´Магнитная полоса может быть изготовлена для различных мощностей магнитного поля, и по этому параметру различают высококоэрцитивную (HiCo) и низкокоэрцитивную (LoCo). Степень коэрцитивности влияет на устойчивость записанной информации к размагничиванию. Пластиковые карты с магнитной полосой HiCo более надежны и долговечны, так как информация на магнитных полосах HiCo менее подвержена размагничиванию внешними магнитными полями, чем на полосах LoCo.

**Штрих-код**

´Штрих-код — это наносимая в виде штрихов закодированная информация, считываемая при помощи специальных устройств. C помощью штрихового кода кодируют информацию о некоторых наиболее существенных параметрах объекта.

´Был разработан в 1973 году.

´26 июня 1974 года был просканирован первый товар — блок 10 фруктовых жевательных резинок компании Wrigley.

´Первоначально 11 цифр кода были распределены следующим образом:

ØПрефикс — 1 цифра.

ØКод производителя — 5 цифр.

ØКод товара — 5 цифр.

1.Суммируются все цифры на нечётных позициях (первая, третья, пятая, и т. д.) и результат умножается на три.

2.Суммируются все цифры на чётных позициях (вторая, четвёртая, шестая, и т. д.).

3.Числа, полученные на предыдущих двух шагах, складываются, и из полученного результата оставляется только последняя цифра.

4.Эту цифру вычитают из 10.

5.Конечный результат этих вычислений и есть

контрольная цифра (десятке соответствует

цифра 0).

**QR-код**

´QR-код (англ. quick response - быстрый отклик) – двумерный штрихкод, разработанный в 1994 году японской фирмой Denso-Wave. В нём кодируется информация, состоящая из символов (включая кириллицу, цифры и спецсимволы).

´Максимальное количество символов, которые помещаются в один QR-код:

Øцифры — 7089;

Øцифры и буквы (латиница) — 4296;

Øдвоичный код — 2953 байт (следовательно, около 2953 букв кириллицы в кодировке windows-1251 или около 1450 букв кириллицы в utf-8);

Øиероглифы — 1817.

´Есть четыре уровня избыточности: 7, 15, 25 и 30 %. Благодаря исправлению ошибок, удаётся нанести на QR-код рисунок и всё равно оставить его читаемым.

**Технологии аутентификации**

´**Двухфакторная аутентификация** — это метод идентификации пользователя в каком-либо сервисе при помощи запроса аутентификационных данных двух разных типов, что обеспечивает более эффективную защиту аккаунта. *На практике это обычно выглядит так:*

´ *первый рубеж — это логин и пароль,*

´*второй — специальный код, приходящий по SMS или электронной почте.*

´*Реже второй «слой» защиты запрашивает специальный USB-ключ или биометрические данные пользователя. В общем, суть подхода очень проста: чтобы куда-то попасть, нужно дважды подтвердить тот факт, что вы — это вы, причем при помощи двух «ключей», одним из которых вы владеете, а другой держите в памяти.*

´*Интернет-банкинг, аккаунты в соцсетях, учетка в iCloud, почтовые ящики и особенно ваши служебные учетные записи — все это однозначно стоит защитить двухфакторной аутентификацией. Сервисы Google, Apple и все основные социальные сети позволяют это сделать в настройках без особого труда.*

´*Двухфакторная аутентификация — один из лучших методов защиты учетных записей.*

´**Многофакторная аутентификация** – в процессе которой используются аутентификационные факторы нескольких типов.

**Смарт-карты**

**Аппаратный токен** – это устройство, предназначенное специально для аутентификации.

Все смарт-карты можно разделить по способу обмена со считывающим устройством на:

´контактные смарт-карты с интерфейсом ISO 7816;

´контактные смарт-карты с USB-интерфейсом;

´бесконтактные (RFID) смарт-карты.

По функциональности карты можно разделить на:

´карты памяти;

´интеллектуальные карты.

´**Смарт-карты** представляют собой пластиковые карты со встроенной микросхемой. В большинстве случаев смарт-карты содержат микропроцессор и операционную систему, контролирующую устройство и доступ к объектам в его памяти. *Смарт-карты обладают возможностью проводить криптографические вычисления.*

´**Назначение смарт-карт** — одно- и двухфакторная аутентификация пользователей, хранение ключевой информации и проведение криптографических операций в доверенной среде.

´Все смарт-карты можно разделить ***по способу обмена со считывающим устройством*** на:

´Контактные смарт-карты с интерфейсом ISO 7816.

´*Контактные смарт-карты имеют зону соприкосновения, содержащую несколько небольших контактных лепестков. Когда карта вставляется в считыватель, чип соприкасается с электрическими коннекторами, и считыватель может считать и\или записать информацию с чипа.*

´Контактные смарт-карты с USB интерфейсом.

´*Обычно представляют из себя микросхему обычной ISO 7816 карты совмещенную с USB-считывателем в одном миниатюрном корпусе. Это делает применение смарт-карт для компьютерной аутентификации гораздо удобнее.*

´Бесконтактные (RFID) смарт-карты.

´*Это смарт-карты, в которых карта общается со считывателем через технологию RFID (Radio Frequency IDentification). Требуется подносить карточки достаточно близко к считывателю, чтобы провести необходимые операции. Они часто применяются в областях, где необходимо провести операцию быстро, например, в общественном транспорте.*

´**Применение смарт-карт:**

´**Компьютерная безопасность**

´Некоторые системы дискового шифрования, такие как FreeOTFE, TrueCrypt и Microsoft Windows 7BitLocker, могут использовать смарт-карты для безопасного хранения ключей и также для добавления дополнительного уровня шифрования для критичных частей на защищаемом диске. Смарт-карты также используются для единого входа в систему.

