ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лекция 1:

«Введение в дисциплину. Основы государственной политики РФ в информационной сфере»

Вопросы:

1. Введение в дисциплину.
2. Национальная безопасность РФ.
3. Национальные интересы РФ в информационной сфере и их обеспечение.
4. Основные информационные угрозы и задачи обеспечения информационной безопасности.
5. Роль специалиста по защите информации.

Вопрос 1: «Введение в дисциплину»

- **Цель дисциплины – изучение:**
- **принципов** обеспечения информационной безопасности,
- **подходов к анализу угроз** информационной инфраструктуры,
- **основных понятий** в области **информационной безопасности (ИБ)** и решения задач **защиты информации (ЗИ)** в информационных системах **(ИС).**

В результате изучения дисциплины студенты (слушатели) должны:

- **иметь представление:**
- о целях, задачах, принципах и основных направлениях обеспечения информационной безопасности;
- о методологии создания систем ЗИ;
- о перспективных направлениях развития средств и методов ЗИ;

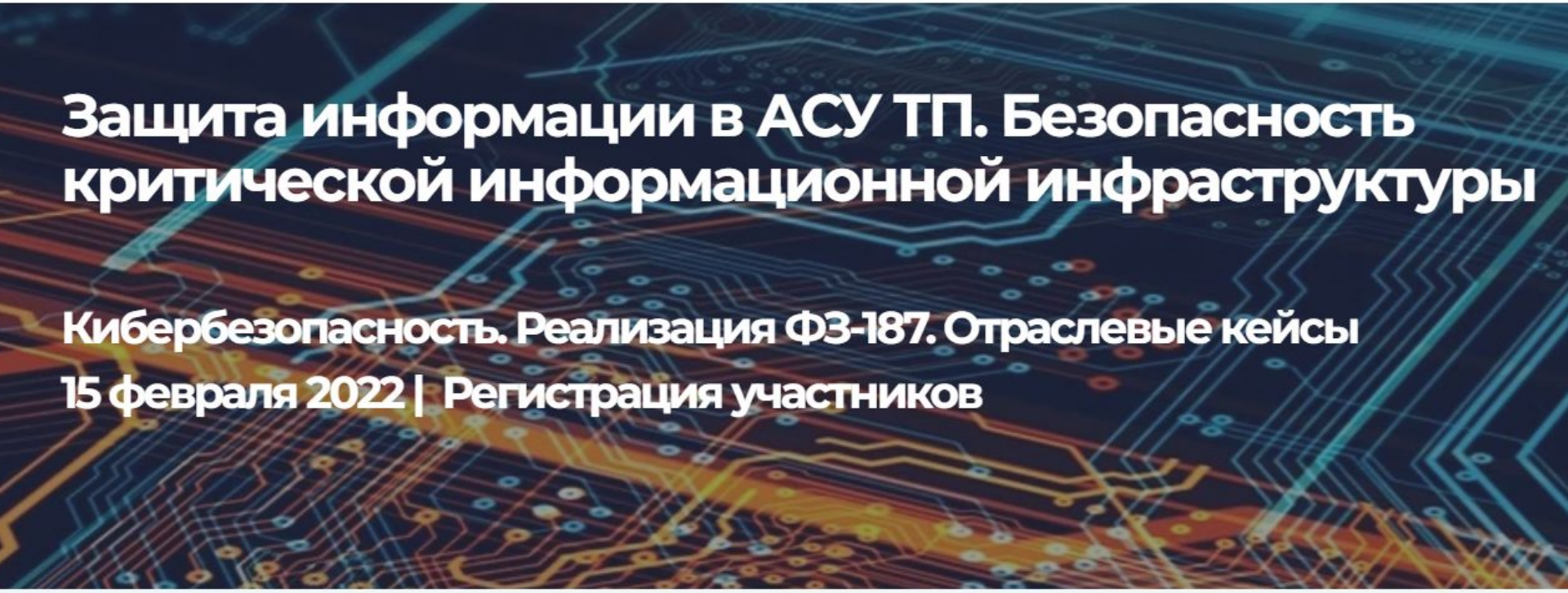
- **знать:**
- роль и место ИБ в системе национальной безопасности страны;
- угрозы ИБ государства;
- содержание информационной войны, методы и средства ее ведения;
- современные подходы к построению систем ЗИ;
- ИС как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее ИБ;
- особенности обеспечения ИБ компьютерных систем при обработке информации;

- **уметь:**
- выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств ЗИ;
- пользоваться современной научно-технической информацией по вопросам ЗИ;
- применять полученные знания при выполнении курсовых проектов и ВКР, а также в ходе научных исследований;
- **иметь навыки:**
- анализа информации для организации защиты информации от актуальных угроз безопасности;
- формальной постановки и решения задачи обеспечения ИБ компьютерных систем.

Основная литература

Дополнительная литература

- **Основы информационной безопасности.** Учебное пособие для вузов / Е.Б. Белов и др. - М.: Горячая линия - Телеком, 2006.
- **Основы информационной безопасности:** учебное пособие / А. Н. Данилов, С. А. Данилова, А. А. Зорин. - Пермь: Изд-во ПГТУ, 2008.
- Ярочкин В. И. **Информационная безопасность информационных систем**. М: Гаудемаус, 2006.



ОТРАСЛЬ

Клиенты Solar JSOC смогут контролировать работу всех сервисов в едином личном кабинете

Европарламент запретит агрессивную интернет-рекламу

УГРОЗЫ

Исходный код вредоноса BotenaGo опубликован на GitHub

Аресты участников группировки REvil никак не сказались на ее активности

ПРЕСТУПЛЕНИЯ

Уязвимость в Microsoft Outlook позволила хакерам обойти защиту электронной почты

Хакеры атаковали чиновников и оборонные компании в Западной Азии

Информзащита
Учебный центр

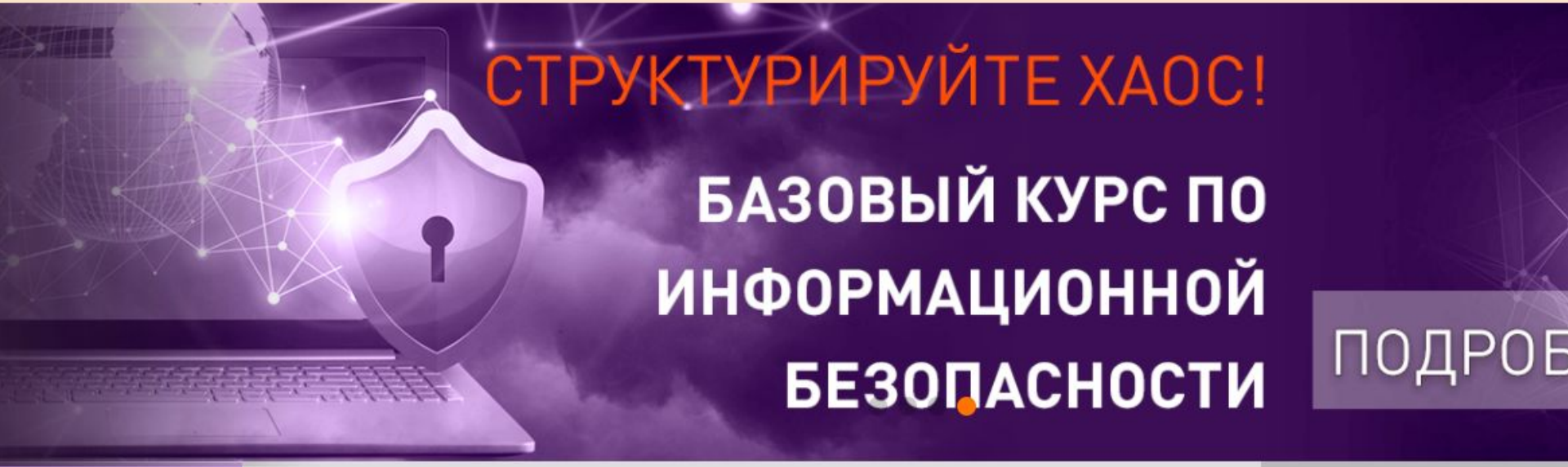
+7 (495) 980 23 45 (*04)
edu@itsecurity.ru

УЧЕБНЫЙ ПОРТАЛ

КАЗАТЬ ЗВОНОК

Найти на сайте

КАТАЛОГ КУРСОВ | РАСПИСАНИЕ | ПОВЫШЕНИЕ ОСВЕДОМЛЕННОСТИ | УЧЕБНЫЙ ЦЕНТР | КОНТАКТ



НАПРАВЛЕНИЕ

ВЕНДОР

ЕЩЕ ФИЛЬТРЫ

- Авторизованное обучение
- Базовые курсы по информационной безопасности
- Безопасность IT инфраструктуры
- Безопасность прикладных систем
- Защита информации от утечек по техническим каналам
- Защита персональных данных/критической информационной инфраструктуры/государственных информационных систем
- Курсы по требованиям регуляторов
- Обучение по технологиям ЭП и PKI
- Программы переподготовки
- Экономическая и кадровая безопасность

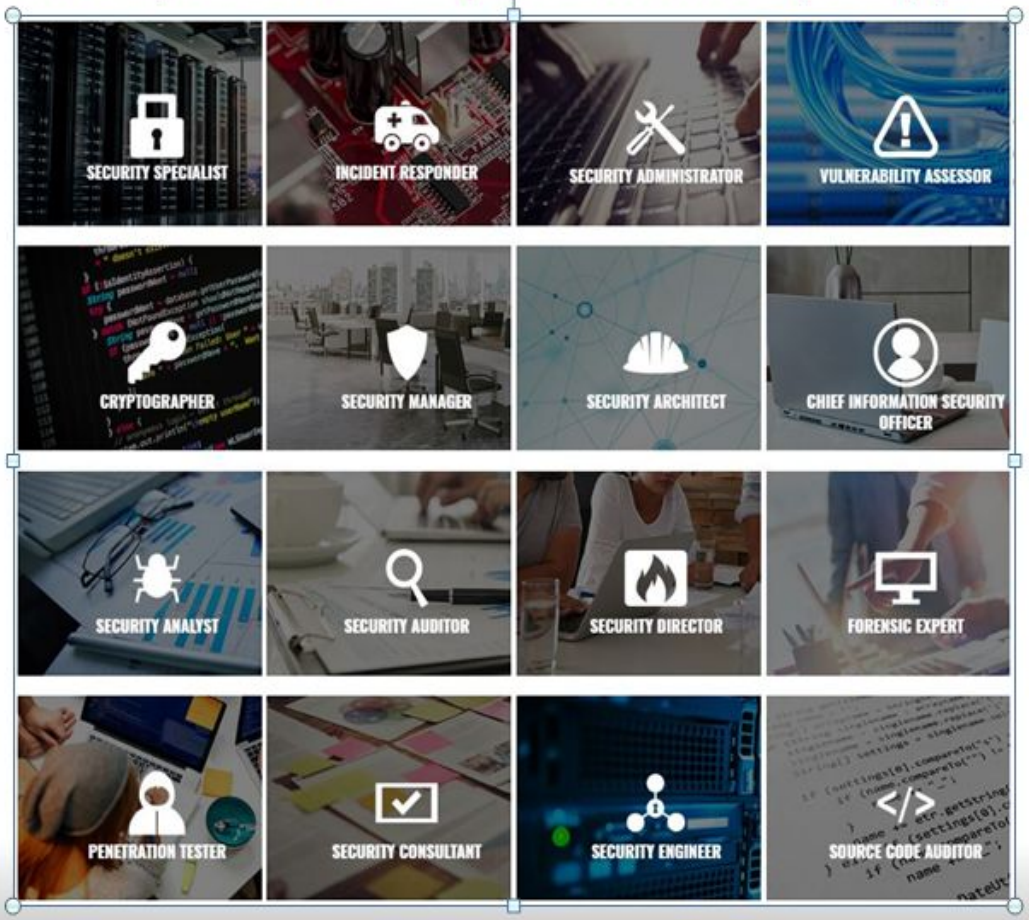
ПОКАЗАТЬ

ПОМОЖЕМ ПО

Email или номер телефона

Ваш вопрос

Интересные зарубежные ресурсы



CYBER SECURITY EDUCATION

www.cybersecurityeducation.org

Информзащита
Учебный центр

Полезные ресурсы для поддержания тонуса

- **Новостные ленты по ИБ**
  - Security Lab https://www.securitylab.ru/
  - Threatpost https://threatpost.ru/
  - Anti-Malware https://www.anti-malware.ru/
  - Сайт ассоциации BISA https://bis-expert.ru/
  - Dark Reading http://www.darkreading.com/
  - Help Net Security https://www.helpnetsecurity.com/

Вопрос 2: «Национальная безопасность Российской Федерации»

Указ Президента Российской Федерации

от 31 декабря 2015 года **N 683**

«О Стратегии национальной безопасности Российской Федерации»

- основа государственной политики в сфере обеспечения национальной безопасности

Национальная безопасность включает в себя

- оборону страны и все виды безопасности, предусмотренные Конституцией РФ и законодательством РФ, прежде всего государственную, общественную, информационную, экологическую, экономическую, транспортную, энергетическую безопасность, безопасность личности…


Оборона страны
Государственная и общественная безопасность
Повышение качества жизни российских граждан
СТРАТЕГИЧЕСКИЕ НАЦИОНАЛЬНЫЕ ПРИОРИТЕТЫ
Экология живых систем и рациональное природопользование
Наука, технологии, образование, здравоохранение и культура
Экономический рост
Стратегическая стабильность и равноправное стратегическое партнерство

К основным угрозам государственной и общественной безопасности относятся

- **разведывательная и иная деятельность** специальных служб и организаций иностранных государств, отдельных лиц, наносящая ущерб национальным интересам;
- **нарушения безопасности и устойчивости функционирования** критической информационной инфраструктуры РФ;
- **деятельность, связанная с использованием информационных и коммуникационных технологий** для распространения и пропаганды идеологии фашизма, экстремизма, терроризма и сепаратизма, нанесения ущерба гражданскому миру, политической и социальной стабильности в обществе…

В целях обеспечения государственной и общественной безопасности

- **укрепляется режим безопасного функционирования** критически важных и потенциально опасных объектов;
- **совершенствуется система выявления и анализа угроз в информационной сфере**, противодействия им;
- принимаются меры для **повышения защищенности граждан и общества от деструктивного информационного воздействия** со стороны экстремистских и террористических организаций, иностранных специальных служб и пропагандистских структур;

Повышение качества жизни российских граждан

- Для противодействия угрозам качеству жизни граждан органы государственной власти и органы местного самоуправления во взаимодействии с институтами гражданского общества:
- обеспечивают развитие информационной инфраструктуры, **доступность информации** по различным вопросам социально-политической, экономической и духовной жизни общества, равный доступ к государственным услугам на всей территории РФ, в том числе **с использованием информационных и коммуникационных технологий**;

Экономический рост

- К главным стратегическим угрозам национальной безопасности в области экономики, относится **уязвимость ее информационной инфраструктуры**.
- Важнейший фактор обеспечения экономической безопасности - **стабильность функционирования и развития финансовой системы, повышение ее защищенности.**

Наука, технологии, образование, здравоохранение и культура

- Одно из главных направлений обеспечения национальной безопасности в области науки, технологий и образования - повышение уровня **технологической безопасности, в том числе в информационной сфере.**
- **Угрозами национальной безопасности в области культуры являются** … пропаганды вседозволенности и насилия, расовой, национальной и религиозной нетерпимости, а также снижение роли русского языка в мире, качества его преподавания в России и за рубежом, **попытки фальсификации российской и мировой истории…**

Вопрос 3: «Национальные интересы РФ в информационной сфере и их обеспечение»

Информационные отношения

Безопасность – гарантия информационных отношений

Доктрина информационной безопасности Российской Федерации от 5 декабря 2016 г. № Пр-646

- **Информационная безопасность РФ -** состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие РФ, оборона и безопасность государства.

Успешному решению вопросов обеспечения информационной безопасности РФ способствуют:

Национальными интересами в информационной сфере являются:

Вопрос 4: «Основные информационные угрозы и задачи обеспечения ИБ»

Негативные факторы, влияющие на состояние информационной безопасности (УГРОЗЫ):

1. Наращивание рядом зарубежных стран возможностей **информационно-технического воздействия** на информационную инфраструктуру в военных целях;

2. Расширение масштабов использования **информационно-психологического воздействия**;

3. Увеличение в зарубежных СМИ объема материалов, содержащих **предвзятую оценку государственной политики** РФ;

4. Информационное воздействия террористическими и экстремистскими организациями **на индивидуальное, групповое и общественное сознание**;

5. Увеличение масштабов **компьютерной преступности**, прежде всего **в кредитно-финансовой сфере;**

6. Увеличение числа преступлений, связанных с **нарушением конституционных прав и свобод человека и гражданина**, при обработке **персональных данных**;

7. Увеличение масштабов применения **информационных технологий в военно-политических целях**, направленных на подрыв суверенитета, политической и социальной стабильности, территориальной целостности РФ и ее союзников;

8. Постоянное повышение сложности, увеличение масштабов и рост скоординированности **компьютерных атак на объекты критической информационной инфраструктуры;**

9. Высокий уровень **зависимости** отечественной промышленности от зарубежных информационных технологий;

10. Недостаточная эффективность научных исследований, направленных на создание перспективных информационных технологий, **низкий уровень внедрения отечественных разработок** и **недостаточное кадровое обеспечение** в области ИБ, а также **низкая осведомленность граждан** в вопросах обеспечения **личной ИБ**;

11. Стремление отдельных государств использовать технологическое превосходство для доминирования в информационном пространстве;

12. Отсутствие международно-правовых норм, регулирующих межгосударственные отношения в информационном пространстве, а также механизмов и процедур их применения.

Основные направления обеспечения информационной безопасности

В области обороны страны:

- стратегическое сдерживание и **предотвращение военных конфликтов;**
- **совершенствование системы обеспечения ИБ** ВС РФ;
- прогнозирование, обнаружение и **оценка информационных угроз**;
- содействие обеспечению **защиты интересов союзников РФ** в информационной сфере;
- нейтрализация **информационно-психологического воздействия.**

В области государственной и общественной безопасности:

- противодействие использованию **информационных технологий для пропаганды экстремистской идеологии**;
- пресечение деятельности, наносящей ущерб, осуществляемой с **использованием тех. средств и информационных технологий спец. службами** и организациями иностранных государств;
- **повышение защищенности критической информационной инфраструктуры**;
- повышение **безопасности функционирования объектов информационной инфраструктуры;**

- повышение эффективности **профилактики правонарушений**, совершаемых с использованием информационных технологий;
- обеспечение защиты информации, содержащей **сведения, составляющие государственную тайну**, иной информации ограниченного доступа;
- совершенствование методов и способов **производства и безопасного применения продукции, оказания услуг на основе ИТ** с использованием отечественных разработок;
- повышение **эффективности информационного обеспечения реализации государственной политики** РФ;
- **нейтрализация информационного воздействия**, направленного на размывание духовно-нравственных ценностей.

В экономической сфере:

- инновационное развитие **отрасли ИТ и электронной промышленности;**
- **ликвидация зависимости** отечественной промышленности от зарубежных ИТ и средств обеспечения ИБ;
- **повышение конкурентоспособности российских компаний**, осуществляющих разработку ИТ, производство и эксплуатацию средств обеспечения ИБ, оказывающих услуги в области обеспечения ИБ;
- **развитие отечественной конкурентоспособной электронной компонентной базы и технологий** производства электронных компонентов, обеспечение потребности внутреннего рынка в такой продукции и выхода этой продукции на мировой рынок.

В области науки, технологий и образования:

- достижение **конкурентоспособности российских ИТ** и развитие научно-технического потенциала в области обеспечения ИБ;
- создание и внедрение ИТ, изначально **устойчивых к различным видам воздействия**;
- **проведение научных исследований** и осуществление опытных разработок в целях создания перспективных ИТ и средств обеспечения ИБ;
- **развитие кадрового потенциала в области обеспечения ИБ и применения ИТ;**
- обеспечение **защищенности граждан от информационных угроз**, в том числе за счет формирования **культуры личной ИБ.**

В области стратегической стабильности и равноправного стратегического партнерства:

- **защита суверенитета РФ в информационном пространстве** посредством осуществления самостоятельной и независимой политики в информационной сфере;
- участие в формировании **системы международной ИБ;**
- **создание международно-правовых механизмов**, учитывающих специфику информационных технологий в информационном пространстве;
- **продвижение** в рамках деятельности международных организаций **позиции РФ**;
- **развитие национальной системы управления** российским сегментом сети «Интернет».

ФСТЭК России

Федеральная служба по техническому и экспортному контролю

Ключевые слова

Административный регламент	21
Закон	32
Информационный материал	213
Методический документ	33
Официальное мероприятие	498
Перечень обязательных требований	34
План	26
Положение	1
Постановление	56
Приказ	156
Проект	15
Реестр / перечень / список	54
Резолюция	8
Руководящий документ	13
Указ	44
Форма / бланк	4

Территориальные органы

Новости

Со… …осмотров: 115261

Инфор…

Об обно… …сертификации средств защиты информации и аттестации объектов информатизации

Информационный материал

Создано: 22 декабря 2021 г. 13:50 Просмотров: 2245

Заседание Координационного совета 22 декабря 2021 г., г. Екатеринбург

По вопросам обеспечения безопасности значимых объектов критической информационной инфраструктуры Уральского федерального округа

3-4 февраля 2022 | здание Правительства г. Москвы

Большой Национальный форум информационной безопасности ИНФОФОРУМ-2022

ПРОГРАММА УСЛОВИЯ УЧАСТИЯ

2 дня событий

2000+ участников

100+ докладов

+ онлайн-трансляция

ГОСУДАРСТВЕННАЯ ДУМА

АППАРАТ СОВЕТА БЕЗОПАСНОСТИ РФ

МИНЦИФРЫ РОССИИ

ИНФОФОРУМ-2022: тематические направления

1. **Искусственный интеллект: вопросы ИБ.**
2. **Информационный суверенитет и международная ИБ.**
3. **Российский бизнес шаг за шагом к цифровой независимости.**
4. **Вопросы обеспечения безопасности КИИ и противодействия компьютерным инцидентам.**
5. **ИБ как сервис. Отраслевые особенности центров мониторинга ИБ.**

6. **Облачные технологии и большие данные. Преодоление рисков ИБ.**
7. **Цифровая трансформация, импортозамещение и ИБ: успехи, состояние, задачи.**
8. **Сети связи. Обеспечение целостности, устойчивости функционирования и безопасности сетей связи общего пользования.**
9. **ПРАКТИКО-ОРИЕНТИРОВАННОЕ ОБРАЗОВАНИЕ.**
10. **СМИ и информационная безопасность.**
11. **Финтех (FinTech) и проблемы ИБ.**

Вопрос 5: «Роль специалиста по защите информации в обеспечении национальной безопасности государства»

- **Область профессиональной деятельности специалистов по защите информации** включает сферы науки, техники и технологии, охватывающие **совокупность проблем, связанных с обеспечением информационной безопасности социально-технических и информационных систем** в условиях существования угроз в инфс сфере.

6 437 вакансий «Информационная безопасность»

Подработка Свежие Сменный график Удаленная работа Нет опыта

По соответствию За всё время

Постоянная работа

Подработка

Исключить слова

Уровень дохода руб.

- Не имеет значения
- от 65 000 руб. *1 433*
- от 120 000 руб. *743*
- от 180 000 руб. *326*
- от 235 000 руб. *169*
- от 290 000 руб. *79*
- Своя зарплата

Главный эксперт по кибербезопасности (защита систем корпоративного блока)

Сбер. Экспертам и руководителям
Москва

Проработка и внедрение решений для обеспечения кибербезопасности продуктов и процессов корпоративного бизнеса Банка по всем пре областям **информационной безопасности**.
...**информационных** технологий с учетом банковской специфики. Навыки управления рисками **информационной безопасности**. Знание применения лучших практик обеспечения **информационной безопасности**.

Откликнуться

Специалист по информационной безопасности

от 150 000 руб.

inDriver
Москва, Белорусская

Информационная безопасность
Найти

Вакансии Резюме Компании

100 вакансий «Информационная безопасность»

Подработка Свежие Сменный график Удаленная работа Нет опыта

По соответствию За всё время

Постоянная работа

Подработка

Исключить слова

Уровень дохода руб.

- Не имеет значения
- от 40 000 руб. *26*
- от 65 000 руб. *14*
- от 85 000 руб. *8*
- от 110 000 руб. *6*
- от 130 000 руб. *5*
- Своя зарплата

от

Указан доход *39*

Регион

Пермь *100*

Специалист по информационной безопасности

ЗАО Почтобанк, АКИБ
Пермь

Отклик без резюме Будьте первыми

...области **информационной безопасности**. Настройка функционирования аппаратных средств **защиты информации**, проведение регламентных работ. Разработка локальных нормативно-правовых актов, касающихся **информационной безопасности**.
Техническое образование. Знания в настройке различных программных средств для работы с электронной цифровой подписью. Опыт настройки антивирусных систем.
Информационная безопасность, Технические средства **информационной** защиты, Внедрение систем **информационной безопасности**

Откликнуться Показать контакты

Специалист по информационной безопасности

50 000 – 70 000 руб.

ООО Меридиан
Пермь

Отклик без резюме Будьте первыми

Участвовать в расследовании инцидентов **информационной безопасности**. Обеспечивать функционирование и контроль работоспособности программного и аппаратного обеспечения, системы (средств) **защиты информации**.
Знания принципов **информационной безопасности**, моделей угроз. Опыт работы с активным сетевым оборудованием (маршрутизаторы, коммутаторы). Аналитический склад ума. Наличие профильных сертификатов

Типовые роли специалистов по ЗИ

- **Руководитель**
  - организация работ по созданию системы защиты и состояние безопасности
- **Аналитик**
  - определение требований к защищенности и разработку необходимых НМД по вопросам ЗИ
- **Аудитор**
  - контроль текущего состояния системы защиты на предмет соответствия ее заявленным целям
- **Администратор средств защиты**
  - сопровождение штатных и дополнительных средств защиты
- **Специалист по работе с пользователями**
  - реализация и контроль исполнения регламентов

Чего хотят работодатели (пример вакансии с hh.ru)

- Анализ информационных рисков компании
- Выявление возможных каналов утечки
- Разработка организационно-распорядительных документов
- Организация и координация работ, проводимых в рамках обеспечения ИБ
- Проведение аудита состояния ИБ
- Установка, настройка и сопровождение технических средств защиты
- Защита локальных компьютерных сетей от вирусных атак и взломов

- Участие в реализации требований 382-П, комплекса стандартов СТО БР ИББС
- Разработка нормативных документов по информационной безопасности
- Проведение внутренних аудитов по ИБ
- Контроль соблюдения требований информационной безопасности
- Выявление и расследование инцидентов ИБ
- Проведение обучения и проверки знаний сотрудников по вопросам ИБ
- Эксплуатация системы выявления утечек информации
- Эксплуатация средств СКЗИ, защиты от вредоносного ПО
- Управление межсетевым экраном, ключевой инфраструктурой PKI

Код	Направление/Специальность (10.00.00)	Квалификация
СРЕДНЕЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАНИЕ		
10.02.01	Организация и технология защиты информации	Техник по защите информации
10.02.02	Информационная безопасность телекоммуникационных систем	
10.02.02	Информационная безопасность автоматизированных систем	
ВЫСШЕЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАНИЕ		
10.03.01	Направление «Информационная безопасность»	Бакалавр
10.04.01	Направление «Информационная безопасность»	Магистр
10.05.01	Компьютерная безопасность	Специалист по защите информации
10.05.02	Информационная безопасность телекоммуникационных систем	
10.05.03	Информационная безопасность автоматизированных систем	
10.05.04	Информационно-аналитические системы безопасности	
10.05.05	Безопасность информационных технологий в правоохранительной сфере	
10.05.06	Криптография	
10.05.07	Противодействие техническим разведкам	
10.06.01	Информационная безопасность	Исследователь (преподаватель-исследователь)

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лекция 2:

«Основные понятия, общеметодологические принципы теории информационной безопасности»

Вопросы:

1. **Основные понятия информационной безопасности.**
2. **Общеметодологические принципы теории информационной безопасности.**

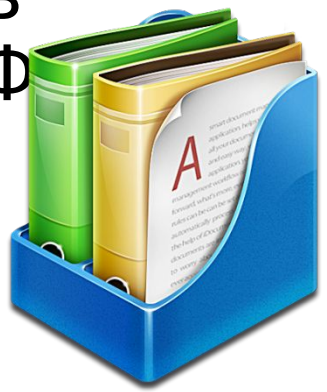
Вопрос 1: «Основные понятия информационной безопасности»

- **Понятие** – это форма мышления, мысль о предмете, выражающая его существенные признаки (***Логика***)
- **Основные понятия информационной безопасности:**
  - **информация;**
  - **безопасность информации;**
  - **конфиденциальность информации;**
  - **целостность информации;**
  - **доступность информации;**
  - **защита информации и т.д.**

Основные источники понятий в области информационной безопасности

Федеральный закон № 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и защите информации»

- **Информация** - сведения (сообщения, данные) независимо от формы их представления.
- **Документированная информация** - зафиксированная на **материальном носителе** путем документирования **информация** с реквизитами, позволяющими определить такую информацию или в установленных законодательством РФ случаях ее материальный носитель.



ГОСТ Р 53113.1-2008 ИТ. Защита информационных технологий и АС от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения

- **Информационная безопасность (information security):** Все аспекты, связанные с определением, достижением и поддержанием **конфиденциальности, целостности, доступности**, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки.

Основные критерии защиты информации

- **Безопасность информации (данных):** Состояние защищенности информации (данных), при котором обеспечены ее (их) **конфиденциальность, доступность и целостность.**
  - *(ГОСТ Р 50922-2006)*

- **Конфиденциальность информации** - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Руководящий документ. Защита от несанкционированного доступа к информации Термины и определения

- **Целостность информации** (Information integrity) - способность средства вычислительной техники или АС обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения).

Рекомендации по стандартизации «Информационные технологии. Основные термины и определения в области технической защиты информации» (Р 50.1.053-2005).

- **Доступность** (информации (англ. availability) - состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать их беспрепятственно.
- **К правам доступа относятся:** право на чтение, изменение, копирование, уничтожение информации, а также права на изменение, использование, уничтожение ресурсов.

- **Защита информации** представляет собой принятие **правовых**, **организационных** **и технических** **мер**, направленных на:
  1) обеспечение защиты информации от **неправомерного доступа**, **уничтожения, модифицирования, блокирования, копирования, предоставления, распространения,** а также от иных неправомерных действий в отношении такой информации;
  2) соблюдение **конфиденциальности** информации ограниченного доступа;
  3) реализацию права на **доступ** к информации.

ГОСТ Р 50922-2006 Государственный стандарт Российской Федерации. Защита информации. Основные термины и определения

- **Защита информации** (ЗИ) - деятельность, направленная на предотвращение:
- **утечки защищаемой информации**,
- **несанкционированных и непреднамеренных воздействий** на защищаемую информации.

- **Несанкционированное воздействие на информацию:** Воздействие на защищаемую информацию **с нарушением установленных прав и (или) правил доступа**, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

- **Средство защиты информации** - техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.
- **Способ защиты информации** - порядок и правила применения определенных принципов и средств защиты информации.

- **Защита информации от утечки** - деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее **разглашения, несанкционированного доступа** к информации и **получения защищаемой информации разведками**.

- **Защита информации от несанкционированного воздействия** (защита информации от НСВ) - деятельность, направленная на предотвращение воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящего к ее искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

- **Защита информации от непреднамеренного воздействия** - деятельность, направленная на предотвращение воздействия на защищаемую информацию **ошибок ее пользователя**, сбоя технических и программных средств информационных систем, **природных явлений** или иных нецеленаправленных на изменение информации мероприятий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

- **Защита информации от несанкционированного доступа** (защита информации от НСД) - деятельность, направленная на предотвращение получения защищаемой информации **заинтересованным субъектом с нарушением установленных** правовыми документами или собственником, владельцем информации **прав или правил** доступа к защищаемой информации.

- **Защита информации от разглашения -** деятельность, направленная на предотвращение несанкционированного доведения защищаемой информации до потребителей, не имеющих права доступа к этой информации.

- **Система защиты информации** – совокупность:
  - **органов и (или) исполнителей,**
  - **используемой ими техники защиты информации,**
  - **а также объектов защиты,**
- организованная и функционирующая **по правилам, установленным** соответствующими правовыми, организационно-распорядительными и **нормативными документами** в области защиты информации.

Вопрос 2: «Общеметодологические принципы теории информационной безопасности»

1) системности;
2) комплексности;
3) своевременности;
4) непрерывности защиты;
5) разумной достаточности;
6) гибкости;
7) специализации;
8) планирования;
9) совершенствования;
10) централизации и управления;
11) активности;
12) экономической эффективности;
13) простоты применяемых защитных мер и средств.

1. ПРИНЦИП СИСТЕМНОСТИ

- Предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности.
- **Системный подход.**

2. ПРИНЦИП КОМПЛЕКСНОСТИ

- СЗИ должна включать совокупность объектов защиты, сил и средств, принимаемых мер, проводимых мероприятий и действий по обеспечению безопасности **всеми доступными законными средствами, методами и мероприятиями.**
- Зашита должна строиться **эшелонированно.**

3. ПРИНЦИП СВОЕВРЕМЕННОСТИ

- Меры защиты должны реагировать **своевременно.**
- Организационные и правовые меры должны предприниматься **заблаговременно.**

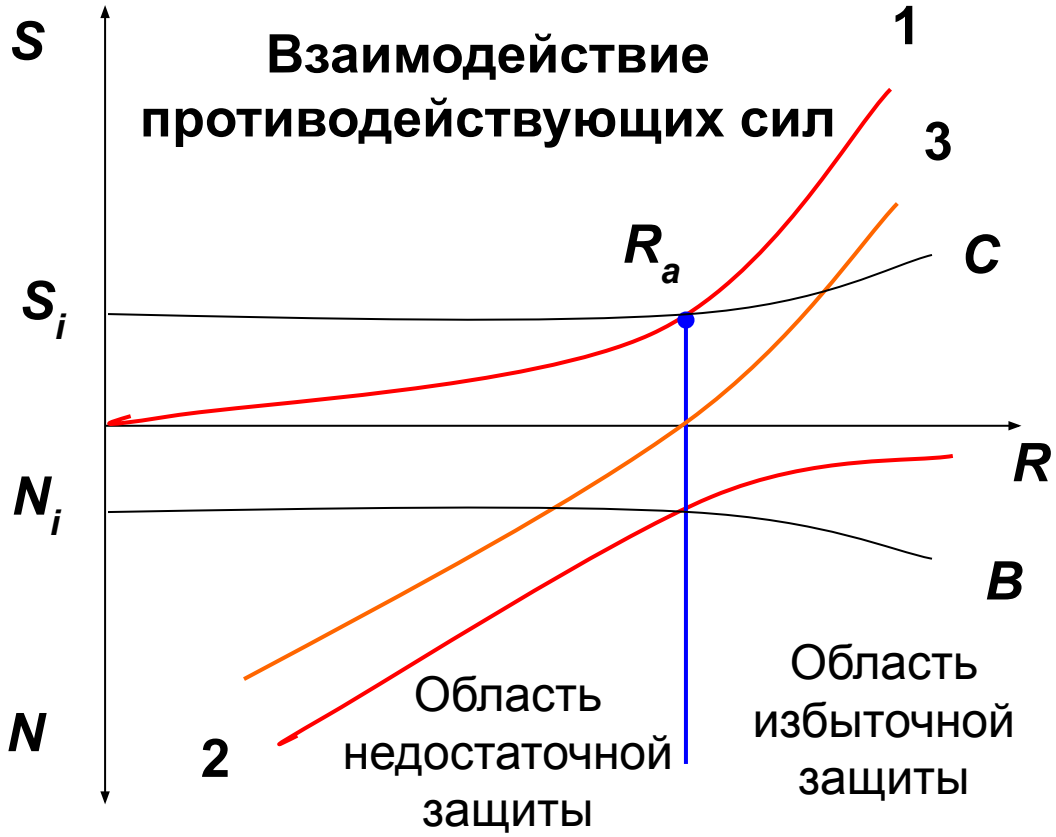
4. ПРИНЦИП НЕПРЕРЫВНОСТИ

- Защита информации - непрерывный целенаправленный процесс.
- **Принятие соответствующих мер на всех этапах жизненного цикла систем**, начиная с самых ранних стадий проектирования, а не только на этапе их эксплуатации.
- Подчеркивает **недопустимость перерывов в работе средств защиты**, устанавливая повышенные требования к их надежности.

5. ПРИНЦИП РАЗУМНОЙ ДОСТАТОЧНОСТИ

- Важно правильно выбрать тот **достаточный уровень защиты**, при котором затраты, риск и размер возможного ущерба были бы приемлемыми (задача анализа риска).
- Для обеспечения возможности варьирования уровня защищенности средства защиты должны обладать определенной **гибкостью**.

Разумная достаточность защищенности



- ***ось S*** — защищенность;
- ***ось N*** — реализация угроз;
- ***ось R*** — уровень экономического развития предприятия;
- ***Ra*** — состояние, при котором защищенность предприятия ***Si*** такова, что отражает все угрозы ***Ni***

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лекция 3:

«Понятие и виды информации ограниченного доступа»

Вопросы:

1. **Понятие и сущность информации ограниченного доступа.**
2. **Виды информации ограниченного доступа.**
3. **Понятие интеллектуальной собственности.**

Вопрос 1: «Понятие и сущность информации ограниченного доступа»

- **Информация ограниченного доступа** - информация, доступ к которой ограничен федеральными законами.
  - ***ФЗ № 149-ФЗ от 27.07. 2006 г. «Об информации, информационных технологиях и защите информации»***

Обладатель информации вправе:

- **разрешать или ограничивать доступ** к информации, определять порядок и условия такого доступа;
- **использовать информацию**, в том числе распространять ее, по своему усмотрению;
- **передавать информацию другим лицам по договору** или на ином установленном законом основании;
- **защищать установленными законом способами свои права** в случае незаконного получения информации или ее незаконного использования иными лицами;
- **осуществлять иные действия с информацией** или разрешать осуществление таких действий.

Обладатель информации обязан:

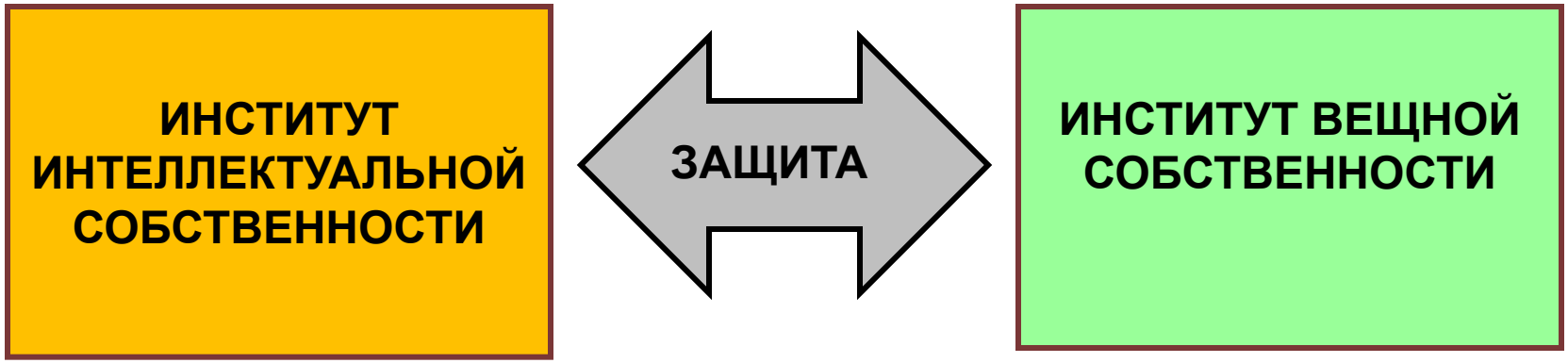
1. Соблюдать права и законные интересы иных лиц.
2. Принимать меры по защите информации.
3. Ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Обладатель информации, оператор ИС обязан обеспечивать:

1. **Предотвращение НСД к информации;**
2. **Обнаружение фактов НСД к информации;**
3. **Предупреждение возможности последствий нарушения порядка доступа;**
4. **Недопущение воздействия на ТС обработки информации с нарушением функционирования;**
5. **Возможность восстановления информации, модифицированной вследствие НСД к ней;**
6. **Постоянный контроль за обеспечением УЗ;**
7. **Нахождение на территории РФ БД ПДн граждан РФ.**

Особенности защиты документированной информации

- **Двуединство информации и материального носителя** дает возможность защищать документированную информацию с использованием одновременно двух институтов:



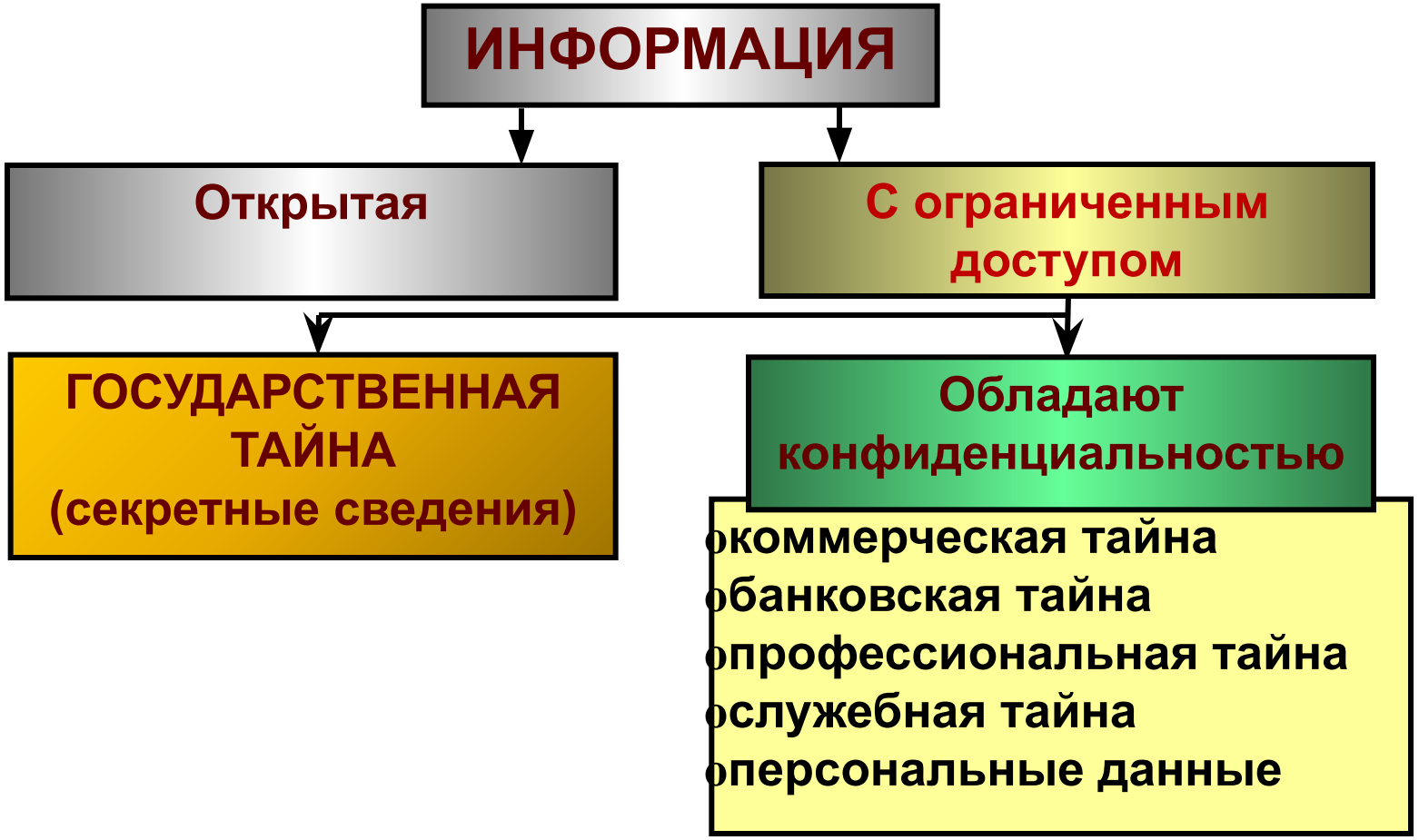
Особенности доступа к информации

- Информация **в зависимости от категории доступа** к ней подразделяется на:
  - общедоступную информацию;
  - информацию, доступ к которой ограничен федеральными законами (**информация ограниченного доступа**).

Ограничение доступа к информации

- Ограничение доступа к информации **устанавливается федеральными законами** в целях:
  - защиты основ конституционного строя,
  - нравственности,
  - здоровья,
  - прав и законных интересов других лиц,
  - обеспечения обороны страны и безопасности государства.
- Обязательным является **соблюдение конфиденциальности информации**, доступ к которой ограничен федеральными законами.

Вопрос 2: «Виды информации ограниченного доступа»



Информация ограниченного доступа, установленная в законодательстве Российской Федерации

Вид информации ограниченного доступа	Основные НПА, устанавливающие ограничение доступа к информации
1. Государственная тайна	Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне»
2. Коммерческая тайна	Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»
3. Налоговая тайна	Налоговый кодекс Российской Федерации
4. Банковская тайна	Федеральный закон от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности»
5. Тайна следствия	Уголовно-процессуальный кодекс Российской Федерации
6. Персональные данные	Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»
…	…
40. Тайна исповеди	ФЗ от 26 сентября 1997 г. № 125-ФЗ «О свободе совести и религиозных объединениях»
ВСЕГО БОЛЕЕ 40 ВИДОВ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА	

Государственная тайна

- **Государственная тайна** — защищаемые государством сведения в области его **военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности**, распространение которых может нанести ущерб безопасности Российской Федерации.
  - ***Закон РФ «О государственной тайне»***

- **Перечень сведений, составляющих государственную тайну**, - совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством.

Конфиденциальность информации

- **Конфиденциальность информации** - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя
  - ***Закон РФ «Об информации, информационных технологиях и защите информации»***

ПЕРЕЧЕНЬ СВЕДЕНИЙ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА

(Указ Президента РФ от 6 марта 1997 г.
С изменениями и дополнениями от ред. от 13.07.2015г.)

1. **Персональные данные.**
2. **Тайна следствия и судопроизводства.**
3. **Служебная тайна.**
4. **Профессиональная тайна.**
5. **Коммерческая тайна.**
6. **Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.**
7. **Сведения, содержащиеся в личных делах осужденных.**

Коммерческая тайна

- **Коммерческая тайна** - конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду
  - ***Закон РФ «О коммерческой тайне»***

ИНФОРМАЦИЯ, СОСТАВЛЯЮЩАЯ КОММЕРЧЕСКУЮ ТАЙНУ

концептуальная:
- новые идеи
- стратегии
- концепции развития

организационная:
- деловые связи
- управленческие решения
- планы производства

технологическая:
- управление предприятием
- управление финансами
- технологии

параметрическая:
- расчеты эффективности
- структура цены
- издержки

эксплуатационная:
- эксплуатация оборудования
- утилизация оборудования
- сведения о системе безопасности

Банковская тайна

- **Банковская тайна** — защищаемые банками и иными кредитными организациями сведения о банковских операциях по счетам и сделкам в интересах клиентов, счетах и вкладах своих клиентов и корреспондентов, а также сведения о клиентах и корреспондентах, разглашение которых может нарушить право последних на неприкосновенность частной жизни.

