Основы защиты информации

План курса

1. Проблемы безопасности информации. Понятия и определения.

2. Криптографические преобразования и протоколы. История криптографии.
3. Аутентификация и распределение ключей. Специальные криптографические протоколы. Квантовая криптография. Основы стеганографии.

4. Основные понятия ОС. Механизмы защиты операционных систем и программного обеспечения.
5. Средства защиты ОС UNIX и Windows. Безопасность доменов Windows. Механизмы защиты СУБД.

6. Техническая защита информации.

7. Основные понятия КС. Протоколы утечки информации. Безопасность сетевых соединений.
8. Защита прикладных служб (PGP, HTTPs. SSL, DNS, Java, ActiveX). Безопасность коммутируемых сетей. Безопасность беспроводных сетей.
9. Архитектура защищенных сетей (защита сетевой инфраструктуры). Сетевые экраны и средства обнаружения атак. Виртуальные защищенные сети. Протоколы PPTP и IPSec. Инфраструктура открытых ключей.

10. Корпоративная безопасность (Политика безопасности. Управление инцидентами. Криминалистический анализ). Управление информационной безопасностью.
11. Нормативно – правовая база Украины в области защиты информации. Создание и сопровождение комплексной системы защиты информации. Международные стандарты информационной безопасности и их эволюция.

Рекомендованная литература:

- Грайворонський М.В., Новіков О.М. Безпека інформаційно – комунікаційних систем. – К: Видавнича група BHV, 2009. – 608 с.

- Макнамара Д. Секреты компьютерного шпионажа: Тактика и контрмеры. - М.: БИНОМ, 2004 - 536 с.
- Столлингс В. Основы защиты сетей. Приложения и стандарты. – М.: «Вильямс», 2002. – 432 с.
- Эриксон Дж. Хакинг: искусство эксплойта. 2-е изд. - Пер. с англ. - Спб.: Символ-Плюс, 2010. - 512с.

- Антонюк А.О. Основи захисту інформації в автоматизованих системах. Навч. посібн.-К.: Видавн. дім "КМ Академія", 2003.-244 с.
- Скляров И.С. Головоломки для хакера. – СПб.: БХВ – Петербург, 2007. – 320 с.
- Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире. – СПб.: Питер, 2003. – 368с.RFC 2828. Internet Security Glossary.
- www.ietf.org/rfc/rfc2828.txt

ПРЕДМЕТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ОБЩИЕ ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Свойства и классификация информации.
Объекты и субъекты информационной безопасности.
Классификация угроз, уязвимостей и атак.

Политика безопасности. Процесс разработки политики безопасности.
Модель угроз. Классификация угроз. Модель нарушителя.

Уровни безопасности. Направления защиты ИС. Методы, меры и подсистемы защиты.
Физическая безопасность и техническая защита информации.
Задачи идентификации и аутентификации.
Виды политики разделения доступа.

Цель безопасности – сохранение значений некоторых параметров (состояния) объекта.
Цель информационной безопасности - обеспечение состояния **конфиденциальности, целостности (достоверности), доступности и наблюдаемости объекта.**

Защищаемые свойства информации (Information security Objectives, сервисы безопасности):

- Конфиденциальность (Confidentiality)
- Целостность (Integrity)
- Доступность (Availability)
- Наблюдаемость (Accountability)

Классификация информации
Категории информации: критическая, важная, полезная, не существенная…

Уровни секретности (грифы, шкала ценности):

- открытая, для служебного пользования, секретная, совершенно секретная
- unclassified, confidential, secret, top secret

Объекты *информационной* безопасности – информационная система, операционная система, протоколы передачи данных, информационные ресурсы, информация.

Субъекты *информационной* безопасности – администратор, нарушитель, аудитор, персонал.

Доступ: Субъект — Метод доступа - Объект

Субъект: пользователь, процесс или устройство
Метод доступа: чтение, запись…
Объект: записи, блоки, страницы, сегменты, файлы, директории, биты, байты, слова, терминалы, узлы, сеть...

Субъекты нарушений безопасности:
- аудитор (исследователь)
- hacker
- взломщик (cracker)
- phreaker
- spammer
- phisher

Угроза (threat) - потенциально возможное нарушение безопасности (путь реализации нарушения)
Уязвимость (vulnerability) – слабость в защите, способная привести к компрометации
Атака – попытка реализации угрозы
Exploit – механизм реализации уязвимости (чаще всего программный)

Риск — вероятность, что некоторая атака использует некоторую уязвимость системы.

Под **угрозами** подразумеваются пути реализации воздействий, которые считаются опасными.

Угроза вычислительной системе — это возможное происшествие, преднамеренное или нет, которое может оказать нежелательное воздействие на активы и ресурсы, связанные с вычислительной системой.

Угроза безопасности компьютерной сети — совокупность условий и факторов, определяющих потенциальную или реально существующую опасность нарушения конфиденциальности, целостности, доступности информации и/или снижения надежности (безотказности и аутентичности) реализации функций КС.

Угроза безопасности информации — совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее.

Типы угроз:

- Раскрытия (утечка информации, несанкционированный доступ, утрата контроля над системой безопасности)
- Нарушения целостности (целенаправленное изменение или случайные ошибки; незаконное уничтожение или модификация информации)
- Отказа служб (доступности)

Трем типам угроз соответствуют три *свойства* информации: конфиденциальность(секретность), целостность и доступность.

Конфиденциальность информации — свойство, позволяющее не давать права за доступ к информации или не раскрывать ее неполномочным лицам, логическим объектам или процессам;

Целостность информации — способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения);

Доступность — свойство быть доступным и используемым по запросу со стороны уполномоченного логического объекта.

Угрозами безопасности информационных и телекоммуникационных средств и систем могут являться:

- противоправные сбор и использование информации; нарушения технологии обработки информации; нарушение законных ограничений на распространение информации;
- несанкционированный доступ к информации, находящейся в банках и базах данных;
- внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещениях органов государственной власти, предприятии, учреждении и организаций;
- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
- перехват информации в сетях передачи данных и на линиях связи, дешифрованиве этой информации и навязывание ложной информации;
- утечка информации по техническим каналам;
- воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
- компрометация ключей и средств криптографической защиты информации;
- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;
- уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;

Методика классификации угроз STRIDE
(используется при построении модели угроз)

- Подмена объектов (spoofing identity) – в т.ч. лица пользователя
- Модификация данных (tampering with data)
- Отказ от авторства (repudiation of origin)
- Разглашение информации (information disclosure)
- Отказ в обслуживании (denial of service)
- Повышение привилегий (elevation of privilege)

Классификация уязвимостей (vulnerabilities, weaknesses)

- **В технологиях** (Technological weaknesses)

Программного обеспечения (переполнение буфера, ошибки обработки текстовых строк)
Уязвимости операционных системы
Уязвимости протоколов (HTTP, FTP, ICMP, SNMP, SMTP – не защищены)
Уязвимости сетевого оборудования (защита паролей, аутентификация, протоколы маршрутизации, межсетевые экраны)

- **В настройках** (Configuration weaknesses)

Уязвимости конфигурации (уязвимость учетных записей – небезопасная передача по сети и слабые пароли, уязвимость сетевых сервисов – JavaScript, IIS, FTP, Terminal Service; слабые настройки «по- умолчанию»)
Уязвимости сетевого оборудования (специфические)

- **В политике безопасности** (Security policy weaknesses; человеческий фактор)

Отсутствие документации, слабые политики учетных записей/паролей, неадекватный мониторинг и аудит (неавторизированное использование сервисов и возможность атаки), несогласованность (например, в изменении и установке ПО), отсутствие плана восстановления

«Хакеры не гении, они просто очень настойчивы»
«Чтобы понять природу атак – нужно научиться мыслить как хакер»

Типы атак (классификация)

- Локальные (внутренние)
- Удаленные (сетевые)
- На поток данных (прослушивание и анализ, изменение, блокировка, повтор)

- **На конфиденциальность** (разглашение информации, повышение привилегий)
- **На целостность** (подмена и модификация объектов, отказ от авторства)
- **На доступность** (отказ в обслуживании)

Сетевые атаки (атаки на сеть):

- Reconnaissance (разведка, зондирование)
- Access (доступ)
- Denial of Service (отказ в обслуживании)
- Worms, Viruses, and Trojan Horses (черви, вирусы и трояны)

Вредоносное ПО (Worms, Viruses, Trojan Horses)

-**Вирусы** (Viruses**)** – распространяют себя на компьютере автоматически (файловые, загрузочные, макровирусы, скриптовые вирусы)

-**Черви** (Worms) - Имеют механизм распространения через сеть автоматически (используют уязвимости ОС или ПО для проникновения)

-**Трояны** (Trojans) – маскируются под полезное ПО, запускаются с согласия пользователя, могут содержать нежелательные функции - вирус или червь

-**Программные закладки** (шпионские программы, перехватчики клавиатурного ввода, логические бомбы, люки; могут использовать вирусы, черви или трояны)

-**Хакерские утилиты** (эксплоиты (средства атаки), технологические программы,

“Not trust anyone you want to keep secrets”…

Социальная инженерия – попытка хакера с помощью обмана или ложных советов принудить какого-либо пользователя помочь ему в проведении атаки.

- Действия от имени вышестоящих инстанций
- Самозванство
- Сочувствие
- Ставка на личные качества
- Лесть
- Незаметное вторжение
- Вознаграждение

Противодействие социальной инженерии:

- Не доверяйте никому
- Задавайте побольше вопросов
- Будьте бюрократами
- Проверка личности
- Говорите «нет»
- Обучение пользователей

Политика безопасности определяет правила передачи и хранения информации и области ответственности.

Политику безопасности вычислительной системы организации необходимо сформулировать для того, чтобы определить, от каких именно угроз и каким образом защищается информация в вычислительной системе. Под политикой безопасности понимается набор правовых, организационных и технических мер по защите информации, принятый в конкретной организации. Политика безопасности определяет множество требований, которые должны быть выполнены в конкретной реализации системы.
Политика безопасности вычислительной системы может состоять из множества частных политик, направленных на конкретные аспекты защиты информации.

Задачи **политики безопасности**:

- Информирование персонала относительно их обязанностей по соблюдению ИБ
- Определение механизмов обеспечения безопасности
- Описание базового уровня безопасности (baseline) для последующего аудита и модернизации

- Защита персонала и информации
- Формулировка должностных инструкций разных категорий персонала
- Определение прав доступа
- Определение ответственных за обеспечение и контроль безопасности
- Описание инструкций на случай нарушения безопасности

Политика безопасности – совокупность норм и правил, регулирующих процесс обеспечения безопасности. ***Защита –*** процесс обеспечения **безопасности**

Процесс разработки политики безопасности

Разработка политики безопасности начинается с описания структуры ценностей, анализа рисков и определения правил разделения доступа.

Модель безопасности – описание политики безопасности. Используется при проектировании системы для определения механизмов и алгоритмов защиты, а также во время анализа защищенности системы для проверки и подтверждения корректности и достаточности реализованных механизмов.