´**Применения в финансовой сфере**

´*Приложения смарт-карт включают их использование в банковских, дисконтных, телефонных карточках и карточках оплаты проезда, различных бытовых услуг, карт с хранимой стоимостью и т.д.*

´**Идентификация**

´*Быстро развивается применение смарт-карт в цифровой идентификации. В этой сфере карты используются для удостоверения личности.*

´**Цифровое телевидение**

´**Телефония**

**Парольная аутентификация**

´В настоящее время парольная аутентификация является наиболее распространенной, прежде всего, благодаря своему единственному достоинству – простоте использования.

недостатки:

´Пароли пользователя можно подобрать из-за достаточно небрежного отношения большинства пользователей к формированию пароля. Часто встречаются случаи выбора пользователями легко предугадываемых паролей, например:

´пароль эквивалентен идентификатору (имени) пользователя (или имени пользователя, записанному в обратном порядке, или легко формируется из имени пользователя и т.д.);

´паролем является слово или фраза какого-либо языка; такие пароли могут быть подобраны за ограниченное время путем перебора всех слов согласно словарю;

´достаточно часто пользователи применяют короткие пароли, которые взламываются простым перебором всех возможных вариантов.

´Существуют свободно доступны различные утилиты подбора паролей, в том числе, специализированные для конкретных широкораспространенных программных средств.

´Пароль может быть получен путем применения насилия к его владельцу.

´Пароль может быть подсмотрен или перехвачен при вводе.

**Меры, позволяющие значительно повысить надежность парольной защиты:**

·*наложение технических ограничений* (пароль должен быть не слишком коротким, он должен содержать буквы, цифры, знаки пунктуации и т.п.);

·*управление сроком действия паролей*, их периодическая смена;

·ограничение доступа к файлу паролей;

·ограничение числа неудачных попыток входа в систему (это затруднит применение "метода грубой силы");

·обучение пользователей;

·использование программных *генераторов паролей* (такая программа, основываясь на несложных правилах, может порождать только благозвучные и, следовательно, запоминающиеся пароли).

Перечисленные меры целесообразно применять всегда, даже если наряду с паролями используются другие методы аутентификации.

**Одноразовые пароли** (*OTP – One Time Password)*

´ Самая простая идея одноразовых паролей заключается в том, что пользователь получает **список паролей** P1, Р2,..., Рn. Каждый из паролей действует только на один сеанс входа (Р1 — на первый, Р2 — на второй и т.д.). В этом случае знание уже использовавшегося пользователем пароля ничего не даст нарушителю, а при каждом входе легального пользователя возможна проверка на использование данного пароля кем-либо еще.

´Подобная схема имеет свои **трудности**:

´организация защищенного хранения длинного списка паролей (либо его запоминание, что маловероятно);

´неясность с номером следующего пароля, если после ввода предыдущего пароля из списка вход пользователя в систему не был осуществлен из-за сбоя в работе КС.

´Указанные недостатки могут быть устранены, если список паролей **генерировать на основе некоторой необратимой функции**, например функции хеширования.

**Хэширование**

´**Хэширование** – ввод информации любой длины и размера в исходной строке и выдачу результата фиксированной длины, заданной алгоритмом функции хэширования.

´Примеры алгоритмов хеширования: md5, sha-1, CRC32, ГОСТ Р 34.11-2012

´При сбое в процессе входа пользователя всегда осуществляется выбор следующего пароля из списка, а система последовательно применяет функцию F к введенному пользователем паролю, вплоть до совпадения с последним принятым от него паролем (и тогда пользователь допускается к работе в системе) или до превышения длины списка паролей (в этом случае попытка входа пользователя в КС отвергается). На базе этой идеи и работают все современные технологии аутентификации с помощью одноразовых паролей.

´**Метод «запрос-ответ»**

´Принцип работы:

´Пользователь отправляет на сервер свой логин.

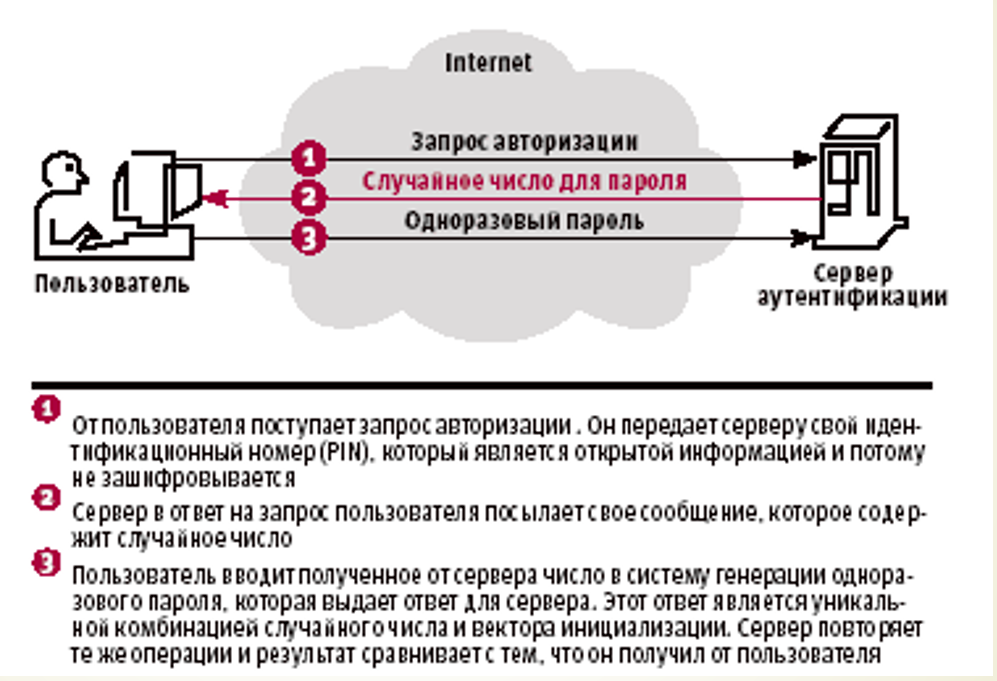
´Сервер генерирует некую случайную строку и посылает ее обратно.