К основным объектам банковской тайны относятся:

1. Тайна банковского счета.
2. Тайна операций по банковскому счету.
3. Тайна банковского вклада.
4. Тайна частной жизни клиента или корреспондента.

Профессиональная тайна

- **Профессиональная тайна** — защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, распространение которой может нанести ущерб правам и законным интересам другого лица (доверителя), доверившего эти сведения, и не являющаяся государственной или коммерческой тайной.
  - ***Закон РФ «Об информации, информационных технологиях и защите информации»***

Объекты профессиональной тайны:

- Нотариальная тайна
  - (тайна завещания)
- Врачебная тайна
- Адвокатская тайна
- Тайна страхования
- Аудиторская тайна
- Тайна связи
  - (тайна переписки, почтовых, телеграфных и иных сообщений)
- Тайна ломбарда
- Тайна усыновления
- Тайна исповеди

Служебная тайна

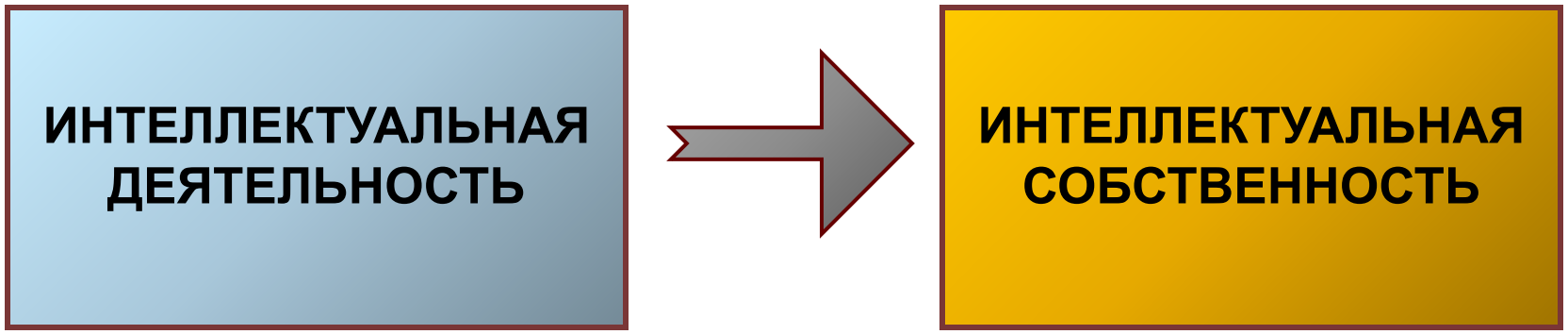
- **Служебная тайна** — защищаемая по закону конфиденциальная информация, ставшая известной в государственных органах и органах местного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости.
  - ***ГОСТ 34.003–90. Автоматизированные системы Термины и определения***

Персональные данные

- **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
  - ***Федеральный закон «О персональных данных»***

Вопрос 3: «Понятие интеллектуальной собственности»

- Законодательными актами РФ регламентируется право собственности на информацию, полученную юридическими и физическими лицами **в результате интеллектуальной деятельности.**



Интеллектуальная собственность

- **Интеллектуальная собственность** - это результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий, которым предоставляется правовая охрана.
  - ***часть IV Гражданского Кодекса РФ***

Статья 128 ГК РФ. Объекты гражданских прав

- **К объектам гражданских прав относятся** вещи (включая наличные деньги и документарные ценные бумаги), иное имущество, в том числе имущественные права (**включая безналичные денежные средства, бездокументарные ценные бумаги, цифровые права**); результаты работ и оказание услуг; **охраняемые результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации (интеллектуальная собственность); нематериальные блага.**

Результатами интеллектуальной деятельности являются:

- произведения науки, литературы и искусства;
- программы для электронных вычислительных машин (программы для ЭВМ);
- базы данных;
- исполнения;
- фонограммы;
- сообщение в эфир или по кабелю радио- или телепередач (вещание организаций эфирного или кабельного вещания);
- изобретения;

- полезные модели;
- промышленные образцы;
- селекционные достижения;
- топологии интегральных микросхе. .,
- секреты производства (ноу-хау);
- фирменные наименования;
- товарные знаки и знаки обслуживания;
- наименования мест происхождения товаров;
- коммерческие обозначения.
- **Интеллектуальная собственность охраняется законом!**

- **Автором** результата интеллектуальной деятельности признается гражданин, творческим трудом которого создан такой результат.
- **Интеллектуальные права** включают исключительное право (**имущественное право**), которые не зависят от права собственности на материальный носитель, в котором выражены результаты интеллектуальной деятельности.
- Обладающий исключительным правом на результат интеллектуальной деятельности является **правообладателем.**

Институты права интеллектуальной собственности:

- авторское право;
- права, смежные с авторскими;
- патентное право;
- право на селекционное достижение;
- право на секрет производства (ноу-хау);
- права на средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий;
- право использования результатов интеллектуальной деятельности в составе единой технологии.

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лекция 4:

«Понятие и виды угроз информационной безопасности»

Вопросы:

1. **Понятие угрозы информационной безопасности.**
2. **Виды и классификация угроз информационной безопасности.**
3. **Источники угроз информационной безопасности.**

Вопрос 1: «Понятие угрозы информационной безопасности»

- **Угроза:**
- наиболее конкретная и непосредственная **форма опасности**, характеризуемая конкретной формой проявления и способом воздействия;
- **совокупность условий и факторов, создающих опасность** интересам граждан, общества и государства, а также национальным ценностям.

В зависимости от сферы проявления угроз, необходимо обеспечивается :

- экологическая безопасность;
- экономическая безопасность;
- военная безопасность;
- ресурсная безопасность;
- **информационная безопасность;**
- социальная безопасность;
- энергетическая безопасность;
- ядерная безопасность;
- политическая безопасность;
- правовая безопасность;
- культурная безопасность;
- техническая безопасность и др.

К основным угрозам государственной и общественной безопасности относятся

- **разведывательная и иная деятельность** специальных служб и организаций иностранных государств, отдельных лиц, наносящая ущерб национальным интересам;
- **нарушения безопасности и устойчивости функционирования** критической информационной инфраструктуры РФ;
- **деятельность, связанная с использованием информационных и коммуникационных технологий** для распространения и пропаганды идеологии фашизма, экстремизма, терроризма и сепаратизма, нанесения ущерба гражданскому миру, политической и социальной стабильности в обществе…

Указ Президента Российской Федерации от 15.01.2013 № 31с

УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

- **Угроза (безопасности информации)** - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.
  - ***ГОСТ Р 50922-2006 Национальный стандарт РФ. Защита информации. Основные термины и определения***

- **Угроза реализуется в виде атаки, в результате чего и происходит нарушение безопасности информации.**
- **Основные виды нарушения безопасности информации:**
- нарушение **конфиденциальности**;
- нарушение **целостности**;
- нарушение **доступности**.

- **Угроза безопасности информации (threat):** совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации, и/или несанкционированными и/или непреднамеренными воздействиями на нее.
  - ***ГОСТ Р 53113.1-2008. Национальный стандарт РФ. Информационная технология. Защита информационных технологий и АС от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения***

Как системы класса DLP помогают выполнить требования GDPR

ОТРАСЛЬ

McAfee даёт 10 рекомендаций по защите облачных данных компаний

Открыта регистрация НА IX всероссийскую научную техническую конференцию «электромагнитная совместимость»

В Европе увидели риски для конфиденциальности пользователей в сделке Google и Fitbit

УГРОЗЫ

Уязвимость в OpenSMTPD затрагивает BSD- и Linux-серверы

Dell, HP и Lenovo признали, что периферия их ПК лишена средств проверки цифровой подписи

iOS-приложения могут красть данные из буфера обмена устройства

ПРЕСТУПЛЕНИЯ

Злоумышленники обчищают кошельки PayPal через неизвестную уязвимость

Преступники атаковали крупнейшую в Хорватии нефтяную компанию

13 известных компаний стали объектами масштабной фишинговой атаки

- **Фактор, воздействующий на защищаемую информацию** - явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней.
  - ***ГОСТ Р 50922-2006 Национальный стандарт РФ. Защита информации. Основные термины и определения***

ГОСТ Р 51275—99

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

ОБЪЕКТ ИНФОРМАТИЗАЦИИ. ФАКТОРЫ, ВОЗДЕЙСТВУЮЩИЕ НА ИНФОРМАЦИЮ

Общие положения

Издание официальное

БЗ 8—2003

ГОССТАНДАРТ РОССИИ
Москва

Классификация факторов, воздействующих на защищаемую информацию

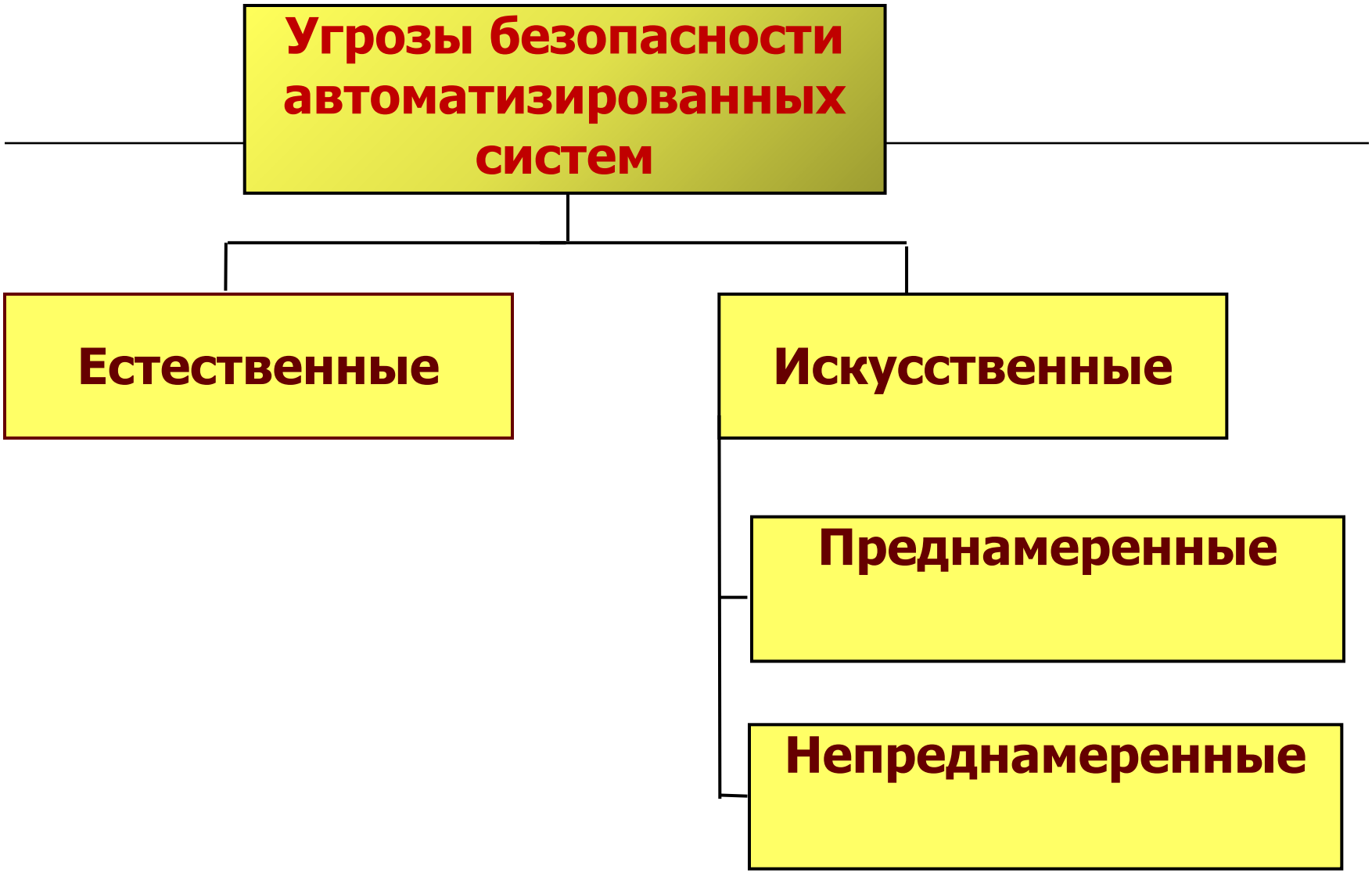
- Факторы, воздействующие на защищаемую информацию и подлежащие учету при организации защиты информации, **по признаку отношения к природе возникновения** делят на классы:
  - объективные;
  - субъективные.
- **По отношению к ОИ факторы**, воздействующие на защищаемую информацию, подразделяют на:
  - внутренние;
  - внешние.

Типы дестабилизирующих факторов

- Количественная недостаточность системы защиты.
- Качественная недостаточность системы защиты.
- Отказы.
- Сбои.
- Ошибки операторов АС.
- Стихийные бедствия.
- Злоумышленные действия.
- Побочные явления.

Вопрос 2: «Классификация и виды угроз информационной безопасности»

- **Классификация угроз** – процесс определения видов угроз безопасности информации по видообразующему признаку

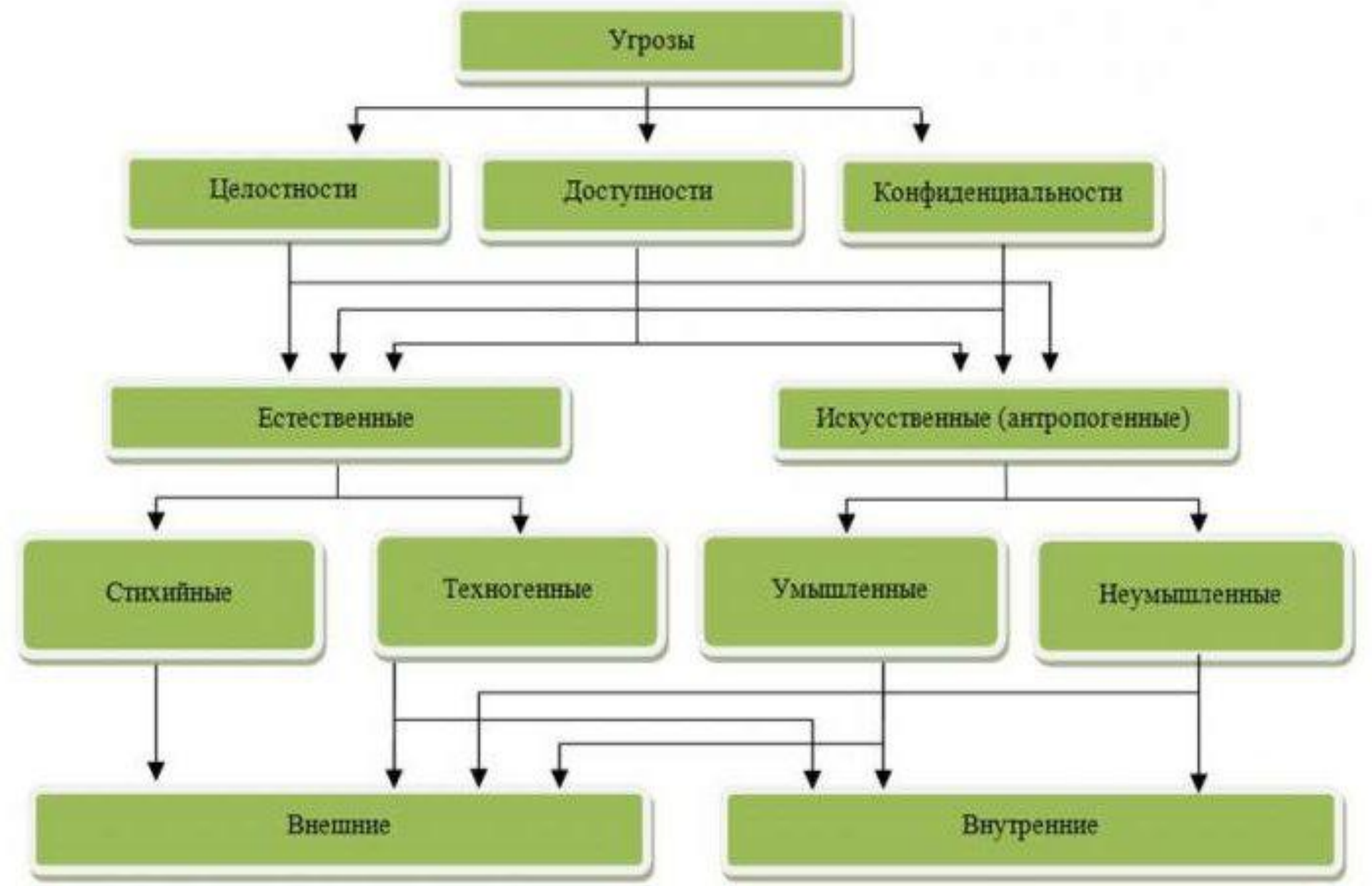

Угрозы безопасности автоматизированных систем
Естественные
Искусственные
Преднамеренные
Непреднамеренные

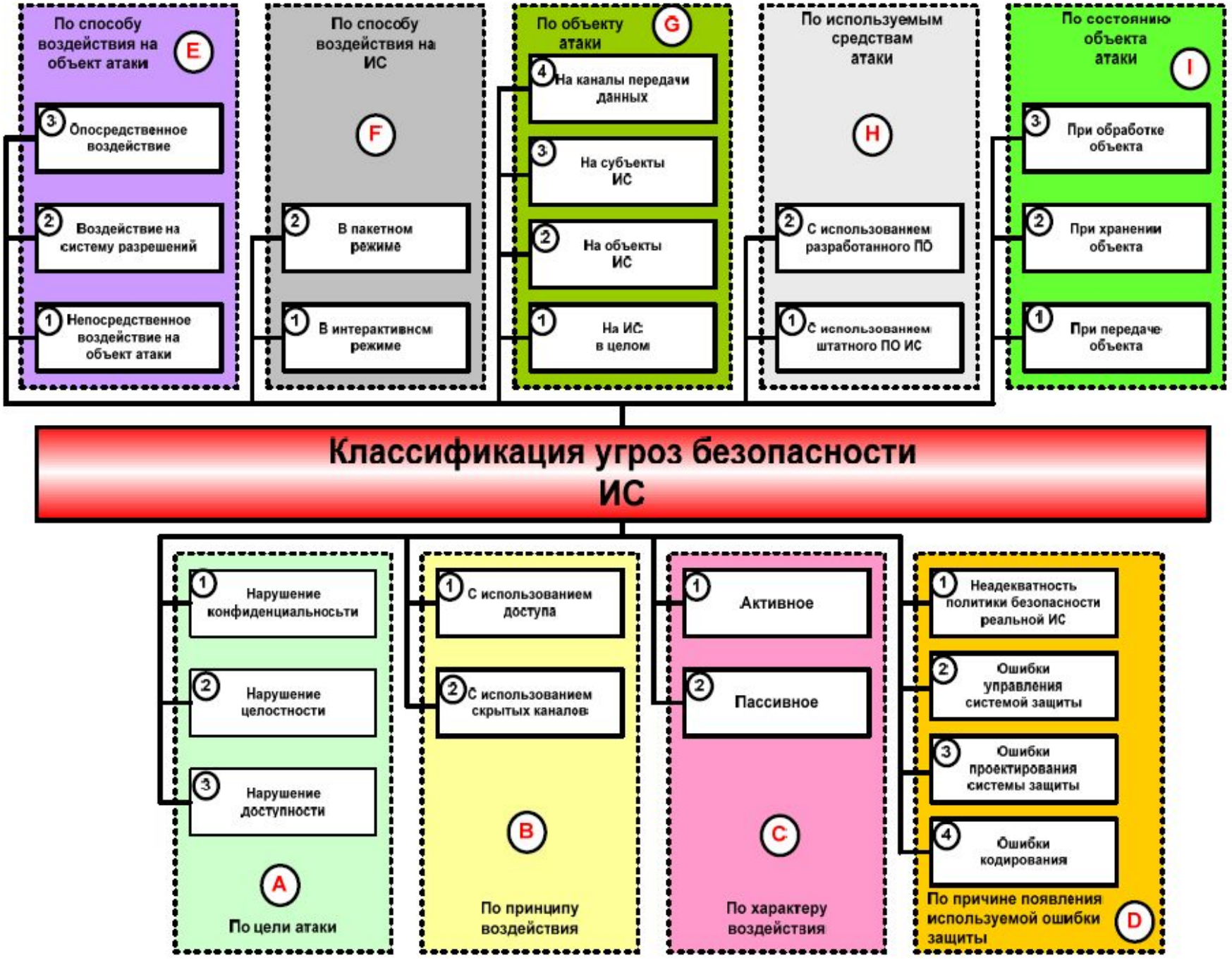
внешние угрозы:

- недобросовестные конкуренты;
- криминальные группы и формирования;
- противозаконные действия административного аппарата.

внутренние угрозы:

- преднамеренные и непреднамеренные действия персонала;
- отказ оборудования, технических средств;
- сбои программного обеспечения.


Угрозы
Целостности
Доступности
Конфиденциальности
Естественные
Искусственные (антропогенные)
Стихийные
Техногенные
Умышленные
Неумышленные
Внешние
Внутренние


По способу воздействия на объект атаки
E
3 Опосредственное воздействие
2 Воздействие на систему разрешений
1 Непосредственное воздействие на объект атаки
По способу воздействия на ИС
F
2 В пакетном режиме
1 В интерактивном режиме
По объекту атаки
G
4 На каналы передачи данных
3 На субъекты ИС
2 На объекты ИС
1 На ИС в целом
По используемым средствам атаки
H
2 С использованием разработанного ПО
1 С использованием штатного ПО ИС
По состоянию объекта атаки
I
3 При обработке объекта
2 При хранении объекта
1 При передаче объекта
Классификация угроз безопасности ИС
1 Нарушение конфиденциальности
2 Нарушение целостности
3 Нарушение доступности
A
По цели атаки
1 С использованием доступа
2 С использованием скрытых каналов
B
По принципу воздействия
1 Активное
2 Пассивное
C
По характеру воздействия
1 Неадекватность политики безопасности реальной ИС
2 Ошибки управления системой защиты
3 Ошибки проектирования системы защиты
4 Ошибки кодирования
По причине появления используемой ошибки защиты
D

Утечка информации -

- неправомерный выход конфиденциальных сведений за пределы организации или круга лиц, которым эти сведения были доверены.

Классификация каналов утечки информации

Социальный канал утечки информации

Собственные сотрудники организации
- вербовка;
- злой умысел;
- неумышленные ошибочные действия;
- другие.

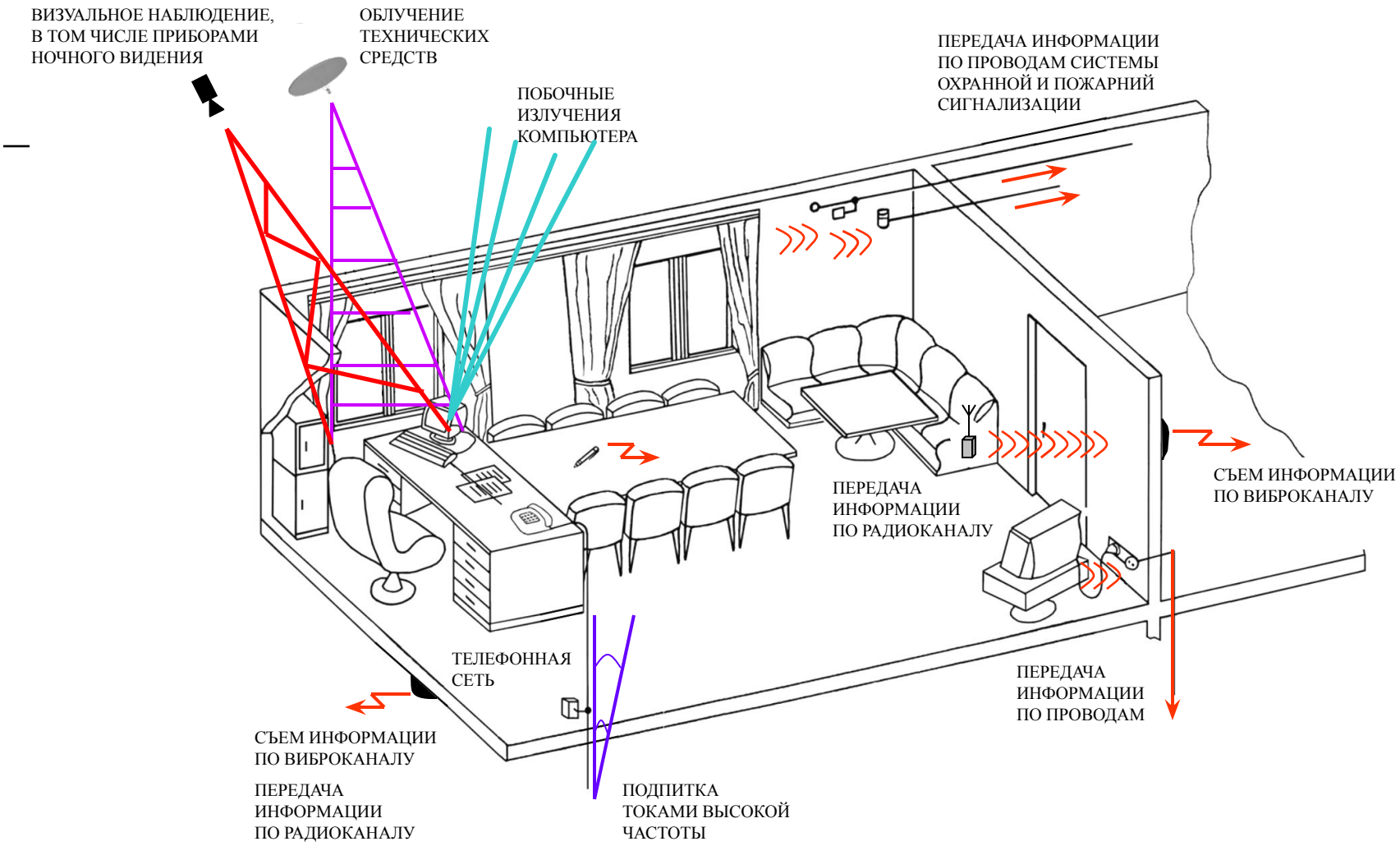
Технический канал утечки информации

Акустика
Виброакустика
Электромагнитные поля
(ПЭМИН)
Компьютерные сети
(Сети Интернет, локальные сети и др.)

Материально-вещественный канал утечки информации

Печатные документы
Электронные носители
Аппаратура
(элементы аппаратуры)
«мусор»

ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ



Каналы утечки информации

- **Прямые** - каналы, использование которых требует проникновения в помещения, где расположены компоненты системы **(НСД).**
- **Косвенные** - каналы, использование которых не требует проникновения в помещения, где расположены компоненты системы.

Банк данных угроз безопасности информации

Федеральная служба по техническому и экспортному контролю

ФСТЭК России

Государственный научно-исследовательский испытате
технической защиты информации

ФАУ «ГНИИИ ПТЗИ ФСТЭК России»

ФИЛЬТРАЦИЯ

Контекстный поиск по названию угрозы

Введите слово или словосочетание

Источник угрозы

Доступен множественный выбор

Последствия реализации угрозы:

- Нарушение конфиденциальности
- Нарушение целостности
- Нарушение доступности

Сброс | Применить

Выводить по: 10, 20, 50, 100

Элементы с

УБИ. 001	Угроза автоматического распространения вредоносного кода в грид-системе
УБИ. 002	Угроза агрегирования данных, передаваемых в грид-системе
УБИ. 003	Угроза использования слабостей криптографических алгоритмов и уязвимостей в программном обеспечении их реализации
УБИ. 004	Угроза аппаратного сброса пароля BIOS
УБИ. 005	Угроза внедрения вредоносного кода в BIOS
УБИ. 006	Угроза внедрения кода или данных
УБИ. 007	Угроза воздействия на программы с высокими привилегиями
УБИ. 008	Угроза восстановления и/или повторного использования аутентификационной информации
УБИ. 009	Угроза восстановления предыдущей уязвимой версии BIOS
УБИ. 010	Угроза выхода процесса за пределы виртуальной машины

<< < 1 2 3 4 5 6 7 8 9 10 > >>

Скачать сведения об угрозах

УБИ.001: Угроза автоматического распространения вредоносного кода в грид-системе

Описание угрозы	Угроза заключается в возможности внедрения и запуска вредоносного кода от имени доверенного процесса на л ресурсных центров грид-системы и его автоматического распространения на все узлы грид-системы. Данная угроза обусловлена слабостями технологии грид-вычислений – высоким уровнем автоматизации при ма администрируемости грид-системы. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий легального пользователя г системы
Источники угрозы	Внутренний нарушитель со средним потенциалом Внешний нарушитель со средним потенциалом
Объект воздействия	Ресурсные центры грид-системы
Последствия реализации угрозы	Нарушение конфиденциальности Нарушение целостности Нарушение доступности

ФИЛЬТРАЦИЯ

Контекстный поиск по названию уязвимости

Введите слово или словосочетание

Производитель ПО

Выберите производителя ПО

Тип ПО

Выберите тип ПО

Программное обеспечение

Выберите программное обеспечение

Аппаратная платформа

Выберите платформу

Версия ПО

Выберите версию ПО

Статус уязвимости

Выберите статус уязвимости

Доп. параметры

Диапазон дат

с | по

Класс уязвимости

Выберите класс уязвимости

Уровень опасности

Выберите уровень опасности уязвимости

Базовый вектор

AV | AC | Au | C | I | A

Идентификатор типа ошибки

Доступен множественный выбор

Другие системы идентификации

Выберите идентификатор

Наличие эксплойта

Выберите значение

Выводить по: 10, 20, 50, 100 Сортировка:

Элемен

BDU:2020-00706	Уязвимость службы Windows Cryptography Next Generation (CNG) операционных систем Windows, позволяющая нарушителю раскрыть защищаемую информацию Microsoft Corp. Windows Server 2008 R2 SP1
BDU:2020-00705	Уязвимость обработчика PDF-содержимого PDFium веб-браузера Google Chrome, позволяющая нарушителю получить несанкционированный доступ к информации Novell Inc. OpenSUSE Leap 42.3
BDU:2020-00704	Уязвимость функции pnv_lpc_do_eccb (hw/ppc/pnv_lpc.c) эмулятора аппаратного обеспечения QEMU, позволяющая нарушителю вызвать отказ в обслуживании и получить несанкционированный доступ к памяти PowerNV Canonical Ltd. Ubuntu 14.04 LTS
BDU:2020-00703	Уязвимость функций v9fs_wstat (hw/9pfs/9p.c) эмулятора аппаратного обеспечения QEMU, позволяющая нарушителю вызвать отказ в обслуживании Canonical Ltd. Ubuntu 14.04 LTS
BDU:2020-00702	Уязвимость функции «setMethod» (symfony/http-foundation) программной платформы для разработки и управления веб-приложениями Symfony, связанная с отсутствием мер по защите структур SQL запросов, позволяющая нарушителю выполнить произвольный код через SQL-инъекцию АО «НПО РусБИТех» Astra Linux 1.6 «Смоленск»
BDU:2020-00701	Уязвимость гостевого представления расширений браузера Google Chrome, позволяющая нарушителю вызвать отказ в обслуживании Novell Inc. OpenSUSE Leap 42.3
BDU:2020-00700	Уязвимость функций interface_release_resource (hw/display/qxl.c) эмулятора аппаратного обеспечения QEMU, связанная с разыменованием нулевого указателя, позволяющая нарушителю вызвать отказ в обслуживании Red Hat Inc. Red Hat Enterprise Linux 6
BDU:2020-00699	Уязвимость функции проверки сообщения в symfony/framework-bundle программной платформы для разработки и управления веб-приложениями Symfony, связанная с отсутствием мер по защите структур веб-страницы, позволяющая нарушителю произвести XSS-атаку АО «НПО РусБИТех» Astra Linux 1.6 «Смоленск»
BDU:2020-00698	Уязвимость компонентов hw/9pfs/cofile.c и hw/9pfs/9p.c эмулятора аппаратного обеспечения QEMU, связанная с повторным обращением к освобожденной области памяти, позволяющая нарушителю вызвать отказ в обслуживании Canonical Ltd. Ubuntu 14.04 LTS
BDU:2020-00697	Уязвимость конфигурации AD DC программ сетевого взаимодействия Samba, позволяющая нарушителю оказать воздействие на целостность информации АО «НПО РусБИТех» Astra Linux 1.6 «Смоленск»

Вопрос 3: «Источники угроз информационной безопасности»

- **Источник угрозы безопасности информации -** субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.

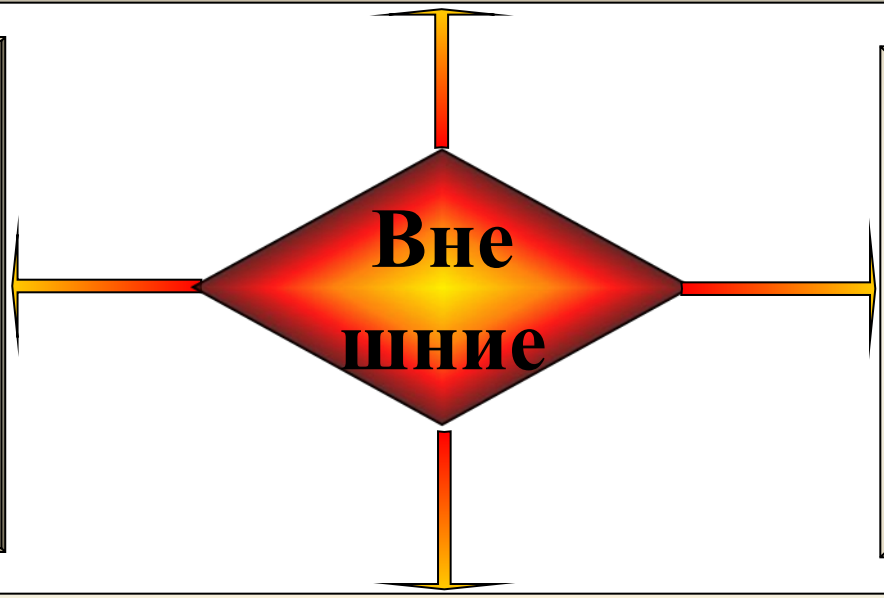
Основные элементы канала реализации угрозы безопасности информации

- **Среда (путь) распространения информации** и воздействий, в которой физическое поле, сигнал, данные или программы могут распространяться и воздействовать на защищаемые свойства (конфиденциальность, целостность, доступность) информации;
- **Носитель защищаемой информации -** физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Внешние источники угроз безопасности информации

Деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере

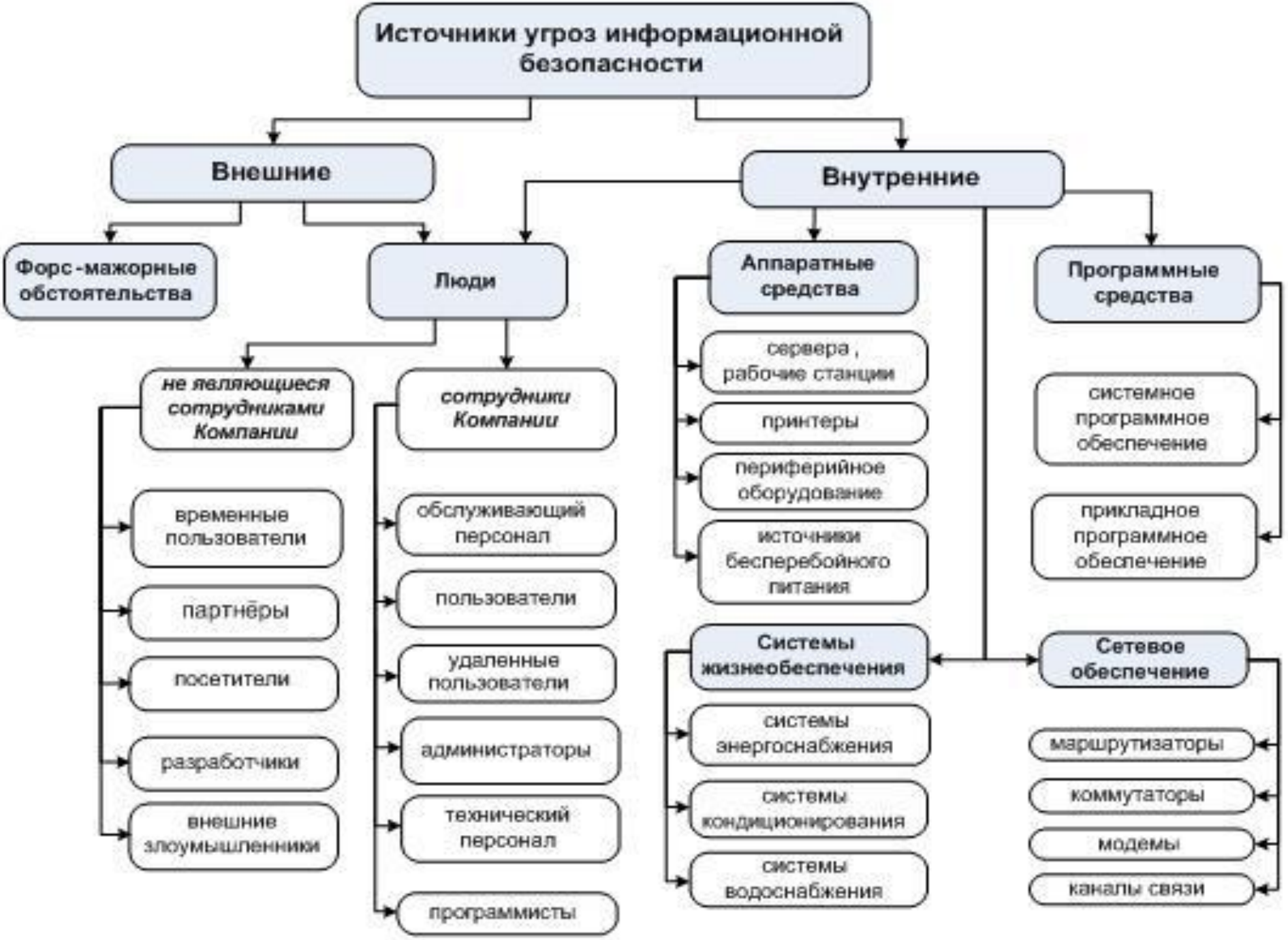
Деятельность международных террористических организаций



Разработка рядом государств концепций информационных войн

Использование иностранными государствами космических, воздушных, морских и наземных технических средств разведки, наблюдения и контроля

Внутренние источники угроз безопасности информации


Источники угроз информационной безопасности
Внешние
Внутренние
Форс-мажорные обстоятельства
Люди
Аппаратные средства
Программные средства
не являющиеся сотрудниками Компании
сотрудники Компании
сервера, рабочие станции
принтеры
периферийное оборудование
источники бесперебойного питания
системное программное обеспечение
прикладное программное обеспечение
временные пользователи
партнёры
посетители
разработчики
внешние злоумышленники
обслуживающий персонал
пользователи
удаленные пользователи
администраторы
технический персонал
программисты
Системы жизнеобеспечения
Сетевое обеспечение
системы энергоснабжения
системы кондиционирования
системы водоснабжения
маршрутизаторы
коммутаторы
модемы
каналы связи

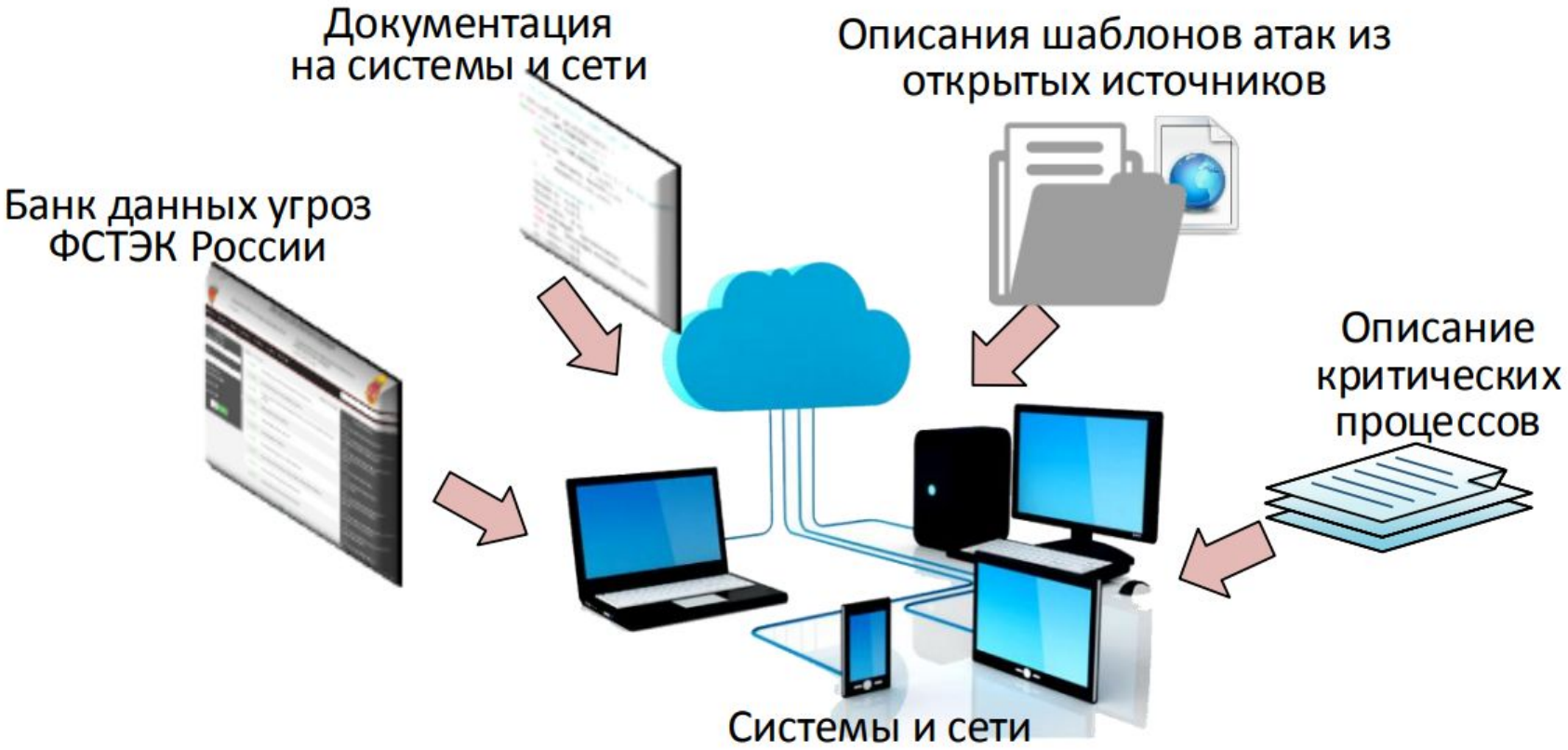
ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

Утвержден ФСТЭК России
5 февраля 2021 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

МЕТОДИКА
ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Общая схема проведения оценки угроз безопасности информации




Этап 1. Определение негативных последствий
Анализ документации систем и сетей и иных исходных данных
Определение негативных последствий от реализации угроз
Этап 2. Определение объектов воздействий
Анализ документации систем и сетей и иных исходных данных
Инвентаризация систем и сетей
Определение групп информационных ресурсов и компонентов систем и сетей
Этап 3. Оценка возможности реализации угроз и их актуальности
Определение источников угроз
Оценка способов реализации угроз
Оценка актуальности угроз

- **Нарушитель безопасности информации** (*Attacker (intruder, violator, troublemaker*). физическое лицо (субъект), случайно или преднамеренно совершившее действия, следствием которых является **нарушение безопасности информации** при ее обработке техническими средствами в **информационных** системах.

Внутренний нарушитель

- пользователи (операторы) системы;
- персонал, обслуживающий технические средства (инженеры, техники);
- сотрудники отделов разработки и сопровождения ПО (прикладные и системные программисты);
- технический персонал, обслуживающий здания (уборщики, электрики, сантехники и другие сотрудники, имеющие доступ в здания и помещения, где расположены компоненты АС);
- сотрудники службы безопасности АС;
- руководители различных уровней должностной иерархии.

Внешний нарушитель

- клиенты (представители организаций, граждане);
- посетители (приглашенные по какому-либо поводу);
- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго-, водо-, теплоснабжения и т. п.);
- представители конкурирующих организаций (иностранных спецслужб) или лица, действующие по их заданию;
- лица, случайно или умышленно нарушившие пропускной режим (без цели нарушить безопасность АС);
- любые лица за пределами контролируемой территории.

Модель нарушителя

- **абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа.**
- **Модель нарушителя может определять:**
- **категории (типы)** нарушителей;
- **цели,** которые могут преследовать нарушители, возможный количественный состав, используемые средства;
- **типовые сценарии возможных действий** (алгоритм) групп и отдельных нарушителей, способы их действий на каждом этапе.


ИСКУССТВО
ОБМАНА
Кевин Д. Митник
Вильям Л. Саймон
eSoul.ru

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лекция 5:

«Информационная безопасность и информационное противоборство»

Вопросы:

1. Сущность информационного противоборства.
2. Информационное оружие и методы ведения информационных войн.
3. Информационная война как способ воздействия на информационные системы.

Вопрос 1: «Сущность информационного противоборства»

- **Информационное противоборство** – соперничество социальных систем в информационно-психологической сфере **по поводу влияния на:**
  - **сферы социальных отношений,**
  - **установления контроля над источниками стратегических ресурсов**,
- для **получения преимущества**, необходимого для дальнейшего развития самой системы.

Субъекты информационного противоборства:

- государства, их союзы и коалиции;
- международные организации;
- негосударственные незаконные вооруженные формирования и организации;
- транснациональные корпорации;
- виртуальные социальные сообщества;
- медиа-корпорации (СМИ и МК).
- виртуальные коалиции.

Цель информационного противоборства – обеспечение национальных интересов в информационно-психологической сфере:

1) обеспечение геополитической и **информационно-психологической безопасности** государства;
2) достижение **военно-политического превосходства** и лидерства в сфере международных отношений;
3) **обеспечение достижения целей** национальной экономической, идеологической, культурной, информационно-психологической экспансии **в соответствии с собственными принципами формирования информационной картины мира**.

Основные способы достижения целей в информационном противоборстве:

1. **Информационно-психологическое** превосходство (**доминирование**);
2. **Асимметричный ответ** на внешние воздействия более сильных субъектов.

Способы достижения информационно-психологического превосходства:

- тайное управление деятельностью органов власти государства-конкурента, информационными процессами;
- информационно-психологическая агрессия;
- информационно-психологическая война.

Основные принципы информационного противоборства:

- информационная асимметрия;
- информационное доминирование;
- скрытость процессов информационно-психологической борьбы;
- внезапность нападения на противника;
- обеспечение стратегического баланса сил в информационно-психологическом пространстве;
- использование отсутствия единых юридически закрепленных правовых норм («война без правил»);
- борьбы в составе коалиции и против других ее членов.

