

Уровни информационной безопасности.

- **Законодательный**
- **Административный** (приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами)
- **Процедурный** (меры безопасности, ориентированные на людей)
- **Программно-технический**

Законодательный уровень.

I. *«Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это осуждается и/или наказывается обществом, потому, что так поступать не принято.»*

II. *Две группы мер*

- Меры, направленные на создание и поддержание в обществе негативного (в том числе с применением наказаний) отношения к нарушениям и нарушителям информационной безопасности (*меры ограничительной направленности*)
- Направляющие и координирующие меры, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности (*меры созидательной направленности*)

Законодательство РФ.

Основным законом Российской Федерации является Конституция, принятая 12 декабря 1993 года.

А как же новая конституция?

Статья 41 гарантирует право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей.

Статья 42 - право на знание достоверной информации о состоянии окружающей среды.

В принципе, право на информацию может реализовываться средствами бумажных технологий, но в современных условиях наиболее практичным и удобным для граждан является создание соответствующими законодательными, исполнительными и судебными органами информационных серверов и поддержание доступности и целостности представленных на них сведений, то есть обеспечение их (серверов) информационной безопасности.

Статья 23 гарантирует право на личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений

Статья 29 - право свободно искать, получать, передавать, производить и распространять информацию любым законным способом.

Современная интерпретация этих положений включает обеспечение конфиденциальности данных, в том числе в процессе их передачи по компьютерным сетям, а также доступ к средствам защиты информации.

В Гражданском кодексе Российской Федерации фигурируют такие понятия, как **банковская, коммерческая и служебная тайна.**

Согласно статье 139, информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности.

Это подразумевает, как минимум, компетентность в вопросах ИБ и наличие доступных (и законных) средств обеспечения конфиденциальности.

Законодательство РФ.

Уголовный кодекс Российской Федерации.

Глава 28 - "Преступления в сфере компьютерной информации" - содержит три статьи:

- статья 272. Неправомерный доступ к компьютерной информации;
- статья 273. Создание, использование и распространение вредоносных программ для ЭВМ;
- статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Статья 138 УК РФ, защищая конфиденциальность персональных данных, предусматривает наказание за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.

Статья 183 УК РФ – имеет аналогичную роль для банковской и коммерческой тайны.

Интересы **государства** в плане обеспечения конфиденциальности информации нашли наиболее полное выражение в Законе *"О государственной тайне"*.

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

Определение **средств защиты информации** – «технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну; средства, в которых они реализованы, а также средства контроля эффективности защиты информации. Подчеркнем важность последней части определения».

Законодательство РФ.

Закон "Об информации, информатизации и защите информации".

- ✓ Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;
- ✓ Документированная информация (документ) – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;
- ✓ Информационные процессы – процессы сбора, обработки, накопления, хранения, поиска и распространения информации;
- ✓ Информационная система – организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы;
- ✓ Информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);
- ✓ Информация о гражданах (персональные данные) – сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;
- ✓ Конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации;
- ✓ Пользователь – субъект ...
- ✓ ...

Закон выделяет следующие цели защиты информации:

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

Законодательство РФ.

Закон "Об информации, информатизации и защите информации".

"Режим защиты информации устанавливается:

- ✓ в отношении сведений, отнесенных к государственной тайне – уполномоченными органами на основании Закона Российской Федерации "О государственной тайне";
- ✓ в отношении конфиденциальной документированной информации – собственником информационных ресурсов или уполномоченным лицом на основании настоящего Федерального закона;
- ✓ в отношении персональных данных – федеральным законом."

Обратим внимание, что защиту государственной тайны и персональных данных берет на себя государство; за другую конфиденциальную информацию отвечают ее собственники. Так же вопрос «документальной информации»?

Как же защищать информацию?

В качестве основного закон предлагает для этой цели мощные универсальные средства: **лицензирование и сертификацию**. Из статьи 19:

- Информационные системы, базы и банки данных, предназначенные для информационного обслуживания граждан и организаций, подлежат сертификации в порядке, установленном Законом Российской Федерации "О сертификации продукции и услуг".
- Информационные системы органов государственной власти Российской Федерации и органов государственной власти субъектов Российской Федерации, других государственных органов, организаций, которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих систем подлежат обязательной сертификации. Порядок сертификации определяется законодательством Российской Федерации.
- Организации, выполняющие работы в области проектирования, производства средств защиты информации и обработки персональных данных, получают лицензии на этот вид деятельности. Порядок лицензирования определяется законодательством Российской Федерации.
- Интересы потребителя информации при использовании импортной продукции в информационных системах защищаются таможенными органами Российской Федерации на основе международной системы сертификации.

Законодательство РФ.