´Пользователь с помощью своего ключа зашифровывает эти данные и возвращает их серверу.

´Сервер же в это время «находит» в своей памяти секретный ключ данного пользователя и кодирует с его помощью исходную строку.

´Сравнение обоих результатов шифрования. При их полном совпадении считается, что аутентификация прошла успешно.

´Этот метод реализации технологии одноразовых паролей называется **асинхронным**, поскольку процесс аутентификации не зависит от истории работы пользователя с сервером и других факторов.



**Метод «только ответ»**

´Программное или аппаратное обеспечение пользователя генерирует исходные данные, которые будут зашифрованы и отправлены на сервер для сравнения. В процессе создания строки используется значение предыдущего запроса.

´Сервер тоже обладает этими сведениями; зная имя пользователя, он находит значение предыдущего его запроса и генерирует по тому же алгоритму точно такую же строку.

´Зашифровав ее с помощью секретного ключа пользователя (он также хранится на сервере), сервер получает значение, которое должно полностью совпадать с присланными пользователем данными.

**Метод «синхронизация по времени»**

´В нем в качестве исходной строки выступают текущие показания таймера специального устройства или компьютера, на котором работает человек. При этом обычно используется не точное указание времени, а текущий интервал с установленными заранее границами (например, 30 с).

´Эти данные зашифровываются с помощью секретного ключа и в открытом виде отправляются на сервер вместе с именем пользователя.

´Сервер при получении запроса на аутентификацию выполняет те же действия: получает текущее время от своего таймера и зашифровывает его.

´После этого сервер сравнивает два значения: вычисленное и полученное от удаленного компьютера.

**Метод «синхронизация по событию»**

´Этот метод практически идентичен предыдущему.

´В качестве исходной строки в нем используется не время, а количество успешных процедур аутентификации, проведенных до текущей.

´Это значение подсчитывается обеими сторонами отдельно друг от друга.

´В настоящее время этот метод получил наиболее широкое распространение.

´В некоторых системах реализуются так называемые смешанные методы, где в качестве начального значения используется два типа информации или больше. Например, существуют системы, которые учитывают как счетчики аутентификаций, так и показания встроенных таймеров. Такой подход позволяет избежать недостатков отдельных методов.

Меры предосторожности

С учетом важности пароля как средства повышения безопасности информации от несанкционированного использования необходимо соблюдать следующие меры предосторожности:

1) не хранить пароли в вычислительной системе в незашифрованном месте;

2) не печатать и не отображать пароли в открытом виде на терминале пользователя;

3) не применять в качестве пароля свое имя или имена родственников, а также личную информацию (дата рождения, номер домашнего или служебного телефона, название улицы);

4) не применять реальные слова из энциклопедии или толкового словаря;

5) использовать длинные пароли;

6) применять смесь символов верхнего и нижнего регистров клавиатуры;

7) применять комбинации из двух простых слов, соединенных специальными символами (например, +,=,<);

8) использовать несуществующие новые слова (абсурдные или даже бредового содержания);

9) как можно чаще менять пароль.

СИСТЕМА **S/KEY**

´Наиболее известным программным *генератором одноразовых паролей* является система S/KEY компании Bellcore. Идея этой системы состоит в следующем. 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, далее, 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);

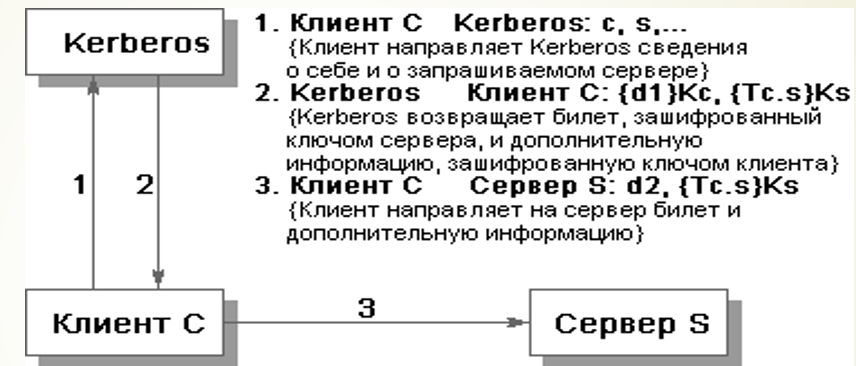
·пользователь применяет функцию f к секретному ключу K (n-1) раз и отправляет результат по сети на сервер аутентификации;

·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).

**Сервер аутентификации Kerberos**

´Kerberos– это программный продукт, разработанный в середине 1980-х годов в Массачусетском технологическом институте и претерпевший с тех пор ряд принципиальных изменений. Клиентские компоненты Kerberos присутствуют в большинстве современных операционных систем.

´Система Kerberos представляет собой доверенную третью сторону(то есть сторону, которой доверяют все), владеющую секретными ключами обслуживаемых субъектов и помогающую им в попарной проверке подлинности.