Стадии информационного противоборства:

Вопрос 2: «Информационное оружие и методы ведения информационных войн»

- **Информационное оружие -** совокупность специализированных (***физических, информационных, программных, радиоэлектронных и т.п.***) методов и средств временного или безвозвратного вывода из строя функций или служб информационной инфраструктуры в целом или отдельных ее элементов.

ИНФОРМАЦИОННОЕ ОРУЖИЕ

Средства пропаганды и дезинформации	Психотронное оружие	Средства воздействия на ИС

Средства РЭБ	Средства СПТВ

Средства психологического воздействия, пропаганды, дезинформации

- **ПРОПАГАНДА** (***лат. propaganda «подлежащая распространению»)*** - систематическое распространение фактов, аргументов, слухов и других сведений (в т.ч. заведомо ложных), для воздействия на общественное мнение.
- **ДЕЗИНФОРМАЦИЯ** - элемент оперативной, тактической и стратегической маскировки своих намерений. (Распространяется в целях **оказания необходимого влияния на оппонента** (конкурента) и снижения его возможностей по управлению и контролю за складывающейся ситуацией).

Психотронное оружие

- **Психотронное оружие** - устройства, осуществляющие воздействие на человека путем передачи информации через внечувственное (неосознаваемое) восприятие.
- **Принцип воздействия:** воздействие на психико-физиологическое состояние индивида или коллектива людей, вызывая у них **страх, подавленность или другие чувства** через **резонансные частоты** органов чувств человека.

Принцип возникновения слухового эффекта

Антенна передает голосовые модуляции, наложенные на определенный диапазон сверхвысоких частот

СВЧ-луч, направленный на человека, генерирует в тканях мозга колебания звуковой частоты

Под воздействием сигнала человеку кажется, что он слышит голоса

Средства воздействия на ИС

- Выявление отдельных **элементов ИС управления**, распознание, наведение и огневое поражение в целях физического уничтожения.
- Временный или необратимый вывод из строя **отдельных компонентов** радиоэлектронных систем.
- Вывод из строя либо изменение алгоритма функционирования **ПО управляющих систем** посредством использования **СПТВ.**

Средства радиоэлектронной борьбы (РЭБ)

- **Средства радиоэлектронной борьбы (РЭБ)** - средства для выявления и радиоэлектронного подавления СУ ВиО противника, его систем разведки и навигации, а также средства для обеспечения устойчивой работы своих ИС.

Современные технологии РЭБ против высокоточного оружия и беспилотных ЛА

Средства специального программно-технического воздействия (СПТВ)

- **Средства специального программно-технического воздействия (СПТВ) -** программные, аппаратные или программно-аппаратные средства, с использованием которых может быть осуществлено несанкционированное копирование, искажение, уничтожение информации, ее передача за пределы контролируемой зоны или блокирование доступа к ней.

- **Информационное оружие – основное средство ведения информационных войн!**

- **ИНФОРМАЦИОННАЯ ВОЙНА - комплексная стратегия достижения информационного превосходства при противоборстве в конфликте путем воздействия на информационную среду противника при одновременном обеспечении безопасности собственной информационной среды.**

«ХОЛОДНЫЕ» ВОЙНЫ ИЛИ КУЛЬТУРНОЕ СОТРУДНИЧЕСТВО

«ГОРЯЧИЕ» ВОЙНЫ

ИНФОРМАЦИОННОЕ ОРУЖИЕ

МАТЕРИАЛЬНОЕ ОРУЖИЕ

МИРОВОЗЗРЕНЧЕСКИЙ 1

1. МИРОВОЗЗРЕНИЕ, МЕТОДОЛОГИЯ, ФИЛОСОФИЯ

ХРОНОЛОГИЧЕСКИЙ 2

2. ХРОНОЛОГИЯ ВСЕХ ОТРАСЛЕЙ ЗНАНИЯ

ИДЕОЛОГИЧЕСКИЙ 3

РЕЛИГИИ, ИДЕОЛОГИИ, ТЕХНОЛОГИИ

ЭКОНОМИЧЕСКИЙ 4

СРЕДСТВА ЭКОНОМИЧЕСКОЙ БОРЬБЫ

ОРУЖИЕ ГЕНОЦИДА 5

АЛКОГОЛЬ, НАРКОТИКИ, «ПИЩЕВЫЕ» ДОБАВКИ, ГЕННАЯ ИНЖЕНЕРИЯ

ОРУЖИЕ УНИЧТОЖЕНИЯ 6

ТРАДИЦИОННЫЕ ВИДЫ ВООРУЖЕНИЙ (САМОЛЕТЫ, ТАНКИ, КОРАБЛИ И ДР.)

ХАРАКТЕРИСТИКИ

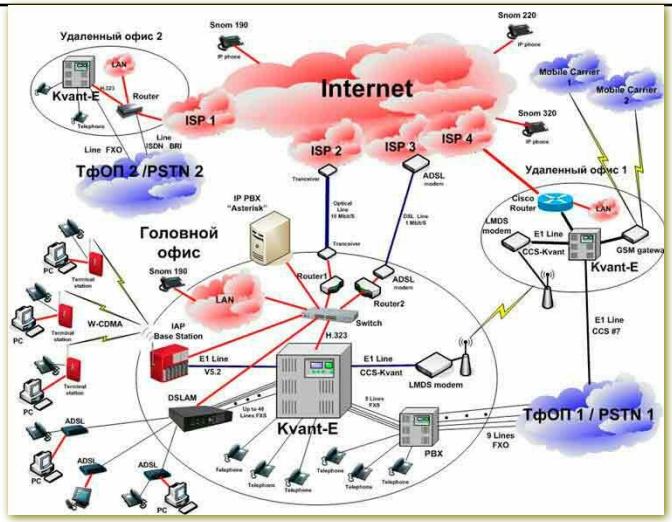
min max

БЫСТРОДЕЙСТВИЕ

max min

МОЩНОСТЬ

Основные объекты воздействия в информационной войне



Сети связи, ИВС государства и предприятий

Военная информационная инфраструктура

СМИ

Мартин Либики «Что такое информационная война?»

- **7 разновидностей информационной войны:**
- командно-управленческая;
- разведывательная;
- электронная
- психологическая;
- хакерская,
- экономическая,
- кибервойна.

- **Командно-управленческая (Command-and-control) война**
- Основной объект воздействия - каналы связи между командованием и исполнителями.
- Блокируя каналы связи, нападающий изолирует пункты управления от исполнительных органов.
- ***Лучше, чем просто убивать «голову».***

- **Разведывательная война** имеет целью сбор важной в военном отношении информации и защиту собственной.
- **Важная составляющая** – криптографическая защита информации.

- **Электронная война** (ЭВ) - комплекс мер с использованием средств ЭМ излучения, направленный на снижение эффективности или воспрещение применения противником ЭМ спектра, а также на обеспечение эффективного использования ЭМ спектра своими войсками.

- **Объект воздействия ЭВ** - средства электронных коммуникаций (радиосвязи, радаров, компьютерных сетей).
- **ЭВ включает:**
  - электронную поддержку (Electronic Support);
  - электронную атаку (Electronic Attack),
  - борьбу с электронным противодействием, или электронное контрпротиводействие (Electronic Protection).

- **Психологическая война** - осуществляется путем пропаганды и другими методами информационной обработки населения.
- **Составляющие психологической войны:**

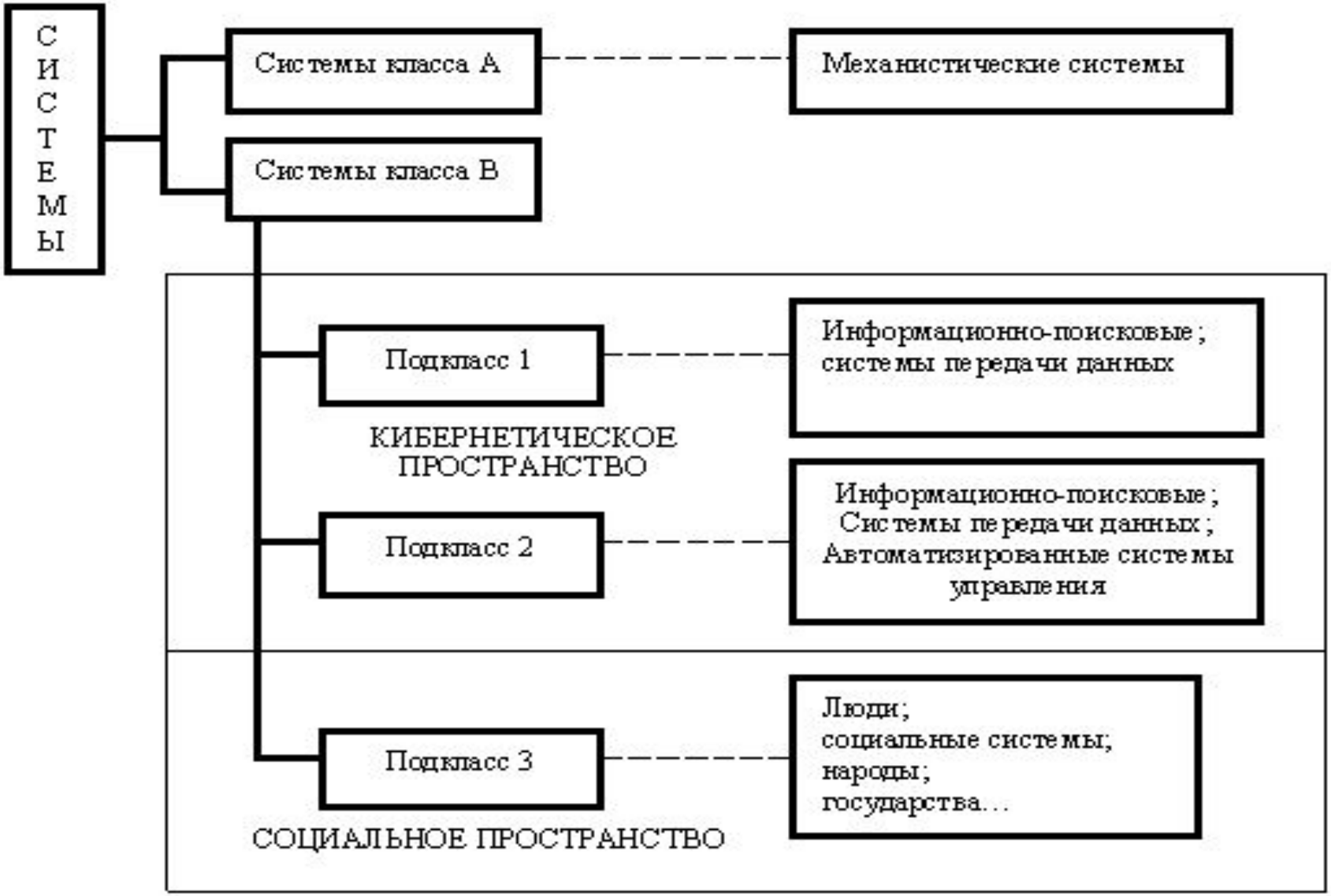
1) подрыв гражданского духа;
2) деморализация вооруженных сил;
3) дезориентация командования;
4) война культур ***(Kulturkampf).***

- **Хакерская война.** Цель – вывод из строя ИС, перебои связи, введение ошибок в пересылку данных, хищение информации, тайный мониторинг, НСД к закрытым данным.
- Используется вредоносное ПТВ.
- **Экономическая война.**
- Формы:
  - информационная блокада
  - информационный империализм.

- **Кибервойна** - военные действия в киберпространстве (атаки против ВС противника - выведение из строя КВО и каналов связи, атаки против гражданского населения).

Вопрос 3: «Информационная война как способ воздействия на информационные системы»

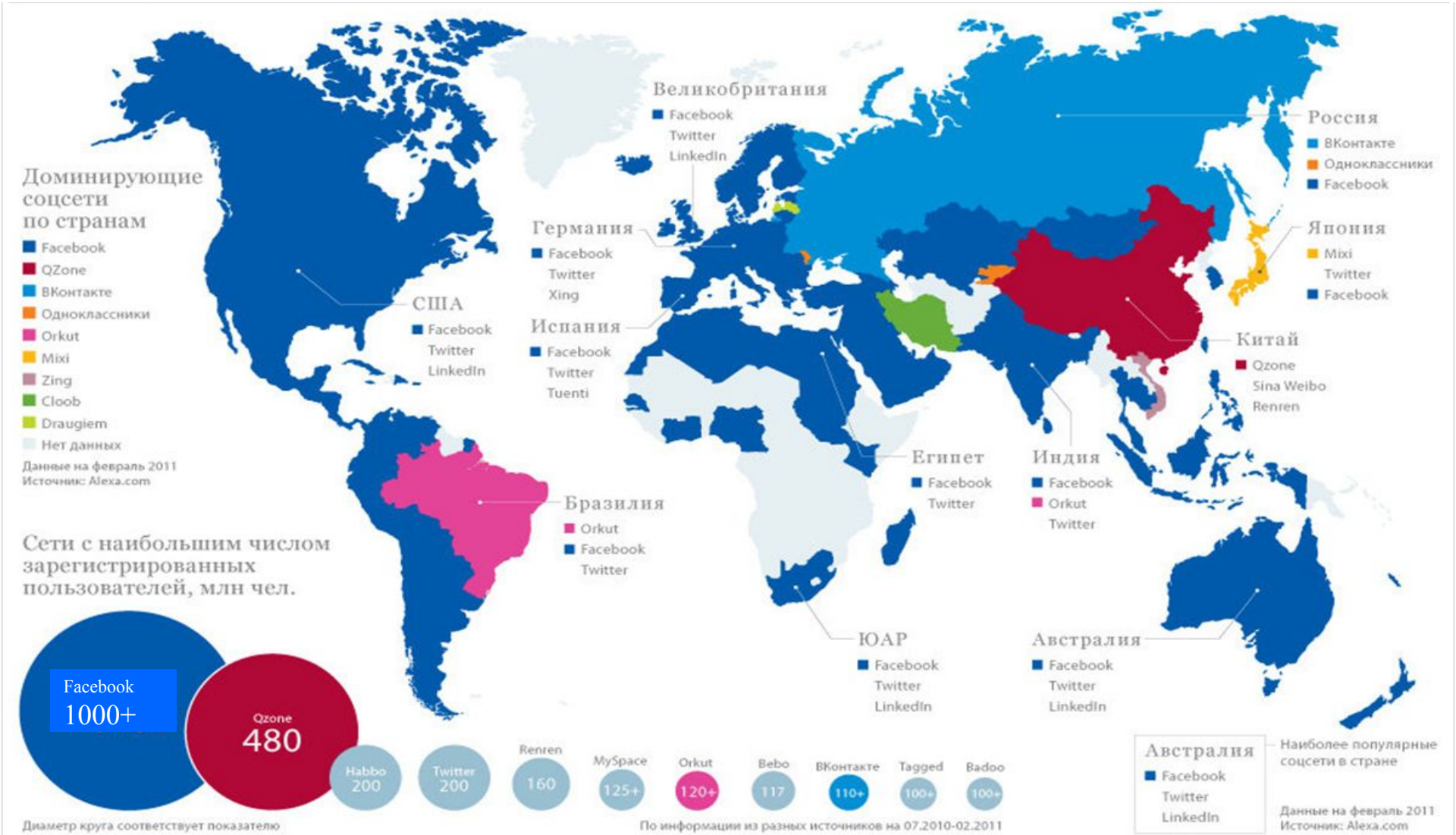
- **Информационная система** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.
  - ***ФЗ «Об информации, информационных технологиях и защите информации»***


СИСТЕМЫ
Системы класса А
Механистические системы
Системы класса В
Подкласс 1
Информационно-поисковые;
системы передачи данных
КИБЕРНЕТИЧЕСКОЕ
ПРОСТРАНСТВО
Подкласс 2
Информационно-поисковые;
Системы передачи данных;
Автоматизированные системы
управления
Подкласс 3
Люди;
социальные системы;
народы;
государства…
СОЦИАЛЬНОЕ ПРОСТРАНСТВО

Использования социальных сетей в информационных войнах

- 2010 г. Госдеп США разработал **«Стратегический план развития информационных технологий в 2011–2013 гг.: цифровая дипломатия».**
- **Ключевой инструмент** в дипломатической практике правительства США - **применение социальных сетей.**

СОЦИАЛЬНЫЕ СЕТИ В МИРЕ



Тендер ФБР (FBI) о разработке ПО контент-анализа соцсетей

Social Media Application

Solicitation Number: SocialMediaApplication

Agency: Department of Justice

Office: Federal Bureau of Investigation

Location: Procurement Section

Notice Type:
Modification/Amendment

Original Posted Date:
January 19, 2012

Posted Date:
January 20, 2012

Response Date:
Feb 10, 2012 11:59 pm Eastern

Original Response Date:
Feb 07, 2012 11:59 pm Eastern

Archiving Policy:
Automatic, on specified date

Original Archive Date:
February 16, 2012

Archive Date:
February 16, 2012

Original Set Aside:
N/A

Set Aside:
N/A

Classification Code:
70 -- General purpose information technology equipment

NAICS Code:
519 -- Other Information Services/519130 -- Internet Publishing and Broadcasting and Web Search Portals

---

Synopsis:

Added: Jan 19, 2012 4:14 pm Modified: Jan 20, 2012 3:34 pm Track Changes

Please review the Request for Information (RFI) that is attached. The Federal Bureau of Investigations is

- **Субъекты КИИ** – гос. органы, учреждения, российские юр. лица, ИП, которым принадлежат ИС, ИТС, АСУ, функционирующие в сфере **здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности**, российские юр. лица, ИП, которые обеспечивают взаимодействие указанных систем или сетей.

Результаты воздействия на КИИ

Аварии

И их последствия…

Кибератака на ядерные объекты Ирана

- «Несколько **иранских центрифуг**, обогащающих уран, центре по обогащению урана в окрестностях **города Натанз подверглись кибератаке**, что нарушило их работу».

Примеры вредоносного ПО (кибероружия)

- **Stuxnet** - воздействие на ПО ПЛК Siemens Simatic S7;
- **Duqu -** кража информации;
- **Wiper -** удаление информации с жестких дисков ПК;
- **Flame** - бэкдор, шпионаж;
- **Gauss -** перехват cookie-файлов, паролей, данных по учетным записям в социальных сетях, почтовых сервисах;
- **Captivatedaudience** - перехват разговоров с микрофона заражённого ПК;
- **Gumfish** - перехват изображений с веб-камеры;
- **Foggybottom** - копирование данных об интернет-журналах, паролях и логинах;
- **Grok** - считывание информации о нажатии клавиш; **Salvagerabbit**,- собирание данных с флеш-накопителей;
- **Gameover Zeus –** кража банковской информации;
- **Wanna Cry, Petya, Bad Rabbit** – вирусы-шифровальщики;
- **Clop Ransomware -** версия программы-вымогателя CryptoMix**.**

Бейся там, где стоишь!

Информационная война - вот твоя битва.

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лекция 6:

«Уровни и сервисы защиты информации в автоматизированных системах»

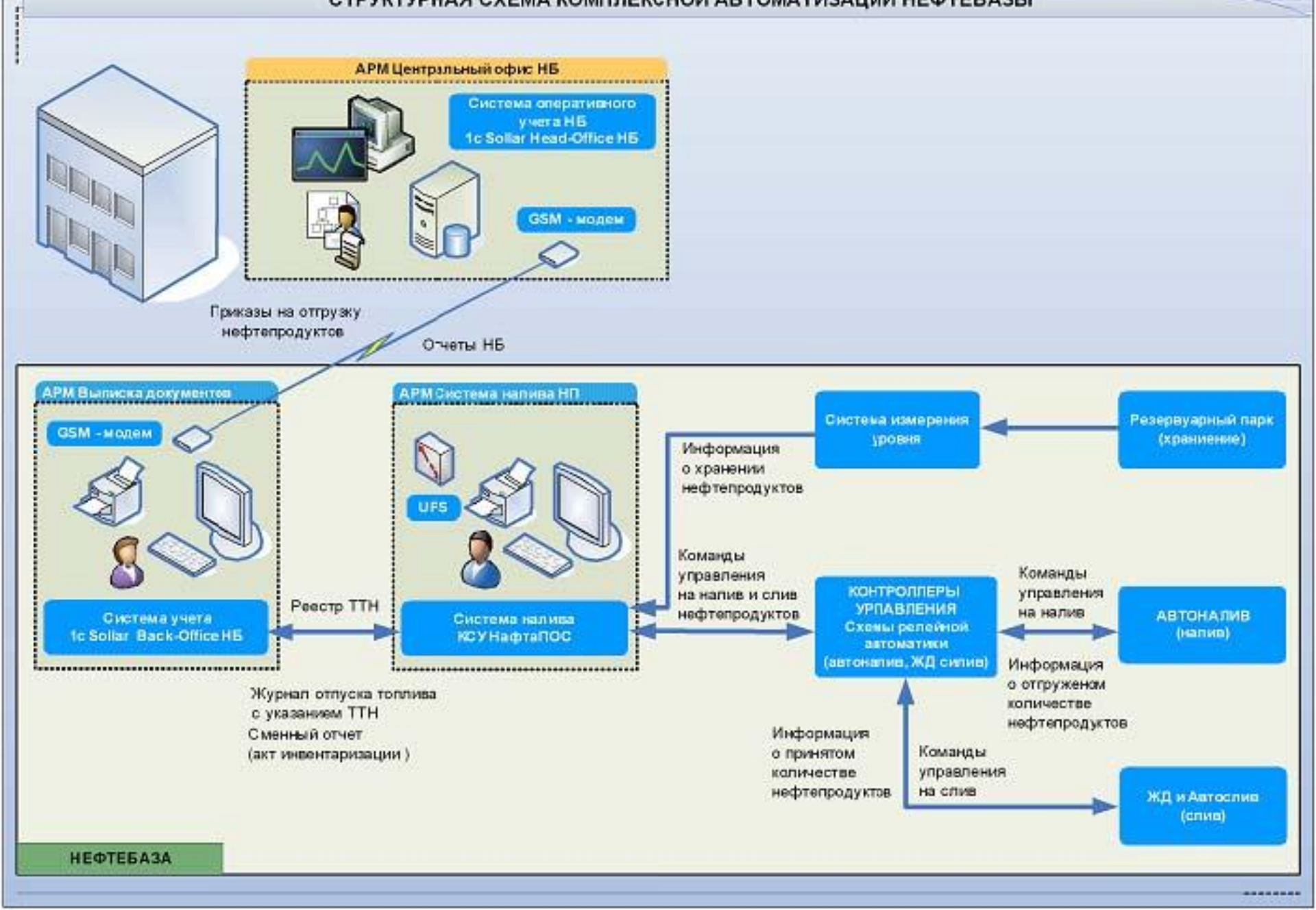
Вопросы:

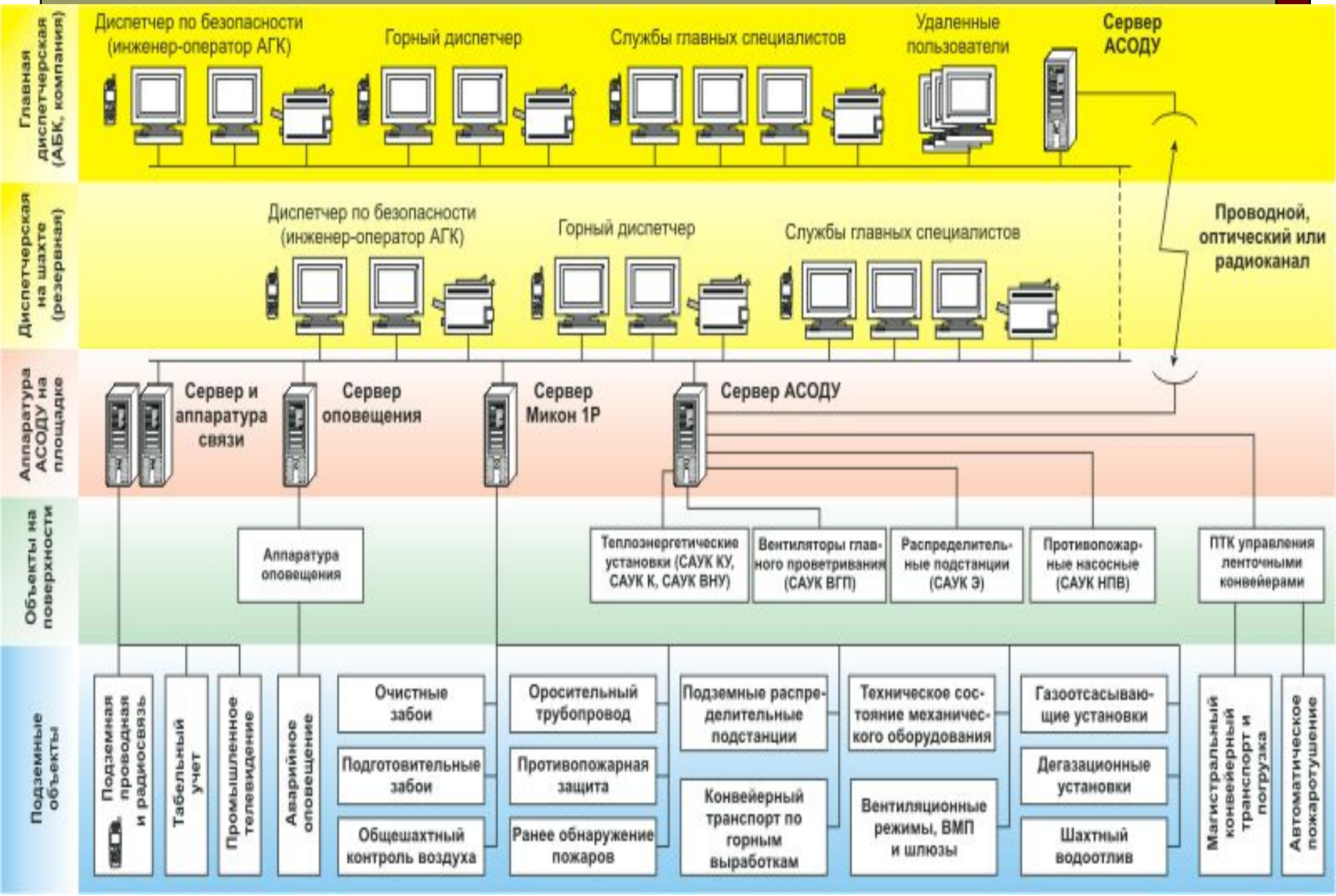
1. **Автоматизированная система, как объект информационной безопасности.**
2. **Уровни информационной безопасности.**
3. **Содержание сервисов безопасности программно-технического уровня.**

Вопрос 1: «Автоматизированная система, как объект информационной безопасности»

- **Автоматизированная система (АС) - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.**
  - *ГОСТ 34.003–90*
  - *Автоматизированные системы Термины и определения*

СТРУКТУРНАЯ СХЕМА КОМПЛЕКСНОЙ АВТОМАТИЗАЦИИ НЕФТЕБАЗЫ




Главная диспетчерская (АБК, компания)
Диспетчер по безопасности (инженер-оператор АГК)
Горный диспетчер
Службы главных специалистов
Удаленные пользователи
Сервер АСОДУ
Диспетчерская на шахте (резервная)
Диспетчер по безопасности (инженер-оператор АГК)
Горный диспетчер
Службы главных специалистов
Проводной, оптический или радиоканал
Аппаратура АСОДУ на площадке
Сервер и аппаратура связи
Сервер оповещения
Сервер Микон 1Р
Сервер АСОДУ
Объекты на поверхности
Аппаратура оповещения
Теплоэнергетические установки (САУК КУ, САУК К, САУК ВНУ)
Вентиляторы главного проветривания (САУК ВГП)
Распределительные подстанции (САУК Э)
Противопожарные насосные (САУК НПВ)
ПТК управления ленточными конвейерами
Подземные объекты
Подземная проводная и радиосвязь
Табельный учет
Промышленное телевидение
Аварийное оповещение
Очистные забои
Подготовительные забои
Общешахтный контроль воздуха
Оросительный трубопровод
Противопожарная защита
Ранее обнаружение пожаров
Подземные распределительные подстанции
Конвейерный транспорт по горным выработкам
Техническое состояние механического оборудования
Вентиляционные режимы, ВМП и шлюзы
Газоотсасывающие установки
Дегазационные установки
Шахтный водоотлив
Магистральный конвейерный транспорт и погрузка
Автоматическое пожаротушение

- **Политика безопасности (Security Policy)** - совокупность норм и правил, обеспечивающих эффективную защиту системы обработки информации от заданного множества угроз безопасности.
- **Модель безопасности (Security Model)** - формальное представление политики безопасности.

- **Субъект доступа (Access subject) -** лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Объект доступа (Access object) – единица информационного ресурса автоматизированной системы, доступ к которой регламентируются правилами разграничения доступа.

Вопрос 2: «Уровни информационной безопасности»

- **Среда безопасности включает уровни:**

1. **Законодательный**
2. **Административный**
3. **Процедурный**
4. **Программно-технический**

Законодательный уровень

–

Основные направления деятельности на законодательном уровне:

- разработка новых законов;
- ориентация на созидательные, а не на карательные меры;
- интеграция в мировое пространство;
- учет современного уровня развития IT.

Минимальные требования безопасности (базовые)

Административный уровень

Процедурный уровень

Программно-технический уровень

Административный уровень

- **Главная цель** - сформировать программу работ в области ИБ и обеспечить ее выполнение, выделяя необходимые **ресурсы** и **контролируя** состояние дел.
- Основа программы - **политика безопасности**, отражающая подход организации к защите информации.

- **Политика безопасности (SP)** - совокупность документированных правил в области безопасности информации, которыми руководствуется организация в своей деятельности.
- SP строится на основе **анализа рисков**.
- **Риск** — сочетание вероятности и последствий наступления неблагоприятных событий.

Процедурный уровень

- **Выделяются направления деятельности:**
- **управление персоналом;**
- **физическая защита;**
- **поддержание работоспособности СЗИ;**
- **реагирование на нарушения режима безопасности;**
- **планирование восстановительных работ и т. д.**

Программно-технический уровень

1. Идентификация и аутентификация.
2. Управление доступом.
3. Протоколирование и аудит.
4. Шифрование.
5. Контроль целостности.
6. Экранирование.
7. Анализ защищенности.
8. Обеспечение отказоустойчивости.
9. Обеспечение безопасного восстановления.
10. Туннелирование.
11. Управление.

Вопрос 3: «Содержание сервисов безопасности программно-технического уровня»

- **Сервисы информационной системы** обеспечивают ее функционирование и определяют требуемые свойства.

Виды мер безопасности:

1. **Превентивные, препятствующие нарушениям ИБ (основные).**
2. Меры обнаружения нарушений.
3. Локализующие, сужающие зону воздействия нарушений.
4. Меры по выявлению нарушителя.
5. Меры восстановления режима безопасности.

ИДЕНТИФИКАЦИЯ

- **Идентификация -** действия по присвоению субъектам и объектам доступа идентификаторов и (или) действия по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов.
  - ***50.1.053-2005 «Информационные технологии. Основные термины и определения в области ТЗИ»***

АУТЕНТИФИКАЦИЯ

- **Аутентификация** (субъекта доступа) - действия по проверке подлинности субъекта доступа в автоматизированной информационной системе.
- **Аутентификация «authentication»:**
  - **односторонняя** (процедура входа пользователя в систему);
  - **двусторонняя** (взаимная).

- **Для подтверждения подлинности субъект предъявляет:**
- **нечто, что он знает** (пароль, личный идентификационный номер, криптографический ключ и т.п.);
- **нечто, чем он владеет** (личную карточку или иное устройство аналогичного назначения);
- **нечто, что есть часть его самого** (голос, отпечатки пальцев и т.п., то есть свои биометрические характеристики).

УПРАВЛЕНИЕ ДОСТУПОМ

- сервис, позволяющий специфицировать и контролировать действия, которые **субъекты** (пользователи и процессы) могут выполнять над **объектами** (информацией и другими ресурсами АС).
- **Различается:**
  - **физическое управление** доступом;
  - **логическое управление** доступом.

- **Логическое управление доступом** –механизм многопользовательских АС, призванный обеспечить конфиденциальность, целостность и доступность (путем запрещения обслуживания **неавторизованных пользователей**).

Отношение «субъекты-объекты»

Фрагмент матрицы доступа				
	Файл	**Программа**	**Линия связи**	**Реляционная таблица**
Пользователь 1	orw с системной консоли	e	rw с 8:00 до 18:00	
Пользователь 2				a

"o" – разрешение на передачу прав доступа другим пользователям
"r" – чтение,
"w" – запись,
"e" – выполнение,
"a" – добавление информации

АВТОРИЗАЦИЯ

- **предоставление субъекту прав на доступ к объекту**.
- **В информационных технологиях** реализация права доступа к ресурсам и системам обработки данных.
- **В финансовой сфере** при использовании банковских платежных, кредитных карт.
- **В бизнесе** — выдача лицензии (напр. авторизированный автомобильный дилер).

ПРОТОКОЛИРОВАНИЕ

- **сбор и накопление информации о событиях, происходящих в АС.**
- У каждого сервиса **свой набор возможных событий**:
- **внешних** (вызванных действиями других сервисов);
- **внутренних** (вызванных действиями самого сервиса);
- **клиентских** (вызванных действиями пользователей и администраторов).

При протоколировании события рекомендуется записывать следующую информацию:

- дата и время события;
- уникальный идентификатор пользователя - инициатора действия;
- тип события;
- результат действия (успех или неудача);
- источник запроса (например, имя терминала);
- имена затронутых объектов (например, открываемых или удаляемых файлов);
- описание изменений, внесенных в базы данных защиты (например, новая метка безопасности объекта).

АУДИТ

- анализ накопленной информации, проводимый оперативно, в реальном времени или периодически (раз в день).
- **Оперативный аудит** с автоматическим реагированием на выявленные нештатные ситуации называется **активным.**

Реализация протоколирования и аудита решает задачи:

- обеспечение **подотчетности** пользователей и администраторов;
- обеспечение возможности **реконструкции последовательности событий**;
- **обнаружение попыток нарушений** информационной безопасности;
- **предоставление информации** для выявления и анализа проблем.

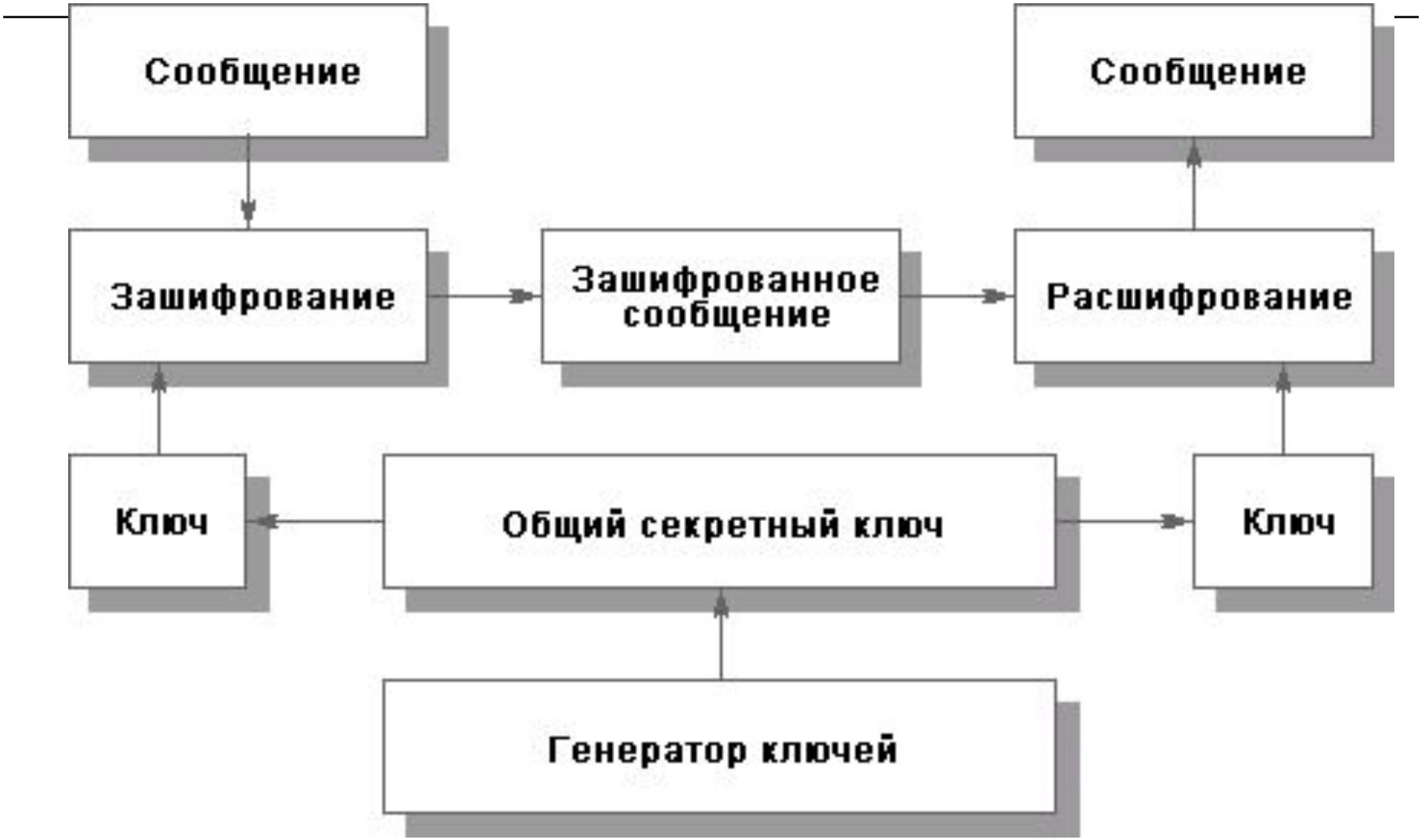
Криптография для сервисов безопасности

- На основе криптографии реализуются сервисы безопасности:
- **шифрование**;
- **контроль целостности**;
- **аутентификация** (этот сервис был рассмотрен нами ранее).

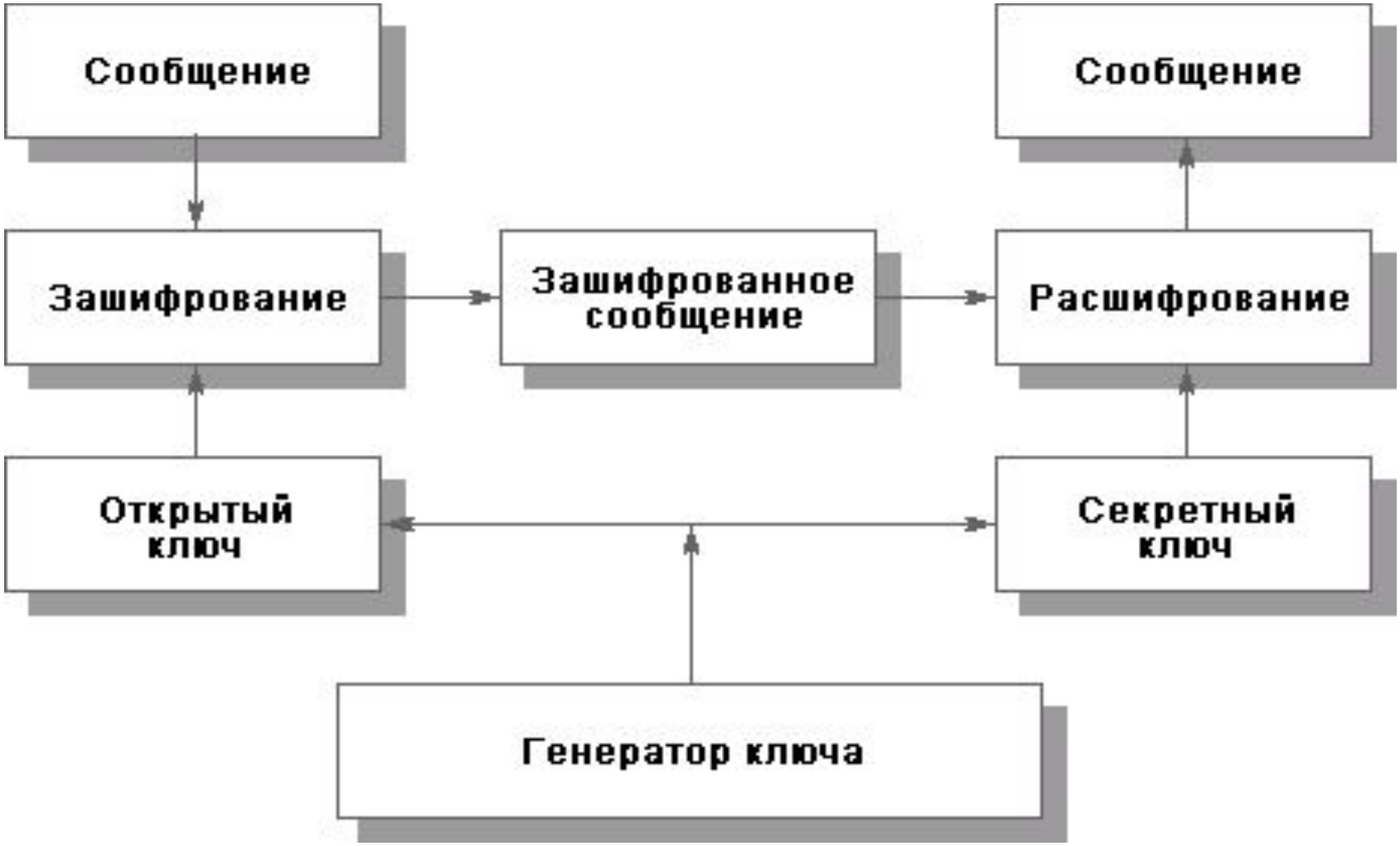
ШИФРОВАНИЕ

- Методы шифрования:
- **Симметричный** (один и тот же секретный ключ используется и для зашифрования, и для **расшифрования** данных (*ГОСТ 28147-89*);
- **Асимметричный** (шифрование и расшифровывание разными ключами (*метод RSA)*.

Симметричный метод шифрования



Асимметричный метод шифрования



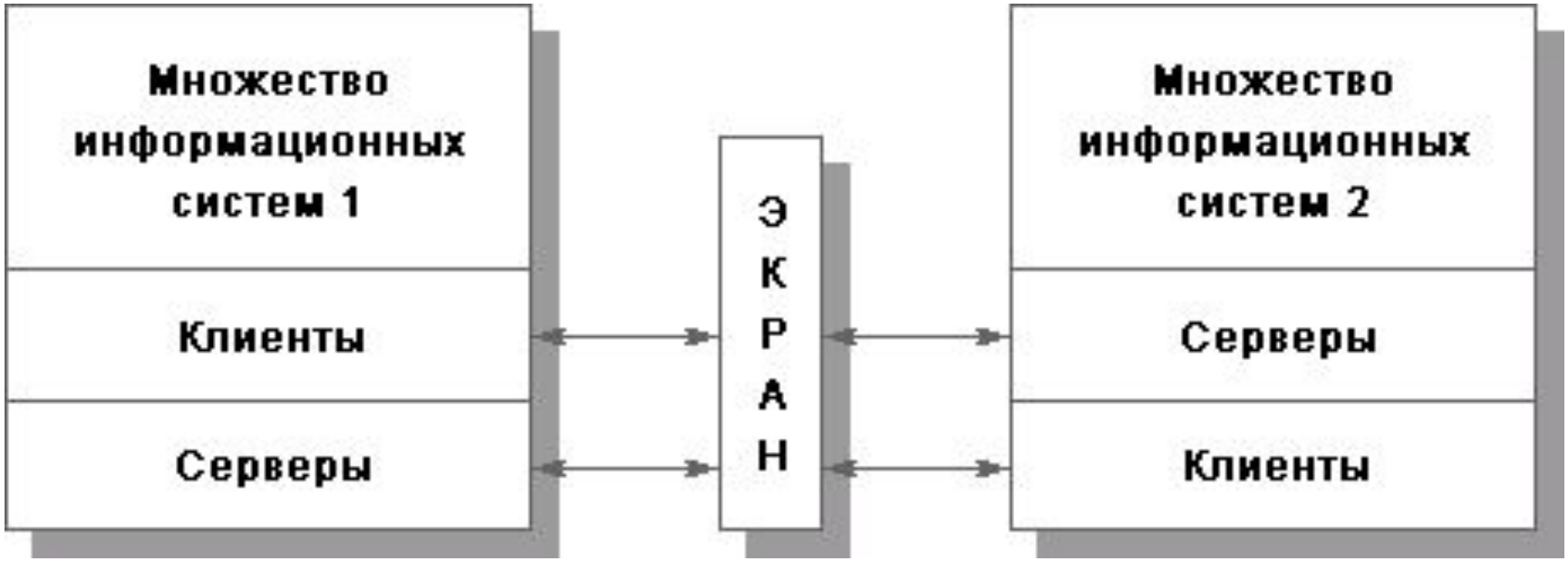
КОНТРОЛЬ ЦЕЛОСТНОСТИ

- **Криптографический контроль целостности на основе:**
  - хэш-функции;
  - электронной подписи (ЭП).
- **Хэш-функция** - труднообратимое преобразование данных (**односторонняя функция**), реализуемое средствами симметричного шифрования.

ЭКРАНИРОВАНИЕ

- **Экран** - средство разграничения информационных потоков на границе защищаемой АС (*IP, порты, параметры заголовков*).
- **Системы обнаружения вторжений** (Intrusion Detection System, IDS) – программно-аппаратный комплекс для выявления попыток НСД к ресурсам АС *(IDS уровня сети, IDS уровня хоста).*

Экранирование



Функционирование экрана

АНАЛИЗ ЗАЩИЩЕННОСТИ

- Для выявления уязвимых мест (ошибки администрирования) с целью их оперативной ликвидации.
- Помогает **обнаружить «бреши»** в защите **(и устранить их)** раньше, чем их сможет использовать злоумышленник.
- **Сканеры защищенности** основаны на накоплении и использовании знаний.

ДОСТУПНОСТЬ

- **Достигается за счет применения мер, направленных на повышение:**
- **безотказности** (минимизация вероятности возникновения отказа);
- **отказоустойчивости** (резервирования аппаратуры);
- **обслуживаемости** (минимизация времени простоя отказавших компонентов).

ТУННЕЛИРОВАНИЕ

- Для согласования транспортных протоколов (**инкапсуляции**), либо для создания защищённого соединения между узлами сети.
- **Применяется для:**
- передачи через сеть пакетов, принадлежащих протоколу, который **в данной сети не поддерживается**;
- обеспечения **слабой формы конфиденциальности** за счет сокрытия истинных адресов;
- обеспечения конфиденциальности и целостности передаваемых данных при использовании **вместе с криптографическими сервисами**.

УПРАВЛЕНИЕ

- **Управление** - интегрирующая оболочка информационных сервисов и сервисов безопасности, обеспечивающую их нормальное, согласованное функционирование под контролем администратора ИС.
- **Подразделяется на:**
- **мониторинг** компонентов;
- **контроль** (выдачу и реализацию управляющих воздействий);
- **координацию** работы компонентов системы.


