ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА БИЗНЕС-ИНФОРМАЦИИ

Губенко Инна Михайловна
img0504@yandex.ru

Литература

1. Хорев П.Б. Методы и средства защиты информации в компьютерных системах.
2. Хорев П.Б. Программно-аппаратная защита информации.
3. Романец Ю.В., Тимофеев П.А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях.
4. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах.

Дополнительная литература

1. Хорев П.Б. Криптографические интерфейсы и их использование.
2. Б. Шнайер. Прикладная криптография
3. Галатенко В.А. Стандарты информационной безопасности.
4. Проскурин В.Г., Крутов С.В., Мацкевич И.В. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах.

Содержание лекции

1. Основные понятия защиты информации.
2. Угрозы безопасности информации.
3. Классификация методов и средств защиты информации

Основные понятия защиты информации

- *Информация* - сведения (сообщения, данные) независимо от формы их представления. В зависимости от формы представления информация может быть разделена на речевую, телекоммуникационную и документированную.

Компьютерная (автоматизированная) система

Организационно-техническая система, включающая в себя информационные ресурсы, программно-аппаратные средства, а также обслуживающий персонал и пользователей.

Виды информации

- *Общедоступная.*
- *Ограниченного доступа:*
  - государственная тайна;
  - конфиденциальная информация:
    - служебная тайна (например, тайна суда и следствия);
    - профессиональная тайна (врачебная, адвокатская и т.п.);
    - коммерческая тайна;
    - персональные данные (сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность).

Обладатель информации

Физическое или юридическое лицо, Российская Федерация, ее субъект, муниципальное образование, которое:

- самостоятельно создало информацию

или

- в соответствии с законодательством или договором получило право управлять доступом к информации.

Защищаемая информация

Информация, имеющая обладателя и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми обладателем информации.

Защита информации

Деятельность по предотвращению

- утечки защищаемой информации,
- несанкционированных и
- непреднамеренных воздействий на защищаемую информацию.

Характеристики защищенности информации

- *Конфиденциальность (*известность содержания информации только имеющим соответствующие полномочия субъектам).

- *Целостность* (неизменность информации в условиях ее случайного и (или) преднамеренного искажения или разрушения).

- *Доступность* (способность обеспечения беспрепятственного доступа субъектов к интересующей их информации).

Утечка (копирование) информации

Неконтролируемое распространение защищаемой информации.

- *Разглашение*.
- *Несанкционированный доступ*.
- Вследствие использования *средств разведки.*

Воздействие на информацию (модификация, подмена, уничтожение)

- *Несанкционированное*.
- *Непреднамеренное.*

Цель и объекты защиты

- *Целью* защиты информации - предотвращение ущерба обладателю или пользователю информации.
- *Объект защиты* - информация, ее носитель или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью.

Информационная безопасность

- Совокупность информационных ресурсов и системы формирования, распространения и использования информации называют *информационной средой* общества.
- Под *информационной безопасностью* понимают состояние защищенности информационной среды, обеспечивающее ее формирование и развитие.

Политика (концепция) информационной безопасности

Набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа.

Угрозы безопасности

- Событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.
- *Уязвимость информации* – это возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

Атака на компьютерную систему

- *Д*ействие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости. Иначе атака на КС является попыткой реализации угрозы безопасности информации в ней.

Цели угроз безопасности информации

- Нарушение конфиденциальности (перехват, утечка или копирование информации).
- Нарушение целостности (разрушение, модификация или подделка информации).
- Нарушение доступности (блокирование информации или отказ в обслуживании).

Естественные и искусственные угрозы

- Угрозы, не зависящие от деятельности человека (*естественные* угрозы физических воздействий на информацию стихийных природных явлений).
- Угрозы, вызванные человеческой деятельностью (*искусственные* угрозы):
  - *непреднамеренные* (случайные);
  - *преднамеренные* (умышленные).

Случайные искусственные угрозы

- ошибки в проектировании КС;
- ошибки в разработке программных средств КС;
- случайные сбои в работе аппаратных средств КС, линий связи, энергоснабжения;
- ошибки пользователей КС;
- воздействие на аппаратные средства КС физических полей других электронных устройств (при несоблюдении условий их электромагнитной совместимости) и др.

Умышленные искуственные угрозы

- несанкционированные действия обслуживающего персонала КС;
- несанкционированный доступ к ресурсам КС со стороны пользователей КС и посторонних лиц.
- использование подслушивающих (радиозакладных) устройств;
- дистанционное видеонаблюдение;
- хищение носителей информации;
- сбор производственных отходов;
- намеренное копирование файлов;
- чтение остаточной информации после выполнения заданий других пользователей.

Примеры НСД к информации в КС

- модификация средств защиты (например, внедрение программных закладок);
- «ручной» или программный подбор паролей;
- подключение к КС в момент кратковременного прекращения работы легального пользователя, не заблокировавшего свой терминал;
- выдача себя за легального пользователя с применением похищенной у него или полученной обманным путем идентифицирующей информации;
- тщательное изучение подсистемы защиты КС и используемой в ней политики безопасности, выявление уязвимостей в программных средствах защиты информации в КС, внедрение программных закладок.