Другие законы и нормативные акты

- ✓ Закон "О лицензировании отдельных видов деятельности" (Лицензия, вид деятельности и пр.)
 - Перечень видов деятельности (ст. 17).
 - Лицензирующие органы

- ✓ Закон «Об участии в международном информационном обмене»
 - Сертификация ...

- ✓ Закон «Об электронной цифровой подписи»
 - Определения
 - Условия
 - Сведения в сертификате

- ✓ Закон «О персональных данных»
 - Везде, где не надо
 - Нестыковки

Зарубежное законодательство.

Другие законы и нормативные акты

✓ США

- «Закон об информационной безопасности». (Computer Security Act)
- NIST, комиссия по информационной безопасности, план обеспечения ИБ.
- Добровольные стандарты, руководства, средства и методы для инфраструктуры открытых ключей
- Программа безопасности

✓ Германия.

- Federal Data Protection Act.

✓ Великобритания.

- Добровольные стандарты BS 7799.

✓ Мир в целом

- Аргентина
- РФ и чего не хватает. (механизм согласования ..., сертификация..., госконтроль ..., согласование нормативной базы..., иностранное ПО и хард...,)
- Итоги – что надо делать.
 - ✓ разработка новых законов с учетом интересов всех категорий субъектов информационных отношений;
 - ✓ обеспечение баланса созидательных и ограничительных (в первую очередь преследующих цель наказать виновных) законов;
 - ✓ интеграция в мировое правовое пространство.

Административный уровень.

Главная цель мер административного уровня – сформировать **программу работ** в области информационной безопасности и обеспечить ее выполнение, *выделяя необходимые ресурсы и контролируя состояние дел.*

Основой программы является **политика безопасности**, отражающая *подход организации к защите своих информационных активов.*

Руководство каждой организации *должно осознать* необходимость поддержания режима безопасности и выделения на эти цели значительных ресурсов.

Политика безопасности строится на основе **анализа рисков**, которые признаются реальными для информационной системы организации.

Когда риски проанализированы и стратегия защиты определена, составляется **программа обеспечения информационной безопасности.**

Под эту программу выделяются **ресурсы**, назначаются **ответственные**, определяется **порядок контроля** выполнения программы и т.п.

«политика безопасности» vs “security policy”?

Политика безопасности.

- Верхний уровень – решение, цели, база, решения. (стандарт BS7799 ...)
- Средний уровень – отдельные аспекты ИБ (описание, область, ..., т. контакта, примеры)
- Нижний уровень – сервисы (описание, аспекты)


Программа безопасности.

- Верхний/центральный уровень – стратегия, риски, решения, ответственные.
- Нижний/служебный уровень – конкретные сервисы
- Синхронизация с Жизненным циклом (описание про сервисы и этапы)

Управление рисками.

- Почему на Административном уровне?
- Для кого (каких организаций) актуально и почему?
- Опять **неприемлемый** ущерб?

Что надо делать?

- 
- (пере)оценка (измерение) рисков.
 - выбор эффективных и экономичных защитных средств (нейтрализация рисков)

По отношению к выявленным рискам возможны следующие действия:

- ликвидация риска (например, за счет устранения причины);
- уменьшение риска (например, за счет использования дополнительных защитных средств);
- принятие риска (и выработка плана действия в соответствующих условиях);
- переадресация риска (например, путем заключения страхового соглашения).

Управление рисками: этапы процесса.

1. Выбор анализируемых объектов и уровня детализации их рассмотрения.
2. Выбор методологии оценки рисков.
3. Идентификация активов.
4. Анализ угроз и их последствий, выявление уязвимых мест в защите.
5. Оценка рисков.
6. Выбор защитных мер.
7. Реализация и проверка выбранных мер.
8. Оценка остаточного риска.

Этапы 6 и 7 относятся к выбору защитных средств (нейтрализации рисков), остальные - к оценке рисков.

И опять ... Жизненный цикл!

Процедурный уровень.

- **Люди** и их действия.
- «Компьютерная грамотность» и «цифровая гигиена».

Основные классы мер:

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

Классы мер.

➤ Управление персоналом.

- ❖ разделение обязанностей;
- ❖ минимизация привилегий.

И ... опять ... **Жизненный цикл!**

Администрирование – внутреннее и внешнее

➤ Физическая защита.

! Непрерывность защиты в пространстве и времени !

- ❖ физическое управление доступом;
- ❖ противопожарные меры;
- ❖ защита поддерживающей инфраструктуры;
- ❖ защита от перехвата данных;
- ❖ защита мобильных систем.

Классы мер.