План защиты:
Моделирование и анализ системы (активы, информационные потоки, роли...)
Анализ угроз (идентификация объектов, модель угроз, модель нарушителя)
Анализ рисков (оценка и обработка)
Принятие решения о применении средств защиты
Разработка политик управления ресурсами (управление правами доступа, физическая безопасность, права и обязанности)
Аварийный план (реагирование на инциденты, расследование, восстановление), управление бесперебойной работой

Модель информационных потоков (системы, документооборота, бизнес-процесса) **–** описание процессов, происходящих в системе с точки зрения жизненного цикла обрабатываемой информации (в том числе и в «бумажном» виде).

Модель угроз – структурированное описание методов и способов осуществления угроз

- Цели нарушения (свойства информации или АС, на нарушение которых направлена атака): конфиденциальность, целостность, доступность, наблюдаемость и управляемость;
- Источники возникновения угроз: внутренние или внешние субъекты;
- Пути реализации угроз: угроза физического или логического уровня (технические каналы или путем дистанционного воздействия через каналы передачи данных).

“Homo homini lupus est”

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

Три основных **мотива нарушений**: безответственность, самоутверждение и корыстный интерес. При нарушениях, вызванных безответственностью, пользователь целенаправленно или случайно производит какие-либо разрушающие действия, не связанные тем не менее со злым умыслом. В большинстве случаев это следствие некомпетентности или небрежности.

Основные **причины нарушения** безопасности АС:

-не соответствие модели безопасности
-неправильное внедрение модели безопасности
-отсутствие идентификации/аутентификации
-отсутствие контроля целостности
-ошибки в программной реализации, наличие люков
-ошибки администрирования

Модель нарушителя — это абстрактное (формализованное или неформализованное) описание нарушителя.

При разработке модели нарушителя определяются:

- предположения о категориях лиц, к которым может принадлежать нарушитель;
- предположения о мотивах действий нарушителя (преследуемых нарушителем целях);
- предположения о квалификации нарушителя и его технической оснащенности (об используемых для совершения нарушения методах и средствах);
- ограничения и предположения о характере возможных действий нарушителя.

- Категории нарушителей: внутренние/внешние, пользователи/ тех.персонал/руководители.
- Цель и мотивы нарушителя: получение и изменение информации, уничтожение ценностей или отказ в обслуживании.
- Полномочия, теоретические и практические возможности нарушителя (методы и средства): запуск фиксированного набора программ, создание и запуск собственных программ, внесение изменений в настройки системы;
- Уровень знаний об автоматизированной системе. Возможность подключения ложных устройств;
- Техническое оснащение: аппаратные, программные и прочие средства;
- Квалификация нарушителя: максимально возможная.
- Характер и возможные действия. Предусмотреть возможность сговора.

Модель угроз и *модель нарушителя* – входная информация при разработке политики безопасности и проектировании систем защиты.

Методы (меры, средства, направления) защиты:

- Технические (аппаратные, программные)
- Криптографические
- Административные (организационные, законодательные)

Средства защиты:

ОС:

-защита адресного пространства, управление процессами;
-аутентификация, разделение доступа;
-аудит;
-сканеры, антивирусы;
-контроль целостности объектов.

Сетевые средства:

-защита устройств;
-защита периметра, фильтрация, наблюдение (сетевые экраны, IDS/IPS);
-защита соединений (SSL, VPN);
-защита сервисов (проверка синтаксиса, управление ресурсами, актуализация);
-сетевая аутентификация (802.1X, RADIUS...);
-аудит (нотаризация).

Меры защиты (Mitigation Techniques)**:**

- Контроль физического доступа к системе
- Использовать сильные пароли и часто их менять
- Отключить редко используемые службы
- Антивирусы, актуализация ПО, карантин
- Актуальные патчи ОС
- Регулярное резервное копирование и проверка резервных копий
- Персональные экраны
- Система выявления атак (сетевая)

Подсистемы защиты:

- Идентификации и аутентификации
- Управления доступом
- Регистрации событий (аудита)
- Обеспечения целостности
- Криптографическая защита

Общие направления защиты ИС (places of defense)

- минимизация неиспользуемых функций и сервисов
- безопасность доступа, учетных записей, паролей
- политика безопасности

“Самый надежный корабль всегда стоит на берегу и никогда не выходит в море”

Уровни безопасности информационной системы:

- Физическая безопасность
- Безопасность ОС
- Безопасность протоколов передачи данных (канального, сетевого, транспортного, прикладного уровня)
- Системная безопасность

Физическая безопасность:

- Физический доступ (замки, камеры, охрана, …)
- Безопасность среды (температура, обдув, влажность, сигнализация,…)
- Электробезопасность (UPS, избыточность, автономный генератор, система оповещения)
- Обслуживание (безопасность кабельной структуры, документация,…)

Техническая защита информации:
Защита от несанкционированного доступа (нарушения прав разделения доступа)
Защита от утечки информации по техническим каналам (оптические, акустические, побочные электромагнитные излучения и наводки)

Каналы утечки информации

- Физические (электромагнитные, акустические, оптические)
- Информационные (временные, с памятью)

Идентификация: распознавание объектов и назначение идентификаторов
Аутентификация: проверка подлинности

Виды аутентификации в АС:

- Парольная система
- По цифровым сертификатам
- Электронные ключи
- Биометрия (дактилоскопия, по форме ладони, по радужной оболочке глаза, лицевая термография, распознавание голоса, распознавание подписи, распознавание клавиатурного почерка, распознавание генетического кода…)

Виды политик управления доступом

Дискреционная политика:

- однозначная идентификация субъектов и объектов
- разделение доступа на основе матрицы доступа (списков контроля доступа или списки возможностей)

Нормативная (мандатная) политика (модель Беллы-ЛаПадула)**:**

- однозначная идентификация субъектов и объектов
- упорядоченная шкала меток секретности объектов (ценности информации)
- субъектам назначен уровень доступа (уровень доверия - максимальная метка секретности, к которой субъект может получить доступ)

Цель *нормативной политики*: предотвращение утечки информации (информационных потоков) от объектов с высоким уровнем доступа к объектам с низким уровнем доступа

Ролевая политика:

- Правила назначения ролей субъектам
- Матрица прав доступа для ролей

Чаще всего используется иерархическая организация ролей

“Безопасность — это процесс, а не результат («Security is a process, not a product»)”

(Bruce Schneier)

Процесс безопасности (security wheel):

- Обеспечение защиты (VPN, политика доступа (кто- что), аутентификация)
- Мониторинг (Монитор трафика, система учета)
- Тестирование
- Модернизация защиты ….

Защита информации должна обеспечиваться на всех стадиях жизненного цикла ИС.

Вопросы по теме 1:

- В чем цель обеспечения информационной безопасности.
- Свойства и категории информации.
- Объекты и субъекты информационной безопасности.
- Субъекты нарушения информационной безопасности.

- Что такое угроза, уязвимость и атака. Их отличие.
- Классификация и примеры типов угроз информационной безопасности.
- Классификация уязвимостей информационных систем.
- Назовите основные уязвимости ИС каждого типа и соответствующие меры противодействия.
- Классификация атак.
- Виды сетевых атак.
- Классификация вредоносного ПО.
- Методы социальной инженерии и способы противодействия им.

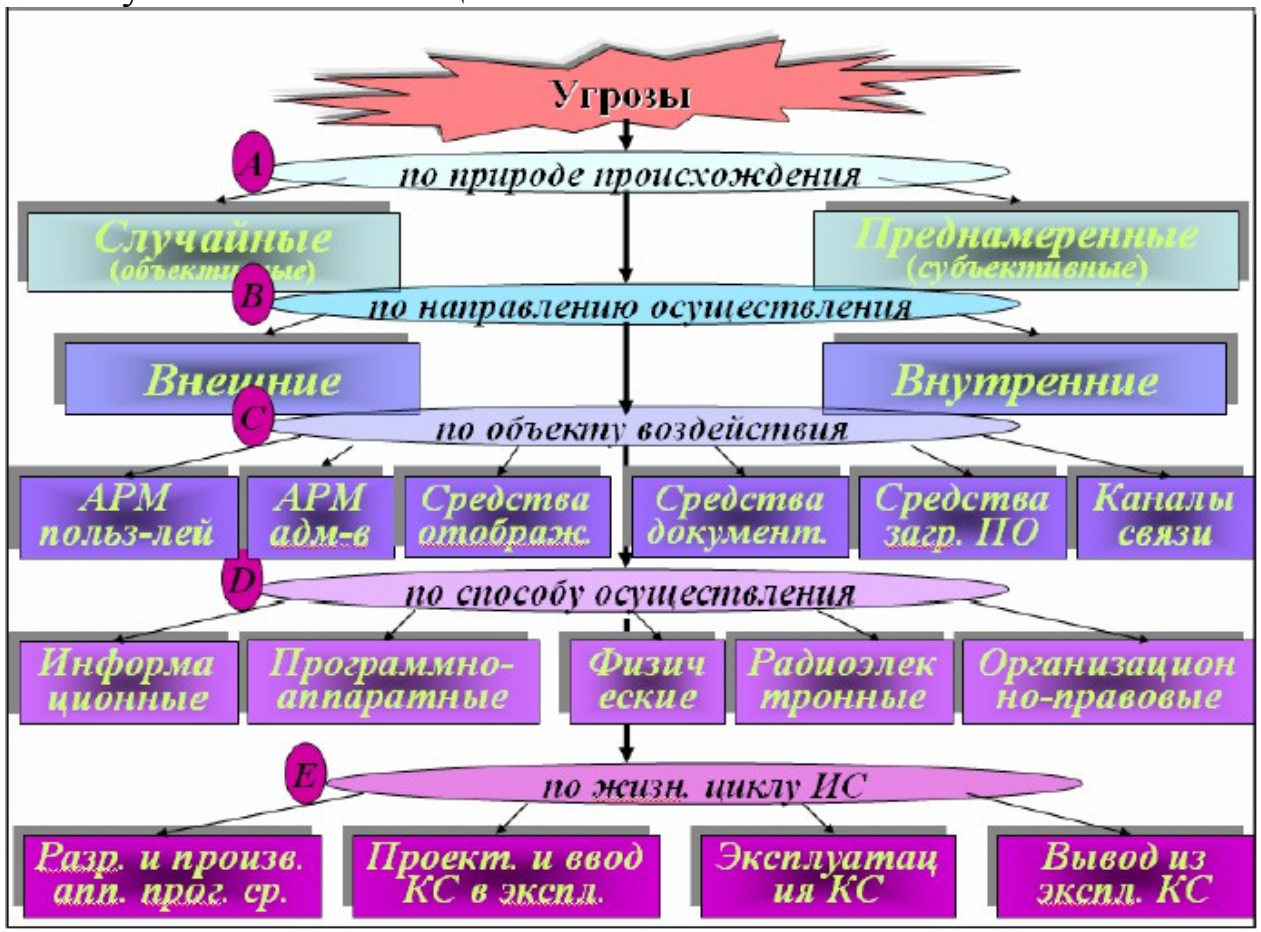
- Направления обеспечения безопасности ИС.
- Методы защиты информации в ИС.
- Подсистемы защиты в ИС.
- Уровни безопасности в ИС.
- Направления обеспечения физической безопасности.
- Задачи технической защиты информации.
- Каналы утечки информации.
- Задачи идентификации и аутентификации. Виды аутентификации.

- Что такое политика безопасности ИС, ее задачи.
- Виды политик управления доступом
- Что такое модель безопасности.
- Что такое модель угроз и модель нарушителя. Для чего они используются и что описывают
- Классификация угроз.