Основные группы методов и средств защиты информации

- методы организационно-правовой защиты информации;
- средства инженерно-технической защиты информации;
- криптографические методы и средства защиты информации;
- программно-аппаратные средства защиты информации.

Основные свойства методов организационной защиты

1. Обеспечивают полное или частичное перекрытие значительной части каналов утечки информации.
2. Объединяют все используемые в КС методы и средства в целостный механизм защиты информации.

Методы организационной защиты информации

- ограничение физического доступа к объектам КС и реализация режимных мер;
- разграничение доступа к информационным ресурсам и процессам КС:
  - установка правил разграничения доступа;
  - обеспечение шифрования информации при ее хранении и передаче;
  - обнаружение и уничтожение аппаратных и программных закладок;

Методы организационной защиты информации

- резервное копирование наиболее важных с точки зрения утраты массивов документов;
- профилактика заражения компьютерными вирусами.

Инженерно-технические средства защиты информации

Физические объекты, механические, электрические и электронные устройства, элементы конструкции зданий, средства пожаротушения и другие средства.

Назначение инженерно-технических средств защиты информации

- защита территории и помещений КС от проникновения нарушителей;
- защита аппаратных средств КС и носителей информации от хищения;
- предотвращение возможности удаленного видеонаблюдения (подслушивания) за работой персонала и функционированием технических средств КС;

Назначение инженерно-технических средств защиты информации

- организация доступа в помещения КС сотрудников;
- контроль над режимом работы персонала КС;
- контроль над перемещением сотрудников КС;
- противопожарная защита помещений КС;
- минимизация материального ущерба от потерь информации, возникших в результате стихийных бедствий и техногенных аварий.

Технические средства охраны

Образуют первый рубеж защиты КС и включают в себя:

- средства контроля и управления доступом (СКУД);
- средства охранной сигнализации;
- средства видеонаблюдения (охранного телевидения, CCTV).

СКУД

Карты Proximity, программатор и считыватели для них

СКУД

Охранная сигнализация. Потолочный датчик движения.

Беспроводная IP-камера

Нелинейный локатор

Аппаратные средства защиты информации

Электронные и электронно-механические устройства, включаемые в состав технических средств КС и выполняющие (самостоятельно или в едином комплексе с программными средствами) некоторые функции обеспечения информационной безопасности. Критерием отнесения устройства к аппаратным, а не инженерно-техническим средствам защиты является именно обязательное включение в состав технических средств КС.

Аппаратные шифраторы

Элементы и считыватели TouchMemory

Смарт-карты и считыватели для них

Карты Proximity, программатор и считыватели для них

Смарт-карты и считыватели для них

Токены


USB-ключ eToken PRO/32K
с интегрированной RFID-меткой


eToken

Генераторы одноразовых паролей

Программные средства защиты информации

Специальные программы, включаемые в состав программного обеспечения КС исключительно для выполнения защитных функций.

Программные средства защиты информации

- программы идентификации и аутентификации пользователей КС;
- программы разграничения доступа пользователей к ресурсам КС;
- программы шифрования информации;
- программы защиты информационных ресурсов от несанкционированного изменения, использования и копирования;
- Антивирусные средства
- Межсетевые экраны
- IDS и IPS
- Сканеры уязвимости
- Программы анализа содержания

Программные средства защиты информации

- программы уничтожения остаточной информации;
- программы аудита (ведения регистрационных журналов) событий, связанных с безопасностью КС;
- программы имитации работы с нарушителем;
- программы тестового контроля защищенности КС и др.

Идентификация и аутентификация

- Под *идентификацией*, применительно к обеспечению информационной безопасности КС, понимают однозначное распознавание уникального имени субъекта КС (проверка его регистрации в системе).
- *Аутентификация* при этом означает подтверждение того, что предъявленное имя соответствует данному субъекту (подтверждение подлинности субъекта).
- *Авторизация* – назначение прав доступа.
- *Аудит* – ведение журнала пользователей.

Способы аутентификации пользователей в КС

- То, что мы знаем (пароль)
- То, что у нас есть (Proximity-card)
- То, что является частью нас самих (биометрическая аутентификация)

Парольная защита. Оценка сложности подбора паролей

Сложность подбора пароля определяется мощностью множества символов, используемого при выборе пароля (N), и минимально возможной **длиной пароля** (k). В этом случае количество различных паролей может быть оценено как $\mathbf{C_p = N^k}$.

Оценка сложности подбора паролей

Например, если множество символов пароля образуют строчные латинские буквы, а минимальная длина пароля равна 3, то $Cp=26^3= 17\ 576$ (что совсем немного для программного подбора). Если же множество символов пароля состоит из строчных и прописных латинских букв, а также цифр, и минимальная длина пароля равна 6, то $Cp=62^6= 56\ 800\ 235\ 584$.