➤ **Поддержание работоспособности.**

- ❖ поддержка пользователей;
- ❖ поддержка программного обеспечения;
- ❖ конфигурационное управление;
- ❖ резервное копирование;
- ❖ управление носителями;
- ❖ документирование;
- ❖ регламентные работы.

➤ **Реагирование на нарушения режима безопасности.**

- ❖ локализация инцидента и уменьшение наносимого вреда;
- ❖ выявление нарушителя;
- ❖ предупреждение повторных нарушений.

Классы мер.

➤ Планирование восстановительных работ.

- ❖ выявление критически важных функций организации, установление приоритетов;
 - ✓ персонал (состав, резерв);
 - ✓ информационная инфраструктура (компы, ПО, внешние сервисы, документы);
 - ✓ физическая инфраструктура
- ❖ идентификация ресурсов, необходимых для выполнения критически важных функций;
- ❖ определение перечня возможных аварий;
- ❖ разработка стратегии восстановительных работ;
- ❖ подготовка к реализации выбранной стратегии;
- ❖ проверка стратегии.

Программно-технический уровень.

- Оборудование, программ и данные.
- Люди – автоматизация.

Особенности уровня:

- ✓ повышение быстродействия микросхем, развитие архитектур с высокой степенью параллелизма – ... ;
- ✓ развитие сетей и сетевых технологий, увеличение числа связей между информационными системами, рост пропускной способности каналов – ... ;
- ✓ появление новых информационных сервисов – ... ;
- ✓ конкуренция среди производителей программного обеспечения – ... ;
- ✓ навязываемая потребителям парадигма постоянного наращивания мощности аппаратного и программного обеспечения –

Современные ИС.

- ✓ **корпоративная сеть** имеет несколько территориально разнесенных частей;
- ✓ корпоративная сеть имеет несколько различных подключений к **Internet**;
- ✓ на каждой из производственных площадок есть критически важные серверы, в доступе к которым нуждаются сотрудники, работающие на других площадках, мобильные пользователи и, возможно, сотрудники других организаций;
- ✓ для доступа пользователей могут применяться не только компьютеры, но и потребительские устройства, использующие, в частности, беспроводную связь;
- ✓ в течение одного сеанса работы пользователю приходится обращаться к нескольким информационным сервисам, опирающимся на разные аппаратно-программные платформы;
- ✓ к **доступности** информационных сервисов предъявляются жесткие требования, которые обычно выражаются в необходимости круглосуточного функционирования с максимальным временем простоя порядка нескольких секунд;
- ✓ информационная система представляет собой сеть с **активными агентами**, то есть в процессе работы различные программные компоненты, передаются с одной машины на другую и выполняются в целевой среде, поддерживая связь с удаленными компонентами;
- ✓ не все пользовательские системы контролируются сетевыми и/или системными администраторами организации;
- ✓ программное обеспечение, особенно полученное по сети, не может считаться надежным, в нем могут быть ошибки, создающие проблемы в защите;
- ✓ конфигурация информационной системы постоянно изменяется на уровнях административных данных, программ и аппаратуры (меняется состав пользователей, их привилегии и версии программ, появляются новые сервисы, новая аппаратура и т.п.).

Сервисы безопасности.

- Идентификация и аутентификация;
- Управление доступом;
- Протоколирование и аудит;
- Шифрование;
- Контроль целостности;
- Экранирование;
- Анализ защищенности;
- Обеспечение отказоустойчивости;
- Обеспечение безопасного восстановления;
- Туннелирование;
- Управление.

- ✓ превентивные, препятствующие нарушениям ИБ;
- ✓ меры обнаружения нарушений;
- ✓ локализирующие зону воздействия нарушений;
- ✓ меры по выявлению нарушителя;
- ✓ меры восстановления режима безопасности

Сервисы безопасности.

➤ Идентификация и аутентификация

- ✓ нечто, что он знает (пароль, идентификационный номер, криптографический ключ и т.п.);
 - ❖ *Парольная аутентификация - что такое + и -*
 - ❖ *Одноразовые пароли - функция + и -*
 - ❖ *Сервер аутентификации Kerberos*
- ✓ нечто, чем он владеет (личную карточку или иное устройство аналогичного назначения);
- ✓ нечто, что есть часть его самого (голос, отпечатки пальцев, ... – биометрические хар-ки).

➤ Управление доступом

- ✓ матрицы доступа
- ✓ произвольное (или дискреционное) управление доступом;
- ✓ принудительное (мандатное) управление доступом

- ✓ Ролевое управление доступом (наследование ролей, иерархии ролей, минимизации привилегий + разделения обязанностей)
 - ✓ Статическое/Динамическое разделение обязанностей

Сервисы безопасности.