**Проверка сервером S подлинности клиента C**

´Здесь c и s – сведения (например, имя), соответственно, о клиенте и сервере,

´d1 и d2 – дополнительная (по отношению к билету) информация,

´Tc.s – билет для клиента C на обслуживание у сервера S,

´Kc и Ks – секретные ключи клиента и сервера,

´{info}K – информация info, зашифрованная ключом K.

**Системы биометрической аутентификации**

Такие системы начали внедряться с середины 1970-х гг., но наибольшее распространение получили только в последние 30 лет.

Основные требования к подобным системам:

´Считывание не должно вызывать у пользователя чувства дискомфорта,

´Считыватели должны быть легки в использовании и работать достаточно быстро,

´Считыватели должны работать корректно, однозначно обеспечивая доступ авторизованных лиц и отсечение неавторизованных

Одними из основных параметров систем биометрической аутентификации являются следующие технические характеристики:

´Вероятность ложного срабатывания (должна быть порядка 0,0001÷0,1 %),

´Вероятность несрабатывания (0,00066÷1 %),

´Чтобы уменьшить время анализа (поиск в БД), в системах могут быть встроены клавиатуры – для набора личного кода.

Следует отметить, что кроме отмеченных выше систем, анализирующих статический образ пользователя, разработаны биометрические системы, анализирующие динамические образы:

´динамика воспроизведения подписи,

´ключевого слова или фразы,

´клавиатурного почерка,

´реакция на нестандартные вопросы,

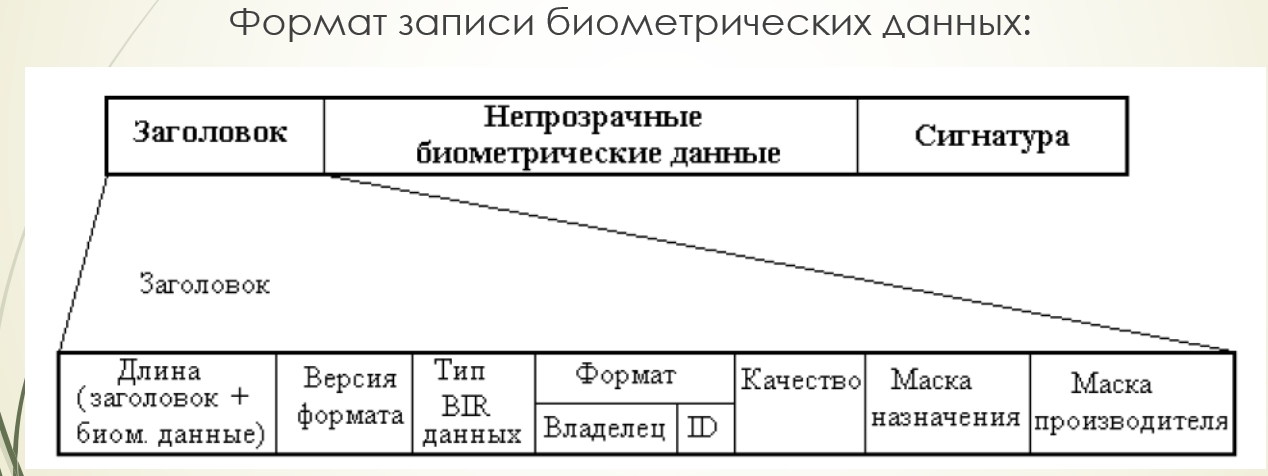
´ситуации в процессе интерактивного диалога и работы.

Из унифицированных программных интерфейсов приложений наиболее универсальным является интерфейс *BioAPI.*

В интерфейсе *BioAPI* определены два уровня.

´Уровень '*H*' (high) является «верхним» уровнем, на котором выполняются основные биометрические функции, вызываемые приложением для идентификации (аутентификации) человека

´Уровень *SPI* (Service Provider Interface) определяет интерфейс к практически любой поддерживающие этот интерфейс биометрической системе, устройства или программному обеспечению

****

**Биометрия**

´Биометрия - это идентификация человека по уникальным биологическим признакам. Методы биометрической идентификации делятся на две группы:

´1. Статические методы

´Основываются на уникальной физиологической (статической) характеристике человека, данной ему от рождения и неотъемлемой от него.

´2. Динамические методы

´Основываются на поведенческой (динамической) характеристике человека, построены на особенностях, характерных для подсознательных движений в процессе воспроизведения какого-либо действия.

**Статические методы**

´По отпечатку пальца.

´По форме ладони.

´По расположению вен на лицевой стороне ладони.

´По сетчатке глаза.

´По радужной оболочке глаза.

´По форме лица.

´По термограмме лица.

´По ДНК.

**Динамические методы**

По рукописному почерку.

´По клавиатурному почерку.

´По голосу.

**Для верхнего уровня определены три основные абстрактные функции:**

´*Enroll* (*регистрация*)*.*

´*Verify* (*верификация, распознавание один к одному*)*.*

´*Identify* (*идентификация, распознавание один ко многим*)*.*

**Для клиент-серверной обработки биометрических данных используют следующие базовые функции:**

´*Process* (*Обработка*)*.*

´*Match* (*Сопоставление*)*.*

´*CreateTemplate* (*Создание шаблона*)*.*

´*StreamingCallback(*Потоковый обратный вызов*)*.

**Полезные возможности, позволяющих компенсировать некоторые отрицательные стороны существующих биометрических технологий:**

´запрос и получение качества биометрических данных при их фиксации и обработке;

´запрос и получение фактических вероятностных характеристик биометрической системы для конкретного пользователя;

´управление графическим интерфейсом пользователя (*GUI*) со стороны приложения;

´обнаружение источника биометрических данных;

´использование клиент-серверной технологии;

´адаптация шаблонов;

´работа с автономными биометрическими устройствами;

´ограничение размерности области поиска в базах данных при идентификации один ко многим.