Приложение 1. Классифкация угроз:

Типы угроз

- **Неструктурированные** (доступны инструменты)
- **Структурированные** (мотивация и компетенция)
- **Объективные и субъективные** (случайные и преднамеренные)
- **Внутренние и внешние**
- **Social Engineering** (эксплуатация наивности и доверчивости с целью получения информации). Человек – самое уязвимое звено в цепочке безопасности.



Виды угроз (антропогенные, технические, стихийные):

Ошибки, повреждения, поломки, несчастные случаи
Нарушения

Шпионаж
Разглашение (раскрытие)
НСД, подключения
Завладение, кража, потеря
Копирование
Модификация, отказ от истинности
Перехват
Навязывание
Вредоносные программы

Характер происхождения угроз:
объективные
субъективные (умышленные, не умышленные)

Источники угроз:
Люди (хакеры, инсайдеры)
Технические устройства
Алгоритмы (схемы) обработки информации
Внешняя среда

Каналы утечки информации (НСД):
Потеря
Чтение с экрана
Кража носителей
ПЭМИН
Соц инженерия

Электро
Физические
Оптические
Информационные

Причины нарушения целостности:
Субъективные:
- **Преднамеренные:**
- Диверсия
- Действия над носителями
- Информационные воздействия
- **Непреднамеренные:**
- Отказы обслуживающего персонала
- Сбои и ошибки людей

Объективные, непреднамеренные:
- Отказы аппаратуры, программ, системы питания
- Сбои, электромагнитная несовместимость
- Стихийные бедствия
- Несчастные случаи

Изменение, фальсификация, уничтожение, потеря, выход из строя, отказ от действий, нарушение транзакций, НСД, заражение

Потенциально возможные злоумышленные действия:

Изучение открытой информации
Выведывание информации (в пределах контролируемой области или вне)
Осмотр мусора
Халатность персонала
Диверсия, физ уничтожение
Дезорганизация (саботаж)

Использование материалов в корыстных целях
Копирование информации с носителей
Кражи, хищение носителей
Удаление, повреждение
Изменение
Снятие информации с памяти устройств

Ввод несанкционированных программных продуктов
Установка закладных устройств

Вторжение (проникновение) в ИС, внедрение агентов
Подслушивание, снятие с акустических каналов
Оптическая разведка, фото- видеосъемка, копирование с устройств отображения
Снятие ПЭМИН, навязывание ПЭМИН
Подключение к ИС по линиям связи, перехват информации, атаки на протоколы,
Криптоанализ

КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ

Задачи и принципы криптографии.
Базовые операции шифрования.
Симметричное шифрование.
Стандарты DES, 3DES, ГОСТ 28174-89
Стандарт AES
Режимы работы алгоритмов шифрования
Асимметричное шифрование. Алгоритм RSA.
Алгоритмы цифровой подписи.
Управление ключами шифрование. Инфраструктура открытых ключей.
Аутентификация. Протоколы аутентификации.

Криптография. Решаемые задачи:

Конфиденциальность - шифрование
Целостность - хеш функция
Аутентификация сообщения (подтверждение источника) — хеш функция
Аутентификация сторон — протоколы аутентификации
Управление ключами и сертификаты открытых ключей

P – открытый текст
$C=E_K(P)$; E_K – функция шифрования, C – зашифрованный текст
$P=D_K(C)=D_K(E_K(P))$ – расшифровка (восстановление) текста; злоумышленник не знает ключ

Требуется исключить расшифровку (сделать максимально трудной

- Алгоритмы шифрования общедоступны, секретны только ключи

(правило Керкгоффа)

Секретность – свойство криптографической системы (протокола) противостоять атакам раскрытия зашифрованной информации.

- атака на основе зашифрованного текста
- атака с известной частью открытого текста
- атака с выбранным открытым текстом (для асимметричных алгоритмов - всегда)

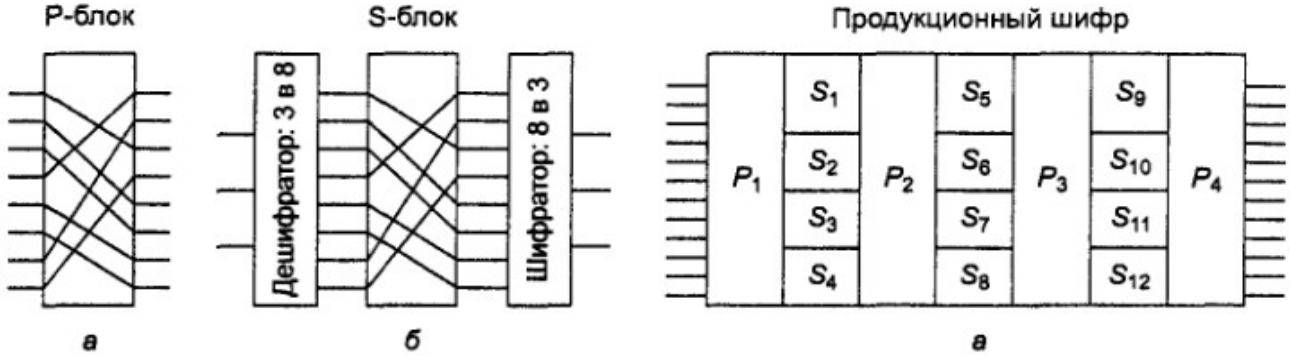
Имитостойкость (imitation resistance)- свойство криптографической системы (криптографического протокола), характеризующее способность противостоять активным атакам со стороны противника и/или нарушителя, целью которых является *навязывание* ложного сообщения, *подмена* передаваемого сообщения или *изменение* хранимых данных.

1. Зашифрованные сообщения должны содержать избыточность (отличать от мусора)
2. Необходим способ борьбы с повторной отправкой ранее посланных сообщений (anty-reply)

Базовые операции шифрования

Подстановка (замена, подстановка, substitution, S-блок) – каждый символ или группа символов заменяется другим символом или группой символов (моноалфавитные подстановки – шифр Цезаря). Сохраняют порядок символов, но изменяют сами символы.

Перестановка (транспозиция, permutation, P-блок) – меняет порядок символов, но не изменяют сами символы



Основные элементы продукционных шифров: P-блок (*а*); S-блок (*б*); продукционный шифр (*в*)

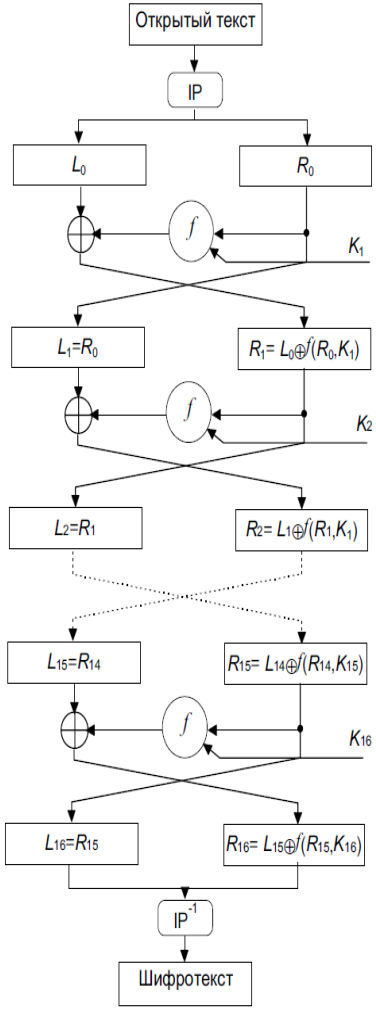
Одноразовый шифрблокнот (гамма, шифр Вернама) – случайная или псевдослучайная последовательность, применяемая для шифрования (гаммирования). Теоретически мощное средство, практически возможно хранение и передача ключа ограниченного размера.

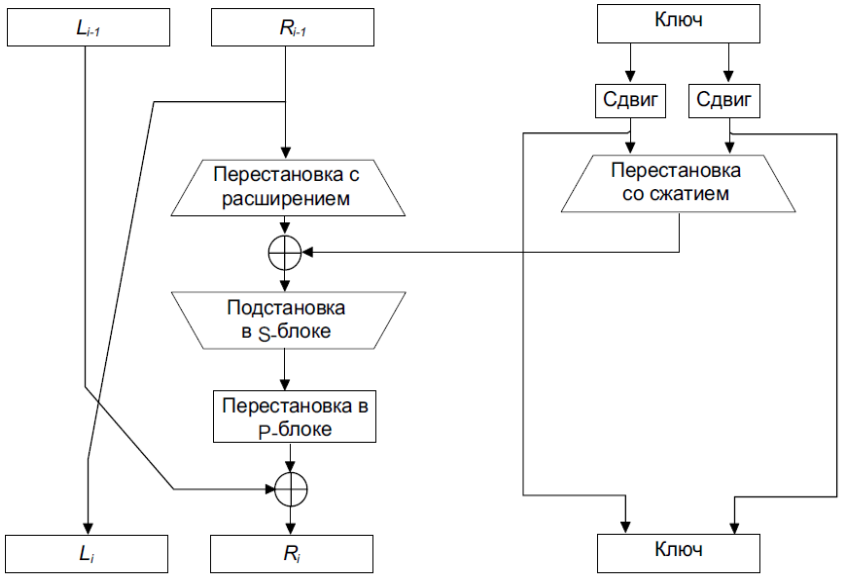
Симметричные и асимметричные алгоритмы шифрования

Поточные и блочные шифры

Стандарт DES (Data Encryption Standard, 1977 г.)

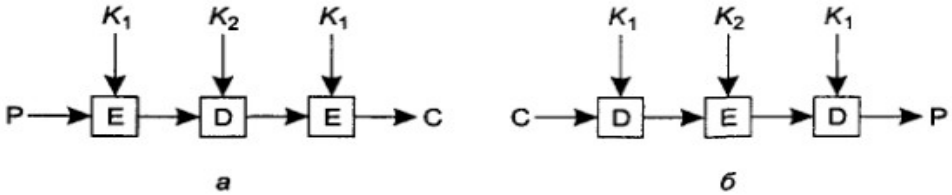
Размер блока – 64 бита (вход – 64 бита, выход – 64 бита). Длина ключа – 56 битов.





Один этап DES.

Тройное шифрование DES (3DES)



Тройное шифрование с помощью DES (*а*); дешифрация (*б*)

В 3DES – 2 ключа и 3 этапа шифрования.
Последовательность операций EDE – для совместимости с обычным DES.

ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»

Блочный шифроалгоритм. При использовании метода шифрования с гаммированием, может выполнять функции поточного шифроалгоритма. В основе, как и в DES, лежит сеть Фейстеля.

Размер блока – 64 бита; Длина ключа – 256 бит; Количество циклов – 32/16
Может использовать различные S-блоки (как дополнительный ключ или как параметр схемы)

Недостатки:
Нельзя определить криптостойкость, не зная таблицы замен (S- блоков).
Могут поставляться преднамеренно слабые таблицы замен.
Несовместимость при использовании разных таблиц замен.