➤ **Протоколирование и аудит**

- ✓ **Для чего?** (подотчетность, возможность реконструкции, обнаружение нарушений, выявление и анализ проблем)
- ✓ **Аудит чего?**
- ✓ **Что протоколировать?**

Активный аудит.

➤ **Шифрование**

- ✓ шифрование;
- ✓ контроль целостности;
- ✓ Аутентификация.

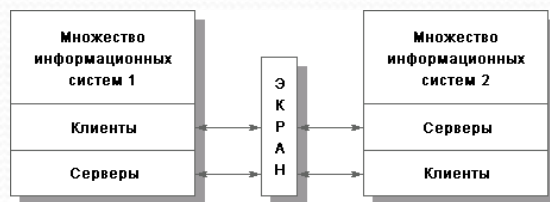
Методы шифрования: симметричный и асимметричный!

Сервисы безопасности.

➤ Контроль целостности

- ✓ хэш-функция;
- ✓ электронная цифровая подпись (ЭЦП);
- ✓ Цифровые сертификаты.

➤ Экранирование



➤ Анализ защищенности

- ✓ сканеры защищенности
- ✓ база уязвимых мест

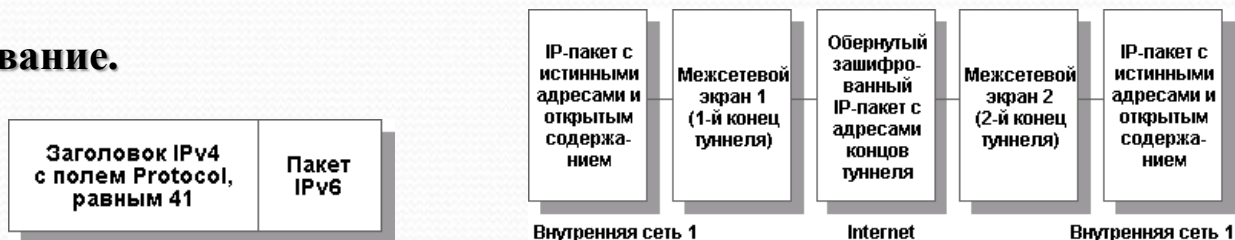
Сервисы безопасности.

➤ Обеспечение отказоустойчивости – цель.

Живучесть, зоны риска, зоны поражения, тиражируемость и резервирование.

➤ Обеспечение безопасного восстановления – как следствие.

➤ Туннелирование.



➤ Управление.

- ✓ **мониторинг** компонентов;
- ✓ **контроль** (то есть выдачу и реализацию управляющих воздействий);
- ✓ **координацию** работы компонентов системы.
- ✓ **Функциональные области управления:**
 - ✓ **управление конфигурацией** (установка параметров, запуск и остановка компонентов, сбор информации о текущем состоянии системы, прием извещений, изменение конфигурации системы);
 - ✓ **управление отказами** (выявление отказов, их изоляция и восстановление работоспособности);
 - ✓ **управление производительностью** (сбор и анализ статистической информации, определение производительности системы в штатных и нештатных условиях, изменение режима работы);
 - ✓ **управление безопасностью** (реализация политики безопасности путем создания, удаления и изменения сервисов и механизмов безопасности, а так же реагирование на инциденты);
 - ✓ **управление учетной информацией** (т.е. взимание платы за пользование ресурсами).

Архитектурная безопасность.

- I. «Пусть каждый субъект (то есть процесс, действующий от имени какого-либо пользователя) заключен внутри одного компонента и может осуществлять непосредственный доступ к объектам только в пределах этого компонента. Далее пусть каждый компонент содержит свой монитор обращений, отслеживающий все локальные попытки доступа, и все мониторы проводят в жизнь согласованную политику безопасности. Пусть, наконец, коммуникационные каналы, связывающие компоненты, сохраняют конфиденциальность и целостность передаваемой информации. Тогда совокупность всех мониторов образует единый монитор обращений для всей сетевой конфигурации.»
- II. Принципы архитектурной безопасности:
- **непрерывность защиты** в пространстве и времени, невозможность миновать защитные средства;
 - следование признанным стандартам, использование апробированных решений;
 - иерархическая организация ИС с небольшим числом сущностей на каждом уровне;
 - усиление самого **слабого звена**;
 - невозможность перехода в **небезопасное состояние**;
 - минимизация привилегий;
 - разделение обязанностей;
 - **эшелонированность обороны**;
 - разнообразие защитных средств;
 - простота и управляемость информационной системы.
- III. Обеспечение высокой доступности – **избыточность**, обнаружение нештатных ситуаций, **реконфигурирование, изоляция**, отсутствие **единой точки отказа**, выделение подсетей,
- IV. Минимизация объема защитных средств, выносимых на клиентские системы.