Минимальные требования безопасности
Информирование и обучение персонала
Планирование
Реагирование на нарушения ИБ
Оценка рисков
Физическая защита
Политика ИБ
Защита систем и телекоммуникаций
Действия ИБ к сервисам и системам
Сертификация, аккредитация и оценки ИБ
Управление конфигурацией
Кадровая безопасность
Мониторинг регуляторов ИБ
Протоколирование и аудит
Аутентификация, авторизация
Обеспечение целостности
Защита носителей

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лекция 7:

«Формальные модели безопасности»

Вопросы:

1. Назначение формальных моделей безопасности.
2. Формальные модели управления доступом.
3. Формальные модели целостности.
4. Ролевое управление доступом.

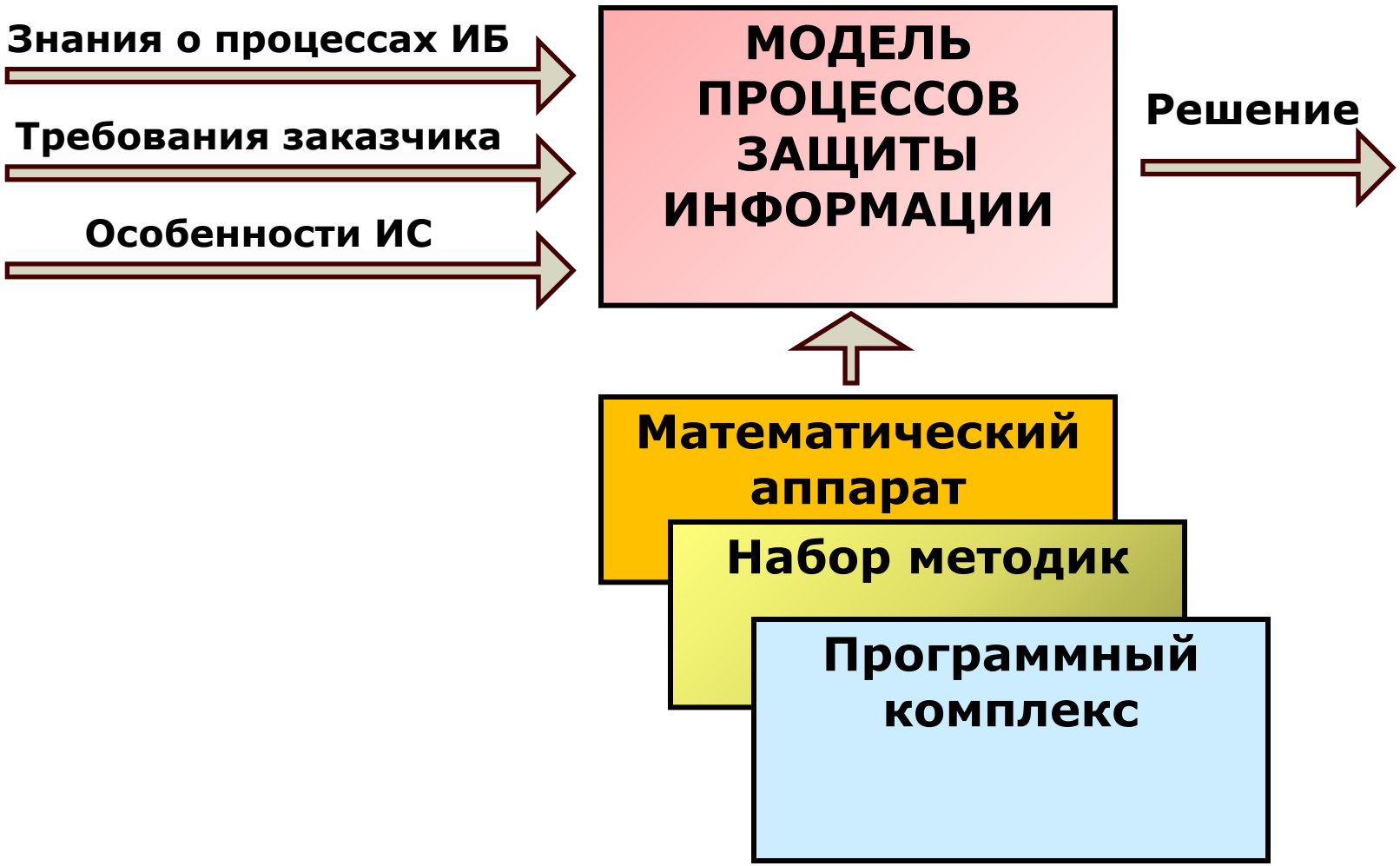
Вопрос 1: «Назначение формальных моделей безопасности»

- **Модель** (*фр. modèle, от лат. modulus — «мера, аналог, образец»*) **— абстрактное описание системы (объекта, процесса, проблемы, понятия) в некоторой форме, отличной от формы их реального существования.**

Моделирование системы защиты информации

- построение образа (модели) СЗИ, адекватного (с точностью до целей моделирования) моделируемой системе, и получения с помощью построенной модели необходимых характеристик реальных систем защиты информации.

Модель представления системы информационной безопасности



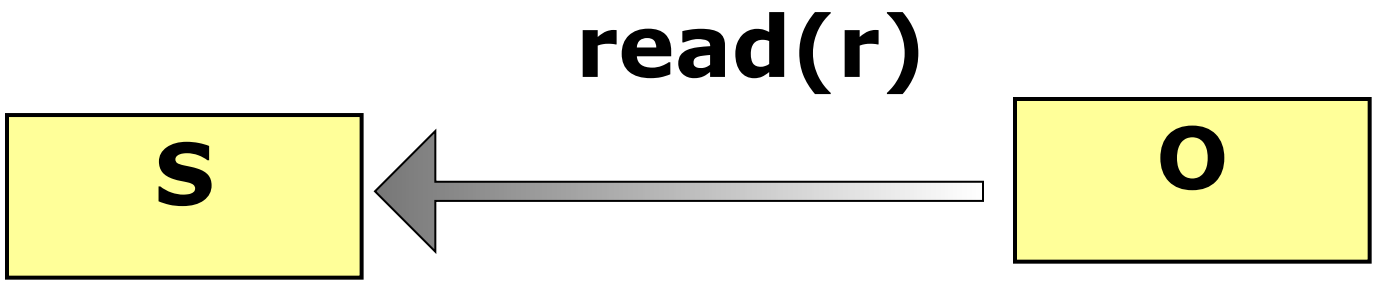
Варианты моделей защиты

1. Общая модель процесса защиты информации.
2. Модель оценки угроз информационной безопасности.
3. Модели анализа систем разграничения доступа к ресурсам АС.

- **Политика безопасности –** свод формальных правил, определяющих **обработку, распространение и защиту информации**.
- **Модель политики безопасности – формальное представление политики безопасности** для определенной системы или класса систем, определяющее методы обработки, распространения и защиты информации.

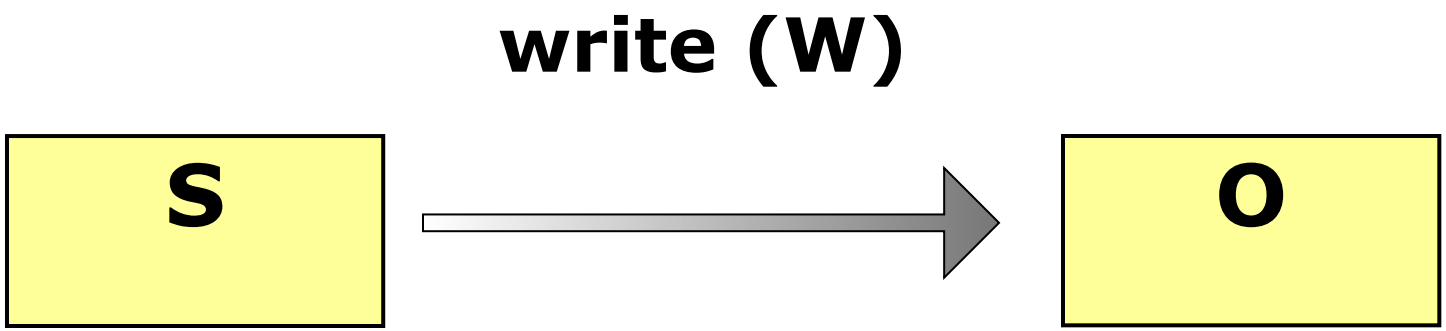
Формализация процедуры доступа

- **Чтение (информационный поток от O к S)**

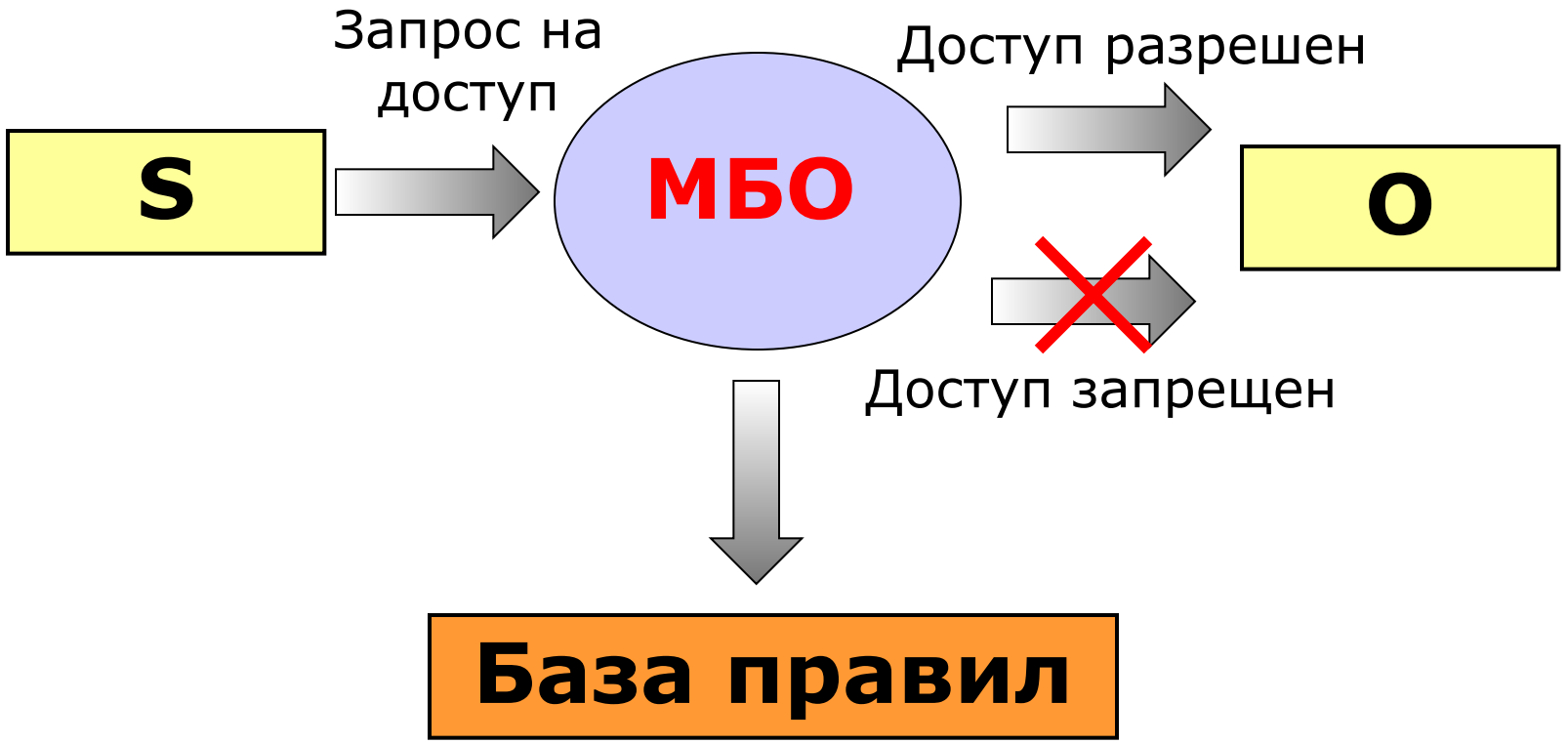


Формализация процедуры доступа

- **Запись (информационный поток от S к O)**



Монитор безопасности обращений



Вопрос 2: «Формальные модели управления доступом»

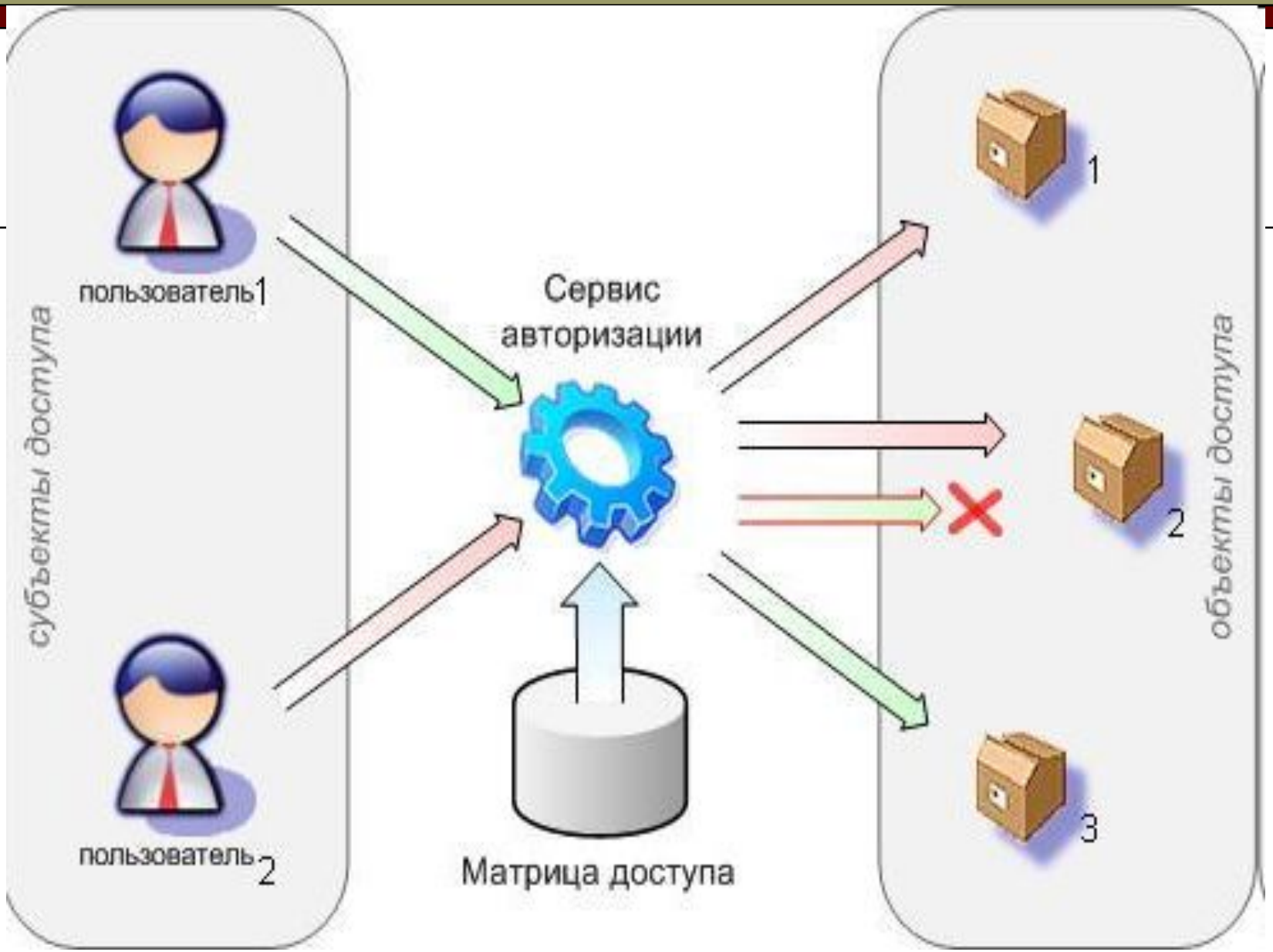
- **Назначение**
  - Формальное выражение политики безопасности по управлению доступом
- **Основные понятия и определения**
  - O – объекты системы
  - S – субъекты системы
  - R – права доступа

Типы моделей

- **Дискреционная модель** (свободная) ***Discretionary Access Control*** (права определяются владельцем).
- **Мандатная модель** (нормативная) ***Mandatory Access Control*** (установлен нормативный порядок).

Дискреционная модель

- Реализует **разграничение доступа** между поименованными **субъектами** и поименованными **объектами**.
- Для каждой пары (субъект — объект) должно быть задано явное и недвусмысленное **перечисление допустимых типов доступа** (читать, писать и т. д.), санкционированных для данного субъекта (индивида или группы индивидов) к данному ресурсу (объекту).


субъекты доступа
пользователь1
пользователь2
Сервис авторизации
Матрица доступа
объекты доступа
1
2
3

Варианты построения дискреционного управления доступом

1. Каждый объект системы имеет привязанного к нему субъекта **(владельца).** Владелец устанавливает права доступа к объекту.
2. Система имеет одного выделенного субъекта — **суперпользователя**, который имеет право устанавливать права владения для всех остальных субъектов системы.
3. Субъект с определенным правом доступа может передать это право любому другому субъекту.

- **Смешанные варианты построения:** одновременно в системе присутствуют владельцы, устанавливающие права доступа к своим объектам, так и суперпользователь.
- Реализован в большинстве операционных систем: **UNIX**- системах, системе **Windows NT.**
- Является основной реализацией разграничительной политики доступа к ресурсам **при обработке конфиденциальных сведений**, согласно требованиям к системе защиты информации.

Модель HRU (Харрисона – Руззо – Ульмана)

- **Определены множества:**
  - O – объектов доступа
  - S – субъектов доступа
  - R = {r_1,r_2…r_n}– прав доступа
- **Матрица прав доступа M**
  - Ячейка M[s, o] содержит набор {r} прав доступа субъекта S к объекту O
- **Состояние системы** Q = (S,O,M)
- Эволюция системы во времени через изменение матрицы M (действия пользователя).

Матрица прав доступа

	O1	O2	…	On
S1	orw	e		rw
S2	rw	r		
…				
Sn	w	a		r

"o" – разрешение на передачу прав доступа
"r" – чтение,
"w" – запись,
"e" – выполнение,
"a" – добавление информации.

Допускаются только следующие операции

- **Enter r into M[s, o]** (добавление субъекту s права r для объекта o)
- **Delete r from M[s, o]** (удаление у субъекту s права r для объекта o)
- **Create subject s** (создание нового субъекта s)
- **Create object o** (создание нового объекта o)
- **Destroy subject s** (удаление существующего субъекта s)
- **Destroy object o** (удаление существующего субъекта o)

Формальный критерий безопасности

- **Начальное состояние Q является безопасным относительно права r, если не существует последовательности команд, добавляющей в ячейку матрицы M право r, изначально отсутствовавшее в данной системе.**

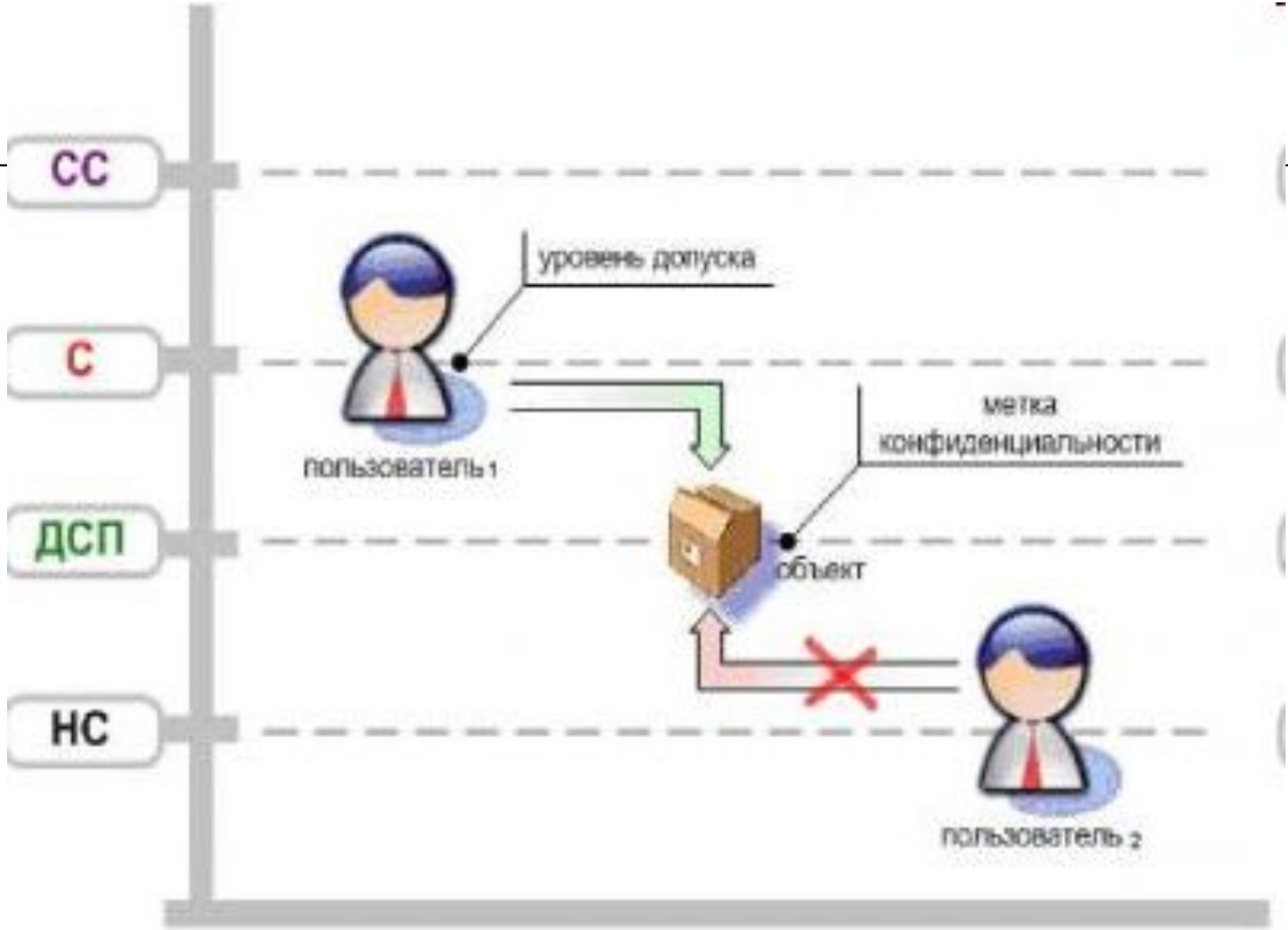
Проблемы безопасности системы

- Модель **не налагает ограничений на смысл прав доступа** и их использование в условиях команд, считая их равнозначными.
- **Алгоритмически неразрешима** (по начальному состоянию М прогноз не возможен).
- **Разрешима при ограничениях** на команды из множества С.
- Ограничения на команды **снижают практическую применимость модели**.

- Развитие модели **HRU** - модель **TAM (Time Access Matrix)**, дополненная концепцией **типов объектов и субъектов**.

Мандатная модель

- Разграничение доступа субъектов к объектам, основанное на характеризуемой:
- **меткой конфиденциальности информации**, содержащейся в объектах,
- **официальном разрешении (допуске)** субъектов обращаться к информации такого уровня конфиденциальности.

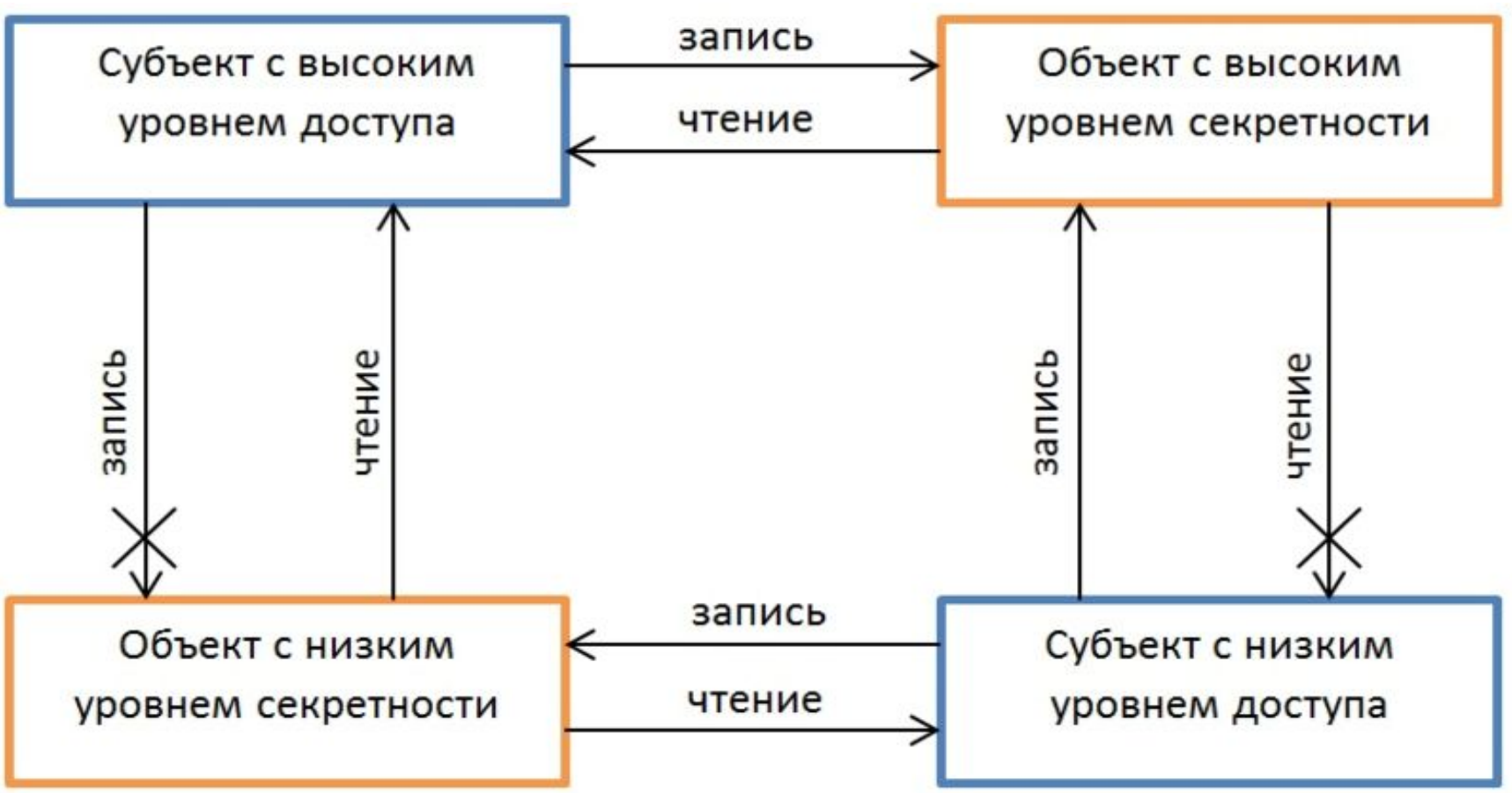

СС
С
ДСП
НС
уровень допуска
пользователь 1
метка конфиденциальности
объект
пользователь 2

Модель Белла – Ла Падулы

- ***Bell-LaPadula model*** создана в 1973-74 годах по заказу ВВС США.
- Модель описывается составляющими:
- ***Элементы*** - составные части системы:
  - Субъекты - активные объекты (пользователи, программы)
  - Объекты – пассивные объекты (документы, пароли)
  - Атрибуты доступа – всевозможные действия субъектов над объектами: чтение, запись (изменение, дополнение (без чтения).

- ***Компоненты*** - структуры, полностью описывающие состояние системы.
- ***Свойства*** :
  - ***простая безопасность:*** субъект может только читать объект, если класс доступа субъекта доминирует над классом доступа объекта (субъект может читать «вниз», но не может читать «вверх»)
  - ***свойство ограничения:*** субъект может только записать в объект, если класс доступа субъекта превосходит класс доступа объекта. Субъект может записывать «вверх», но не может записать «вниз».

Диаграмма информационных потоков



- **Модель системы $\Sigma (V_0,R,T)$ состоит из:**
- начального состояния V_0;
- множества запросов R;
- функции перехода $T: (V \times R) \rightarrow V$, которая в ходе множества запросов переводит систему из одного состояния в другое.
- **Множество состояний представляется в виде набора упорядоченных пар (F, M), где:**
  - F -функция уровня безопасности;
  - M- матрица доступа, отражающая текущую ситуацию с правами доступа субъекта к объектам.

- ***Критерий безопасности:*** достижимость только безопасных состояний.
- **Основная теорема безопасности:** если начальное состояние системы является безопасным и все последующие переходы системы из одного состояния в другое являются безопасными, то система полностью безопасна.

- При формализации многоуровневого управления безопасностью, модель Белла-Ла Падула определяет структуру класса доступа и устанавливает упорядочивание отношений между классами доступа (**доминирование**).
- Определяются два уникальных класса доступа:
  - ***SYSTEM HIGH*** (превосходит все остальные классы доступа);
  - ***SYSTEM LOW*** (превосходят все другие классы).
- **Изменения классов доступа в рамках модели Белл-Ла Падула не допускаются!**

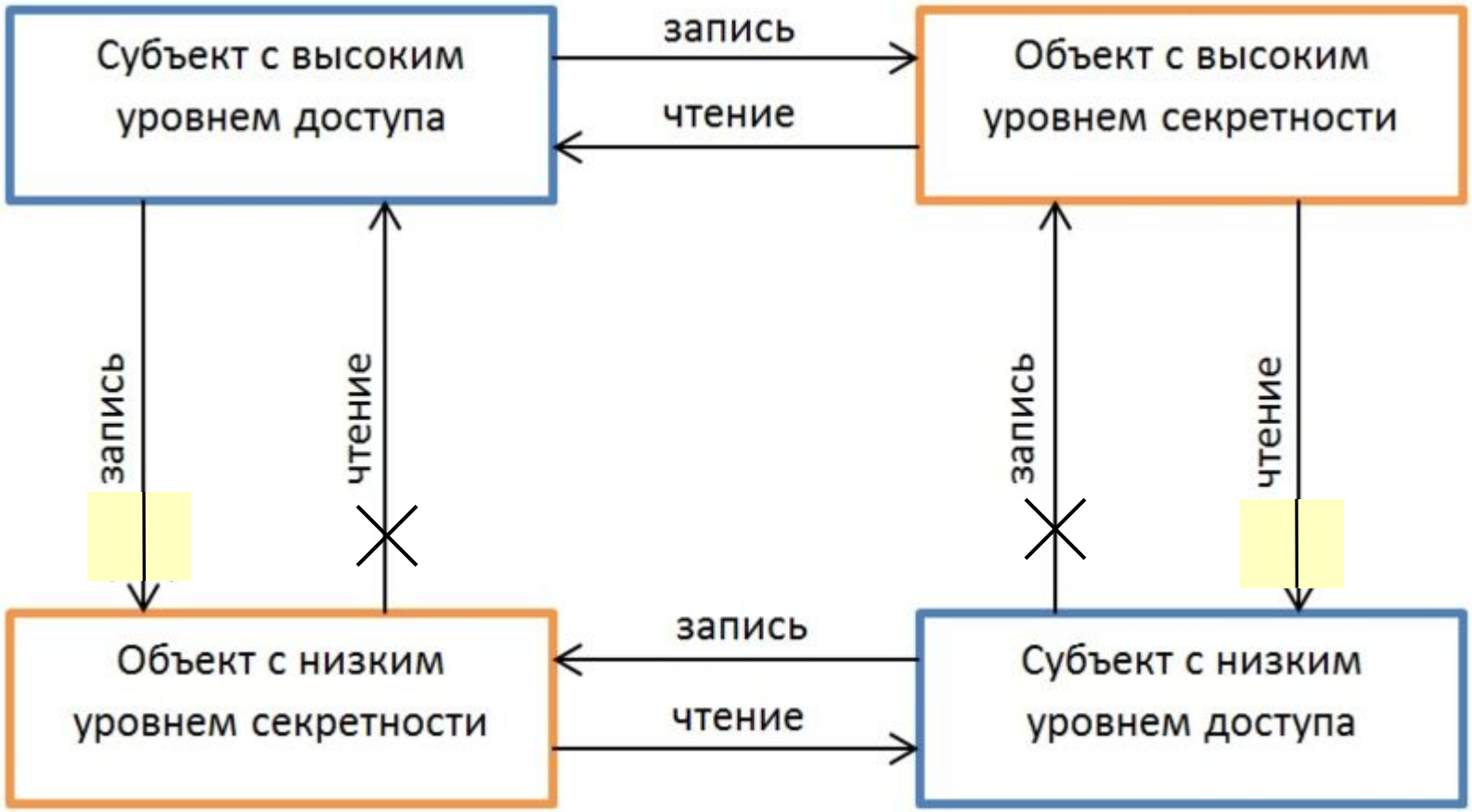
Вопрос 3: «Формальные модели обеспечения целостности»

- **Целостность информации (целостность данных)** — условие при котором данные не были изменены при выполнении любой операции над ними (передача, хранение и т.п.)
- **Примеры нарушения целостности данных:**
- изменение номера аккаунта в банковской транзакции;
- изменение при передаче информации или заражении вредоносным кодом;
- искажение фактов СМИ с целью манипуляции общественным мнением.

Модель Биба

- ***Biba Model*** разработана в 1977 году с целью добавление в модель Белла - Ла-Палуды **целостности**.
- Задача реализована путем добавления к субъектам и объектам **уровня целостности** и **запрета** общения субъектов и объектов разных уровней.

Модель Биба (критерий – целостность информации)

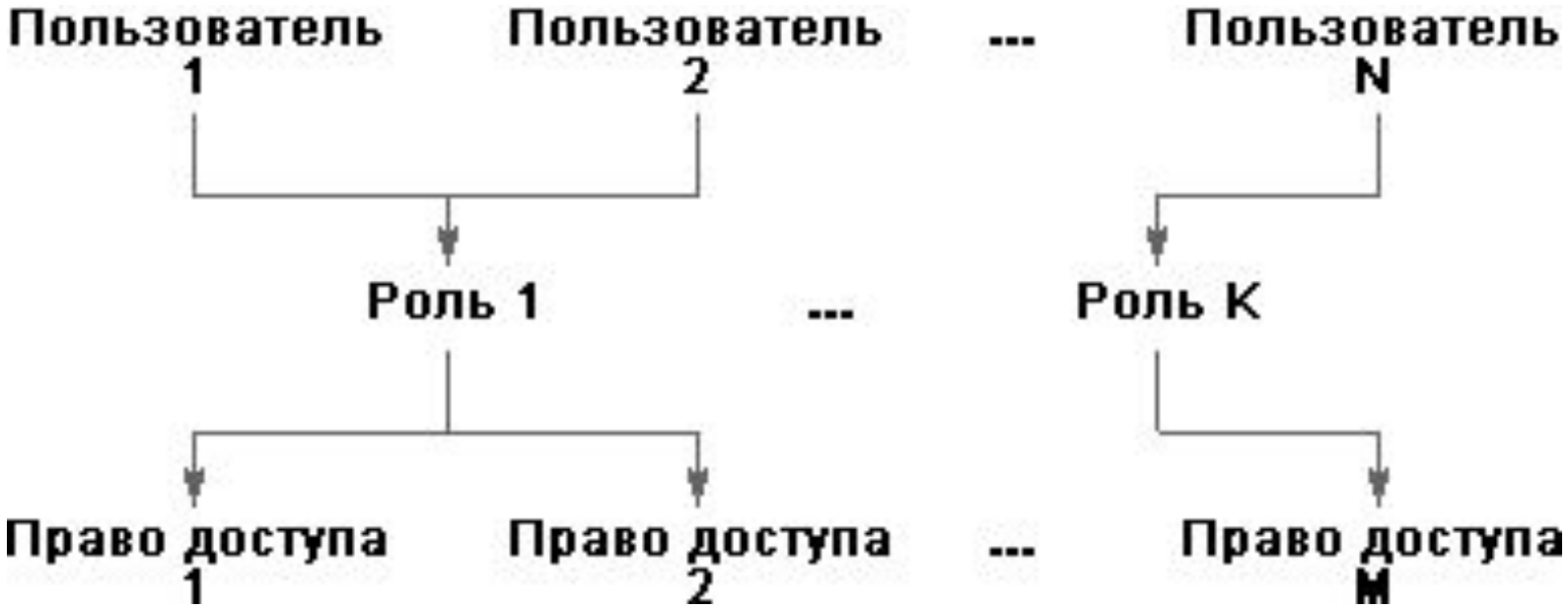


Модель Кларка-Вилсона

- ***Clark-Wilson model***, обеспечивающая требование целостности более практичным методом.
- В 1993 году модель была расширена и включила в себя разделение обязанностей.
- Основной областью применения данной модели является коммерция, банковское дело.

Вопрос 4: «Ролевое управление доступом»

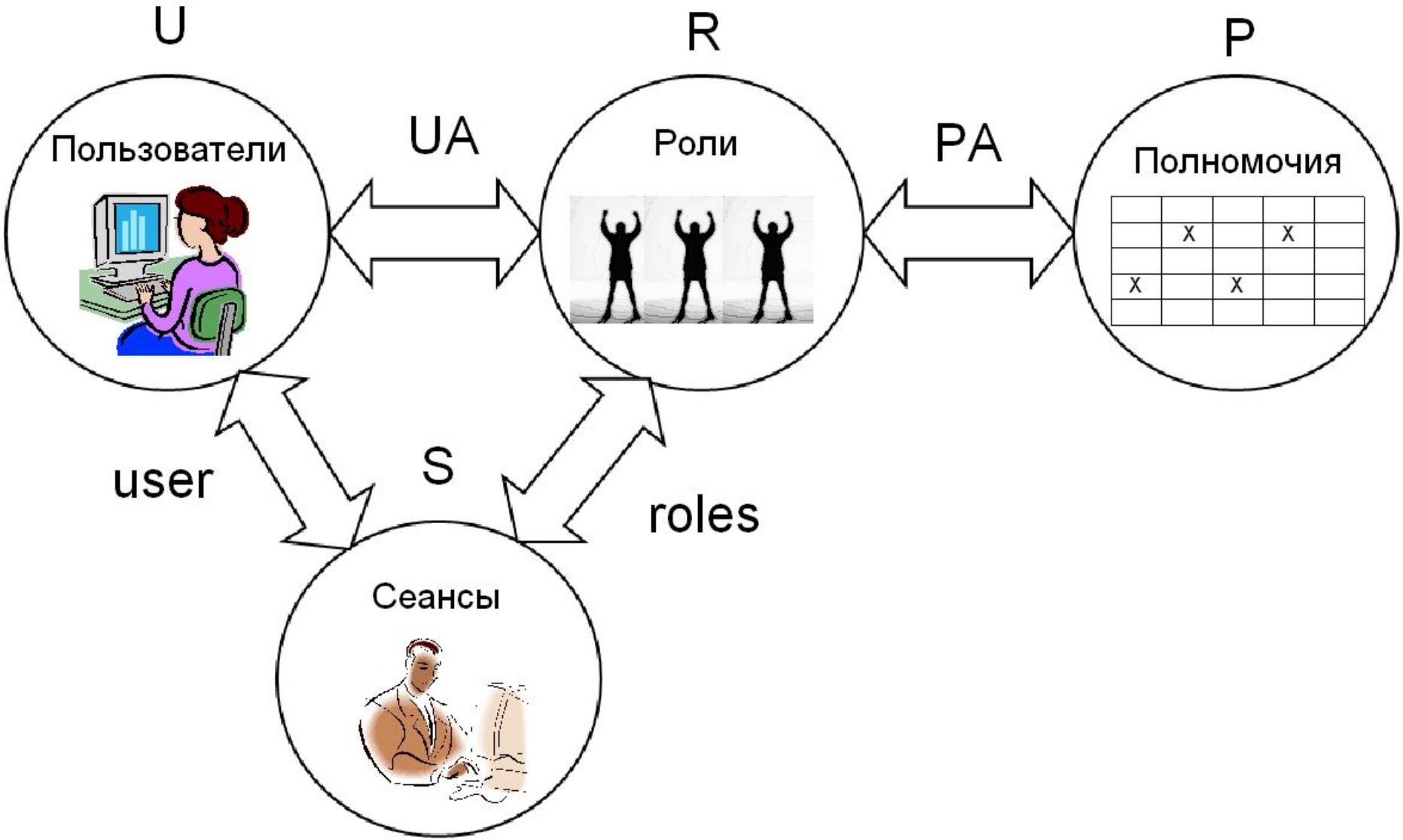
- **Роль** – одновременные полномочия для множества субъектов.



Формализация ролевой модели *(Role Based Access Control)*

- **U —** множество пользователей;
- **R —** множество ролей;
- **P —** совокупность полномочий на доступ к объектам (реализованная, в виде матрицы доступа);
- **S —** множество сеансов работы пользователей с системой.

Контроль доступа, базирующийся на ролях



Критерий безопасности ролевой модели

- Компьютерная система считается безопасной, если любой пользователь системы, работающий в сеансе **S**, может осуществлять действия, требующие полномочия **P** только в том случае, если , т.е. **разрешены данным сеансом**.

Преимущества ролевого доступа

- Нейтрален по отношению к конкретным видам прав и способам их проверки.
- **Облегчает администрирование** (Ролей должно быть значительно меньше, чем пользователей).
- **Число администрируемых связей пропорционально сумме** (а не произведению) количества пользователей и объектов.

Иерархия ролей

- Для каждого пользователя одновременно могут быть активными ***несколько ролей.***
- Между ролями может быть определено ***наследование.***
- Отношение наследования является ***иерархическим.***

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лекция 8:

«Способы и средства защиты информации»

Вопросы:

1. **Способы защиты информации.**
2. **Средства защиты информации.**

Вопрос № 1: «Способы защиты информации»

- **Способ защиты информации** - порядок и правила применения определенных принципов и средств защиты информации.

К основным способам защиты информации относятся:

1. **Маскировка информации.**
2. **Препятствие на пути злоумышленника.**
3. **Мотивация.**
4. **Принуждение.**
5. **Регламентация доступа к информации.**
6. **Управление силами и средствами защиты.**

1. Маскировка информации

- **Преобразования информации**, вследствие которых она становится недоступной для злоумышленников или такой доступ существенно затрудняется.
- Реализуется **криптографическими методами** преобразования информации, скрытием объекта (информации), дезинформацией и легендированием, созданием шумовых полей, маскирующих информационных сигналов.

2. Препятствие на пути злоумышленника

- Создание на пути дестабилизирующего фактора **барьера**, не позволяющего соответствующему фактору принять опасные размеры.
- Примеры препятствий: **физические препятствия, блокировки**, экранирование помещений и технических средств и т д.

3. Мотивация

- Способ защиты информации, при котором пользователи и персонал объекта, внутренне руководствуясь моральными, этическими, психологическими побуждениями или материальными поощрениями **сознательно соблюдают все правила обработки и хранения конфиденциальной информации.**

4. Принуждение

- Способ защиты, при котором пользователи и персонал системы **вынуждены соблюдать правила** обработки, передачи и использования защищаемой информации под угрозой **материальной, административной или уголовной ответственности.**

5. Регламентация доступа к информации

- Разработка и реализация комплекса мероприятий, создающих **условия, при которых существенно затрудняются** проявление и воздействие угроз.
- **Разработка правил** обращения с КИ и средствами ее обработки, максимально затрудняющими получение этой информации злоумышленником.

6. Управление силами и средствами защиты

- Выработка управляющих воздействий на элементы системы защиты, которые должным образом **реагируют на проявление дестабилизирующих воздействий.**
- **Для управления необходим** сбор, передача, обобщение и анализ данных.

