## **30 билетов Шилова (новые)**

## Билет 1

### 1. Модель информационной безопасности Кларка–Вилсона. Ее основные принципы. Применение модели Кларка–Вилсона

**Суть модели**

* Основана на разделении доступа и ролевом контроле над данными.
* Ключевые объекты: конечные объекты целостности (CDI — Constrained Data Items), преобразующие процедуры (TP — Transformation Procedures) и нетребующие контроля данные (UDI — Unconstrained Data Items).
* Модель уделяет особое внимание целостности данных, обеспечивая её при помощи специально определённых процедур и разделения ролей.

**Основные принципы**

1. **Разделение обязанностей** (Separation of Duties): недопустимость, чтобы один пользователь обладал полномочиями на полный цикл операций, способных исказить данные.
2. **Аудит и контроль**: все операции должны регистрироваться и контролироваться.
3. **Авторизованные процедуры**: доступ к данным осуществляется исключительно через доверенные процедуры (TP).
4. **Сохранение целостности**: каждый элемент данных (CDI) должен модифицироваться только корректными процедурами.

**Применение**

* Используется в финансовых системах, банковских приложениях, ERP-системах.
* Подходит для сред, где критична корректность и целостность данных, а не только конфиденциальность.

### 2. Аудит информационной безопасности. Виды аудита информационной безопасности. Методы проведения аудита информационной безопасности

**Аудит ИБ** — это проверка соответствия системы, процессов, инфраструктуры требованиям стандартов, законодательству, внутренним политикам.

**Виды аудита**

1. **Внутренний аудит**: проводится собственными силами организации.
2. **Внешний аудит**: проводится внешними независимыми аудиторами или сертификационными органами.
3. **Комплаенс-аудит**: проверка на соответствие конкретным стандартам или регуляторным требованиям (например, ISO 27001, PCI DSS).
4. **Технический аудит** (пентест, сканирование уязвимостей, аудит конфигураций) и **организационный аудит** (проверка политик, процессов).

**Методы**

* **Анализ документации** (политики, регламенты, журналы).
* **Интервью** с сотрудниками.
* **Наблюдение** за процессами.
* **Инструментальное тестирование** (сканирование уязвимостей, тесты на проникновение).
* **Сравнение с эталонами** (baseline, бенчмарки CIS и др.).

## Билет 2

### 1. Стандарты в области информационной безопасности

К ключевым стандартам относятся:

* **ISO/IEC 27000** (особенно ISO/IEC 27001 — система управления информационной безопасностью, ISO/IEC 27002 — практические меры ИБ).
* **NIST Special Publications** (например, NIST SP 800-53 — меры безопасности).
* **COBIT** (управление ИТ-процессами, включая ИБ).
* **ГОСТ**-стандарты России (например, ГОСТ Р ИСО/МЭК 27001-2021 и др.).
* **Международные и отраслевые**: PCI DSS (для платежных карт), HIPAA (медицина), GDPR (персональные данные в ЕС).

### 2. Идентификация, аутентификация и авторизация. Определения, отличия и сходство

1. **Идентификация** — процедура, в ходе которой субъект сообщает системе свои идентификационные данные (логин, номер удостоверения и т. п.).
2. **Аутентификация** — проверка подлинности идентификатора (например, проверка пароля, ключа, биометрии).
3. **Авторизация** — предоставление прав и определение полномочий на доступ к ресурсам после успешной аутентификации.

**Отличия**

* Идентификация: «Кто вы?»
* Аутентификация: «Докажите, что вы действительно тот, за кого себя выдаёте».
* Авторизация: «Что вам разрешено делать?»

**Сходство** — все стадии являются элементами единого процесса контроля доступа и связаны с безопасным доступом к информационным ресурсам.

## Билет 3

### 1. Международные стандарты информационной безопасности. Серия ISO 27000. ГОСТ Р ИСО/МЭК 27000-2021

* **ISO/IEC 27000**: общий обзор серии, терминология.
* **ISO/IEC 27001**: требования к Системе менеджмента информационной безопасности (СМИБ).
* **ISO/IEC 27002**: практические рекомендации по мерам безопасности.
* **ISO/IEC 27005**: управление рисками в области ИБ.
* **ГОСТ Р ИСО/МЭК 27000-2021**: адаптированный для РФ перевод и уточнение терминологии ISO/IEC 27000.
* Цель всех стандартов серии — единый подход к управлению информационной безопасностью, непрерывное улучшение и соответствие лучшим мировым практикам.

### 2. Базовые технологии безопасности информационных систем

* **Шифрование** (симметричное, асимметричное).
* **Электронная цифровая подпись** (гарантия целостности, неотказуемости).
* **Инфраструктура открытых ключей (PKI)**.
* **Контроль доступа** (DAC, MAC, RBAC, ABAC).
* **Антивирусное ПО, межсетевые экраны, системы обнаружения и предотвращения атак (IDS/IPS)**.
* **Многофакторная аутентификация**.
* **Средства резервного копирования** и **системы отказоустойчивости**.

## Билет 4

### 1. Основные атаки и угрозы информационным системам

* **Вредоносное ПО** (вирусы, черви, трояны, ransomware).
* **Фишинг** и **социальная инженерия**.
* **DDoS-атаки**.
* **SQL-инъекции**, **XSS** (web-уязвимости).
* **MITM (Man-in-the-Middle)**.
* **Брутфорс** (подбор паролей).
* **Эксплойты уязвимостей** (в ОС, приложениях).

### 2. Ключевые термины информационной безопасности. Триада CIA

* **Конфиденциальность (Confidentiality)**: защита от несанкционированного раскрытия данных.
* **Целостность (Integrity)**: защита от несанкционированных изменений данных.
* **Доступность (Availability)**: обеспечение доступности информации и ресурсов при необходимости.

## Билет 5

### 1. Комбинированные политики безопасности

* Подход, сочетающий несколько типов политик (дискреционные, мандатные, ролевые, атрибутивные и т. д.) в одной системе.
* Применяется там, где требуется гибкость (дискреция) и жёсткое регулирование (мандат) одновременно.
* Позволяет учесть разные требования — от регуляторных норм до внутренних рисков.

### 2. Парольные системы. Выбор пароля. Требования к паролю. Достоинства и недостатки парольной аутентификации

**Требования к паролю**: достаточная длина, сложность (буквы разных регистров, цифры, спецсимволы), регулярная смена, неиспользование словарных слов и т. п.