Аутентификация по отпечаткам пальцев

Мышь со

Ноутбук со сканером

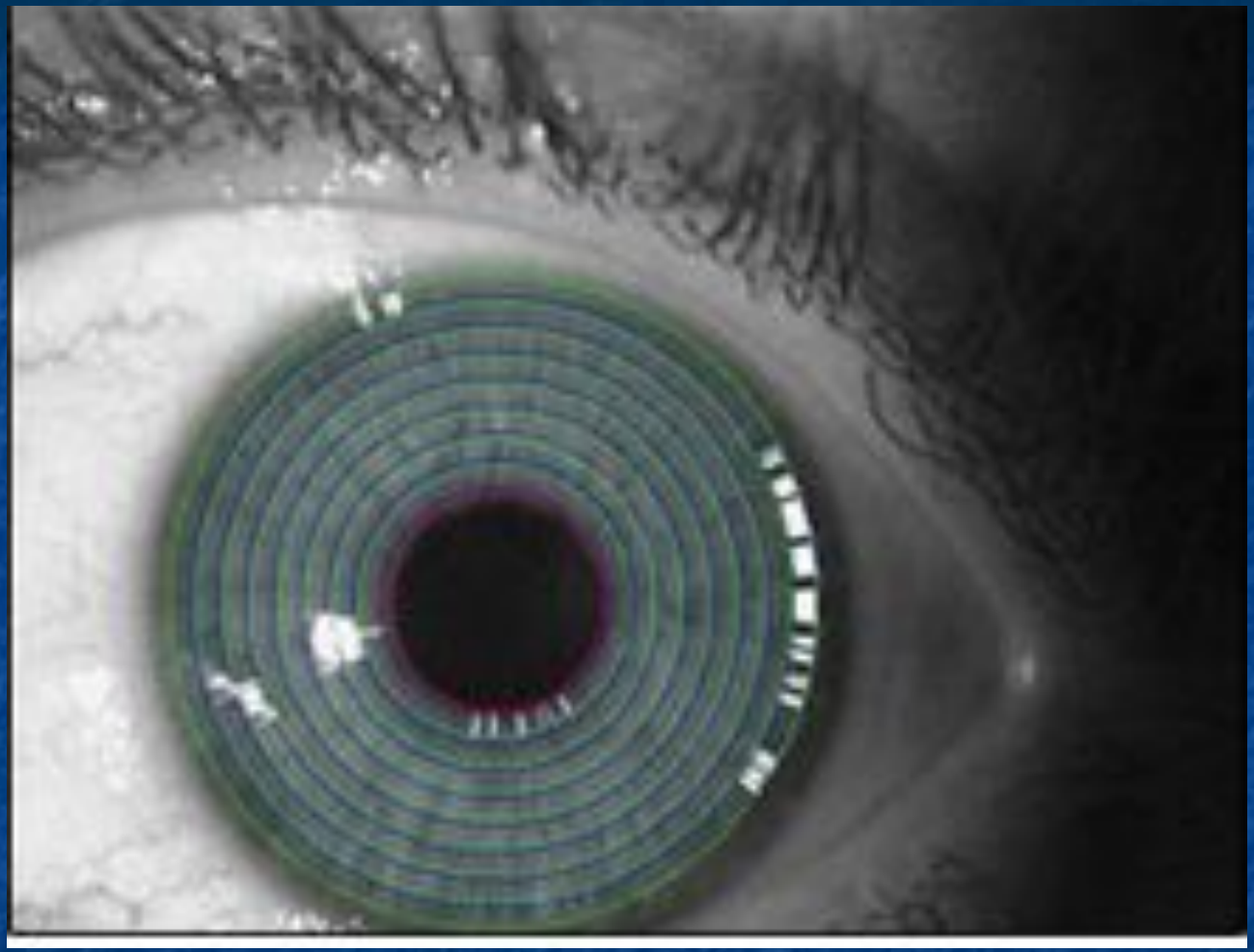
Папиллярные узоры уникальны

Аутентификация по геометрической форме руки

Камера и несколько подсвечивающих диодов

Система распознавания по радужной оболочке глаза

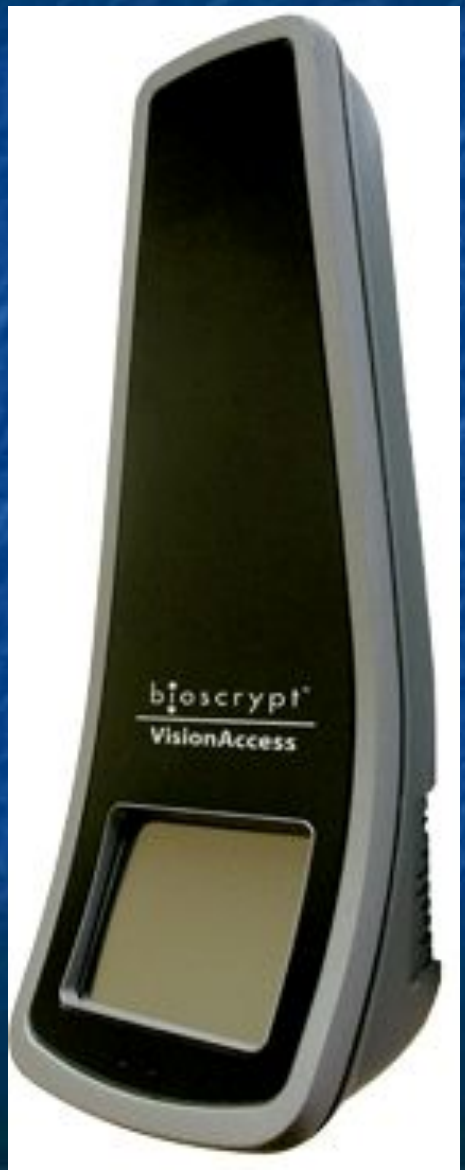
Портативный сканер сетчатки глаза



Может поместиться, например, в мобильном телефоне.

3D-сканер лица

Работает в инфракрасном диапазоне.



Термограмма лица, шеи и передней поверхности груди

Динамические биометрические характеристики

- Голос.
- Рукописная подпись.
- Темп работы с клавиатурой (клавиатурный «почерк»).
- Темп работы с мышью («роспись» мышью).

Зависят от физического и психического состояния человека (в определенных случаях может являться преимуществом)

Основные требования политики аудита

- Ассоциирование пользователя с событием аудита;
- обязательность аудита стандартного набора событий – идентификации и аутентификации пользователя, доступа к объектам, уничтожения объектов, действий привилегированного пользователя и др.;
- наличие необходимого набора атрибутов записи журнала аудита – даты и времени события, логического имени инициировавшего событие пользователя, типа события, признака успешного или неудачного завершения вызвавшего событие действия, имени связанного с событием объекта;
- возможность фильтрации записей журнала аудита;
- поддержка и защита от несанкционированного доступа к журналу аудита.

Межсетевые экраны

Реализуют набор правил, которые определяют условия прохождения пакетов данных из одной части распределенной компьютерной системы (открытой) в другую (защищенную). Обычно межсетевые экраны (МЭ) устанавливаются между сетью Интернет и локальной вычислительной сетью организации, но могут устанавливаться и на каждый хост локальной сети (персональные МЭ).

Сканеры уязвимости

Основные функции:

- проверка используемых в системе средств идентификации и аутентификации, разграничения доступа, аудита и правильности их настроек с точки зрения безопасности информации в КС;
- контроль целостности системного и прикладного программного обеспечения КС;
- проверка наличия известных, но не устранённых уязвимостей в системных и прикладных программах, используемых в КС и др.

Сканеры уязвимости

Работают на основе сценариев проверки, хранящихся в специальных базах данных, и выдают результаты своей работы в виде отчетов, которые могут быть конвертированы в различные форматы (электронных таблиц Microsoft Excel, баз данных Microsoft Access и т.п.).