Стандарт AES (основан на алгоритме Rijndael, 2001 г.)
Размер блока 128 бит Длина ключа 128, 192, 256 бит

Простая алгебраическая структура.
В теории конечных полей (Галуа) возможно строго доказать свойства AES.
Используются S и P блоки.
Операции производятся над целыми байтами (эффективность в программной реализации).
Число итераций зависит от размера ключа.
Порог безопасности – минимальное число однотипных итераций (шагов), требуемых для сохранения секретности

Схематичный алгоритм метода Rijndael

```
#define LENGTH 16 /* Число байтов в блоке данных или ключе */
#define NROWS 4 /* Число строк в массиве state */
#define NCOLS 4 /* Число столбцов в массиве state */
#define ROUNDS 10 /* Число итераций: 10, 12, 14 в зависимости от длины ключа*/
typedef unsigned char byte /8-разрядное целое без знака */

rijndael(byte plaintext[LENGTH], byte ciphertext[LENGTH], byte key[LENGTH])
{
int r; /* Счетчик цикла */
byte state[NROWS][NCOLS]; /* Текущее состояние - модифицируемый текст */
struct{byte k[NROWS][NCOLS];}  rk[ROUNDS+1]; / * Ключи итерации */

expand_key(key.rk); /* Сформировать ключи итерации */
copy_plaintext_to_text(state, plaintext); / * Инициализация текущего состояния;*/
xor_roundkey_into_state(state, rk[0]);  / * Сложить по модулю 2 ключ с текущим состоянием*/

for(r=1; r<=ROUNDS; r++) {
substitute(state); /* Пропустить каждый байт через S-блок (подстановка)*/
rotate_rows(state); /* Повернуть строку i на i байт (поворот – сдвиг строк)*/
if(r < ROUNDS) mix_columns(state); /* Смешивающая функция (умножение в поле Галуа)*/
xor_roundkey_into_state(state, rk[r]); /* Сложить по модулю 2 ключ с текущим состоянием */ }
copy_state_to_ciphertext(ciphertext, state); /* Вернуть результат */     }
```

Режимы работы алгоритмов шифрования

Блочное шифрование:

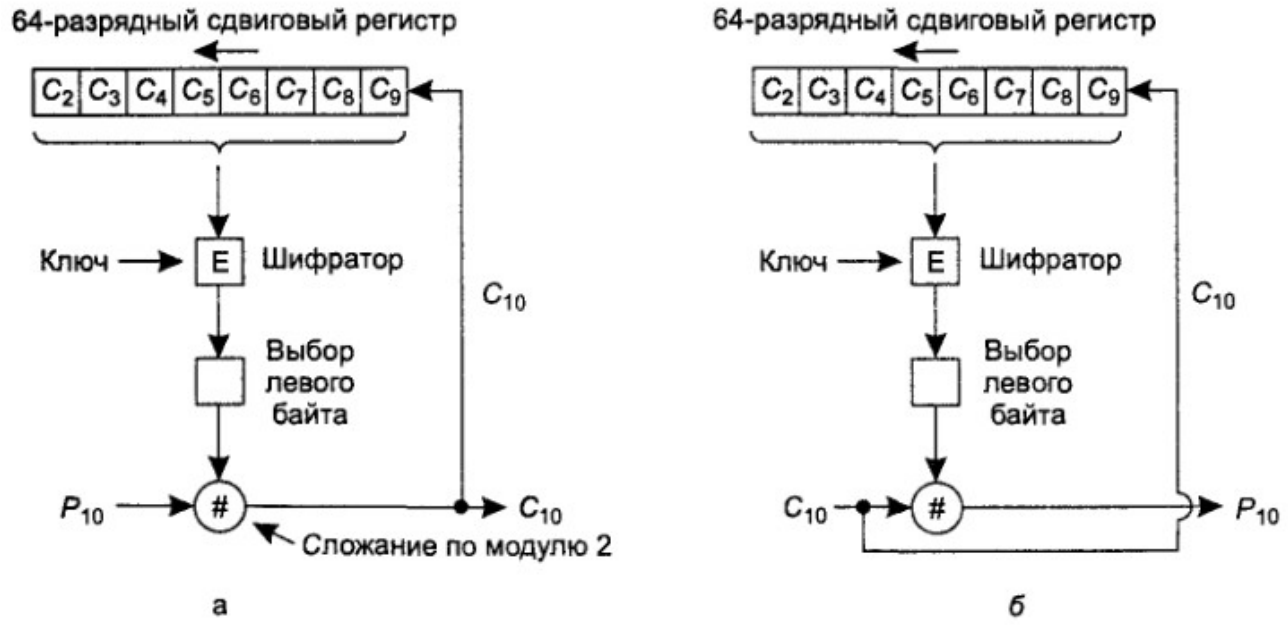
Режим электронного шифроблокнота (или электронной кодовой книги, ECB – Electronic Codebook Mode).

Сцепление блоков шифра (CBC – Cipher Block Chaining)

Сцепление зашифрованных блоков: шифрование (*а*); дешифрация (*б*)

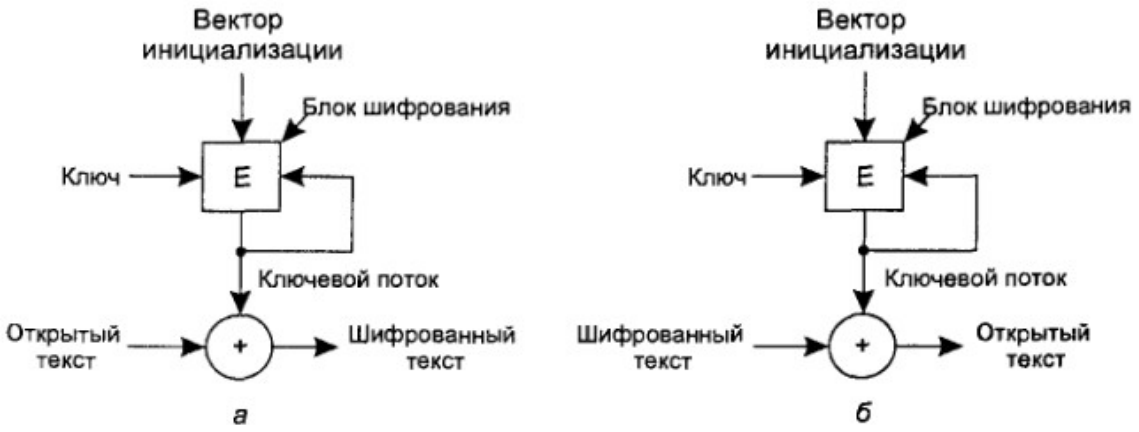
Недостатки: распространение ошибки

Потоковое шифрование:
Р*ежимы шифрованной обратной связи* (или с обратной связью по шифртексту, CFB – Cipher Feedback)



Режим шифрованной обратной связи (*а*); обратная связь по выходу (*б*)

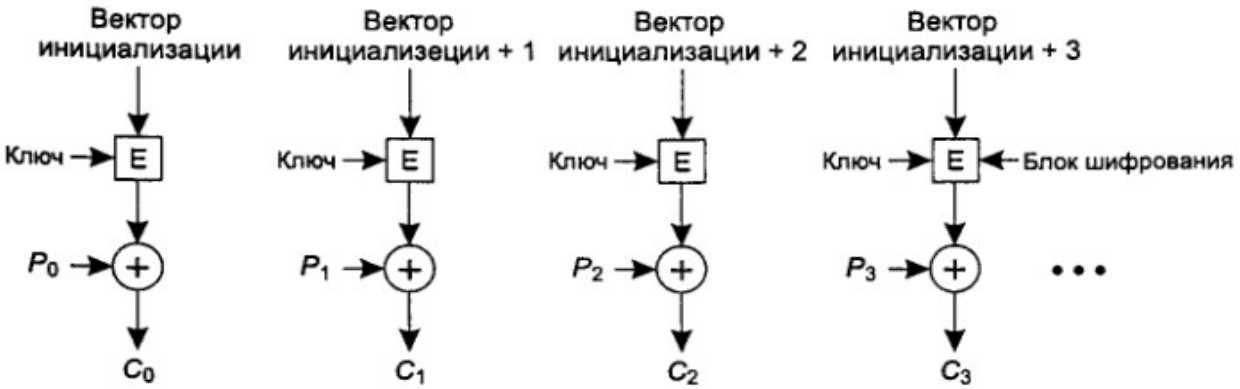
*Режим шифрования с обратной связью по выходу (*OFB – Output Feedback*)*



Групповой шифр: шифрование (*а*); дешифрация (*б*)

Генерация шифрпотока на основе блочного шифра
Ключевые блоки складываются с открытым текстом
Дешифрация – зеркально
Позволяет функционировать кодам с исправлением ошибок
Ключевой поток генерируется независимо от текста

Р*ежим счетчика (*CTR – Counter Mode*)*



Шифрование в режиме счетчика

Режим электронного шифрблокнота – уязвим к атакам замены блоков
Сцепление блоков шифра – должен появиться целый блок
Шифрование с обратной связью – повреждение одного бита влияет на 8 байт
Режим счетчика – доступ к произвольной части текста

Асимметричная криптография (шифрование с открытым ключом)
(передача ключа всегда была слабой стороной криптосистемы)

1976 г., Диффи и Хеллман

- D(E(P))=P
- Сложно вывести D из E (односторонняя функция с секретом)
- E нельзя взломать при помощи произвольного открытого текста

E_A – алгоритм шифрования (открытый ключ)
D_A – алгоритм дешифрации (секретный ключ)

Асимметричные алгоритмы шифрования используют сложность нахождения делителей больших чисел (разложения на простые множители) (RSA) или вычисления дискретных логарифмов (схема Эль-Гамаля, 1985 г., алгоритм DSS) или операции в группах на эллиптических кривых.

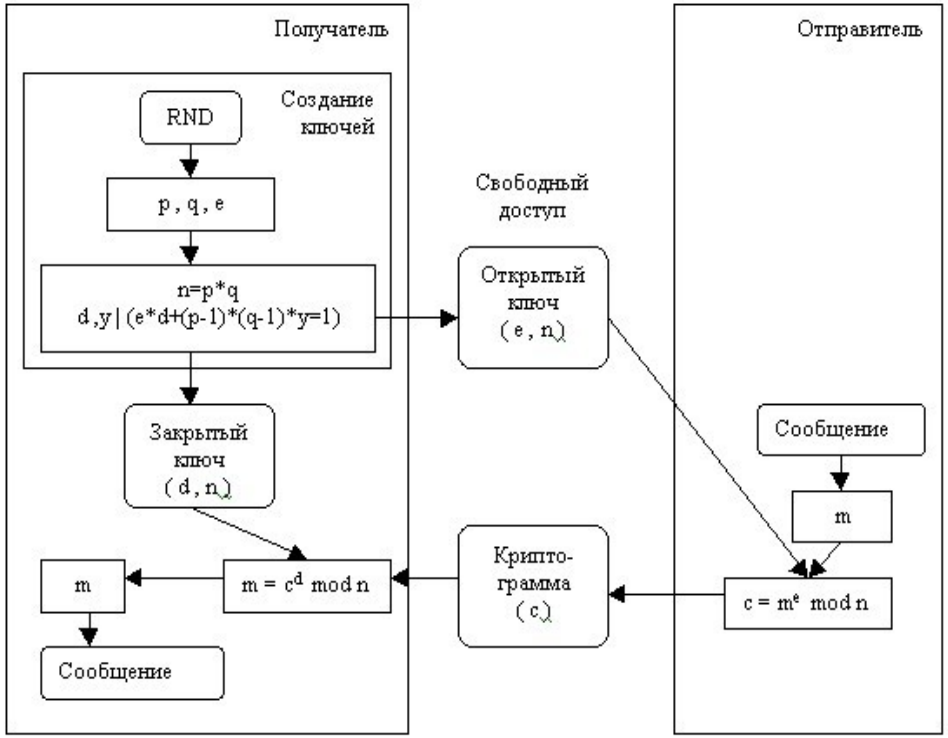
Алгоритм RSA (Rivest, Shamir, Adleman)

1. Выберем два больших простых числа p и q (обычно длиной 1024 бита).
2. Сосчитаем $n=pq$ и $z = (p- 1)(q - 1)$.
3. Выберем число d, являющееся взаимно простым с числом z.
4. Найдем такое число e, что остаток от деления произведения ed на число z равен 1.