**Достоинства**

* Простота использования.
* Низкая стоимость внедрения.

**Недостатки**

* Уязвимость к подбору (брутфорс, атакам со словарём).
* Риск компрометации (фишинг, утечка).
* Зависимость от пользователя (человеческий фактор).

## Билет 6

### 1. Использование MITRE ATT&CK и охота за угрозами (Threat Hunting). Примеры атак на информационную безопасность

* **MITRE ATT&CK** — база знаний, которая классифицирует тактики и техники, используемые злоумышленниками.
* Применение: анализ инцидентов, построение карт угроз, повышение эффективности SOC.
* **Threat Hunting** — проактивный поиск признаков компрометации (IOC, TTP).
* Примеры атак: трояны (Emotet), атаки с использованием PowerShell-скриптов (living off the land), атаки на цепочки поставок (supply chain attacks).

### 2. Классификация нормативно-правовых актов по информационной безопасности

1. **Международные** (GDPR, директивы ЕС, Конвенция о киберпреступности).
2. **Федеральные законы** (в РФ — «О персональных данных», «О коммерческой тайне», «О критической информационной инфраструктуре» и т. д.).
3. **Подзаконные акты**, указы и постановления Правительства.
4. **Приказы регуляторов** (ФСТЭК, ФСБ, Роскомнадзор).
5. **Отраслевые стандарты** (PCI DSS, ISO 27001) и др.

## Билет 7

### 1. Политики безопасности. Определение и примеры политик безопасности

* **Политика безопасности** — свод правил и процедур, регламентирующих, как организация защищает информацию и ИТ-системы.
* Примеры: политика управления паролями, политика резервного копирования, политика разграничения доступа, политика работы с мобильными устройствами.

### 2. Основные методы и средства защиты от DDoS-атак. Примеры инструментов защиты

1. **Фильтрация на сетевом уровне** (ACL, rate limiting).
2. **Сетевые экраны (firewalls), IDS/IPS**, системы обнаружения аномалий.
3. **Скруббинг-центры** (облачные провайдеры, перенаправляющие malicious-трафик на очистку).
4. **Anycast**-архитектура для распределения нагрузки.
5. **Инструменты**: Cloudflare, Akamai, Radware, Arbor Networks и др.

## Билет 8

### 1. Модель Белла–Лападулы

* Предназначена для защиты конфиденциальности данных.
* Основные принципы:
  + Не считывай сверху (no read up) — субъект с более низким уровнем доступа не может читать объекты с более высоким уровнем конфиденциальности.
  + Не записывай вниз (no write down) — субъект с более высоким уровнем доступа не может записывать данные в объекты с более низким уровнем.
* Используется в военных и государственных системах.

### 2. Основные принципы защиты информационной безопасности

1. **Принцип минимальных привилегий** (least privilege).
2. **Принцип разделения обязанностей** (separation of duties).
3. **Принцип «отказ по умолчанию»** (default deny).
4. **Многоуровневая защита** (defense in depth).
5. **Регулярное обновление и мониторинг** (patch management, мониторинг событий ИБ).
6. **Аутентификация и авторизация**.

## Билет 9

### 1. Модель Биба

* Аналог модели Белла–Лападулы, но с фокусом на целостности данных.
* Основные правила:
  + Не читай снизу (no read down) — субъект не может читать объекты более низкого уровня целостности, чтобы не «загрязнить» свои данные.
  + Не записывай вверх (no write up) — субъект не может записывать данные в объекты более высокого уровня целостности.

### 2. Аутентификация с использованием биометрии: виды, достоинства и ограничения. Способы аутентификации. Многофакторная аутентификация

* **Виды биометрии**: отпечатки пальцев, распознавание лица, радужки глаза, голосовая биометрия и т. д.
* **Достоинства**: высокий уровень защиты, сложно подделать (при корректном внедрении).
* **Ограничения**: стоимость, возможность ложных срабатываний, сложность корректного хранения биометрических шаблонов, вопросы приватности.
* **Способы аутентификации**: по знаниям (пароль), по владению (токен, смарт-карта), по биометрии (отпечаток).
* **Многофакторная аутентификация**: комбинация двух и более факторов (например, пароль + SMS-код + отпечаток пальца).

## Билет 10

### 1. Мандатные политики безопасности

* Жёсткий контроль доступа на основе классификации и меток безопасности.
* Назначение меток (уровней конфиденциальности) объектам и субъектам.
* Пользователь не может изменить политику доступа произвольно.
* Типичный пример: военные системы, где документы имеют грифы секретности.

### 2. Управление учетными записями пользователей в Windows. Локальные группы и пользователи

* **Учетные записи**: локальные, доменные (Active Directory).
* **Локальные группы**: позволяют объединять пользователей для упрощения управления правами.
* Типы локальных групп: Administrators, Users, Guests, Power Users (в старых версиях).
* Практики безопасности: принцип минимальных привилегий, регулярная ревизия, включение/выключение учётных записей, строгая политика паролей.

## Билет 11

### 1. Ролевые политики безопасности (RBAC)

* Доступ определяется ролями, а не конкретными пользователями.
* Пользователь получает права, принадлежащие его роли (например, “Менеджер”, “Бухгалтер”).
* Удобно для крупных организаций: облегчает управление правами и их аудит.

### 2. Классификация алгоритмов шифрования

1. **По типу ключей**:
   * Симметричные (один ключ для шифрования/расшифрования).
   * Асимметричные (пара ключей: открытый и закрытый).
2. **По способу обработки**:
   * Потоковые (обрабатывают данные побитово/побайтово).
   * Блочные (обрабатывают данные блоками фиксированной длины).
3. **По назначению**: шифрование, ЭЦП, хеширование.

## Билет 12

### 1. Дискреционные политики безопасности

* Контроль доступа определяет владелец объекта (файл, документ).
* Владелец сам решает, кто и с какими правами может получить доступ (read/write/execute).
* Используется в большинстве ОС (Windows, UNIX) в базовой модели прав.

### 2. Криптостойкость алгоритмов шифрования. Уровень криптостойкости

* **Криптостойкость**: мера сложности взлома алгоритма перебором или иными методами.
* Зависит от длины ключа, сложности математической основы, отсутствия уязвимостей в реализации.
* **Уровень криптостойкости** часто оценивается в битах (например, 128-бит, 256-бит) и указывает на количество операций перебора (2^128 и т. д.).
* Для современных стандартов обычно рекомендуются ключи от 128 бит и более (в симметричных алгоритмах).