Классификация сканеров уязвимости

- Уровня хоста (анализируют защищенность конкретного компьютера «изнутри»).
- Уровня сети (анализируют защищенность компьютерной системы «извне»).

Системы обнаружения атак

- Уровня хоста (обнаружение признаков атак на основе анализа журналов безопасности операционной системы, журналов МЭ и других системных и сетевых служб).
- Уровня сети (инспекция пакетов данных непосредственно в каналах связи), которые могут размещаться последовательно или параллельно с межсетевым экраном, маршрутизатором, коммутатором или концентратором.

Системы обнаружения атак

- Используют базы данных с зафиксированными сетевыми событиями и шаблонами известных атак.
- Работают в реальном масштабе времени и реагируют на попытки использования известных уязвимостей КС или несанкционированного исследования защищенной части сети организации.
- Ведут журнал регистрации зафиксированных событий для последующего анализа.

Системы контроля содержания

Предотвращаемые угрозы:

- Увеличение расходов на оплату личных Интернет-услуг сотрудников организации.
- Снижение производительности труда сотрудников.
- Снижение пропускной способности сети организации для деловых нужд.
- Утечки конфиденциальной информации.
- Репутационный ущерб для организации.

Роль правового обеспечения

- Основой проведения организационных мероприятий является использование и подготовка законодательных и нормативных документов в области информационной безопасности, которые на правовом уровне должны регулировать доступ к информации со стороны потребителей.

Уровни правового обеспечения информационной безопасности

Первый уровень образуют международные договора, к которым присоединилась Российская Федерация, и федеральные законы России:

- международные (всемирные) конвенции об охране промышленной собственности, об охране интеллектуальной собственности, об авторском праве;
- Конституция РФ (статья 23 определяет право граждан на тайну переписки, телефонных, телеграфных и иных сообщений);

Первый уровень правового обеспечения информационной безопасности

- Гражданский кодекс РФ (в статье 139 устанавливается право на возмещение убытков от утечки с помощью незаконных методов информации, относящейся к служебной и коммерческой тайне, четвертая часть посвящена вопросам правовой охраны интеллектуальной собственности – прав авторов и изобретателей, создателей баз данных и т.п.);