**Недостатки Биометрии:**

´Необходимо учитывать, что биометрия подвержена тем же угрозам, что и другие методы аутентификации.

´Во-первых, биометрический шаблон сравнивается не с результатом первоначальной обработки характеристик пользователя, а с тем, что пришло к месту сравнения. А, как известно, за время пути... много чего может произойти.

´Во-вторых, биометрические методы не более надежны, чем база данных шаблонов.

´ В-третьих, следует учитывать разницу между применением биометрии на контролируемой территории, под бдительным оком охраны, и в "полевых" условиях, когда, например к устройству сканирования роговицы могут поднести муляж и т.п.

´В-четвертых, биометрические данные человека меняются, так что база шаблонов нуждается в сопровождении, что создает определенные проблемы и для пользователей, и для администраторов.

´Но главная опасность состоит в том, что любая "пробоина" для биометрии оказывается фатальной. Пароли, при всей их ненадежности, в крайнем случае можно сменить.

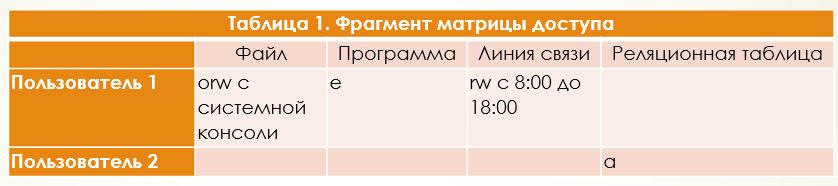
´Утерянную аутентификационную карту можно аннулировать и завести новую. Палец же, глаз или голос сменить нельзя. Если биометрические данные окажутся скомпрометированы, придется как минимум производить существенную модернизацию всей системы.

**Управление доступом**

´С традиционной точки зрения средства управления доступом позволяют специфицировать и контролировать действия, которые субъекты (пользователи и процессы) могут выполнять над объектами(информацией и другими компьютерными ресурсами).

´Логическое управление доступом – это основной механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность объектов и, до некоторой степени, их доступность (путем запрещения обслуживания неавторизованных пользователей).

**Матрица доступа**

****

´"o" – обозначает разрешение на передачу прав доступа другим пользователям,

´"r" – чтение,

´"w" – запись,

´"e" – выполнение,

´"a" – добавление информации

**Логическое управление доступом**

´Тема логического управления доступом – одна из сложнейших в области информационной безопасности. Дело в том, что само 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.

´При принятии решения о предоставлении доступа обычно анализируется следующая информация:

´идентификатор субъекта (идентификатор пользователя, сетевой адрес компьютера и т.п.). Подобные идентификаторы являются основой **произвольного (или дискреционного) управления доступом**;

´атрибуты субъекта (метка безопасности, группа пользователя и т.п.). Метки безопасности – основа **принудительного (мандатного) управления доступом**.

´Матрицу доступа, ввиду ее разреженности (большинство клеток – пустые), неразумно хранить в виде двухмерного массива. Обычно ее хранят по столбцам, то есть для каждого объекта поддерживается список "допущенных" субъектов вместе с их правами.

´Списки доступа – исключительно гибкое средство. С их помощью легко выполнить требование о гранулярности прав с точностью до пользователя. Посредством списков несложно добавить права или явным образом запретить доступ (например, чтобы наказать нескольких членов группы пользователей). Безусловно, списки являются лучшим средством произвольного управления доступом.

´Подавляющее большинство операционных систем и систем управления базами данных реализуют именно произвольное управление доступом. Основное достоинство произвольного управления – гибкость. Где для каждой пары "субъект-объект" можно независимо задавать права доступа.

Произвольное управление доступом недостатки:

´1. Рассредоточенность управления доступом ведет к тому, что доверенными должны быть многие пользователи, а не только системные операторы или администраторы. Из-за рассеянности или некомпетентности сотрудника, владеющего секретной информацией, эту информацию могут узнать и все остальные пользователи.

´2. 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 ее "троянским" аналогом.

´Удобной надстройкой над средствами логического управления доступом является **ограничивающий интерфейс**, когда пользователя лишают самой возможности попытаться совершить несанкционированные действия, включив в число видимых ему объектов только те, к которым он имеет доступ. Подобный подход обычно реализуют в рамках системы меню (пользователю показывают лишь допустимые варианты выбора) или посредством ограничивающих оболочек, таких как restricted shell в ОС Unix.

Ролевое управление доступом



´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

´**Пользователь** (человек, интеллектуальный автономный агент и т.п.);

´**Сеанс работы пользователя**;

´**Роль** (обычно определяется в соответствии с организационной структурой);

´**Объект** (сущность, доступ к которой разграничивается; например, файл ОС или таблица СУБД);

´**Операция** (зависит от объекта; для файлов ОС – чтение, запись, выполнение и т.п.; для таблиц СУБД – вставка, удаление и т.п., для прикладных объектов операции могут быть более сложными);

´**Право доступа** (разрешение выполнять определенные операции над определенными объектами).

´**Статическое разделение обязанностей** налагает ограничения на **приписывание пользователей ролям**. В простейшем случае членство в некоторой роли запрещает приписывание пользователя определенному множеству других ролей. В общем случае данное ограничение задается как пара "множество ролей – число" (где множество состоит, по крайней мере, из двух ролей, а число должно быть больше 1), так что никакой пользователь не может быть приписан указанному (или большему) числу ролей из заданного множества. Например, может существовать пять бухгалтерских ролей, но политика безопасности допускает членство не более чем в двух таких ролях (здесь число=3).