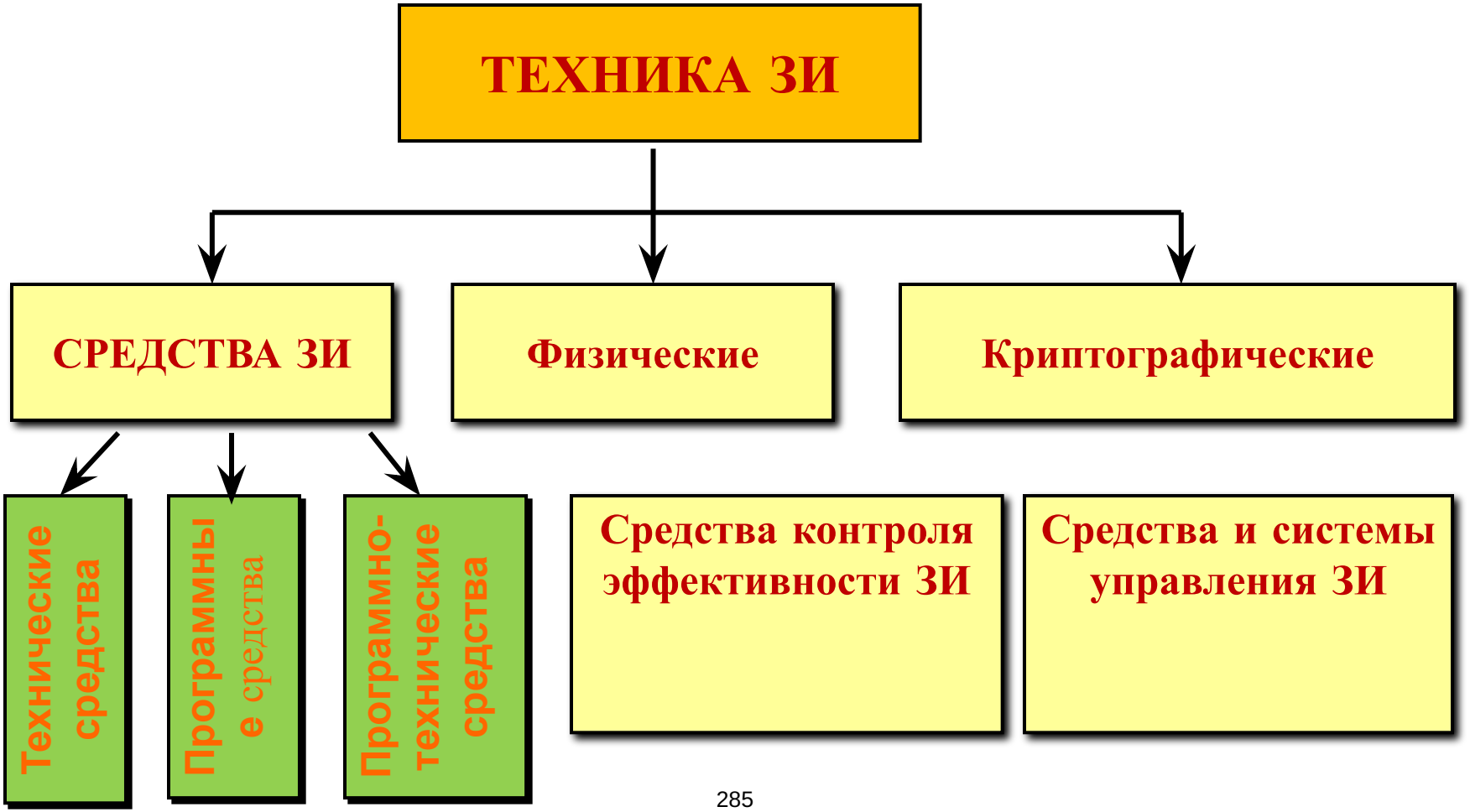
Вопрос № 2: «Средства защиты информации»

- **Средство защиты информации:** **техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.**
  - ***ГОСТ Р 50922-2006 Государственный стандарт РФ. Защита информации. Основные термины и определения***

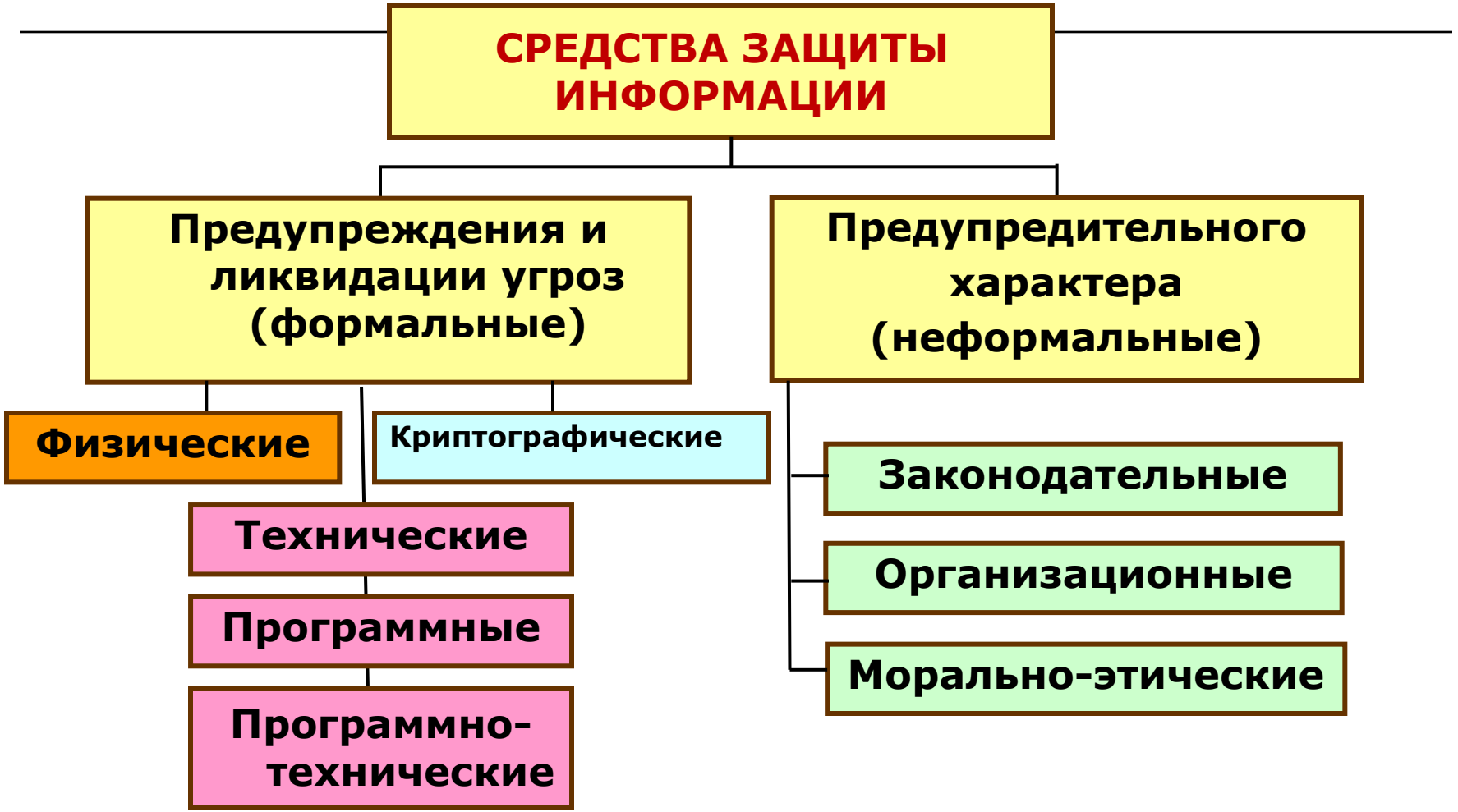

ФОРМАЛЬНЫЕ
Физические
Криптографические
Технические
Программные
Управление
Препятствие
Маскировка
Регламентация
Побуждение
Принуждение
Методы защиты данных
НЕФОРМАЛЬНЫЕ
Организационные
Законодательные
Морально-этические
Средства защиты данных

- **Техника защиты информации** - средства защиты информации, в том числе средства **физической** защиты информации, **криптографические средства** защиты информации, средства **контроля эффективности** защиты информации, средства и системы **управления**, предназначенные для обеспечения защиты информации.

Техника защиты информации (ГОСТ Р 50922-2006)



Средства защиты информации



- **Средство физической защиты информации -** средство защиты информации, предназначенное или используемое для обеспечения **физической защиты объекта защиты информации.**
- **Напоминание: физическая** ЗИ - путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных **физических** лиц к объекту **защиты**.

Средство физической защиты информации

- **Криптографическое средство защиты информации** - средство защиты информации, **реализующее алгоритмы криптографического преобразования информации**.

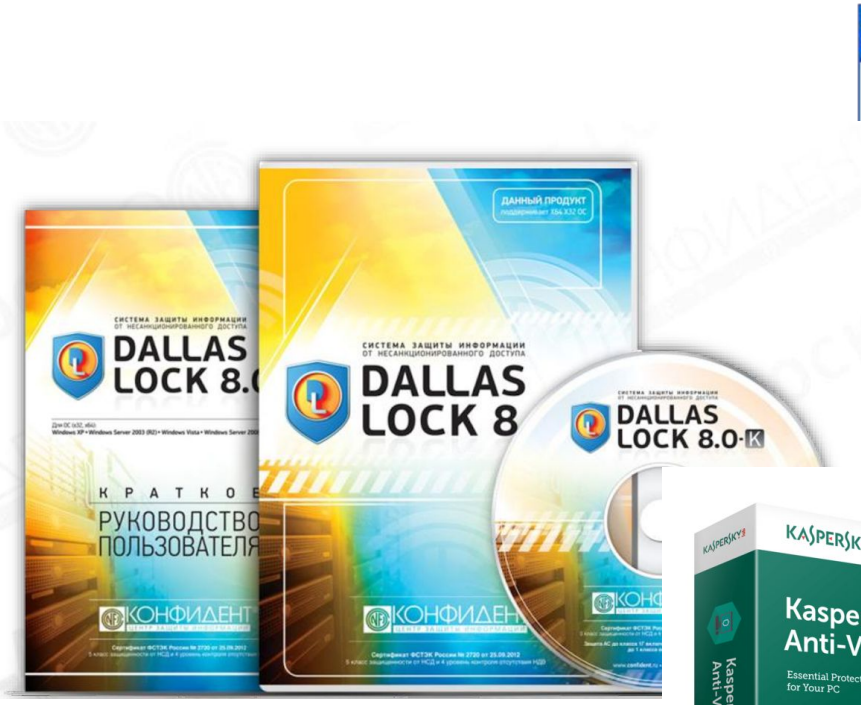
Криптографическое средство защиты информации

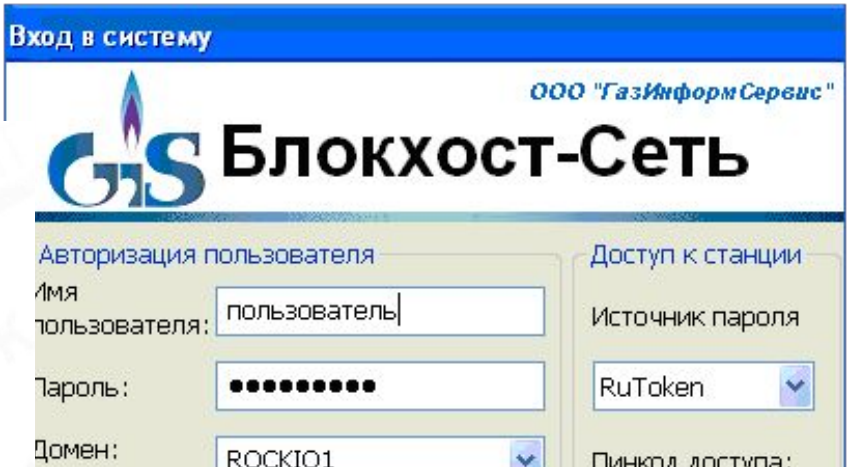
КриптоПро
РУТОКЕН CSP

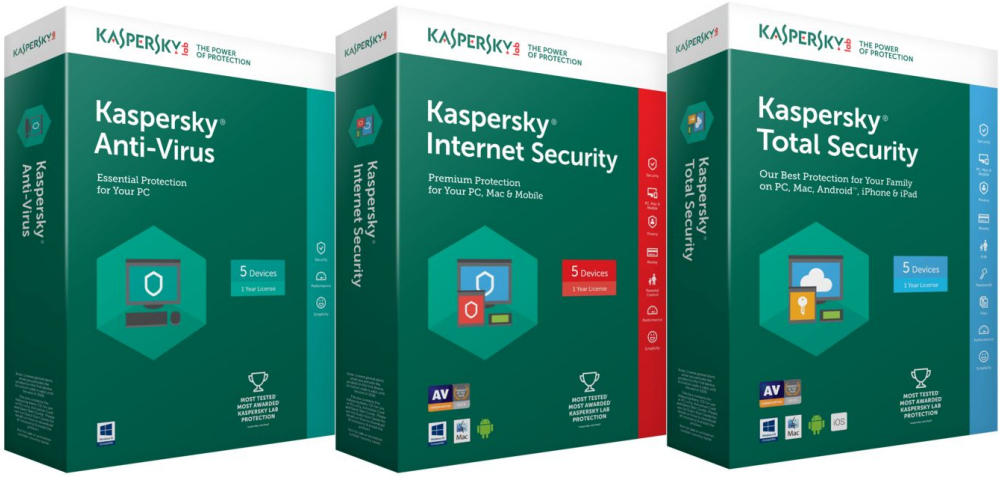
- **Техническая защита информации (ТЗИ) –** защита информации, заключающаяся в обеспечении безопасности информации (данных) **некриптографическими методами** , подлежащей (подлежащих) защите в соответствии **с действующим законодательством**, с применением **технических, программных и программно-технических средств**.

Техническое средство защиты информации

Программное средство защиты информации







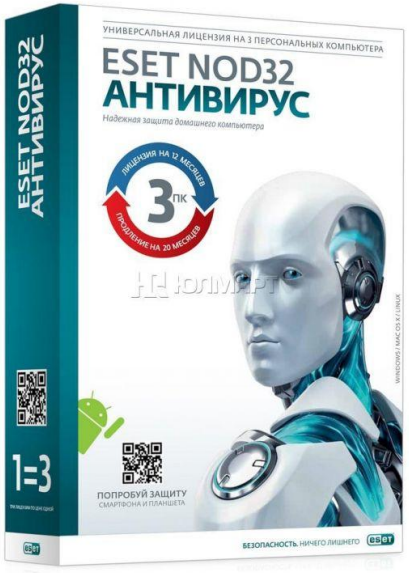
Программно-техническое средство защиты информации

Типовые СЗИ

- **Системы обнаружения /предотвращения вторжений (СОВ) *(Intrusion Prevention System/Intrusion Detection System IDS/IPS)*** – комплекс ПАС для выявления фактов и предотвращения попыток НСД в корпоративную систему.

Средства антивирусной защиты (САВЗ)

- Acronis AntiVirus • AVS • AhnLab Internet Security • AOL Virus Protection • ArcaVir • Ashampoo AntiMalware • Avast! • AVG • Avira AntiVir • AVZ • A-square anti-malware • BitDefender • CA Antivirus • Clam Antivirus • ClamWin • Command Anti-Malware • Comodo Antivirus • Dr.Web • eScan Antivirus • F-PROT Antivirus • F-Secure Anti-Virus • ; • Graugon Antivirus• IKARUS нтивирус Касперского • I osoft Security Essentials • Multicore antivirus • NO orton AntiVirus • Outpost ivirus • PC-cillin • TrustPo ıs • Quick Heal AntiVirus n`Sec • Simple Antivirus • сБлокАда • ViRobot • Vir ooch • Zillya! • ZoneAlarm Antivirus



Типы средств антивирусной защиты (САВЗ)

- **САВЗ типа «А»** – САЗ, предназначенные **для централизованного администрирования** средствами антивирусной защиты, установленными на компонентах ИС (серверах, АРМ);
- **САВЗ типа «Б»** – САЗ, предназначенные **для применения на серверах** ИС;
- **САВЗ типа «В»** – САЗ, предназначенные **для применения на АРМ** местах ИС;
- **САВЗ типа «Г»** – САЗ, предназначенные **для применения на автономных АРМ**.

Типовые СЗИ

- **Средства (модули) доверенной загр узки(СДЗ, МДЗ)** - защита данных от угроз НСД и защиты от вирусных атак на BIOS.

Типовые СЗИ

- **Средства контроля съемных носителей (СКН) -** контроль использования интерфейсов ввода/вывода СВТ, подключения внешних ПАС и конкретных СМН информации.
- **Межсетевые экраны (МЭ, Firewall) -** АПС/АС для контроля и фильтрации проходящих через него сетевых пакетов в соответствии с заданными правилами.

Средства межсетевого экранирования

- **Бесплатные:** Outpost Security Suite Free • Ashampoo FireWall Free • Comodo • Core Force (англ.) • Online Armor • PC Tools • PeerGuardian (англ.) • Sygate (англ.)
- **Проприетарные:** Ashampoo FireWall Pro • AVG Internet Security • CA Personal Firewall • Jetico (англ.) • Kaspersky • Microsoft ISA Server • Norton • Outpost • Trend Micro (англ.) • Windows Firewall • Sunbelt (англ.) • Kerio Control
- **Для Linux:** Netfilter (Iptables • Firestarter • Iplist • NuFW • Shorewall) • Uncomplicated Firewall

- **Средство контроля эффективности защиты информации -** средство защиты информации, предназначенное или используемое для контроля эффективности защиты информации.

Сетевые сканеры безопасности

- для инвентаризации сетевых ресурсов;
- в ходе проведения «тестов на проникновение»;
- в процессе проверки систем на соответствие различным требованиям.
  - **Nessus**
  - **MaxPatrol**
  - **Internet Scanner**
  - **Retina Network Security Scanner**
  - **Shadow Security Scanner (SSS)**
  - **NetClarity Auditor**

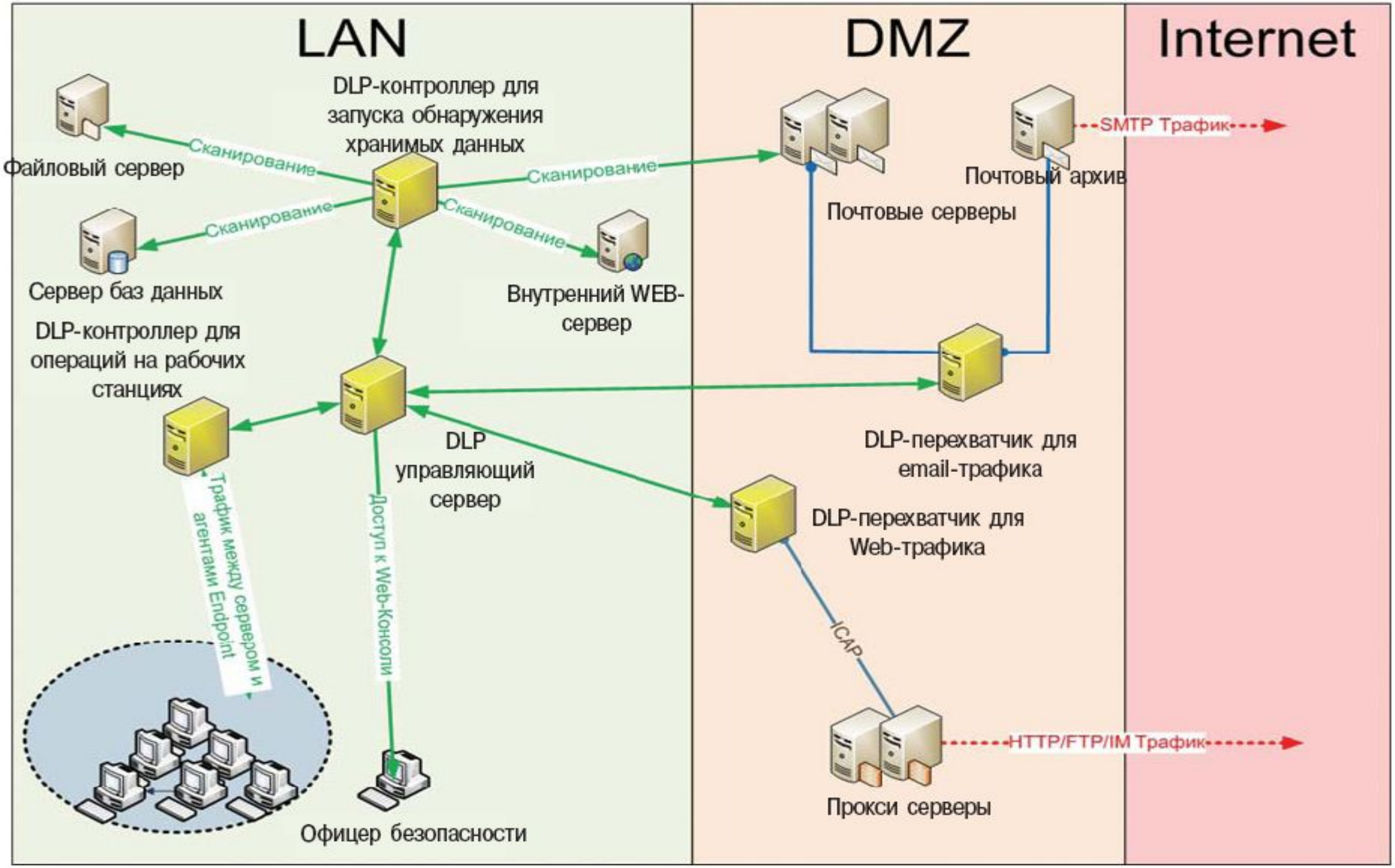
Средства предотвращения утечек информации

- **DLP (*Data Loss Prevention*) — технологии предотвращения утечек КИ из информационной системы.**
- При детектировании в потоке КИ, пересекающего периметр системы, срабатывает **активная компонента** и передача сообщения (пакета, потока, сессии) **блокируется.**

SearchInform

«Контур информационной безопасности SearchInform»

Типовая архитектура построения системы защиты информации на основе DLP технологии

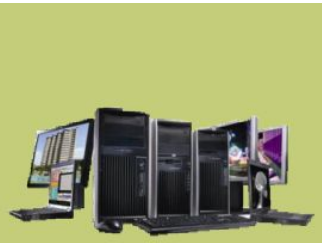


Технология SIEM

- **SIEM (Security information and event management):**
- **SIM** (*Security information management*) — управление информационной безопасностью;
- **SEM** (*Security event management*) — управление событиями безопасности.
- **Анализ в реальном времени событий ИБ, исходящих от сетевых устройств и приложений.**

MaxPatrol SIEM

Комплексные решения в обеспечении защиты информации



Рабочие станции и сервера

СЗИ от НСД

АПМДЗ

СЗИ от НСД (linux)

МЭ

САВЗ, МЭ, HIPS

Доверенная ЭЦП (Jinn)

Код Безопасности

Secret MDM

Мобильные устройства

АПКШ Континент

- АПКШ Континент L3VPN
- АПКШ Континент L2VPN
- АПКШ Континент СД
- Континент АП
- Континент TLS VPN
- Континент ДА (IDC/IPS)
- Континент WAF
- Континент Т-15Т

Локальные сети и межсетевое взаимодействие

vGate for VMware vSphere
vGate for Microsoft Hyper-V

Виртуализация

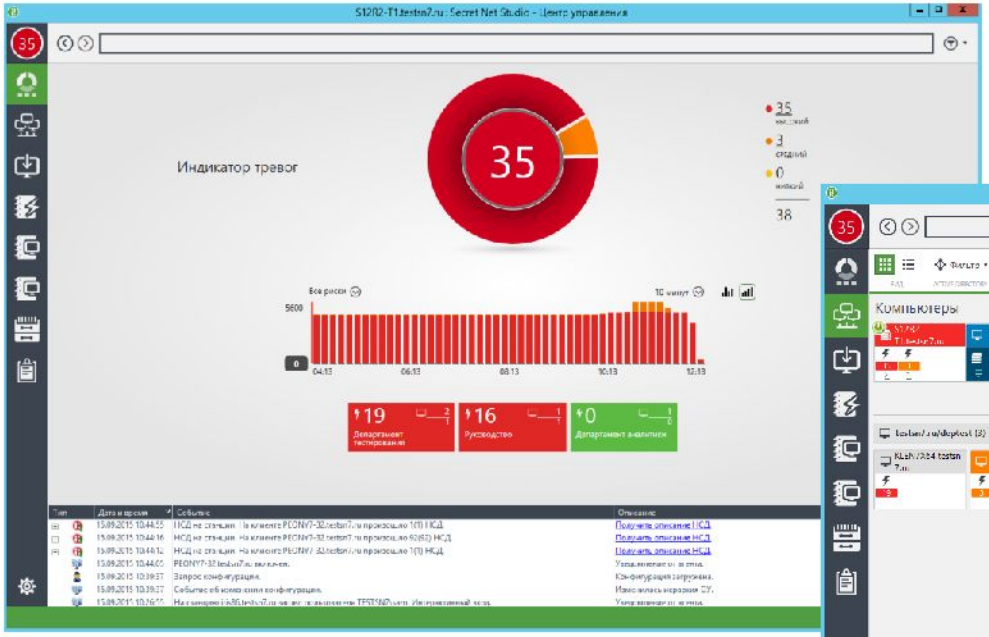
КОД БЕЗОПАСНОСТИ

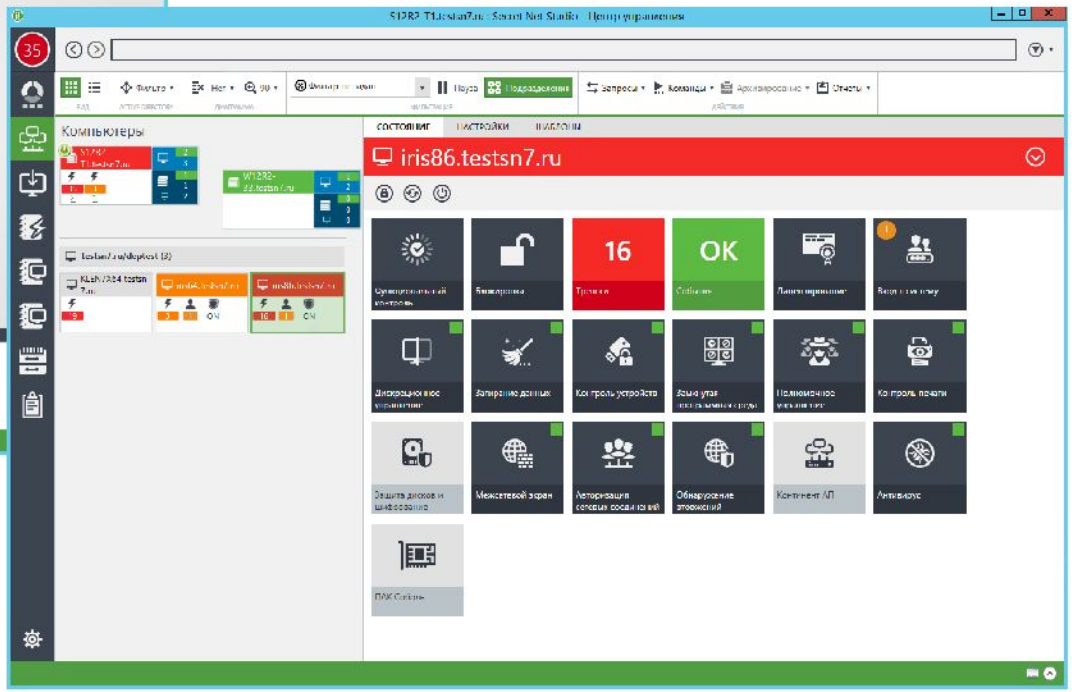
ЗАЩИТНЫЕ МЕХАНИЗМЫ

- Шифрование данных
- Теневое копирование
- Маркировка документов
- Замкнутая программная среда
- Межсетевой экран
- Авторизация сетевых соединений
- Защита от вторжений
- «Континент-АП» (VPN-клиент)
- Усиленный вход в систему
- Контроль целостности
- Антивирус
- Дискреционное управление доступом
- Мандатное управление доступом
- Затирание данных
- Контроль устройств
- Контроль печати
- Интеграция с ПАК «Соболь»

КОД БЕЗОПАСНОСТИ

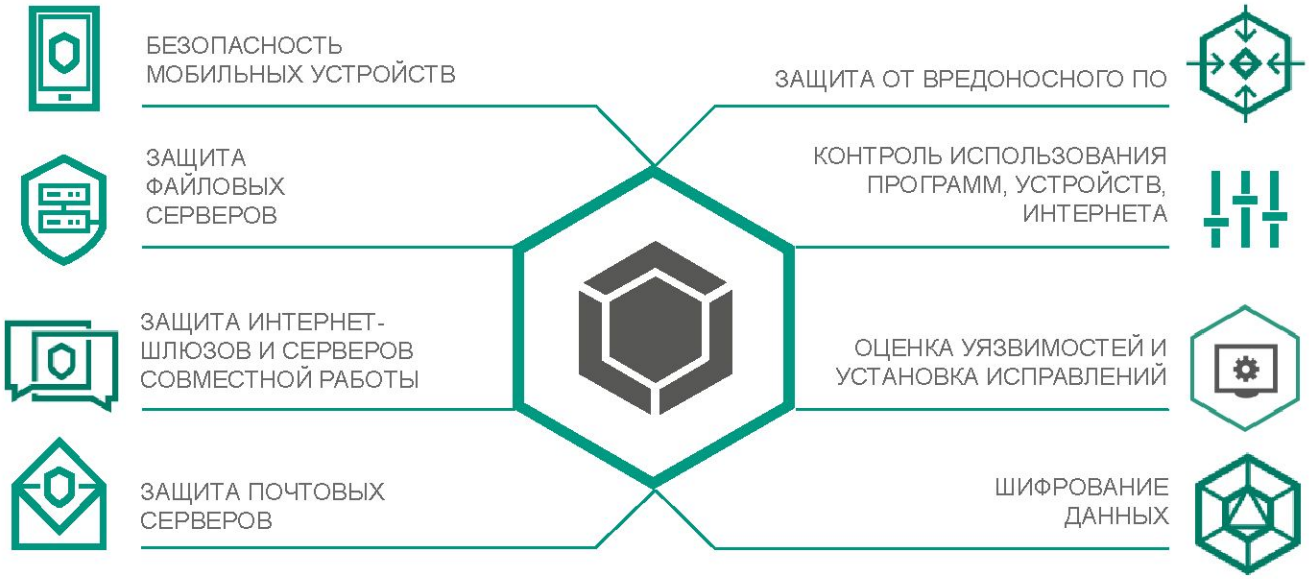
ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИ





KASPERSKY SECURITY ДЛЯ БИЗНЕСА: КРАТКИЙ ОБЗОР ЛИНЕЙКИ

Kaspersky **TOTAL** Security для бизнеса



ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лекция 9:

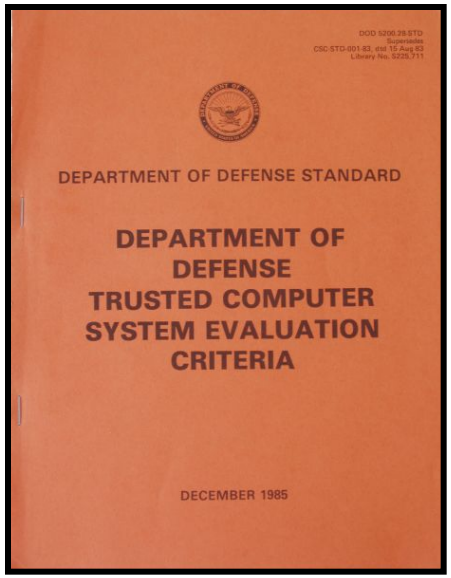
«Критерии оценки защищенности информационных систем»

Вопросы:

1. Критерии безопасности компьютерных систем.
2. Критерии и классы защищенности СВТ и АС (РД ГТК).
3. Общие критерии безопасности информационных технологий.
4. Руководящие документы (РД) ФСТЭК России.
5. Стандарты по управлению ИБ ISO/IEC 27000.

Вопрос 1: «Критерии безопасности компьютерных систем

- **«Критерии безопасности компьютерных систем министерства обороны США»**
- ***(Trusted Computer System Evaluation Criteria -TCSEC) «Оранжевая книга»***
- **Категории требований безопасности:**
  - политика безопасности;
  - аудит;
  - корректность.



Политика безопасности

- **Требование 1. Политика безопасности.** Система должна поддерживать точно определенную политику безопасности **(управление доступом).**
- **Требование 2. Метки.** С объектами ассоциированы метки безопасности, **определяющие степень конфиденциальности (гриф секретности)** объекта.

Аудит

- **Требование 3. Идентификация и аутентификация.** Все субъекты должны иметь уникальные идентификаторы. Контроль доступа на основании **(аутентификации)** и правил разграничения доступа.
- **Требование 4. Регистрация и учет.** Все происходящие события, важные с точки зрения безопасности, должны отслеживаться и **регистрироваться в защищенном протоколе**.

Корректность

- **Требование 5. Контроль корректности функционирования средств защиты.** Средства защиты содержат компоненты, обеспечивающие работоспособность функций защиты.
- **Требование 6. Непрерывность защиты.** Все средства защиты должны быть защищены от несанкционированного вмешательства и/или отключения.

Классы безопасности компьютерных систем TCSEC

- **группа D -** Minimal Protection (минимальная защита)
- **группа C** (C1, C2) - Discretionary Protection (избирательная защита).
- **группа B** (B1, B2,B3)- Mandatory Protection (полномочная защита).
- **группа A -** Verified Protection (проверяемая защита).

Интерпретации TCSEC

- **Для компьютерных сетей** (Trusted Network Interpretation);
- **Для систем управления базами данных** (Trusted Database Management System Interpretation).

Недостатки TCSEC:

- не рассматриваются **угрозы доступности**;
- **не учитывается специфика** конкретных систем и продуктов;
- **не формализованы методы проверки корректности** и адекватности реализации функциональных требований;
- некоторые **требования неоднозначно трактуются**.

Вопрос 2: «Критерии и классы защищенности СВТ и АС»

- **Руководящие документы (РД ГТК/ФСТЭК России):**
- **Защита от НСД к информации. Термины и определения.**
- **Концепция защиты СВТ от НСД к информации.**
- **СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации.**

- **АС. Защита от НСД к информации. Классификация АС и требования по защите информации.**
- **СВТ. МЭ. Защита от НСД к информации. Показатели защищенности от НСД к информации**
- **Защита от НСД к информации. Часть 1. ПО средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей.**

Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации

Категории, содержащие информационные материалы:

Законы 3

Указы 5

Постановления 1

Приказы 6

Специальные нормативные документы 12

Национальные стандарты 1

Проекты 1

Если заметили ошибку в тексте, выделите ее курсором мыши и нажмите Ctrl + Enter или воспользуйтесь сервисом Обратной связи в правом верхнем углу страницы

Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации

Создано: 05 февраля 2021 г. 11:56 Обновлено: 16 февраля 2021 г. 16:37 Просмотров: 49408

Методический документ. Утвержден ФСТЭК России 5 февраля 2021 г.

PDF	Методический документ. Утвержден ФСТЭК России 5 февраля 2021 г.	2679 КБ	122041
RTF	Методический документ. Утвержден ФСТЭК России 5 февраля 2021 г.	448883 КБ	20562

Методика оценки угроз безопасности информации

Методический документ

Создано: 26 июня 2018 г. 09:55 Обновлено: 11 июля 2018 г. 13:16 Просмотров: 16767

Методический документ. Утвержден ФСТЭК России 26 июня 2018 г.

PDF	Методический документ	308 КБ	9370
RTF	Методический документ	361 КБ	2513

Регламент включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в Банк данных угроз безопасности информации ФСТЭК России

Методический документ

Создано: 18 февраля 2014 г. 14:29 Обновлено: 12 января 2015 г. 07:36 Просмотров: 91083

Методический документ. Утвержден ФСТЭК России 11 февраля 2014 г.

PDF	Методический документ	1349 КБ	313334

Меры защиты информации в государственных информационных системах

Методический документ

Создано: 09 января 2008 г. 13:00 Обновлено: 09 января 2013 г. 14:00 Просмотров: 144698

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год

PDF	Модель	2088 КБ	447585

При рассмотрении угроз утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН) необходимо применять полную версию данного документа

Создано: 09 января 2008 г. 13:00 Обновлено: 06 мая 2015 г. 09:10 Просмотров: 251706

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год

PDF	Методика	303 КБ	128961

СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации

- Применяются к общесистемным программным средствам и операционным системам.
- Конкретные перечни показателей определяют **классы защищенности СВТ.**
- Уменьшение или изменение перечня показателей, соответствующего конкретному классу защищенности СВТ, **не допускается.**

Требования к защищенности АС

Наименование показателя	Класс защищенности					
	6	5	4	3	2	1
Дискреционный принцип контроля доступа	+	+	+	=	+	=
Мандатный принцип контроля доступа	-	-	+	=	=	=
Очистка памяти	-	+	+	+	=	=
Изоляция модулей	-	-	+	=	+	=
Маркировка документов	-	-	+	=	=	=
...						
Текстовая документация	+	+	+	+	+	=
Конструкторская (проектная) документация	+	+	+	+	+	+

АС. Защита от НСД к информации. Классификация АС и требования по защите информации

- Распространяется на все действующие и проектируемые АС учреждений, организаций и предприятий, **обрабатывающие КИ.**
- Деление АС на классы **в целях разработки и применения обоснованных мер по достижению требуемого уровня ЗИ.**
- **Дифференциация определяется:**
  - важностью обрабатываемой информации;
  - различием АС;
  - количественному и качественному составу пользователей и обслуживающего персонала.

КЛАССИФИКАЦИЯ АС

9 КЛАССОВ ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА:

1 А | 1 Б | 1 В | 1 Г | 1 Д | 2 А | 2 Б | 3 А | 3 Б

3 ГРУППЫ АС:

П Е Р В А Я
Многопользовательские АС, с информацией разного уровня конфиденциальности. Пользователи имеют разные права доступа к информации.

В Т О Р А Я
Многопользовательские АС, с информацией разного уровня конфиденциальности. Пользователи имеют одинаковые права доступа к информации.

Т Р Е Т Ь Я
Однопользовательская АС, с информацией одного уровня конфиденциальности.

Соответствие классов защищенности МЭ и АС

Класс МЭ	Класс АС
5	1Д
4	1Г
3	1В
2	1Б
1	1А

Вопрос 3: «Общие критерии безопасности информационных технологий»

- **Стандарт ISO/IEC 15408 «Common Criteria» «Общие критерии»**
- **Не содержат предопределенных «классов безопасности».**
- Классы строятся, исходя из **требований безопасности**, существующих для **конкретной организации и/или конкретной ИС.**
- **ГОСТ Р ИСО/МЭК 15408-2002**

Объект оценки

- **Объект оценки – произвольный продукт IT, или система с руководствами администратора и пользователя** (например, ОС, средство ЗИ, АСУ и т.п.)
- **Категории пользователей:**
  - потребители;
  - разработчики»;
  - оценщики.

Среда безопасности ОО

Среда безопасности ОО

- **Законодательная среда** (законы и НПА);
- **Административная среда** (политики безопасности);
- **Процедурная среда** (меры физической защиты, персонал);
- **Программно-техническая среда** (назначение ОО, области применения).

При подготовке к оценке формализуются аспекты среды ОО

1. **Предположения безопасности** (границы рассмотрения).
2. **Угрозы безопасности:**
   - источник угрозы;
   - метод воздействия;
   - уязвимые места, которые могут быть использованы;
   - ресурсы (активы), которые могут пострадать.

- **Политики безопасности.**

Классы функциональных требований

(11 классов, 66 семейств, 135 компонентов)

1. **идентификация и аутентификация;**
2. **защита данных пользователя;**
3. **защита функций безопасности;**
4. **управление безопасностью;**
5. **аудит безопасности;**
6. **доступ к объекту оценки;**
7. **приватность;**
8. **использование ресурсов;**
9. **криптографическая поддержка;**
10. **связь;**
11. **доверенный маршрут/канал.**

Классы требований доверия
(10 классов, 44 семейств, 93 компонента)

1. **разработка** (требования для поэтапной детализации функций безопасности от краткой спецификации до реализации);
2. **поддержка жизненного цикла** (требования к модели жизненного цикла, включая порядок устранения недостатков и защиту среды разработки);
3. **тестирование;**
4. **оценка уязвимостей** (включая оценку стойкости функций безопасности);
5. **поставка и эксплуатация;**
6. **управление конфигурацией**;
7. **руководства** (требования к эксплуатационной документации);
8. **поддержка довери**я (для поддержки этапов жизненного цикла после сертификации);
9. **оценка профиля защиты;**
10. **оценка задания по безопасности**.

Документы, разрабатываемые для объекта оценки

- **Профиль защиты (ПЗ)** - типовой набор требований, которым должны удовлетворять продукты и/или системы определенного класса (*ОС на компьютерах в правительственных организациях*).
- **Задание по безопасности** содержит совокупность требований к конкретной разработке, выполнение которых обеспечивает достижение поставленных целей безопасности.

Вопрос 4: «Руководящие документы ФСТЭК России»

- **РД ГТК** Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности.
- **Приказ ФСТЭК России от 31 августа 2010 г. № 489** Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования.

- **Приказ ФСТЭК России №17 от 11.02.2013 Об утверждении Требований о ЗИ, не составляющей ГТ, содержащейся в ГИС.**
- **Приказ ФСТЭК России №21 от 18.02.2013 Состав и содержание организационных и технических мер по обеспечению безопасности ПДн при обработке в ИС ПДн для каждого УЗ.**
- **Приказ ФСТЭК России №31 от 14.03.2014 Об утверждении Требований к обеспечению ЗИ в АСУ ТП на КВО…».**
- **Приказ ФСТЭК России №239 от 25.12.2017 Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ.**

Уровни защищенности персональных данных

Тип ИСПДн	Сотрудники оператора	Количество субъектов	Тип актуальных угроз		
			1	2	3
ИСПДн-С	Нет	> 100 000	УЗ-1	УЗ-1	УЗ-2
	Нет	< 100 000	УЗ-1	УЗ-2	УЗ-3
	Да				
ИСПДн-Б			УЗ-1	УЗ-2	УЗ-3
ИСПДн-И	Нет	> 100 000	УЗ-1	УЗ-2	УЗ-3
	Нет	< 100 000	УЗ-2	УЗ-3	УЗ-4
	Да				
ИСПДн-О	Нет	> 100 000	УЗ-2	УЗ-2	УЗ-4
	Нет	< 100 000	УЗ-2	УЗ-3	УЗ-4
	Да				

Классы защищенности ГИС

Уровень значимости информации	Масштаб информационной системы		
	Федеральный	Региональный	Объектовый
УЗ 1	К1	К1	К1
УЗ 2	К1	К2	К2
УЗ 3	К2	К3	К3

Меры по ЗИ ИСПДн (Пр.ФСТЭК № 21)

Номер и условное обозначен. меры	Меры по обеспечению безопасности ПДн	Уровень защищенности ПДн			
		4	3	2	1
		Количество мер			
1.	Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	5	5	6	6
2.	Управление доступом субъектов доступа к объектам доступа (УПД)	10	12	13	13
3.	Ограничение программной среды (ОПС)	0	0	1	2
4.	Защита машинных носителей ПДн (ЗНИ)	0	1	3	3
5.	Регистрация событий безопасности (РСБ)	4	4	5	5
6.	Антивирусная защита (АВЗ)	2	2	2	2
7.	Обнаружение вторжений (СОВ)	0	0	2	2
8.	Контроль (анализ) защищенности персональных данных (АНЗ)	1	4	5	5

Меры по ЗИ ИСПДн (Пр.ФСТЭК № 21)

Номер и условное обозначен. меры	Меры по обеспечению безопасности ПДн	Уровень защищенности ПДн			
		4	3	2	1
		Количество мер			
9.	Обеспечение целостности информационной системы и персональных данных (ОЦЛ)	0	0	2	2
10.	Обеспечение доступности персональных данных (ОДТ)	0	0	2	3
11.	Защита среды виртуализации (ЗСВ)	2	5	8	8
12.	Защита технических средств (ЗТС)	2	2	2	2
13.	Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	1	2	5	6
14.	Выявление инцидентов и реагирование на них (ИНЦ)	0	0	6	6
15.	Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)	0	4	4	4

Требования к СЗИ от утечки за счет НСД

Требования к системам обнаружения вторжений

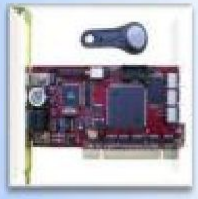
утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638 (зарегистрирован Минюстом России)

12 методических документов, содержащих профили защиты систем обнаружения вторжений

Требования к средствам антивирусной защиты

утверждены приказом ФСТЭК России от 20 марта 2012 г. № 28, зарегистрирован Минюстом России

24 методических документа, содержащих профили защиты средств антивирусной защиты



Требования к средствам доверенной загрузки

утверждены приказом ФСТЭК России от 27 сентября 2013 г. № 119 (зарегистрирован Минюстом России)

10 методических документов, содержащих профили защиты средств доверенной загрузки

Требования к средствам контроля съемных машинных носителей информации

утверждены приказом ФСТЭК России от 28 июля 2014 г. № 87 (зарегистрирован Минюстом России)

10 методических документов, содержащих профили защиты средств контроля съемных МНИ

Требования к межсетевым экранам

утверждены приказом ФСТЭК России от 9 февраля 2016 г. № 9 (зарегистрирован Минюстом России)

24 методических документа, содержащих профили защиты межсетевых экранов

Требования безопасности информации к операционным системам

утверждены приказом ФСТЭК России от 19 августа 2016 г. № 119 (зарегистрирован Минюстом России)

18 методических документов, содержащих профили защиты операционных систем

Требования к межсетевым экранам

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ (ФСТЭК РОССИИ)

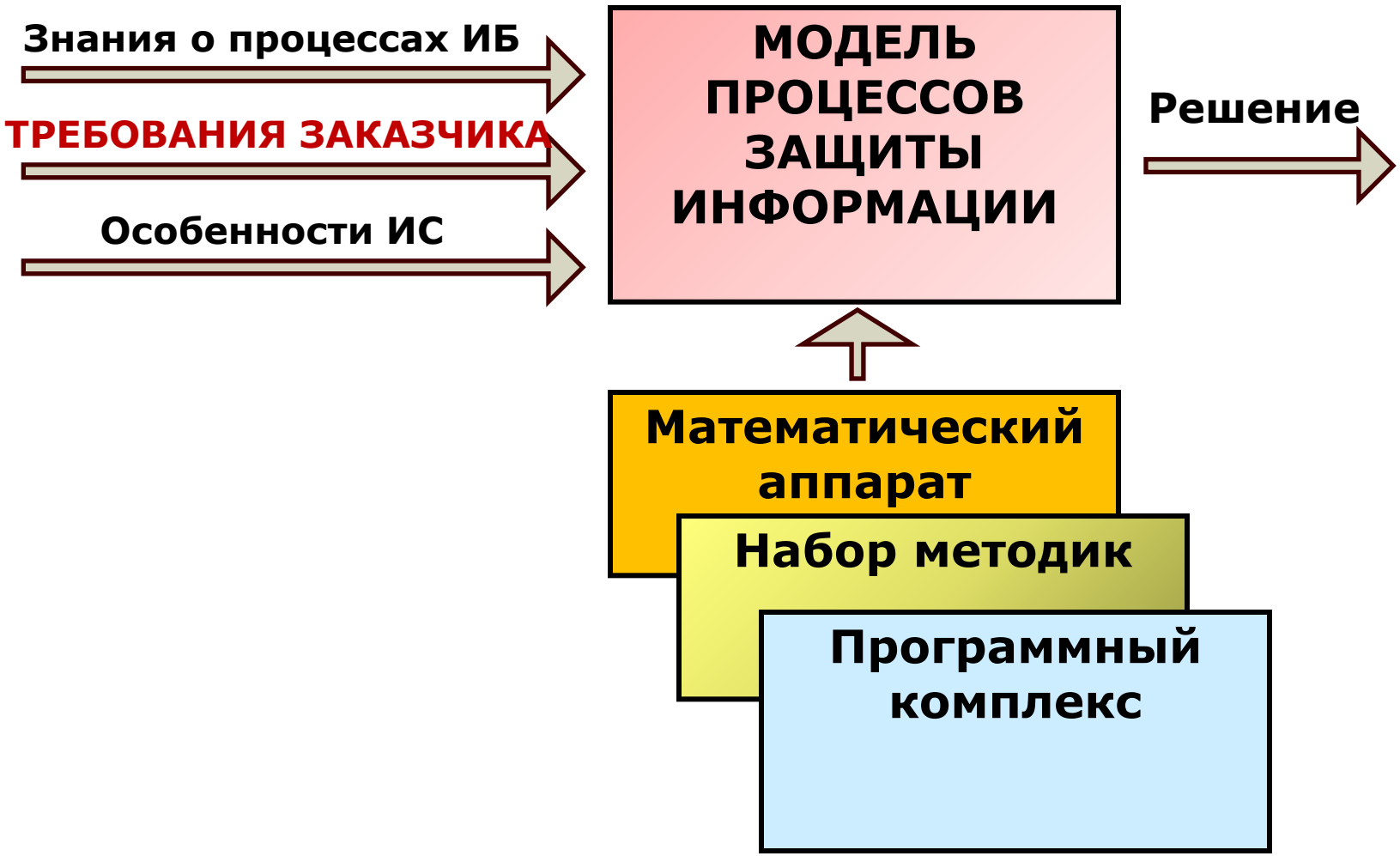
Требования
к межсетевым экранам

Москва, 2016 г.

Выбор сертифицированных средств защиты информации			
Классы			
Класс СЗИ	**ГИС**	**ИСПДн**	**АСУ ТП**
1	Применяются на объектах информатизации, обрабатывающих информацию, содержащую сведения, составляющие государственную тайну		
2			
3			
4	1	1	1
5	2	2	2
6	3	3, 4	3

Типы	
Устанавливается 5 типов межсетевых экранов	
А	Уровня сети
Б	Уровня логических границ сети
В	Уровня узла
Г	Уровня веб-сервера
Д	Уровня промышленной сети (АСУ ТП)

Модель представления системы информационной безопасности



Вопрос 5: «Стандарты по управлению ИБ ISO/IEC 27000»

- **Международная организация по стандартизации, ИСО** *(International Organization for Standardization, ISO)* международная организация, занимающаяся выпуском стандартов.

- **Международная электротехническая комиссия МЭК** *(International Electrotechnical Commission, IEC)* международная организация по стандартизации в области электрических, электронных и смежных технологий.