## Билет 13

### 1. Политики безопасности на основе атрибутов (ABAC). Атрибуты пользователя, ресурса, действия, контекстуальные. Преимущества

* **ABAC (Attribute-Based Access Control)** — решения о доступе принимаются на основе набора атрибутов (профиль пользователя, тип данных, время суток, геолокация и др.).
* **Преимущества**: гибкость, масштабируемость, более тонкая настройка политик, возможность учесть контекст (например, доступ разрешён только в рабочее время из определённого сегмента сети).

### 2. Защита конфиденциальных данных: понятие, законодательные требования и технологии

* **Понятие**: защита личных, коммерческих, государственных сведений от несанкционированного доступа.
* **Законодательные требования** (в РФ: Закон «О персональных данных», в ЕС: GDPR и т. п.).
* **Технологии**: шифрование (в покое и при передаче), разграничение прав, токенизация, DLP-системы (Data Loss Prevention), SIEM (мониторинг).

## Билет 14

### 1. Политики безопасности на основе контекста или тематические политики

* Контекстные политики учитывают текущие условия: место, время, устройство доступа, IP-адрес, состояние системы.
* Могут динамически ограничивать/разрешать доступ (например, запрещать вход в систему вне рабочего времени или из необычной геолокации).

### 2. Симметричные алгоритмы шифрования Магма, Кузнечик (ГОСТ Р 34.12-2015). Длина входного блока, длина ключа

* **Магма** (ранее «ГОСТ 28147-89»): блочный алгоритм с размером блока 64 бита, ключ 256 бит (включая разбиение на подпараметры).
* **Кузнечик**: блочный алгоритм с размером блока 128 бит, ключ 256 бит.
* Являются российскими стандартами симметричного шифрования, регламентируются ФСБ.

## Билет 15

### 1. Правовое регулирование электронной цифровой подписи. Виды электронной подписи, предусмотренные законодательством РФ

В РФ действует Федеральный закон № 63-ФЗ «Об электронной подписи», который определяет:

1. **Простая электронная подпись** — связана с определёнными данными (логин/пароль, код).
2. **Усиленная неквалифицированная** — создаётся средствами, обеспечивающими криптографические методы защиты, но без обязательной аккредитации УЦ.
3. **Усиленная квалифицированная** — создаётся с использованием сертифицированных средств, выданных аккредитованным УЦ (имеет максимально возможную юридическую силу).

### 2. Сравнение симметричного и асимметричного шифрования. Преимущества и недостатки каждого подхода

**Симметричное**

* **Плюсы**: высокая скорость, относительно простая реализация.
* **Минусы**: сложность безопасной передачи ключа.

**Асимметричное**

* **Плюсы**: упрощённое управление ключами (открытый ключ можно распространять свободно), подходит для ЭЦП.
* **Минусы**: ниже скорость, более сложные алгоритмы.

## Билет 16

### 1. Классификация угроз безопасности персональных данных. Законодательные акты по безопасности персональных данных

**Угрозы**

* Несанкционированный доступ, утечка (взлом, фишинг).
* Неправомерное копирование, изменение или удаление.
* Внедрение вредоносного кода.
* Человеческий фактор (ошибки персонала, социальная инженерия).

**Законодательство РФ**

* Федеральный закон № 152-ФЗ «О персональных данных».
* Постановления Правительства РФ, приказы ФСТЭК и ФСБ, методические документы по уровням защищённости ПДн и т. д.

### 2. Шифры перестановки. Шифр Цезаря. Шифр Атбаш

* **Шифры перестановки**: символы сообщения меняют порядок согласно определённому правилу или ключу.
* **Шифр Цезаря**: каждый символ сдвигается на фиксированное число позиций в алфавите.
* **Шифр Атбаш**: зеркальное сопоставление алфавита (A ↔ Z, B ↔ Y и т. д. в латинице или А ↔ Я, Б ↔ Ю в кириллице).

## Билет 17

### 1. Этапы проектирования политики информационной безопасности. Основные элементы политики

**Этапы**

1. Анализ текущего состояния, оценка рисков и требований.
2. Формирование целей и задач политики.
3. Определение мер, процедур, ответственных лиц.
4. Документирование политики и согласование.
5. Внедрение и обучение персонала.
6. Мониторинг, аудит, актуализация.

**Основные элементы**: область действия, терминология, распределение ролей и обязанностей, меры защиты, порядок реагирования на инциденты, управление изменениями.

### 2. Шифр Вернама и метод одноразовых блокнотов. Криптоустойчивость шифра Вернама

* **Шифр Вернама (одноразовый блокнот)**: открытый текст складывается по модулю 2 с ключом равной длины, который используется только один раз.
* При полном соблюдении условий (случайность ключа, длина ключа равна длине сообщения, одноразовое использование) считается **абсолютно стойким**.
* На практике сложно обеспечить генерацию и безопасную передачу ключей.

## Билет 18

### 1. Шифрование методом перестановки. Шифр Цезаря. Шифр Атбаш

(См. предыдущие билеты, вопрос дублируется)

* **Метод перестановки**: символы меняют порядок согласно ключу-перестановке (например, длина блока 6, ключ [3, 1, 4, 6, 2, 5]).
* **Шифр Цезаря**: сдвиг букв.
* **Атбаш**: зеркальное отражение алфавита.

### 2. Правовое регулирование электронной цифровой подписи. Виды электронной подписи, предусмотренные законодательством РФ

(См. билет 15, вопрос дублируется)

* **Основной закон**: № 63-ФЗ «Об электронной подписи».
* **Виды**: простая, усиленная неквалифицированная, усиленная квалифицированная.

## Билет 19

### 1. Критическая информационная инфраструктура (КИИ). Объекты КИИ. Субъекты КИИ. Защита КИИ

* **КИИ** — объекты информационных систем, сетей, автоматизированных систем управления в ключевых отраслях (энергетика, транспорт, финансы, здравоохранение и пр.).
* **Субъекты** — организации, владеющие/эксплуатирующие объекты КИИ (операторы КИИ).
* **Защита** включает: категорирование объектов, выполнение требований ФСТЭК/ФСБ по безопасности, мониторинг инцидентов, внедрение систем обнаружения вторжений и т. д.