´**Динамическое разделение обязанностей** отличается от статического только тем, что рассматриваются роли, одновременно активные (быть может, в разных сеансах) для данного пользователя (а не те, которым пользователь статически приписан). 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**, являющееся аспектом минимизации привилегий.

**Тема 6**

**КОМПЬЮТЕРНЫЕ ВИРУСЫ**

**´*Компьютерный вирус –*** это специально написанная программа, способная самопроизвольно присоединяться к другим программам (заражать их), создавать свои копии и внедрять их в файлы, системные области компьютера и другие объединенные с ним компьютеры в целях нарушения нормальной работы программ, порчи файлов и каталогов, а также создания разных помех при работе на компьютере.

**Появление вирусов в компьютере. Признакам:**

·*•* уменьшение производительности работы компьютера;

·*•* невозможность и замедление загрузки ОС;

·*•* повышение числа файлов на диске;

·*•* замена размеров файлов;

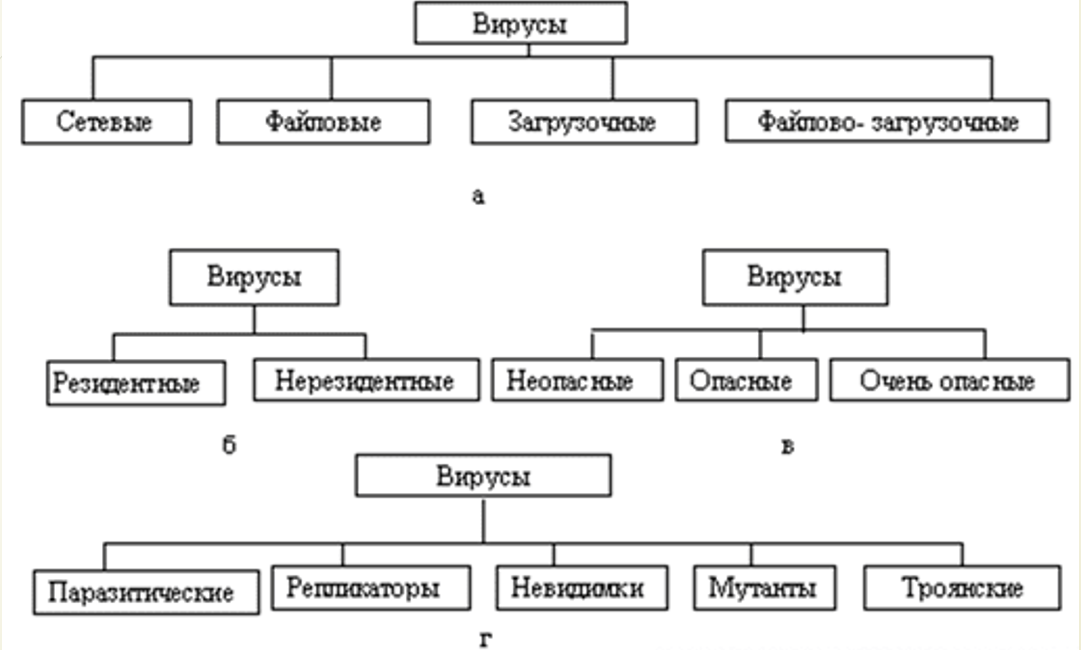
·*•* периодическое появление на экране монитора неуместных сообщений;

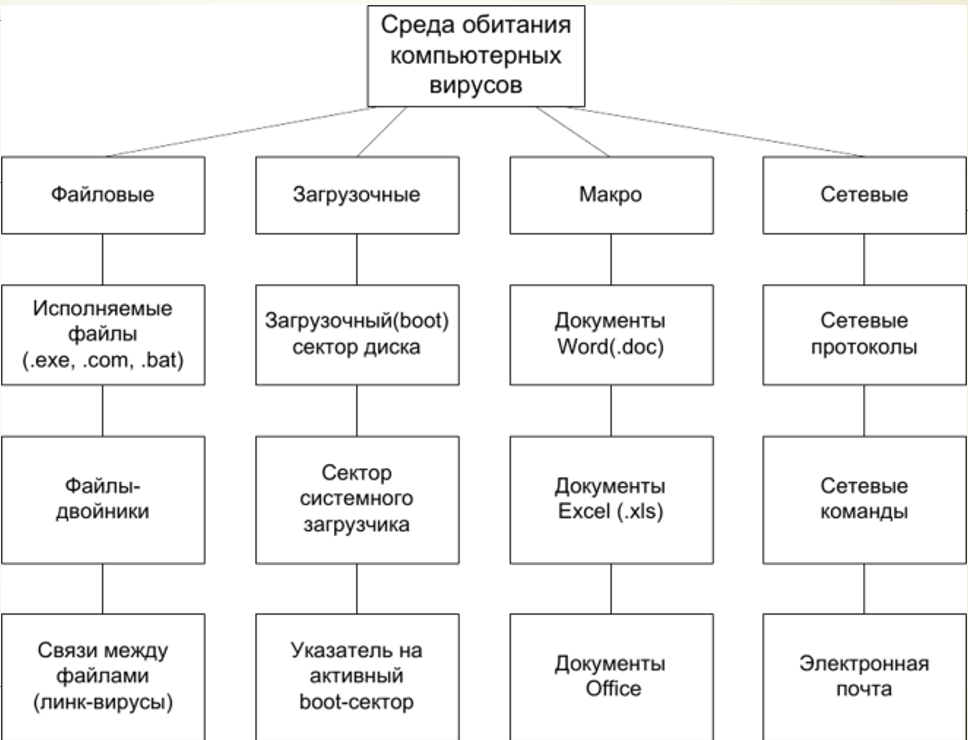
·*•* уменьшение объема свободной ОП;

·*•* резкое возрастание времени доступа к жесткому диску;

·*•* разрушение файловой структуры;

·*•* загорание сигнальной лампочки дисковода, когда к нему нет обращения.