Стандарты ISO/IEC 27000

- **ISO/IEC 27001** — «Системы управления ИБ. Требования»;
- **ISO/IEC 27002** — «Практические правила управления информационной безопасностью» **Переименованный стандарт ISO/IEC 17799;**
- **ISO/IEC 27003** — «Руководство по внедрению Системы Менеджмента ИБ»;

Стандарты ISO/IEC 27000

- **ISO/IEC 27004** — «Измерение эффективности системы управления ИБ»;
- **ISO/IEC 27005** — «Управление рисками информационной безопасности»;
- **ISO/IEC 27006** — «Требования к органам аудита и сертификации систем управления информационной безопасностью».

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лекция 10:

«ЗАЩИТА ИНФОРМАЦИИ ОТ ТЕХНИЧЕСКИХ РАЗВЕДОК»

Вопросы:

1. Понятие и классификация видов технических разведок.
2. Классификация технических каналов утечки информации.
3. Способы и средства защиты информации от утечки по техническим каналам.

Вопрос № 1: «Понятие и классификация видов технических разведок»

- **Техническая разведка-** вид организации разведывательной деятельности, основанный на применении **ТСР (технических средств разведки)** как организационно самостоятельных систем.
- **Решает самостоятельные задачи по сбору и обработке разведывательной информации.**

Виды технической разведки

- **оптическая** (носитель - ЭМ поле в видимом и инфракрасном диапазонах);
- **радиоэлектронная** (носитель - ЭМ поле в радиодиапазоне или эл. ток);
- **акустическая** (носитель – акуст.волна);
- **химическая** (носитель - частицы вещества);
- **радиационная** (носитель - излучения радиоактивных веществ);
- **магнитометрическая** (носитель – магн. поле).

Компьютерная разведка -

получение информации из баз данных ЭВМ, включенных в компьютерные сети, а также информации об особенностях их построения и функционирования.

OSINT

- **OSINT** (**open-source intelligence**, разведка на основе открытых данных) — **сбор информации о человеке или организации из открытых источников** и ее последующий анализ.
- Технология возникла во время Второй мировой войны в Британии и США: специальные подразделения отслеживали трансляции противника.
- Методы **OSINT** используются во внешней политике, экономике, **в сфере информационной безопасности.**

Противодействие техническим средствам разведки (ПД ТСР)

- Совокупность согласованных мероприятий, предназначенных для исключения или существенного затруднения добывания противником охраняемых сведений с помощью ТСР.
- **входит в общую систему мер по ЗГТ и КИ.**

Вопрос № 2: «Классификация технических каналов утечки информации»

- **Утечка информации** - неправомерный выход конфиденциальных сведений за пределы организации или круга лиц, которым эти сведения были доверены.
- **Одна из основных обязанностей администратора информационной безопасности (АИБ) – выявление и блокирование каналов утечки информации!**

Классификация каналов утечки информации

Социальный канал утечки информации

Собственные сотрудники организации
• вербовка;
• злой умысел;
• неумышленные ошибочные действия;
• другие.

Технический канал утечки информации

Акустика
Виброакустика
Электромагнитные поля (ПЭМИН)
Компьютерные сети (Сети Интернет, локальные сети и др.)

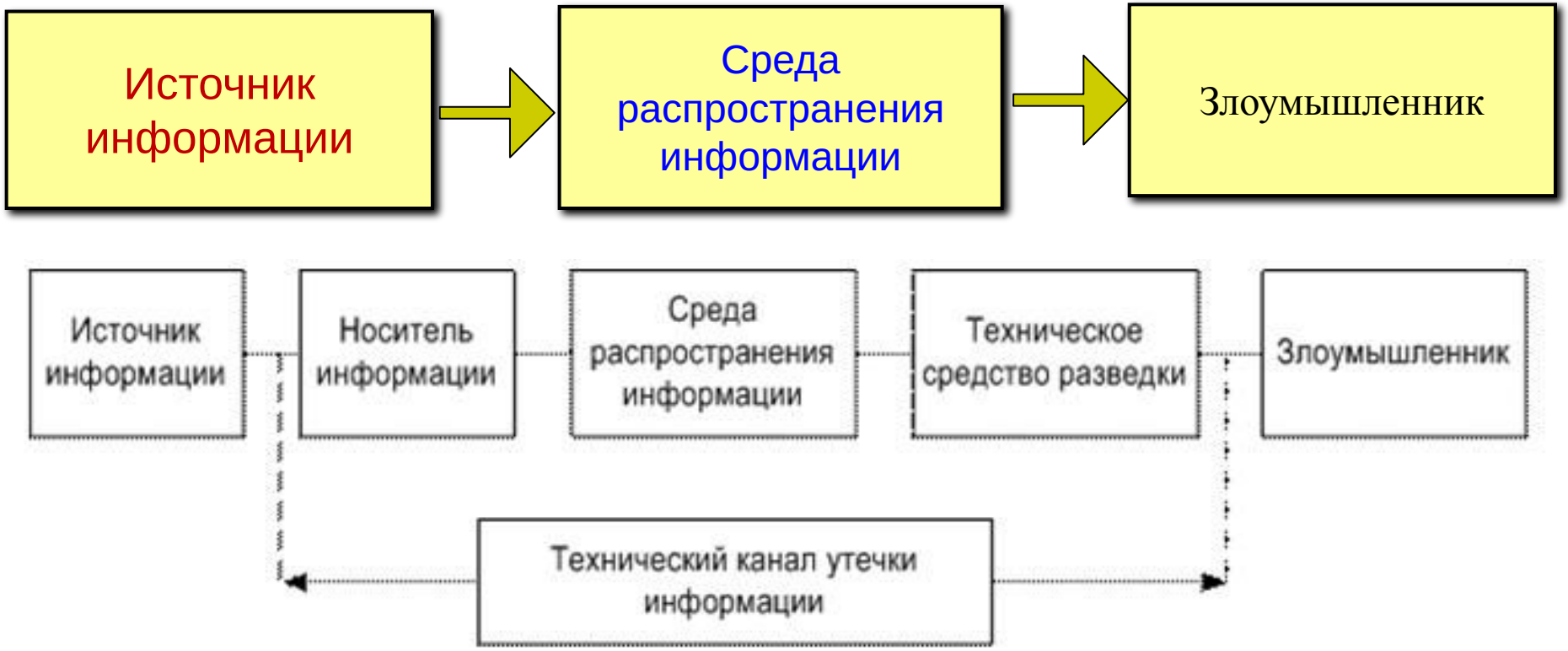
Материально-вещественный канал утечки информации

Печатные документы
Электронные носители
Аппаратура (элементы аппаратуры)
«мусор»

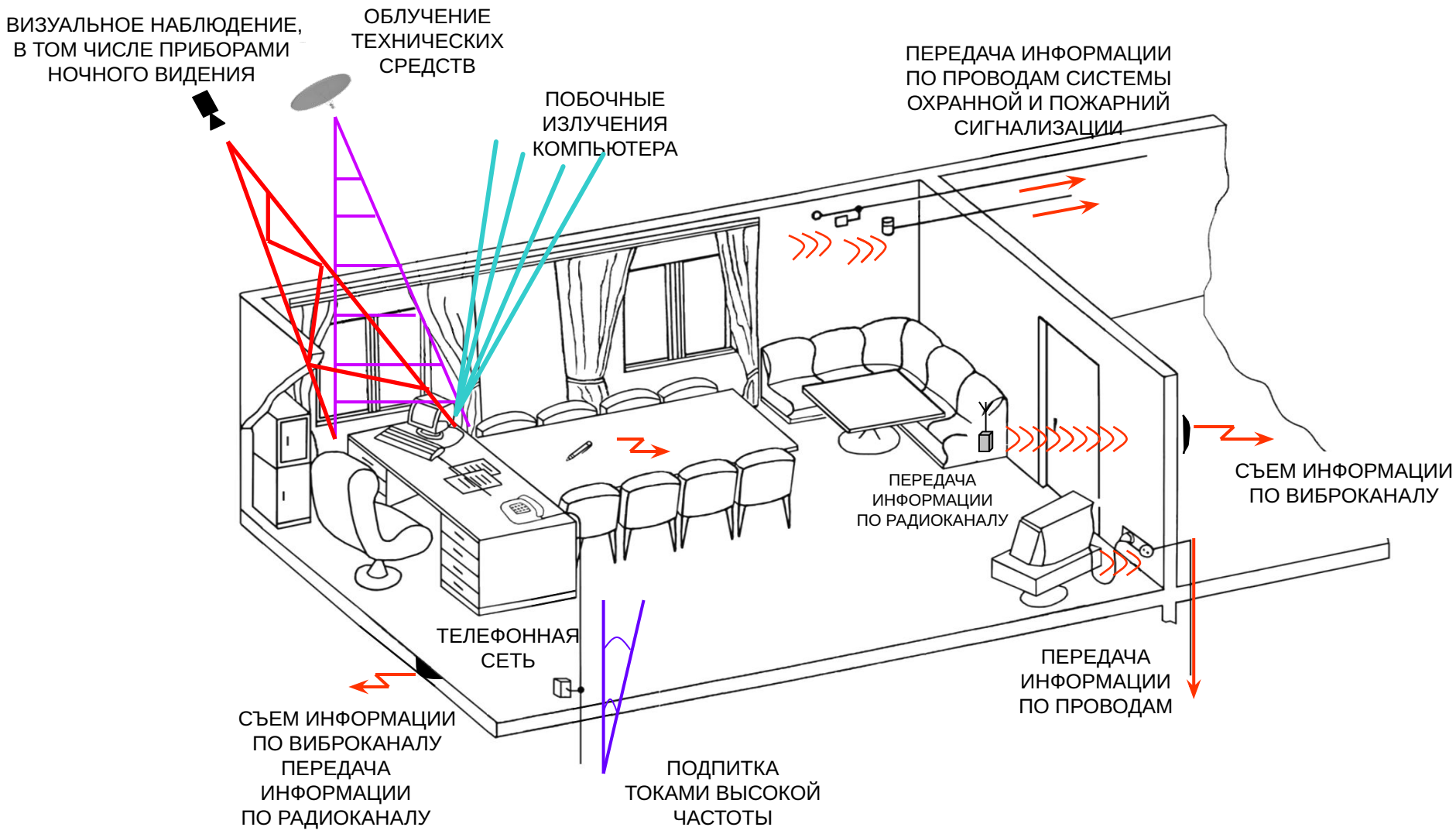
Технический канал утечки информации (ТКУИ)-

- **физический путь от источника информации к злоумышленнику, посредством которого может быть осуществлен несанкционированный доступ к охраняемым сведениям.**

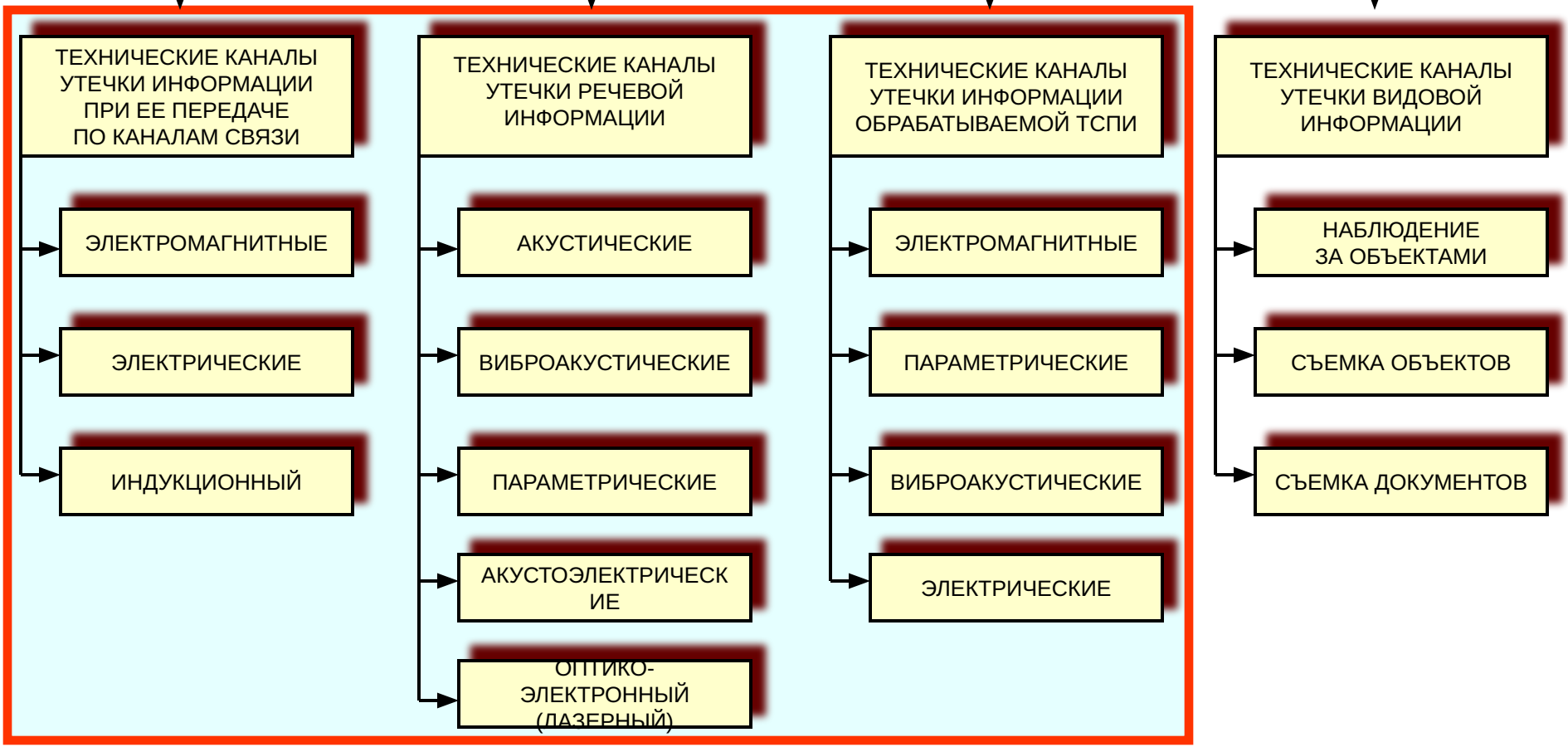
Структура канала утечки информации



ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ



ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ



КЛАССИФИКАЦИЯ ЗАКЛАДНЫХ УСТРОЙСТВ ПЕРЕХВАТА АКУСТИЧЕСКОЙ (РЕЧЕВОЙ) ИНФОРМАЦИИ (АКУСТИЧЕСКИХ ЗАКЛАДОК)

Вопрос № 3: «Средства и способы защиты информации от утечки по техническим каналам»

- **Защита информации от утечки** - защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на **исключение (затруднение) получения защищаемой информации [иностранными] разведками и другими заинтересованными субъектами.**

Индикаторы электромагнитного поля и частотомеры

D-008

PIF-2

PT-022

ST-051

ИЭП

Сканер-3

Protect-1203

Сириус

АПП-7

РИЧ-3

ИПФ-6

CD-100

CUB

SCOUT

M1

Micro RF Detector

Многофункциональная аппаратура

SEL SP-37 ТРАЛ

ПКУ-6М

D-008

ST-032

ПСЧ-5

OSCOR OSC-5000

CPM-700

ST-031P

Программно-аппаратные комплексы

АРК-Д1Т

RS1000

КРОНА-8000

ПАТРУЛЬ

MS-8108 и MS-8108SR

ДЕЛЬТА

КВАДРАТ-М

ПАК предназначенные для проведения аттестации выделенных (защищаемых) помещений

VNK-012GL

ШЕПОТ

СПРУТ-5

ШОРОХ - ТЕСТ

Гриф-АЭ-1001

Системы, комплексы и приборы защиты информации от утечки по акустическим и виброакустическим каналам

ANG-2000

SI-3001

VAG-6/6

БАРОН DIGITAL

СОНАТА-АВ 1М

СКИТ-М-ВА

Вибрационные преобразователи

МОЛОТ
вибрационный излучатель на стену

СЕРП
вибрационный излучатель на раму окна

КОПЕЙКА
вибрационный излучатель на стекло

ВИ-45

FOX VA-07A

КВП-6

КВП-2

КВП-7

SEL
SP-51/AV

Акустические излучатели

SOUND PRESS

SI-310 0

СОНАТА-АВ 1М

СОНАТА-АВ квадро

Генераторы электромагнитных сигналов

ГШ-К-1000

Гном-3М

Гром-ЗИ-4

ЛГШ-501

SEL SP-21B1 Баррикада

Скит-М-П

Бриз

Постановщики помех закладным устройствам передающим снятую информацию по радиоканалу

SEL SP-21B2 СПЕКТР

Равнина-5И

Пелена-6У

ПРП-М

Гром-ЗИ-4

Устройство блокирования работы систем мобильной связи

DLW 4003
DLW 4012

Скат

Москит GSM 3

Мозаика

Сапфир

DLW 2000

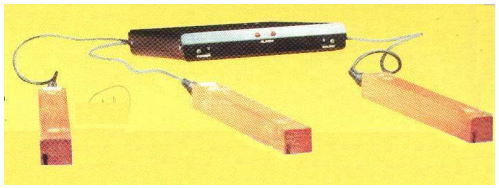
Гамма

C-CUARD-300YK

Обнаружители диктофонов

PTRD-018

ST-041



RM - 200

ST-0110

TRD-800

PTRD-014

RM - 100

Подавители диктофонов

Буран-3М

Рамзес-Дубль

Шторм

Шумотрон-2

Шумотрон

Шумотрон-5

Мангуст

Устройства защиты телефонных переговоров

Атолл-3

Гранит-VIII

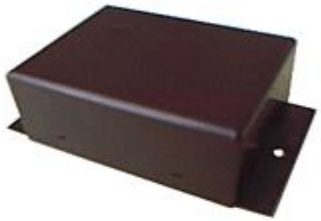
Корунд-М

МП-1Ц

Antifly

SEC-2000 Ultra

SEC-2004 Antifly



Грань-300

Вьюга-4

Устройства защиты телефонных переговоров

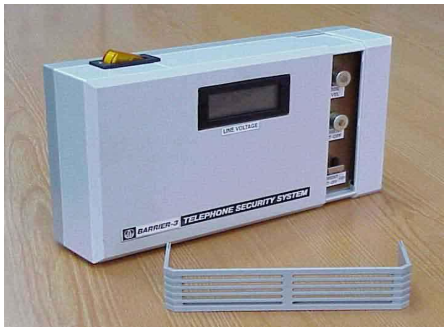
SEL SP-17/T

SI-2001

Акцент

КТЛ-400

SI-2001



Барьер-3

Соната-03М

Многофункциональные устройства защиты

Гром-ЗИ-4

Прокруст-2000

Прокруст ПТЗ-003

TSU-3000

Гром-ЗИ-6

Фаворит

Цикада-М1

Изделия уничтожения устройств несанкционированного снятия информации путем их электрического уничтожения (выжигания)

ГИ-1500

Кобра

BUGROASTER

Помехоподавляющие фильтры

Фильтры серии ФСП

ФСПК

Импульс

Фаза

ЛФС

Активные устройства защиты информации от утечки по цепям питания и системам заземления

SEL SP-41/C

БАРЬЕР-4

СКИТ-М-С

ИМПУЛЬС

МП-3

СОНАТА-С1

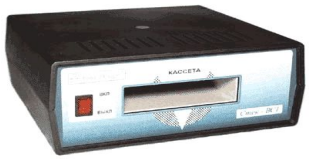
SEL SP-41/D

SI-8001

СОПЕРНИК

ЦИКАДА-М1

Средства экстренного уничтожения информации



Стек-ВС

DISK DESTROYER

ЦУНАМИ АТХ-1

Миг-20DLT-IV

Стек-НСА 2.х

Стек-Н

ТЕНЬ К1

Стек-НС1

Стек-КДС

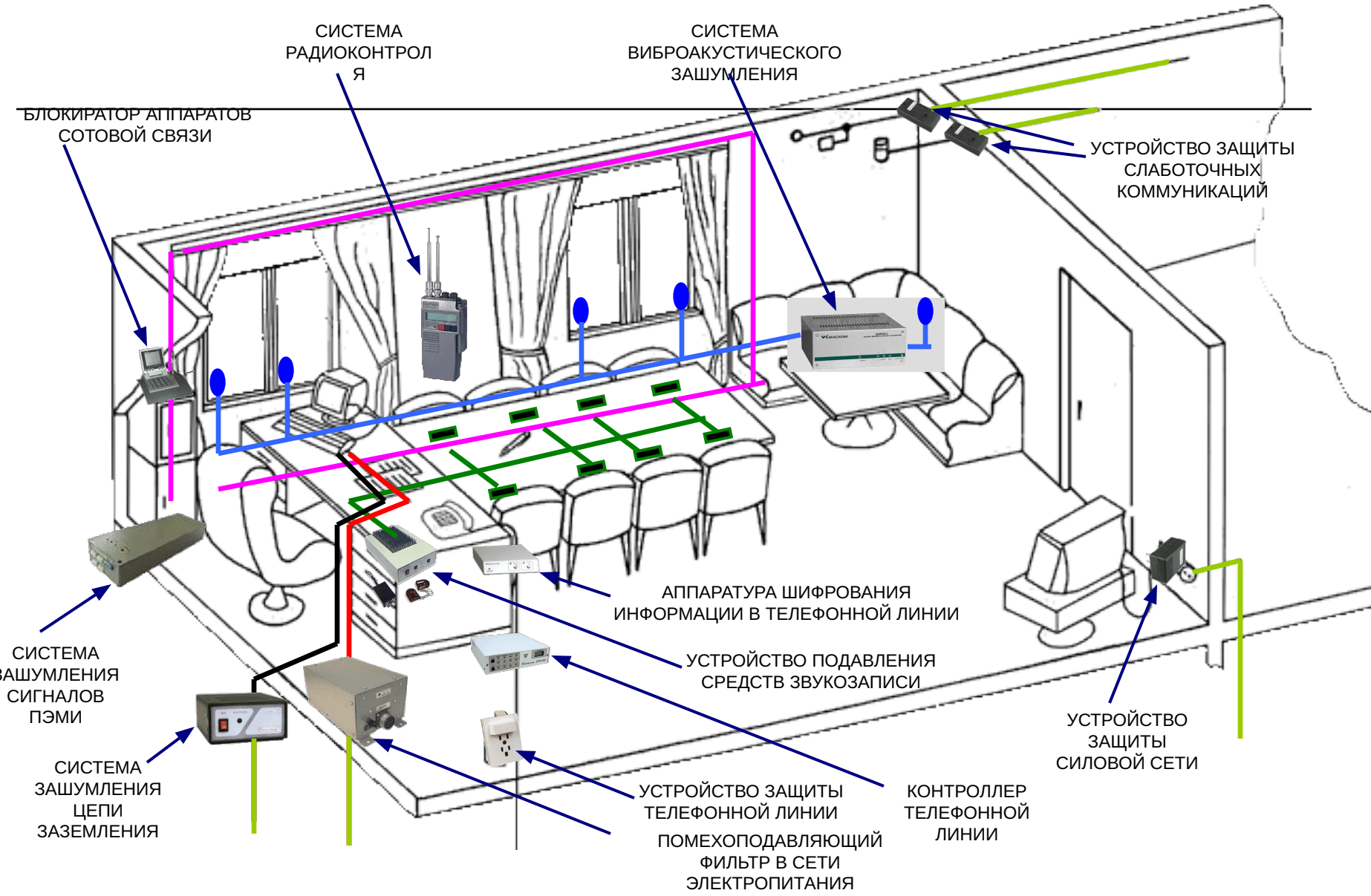
Стек-ВС1

Стек-КДС1

Стек-КДСА2

Стек-НС1в

СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТКУИ



Устройство защиты телефонных переговоров

Телефон-скремблер

Антенна системы радиоконтроля и мониторинга скрытая за фальш-потолком

Акустический микрофон и микровидеокамера скрытый в корпусе охранного датчика

Генератор шума по сетям электро-питания и заземления

Виброакустический излучатель системы защиты информации на системе отопления и стене

Генератор электромагнитного шума

Акустический излучатель системы защиты информации в тамбуре (междверном пространстве)

Акустический излучатель системы защиты информации в вентиляционном канале

Виброакустический излучатель системы защиты информации на стеклах (рамах)

Генератор системы виброакустической защиты

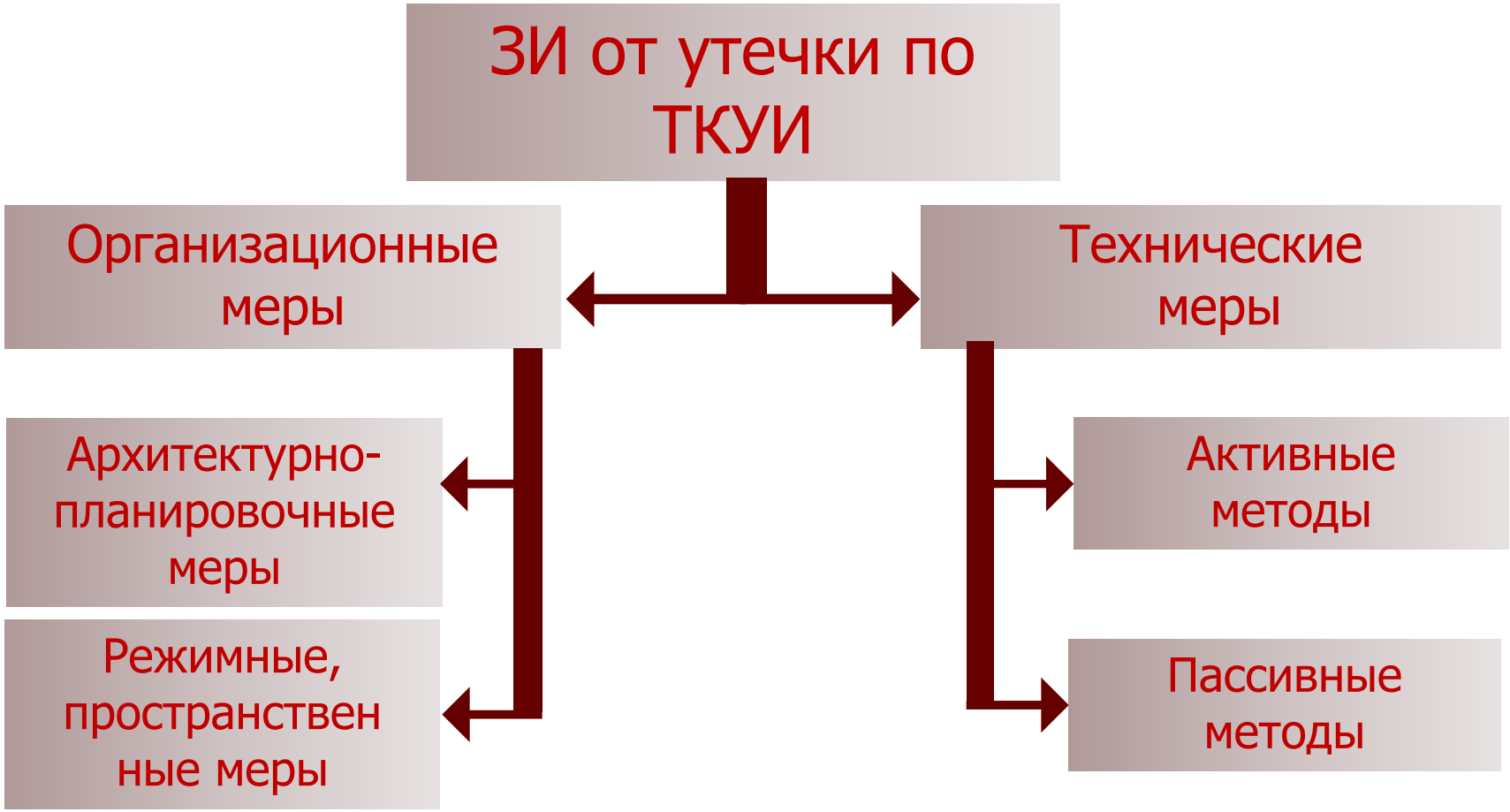
Система защиты информации от несанкционированного доступа

Система гарантированного уничтожения информации на жестком диске ПЭВМ

Устройство подавления сотовой связи и индикатор поля камуфлированные в часах

Акустический сейф для мобильных телефонов

Способы защиты информации



Организационные меры

1. Определение границ контролируемой зоны (КЗ).
2. Категорирование и аттестация объектов информатизации (ОИ) по выполнению требований обеспечения ЗИ.
3. Использование на объекте сертифицированных основных технических средств и систем (ОТСС) и вспомогательных технических средств и систем (ВТСС).

4. Организация контроля и ограничение доступа к ИС и в защищаемые помещения (ЗП).

5. Ведение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите.

6. Отключение на период закрытых мероприятий технических средств, имеющих элементы, выполняющие роль электроакустических преобразователей, от линий связи.

Технические меры
(активные методы)

1. Пространственное зашумление:
   - Электромагнитное зашумление с использованием ГШ;
   - Фильтрация опасных сигналов.
2. Линейное зашумление:
   - линий электропитания;
   - посторонних проводников и соединительных линий ВТСС, имеющих выход за пределы КЗ.
3. Уничтожение закладных устройств.

Зашумление

Пространственное зашумление

Для исключения перехвата ПЭМИН по электромагнитному каналу

Генератор шума Соната-РС2

Линейное зашумление

Для исключения съема наводок ИС с посторонних проводников и соединительных линий ВТСС

Генератор шума Гном-3

Технические меры
(пассивные методы)

1. Контроль и ограничение доступа к ИС и в ЗП с помощью технических средств и систем.
2. Локализация излучений:
   - Экранирование ОТСС и их соединительных линий;
   - Заземление ОТСС и экранов их соединительных линий.

Технические меры
(пассивные методы)

3. Развязывание информационных сигналов:
   1. Установка специальных средств защиты в ВТСС, обладающих "микрофонным эффектом" и имеющих выход за пределы КЗ.
   2. Установка автономных источников электропитания ОТСС.
   3. Установка устройств гарантированного питания ОТСС.
   4. Установка в цепях электропитания ОТСС помехоподавляющих фильтров.

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лекция 11:

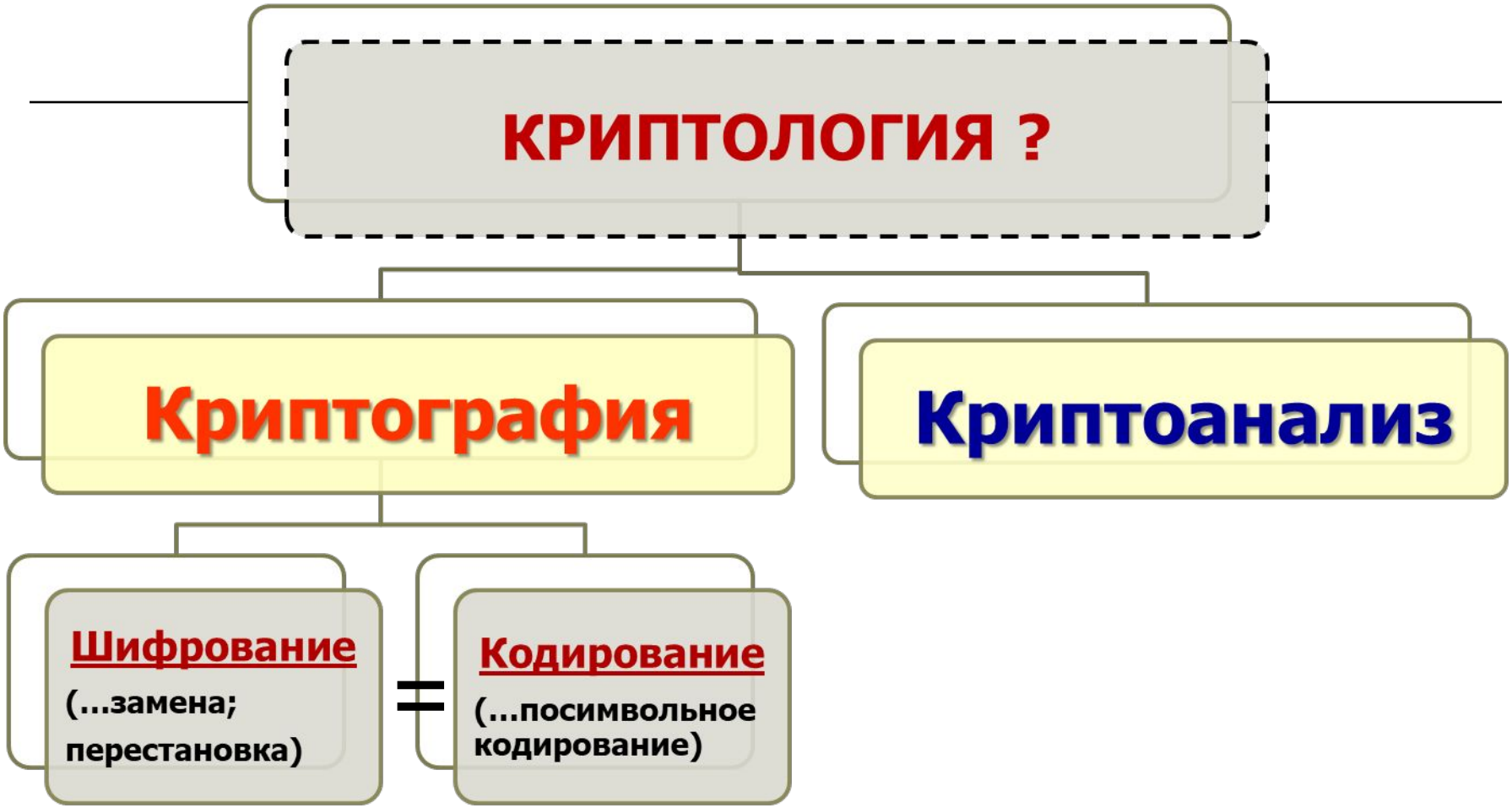
«Защита информации криптографическими методами»

Вопросы:

1. Основы криптографической защиты информации.
2. Управление криптографическими ключами.
3. Криптографические средства защиты информации.

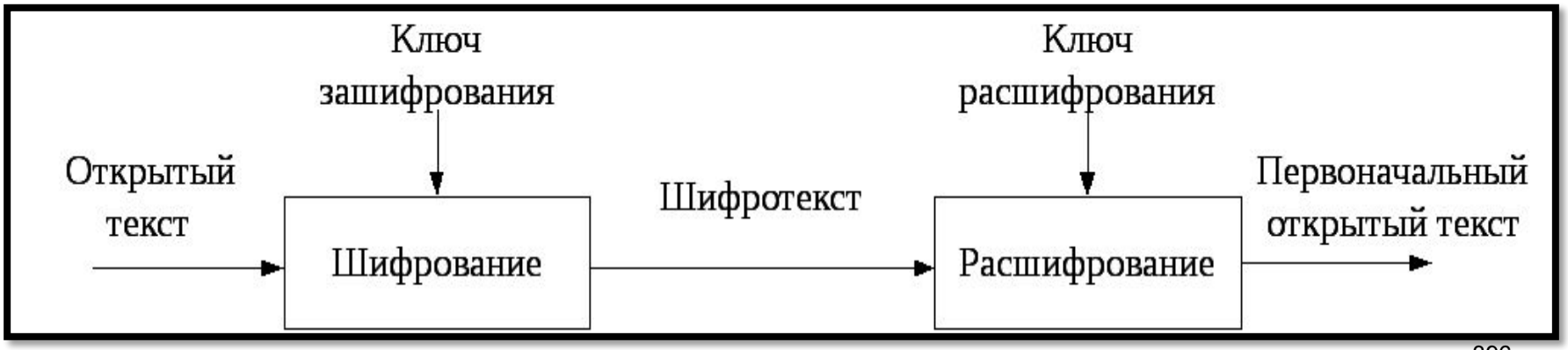
Вопрос 1: «Основы криптографической защиты информации»

- **Криптография** (*от др.-греч. κρυπτός — скрытый и γράφω — пишу*) — наука о методах обеспечения **конфиденциальности** и **аутентичности** (це лостности и подлинности авторства/невозможности отказа от авторства) информации.
- **Криптографическая защита информации – это защита информации с помощью ее криптографического преобразования.**


КРИПТОЛОГИЯ ?
Криптография
Криптоанализ
Шифрование
(…замена; перестановка)
=
Кодирование
(…посимвольное кодирование)

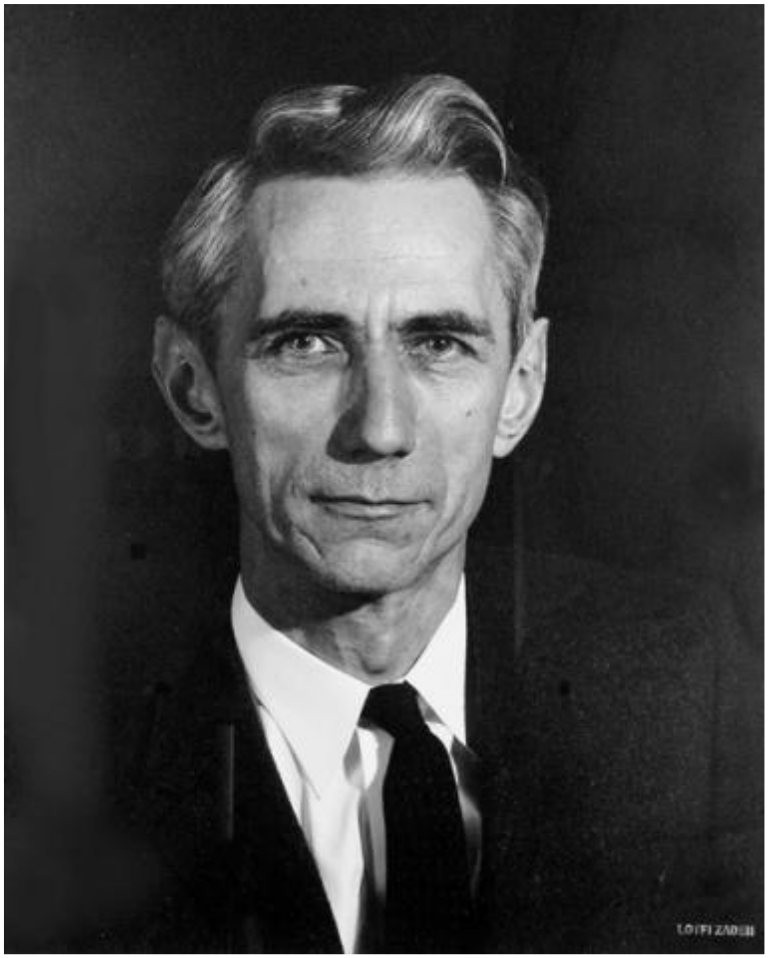
Основные понятия криптографии

- **Шифрование** – процедура преобразования открытого текста под воздействием **ключа**.
- **Расшифровывание** - процедура обратного преобразования шифротекста.



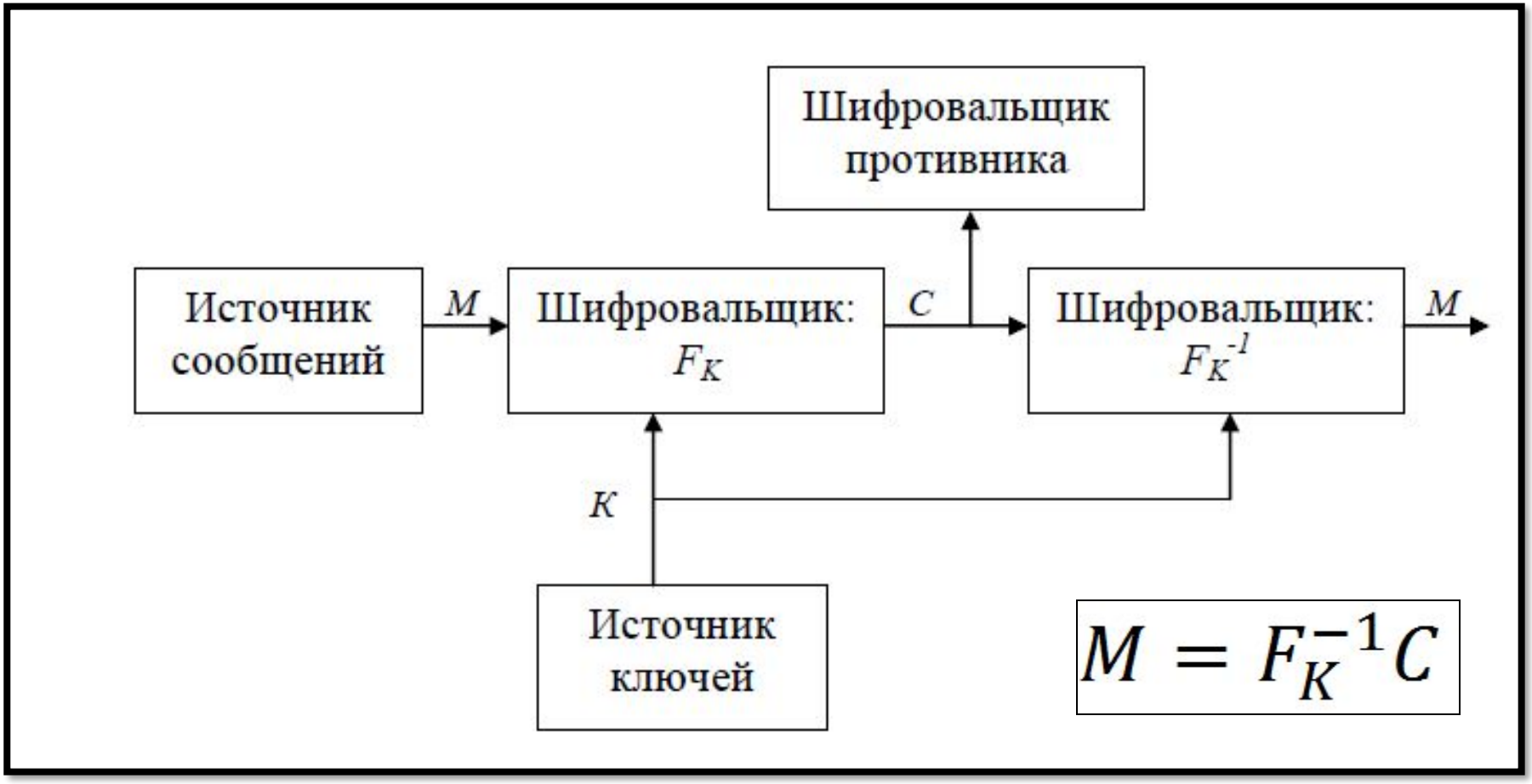
50- 70-е года XX века — переход к математической криптографии.

В работах Шеннона: математические определения *количества информации, передачи данных, энтропии, функций шифрования*.



Клод Шеннон

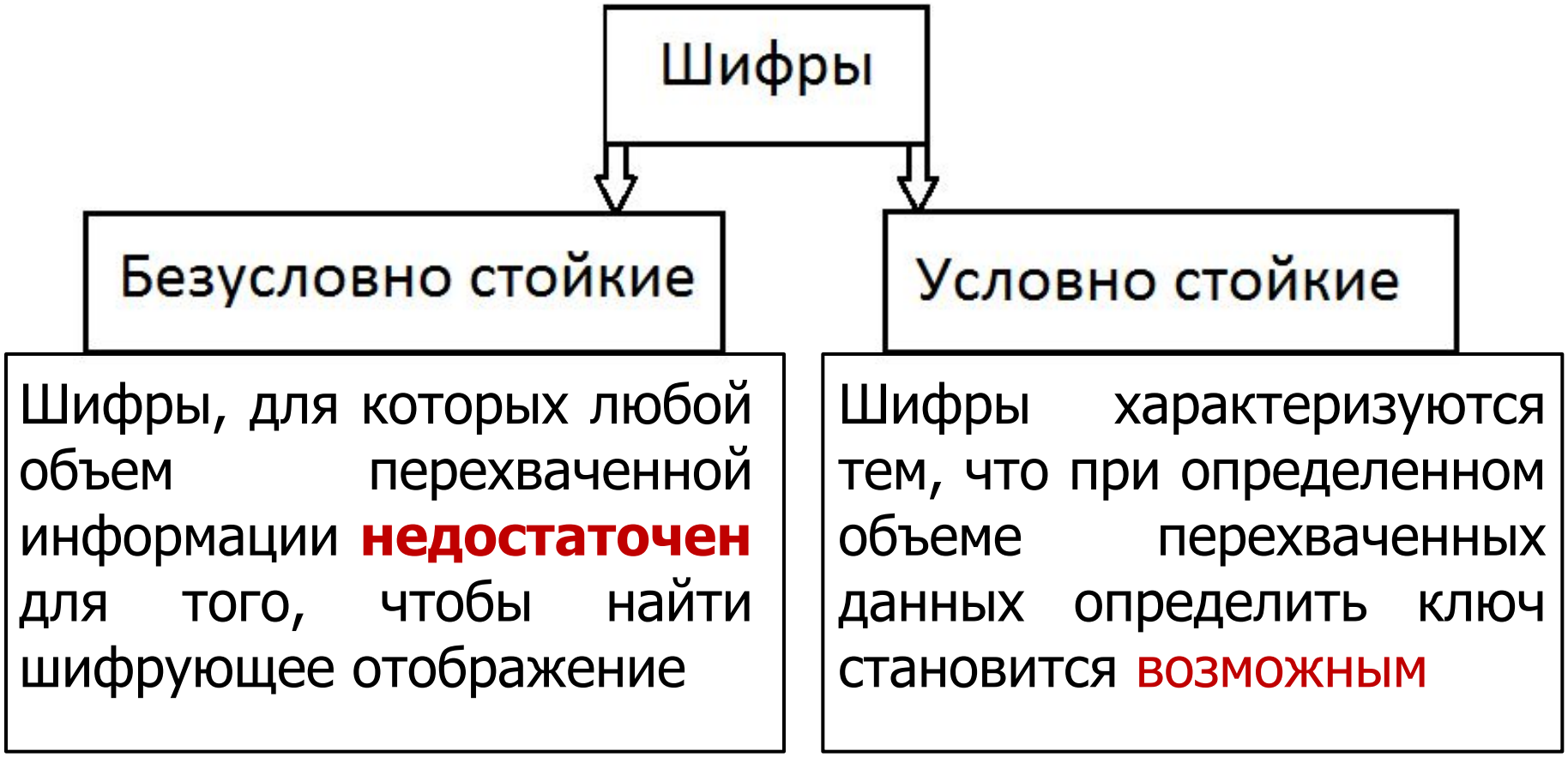
Схема секретной системы Шеннона («Теория связи в секретных системах» 1949 г.)



Основные понятия

- **Секретная система (шифр)** - **система** обратимых преобразований, зависящая от **секретного** параметра (ключа) и предназначенная для обеспечения секретности передаваемой информации.