### 2. Основные принципы защиты информационной безопасности

(См. билет 8, вопрос 2)

* Минимальные привилегии, разделение обязанностей, «отказ по умолчанию», многоуровневая защита, регулярный аудит и т. д.

## Билет 20

### 1. Функции межсетевого экранирования. Межсетевой экран как средство защиты частных сетей

* Межсетевой экран (firewall) контролирует входящий/исходящий трафик на основе заданных правил (IP-адреса, порты, протоколы).
* **Функции**: фильтрация пакетов, трансляция адресов (NAT), VPN-шлюз, ведение логов трафика.
* Предотвращает несанкционированный доступ к внутренним ресурсам.

### 2. Принципы работы антивирусного ПО. Методы обнаружения вредоносного кода

* **Сигнатурный анализ**: сравнение кода с базой известных сигнатур.
* **Эвристический анализ**: поиск типичного подозрительного поведения.
* **Песочницы** (sandbox): запуск подозрительных файлов в изолированной среде.
* **Облачные технологии**: проверка через онлайн-сервисы, базы данных угроз.

## Билет 21

### 1. Аппаратные и программные межсетевые экраны. Критерии выбора межсетевых экранов

* **Аппаратные**: специализированные устройства (например, Cisco, Fortinet), высокая производительность, надёжность, могут быть дороже.
* **Программные**: устанавливаются на ОС (iptables, Windows Firewall), более гибкие, дешевле, но зависят от надёжности и производительности сервера.

**Критерии выбора**

1. Производительность (пропускная способность, задержки).
2. Функциональность (VPN, IDS/IPS, фильтрация приложений).
3. Масштабируемость и управляемость (GUI, консоль, интеграция с SIEM).
4. Безопасность и соответствие стандартам/сертификация.
5. Стоимость владения (TCO).

### 2. Социальная инженерия как угроза информационной безопасности. Методы защиты от социальной инженерии

* **Социальная инженерия**: манипулирование людьми с целью выведать конфиденциальную информацию или спровоцировать определённые действия (открыть файл, перейти по ссылке).
* **Методы защиты**: обучение персонала, проверка личности (call-back), регламенты обмена информацией, использование многофакторной аутентификации, осторожность при переходе по ссылкам и открытии вложений.

## Билет 22

### 1. Роль сертификации в области информационной безопасности. Основные стандарты сертификации

* **Роль**: подтверждение соответствия систем/процессов/продуктов требованиям безопасности, повышение доверия со стороны клиентов, партнёров, регуляторов.
* **Основные стандарты**: ISO/IEC 27001 (сертификация СМИБ), PCI DSS (для компаний, работающих с картами), Common Criteria (сертификация продуктов), ГОСТ Р (в РФ).

### 2. Фишинг как угроза информационной безопасности. Методы защиты от фишинга

* **Фишинг**: мошенническая рассылка писем/сообщений, имитирующих доверенные источники, с целью кражи учётных данных, платежной информации и т. д.
* **Защита**: спам-фильтры, антивирус/ATP (advanced threat protection), обучение сотрудников, проверка ссылок (hover-check), использование 2FA, антивирусные решения с веб-фильтрацией, правила безопасного поведения в сети.

## Билет 23

### 1. Что такое MITRE ATT&CK? Какие основные компоненты включает эта база знаний?

* **MITRE ATT&CK**: открытая база знаний тактик и техник, используемых злоумышленниками на разных стадиях кибератаки.
* **Основные компоненты**:
  + Матрица тактик и техник (Reconnaissance, Resource Development, Initial Access и др.).
  + Enterprise, Mobile, ICS версии.
  + Описания TTP (Tactics, Techniques, Procedures).
  + Sub-techniques, mitigations, descriptions of adversary groups.

### 2. Аппаратные и программные межсетевые экраны. Критерии выбора межсетевых экранов

(Повтор из билета 21)

## Билет 24

### 1. Основные принципы защиты информационной безопасности

(См. выше, билет 8, вопрос 2 и билет 19, вопрос 2)

Повтор: минимальные привилегии, разделение обязанностей, «отказ по умолчанию», многоуровневая защита и др.

### 2. MITM-атака на схему Диффи–Хеллмана

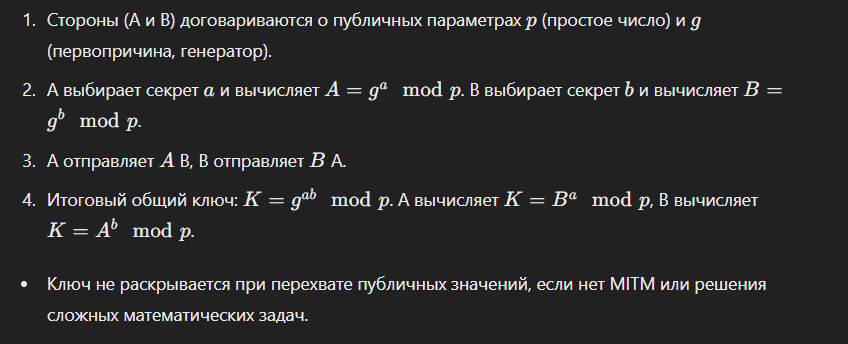
* **Диффи–Хеллман**: протокол обмена ключами. Уязвимость — отсутствие аутентификации сторон.
* **MITM (Man-in-the-Middle)**: атакующий перехватывает сообщения A и B, устанавливая два ключа (A ↔ злоумышленник ↔ B). Стороны думают, что общаются напрямую, но всё идёт через атакующего.
* Защита: добавлять аутентификацию (например, сертификаты, цифровую подпись).

## Билет 25

### 1. Критичность системы или сервиса, уровни критичности. Понятие критичности

* **Критичность**: мера важности для бизнеса/организации (финансовые потери, риски для жизни/здоровья, репутационные последствия).
* **Уровни критичности**: высокий (остановка ведёт к большим потерям), средний, низкий. В некоторых системах — детальное ранжирование (1, 2, 3…).
* Определяется в рамках управления рисками (BCP/DRP-планы).