Первый уровень правового обеспечения информационной безопасности

- Уголовный кодекс РФ (статья 272 устанавливает ответственность за неправомерный доступ к компьютерной информации, статья 273 – за создание, использование и распространение вредоносных программ для ЭВМ, статья 274 – за нарушение правил эксплуатации ЭВМ, систем и сетей);

Первый уровень правового обеспечения информационной безопасности

- федеральный закон «Об информации, информационных технологиях и о защите информации»;
- федеральные законы «О государственной тайне», «О коммерческой тайне», «О персональных данных»;
- федеральные законы «О лицензировании отдельных видов деятельности», «О связи», «Об электронной цифровой подписи»

Уровни правового обеспечения информационной безопасности

Второй уровень правового регулирования защиты информации составляют подзаконные акты, к которым относятся указы Президента и постановления Правительства РФ, а также определения Конституционного суда РФ, письма Высшего арбитражного суда РФ и постановления пленумов Верховного суда РФ.

Второй уровень правового регулирования

- Концепция информационной безопасности Российской Федерации. Утверждена Указом Президента РФ №24 от 10 января 2000 г.
- Указ Президента РФ от 20 января 1996 г. № 71 «Вопросы Межведомственной комиссии по защите государственной тайны».
- Постановление Правительства РФ от 4 сентября 1995 г. №870 «Об утверждении правил отнесения сведений, составляющих государственную тайну, к

Уровни правового обеспечения информационной безопасности

Третий уровень правового обеспечения информационной безопасности составляют государственные стандарты (ГОСТы) в области защиты информации, руководящие документы, нормы, методики и классификаторы, разработанные соответствующими государственными органами (ФСБ, ФСТЭК и др.).

Третий уровень правового обеспечения

- Государственные стандарты РФ «Защита информации. Основные термины и определения», «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования», «Системы обработки информации. Защита криптографическая» и др.
- Руководящие документы, инструкции, методики Федеральной службы по техническому и экспортному контролю (ФСТЭК) и Федеральной службы безопасности (ФСБ).

Уровни правового обеспечения информационной безопасности

Четвертый уровень правового обеспечения информационной безопасности образуют локальные нормативные акты, положения, инструкции, методические рекомендации и другие документы по комплексной защите информации в КС конкретной организации.

Четвертый уровень правового обеспечения

- Приказ об утверждении перечня сведений, составляющих коммерческую тайну предприятия (организации).
- Разделы в трудовых и гражданско-правовых договорах, заключаемых с сотрудниками и контрагентами предприятия (организации) об обязанности возмещения ущерба за разглашение сведений, составляющих коммерческую тайну предприятия.

Четвертый уровень правового обеспечения

- Соглашение о конфиденциальности, заключаемое с каждым сотрудником организации, и др.

Криптографическое обеспечение ИБ

- **Криптография** – наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта), а также невозможности отказа от авторства.
- **Открытый (исходный) текст** — данные (не обязательно текстовые), передаваемые без использования криптографии.
- **Шифротекст**, **шифрованный (закрытый) текст** — данные, полученные после применения криптосистемы (обычно — с некоторым указанным ключом).
- **Ключ** — параметр шифра, определяющий выбор конкретного преобразования данного текста. В современных шифрах криптографическая стойкость шифра целиком определяется секретностью ключа (Принцип Керкгоффса).
- **Шифр**, **криптосистема** — семейство обратимых преобразований открытого текста в шифрованный.
- **Шифрование** — процесс нормального применения криптографического преобразования открытого текста на основе алгоритма и ключа, в результате которого возникает шифрованный текст.
- **Расшифровывание** — процесс нормального применения криптографического преобразования шифрованного текста в открытый.


Открытый текст
Ключ
Зашифрование
Шифртекст
Ключ
Расшифрование
Первоначальный открытый текст
Ключ шифрования
Ключ расшифрования

Современная криптография

- Симметричная криптография
- Криптография с открытым ключом (асимметричная криптография)
- Криптоанализ
- Цифровая подпись
- Управление ключами
- Протоколы аутентификации
- Хэширование
- Стеганография и стеганоанализ
- Квантовая криптография

Математические основы криптографии

- **Простое число** – *натуральное число*, которое не имеет делителей, кроме самого себя и единицы.
- **Взаимно простые числа** – числа, не имеющие общих делителей (кроме единицы), то есть если выполняется условие НОД(a, b)=1.
- **Нахождение остатка от деления** - арифметическая операция, результатом которой является два целых числа: неполное частное и остаток от деления одного целого числа на другое целое число:

  Разделить целое число a на натуральное число b > 0 с остатком, значит представить его в виде:

$$a = bq + r$$

где q – неполное частное , а r - остаток от деления a на b.

Математические основы криптографии

- Два целых числа *a* и *b* **сравнимы по модулю** натурального числа *n*, если при делении на *n* они дают одинаковые остатки.