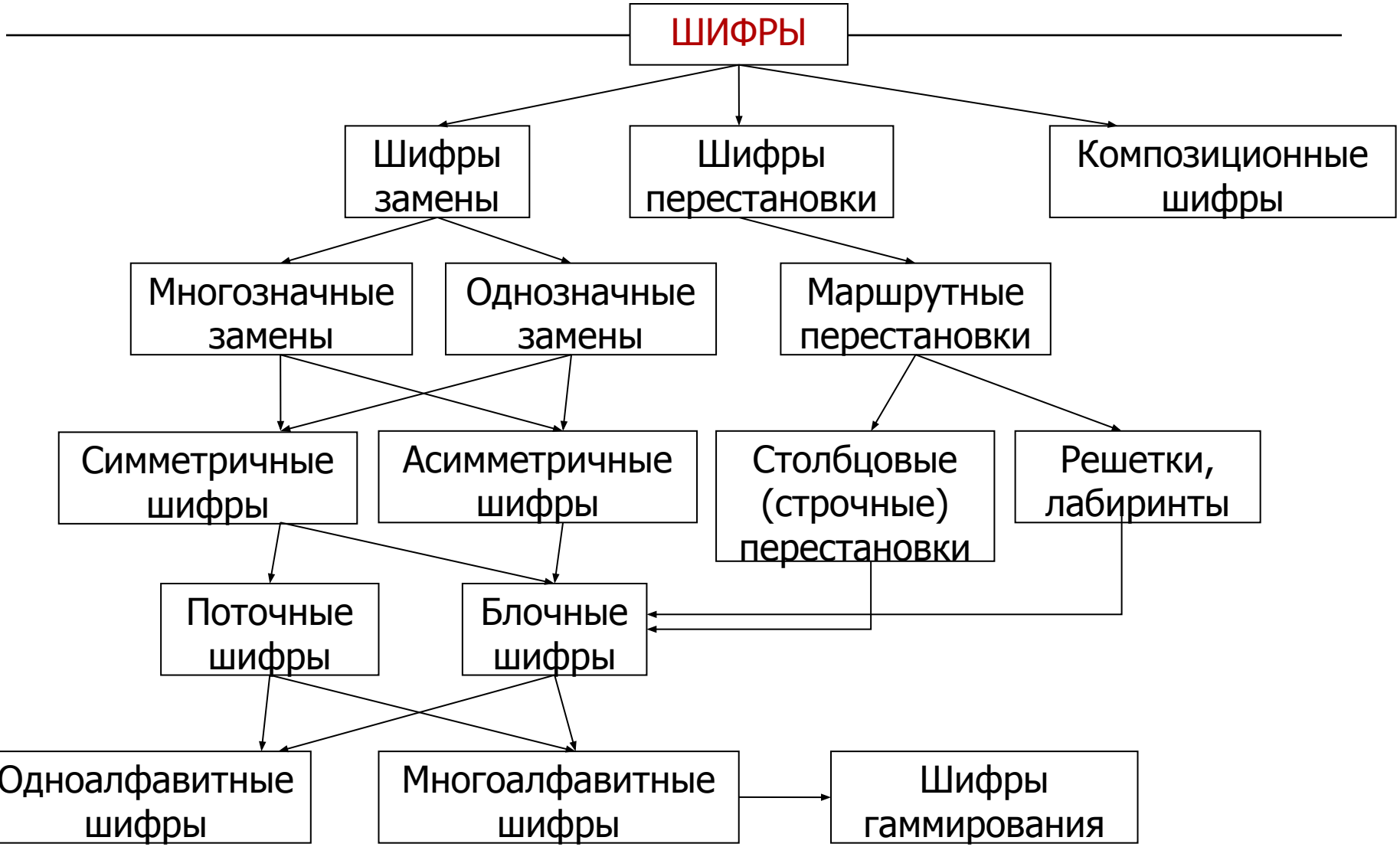
Типы шифров


Шифры
Безусловно стойкие
Условно стойкие
Шифры, для которых любой объем перехваченной информации **недостаточен** для того, чтобы найти шифрующее отображение
Шифры характеризуются тем, что при определенном объеме перехваченных данных определить ключ становится возможным

Свойства шифров

- **Криптостойкость** – стойкость шифра к **раскрытию** методами криптоанализа;
- **Временная сложность** – время, затрачиваемое алгоритмом **для решения задачи;**
- **Емкостная сложность** – объем памяти, необходимой **для хранения** полученных в ходе работы данных.

Классификация шифров



Шифры гаммирования

- **Шифрование гаммированием** предполагает, что символы шифруемого текста складываются с символами некоторой случайной последовательности, называемой **гаммой шифра** или **ключевой гаммой**.

Шифры на основе аналитических преобразований

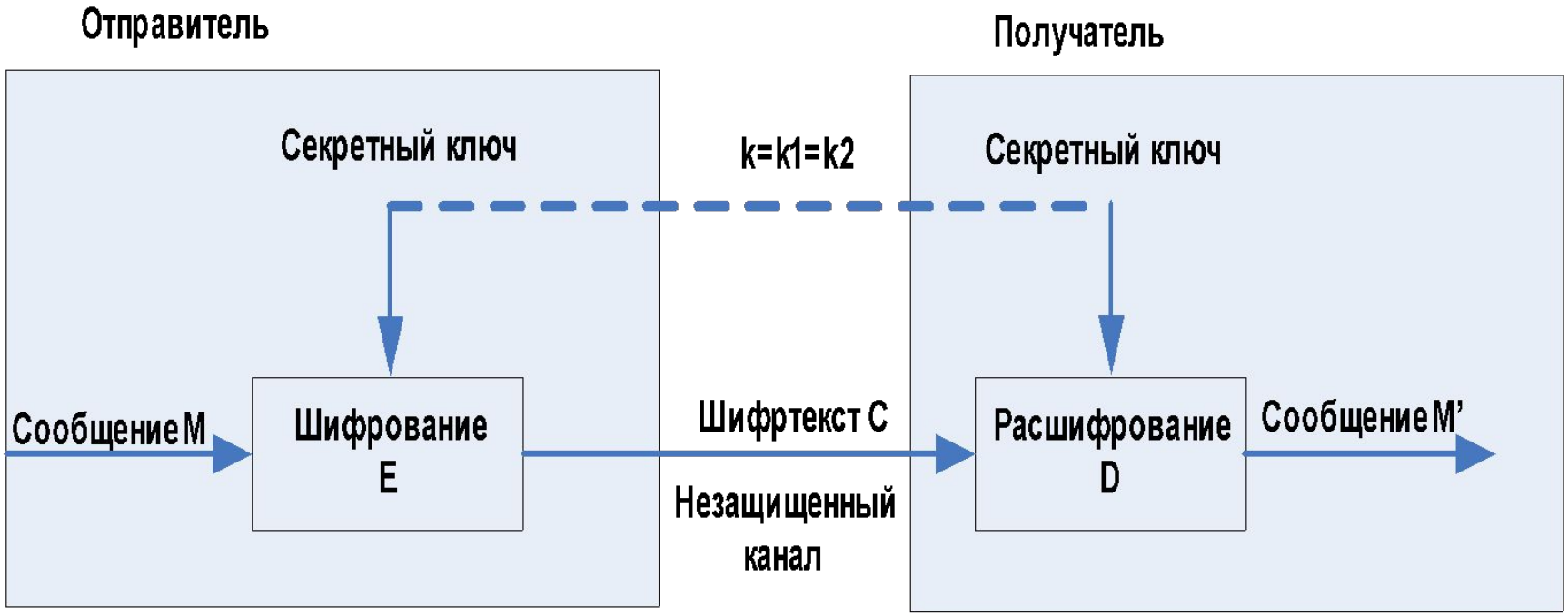
- Шифрование **аналитическими преобразованиями** подразумевает использование аналитического правила, по которому преобразуется текст. Например, методы алгебры матриц.

$$\overline{C} = A \times \overline{B} = \begin{vmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{vmatrix} \times \begin{vmatrix} 2 \\ 0 \\ 19 \end{vmatrix} = \begin{vmatrix} 85 \\ 54 \\ 25 \end{vmatrix},$$

По типу **использования ключей** шифры делятся на:

- **Симметричные,** использующие для шифрования и расшифровывания информации один и тот же ключ;
- **Асимметричные,** использующие для шифрования и расшифровывания два различных ключа.

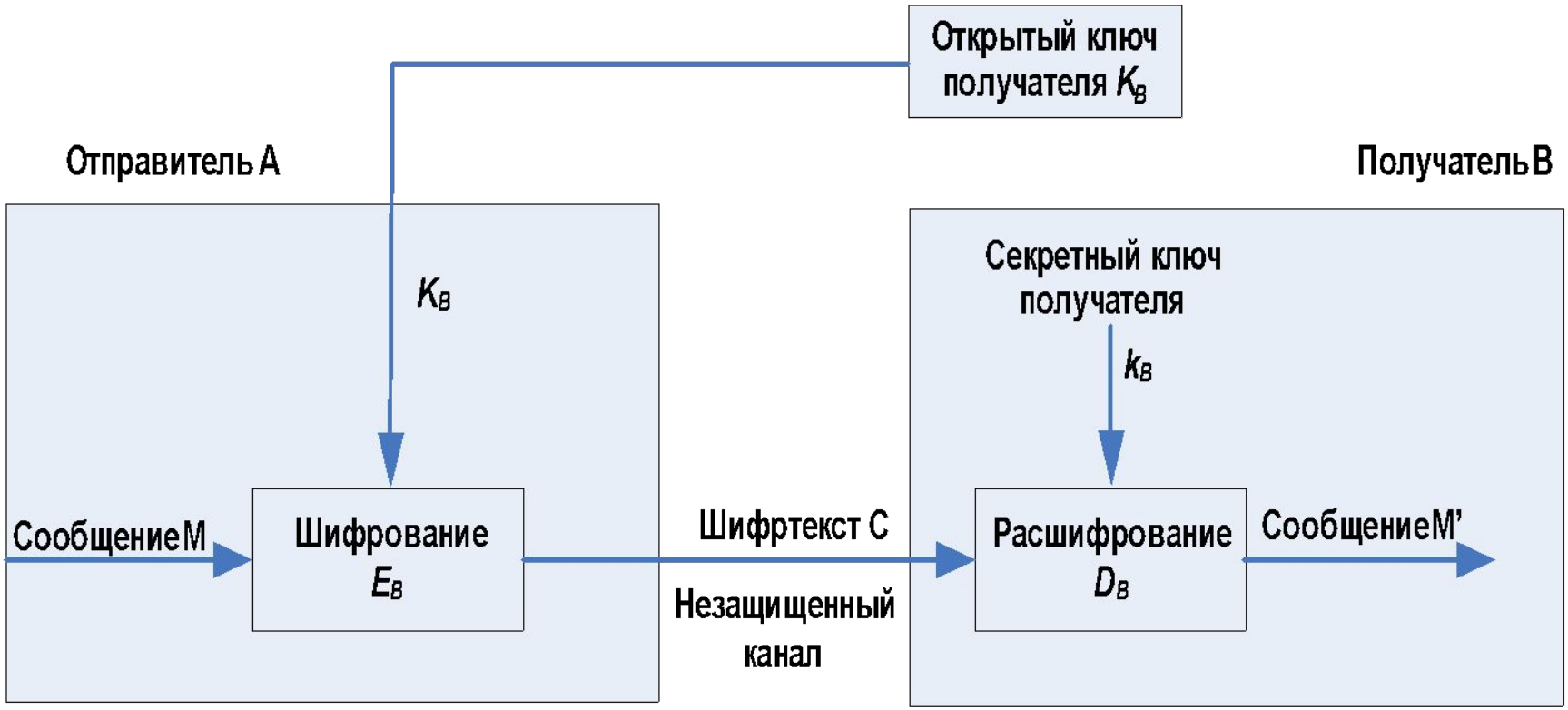
Принцип симметричного шифрования



Примеры симметричных алгоритмов

Алгоритм	Описание
DES	Digital Encryption Standard (стандарт симметричного шифрования), блочный шифр
3DES	тройной DES, более сильная альтернатива DES
Rijndael	блочный шифр, пришел на смену DES
RC2	шифр изобретенный Рональдом Ривестом, блочный шифр

Принцип асимметричного шифрования
(пример, алгоритм шифрования RSA)



Алгоритм шифрования RSA

- в 1978 г. предложили 3 автора:
  - *Ron **R**ivest, Adi **S**hamir, leonard **A**dleman*
- **Режимы работы RSA:**
  - шифрование данных
  - электронная цифровая подпись
- **Надежность RSA**
  - факторизация больших чисел
  - вычисление дискретных логарифмов в конечном поле.

- 3) По **размеру преобразуемого блока** шифры делятся на:

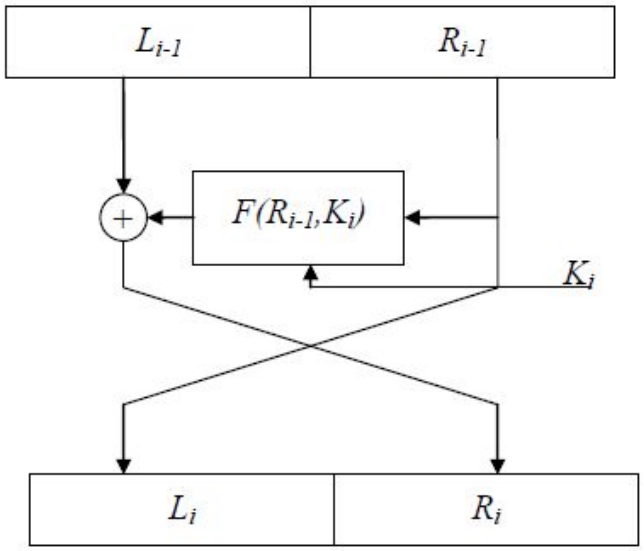
- **Блочные** осуществляют преобразование информации блоками фиксированной длины;
- **Потоковые** шифры предназначены для преобразования сообщения поэлементно.

Схема Фе́йстеля

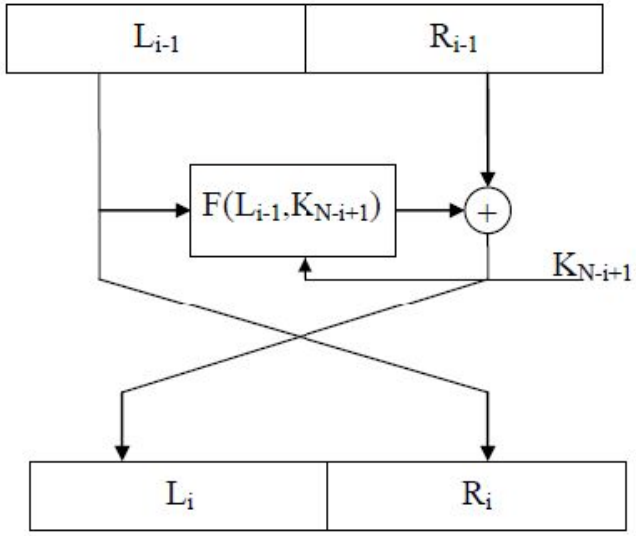
- **Раунд шифрования**- многократные повторения некоторого набора операций преобразования.
- **Раундовый ключ –** часть ключа, используемая в каждом раунде.
- **Расписание использования ключа шифрования**- порядок генерации и использования раундовых ключей.

Преобразование по схеме Фейстеля (используют большинство блочных шифров)

- При шифровании, в первом раунде будет использоваться **первый** раундовый ключ, а в первом раунде при расшифровывании – **последний**.



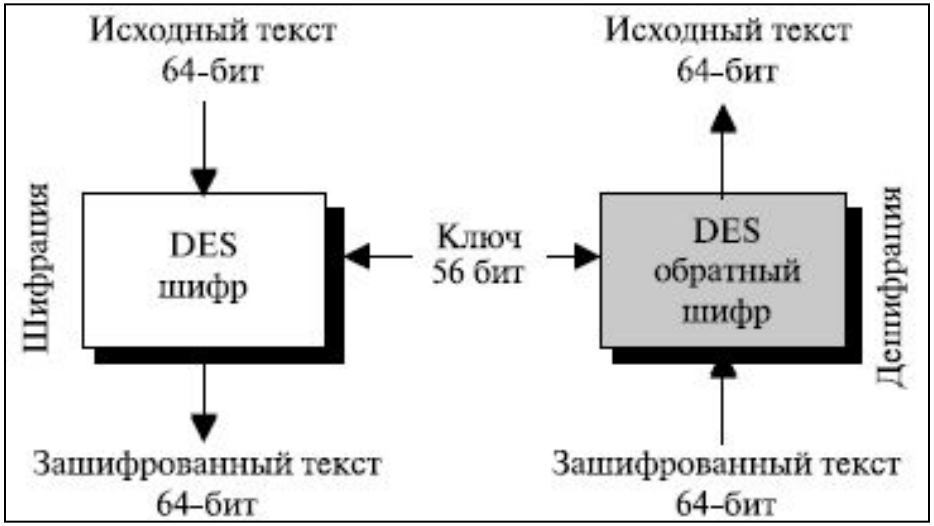
Прямое преобразование по схеме Фейстеля



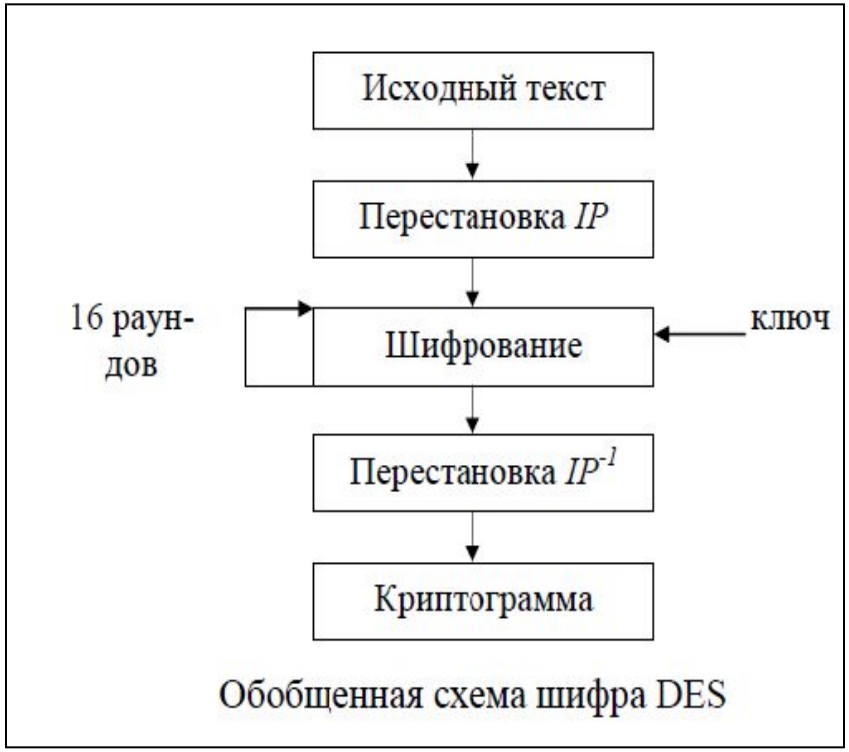
Обратное преобразование по схеме Фейстеля

Шифр DES

- Шифр DES является **блочным** – преобразования в нем проводятся блоками по 64 бита.
- Ключ 64-битный, но значащими являются только 56 бит.



Схемы шифра DES



Обобщенная схема шифра DES

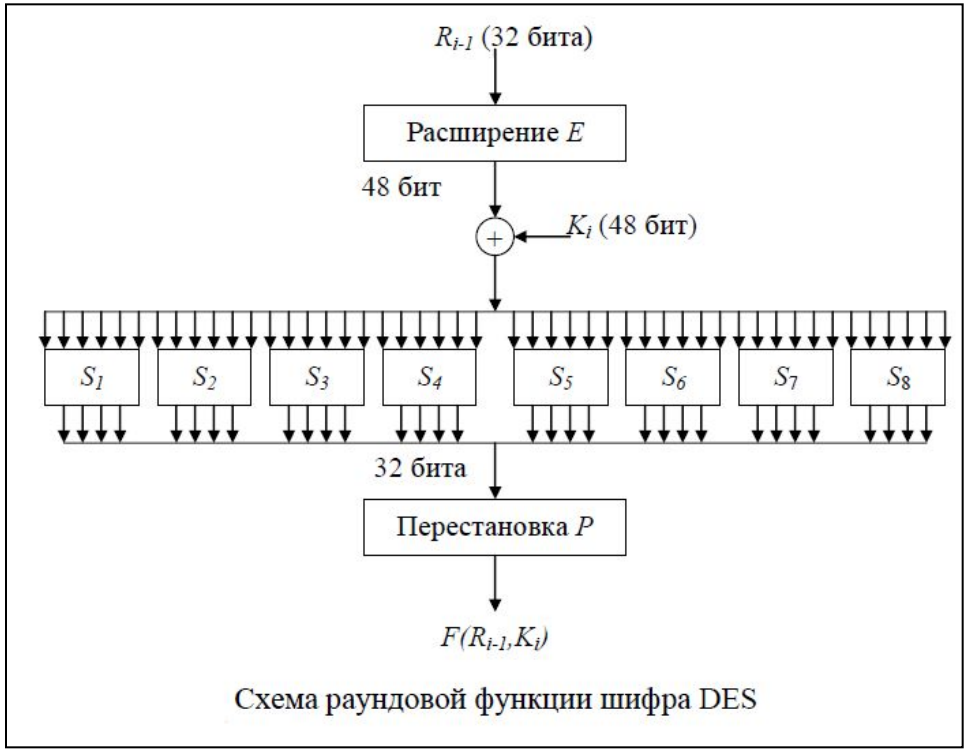


Схема раундовой функции шифра DES

Шифр ГОСТ 28147-89

- Достаточно **стойкий** и **широко используемым** предприятиями, которым необходимо применять сертифицированные КСЗИ.
- Преобразует сообщение 64-битными блоками, преобразование осуществляется в соответствии **со схемой Фейстеля** в 32 раунда, размер ключа – 256 бит.

Алгоритм шифра

Алгоритм предусматривает **4 режима работы**:

- Шифрование данных в режиме простой замены;
- Шифрование данных в режиме гаммирования;
- Шифрование данных в режиме гаммирования с обратной связью;
- Выработка имитовставки.

Гамми́рование, или Шифр XOR, — метод симметричного шифрования, заключающийся в «наложении» последовательности, состоящей из случайных чисел, на открытый текст.

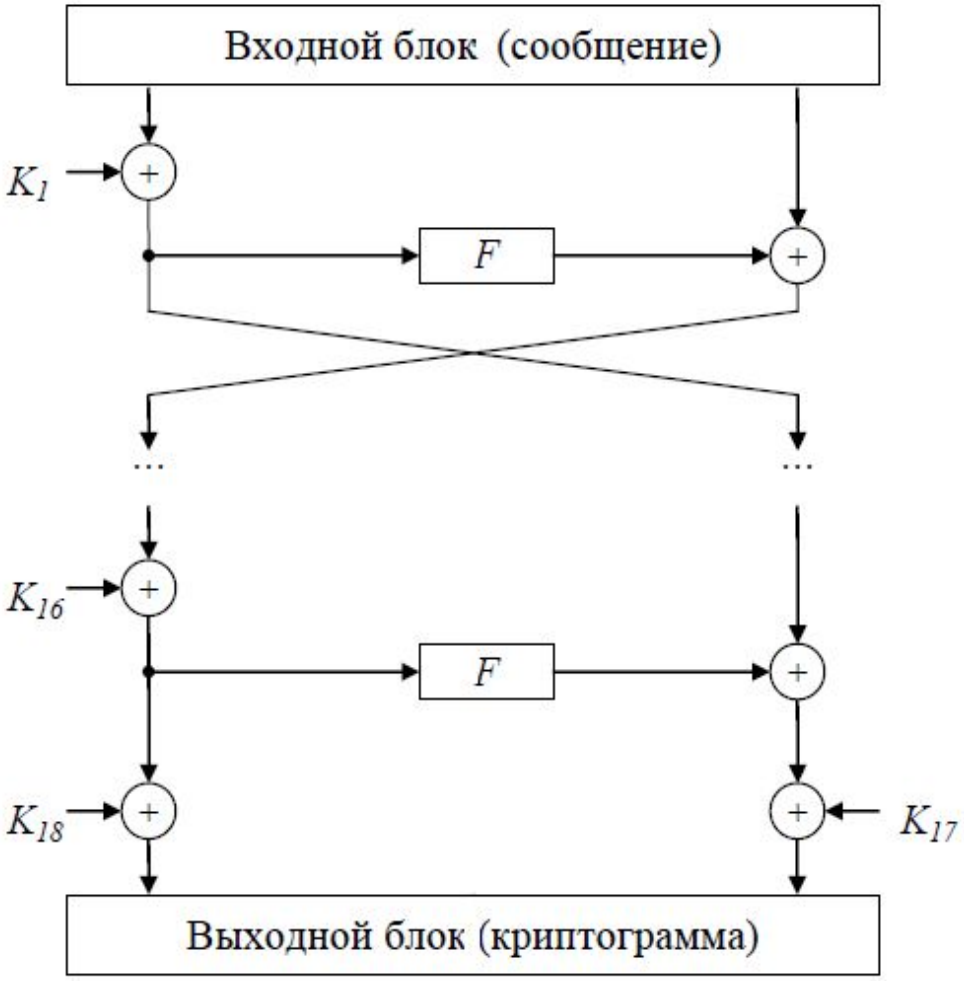
ГОСТ 34.12-2018

- Один из двух описанных в этом стандарте шифров:
- «**Кузнечик**» — блочный шифр с размером блока 128 бит
- «**Магма**» — блочный шифр с размером блока 64 бита

Шифр Blowfish

- Алгоритм ориентирован на программную реализацию на 32-разрядных микропроцессорах.
- Его отличают **высокая скорость**, **криптостойкость** и **возможность использовать ключ переменной длины**.

Схема шифра


Входной блок (сообщение)
K_1
F
...
K_{16}
F
K_{18}
K_{17}
Выходной блок (криптограмма)

Вопрос 2: «Управление криптографическими ключами»

- Под **ключевой информацией** понимают совокупность всех ключей, действующих в системе.
- Процесс управления ключами включает в себя реализацию **трех основных функций**:

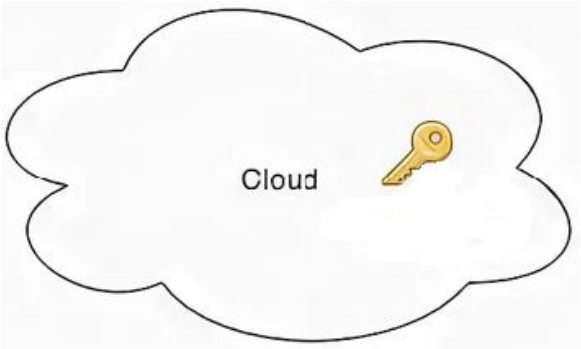
1. **Генерация ключей.**
2. **Хранение ключей.**
3. **Распределение ключей.**

Генерация ключей

- Должна производиться таким образом, чтобы предугадать значение ключа было **невозможно**.
- Для генерации используются аппаратные и программные **средства генерации случайных чисел.**
- Возможна **модификация ключа.**

Хранение ключей

- необходимо обеспечить такие условия работы, чтобы секретные ключи никогда не были записаны в явном виде на носителе, к которому **может получить доступ** нарушитель.
- Возможна **иерархия ключей.**



Распределение ключей

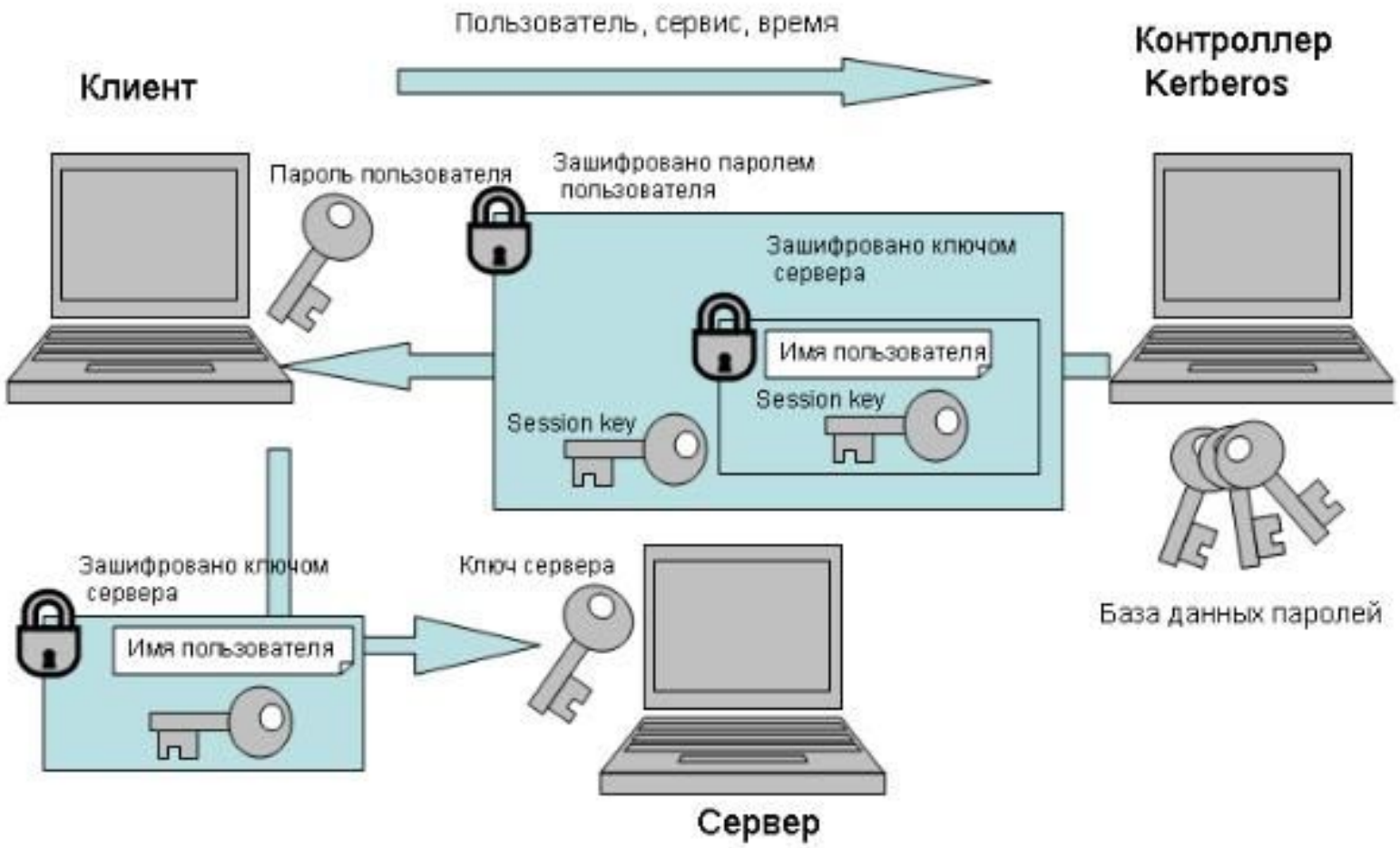
Требования к распределению ключей:

- Обеспечить **оперативность, точность, секретность**.

Протокол Kerberos

- Обеспечивает **распределение** ключей симметричного шифрования и **проверку подлинности** пользователей, работающих в незащищенной сети.
- Реализация Kerberos – это **программная система**, построенная по архитектуре «клиент-сервер».
- Наиболее известное использование Kerberos — это **Microsoft Active Directory**, служба каталогов по умолчанию, включенная в Windows 2000 и более поздних версий для управления доменами и аутентификации пользователей.

Схема функционирования протокола Kerberos

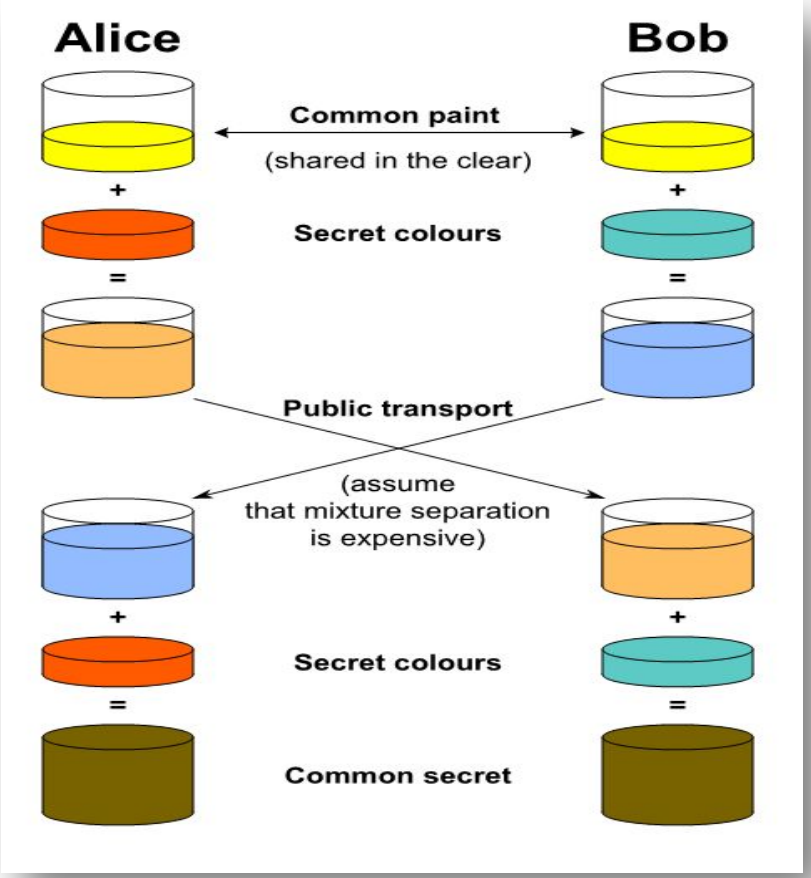


Распределение ключей по схеме Диффи-Хеллмана

- Односторонняя функция

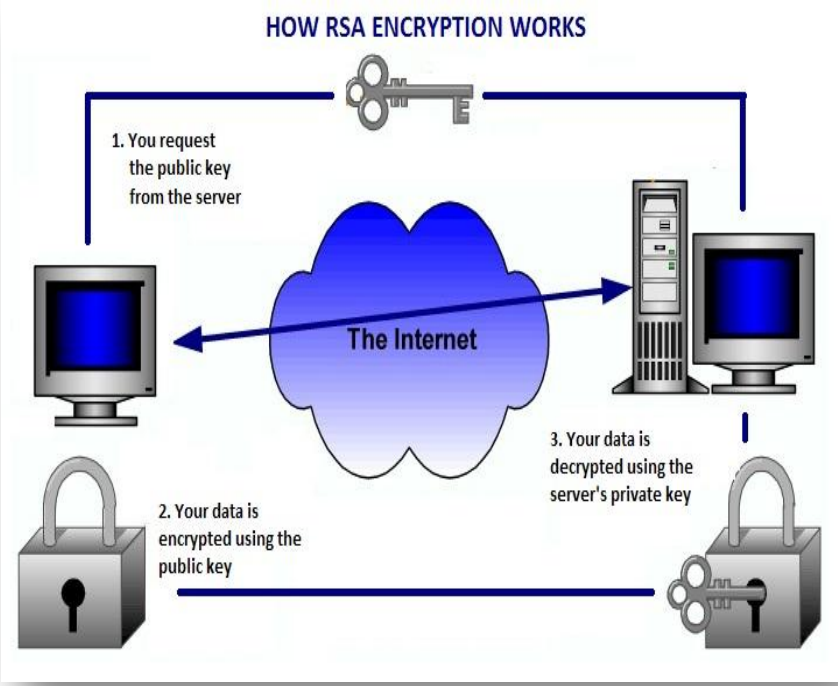
$$y = a^x mod\ p$$

- Алгоритм, позволяет двум абонентам, обмениваясь сообщениями по небезопасному каналу связи, распределить между собой **секретный ключ шифрования**.



Криптографическая система RSA

- Первый полноценный алгоритм **асимметричного шифрования** и **ЭЦП**.
- Первый этап- **генерация ключей**. Второй этап– **шифрование.**
- Третий этап– **расшифрование.**



Криптографическая система Эль-Гамаля

- Алгоритм шифрования с **открытым ключом** и **ЭЦП**.
- При использовании шифра Эль-Гамаля требуется, чтобы выбираемое в процессе шифрования случайное число число, **каждый раз менялось**.

Совместное использование симметричных и асимметричных шифров

- Симметричные и асимметричные алгоритмы часто используют вместе:
- **Для распределения ключей** и **ЭЦП - открытым ключом.**
- **Данные шифруют симметричными алгоритмами.**
- При совместном использовании оценивается **сложность** КС от **взлома** по сложности взлома самого **слабого звена**.

ХЭШ-ФУНКЦИИ

- **Односторонняя функция, преобразующая строку произвольной длины в строку фиксированной длины.**
- **Классы Хэш-функции**

1. Хэш-функции без ключа;
2. Хэш-функции с ключом.

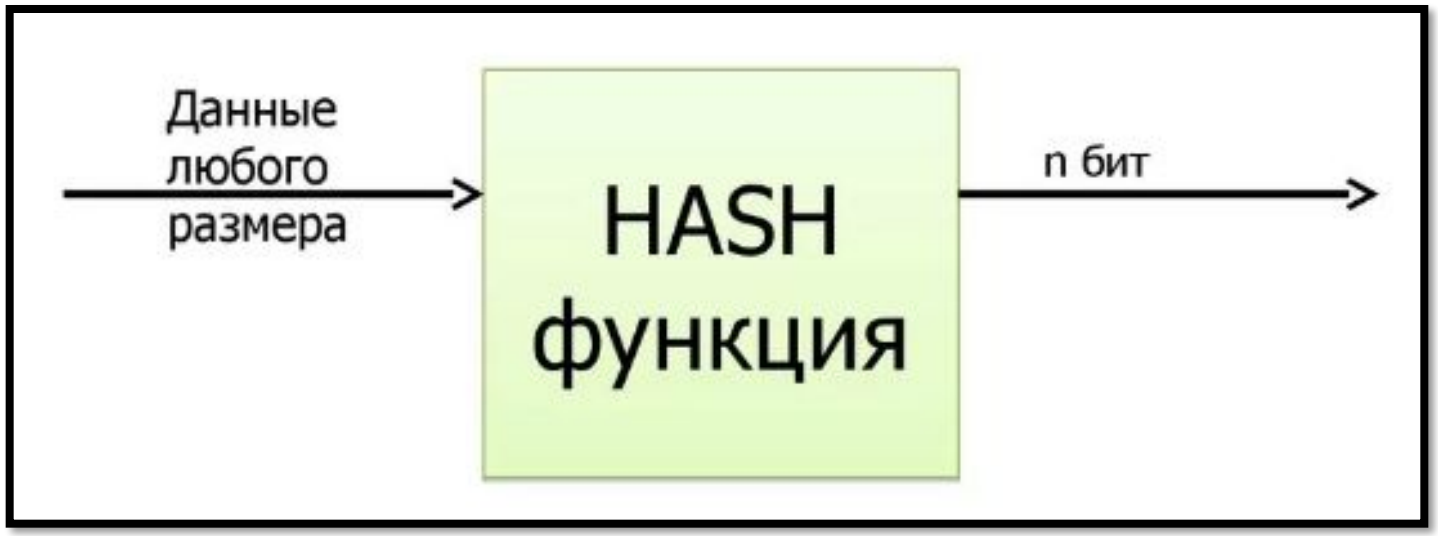
Алгоритм SHA-1 (Secure Hash Algorithm)

- **Алгоритм SHA-1** - **алгоритм** криптографического хеширования.

1. Получение на вход сообщения произвольной длины **менее 264 бит**;
2. SHA-1 формирует 160-битное **выходное сообщение**;
3. Вначале преобразуемое сообщение дополняется до длины, кратной 512битам.

Хэш-функции без ключа

- Хэш-функции без ключа делятся на **слабые** и **сильные**.
- Любая сильная хэш-функция соответствует и требованиям для слабой.

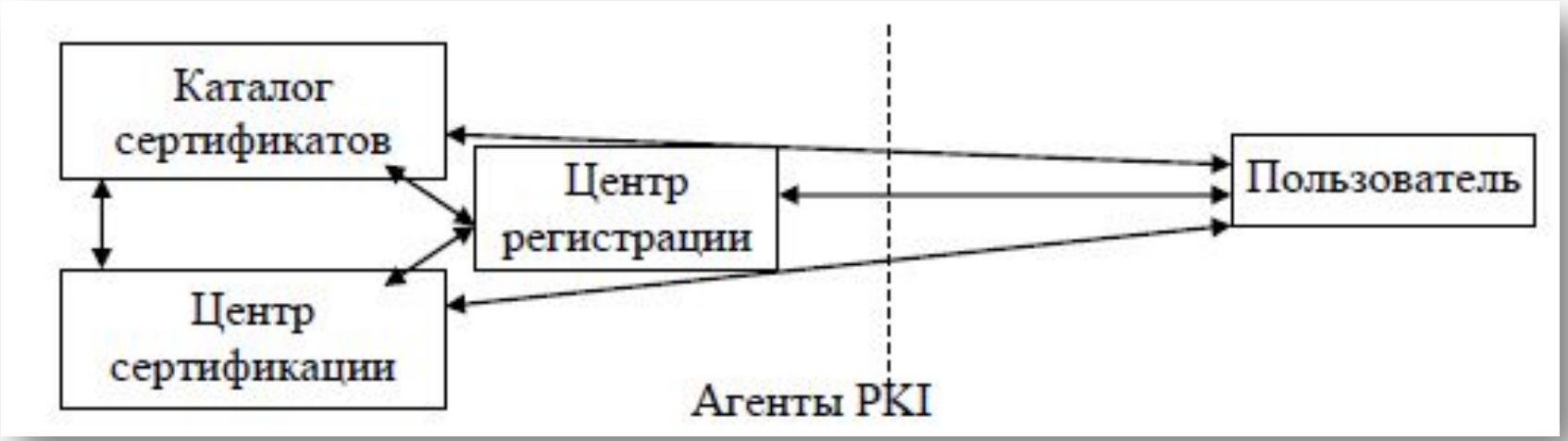


Хэш-функции с ключом

- Часто такие функции называются **кодами аутентификации** сообщений.
- Хэш-функцию с ключом можно построить на базе криптографической **хэш-функции без ключа** или **алгоритма шифрования**.

PKI (Pablic Key Infrastructure)

- **PKI** - набор средств, мер и правил, предназначенных для **управления ключами**, **политикой безопасности** и **обменом защищенными сообщениями**.



ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ

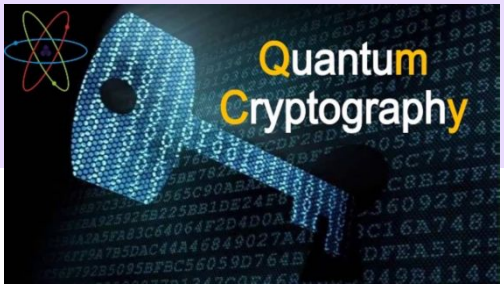
- Использование методов асимметричной криптографии сделало возможным **безопасный обмен** криптографическими ключами между **отправителем** и **получателем**.
- **Проблема** – **как убедиться в том, что имеющийся у Вас открытый ключ другого абонента на самом деле принадлежит ему?**

Цифровые сертификаты

- **Создание доверенной стороны** – арбитр, которому доверяют оба абонента.
- Заверяется ключ с помощью **цифрового сертификата**.
- Для подтверждения подлинности открытых ключей создается **инфраструктура открытых ключей (PKI).**

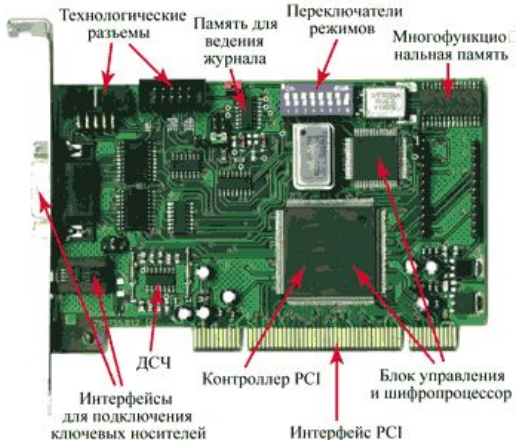
Квантовая криптография

- метод защиты коммуникаций, основанный на **принципах квантовой физики**.
- В отличие от традиционной криптографии, информация переносится с помощью объектов **квантовой механики**.
- Процесс отправки и приёма информации всегда выполняется физическими средствами, например, при помощи **электронов** в электрическом токе, или **фотонов** в линиях **волоконно-оптической связи.**



Вопрос 3: «Средства **криптографической защиты информации»**

- **Средства криптографической защиты информации** (СКЗИ) - аппаратные, программно-аппаратные и программные средства, реализующие криптографические алгоритмы преобразования информации



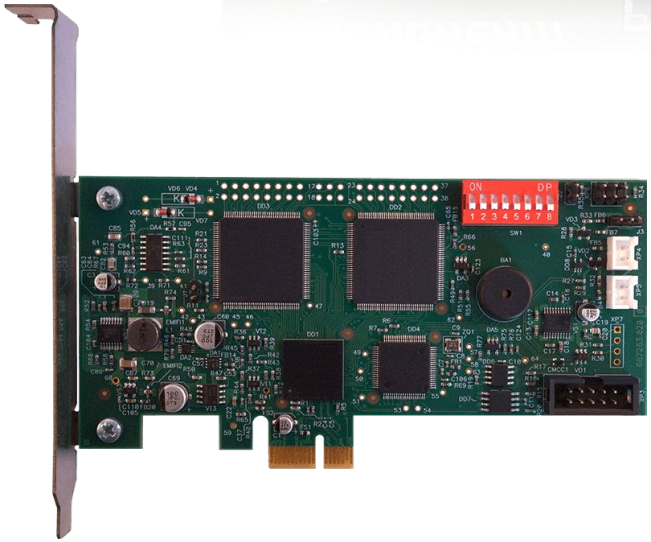
Виды средств криптографической защиты информации

- **средства шифрования;**
- средства имитозащиты;
- **средства электронной подписи;**
- средства кодирования;
- средства изготовления ключевых документов;
- ключевые документы;
- **аппаратные шифровальные (криптографические) средства;**
- программные шифровальные (криптографические) средства;
- программно-аппаратные шифровальные (криптографические) средства.