**Классификация компьютерных вирусов**

****

**´*Загрузочные вирусы*** внедряются в загрузочный сектор диска или в сектор, который содержит программу загрузки системного диска.

**´*Файловые вирусы*** помещаются в основном в исполняемых файлах с расширением .СОМ и .ЕХЕ.

**´*Системные вирусы*** внедряются в системные модули и драйверы периферийных устройств, таблицы размещения файлов и таблицы разделов.

**´*Сетевые вирусы*** находятся в компьютерных сетях, а *файлово-загрузочные –* заражают загрузочные секторы дисков и файлы прикладных программ.

**Классификация вирусов по пути заражения среды обитания :**

**´*Резидентные вирусы*** при заражении компьютера оставляют в оперативной памяти свою резидентную часть, которая после заражения перехватывает обращение ОС к другим объектам заражения, внедряется в них и выполняет свои разрушительные действия, которые могут привести к выключению или перезагрузке компьютера. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера.

**´*Нерезидентные вирусы*** не заражают ОП компьютера и проявляют активность ограниченное время.

**´*Логическая бомба*** является программой, которая встраивается в большой программный комплекс. Она безвредна до наступления определенного события, после которого реализуется ее логический механизм.

**´*Программы-мутанты,*** самовоспроизводясь, создают копии, явно отличающиеся от оригинала.

**´*Вирусы-невидимки,*** или стелс-вирусы, перехватывают обращения ОС к пораженным файлам и секторам дисков и подставляют вместо себя незараженные объекты. Эти вирусы при обращении к файлам применяют достаточно оригинальные алгоритмы, позволяющие «обманывать» резидентные антивирусные мониторы.

**´*Макровирусы*** используют возможности макроязыков, которые встроены в офисные программы обработки данных (текстовые редакторы, электронные таблицы).

**По степени воздействия на ресурсы компьютерных систем и сетей, или по деструктивным возможностям, выделяют:**

**´*Безвредные вирусы*** не оказывают патологического влияния на работу компьютера.

**´*Неопасные вирусы*** не разрушают файлы, однако уменьшают свободную дисковую память, выводят на экран графические или звуковые эффекты.

**´*Опасные вирусы*** часто вызывают значительные нарушения в работе компьютера.

**´*Разрушительные вирусы*** могут привести к стиранию информации, полному или частичному нарушению работы прикладных программ. Важно иметь в виду, что любой файл, способный к загрузке и выполнению кода программы, является потенциальным местом, где может помещаться вирус.

´***Файловые вирусы*** либо внедряются в выполняемые файлы (наиболее распространенный тип вирусов) различными способами, либо создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (link-вирусы).*Файловые вирусы* внедряются главным образом в исполняемые модули, т.е. в файлы, имеющие расширения COM и EXE. Файловые вирусы могут внедряться и в другие типы файлов, но, как правило, записанные в таких файлах, они никогда не получают управления и, следовательно, теряют способность к размножению. Обычно файловые вирусы размещаются в конце файла или в его начальной части, реже в середине файла.

´***Загрузочные вирусы*** записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (MasterBoot Record). Загрузочные вирусы замещают код программы, получающей управление при загрузке системы. В результате при перезагрузке управление передается вирусу. При этом оригинальный boot-сектор обычно переносится в какой-либо другой сектор диска. Иногда загрузочные вирусы называют бутовыми вирусами. Они заражают макропрограммы и файлы документов современных систем обработки информации, в частности файлы-документы и электронные таблицы популярных редакторов Microsoft Word, Microsoft Excel и др. Для размножения макровирусы используют возможности макроязыков и при их помощи переносят себя из одного зараженного файла в другие. Вирусы этого типа получают управление при открытии зараженного файла и инфицируют файлы, к которым впоследствии идет обращение из соответствующего офисного приложения.

**´*Файлово - загрузочные вирусы*** заражают как файлы, так и загрузочные сектора дисков.

**´*Сетевые вирусы*** используют для своего распространения протоколы или команды компьютерных сетей и электронной почты. Иногда сетевые вирусы называют программами типа «червь». Сетевые черви подразделяются на Internet-черви (распространяются по Internet), LAN-черви (распространяются по локальной сети), IRC-черви Internet Relay Chat (распространяются через чаты). Существуют также смешанные типы, которые совмещают в себе сразу несколько технологий. *Сетевые вирусы* распространяются по различным компьютерным сетям. Их первые реализации -- mIRC.Acoragil и mIRC. Simpsalapim -- относятся 1997 г. Названия эти вирусы получили по используемым кодовым словам. Стоило ввести слова Acoragil и Simpsalapim, как вирусы тут же отключали пользователей от канала.

Жизненный цикл вирусов

´*1. латентный период(стадия хранения)*, в течение которого вирусом никаких действий не предпринимается;

´*2. инкубационный период(первая стадия исполнения)*, в рамках которого вирус только размножается;

´*3. период проявления(вторая стадия исполнения)*, в течение которого наряду с размножением выполняется несанкционированные пользователем действия.

´**Стадия хранения** соответствует периоду, когда вирус просто хранится на диске совместно с объектом, в который он внедрен. На этой стадии вирус является наиболее уязвимым со стороны антивирусного ПО, так как он не активен и не может контролировать работу ОС с целью самозащиты.