Символически сравнимость записывается в виде формулы (**сравнения**):

$$a \equiv b \pmod{n}.$$

Число n называется **модулем** сравнения. Например, 32 и −10 сравнимы по модулю 7, так как оба числа при делении на 7 дают остаток 4:

$$32 = 7 \cdot 4 + 4; \quad -10 = 7 \cdot (-2) + 4$$

Симметричное шифрование

- **Симметричные криптосистемы** (также **симметричное шифрование**, **симметричные шифры**)— способ шифрования, в котором для шифрования и расшифровывания приме няется один и тот же криптографический ключ. Ключ алгоритма должен сохраняться в секрете обеими сторонами. Алгоритм шифрования выбирается сторонами до начала обмена сообщениями.

Способы симметричного шифрования

- **Перестановки** - шифр, преобразования из которого изменяют только порядок следования символов исходного текста, но не изменяют их самих.
- **Подстановки или замены** – это шифр, преобразования которого заключаются в замене каждого символа (слова или другой части теста) открытого сообщения на другие символы *(шифрообозначения)*, где порядок следования шифрообозначений совпадает с порядком следования соответствующих им символов в открытом тексте.
- **Гаммирование** - ”наложение”последовательности, состоящей из случайных чисел, на открытый текст. Последовательность случайных чисел называется **гамма-последовательностью** и используется для зашифровывания и расшифровывания данных.

Виды симметричных криптоалгоритмтов

- блочные шифры. Обрабатывают информацию блоками определённой длины (обычно 64, 128 бит), применяя к блоку ключ в установленном порядке, как правило, несколькими циклами перемешивания и подстановки, называемыми раундами. Результатом повторения раундов является лавинный эффект — нарастающая потеря соответствия битов между блоками открытых и зашифрованных данных.
- поточные шифры, в которых шифрование проводится над каждым битом, либо байтом исходного (открытого) текста с использованием гаммирования. Поточный шифр может быть легко создан на основе блочного (например, ГОСТ 28147-89 в режиме гаммирования), запущенного в специальном режиме.

Применяемы алгоритмы симметричного шифрования

Название шифра	Длина блока	Раундов	Длина ключа
DES (Data Encryption Standard)	64	16	64 (8 контрольных)
3-DES (Triple-DES)	64	48	168
DESX (DES eXtended)	64	16	184
ГОСТ 28147-89	64	32	256
IDEA (International Data Encryption Algorithm)	64	8	128
AES (Advanced Encryption Standard)	128	14	128, 192, 256
RC2 (Rivest Cipher 2)	64	Переменное	Переменная
RC5 (Rivest Cipher 5)	32, 64, 128	Переменное	Переменная
RC6 (Rivest Cipher 6)	Переменная	Переменное	Переменная
CAST (C.Adams, S.Tavares)	64	16	128
Blowfish	64	16	Переменная
SAFER+	128	8, 12, 16	128, 192, 256
Skipjack	64	32	80

Асимметричная криптография

- **Криптографическая система с открытым ключом** (или **асимметричное шифрование**, **асимметричный шифр**) — система шифрования и/или электронной подписи (ЭП), при которой *открытый ключ* передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу и используется для проверки ЭП и для шифрования сообщения. Для генерации ЭП и для расшифровки сообщения используется закрытый ключ. Криптографические системы с открытым ключом в настоящее время широко применяются в различных сетевых протоколах, в частности, в протоколах TLS и его предшественнике SSL (лежащих в основе HTTPS), в SSH

Принципы построения асимметричных криптосистем

В основе асимметричных криптографических систем лежит понятие однонаправленной функции f, обладающей следующими свойствами:

1. простое (не требующее больших ресурсов) вычисление значения функции $y=f(x)$;
2. существование обратной функции f^{-1};
3. сложное (требующее ресурсов за переделами возможностей современных компьютеров) вычисление значения обратной функции $x=f^{-1}(y)$.

Современные асимметричные криптосистемы

- RSA (стойкость основана на вычислительной сложности задачи факторизации произвольного целого числа).
  *__Задача факторизации__ – нахождение двух или более натуральных чисел, дающих при перемножении заданное число.
- Диффи-Хеллмана (стойкость основана на вычислительной сложности задачи дискретного логарифмирования).
- Эль-Гамаля (модификация криптосистемы Диффи-Хеллмана для использования в системах электронной цифровой подписи).

Схема RSA

Алгоритм генерации ключей

1. Получатель сообщения выбирает два случайных числа P и G, таких что ;
2. Получатель сообщения выбирает случайное целое число X, такое что ;
3. Вычисляется

$$Y = G^X \bmod P$$

4. Открытым ключом (OK) является тройка (P, G, Y) секретным (SK) – X.

Схема RSA

Алгоритм шифрования

Сообщение шифруется следующим образом:

1. Выбирается сессионный ключ – $1 < K < P - 1$ случайное целое число , такое что
2. Вычисляются числа

$$a = G^{K} \bmod P$$

$$b = Y^{K} M \bmod P$$

3. Пара чисел (a,b) и является шифротекстом.

Электронная цифровая подпись

Угрозы безопасности электронных документов

- подготовка документа от имени другого субъекта;
- отказ автора документа от факта его подготовки;
- изменение получателем документа его содержания;
- изменение содержания документа третьим лицом;
- повторная передача по компьютерной сети ранее переданного документа.