P – сообщение; $0 < P < n$
Шифрование: $C = P^e \ (mod\ n)$; открытый ключ - (e, n)
Дешифрование: $P = C^d \ (\text{mod}\ n)$; секретный ключ - (d, n)

*Вскрытие RSA ~ нахождение делителей числа
* При эквивалентной секретности ключи асимметричных алгоритмов значительно длинее ключей симметричных алгоритмов, а вычисления на несколько порядков дольше.

Алгоритм RSA

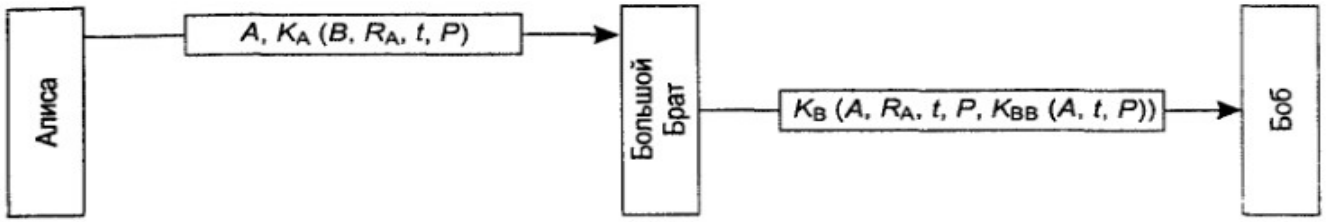


*Не делайте ***n*** общим для группы пользователей.
*Безопасней подписывать ЭЦП хеш сообщения, а не само сообщение.
*Дополняйте сообщения случайными числами.

Цифровые подписи

Функции сообщений:

- подтверждение подлинности сообщения
- получатель мог проверить объявленную личность отправителя (автора);
- отправитель не мог позднее отрицать содержимое сообщения;
- получатель не мог позднее изменить подписанное сообщение.

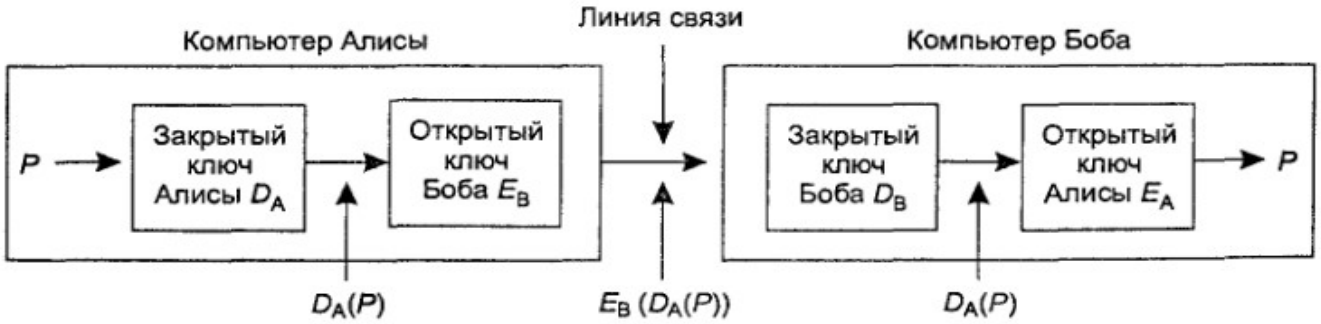


Цифровая подпись Большого Брата

Каждый абонент сам выбирает свой ключ и заносит в удостоверяющий орган.
Все абоненты должны доверять удостоверяющему органу.
R_A – случайное число; t – временная метка; P – текст сообщения; B – адресат
K_A – текст сообщения, зашифрованный ключом A
Случаное число и временная метка – защита от атак воспроизведения (повтора)
Сообщение передается в открытом виде.

Подписи с открытым ключом

Необходимо D(E(P))=P и E(D(P))=P
Для цифровой подписи можно использовать любой алгоритм шифрования с открытым ключом
Существуют специальные алгоритмы только для цифровой подписи, напр. DSS (схема Эль- Гамаля)



Цифровая подпись, полученная при помощи шифрования с открытым ключом

А знает секретный ключ D_A и открытый ключ E_B
Система сохраняет секретность, пока секретен D_A. Проблема смены ключа.

Профили сообщений

(требуется только аутентификация сообщения, но не требуется шифрование всего сообщения – неприкосновенность сообщения без секретности)

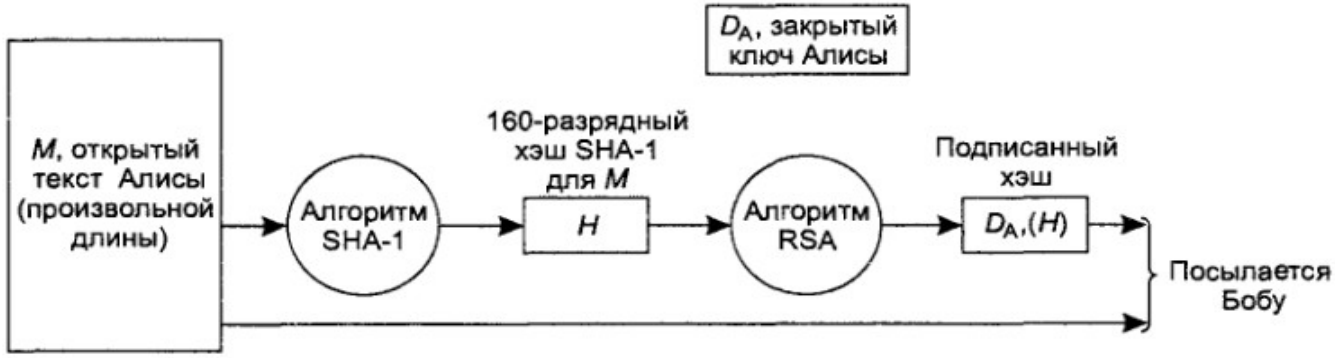
Профили сообщений основаны на односторонней (необратимой, криптографической, безопасной) хеш-функции (профиль сообщения, message digest, MD).
Вход – участок текста произвольной длины, выход – строка битов фиксированной длины.

Чтобы хеш-функция была криптостойкой, должно выполняться:

- По заданному открытому тексту *P* легко сосчитать значение хэш-функции *MD(P).*
- Изменение даже одного бита входной последовательности приводит к очень не похожему результату (лавинный эффект).
- По цифровой подписи *MD(P)* практически невозможно определить значение открытого текста *P.*
- Для данного *P* практически невозможно подобрать такой *P',* чтобы выполнялось равенство *MD(P') = MD(P)* (стойкость к коллизиям первого рода).
- Практически невозможно найти пару (P, P'), что *MD(P') = MD(P)* (стойкость к коллизиям второго рода).

Цифровая подпись с использованием профиля сообщения

MD5 (Rivest, 1992) – 128 битный профиль сообщения
SHA-1(NIST, 1993) - 160 битный профиль сообщения
Размер входного блока в MD5 и SHA-1 – 512 бит.



Применение SHA-1 и RSA для создания подписей несекретных сообщений

(Боб тоже вычисляет хеш сообщения и прверяет его идентичность)

ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Електронний цифровий підпис, що грунтується на еліптичних кривих"

Т.о. криптография с открытым ключом позволяет передавать данные, проверять целостность и аутентичность сообщений, создавать ЭЦП , не обладая общим ключом и без участия 3-й стороны.

Проблема начального обмена ключами не решается в рамках криптосистемы!!!
(если выложит ключ на сайте и т.п. – возможна атака «человек посередине»)

Управление ключами

Центр распределения ключей – выдает сертификаты, удостоверяющие открытые ключи субъектов.
Единый центр - не масштабируется, единая точка уязвимости (ключ центра) и отказа.

Управление сертификации (CA - Certification Authority)

Настоящим удостоверяю, что открытый ключ 1SWV35CNK5VD67ER7EWV5SEKJNVCEP…..WK8WFB1FWD принадлежит Пупкину Ивану Иванычу Какая-то там улица 32 Цурюпинск, 21541 1967 род. 30 февраля Электронный адрес: pupkin@no.domain.com
Хэш SHA-1 данного сертификата подписан закрытым ключом Управления сертификации

Сертификат открытого ключа связывает открытый ключ субъекта-принципала (пользователя, сайта, процесса…) и его атрибуты.
Сертификат не секретен. Злоумышленник не может подделать ЦП Управления сертификации.

Формат сертификата X.509

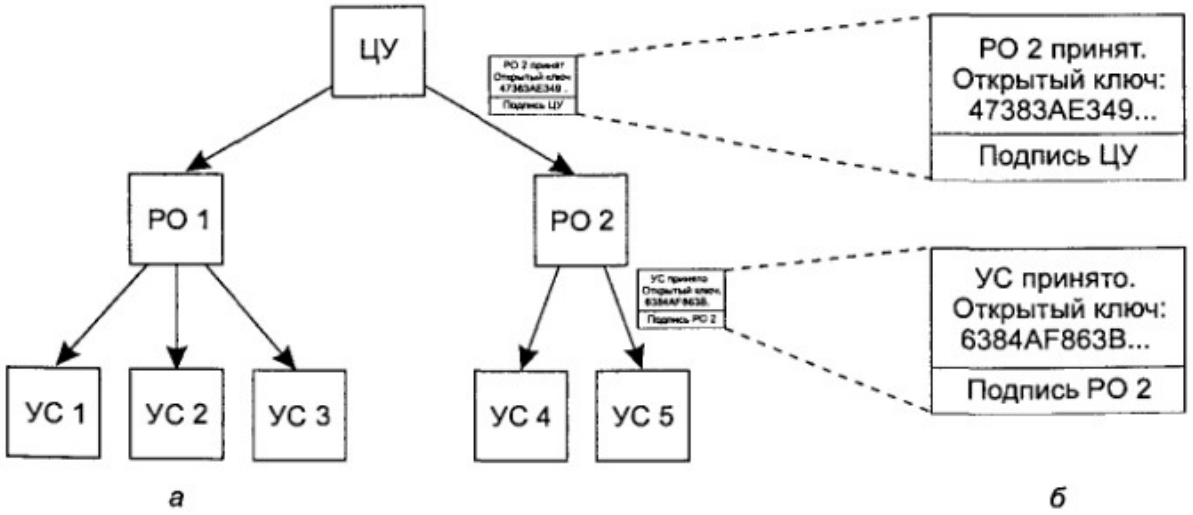
Поле	**Значение**
Version	Версия X.509 (актуальная версия – 3)
Serial number	Это число и название Управления сертификации однозначно идентифицирует сертификат
Signature algorithm	Алгоритм генерации подписи сертификата
Issuer	X.500-имя Управления
Validity period	Начало и конец периода годности
Subject name	Сущность, ключ которой сертифицируется
Public key	Открытый ключ сущности и идентификатор использующего его алгоритма
Issuer ID	Необязательный идентификатор, единственным образом определяющий эмитента (создателя) сертификата
Subject ID	Необязательный идентификатор, единственным образом определяющий владельца сертификата
Extensions	Различные возможные расширения
Signature	Подпись сертификата (генерируется с помощью закрытого ключа Управления сертификации

X.509 – стандарт сертификатов

X.500 – стандарт иерархического именования ресурсов

PKI (Public Key Infrastructure) – инфраструктура открытых ключей

Единое всемирное управление сертификации не выдержало бы нагрузки и стало бы корнем всех проблем. Если использовать ряд идентичных управлений – усиливается проблема утечки ключей.
Альтернатива единому управлению сертификации – инфраструктура открытых ключей.