### 2. Схема работы протокола Диффи–Хеллмана



## Билет 26

### 1. Критическая информационная инфраструктура (КИИ). Объекты КИИ. Субъекты КИИ. Защита КИИ

(См. билет 19, вопрос 1)

### 2. Схема работы протокола Диффи–Хеллмана

(См. билет 25, вопрос 2)

## Билет 27

### 1. Симметричные и асимметричные алгоритмы шифрования

(См. билет 15, вопрос 2 для сравнения)

* **Симметричные** (AES, ГОСТ «Магма», «Кузнечик»): один ключ, быстрее, сложнее управление ключами.
* **Асимметричные** (RSA, ECC, ElGamal): пара ключей, проще обмен ключами, медленнее.

### 2. Криптографические генераторы псевдослучайных последовательностей. Разница между случайными и псевдослучайными последовательностями. Применение ГПСП

* **ГПСП** (PRNG) генерируют последовательности, которые кажутся случайными, но детерминированны при известном начальном состоянии (seed).
* **Истинная случайность** (TRNG) берётся из физических процессов (шум, радиоактивный распад).
* **Псевдослучайность**: важна для криптографических приложений, где необходимо большое количество «случайных» чисел (например, для ключей).
* Применение: генерация ключей, соли, вектор инициализации (IV), одноразовые пароли.

## Билет 28

### 1. Шифр одноразового блокнота

(См. билет 17, вопрос 2 про шифр Вернама)

* Один и тот же ключ (случайная последовательность той же длины, что и сообщение) используется единственный раз. Абсолютная криптостойкость при соблюдении условий.

### 2. Фишинг как угроза информационной безопасности. Методы защиты от фишинга

(См. билет 22, вопрос 2)

* Фильтрация, обучение, 2FA, проверка ссылок, антивирус, антивредоносные решения, осторожное отношение к письмам от неизвестных отправителей.

## Билет 29

### 1. Социальная инженерия как угроза информационной безопасности. Способы защиты от социальной инженерии

(См. билет 21, вопрос 2)

* Основной метод борьбы — обучение и осведомлённость пользователей, проверка подлинности запросов, регламенты, недоверие к неожиданным просьбам и «выгодным» предложениям.

### 2. Шифр одноразового блокнота

(См. билет 17, вопрос 2 и билет 28, вопрос 1)

## Билет 30

### 1. Международные стандарты информационной безопасности. Стандарты серии ISO 27000. ГОСТ Р ИСО/МЭК 27000-2021

(См. билет 3, вопрос 1 — повтор)

* Модель менеджмента ИБ, непрерывное улучшение, соответствие лучшим практикам. ГОСТ Р ИСО/МЭК 27000-2021 — российская адаптация.

### 2. Шифры перестановки. Шифр Цезаря. Шифр Атбаш

(См. билеты 16 и 18 — повтор)

## **60 билетов Шилова (старые)**

## 1. Реализация сетевого протокола SSL

* **SSL (Secure Sockets Layer)**, предшественник TLS, обеспечивает защищённое шифрованное соединение между клиентом и сервером.
* Включает **рукопожатие (handshake)**, во время которого выбираются криптографические параметры, происходит аутентификация сервера (иногда клиента) и устанавливается общий ключ.
* Реализация предполагает использование **цифровых сертификатов**, выданных удостоверяющими центрами (CA), и симметричных алгоритмов шифрования для основного трафика.

## 2. Стандарты информационной безопасности

* Ключевые международные стандарты: **серия ISO/IEC 27000**, NIST SP 800, COBIT, PCI DSS (для платёжных карт).
* В России действуют **ГОСТ**-стандарты, регулирующие криптографию (ГОСТ Р 34.12-2015 «Магма», «Кузнечик»), ЭЦП, а также требования ФСТЭК и ФСБ.
* Цель стандартов: унификация и формализация требований, процедур и методов защиты информации.

## 3. Методы обеспечения безопасности информационных систем

* **Организационные** (политики, регламенты, обучение персонала).
* **Технические** (межсетевые экраны, IDS/IPS, антивирусы, шифрование).
* **Криптографические** (конфиденциальность, целостность, аутентификация, ЭЦП).
* **Процессные** (аудит, мониторинг, тесты на проникновение).

## 4. Основные атаки и угрозы информационным системам

* **Зловредное ПО** (вирусы, трояны, рансомваре).
* **Сетевые атаки** (DDoS, фишинг, MITM, SQL-инъекции, XSS).
* **Социальная инженерия** (обман, фишинг-письма).
* **Внутренние угрозы** (недобросовестные сотрудники, ошибки администраторов).

## 5. Модель предполагаемого противника

* Описание типа, ресурсов, мотивации и возможностей злоумышленника.
* Модель учитывает: **уровень квалификации**, финансовые ресурсы, доступ к эксплойтам, инсайдерские данные.
* Основывается на оценке **рисков** и помогает определить соответствующие меры защиты.

## 6. Внешний периметр, зоны безопасности, контуры защиты, контролируемая зона

* **Внешний периметр** — граница между корпоративной сетью и внешними сетями (Интернет).
* **Зоны безопасности** — сегменты сети с разным уровнем доверия (DMZ, внутренняя сеть и т.д.).
* **Контуры защиты** — уровни (слои) технических и организационных мер, защищающих зоны.
* **Контролируемая зона** — физическая территория или сетевой сегмент, где организация может обеспечить полный контроль.

## 7. Политики безопасности

* Набор формализованных правил и требований, определяющих, как защищается информация в организации.
* Включают политики паролей, резервного копирования, обновлений, управления доступом, реагирования на инциденты.
* Регламентируют **роли и обязанности** персонала, порядок изменения конфигураций и ведения аудита.

## 8. Модель системы защиты

* Определяет архитектуру и принципы реализации ИБ (многоуровневая модель, модель с зонами безопасности, контроль доступа, криптография и т.д.).
* Может опираться на формальные модели (Белла–Лападулы, Биба, Кларка–Вилсона) или на практические стандарты (ISO 27001).
* Цель — обеспечить согласованную защиту **конфиденциальности, целостности и доступности**.

## 9. Специализированные аппаратно-программные системы защиты безопасности

* Устройства и решения «всё в одном» (UTM — Unified Threat Management), HSM (Hardware Security Module), VPN-шлюзы, средства защиты каналов связи.
* Гарантируют высокую производительность и защищённость ключевых операций (например, генерацию, хранение и управление ключами).
* Сертифицируются регулирующими органами (ФСТЭК, ФСБ) для использования в государственных и коммерческих системах.