´Некоторые вирусы на этой стадии используют механизмы защиты своего кода от обнаружения. Наиболее распространенным способом защиты является шифрование большей части тела вируса. Его использование совместно с механизмами мутации кода делает невозможным выделение сигнатур — устойчивых характеристических фрагментов кода вирусов.

´**Стадия исполнения** компьютерных вирусов, как правило, включает пять этапов:

1) загрузка вируса в память;

2) поиск жертвы;

3) заражение найденной жертвы;

4) выполнение деструктивных функций;

5) передача управления программе-носителю вируса.

**1. Загрузка вируса**

´Загрузка вируса в память осуществляется ОС одновременно с загрузкой исполняемого объекта, в который вирус внедрен. Например, если пользователь запустил на исполнение программный файл, содержащий вирус, то, очевидно, вирусный код будет загружен в память как часть этого файла.

´*Полиморфные вирусы* (polymorphic) — это трудно обнаруживаемые вирусы, не имеющие сигнатур, т.е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфного вируса не будут иметь ни одного совпадения. Полиморфизм встречается в вирусах всех типов — файловых, загрузочных и макровирусах.

´Дополнительные действия, которые выполняют полиморфные вирусы на этапе загрузки, состоят в расшифровывании основного тела вируса.

´*Стелс-вирусы* (Stealth) способны скрывать свое присутствие в системе и избегать обнаружения антивирусными программами. Эти вирусы могут перехватывать запросы ОС на чтение/запись зараженных файлов, при этом они либо временно лечат эти файлы, либо «подставляют» вместо себя незараженные участки информации, эмулируя «чистоту» зараженных файлов.

**2. Поиск жертвы**

**´К первому классу** относятся вирусы, осуществляющие «активный» поиск с использованием функций ОС. Примером являются файловые вирусы, использующие механизм поиска исполняемых файлов в текущем каталоге.

**´Второй класс** составляют вирусы, реализующие «пассивный» механизм поиска, т.е. вирусы, расставляющие «ловушки» для программных файлов. Как правило, файловые вирусы устраивают такие ловушки путем перехвата функции Exec ОС, а макровирусы - с помощью перехвата команд типа Save as из меню File.

**3. Заражение жертвы**

В простейшем случае заражение представляет собой самокопирование кода вируса в выбранный в качестве жертвы объект. Классификация вирусов на этом этапе связана с анализом особенностей этого копирования и способов модификации заражаемых объектов.

***Особенности заражения файловыми вирусами***

***´К первому классу*** *относятся вирусы, которые не внедряют свой код непосредственно в программный файл, а изменяют имя файла и создают новый, содержащий тело вируса.*

***´Второй класс*** *составляют вирусы, внедряющиеся непосредственно в файлы-жертвы. Они характеризуются местом внедрения.*

***´Варианты внедрения вирусов в файлы:***

*´Внедрение в начало файла.*

*´Внедрение в конец файла.*

*´Внедрение в середину файла.*

***´Особенности заражения загрузочными вирусами определяются особенностями объектов, в которые они внедряются, —*** *загрузочными секторами жестких дисков и главной загрузочной записью (MBR) жестких дисков.*

***´Существуют различные способы решения этой задачи. Ниже приводится классификация, предложенная Е. Касперским:***

*´Используются псевдосбойные секторы.*

*´Используются редко применяемые секторы в конце раздела.*

*´Используются зарезервированные области разделов.*

*´Короткие вирусы могут уместиться в один сектор загрузчика и полностью взять на себя функции MBR или загрузочного сектора.*

***Особенности заражения макровирусами***

******

***4. Выполнение деструктивных функций***

***По деструктивным возможностям вирусы можно разделить наследующие категории:***

*´Безвредные.*

*´Неопасные.*

*´Опасные.*

*´Очень опасные.*

***5. Передача управления программе-носителю вируса***

*´Разрушающие вирусы не заботятся о сохранении работоспособности инфицированных программ, поэтому для них этот этап функционирования отсутствует.*

*´Для неразрушающих вирусов этот этап связан с восстановлением в памяти программы в том виде, в котором она должна корректно исполняться, и передачей управления программе-носителю вируса.*

***Основные каналы распространения вирусов и других вредоносных программ***

*´Классические способы распространения*

*´Электронная почта*

*´Троянские Web-сайты*

*´Локальные сети*

*´Другие каналы распространения вредоносных программ*

***Признаки проявления вирусов:***

*´прекращение работы или неправильная работа ранее успешно функционировавших программ;*

*´медленная работа компьютера;*

*´невозможность загрузки операционной системы;*

*´исчезновение файла и каталога или искажение их содержимого;*

*´изменение даты и времени модификации файлов;*

*´изменение размеров файлов;*

*´неожиданное значительное увеличение количества файлов на диске;*

*´существенное уменьшение размера свободной оперативной памяти;*

*´вывод на экран непредусмотренных сообщений или изображений;*

*´подача непредусмотренных звуковых сигналов;*

*´частые зависания и сбои в работе компьютера.*

***´Ложные антивирусы (также известные как «scareware») –*** *это программы, которые внешне похожи на приложения для обеспечения безопасности компьютера, но в действительности такой защиты почти или совсем не обеспечивают, генерируют ошибочные или заведомо ложные уведомления об угрозах или пытаются вовлечь пользователя в мошеннические операции.*

***Виды антивирусных программ:***

*´Программы-детекторы;*

*´Программы-доктора или фаги;*

*´Программы-ревизоры;*

*´Программы-фильтры;*

*´Программы-вакцины или иммунизаторы.*

***СОСАТБ***