Иерархия PKI (*а*); цепочка сертификатов (*б*)

В примере показано 3 уровня иерархии центров сертификации. Корневой сервер легализирует (заверяет) сертификаты серверов следующего уровня. Считаем, что ключ ЦУ знают все (например, этот ключ зашит в Интернет – браузере).
Сервера сертификации могут заверять сертификаты субъектов или серверов следующего уровня.

Для открытия *безопасного сеанса* с неким субъектом В необходимо:
1. Получить ключ В, подписанный некоторым УС
2. Запросить сертификат УС, подписанный некоторым РО
3. Пользуясь сертификатом ЦУ, проверить подпись РО.

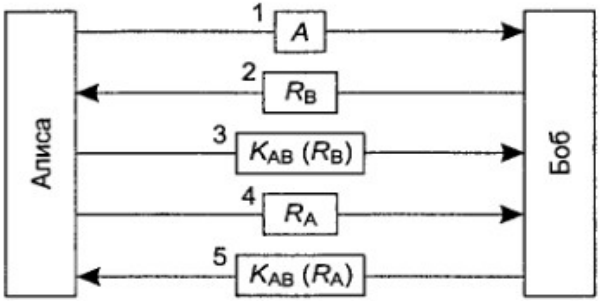
Другой вариант – субъект при открытии сеанса сам предоставляет цепочку удостоверяющих сертификатов.

Проблема аннулирования сертификатов до окончания срока годности.
CRL (Certificate Revocation List – список отозванных сертификатов) – предоставляется и регулярно обновляется корневым сервером.
Проблема восстановления сертификатов.

Хранить сертификаты удобней всего в иерархических каталогах (DNS, LDAP).

Аутентификация - метод, с помощью которого субъект (процесс) удостоверяется в том, что его собеседник является именно тем, за кого он себя выдает.
Аутентификация – проверка подлинности. Авторизация – разрешение на некоторые действия.
Обычно – двусторонняя (взаимная) аутентификация. В процессе аутентификации обычно устанавливается *ключ сеанса* (временный ключ) – основные секретные или открытые ключи используются минимальное число раз.

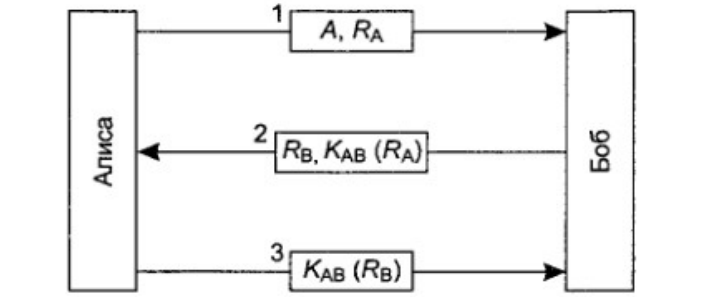
Аутентификация, основанная на общем секретном ключе



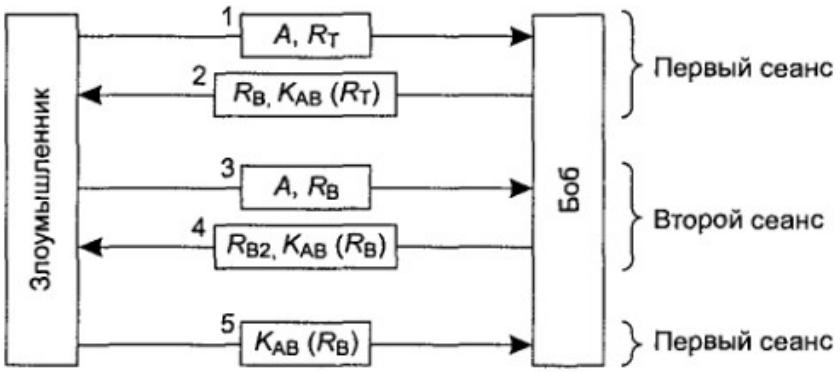
Двусторонняя аутентификация при помощи протокола оклик—отзыв

Пусть у А и В общий ключ шифрования K_{AB} (не передается по сети, злоумышленник не знает ключ). R_B, R_A – «оклик» - случайное число. Маловероятно, что R_A, R_B ранее встречались злоумышленнику. После аутентификации А и В устанавливают ключ сеанса.

Зеркальная атака



Укороченный двусторонний протокол аутентификации



Зеркальная атака

Если сократить число шагов в протоколе до 3-х, то злоумышленник может открыть несколько сеансов и повторить оклик B, в результате заполучив правильное значение K_{AB}.

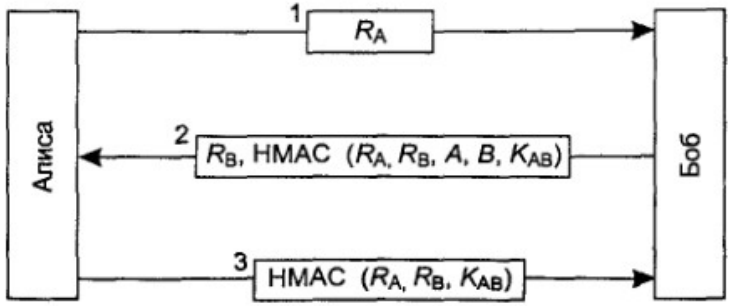
Четыре общих правила, которым должны удовлетворять протоколы аутентификации:

1. Инициатор сеанса должен подтверждать свою личность прежде, чем это сделает отвечающая сторона. В этом случае злоумышленник не сможет получить ценной для него информации, прежде чем подтвердит свою личность (предоставлять как можно меньше информации для возможного анализа).
2. Следует использовать два отличающихся общих секретных ключа: один для инициатора сеанса, а другой для отвечающего, Kab и Kab'.
3. Инициатор и отвечающий должны выбирать оклики из различных непересекающихся наборов. Например, инициатор должен пользоваться четными номерами, а отвечающий - нечетными.
4. Протокол должен уметь противостоять атакам, при которых запускается второй параллельный сеанс, информация для которого извлекается при помощи первого сеанса.

Если нарушается хотя бы одно из этих правил, протокол оказывается уязвимым. На этих правилах основаны методики построения и доказательства корректности протоколов аутентификации.

Протокол аутентификации, использующий функцию HMAC

HMAC (Hashed Message Authentication Code) – безопасная (криптографическая) хеш-функция.



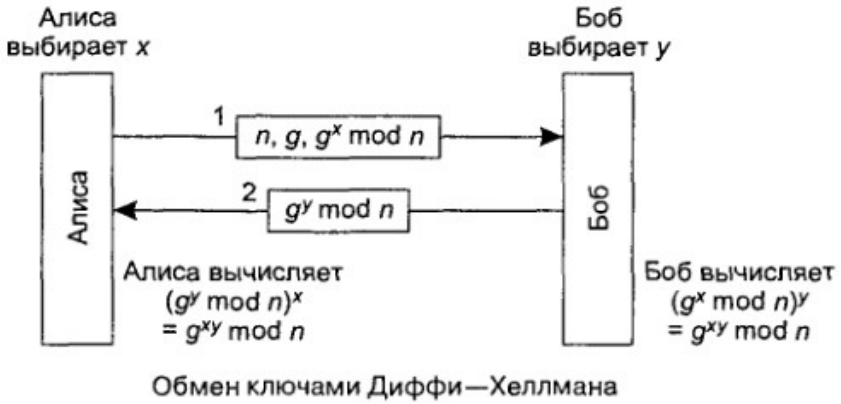
Аутентификация с применением HMAC

R_A – временная отметка, K_{AB} – общий секретный ключ.

Злоумышленник не знает ключ K_{AB} и не может угадать HMAC и также не может заставить любую сторону шифровать выбранное сообщение или применять HMAC.

Оба HMAC содержать значения, выбранные отправителем.

Протокол Диффи-Хеллмана
(протокол выработки общего секретного ключа по открытым каналам)

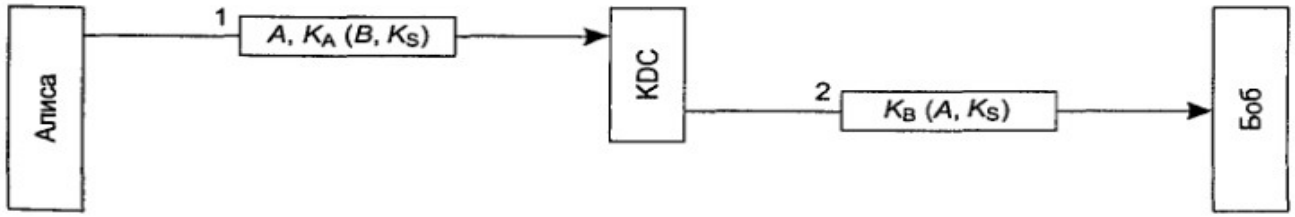


Обмен ключами Диффи—Хеллмана

A и B договариваются о двух простых числах n и g; $(n-1)/2$ – тоже простое
Каждая из сторон выбирает 512-битное число (x и y)
A посылает (n, g, $g^X mod\ n$), B отвечает ($g^Y\ mod\ n$)
Обе стороны вычисляют $g^{XY} mod\ n$ – общий секретный ключ
В результате почти удалось найти общий ключ (протокол не устойчив к атаке «человек посередине»

Сложность обратимости алгоритма сводится к задаче вычисления дискретного логарифма большого простого числа.

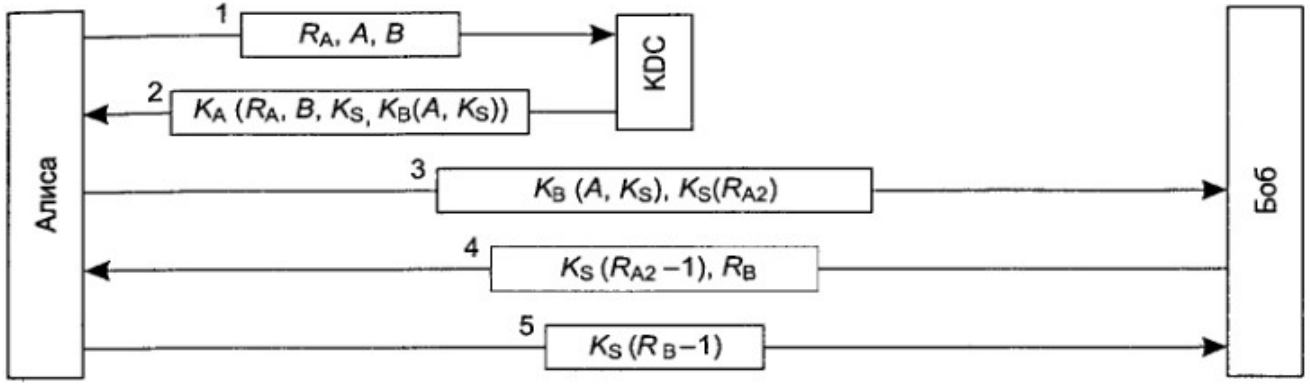
Если организовать центр распространения ключей (KDC – Key Distribution Center) – у каждого пользователя должен быть один ключ, общий с KDC.