## 10. Системы безопасности «Криптоцентр»

* Отечественный программно-аппаратный комплекс для **защиты каналов связи**, организации VPN, управления ключами и сертификатами.
* Может обеспечивать шифрование на уровне IPsec, SSL/TLS, использовать ГОСТ-алгоритмы.
* Предоставляет централизованное администрирование и мониторинг.

## 11. Системы безопасности «Криптон»

* Семейство решений (например, «Криптон-Endpoint» и др.), предназначенных для защиты рабочих станций, серверов, сетевых коммуникаций.
* Как правило, включает **криптографические модули** (ГОСТ) для шифрования каналов и хранения ключей.
* Может также обеспечивать контроль целостности, управление доступом.

## 12. Системы безопасности «Верба»

* Линейка отечественных средств шифрования голоса, данных и IP-трафика (Voice/IP).
* Часто применяется в государственных структурах, силовых ведомствах, обеспечивая безопасную связь.
* Поддерживает механизмы **ГОСТ-шифрования** и сертифицирована в ФСБ/ФСТЭК.

## 13. Системы безопасности «Крипто-Про»

* Популярный в РФ **криптопровайдер** и инструменты для реализации ЭЦП, шифрования, криптографической защиты на рабочих станциях и серверах.
* Участвует в инфраструктуре открытых ключей (PKI), обеспечивает поддержку ГОСТ-алгоритмов и совместимость с программными продуктами (например, 1С, Microsoft).
* Используется для формирования, проверки и управления **квалифицированными сертификатами**.

## 14. Биометрические системы

* Системы аутентификации по **физиологическим** (отпечаток пальца, радужка глаза, лицо) или **поведенческим** (голос, подпись) характеристикам.
* Достоинства: повышенная надёжность (сложнее подделать), удобство для пользователей.
* Недостатки: риск утечки биометрических шаблонов, сложность корректного хранения, возможность ложных срабатываний.

## 15. Правовые аспекты цифровой подписи

* В РФ регламентируется ФЗ № 63 «Об электронной подписи» — три вида: простая, усиленная неквалифицированная, усиленная квалифицированная.
* В международном контексте — eIDAS (ЕС), UETA, ESIGN (США).
* Цифровая подпись (ЭЦП) обеспечивает **неотказуемость**, целостность и аутентичность документа.

## 16. Интегрированная защита компьютерных сетей

* Комплексный подход: межсетевые экраны, IDS/IPS, антивирус, DLP, VPN, система управления уязвимостями и пр.
* Включает как аппаратные, так и программные средства, а также организационные меры (регламенты, обучение).
* Главная цель — **слоистая (эшелонированная) защита**, охватывающая все уровни: от периметра до рабочих станций.

## 17. Политика безопасности управления компьютерными сетями

* Определяет, кто и как администрирует сеть, какие инструменты и каналы удалённого доступа разрешены.
* Включает требования к **аутентификации** администраторов, ведению журналов изменений, сегментации доступа, резервному копированию настроек.
* Регламентирует доступ к сетевым устройствам (маршрутизаторы, коммутаторы, брандмауэры).

## 18. Защита подсистемы управления компьютерными сетями

* Использование **административных VLAN** (Out-of-Band Management), шифрование управления (SSH вместо Telnet, HTTPS вместо HTTP).
* Контроль привилегированных учётных записей, логирование и аудит действий администраторов.
* Защита от атак на SNMP (использование безопасных версий SNMPv3), фильтрация доступа к портам управления.

## 19. Технологии межсетевых экранов: фильтрация пакетов, применение шлюзов, прочие компоненты брандмауэров

* **Фильтрация пакетов** (Packet Filtering): анализ заголовков IP, портов, протоколов.
* **Межсетевые прокси-шлюзы** (Application Gateway): фильтрация на уровне приложений (HTTP, FTP).
* **Системы stateful inspection**: отслеживают состояния соединений, могут динамически открывать/закрывать порты.
* **UTM** (Unified Threat Management): совмещают firewall, IDS, антивирус, контент-фильтрацию.

## 20. Функции межсетевого экранирования

* Контроль и фильтрация входящего/исходящего трафика.
* Разделение сети на сегменты, предотвращение проникновений извне.
* Логирование и мониторинг сетевых сессий, а также поддержка **VPN** (в некоторых решениях).

## 21. Аппаратные брандмауэры

* Специализированные устройства (Cisco ASA, Fortinet, Check Point и др.) с высокой пропускной способностью и надёжностью.
* Удобны для развертывания на **корпоративном периметре**, имеют аппаратное ускорение криптографии.
* Поддерживают расширенные функции: IDS/IPS, VPN, веб-фильтрация, балансировка нагрузки.

## 22. Политика безопасности межсетевого экрана

* Набор **правил фильтрации** (ACL — Access Control Lists) и политик NAT, определяющих, какой трафик разрешён или запрещён.
* Учитывает IP-адреса, порты, протоколы, время, а также аутентификацию пользователей (в некоторых случаях).
* Включает регулярный аудит и обновление правил, ведение логов, отслеживание аномалий.

## 23. Трансляторы сетевых адресов

* **NAT (Network Address Translation)** позволяет отображать частные IP-адреса во внешний (публичный) IP и обратно.
* Способствует маскировке внутренней топологии сети, улучшает безопасность.
* Варианты: **SNAT** (Source NAT), **DNAT** (Destination NAT), **PAT** (перевод многих внутренних адресов на один публичный с разными портами).

## 24. Шлюзы и прокси-серверы

* **Шлюз** (gateway) — узел, совмещающий разные протоколы или сети (например, VoIP-шлюз, VPN-шлюз).
* **Прокси-сервер** — промежуточный сервер, принимающий запросы клиентов и передающий их от своего имени к целевым ресурсам.
* Прокси обеспечивает **кэширование**, фильтрацию трафика, анонимизацию, может собирать статистику и применять правила контент-фильтрации.

## 25. Распознавание контента и его фильтрация

* Контент-фильтрация (URL-фильтрация, антивирусная проверка, DLP) — анализ содержимого пакетов или файлов.
* Может блокировать нежелательный трафик (порнография, азартные игры, вредоносные сайты) или конфиденциальные данные (номера карт, персональные данные).
* Используются решения: **Blue Coat, WebSense, Kaspersky Secure Web Gateway** и т.д.