Электронная цифровая подпись

- Представляет собой относительно небольшой по объему блок данных, передаваемый (хранящийся) вместе (реже – отдельно) с подписываемым с ее помощью документом.
- Механизм ЭЦП состоит из двух процедур – получения (простановки) подписи с помощью закрытого ключа автора документа и проверки ЭЦП при помощи открытого ключа автора документа

Хеширование

Процесс преобразования исходного текста M произвольной длины в хеш-значение (хеш-код, дайджест, образ или просто хеш) H(M) фиксированной длины.

Системы ЭЦП

- RSA (на основе асимметричной криптосистемы RSA);
- DSS (Digital Signature Standard, стандарт США на основе асимметричной криптосистемы Эль-Гамаля);
- ECDSS (Elliptic Curve Digital Signature Standard, стандарт США на основе эллиптических кривых);
- ГОСТ Р 34.10-94 («старый» российский стандарт ЭЦП на основе асимметричной криптосистемы Эль-Гамаля);
- ГОСТ Р 34.10-2001 («новый» российский стандарт ЭЦП, использующий асимметричную криптосистему на основе эллиптических кривых).

Управление ключами

Управление ключами состоит из процедур, обеспечивающих:

- включение пользователей в систему;
- выработку, распределение и введение в аппаратуру ключей;
- контроль использования ключей;
- смену и уничтожение ключей;
- архивирование, хранение и восстановление ключей.

Стеганография

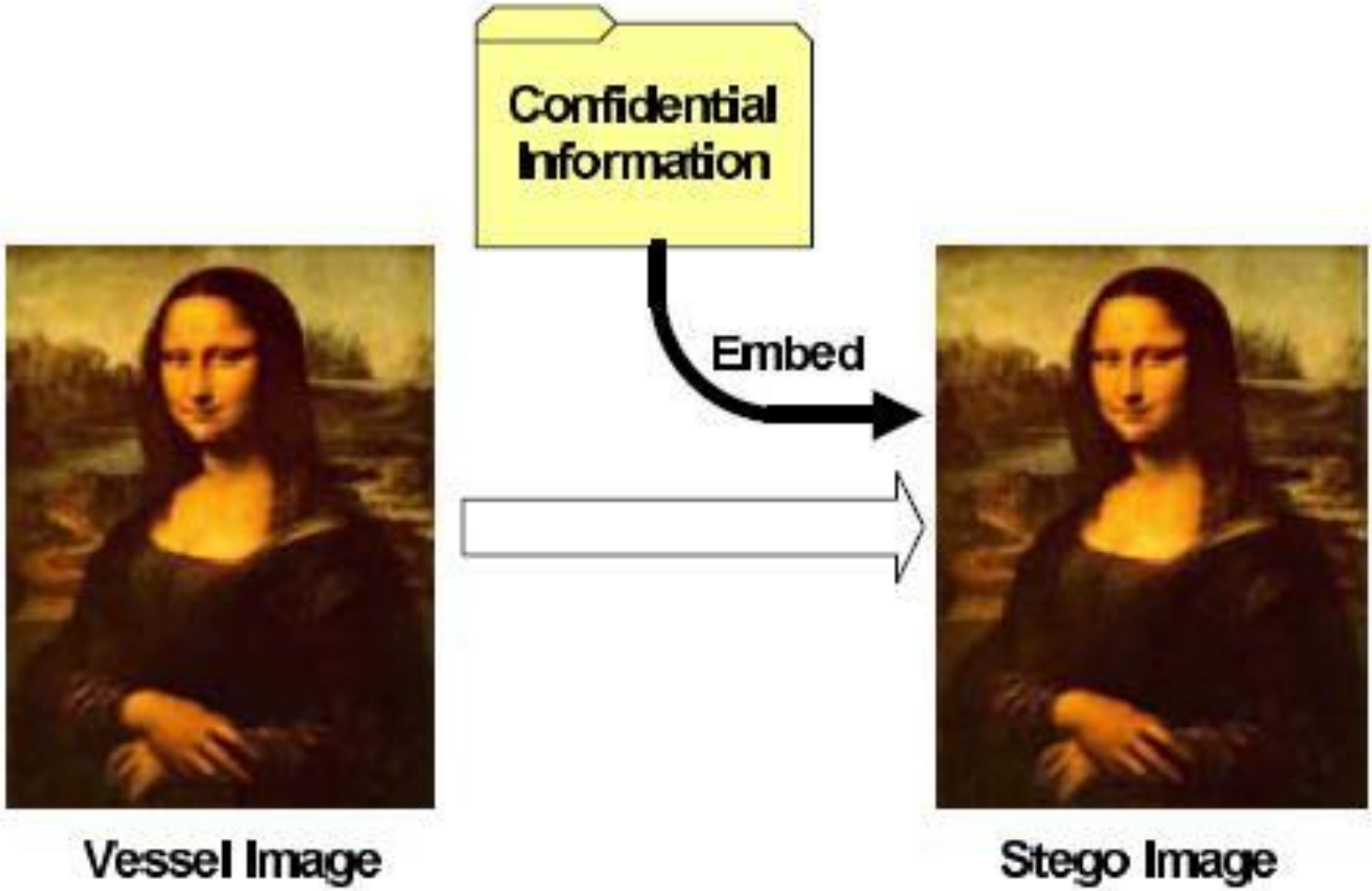
- **Стеганография** — это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи. В отличие от криптографии, которая скрывает содержимое секретного сообщения, стеганография скрывает само его существование.
- **Цифровая стеганография** — направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов.

