Реализация криптографических алгоритмов в ИС

Лекция 1
Введение в криптографию. Основные нормативные и законодательные документы

Содержание лекции

1. **Введение в криптографию**
2. **Основные нормативные и законодательные документы (законы в области защиты информации)**
3. **Правовые основы информационной безопасности**

Лекция 1
Введение в криптографию. Основные нормативные и законодательные документы

1. Введение в криптографию

1. Введение в криптографию

Криптография (от греч. *kryptós* «тайный» и *gráphō* – «пишу») –это наука о методах обеспечения конфиденциальности, целостности и аутентичности информации. Если проще, это искусство создания и взлома шифров.

Криптография работает с двумя основными понятиями:

Шифрование (encryption) — детерминированный процесс преобразования открытого текста в шифртекст с использованием ключа и криптографического алгоритма.

Расшифрование (decryption) — обратный процесс преобразования шифртекста в открытый текст.

1. Введение в криптографию

Основные задачи **криптографии**:

- **Конфиденциальность (Confidentiality)** — обеспечение доступа к информации только авторизованным субъектам.
- **Целостность (Integrity)** — гарантия точности и полноты информации, защита от несанкционированного изменения.
- **Аутентичность (Authenticity)** — подтверждение подлинности источника информации и идентификация участников взаимодействия.
- **Неотрекаемость (Non-repudiation)** — невозможность для стороны отказаться от совершенных ею действий (например, от подписания документа).

1. Введение в криптографию

Криптоанализ — наука, изучающая методы вскрытия шифров без знания ключей.

Симбиоз криптографии и криптоанализа образует более общую дисциплину — **криптологию**.

1. Введение в криптографию
Исторический экскурс: эволюция криптографических парадигм

Историю криптографии принято разделять на два кардинально отличающихся периода:

1. **Классический (докомпьютерный) период (до XX века)**
2. **Современный период: криптография с секретным и открытым ключом**

1. Введение в криптографию
Исторический экскурс: эволюция криптографических парадигм

Классический (докомпьютерный) период (до XX века):

- **Античность:** Спарта — шифр перестановки, шифр Цезаря (Рим) — шифр замены, где каждая буква сдвигалась на фиксированное число позиций в алфавите.
- **Средневековье:** Более сложные моноалфавитные и полиалфавитные шифры. Яркий пример — диск Альберти (XV век), который реализовал первый полиалфавитный шифр.
- **XIX-XX век:** Механические и электромеханические устройства. Легендарная немецкая шифровальная машина «Энигма» времен Второй мировой войны, *взлом которой силами союзников (с участием Алана Тьюринга) значительно повлиял на исход войны.*

2. Современный период:

Начало современной эпохе положила публикация работы Уитфилда Диффи и Мартина Хеллмана «New Directions in Cryptography» (1976). Ими была предложена концепция асимметричной криптографии (криптографии с открытым ключом).

- Вся классическая криптография была симметричной: один и тот же ключ использовался и для шифрования, и для расшифрования. Проблема — как безопасно передать этот ключ второй стороне?
- В 1970-х гг. было предложено асимметричное шифрование (криптография с открытым ключом). Появились два ключа: открытый (public key) для шифрования, который можно всем показывать, и закрытый (private key) для расшифрования, который хранится в секрете. Это решило проблему распределения ключей.

1. Введение в криптографию

Современное состояние криптографии

Современная криптография — это фундамент цифрового мира. Она основана на сложных математических вычислениях, которые практически невозможно реализовать без знания ключа.

Куда она встроена?

Повсюду: мессенджеры (TG, WhatsApp), интернет-банкинг, HTTPS-соединения в браузере, цифровые подписи, криптовалюты (Bitcoin) и блокчейн.

•

1. Введение в криптографию
Современное состояние криптографии

Основные алгоритмы

– **Симметричные** (быстрые, для шифрования больших объемов данных): AES (Advanced Encryption Standard) — мировой стандарт.

– **Асимметричные** (для установки безопасного соединения и цифровых подписей): RSA, ECC (Elliptic Curve Cryptography).

– **Хеш-функции** (для проверки целостности): SHA-256 (используется в Bitcoin).

1. Введение в криптографию
Современное состояние криптографии

Современные вызовы:

– **Квантовые вычисления:** существующие квантовые компьютеры теоретически могут взломать многие современные асимметричные алгоритмы. Уже активно развивается **постквантовая криптография** — новые алгоритмы, устойчивые к таким атакам.