## 26. Основы криптографии

* Наука о методах обеспечения **конфиденциальности**, **целостности**, **аутентичности**, **неотказуемости** информации.
* Включает **симметричные алгоритмы шифрования**, **асимметричные алгоритмы**, **хэш-функции**, **ЭЦП**, протоколы обмена ключами.
* Опирается на математические задачи (дискретное логарифмирование, факторизацию и пр.).

## 27. Симметричные и асимметричные алгоритмы шифрования

* **Симметричные** (один ключ для шифрования и расшифрования): AES, ГОСТ, 3DES. Быстрые, но сложность в безопасной передаче ключа.
* **Асимметричные** (пара ключей: открытый и закрытый): RSA, ECC. Проще обмен ключами, но работают медленнее.

## 28. Потоковые и блочные шифры

* **Потоковые**: шифруют данные побитово или побайтово (RC4, A5/1). Удобны для потоковых каналов, но есть риски, связанные с повторным использованием ключевого потока.
* **Блочные**: шифруют данные блоками фиксированного размера (AES — 128-битный блок, ГОСТ Магма — 64-битный блок). Поддерживают разные режимы (ECB, CBC, CTR и т.п.).

## 29. Криптографические генераторы псевдослучайных последовательностей

* **PRNG** (pseudo-random number generator) формируют последовательности, детерминированно зависящие от начального состояния (seed).
* В криптографии используют криптостойкие PRNG (Fortuna, ANSI X9.17, Hash-DRBG, HMAC-DRBG).
* Отличие от **истинной случайности** (TRNG): PRNG повторяем и предсказуем при известном seed.

## 30. Шифр одноразового блокнота

* **One-Time Pad (OTP)**: каждый символ исходного текста складывается по модулю 2 с символом ключа такой же длины.
* При полностью случайном ключе, равном длине сообщения, и единовременном использовании является **абсолютно стойким**.
* Практически сложно обеспечить надёжное хранение и распространение длинных ключей.

## 31. Криптографические протоколы

* Соглашения о формате и порядке взаимодействия, обеспечивающие безопасную передачу данных.
* Примеры: **SSL/TLS**, SSH, IPsec, Kerberos, PGP/OpenPGP.
* Обычно включают механизмы **аутентификации**, **шифрования**, **контроля целостности**.

## 32. Стандарт ANSI X.917

* Старый криптографический стандарт, описывающий метод генерации псевдослучайных чисел на базе блочного шифра (3DES).
* Применяется для ключевых генераторов в финансовых системах.
* Задаёт схему с «Seed Key» и «Seed Value» для формирования выходной последовательности.

## 33. Алгоритм Диффи-Хеллмана

* Позволяет двум сторонам согласовать **общий секретный ключ** по незащищённому каналу.
* Основан на сложности вычисления дискретного логарифма.
* Не обеспечивает аутентификацию сторон по умолчанию.

## 34. Схема Диффи-Хеллмана

1. Выбор общего простого числа p и основания g.
2. Участник A выбирает секрет a, вычисляет A=  mod p. Участник B выбирает b, вычисляет B=  mod p.
3. Обмен публичными значениями A и B.
4. Общий ключ: K=  mod p. Атака MITM возможна без доп. аутентификации.

## 35. MITM-атака на схему Диффи-Хеллмана

* Злоумышленник перехватывает AAA и BBB, подменяет их своими значениями.
* В результате A и B устанавливают ключи с атакующим, а не друг с другом.
* Защита: использовать **цифровые подписи**, сертификаты или иные методы аутентификации.

## 36. Рекурсивный алгоритм Евклида

* Используется для нахождения **наибольшего общего делителя (НОД)** двух чисел.
* Рекурсивная формула: gcd(a,b)=gcd(b,a mod b).
* Важен в криптографии для работы с ключами (RSA), при вычислении обратных элементов по модулю.

## 37. Расширенный алгоритм Евклида

* Не только вычисляет gcd(a,b), но и находит **коэффициенты** x и y такие, что ax+by=gcd.
* Применяется для вычисления **обратного элемента** по модулю (в RSA, Диффи–Хеллмане и т.д.).
* Реализуется и рекурсивно, и итеративно.

## 38. Алгоритм RSA

1. Выбирают два больших простых числа p и q.
2. Вычисляют n=p×q и ϕ(n)=(p−1)(q−1).
3. Выбирают e взаимно простое с ϕ(n).
4. Определяют d (обратное к e по модулю ϕ(n)).
5. Открытый ключ: (e,n). Закрытый ключ: (d,n).

* Используется для шифрования и ЭЦП.

## 39. Атаки и угрозы для хэш-функций, стойкость хэш-функции

* Основные требования стойкости: **невозможность найти исходное сообщение по хэшу** (preimage resistance) и **трудность найти два сообщения с одинаковым хэшем** (collision resistance).
* Атаки: поиск коллизий (метод дня рождения), выборочные коллизии, расширение длины (для некоторых конструкций).
* Примеры: уязвимости в MD5, SHA-1. Современные – SHA-2 (SHA-256, SHA-512) и SHA-3 (Keccak).

## 40. Хэш-функция SHA

* Семейство **Secure Hash Algorithm**: SHA-1 (160 бит), SHA-2 (224/256/384/512 бит), SHA-3.
* Применяются для проверки целостности, хранения паролей (с солью), формирования ЭЦП.
* SHA-1 признан менее надёжным (есть частичный прецедент коллизий), рекомендован переход на SHA-2/3.

## 41. Алгоритмы ЭЦП: RSA, DSA

* **RSA**: подпись формируется возведением хэша сообщения в степень d (закрытый ключ). Проверка — возведение результата в e (открытый ключ).
* **DSA** (Digital Signature Algorithm): основан на сложности дискретного логарифмирования. Подпись формируется через пару (r,s), проверяется уравнением на модуль p.
* Оба алгоритма требуют **надёжных генераторов** случайных чисел, особенно DSA (ранее были уязвимости с повторным k).

## 42. Российский и американский стандарты шифрования (ГОСТ, DES, AES)

* **ГОСТ Р 34.12-2015**: «Магма» (64-бит блок) и «Кузнечик» (128-бит блок), ключ 256 бит.
* **DES** (Data Encryption Standard), устаревший 56-битный ключ, уязвим к перебору.
* **AES** (Advanced Encryption Standard): блочный 128-битный шифр с ключами 128/192/256 бит. Современный стандарт США.