Первая попытка протокола аутентификации с помощью KDC-центра

K_A, K_B – ключи субъектов; K_S – ключ сеанса.
Протокол не защищен от атаки повтором.
Если ввести в сообщения временной штамп, то возникает проблема синхронизации часов и у сообщений будет срок годности, в течение которого сообщение можно отослать повторно.
Если ввести в сообщения нонс (порядковый номер, «nonce» - данное время), то стороны должны помнить предыдущие нонсы вечно (иначе появляется возможность атаки повтором) – это усложняет протокол.
Вместо этого в протоколе Нидхема-Шредера используется многосторонний оклик – отзыв.

Протокол аутентификации Нидхема – Шредера (протокол взаимной аутентификации)



Протокол аутентификации Нидхэма—Шрёдера

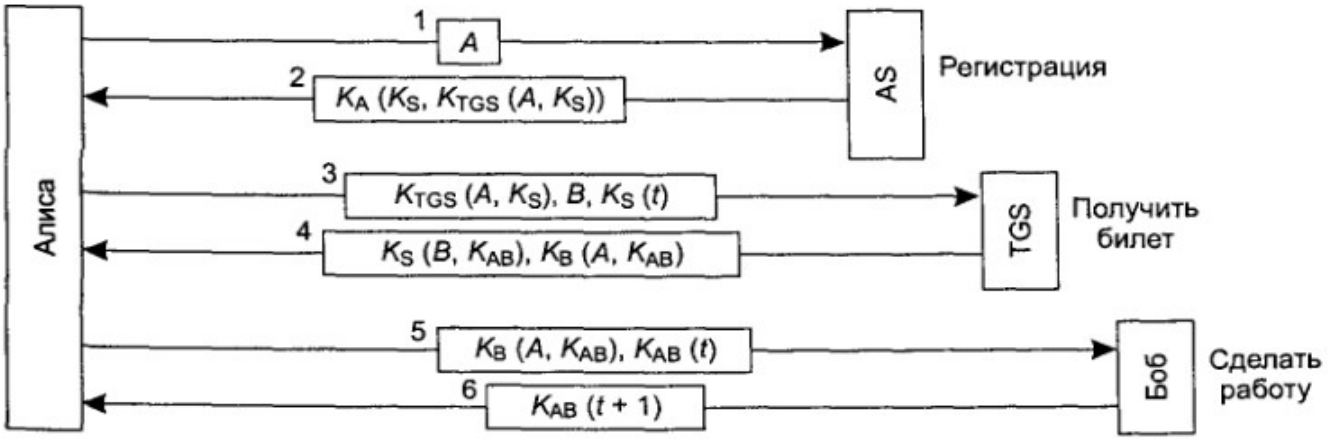
K_S – ключ сеанса; $K_B(A, K_S)$ – билет для B, зашифрованный ключом B.
R_A – случайное число, чтобы убедить A, что сообщение 2 свежее.
Задача Шага 4 – доказать, что B – настоящий.
Задача Шага 5 – убедить B, что он разговаривает с A.

Защита от атак воспроизведения:

1. Временной штамп t — проблема синхронизации и срок годности в течение которого возможно повторить
2. Нонс (или порядковый номер) — должен помниться вечно (усложняет протокол)

Протокол аутентификации Керберос

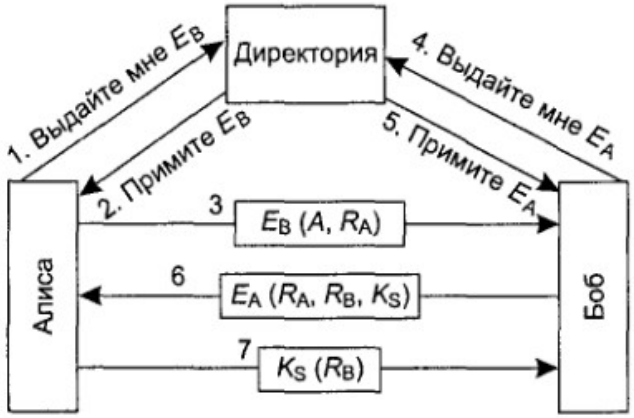
Основан на протоколе Нидхема – Шредера. Использует предположение о синхронизации часов.



Работа протокола Kerberos V4

AS – сервер аутентификации; TGS (Ticket Granting Server) – сервер выдачи билетов.
Используется временной штамп t.
1. Запрос регистрации
2. $K_{tgs}(A, K_S)$ – билет для TGS.
После шага 2 A на основе пароля формирует ключ K_A и пароль уничтожается.
3. Запрос выдачи билета для сеанса с B. $K_{tgs}(A, K_S)$ подтверждает отправителя.
4. TGS выдает A K_{AB} – ключ для сеанса A-B (одна копия зашифрована для A, другая – для B).
B получает ключ сеанса K_{AB}
B подтверждает свою подлинность.
Права доступа для A определяет B.
Для открытия нового сеанса с некоторым сервером C снова обратиться к TGS для выдачи билета.
Пароли по сети не передаются.

Взаимная аутентификация с помощью шифрования с открытым ключом



Взаимная идентификация с помощью открытого ключа

1. Запрос открытого ключа B в PKI (PKI использует, например, структуру серверов LDAP).
2. Получить открытый ключ B.
3. Запрос на установление сеанса с B. Содержит имя A и случайное R_A, зашифрованные ключом B
4. B запрашивает сервер каталогов выдать ключ A
5. Сервер каталоговы выдает ключ A
6. A расшифровывает сообщение и видит свое R_A (подтверждает подлинность B и свежесть сообщения). B формирует ключ сеанса A-B.
7. A проверяет R_A и соглашается на сеанс, посылает метку R_B (сформированную B), зашифрованную ключом сеанса (ключ сеанса сформировал B).

Сфабриковать сообщение 3 мешает R_A.
Сфабриковать сообщение 7 мешает R_B и K_S (нельзя получить не зная секретного ключа A).

Вопросы по теме:

Что такое криптографическое преобразование.
Задача криптографии, криптологии и криптоанализа.
Принцип Керкгоффа.
Основные принципы криптографии.
Что такое имитостойкость шифрования.
Виды атак на криптографические алгоритмы.
Направления криптоанализа.

Базовые операции шифрования.
Операции подстановки и перестановки.
Как выразить операцию подстановки через перестановку.
Метод гаммирования. Что такое «совершенная безопасность»
Что такое одноразовый шифрблокнот. Его свойство.
Отличия симметричных и асимметричных алгоритмов шифрования.
Отличия поточного и блочного шифра.

Стандарт DES. Размер блока и длина ключа.
Какие преобразования использует алгоритм DES.
Что понимается под «лавинным эффектом» в криптопреобразованиях.
Что такое S-блоки. Принципы выбора S-блоков в алгоритме DES.
Какие методы криптоанализа могут использоваться для ускорения вскрытия алгоритма DES.
Какие факторы могут ослабить секретность алгоритма DES.
Модификации алгоритма DES.
Стандарт AES. Размер блока и длина ключа.
Какие основные преобразования использует алгоритм AES.
Какой математический аппарат доказывает свойства алгоритма AES.
От чего зависит число итераций в алгоритме AES.
Что такое порог секретности криптоалгоритма.

Режимы работы алгоритмов шифрования и их особенности.

Свойства асимметричных алгоритмов шифрования.
Что такое односторонняя функция.
Какие математические проблемы лежат в основе сложности обращения асимметричных криптографических алгоритмов.
Алгоритм RSA. Описание работы.

Что такое цифровая подпись. Свойства Ц.П.
Цифровая подпись с открытым ключом. Схема применения.
Что такое профиль сообщения. Его свойства. Примеры.
Что такое цифровой сертификат. Какие параметры он содержит.
Для чего используется инфраструктура открытых ключей.
Принцип делегирования и проверки сертификатов.
Для чего используются «цепочки сертификатов».

Что такое аутентификация. Известные алгоритмы аутентификации.
Пример алгоритма аутентификации.
Правила, которым должны удовлетворять протоколы аутентификации.
Известные протоколы аутентификации.
Протокол аутентификации Керберос.
Протокол аутентификации Диффи- Хеллмана.
Алгоритм аутентификации с использованием шифрования с открытым ключом.

Влияние теории информации на криптографию и криптоанализ.
Что такое энтропия, избыточность и расстояние уникальности. Их свойства.

Свойства алгебраических групп и полей. Примеры групп и полей.
Свойства группы вычетов. Свойства полей Галуа.
Классы сложности математических проблем и алгоритмов.

Что такое стеганография. Методы стеганографии.

Литература:

1. Дориченко С.А., Ященко В.В. 25 этюдов о шифрах. – М.: ТЕИС, 1994 – 69 с.
2. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. М.: КУДИЦ-ОБРАЗ, 2001 – 368 с.
3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. - М.: Триумф, 2002. — 816 с. ISBN 5-89392-055-4

Принципы и протоколы идентификации и аутентификации

Идентификация - именование и распознавание субъектов

Аутентификация - процедура проверки подлинности субъектов
Надежность идентификации обеспечивается уникальностью используемых признаков. Надежность аутентификации обеспечивается трудностью их подделки.

Авторизация - предоставление субъекту ресурсов и полномочий (определение сферы действия и доступные ресурсы)

Подтверждение подлинности субъекта:
-знает что-то (пароль (PIN - код), ключ, ...)
-обладает чем-то (магнитная карта, смарт- карта, устройство...)
-является (неотъемлемые биометрические характеристики)

Способы аутентификации:
-Пароль (PIN, разделяемая информация) - простая аутентификация
-Одноразовый пароль (OTP)
-Протокол Запрос-Ответ
-Цифровая подпись, Сертификат открытого ключа

Одноразовые (динамические) пароли:
-Список паролей
-Функция генерации последовательности паролей (Псевдослучайные числа)
-Пароли, зависящие от функции времени (номера последовательности)
-Аппаратные устройства (черный ящик)

Протокол - набор правил, описывающих процедуру обмена

Атаки на протоколы аутентификации:
-Подмена субъекта
-Воспроизведение (повтор, reply)
-Зеркальная атака
-Человек посередине (двойная игра)

Предотвращение атак воспроизведения - механизм Запрос-Ответ с неповторяющимся элементом:
-"Метка времени" (например, постоянно возрастающая функция)
-Случайное число (не допускать повторения СЧ в рамках *сеанса*)
*Проблема синхронизации времени

Строгая аутентификация - доказывающая сторона демонстрирует знание секрета но сам секрет в ходе обмена не разглашается.
-Односторонняя хеш-функция (дайджест) со случайным числом
-Владение секретным ключом (цифровая подпись с секретным ключом)

Двусторонняя (взаимная) аутентификация - обе стороны обмена аутентифицирют друг-друга

Трехсторонняя аутентификация - аутентификация с привлечением третьей стороны (удостоверяющего центра, сервера аутентификации, сервера выдачи ключей, центра сертификатов...)