– **Сохранить баланс** между правом на приватность и интересами национальной безопасности.

Лекция 1
Введение в криптографию. Основные нормативные и законодательные документы

2. Основные нормативные и законодательные документы (законы в области защиты информации)

2. Основные нормативные и законодательные документы защиты информации

Что защищаем? Основные понятия и объекты защиты

Защищаемая информация — это ключевой актив государства, бизнеса и гражданина.

Основные объекты правовой защиты:

1. **Конфиденциальность:**
2. **Целостность:**
3. **Доступность:** обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

2. Что такое Комплаенс в Информационной Безопасности?

- **Комплаенс в ИБ** — это система соблюдения установленных требований к защите информации.
- **Суть:** Выполнение предписаний законов, стандартов и внутренних правил компании в области кибербезопасности.
- **Основные регуляторы в России:**
- **ФСТЭК России:** Требования к защите информации, особенно персональных данных (152-ФЗ) и критической информационной инфраструктуры (187-ФЗ).
- **ФСБ России:** Требования к использованию шифровальных средств (СКЗИ) и электронной подписи (63-ФЗ).
- **Роскомнадзор:** Контроль за обработкой персональных данных.
- **Международные стандарты:** ISO/IEC 27001, PCI DSS, GDPR.

2. Цель и Польза Комплаенса в ИБ

Цель: систематическое снижение рисков, связанных с нарушением законодательства и стандартов, для минимизации штрафов, репутационных потерь и операционных сбоев.

Польза комплаенса:

- **Снижение рисков -** избежание крупных штрафов и судебных исков.
- **Доверие регуляторов и партнеров -** упрощение проверок и аудитов.
- **Укрепление репутации** - повышение лояльности клиентов, которые уверены в безопасности своих данных.
- **Повышение зрелости процессов ИБ** - помогает выстроить структурированные и измеримые процессы защиты.

2. Основные нормативные и законодательные документы защиты информации

Категории информации, требующие защиты:

- Государственная тайна
- Коммерческая тайна
- Персональные данные (ПДн)
- Служебная тайна
- Профессиональная тайна (врачебная, нотариальная и т.д.)

2. Ключевые законы Российской Федерации

Правовое поле РФ в сфере защиты информации формируется несколькими уровнями законов.

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Базовый, «рамочный» закон.

Определяет основные понятия, принципы регулирования и цели защиты информации.

2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

Ключевой закон для работы с данными граждан.

Устанавливает требования к обработке ПДн, права субъектов ПДн и обязанности операторов.

2. Ключевые законы Российской Федерации

Правовое поле РФ в сфере защиты информации формируется несколькими уровнями законов.

3. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»

Устанавливает виды ЭП (простая, неквалифицированная, квалифицированная), их юридическую значимость и требования к средствам ЭП. Поскольку в основе квалифицированной ЭП (КЭП) лежит криптография, закон напрямую регулирует использование криптографических алгоритмов и средств шифрования для подписи документов. Требует, что средства КЭП должны быть сертифицированы ФСБ России.

2. Ключевые законы Российской Федерации

Правовое поле РФ в сфере защиты информации формируется несколькими уровнями законов.

3. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ»

Регулирует защиту важнейших объектов (энергетика, транспорт, здравоохранение и др.).

Обязывает владельцев объектов КИИ обеспечивать их безопасность и информировать госорганы о кибератаках.

Также важны: Уголовный кодекс РФ (ст. 272, 273, 274), законы о гостайне, коммерческой тайне и лицензировании деятельности по ТЗКИ (технической защите конфиденциальной информации).

2. Ключевые законы Российской Федерации

Что требуют законы от организаций?

- **Для операторов ПДн (152-ФЗ):**
  - Получить согласие на обработку ПДн.
  - Обеспечить конфиденциальность данных.
  - Уведомлять Роскомнадзор о начале обработки.
  - Применять необходимые организационные и технические меры защиты.

2. Ключевые законы Российской Федерации

Что требуют законы от организаций?

- **Для субъектов КИИ (187-ФЗ):**

– Выявить и категоризовать информационные системы.

– Установить систему мониторинга и управления инцидентами.

– Провести аттестацию информационных систем (ИС) на соответствие требованиям ФСТЭК России (Федеральная служба по техническому и экспортному контролю) .