## 43. Сеть Фейстеля

* Конструкция блочного шифра, делит блок на две половины (L, R) и выполняет серию раундов, где одна половина модифицируется на основе функции шифрования от другой половины и ключа.
* Используется в **DES**, **Blowfish**, **Магма**.
* Обеспечивает возможность шифрования/расшифрования с тем же алгоритмом (реверсирование структуры).

## 44. Основные характеристики DES

* Блок 64 бита, ключ 56 бит (на практике 64 бита, но 8 используются для чётности).
* 16 раундов, основанных на **сети Фейстеля**.
* Устаревший по причине малого размера ключа, часто заменяется на 3DES или AES.

## 45. Схема DES: начальная перестановка, раунды

* **Initial Permutation (IP)** — перестановка бит перед началом раундов.
* 16 раундов сети Фейстеля: в каждом формируются подтключи и выполняется функция F (S-блоки, перестановка).
* **Inverse IP** — завершающая перестановка для получения зашифрованного блока.

## 46. Основные характеристики AES

* Блок 128 бит, ключ 128/192/256 бит, разное число раундов (10/12/14).
* Быстрый, эффективен на широком спектре платформ, хорошо исследован на криптостойкость.
* Использует операции над полем GF() (операции «SubBytes», «MixColumns» и т.д.).

## 47. Раунды алгоритма AES: SubBytes, ShiftRows, MixColumns, AddRoundKey

1. **SubBytes** — замена каждого байта по нелинейной S-Box.
2. **ShiftRows** — циклический сдвиг строк в матрице состояния.
3. **MixColumns** — умножение столбцов матрицы состояния в поле GF() (пропускается в последнем раунде).
4. **AddRoundKey** — побитовое XOR состояния с подключом.

## 48. Криптостойкость AES

* При ключе 128 бит полный перебор составляет операций, что пока считается недостижимым.
* Нет практических атак, позволяющих взломать AES быстрее перебора.
* При более длинных ключах (192/256 бит) стойкость ещё выше.

## 49. Алгоритм IDEA

* **International Data Encryption Algorithm**, блок 64 бита, ключ 128 бит.
* Состоит из 8 идентичных раундов и заключительной трансформации, использует **операции модульного умножения**, сложения по модулю и XOR.
* Разработан как замена DES, патент был в Европе и США (срок действия патента истёк).

## 50. Основные характеристики и операции алгоритма IDEA

* Блок: 64 бита, ключ: 128 бит, 8 раундов + выводной раунд.
* Операции в каждом раунде:
  1. Деление блока на 4 части по 16 бит.
  2. Модульное умножение (по ), сложение по модулю , XOR.
  3. Перестановки для следующего шага.
* Обеспечивает хорошую криптостойкость, но менее распространён, чем AES.

## 51. Локальный администратор безопасности

* Специалист/учётная запись с правами на администрирование безопасности в конкретной системе или узле (компьютере).
* Отвечает за установку и настройку программ защиты, управление локальными политиками, мониторинг событий безопасности.
* Может иметь ограниченные полномочия по сравнению с глобальным (доменным) администратором.

## 52. Центр аутентификации

* Служба/компонента, проверяющая подлинность субъектов (пользователей, устройств) при их входе в систему.
* Пример: **Kerberos KDC** (Key Distribution Center), проверяет билеты TGT, выдаёт сервис-билеты.
* Может быть частью инфраструктуры PKI, где используется CA для выпуска сертификатов.

## 53. Диспетчер учетных записей

* Утилита или служба, управляющая созданием, изменением, удалением, блокировкой учётных записей пользователей и групп.
* В Windows это может быть **Local Users and Groups**, в домене – **Active Directory Users and Computers**.
* Обеспечивает безопасность путём настройки паролей, групповых политик, прав и разрешений.

## 54. Монитор безопасности

* ПО или служба, которая **отслеживает события** в системе (журналы, действия пользователей, сетевой трафик), оповещает о подозрительной активности.
* Может быть частью **SIEM** (Security Information and Event Management) — агрегирует и анализирует логи из разных источников.
* Цель: быстрое обнаружение инцидентов, формирование отчётов и алертов.

## 55. Механизмы контроля доступа и аутентификации

* Модели контроля: **DAC** (дискреционная), **MAC** (мандатная), **RBAC** (ролевая), **ABAC** (атрибутивная).
* Методы аутентификации: **по знаниям** (пароль), **по владению** (токен, смарт-карта), **по биометрии**.
* Основные принципы: **минимальные привилегии**, разделение обязанностей, подтверждение личности.

## 56. Слабости парольных протоколов аутентификации

* Угрозы: **брутфорс**, перехват хэша, фишинг.
* Слабые пароли, повторное использование паролей, отсутствие соли при хранении хэшей.
* Меры: многофакторная аутентификация, сложные пароли, защита хранимых хэшей (bcrypt, PBKDF2, Argon2).

## 57. Виды атак и угроз для протоколов аутентификации

* **Перехват сеанса** (session hijacking).
* **Replay-атаки** (повтор ранее перехваченного трафика).
* **MITM** (подмена конечной точки).
* **Phishing** (выманивание паролей).
* Защита: использование TLS, nonce, одноразовых токенов, 2FA.

## 58. Базовые технологии безопасности информационных систем

* **Шифрование** (конфиденциальность), **ЭЦП** (целостность, неотказуемость).
* **Межсетевые экраны** и **IDS/IPS**, антивирусы.
* **Резервное копирование**, **управление доступом** (ACL, RBAC).
* **Аудит, мониторинг**, системное обновление.

## 59. Идентификация, аутентификация и авторизация. Определения, отличия и сходство

* **Идентификация**: субъект сообщает свои данные (логин, ID).
* **Аутентификация**: проверка, действительно ли субъект владеет заявленной идентификацией (пароль, сертификат, биометрия).
* **Авторизация**: предоставление или ограничение прав доступа к ресурсам после успешной аутентификации.
* Все три — части единого процесса контроля доступа.

## 60. Аудит информационной безопасности. Методы проведения аудита информационной безопасности

* **Аудит ИБ** — оценка соответствия системы требованиям (стандартам, политикам, законам).
* Методы: анализ документации, интервью с персоналом, инструментальное тестирование (сканирование уязвимостей, пентесты), наблюдение.
* Результат: отчёт с **выявленными несоответствиями**, рекомендациями по устранению.