Протоколы строгой аутентификации используют:
-симметричные алгоритмы шифрования
-однонаправленные хеш-функции
-асимметричные алгоритмы шифрования
-алгоритмы цифровой подписи (ЭЦП)

Протоколы аутентификации:

-PAP - простая аутентификация, пароль передается в открытом виде
-CHAP – протокол запрос - ответ
-S/Key – система одноразовых паролей
-TACACS(+), **RADIUS** – протоколы аутентификации NAC
-EAP – расширяемый протокол аутентификации

-**Kerberos** – протокол аутентификации в службе Active Directory
-**IKE** (Internet Key Exchange) – протокол аутентификации сторон и выработки общего секретного ключа в архитектуре IPSecurity

Системы однократной регистрации:
-Active Directory
-Novell Directory
-NIS
-IBM Tivolly Identity Manager

Биометрическая аутентификация

-достоверность и трудность фальсификации
-неотделимость от субъекта

Способы биометрической аутентификации:
-Дактилоскопия (отпечатки пальцев)
-Геометрическая форма ладони
-Форма и размеры лица, Инфракрасная карта лица
-Особенности голоса (высота, модуляция и частота звука)
-Характеристики радужной оболочки и сетчатки глаза
-Клавиатурный почерк

Ошибки систем идентификации с распознаванием образов:
-Коэффициент ошибочных отказов
-Коэффициент ошибочных подтверждений

Радиочастотная идентификация (аутентификация) - RFID

Вопросы:

Задача идентификации, аутентификации, авторизации
Способы аутентификации
Атаки на протоколы аутентификации
Способы предотвращения атаки воспроизведения
Что такое строгая аутентификация, взаимная аутентификация, косвенная аутентификация

Литература:

Смит Р. Аутентификация: от паролей до открытых ключей.: М. : Изд. дом "Вильямс". 2002. - 432 с.
Дшхунян В.Л., Шаньгин В.Ф. Электронная идентификация. Бесконтактные электронные идентификаторы и смарт - карты. - М.: ООО "Издательство АСТ": Издательство "НТ Пресс", 2004. - 695 с.

Дополнения к криптографии

Специфические криптографические протоколы

1. Протоколы битовых обязательств – позволяют абоненту спрятать переданное значение и открыт его после (примитив для разработки криптографических протоколов).

Абонент А, подбрасывающий монету, не может изменить результат после получения догадки от абонента В, угадывающего этот результат
(создать случайную последовательность, не обращаясь за помощью к третьей стороне)

Безопасность протокола обеспечена односторонней функцией.

→Бросание жребия (монеты) по телефону
→ Ментальный покер

2. Интерактивное доказательство с нулевым разглашением (наименьшим раскрытием)

В результате работы протокола один абонент может доказать другому абоненту что он владеет некторой секретной информацией, не разглашая ее сути.

Может использоваться для построения протоколов аутентификации и цифровой подписи.

3. Безопасные выборы
Решают проблему неотслеживаемости действий клентов

Конфиденциальность+Достоверность

- Гарантия, что только законные избиратели могут подать голос
- Невозможность в ходе голосования узнать выбор того или иного пользователя
- Право каждого избирателя – убедиться, что его голос правильно учтен

4. Совместная подпись контракта

Предотвращает мошенничество участников, связанное с отказом от контракта.
Схема с арбитром или без арбитра

Групповая подпись

- Только члены группы могут подписывать сообщения
- Получатель может убедиться, что это правильная подпись группы
- Получатель подписи не может определить, кто именно из членов группы подписал документ
- При споре подпись будет раскрыта для определения личности подписавшего

Проблема безопасности протокола – необходим надежный посредник, который знает закрытые ключи каждого из участников и имеет возможность подделывать подписи.

Доверенная подпись (делегировать полномочия подписания документа другому человеку)

- Различимость
- Неподделываемость
- Неотрицаемость

Протоколы существуют только в теоретическом плане

Неоспариваемая подпись

Не может быть проверена без разрешения подписавшей стороны
(Зависит от подписанного документа и закрытого ключа субъекта)

Слепая подпись

Нотариальное засвидетельствование в определенное время.

5. Удостоверяющая почта — получатель не может узнать абсолютно ничего о содержании сообщения до тех пор, пока отправитель не получит сообщение о его получении.

6. Забывающая (рассеянная) передача

Участник A после передачи некоторого секрета участнику B не знает, передал ли он секрет, но участник B точно знает, получил он секрет или не получил.

7. Разделение секрета

Расчленение секрета между участниками и коллективное использование его в последствии для восстановления исходного секрета

Схема с арбитром
Проблема: если одна из частей пропадет – без арбитра секрет будет утерян.

8. Неотслеживаемые электронные деньги

КВАНТОВАЯ КРИПТОГРАФИЯ

Свойства фотонов:

- Отсутствуют методы клонирования фотонов

- Фотон, проходя через поляризационный фильтр, перевернутый на 45° относительно его поляризации, с равной вероятностью может попасть на направление 0 или 1

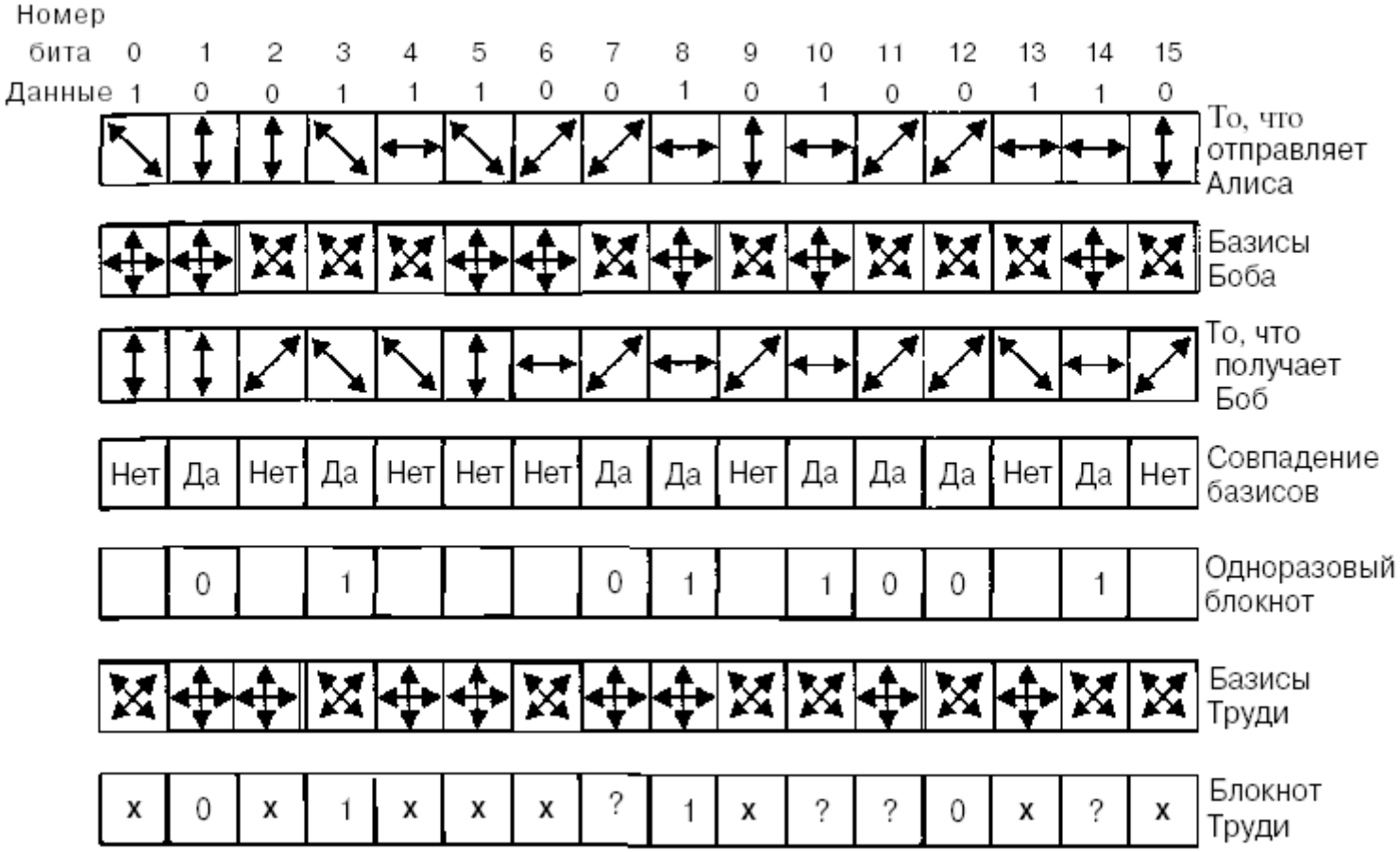
Метод обмена секретным ключом (одноразовой последовательностью)

Выбирается 2 базиса (набора фильтров): прямолинейный и диагональный

1. Алиса генерирует одноразовый блокнот (случайную последовательность)
   Для каждого передаваемого бита случайно выбирается базис и генерируется фотон с требуемой поляризацией.

2. Боб также случайно выбирает базис. Фотон проходит через набор фильтров.
   Базис выбран правильно – правильный бит
   Базис выбран не правильно – случайный бит

3. Боб сообщает Алисе выбранные базисы, Алиса сообщает, какие из них выбраны правильно.
   Биты, переданные и принятые с одинаковым базисом – шифрпоследовательность (~50% начальной последовательности)



4. Труди также выбирает базис случайно и поэтому знает ~50% шифрпоследовательности. Для «усиления секретности» - хеш-функция.
5. Труди передает квантобиты с использованием поляризации, с которой они были приняты -> множество ошибок в блокноте Боба.

Вопросы по теме:

Свойства фотонов.
Операции над фотонами.
Какую поляризацию будет иметь фотон, пройдя через поляризационный фильтр.
Схема квантового обмена ключами.
Применение свойств фотонов в квантовой криптографии.
По каким признакам распознается атака «человек посередине» при квантовом обмене ключами.

Литература:

Брассар Ж. Современная криптология. – М.: Издательско – полиграфическая фирма ПОЛИМЕД, 1999 – 176 с.

СТЕГАНОГРАФИЯ

ВИДЫ СТЕГАНОГРАММ

Лингвистические стеганограммы

Условное письмо:

- Жаргонный код
- Пустышечный шифр (значимы лишь некоторые слова)
- Геометрическая система (в том числе в файлах)

Семаграмма – способ скрыть информацию с помощью знаков или символов (шифрообозначениями являются любые символы, кроме букв и цифр - заглавные буквы, подчеркивания, особенности почерка, пробелы между буквами и словами...).
Малый объем передаваемой информации.

Технические стеганограммы

Микроточки

Невидимые чернила :

- Органические (молочай, крохмал, пирамидон; молоко, моча, уксус, фруктовые соки проявляются при нагревании).
- Симпатические (химические растворы, бесцветные после высыхания, но образующие видимое соединение после обработки другим химикалием — реагентом). Например, железный купорос + цианит калия.

Способы выявления: инфракрасный, ультрафиолетовый или поляризованный свет.