Основной документ по СКЗИ

- **Приказ ФСБ РФ от 09.02.2005 N 66 (ред. от 12.04.2010) «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»**

Средства шифрования



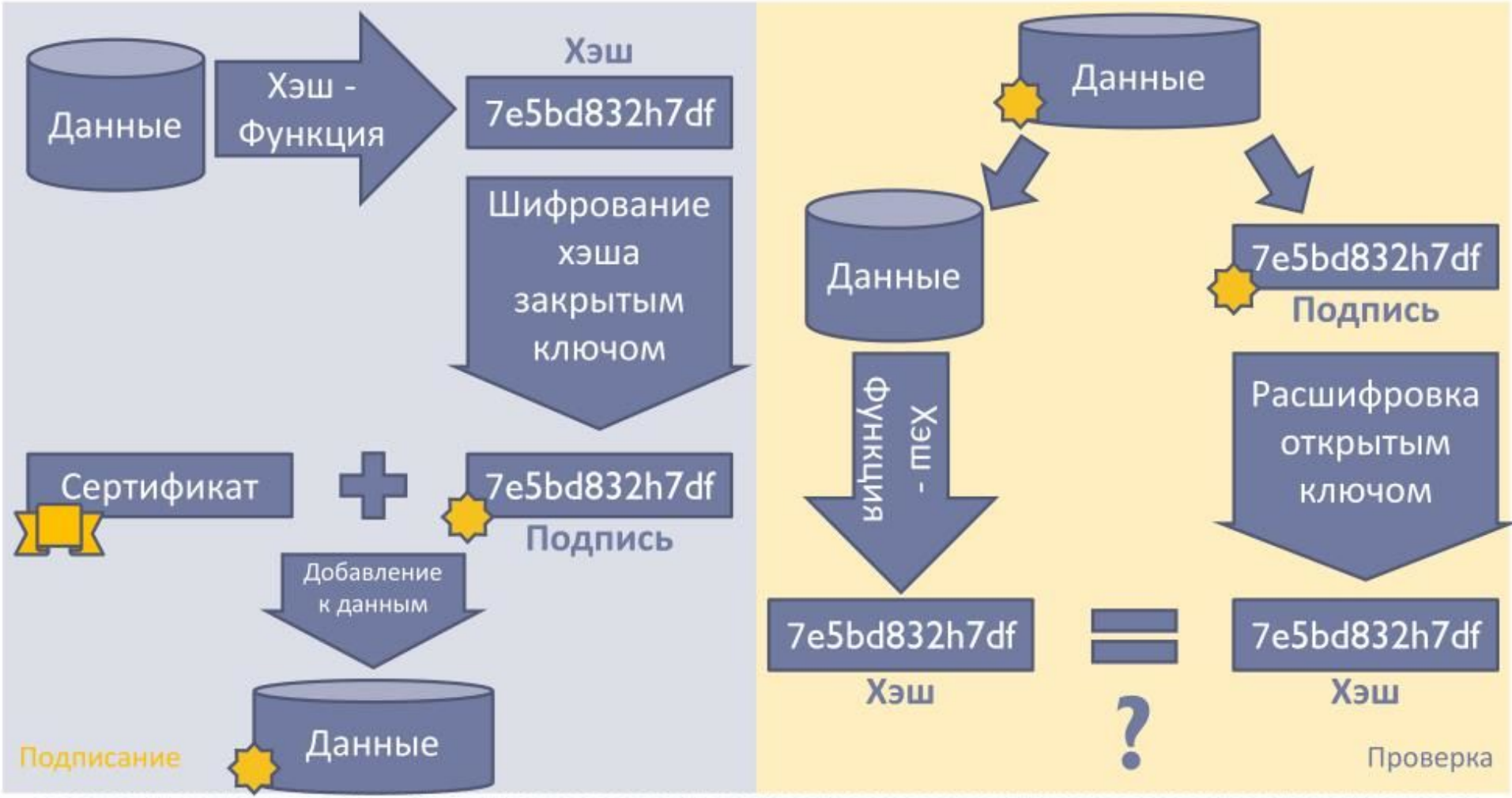
ЭЛЕКТРОННАЯ ПОДПИСЬ

- **Электронная подпись** - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая **используется для определения лица**, подписывающего информацию.

- ***Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи»***

Виды электронных подписей

ПРИНЦИП ДЕЙСТВИЯ ЭЛЕКТРОННОЙ ПОДПИСИ



Нормативные документы по использованию ЭП

- **ПП РФ от 25 июня 2012 г. N 634 «О видах электронной подписи, использование которых допускается при обращении за получением государственных и муниципальных услуг».**
- **ПП РФ от 25.01.13 N 33 «Об использовании простой электронной подписи при оказании государственных и муниципальных услуг»**

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лекция 12:

«Информационная безопасность сетевых технологий»

Вопросы:

1. Базовая архитектура сетевого взаимодействия.
2. Стандартные протоколы защищенного сетевого взаимодействия.
3. Обеспечение информационной безопасности вычислительных сетей.

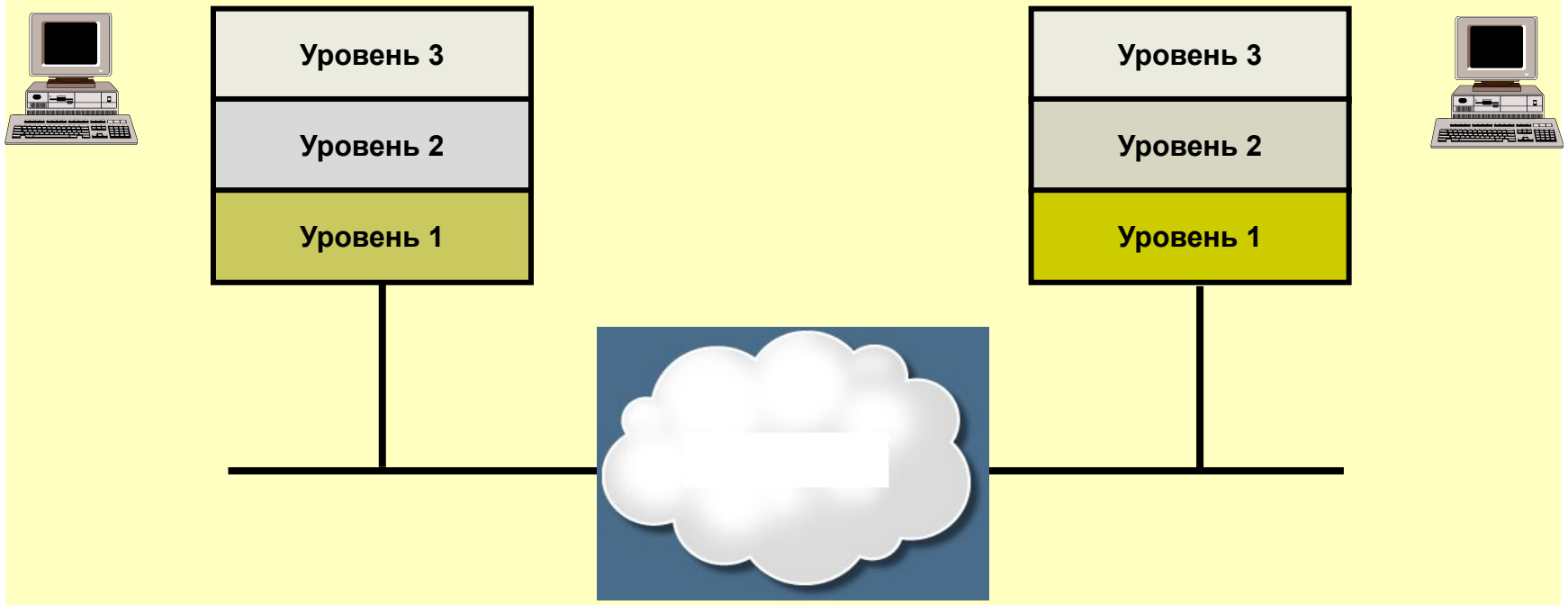
Вопрос 1: «Базовая архитектура сетевого взаимодействия»

- **Архитектура** – концепция, определяющая взаимосвязь, структуру и функции взаимодействия рабочих станций в сети.
- **Предусматривает:** логическую, функциональную и физическую организацию технических и программных средств сети.
- **Определяет:** принципы построения и функционирования аппаратного и программного обеспечения элементов сети.

Модель ISO/OSI

- **Проблема:** разработчики (IBM, Honeywell, Digital и др.) имели закрытые реализации для соединения ПК, приложения, работающие на платформах от различных поставщиков, ***не имели возможности обмениваться данными через сеть.***
- **В 1978 г. Международная организация по стандартизации** (*International Standards Organization*, **ISO**) приняла модель *Open Systems Interconnection* (**OSI**) **Reference Model** – эталонная модель взаимодействия открытых систем

Многоуровневая архитектура – основной



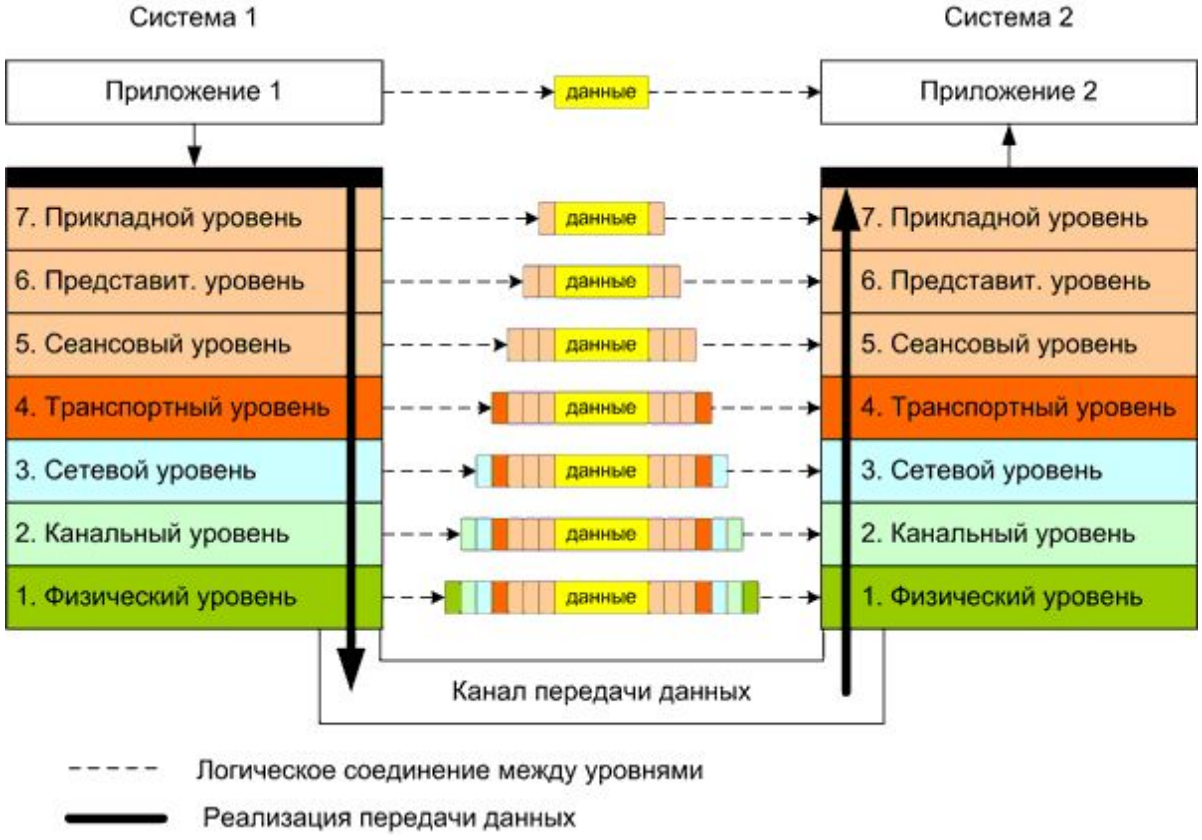
Основные особенности:

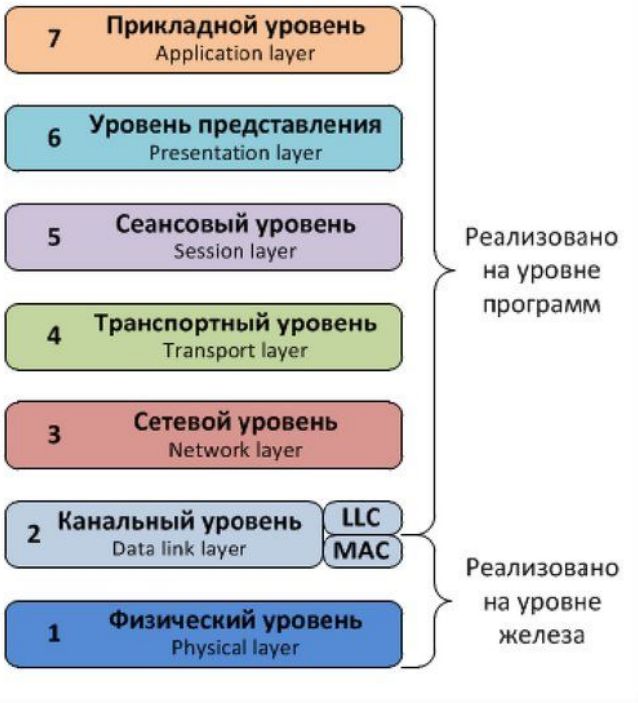
- Стандарт передачи данных, позволяющий системам **различных производителей** устанавливать сетевые соединения.
- Состоит из **семи уровней** со специфическим набором сетевых функций, определенных для каждого уровня, и включает описания межуровневых интерфейсов
- Определяет **набор протоколов и интерфейсов** для применения на каждом уровне.

Уровни модели ISO/OSI

	Уровень (layer)	Тип данных	Функции уровня	Особенность адресации	Примеры протоколов
Уровни хоста (узла)	7. Прикладной (application)	Данные (строки из байтов)	Доступ к сетевым службам	URL	HTTP(S), FTP(S), RPC, POP3
	6. Представительский (представления) (presentation)		Представление (кодировка) и шифрование данных		ASCII, EBCDIC
	5. Сеансовый (session)		Управление сеансом связи		PAP
	4. Транспортный (transport)	Сегменты (segment) / Дейтаграммы (datagram)	Прямая связь между конечными пунктами и надёжность	Порт	TCP, UDP, SCTP, PORTS
Уровни связи (сети)	3. Сетевой (network)	Пакеты (packet)	Определение маршрута и логическая адресация	IP-адрес	IPv4, IPv6, IPsec, AppleTalk
	2. Канальный (data link)	Биты (bit) / Кадры (frame)	Физическая адресация	MAC-адрес (физический адрес компьютера)	PPP, IEEE 802.22, Ethernet, DSL, ARP, L2TP, сетевая карта.
	1. Физический (physical)	Электрические сигналы, Биты (bit)	Работа со средой передачи, сигналами и двоичными данными		USB, кабель ("витая пара", коаксиальный, оптоволоконный), радиоканал

Особенности уровней модели ISO/OSI

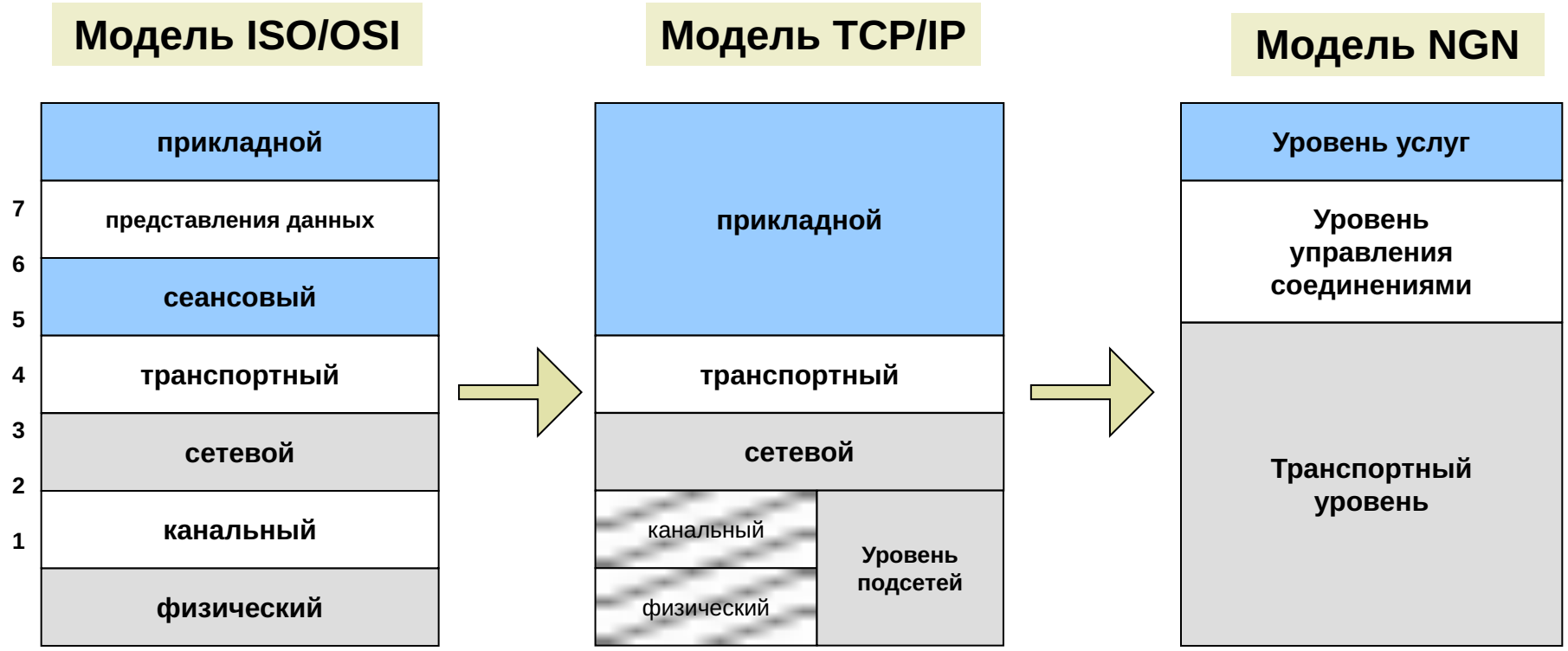




Принципы многоуровневой модели

- Каждый новый уровень модели появляется только тогда, когда требуется новый уровень абстракции.
- Каждый уровень должен выполнять определенную функцию.
- Функция каждого уровня должна быть выбрана на основе международных стандартизированных протоколов
- Границы уровня должны быть выбраны таким образом, чтобы информационный поток через интерфейс был минимален.
- Количество уровней должно быть достаточным, чтобы существовала возможность распределения функций, но и не слишком большим, чтобы сохранить стройную и легкую для восприятия архитектуру.

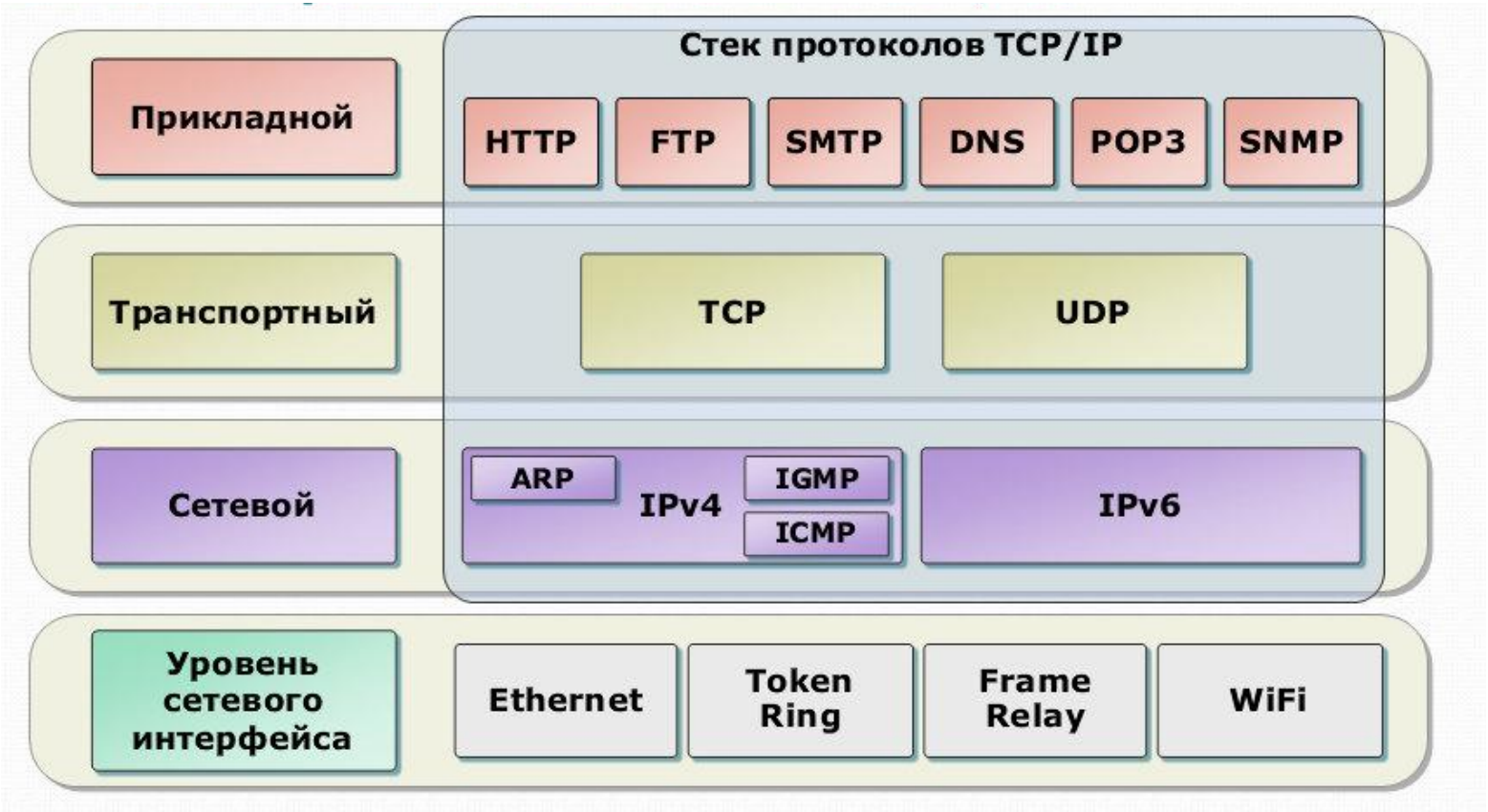
Эволюция от модели ISO/OSI к NGN



Вопрос 2: «Стандартные протоколы защищенного сетевого взаимодействия»

- **Стек протоколов TCP/IP** (англ. *Transmission Control Protocol/Internet Protocol, Протокол управления передачей*) — набор сетевых протоколов разных уровней модели сетевого взаимодействия DOD, используемых в сетях.
- Протоколы работают друг с другом в стеке (*англ. stack, стопка*) — протокол, располагающийся на уровне выше, работает «поверх» нижнего, используя механизмы **инкапсуляции**.

Стек сетевых протоколов TCP/IP



Протокол ARP

- **ARP** (*Address Resolution Protocol — протокол определения адреса*) —для определения **MAC-адреса** другого компьютера по известному IP-адресу.
- Спроектирован для передачи IP-пакетов через пакеты (кадры) Ethernet.
- Принцип выяснения аппаратного адреса целевого хоста, использован в сетях других типов (канальный уровень).
- **Варианты протокола ARP: InARP** и **ATM ARP.**

Атаки канального уровня

- **MAC- spoofing** (*spoof — мистификация*) — метод изменения MAC-адреса сетевого устройства, позволяющий обойти список контроля доступа к серверам, маршрутизаторам, либо скрыть компьютер, что может нарушить работоспособность сети.
- **MAC - flooding.** (*flood — наводнение*) - кибератака, целью которой является компрометация данных, передаваемых на подключенное к сетевому коммутатору устройство (переполнение ARP-таблицы).

RIP (сетевой протокол)

- **Протокол маршрутной информации** (*Routing Information Protocol*)
- Применяется в небольших компьютерных сетях, позволяет маршрутизаторам динамически обновлять маршрутную информацию, получая ее от соседних маршрутизаторов.
- Оперирует транзитными участками (hop) в качестве метрики маршрутизации.

Протокол OSPF

- **OSPF** (*Open Shortest Path First*) — протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (*link-state technology).*
- Распространяет информацию о доступных маршрутах между маршрутизаторами одной автономной системы.
- Оптимальное использование пропускной способности с построением **дерева кратчайших путей** (алгоритм Дейкстры).

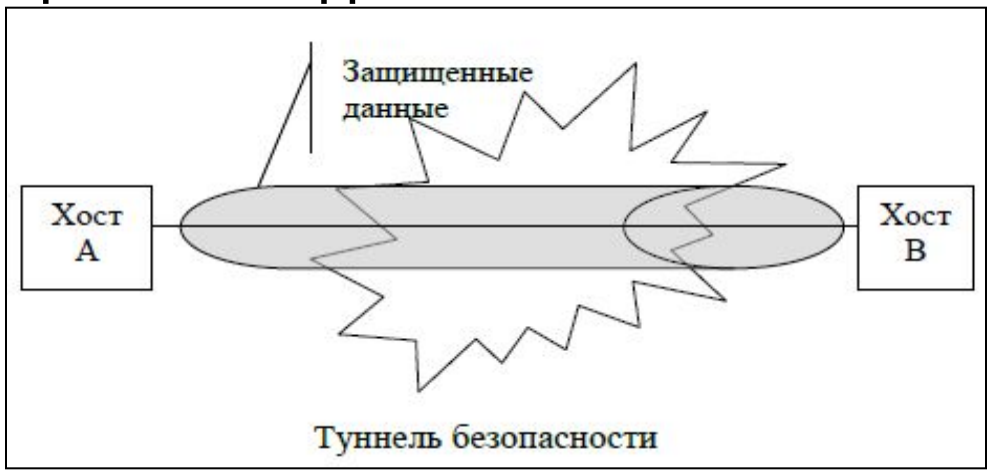
Протоколы IPSec и распределение ключей

- **Протокол IPSec** - базовый протокол обеспечения безопасности на уровне IP-соединения. Предоставляемые возможности:

1. Контроль доступа;
2. Контроль целостности данных;
3. Аутентификацию данных;
4. Защиту от повторений;
5. Обеспечение конфиденциальности.

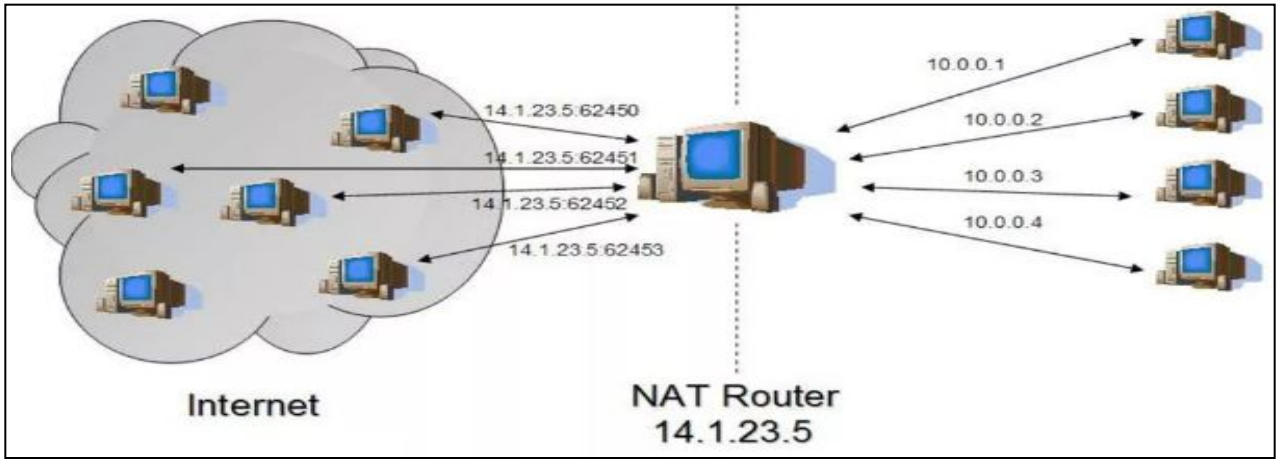
Основная задача IPSec

- **Основная задача IPSec** – создание между двумя компьютерами, связанными через общедоступную IP-сеть, безопасного туннеля, по которому передаются конфиденциальные данные.



Протоколы IP Sec и трансляция сетевых адресов

- Маршрутизатор, внешнему интерфейсу которого назначен один зарегистрированный ip-адрес, **модифицирует ip-заголовки** сетевых пакетов, подставляя вместо частных адресов зарегистрированный адрес.



Протокол AH

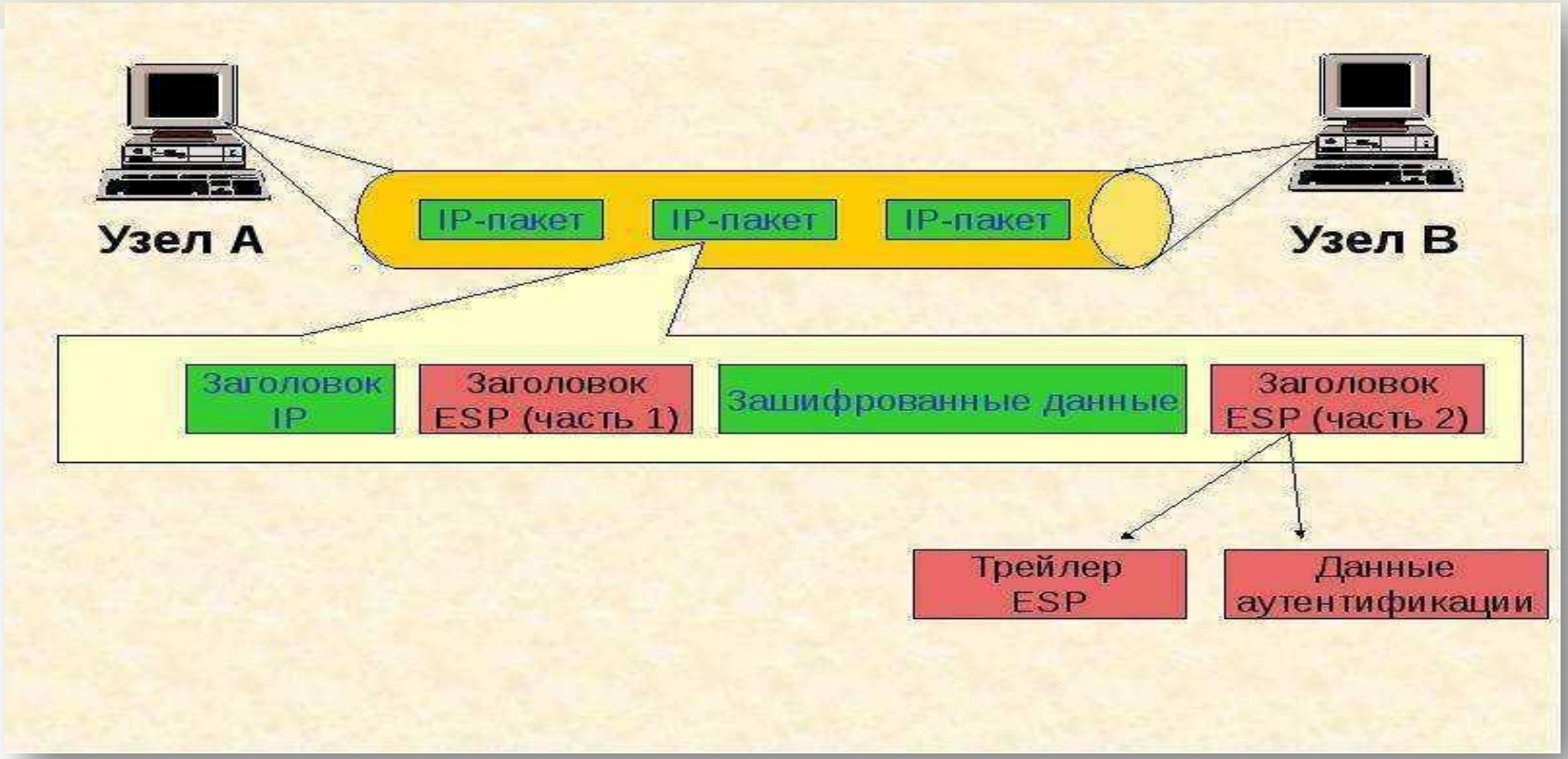
- Протокол AH позволяет **идентифицировать** отправителя данных, а также обеспечивает **целостность** данных и **защиту** от воспроизведения информации.
- Целостность данных проверяется в протоколе AH с помощью **контрольной суммы**, созданный алгоритмом идентификации сообщения.

Протокол ESP

- ESP обеспечивает **конфиденциальность** передаваемых данных.
- ESP работает в **транспортном** и **туннельном** режимах.
- Алгоритмы для ESP:

1. Для формирования имитовставки HMAC-MD5-96;
2. Для шифрования - DES.

Схема протокола ESP



Протоколы ISAKMP и IKE

- **Протокол ISAKMP** – протокол **управления ключами** и **контекстами безопасности**, разработан для решения задач согласования параметров и управления ключами при **формировании защищенного канала**.
- **Протокол IKE** - протокол обмена ключами в Internet, считается более **надежным** и **гибким**.

Протокол IKE

IKE (Internet Key Exchange) — стандартный протокол набора прот околов IPsec, используемый для обеспечения безопасности взаимодействия в VPN. Предназначение IKE — защищенное согласование и доставка идентифицированного материала для "ассоциации безопасности" (SA).

TCP (транспортный протокол)

едаче
один из основных протоколов передачи данных интернета.

- Механизм TCP - поток данных с предварительной установкой соединения, осуществляет повторный запрос данных в случае потери данных и **устраняет дублирование** при получении двух копий одного пакета, **гарантируя целостность передаваемых данных** и уведомление отправителя о результатах передачи.
- Реализации встроены в ядра ОС.
- При передача от ПК к ПК через Интернет, TCP работает на верхнем уровне между двумя конечными системами, например, браузером и веб-сервером.

Протоколы SSL и TLS

- **SSL** (*Secure Socket Layer*) разработан для обеспечения **аутентификации**, **целостности** и **секретности** трафика на **сеансовом уровне** модели OSI (модели стека протоколов TCP/IP).
- Два этапа взаимодействия клиента и сервера:

1) установление SSL-сессии;
2) защищенное взаимодействие.

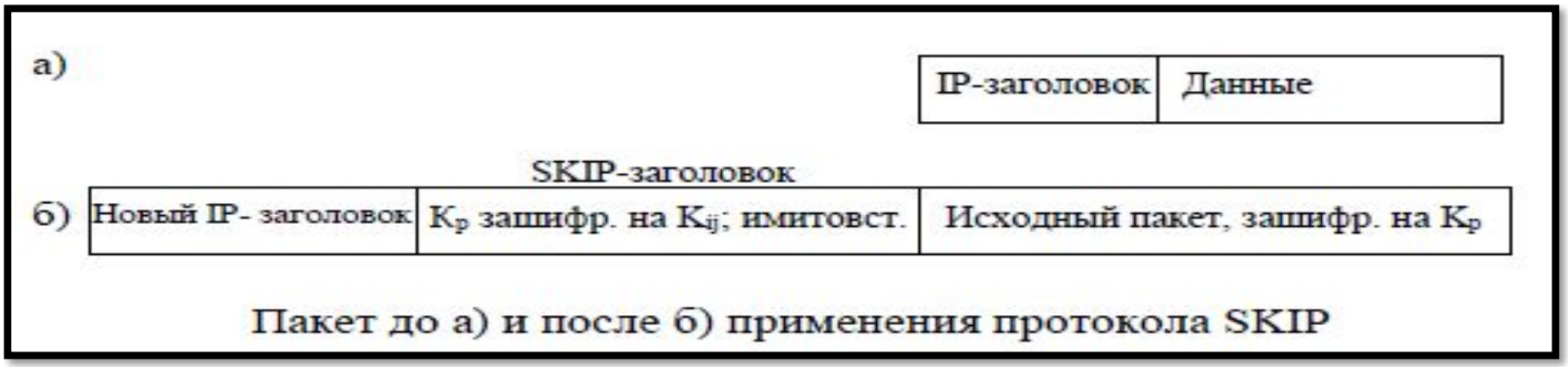
- **TLS** (*transport layer security*)

Назначение протоколов SSL и TLS

- Протоколы SSL и TLS используются для **защиты трафика**, передаваемого по протоколу HTTP в сети Интернет.

Протокол SKIP

- Разновидность протокола SSL, обеспечивает управление ключами и криптозащиту передаваемых данных на сетевом уровне модели OSI.



Пакет до а) и после б) применения протокола SKIP

Протокол защиты электронной почты S/MIME

- **Протокол S/MIME** предназначен для защиты данных, передаваемых в формате MIME, в основном – **электронной почты** **(прикладной уровень)**.
- Протокол S/MIME предоставляет:
  - Проверку **целостности** сообщения;
  - Установление **подлинности** отправителя;
  - Обеспечение **конфиденциальности** передаваемых данных.

Фрагмент электронного письма с подписью

```
Content-Type: multipart/signed;
        protocol="application/pkcs7-signature";
        micalg=sha1; boundary=boundary42

--boundary42
Content-Type: text/plain

This is a clear-signed message.

--boundary42
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s

ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT6
4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbB9HGTrfvbnj
n8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
7GhIGfHfYT64VQbnj756

--boundary42--
```

Протокол DHCP

- **DHCP** (*Dynamic Host Configuration Protocol — протокол динамической настройки узла*) — **прикладной протокол**, позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Работает по модели «клиент-сервер».
- Сетевой администратор может задать ***диапазон адресов***, распределяемых сервером среди компьютеров.
- Позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок.

Протокол HTTPS

- **HTTPS** (*от англ. HyperText Transfer Protocol Secure*) – это безопасный протокол передачи данных, который поддерживает шифрование посредством криптографических протоколов SSL и TLS, и является расширенной версией протокола HTTP.

Вопрос 3: «Обеспечение информационной безопасности вычислительных сетей»

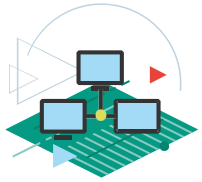
Уровни модели OSI:

Прикладной	Код пользователя
Представления	Передача и шифрование данных
Сеансовый	Обмен данными между системами
Транспортный	TCP и UDP протоколы
Сетевой	Протокол Интернет (IP)
Канальный	Передача данных между двумя узлами (MAC)
Физический	Провода, приёмники и оптика

Концепт сетевых зон

Интернет

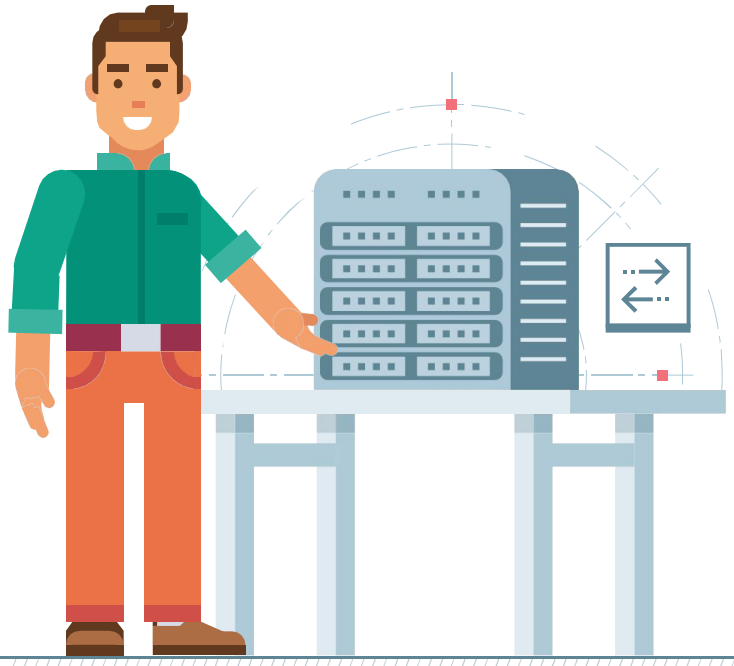
Демилитаризованная зона(DMZ)



Интранет (Локальная сеть)

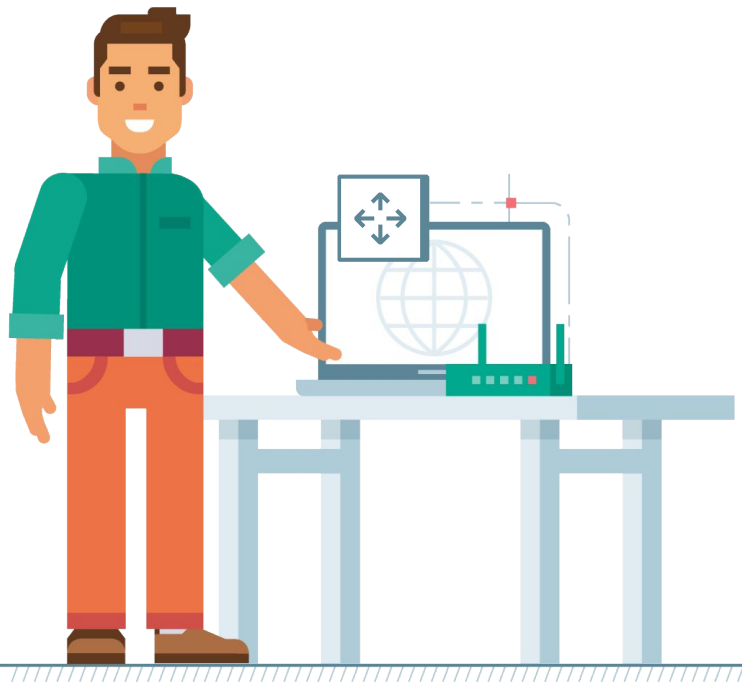
Экстранет

Коммутаторы рабочей сети



- В основном используется на оборудовании канального уровня, но имеет также современные решения для других уровней
- Используется для соединения сетевых устройств через физические адреса (MAC) для защиты сетей
- Гораздо лучше и безопаснее, чем концентраторы, поскольку только необходимые устройства получают сетевой трафик
- Защита коммутаторов от самих атак имеет первостепенное значение для защиты сетей

Маршрутизаторы



- Обычно рассматриваются как устройства сетевого уровня, но некоторые работают на более высоких уровнях
- Используется для соединения сетевых устройств через логические адреса (IP)
- Выполняют маршрутизацию (статическую и динамическую)
- Может использоваться в качестве контрольной точки (как брандмауэр), но с меньшим количеством функций
- В локальной сети обычно виртуальные - эмулируется коммутаторами сетевого уровня (VRF - виртуальная маршрутизация и пересылка)
- Защита коммутаторов от самих атак имеет первостепенное значение для защиты сетей

Виртуальная Частная Сеть (VPN)

По уровням

Сетевой уровень

- Протокол защиты сетевого трафика (IPSec)
- Любые туннели IP к IP (общая инкапсуляция маршрутизации и т. д.)

Канальный уровень

- Протокол туннелирования второго уровня (L2TP) - L2TP создаёт туннель и IPSec обеспечивает безопасность передачи данных
- Туннельный протокол типа точка-точка (PPTP) – использует сетевой протокол (PPP), чтобы защитить данные

Прикладной уровень

- Уровень защищенных сокетов (SSL) и TLS
- OpenVPN использует SSL/TLS
- Протокол безопасной среды(SSH)

По использованию

На основе сети: Безопасное соединение сетей через ненадежную сеть

- IPSec
- Динамические многоточечные VPN
- L3VPN, основанные на MPLS

На основе клиента: соединение пользователя и сети

- IPSec
- SSL/TLS

Типы брандмауэров

Межсетевые экраны с фильтрацией пакетов - при доступе к контролю сетевого и транспортного уровней на основе данных заголовка пакета

Шлюзы на уровне цепей - контролируют установку сеанса, например, TCP-рукопожатия; шлюзы не проверяют сами пакеты

Межсетевые экраны с отслеживанием состояния - проверяют каждый пакет + отслеживают каждый сеанс; новейшие варианты проверяют протоколы без сессий и поток транзакций через несколько уровней OSI

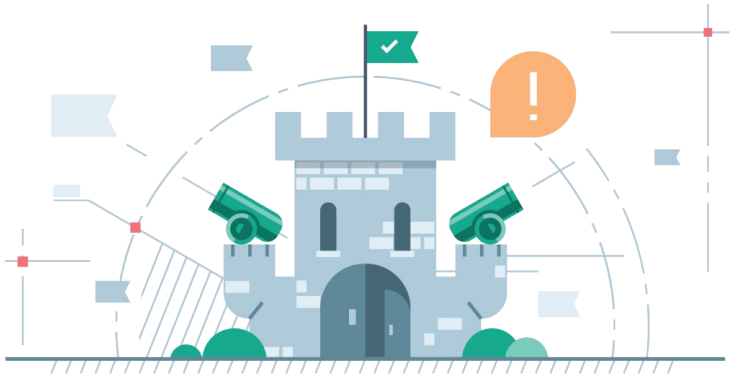
Шлюзы уровня приложения (прокси) - анализируют данные на уровне приложения, чтобы выполнить фильтрацию, также поддерживает адаптацию контента (ICAP - RFC-3705)

Межсетевые экраны «следующего поколения» с отслеживанием состояния + глубокая проверка пакетов
DPI - анализируют также данные в полезной нагрузке пакета (поскольку отслеживает состояние в основном с заголовками)
- «осведомление на уровне приложения»

Прокси: Веб и Почтовые шлюзы

- Защита клиентов
- Протоколы прикладного уровня: HTTP, SMTP
  - Фильтр на основе команд/заголовков
  - Сбор разделов данных
  - Фильтр на основе типа передаваемых данных
  - Адаптация контента в процессе работы
    - Замена, удаление (Блок рекламы)
    - Обработка архивов
  - Отправлять различные части содержимого для стороннего анализа
- Фильтр по репутации сайтов
  - Возможность интеграции с разными источниками
- Понимание распространенных атак

- MITM SSL/TLS
  - Проверка сертификата
  - Поддержка обходов(банкинг)




Корпоративная сеть
Контрагент
Сотрудник
PCI CDE
Удаленные пользователи
Гость
Мобильный гость
Интернет
Безопасность контента
Управление пропускной способностью
Политика контроля
Гибкость системы
Сценарии клиента
Облачный анализ угроз
Централизованное управление
Службы безопасности веб-шлюза
Идентификация пользователя
Фильтрация адресов
Применение политики веб-доступа
Защита от вирусов
Технология единого входа
Технические услуги и поддержка
Журналирование отдела кадров
Системный администратор
Интернет
Разрешенные сайты
Зараженные исполняемые файлы
Сервис обновления
Зараженные приложения
SaaS
Запрещенные сайты

Единое управление угрозами

Достоинства

- Уменьшенная сложность
- Простое развертывание
- Простая интеграция
- Низкая стоимость (одно устройство)
- Межсетевой экран прикладного уровня
- Веб/Почтовый прокси
- Обнаружение и предотвращение вторжений
- Общий антивирус

Недостатки

- Разная эффективность разных компонентов
- Не все функции могут потребоваться
- Ограниченная масштабируемость и надежность
- Единственная точка отказа для всех составляющих системы

Сегментация (не полный список)

- Доступ в Интернет VLAN - разрешен только IP к Интернету
- DMZ - доступ к серверам из Интернета (DNS, MX, WWW и т. д.), IP-доступ к локальной сети ограничен
- Внутренняя DMZ - доступ к серверам внутри филиала
- Партнерская DMZ - доступ к серверам партнеров
- Серверы (может быть несколько, в зависимости от критичности безопасности) - доступны только для серверных приложений
- Многофункциональные устройства в сети - доступ только с принт-серверов и у администраторов
- Резервное копирование всей корпоративной системы
- Пользователи (может быть несколько в зависимости от количества и требования доступа) - пользовательские рабочие станции
- Администраторы – административные рабочие станции – интерфейсы администратора серверов доступа
- Servicedesk - административные рабочие станции, которым разрешено подключаться к рабочим станциям пользователя.
- Специальные рабочие станции с персональным VPN - банки-клиенты, терминалы бронирования
- SCADA (диспетчерский контроль и сбор данных) - системы управления производством
- Беспроводная сеть с ограниченным доступом для мобильного оборудования (как правило, для корпоративных клиентов с различным доступом)
- Удаленный доступ - VLAN для удаленных пользователей (VPN, RAS и т. д.)