Цифровые водяные знаки

- Из рамок цифровой стеганографии вышло наиболее востребованное легальное направление — встраивание цифровых водяных знаков (ЦВЗ) (watermarking), являющееся основой для систем защиты авторских прав и DRM (Digital rights management) систем. Методы этого направления настроены на встраивание скрытых маркеров, устойчивых к различным преобразованиям контейнера (атакам).

Основные понятия стеганографии

- Применительно к стеганографии различают *сообщение* (объект, существование и содержание которого должно быть скрыто) и *контейнер* (объект, в котором скрывается сообщение).
- При помещении сообщения в контейнер может использоваться секретный ключ, определяющий порядок помещения сообщения в контейнер. Этот же ключ должен быть задан при извлечении сообщения из контейнера


Confidential Information
Embed
Vessel Image
Stego Image

Вредоносные программы

- К *вредоносным программам* (иначе называемым *разрушающими программными воздействиями*, malware) относятся компьютерные вирусы и программные закладки.
- Впервые термин *компьютерный вирус* ввел в употребление специалист из США Ф.Коэн в 1984 г.

Компьютерный вирус

Автономно функционирующая программа, обладающая одновременно тремя свойствами:

- способностью к включению своего кода в тела других файлов и системных областей памяти компьютера;
- последующему самостоятельному выполнению;
- самостоятельному распространению в компьютерных системах.

Классификация компьютерных вирусов

1. По способу распространения в компьютерной системе:
   - файловые вирусы, заражающие файлы одного или нескольких типов;
   - загрузочные вирусы, заражающие загрузочные сектора жестких дисков и дискет;
   - комбинированные вирусы, способные заражать и файлы, и загрузочные сектора дисков.

Программные закладки

- «логические бомбы» – уничтожение или внесение изменений в функционирование программного обеспечение компьютерной системы, уничтожение или изменение обрабатываемых в ней данных после выполнения некоторого условия или получения некоторого сообщения извне;
- «троянские» программы – предоставление нарушителю доступа к конфиденциальной информации других пользователей компьютерной системы путем ее копирования и (или) передачи по сети;

Программные закладки

- компьютерные «черви» – распространение в распределенных компьютерных системах с целью реализации той или иной угрозы безопасности информации (в отличие от компьютерных вирусов не должны обладать свойством включения своего кода в тела других файлов);

Программные закладки

- перехватчики паролей пользователей компьютерной системы – имитация приглашения к их вводу или перехват всего ввода пользователей с клавиатуры;
- программы, подменяющие отдельные функции подсистемы защиты компьютерной системы;
- программы-«злые шутки», затрудняющие работу с компьютером и сообщающие пользователю заведомо ложную информацию о своих действиях в компьютерной системе;

Программные закладки

- «ботнеты», предназначенные для рассылки спама, распределенных атак с вызовом отказа в обслуживании (DDoS-атак), внедрения троянских прокси-серверов;
- «руткиты», предназначенные для скрытия следов присутствия нарушителя или вредоносной программы в системе и др.

Основные каналы распространения вредоносных программ

- электронная почта, сообщения которой могут быть заражены или содержать зараженные присоединенные файлы;
- свободное и условно свободное программное обеспечение, размещенное на общедоступных узлах сети Интернет и случайно или намеренно зараженное вредоносным кодом;

Основные каналы распространения вредоносных программ

- размещенные на общедоступных узлах сети Интернет информационные ресурсы, содержащие ссылки на зараженные файлы с элементами управления Active-X;
- локальные компьютерные сети организаций, создающие удобную среду для заражения вирусами объектов на других рабочих станциях и серверах;

Основные каналы распространения вредоносных программ

- обмен зараженными файлами на съемных носителях между пользователями компьютерной системы;
- использование нелицензионного программного обеспечения и других информационных ресурсов.

Методы обнаружения компьютерных вирусов

- Просмотр (сканирование) проверяемых объектов (системных областей дисковой и оперативной памяти, а также файлов заданных типов) в поиске сигнатур (уникальных последовательностей байтов) известных вирусов. Недостатки: необходимость постоянного обновления баз данных сигнатур известных вирусов, неспособность обнаружить новые компьютерные вирусы.

Методы обнаружения компьютерных вирусов

- Эвристический анализ – проверка системных областей памяти и файлов с целью обнаружения фрагментов исполнимого кода, характерного для компьютерных вирусов. Анализируются тысячи различных характеристик каждого файла. Недостатки: длительность процедуры проверки, возможность ложных сообщений о найденных вирусах.