– Предоставлять информацию в ГосСОПКА (Государственная Система Обнаружения, Предупреждения и Анализа Атак на информационные ресурсы России). Это национальный центр кибероборонs, который видит угрозы по всей стране.

2. Ответственность за нарушение в области защиты информации

Административная (**денежные** штрафы по Кодексу РФ об административных правонарушениях РФ - Обработка персональных данных без согласия человека: штраф для компании — **до 300 000 руб.**, а для директора — **до 50 000 руб.**)

Наиболее частый вид наказания. Применяется за сам факт нарушения установленных правил, даже если никакого ущерба еще не произошло.

Кто наказывается? Как **должностные лица** (например, директор, ответственный за IT), так и **юридическое лицо** (сама компания) в целом.

В чем выражается? В основном — в **денежных штрафах**.

2. Ответственность за нарушение в области защиты информации

Уголовная (лишение свободы по УК РФ)

Самая суровая мера ответственности. Применяется не за сам факт нарушения, а когда нарушение повлекло **тяжкие последствия** (крупный ущерб, нарушение работы критической инфраструктуры, суицид потерпевшего и т.д.) или совершено с корыстным умыслом.

Кто наказывается? Только **физические лица** (например, системный администратор, сис.админ, руководитель).

В чем выражается? Не только штрафы, но и:

- **Лишение свободы** (реальный тюремный срок).
- Принудительные работы.
- Лишение права занимать определенные должности.

2. Ответственность за нарушение в области защиты информации

Уголовная (лишение свободы по УК РФ)

Примеры (по ст. 272, 273, 274 УК РФ):

– **Незаконный доступ к информации (ст. 272):**

Если он повлек уничтожение или блокировку данных, — срок **до 5 лет лишения свободы**.

– **Создание и распространение вредоносных программ (ст. 273):**

Повлекшее тяжкие последствия — **до 7 лет лишения свободы**.

– **Нарушение правил эксплуатации средств хранения, обработки или передачи информации (ст. 274):**

Повлекшее по неосторожности тяжкие последствия — **до 5 лет лишения свободы**.

2. Ответственность за нарушение в области защиты информации

Гражданско-правовая (возмещение ущерба)

- Это финансовая компенсация **конкретным людям или организациям**, которым был причинен вред из-за утечки данных или сбоя в работе системы.
- **Кто подает иск?** Пострадавшая сторона (физическое лицо, чьи данные утекли, или компания-партнер, чья работа остановилась из-за сбоя у вас).
- **В чем выражается? Деньги**. Размер ущерба доказывается в суде.

2. Ответственность за нарушение в области защиты информации

Гражданско-правовая (возмещение ущерба)

Примеры:

- После утечки данных паспортов и телефонов клиентов из банка, мошенники взяли кредиты на их имена. Клиенты через суд могут взыскать с банка **компенсацию морального вреда** (например, 50 000 руб. каждому) и **возмещение материального ущерба** (сумму незаконно взятого кредита).
- Компания-поставщик не смогла отгрузить товар из-за хакерской атаки на вашу систему, сорвав контракт. Она может потребовать **компенсацию упущенной выгоды**.

2. Ответственность за нарушение в области защиты информации

Приостановление деятельности

- временный **запрет на работу** всей компании или ее части, связанной с нарушением. Это крайняя мера, применяемая регулятором или судом.
- **Когда применяется?**

Чаще всего, если нарушение создает **непосредственную угрозу** жизни, здоровью людей, безопасности государства или невозможно быстро устранить другим способом.

2. Ответственность за нарушение в области защиты информации

Приостановление деятельности

Примеры:

- Сайт интернет-магазина взломан, и хакеры имеют доступ к базе данных клиентов (номера карт, пароли). Роскомнадзор или суд может **приостановить работу сайта** до полного устранения уязвимостей и обеспечения безопасности, чтобы предотвратить дальнейшие утечки.
- Обнаружено, что оператор связи обрабатывает данные абонентов с грубыми нарушениями, не обеспечивая их защиту. Его деятельность по обработке данных могут приостановить.

Выводы

Защита информации — **не опция, а законодательное требование**.

Правовое поле постоянно **усложняется и ужесточается** в ответ на растущие киберугрозы.

Комплаенс позволяет не только избежать штрафов, но и **повысить устойчивость бизнеса** и **доверие клиентов**.

Развитие регулирования в сфере больших данных и искусственного интеллекта.

Соблюдение законов в области ЗИ — основа цифровой трансформации и безопасности в современном мире.