ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

1. Малюк А.А. Защита информации в информационном обществе: учебное пособие – М.: Горячая линия – Телеком, 2015.
2. Малюк А.А., Горбатов В.С., Королев В.И., Фомичев В.М., Дураковский А.П., Кондратьева Т.А. Введение в информационную безопасность: учебное пособие – М.: Горячая линия – Телеком, 2011.
3. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: учебное пособие – М.: Горячая линия – Телеком, 2006.
4. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: учебное пособие, 2-е издание – М.: Горячая линия - Телеком, 2004.

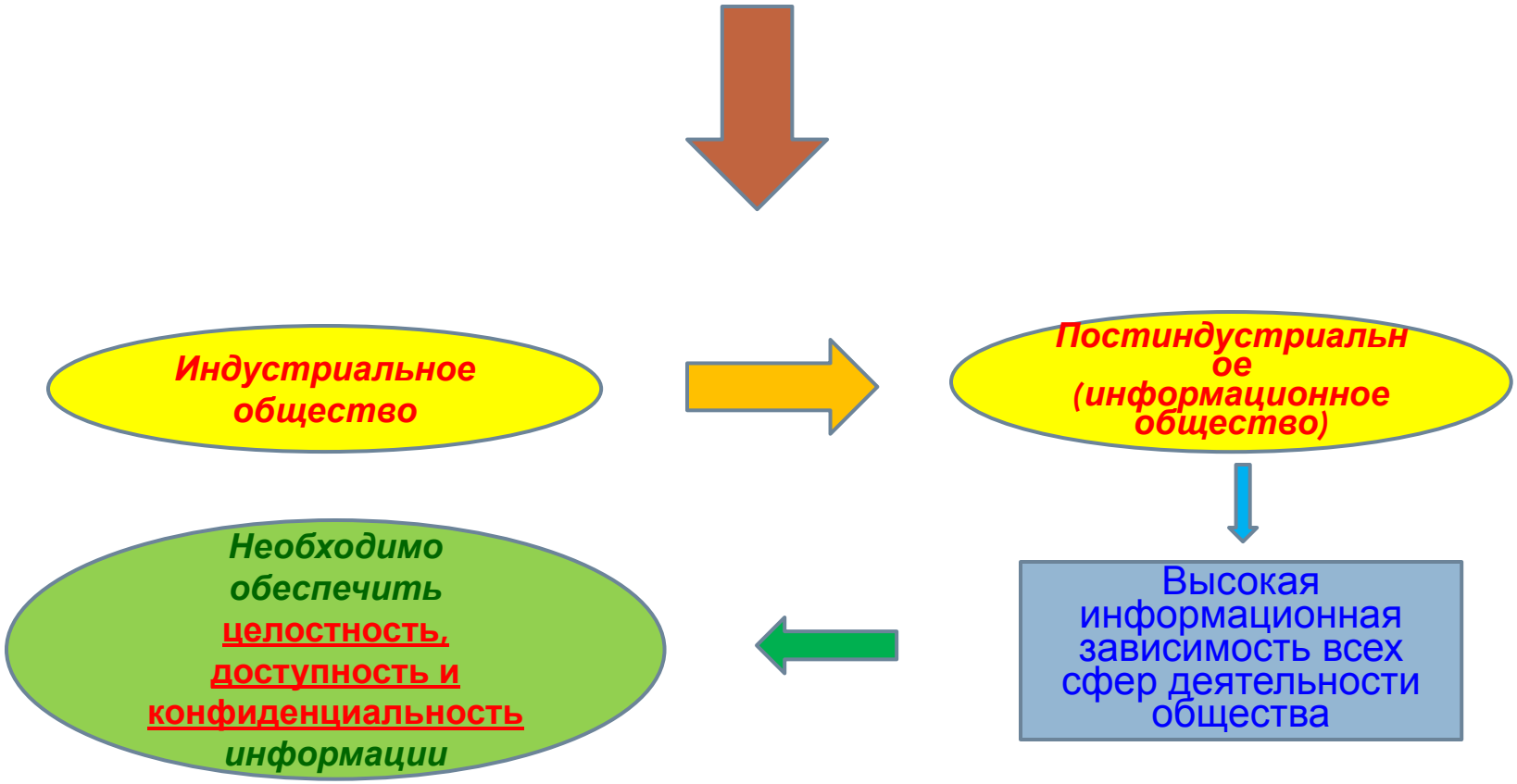
ДОКУМЕНТЫ СОВЕТА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

1. Доктрина информационной безопасности Российской Федерации.
2. Стратегия развития информационного общества в Российской Федерации.
3. Стратегия национальной безопасности Российской Федерации.
4. Основные направления научных исследований в области обеспечения информационной безопасности Российской Федерации.
5. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации.
6. Основы государственной политики Российской Федерации в области

ВВЕДЕНИЕ

Информационное общество и информационная безопасность

Новый исторический этап развития общества



Информационное общество и информационная безопасность

Стратегия развития информационного общества в России (утверждена Президентом Российской Федерации 9 мая 2017 года)

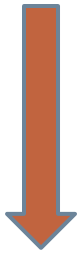
	Отличительные черты информационного общества
	❖ Существенное увеличение в валовом внутреннем продукте доли отраслей экономики, связанных с производством знаний, с созданием и внедрением наукоемких, в том числе информационных, технологий, других продуктов интеллектуальной деятельности, с оказанием услуг в области информатизации, образования, связи, а также в области поиска, передачи, получения и распространения информации (информационных услуг)
	❖ Ускорение научно-технического прогресса и превращение научных знаний в реальный фактор производства, повышения качества жизни человека и общества
	❖ Участие значительной части трудоспособного населения в производственной деятельности, связанной с созданием и использованием информационных технологий, информации и знаний
	❖ Существенное расширение возможностей граждан по поиску, получению, передаче, производству и распространению информации и знаний

Формирование новой сферы деятельности и области знания «*ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*»

Терминология

Формула Декарта:

«Определяйте значения слов и вы избавите мир от половины заблуждений»



Важнейшая проблема – разработка глоссария в области информационной безопасности

Формирование новой сферы деятельности и области знания «*ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*»

Глоссарий

Угроза информации со стороны среды

Угроза среде со стороны информации

Безопасность информации – ***состояние защищенности информации от вредного воздействия среды***

Информационная безопасность – ***состояние защищенности среды от вредного воздействия информации***

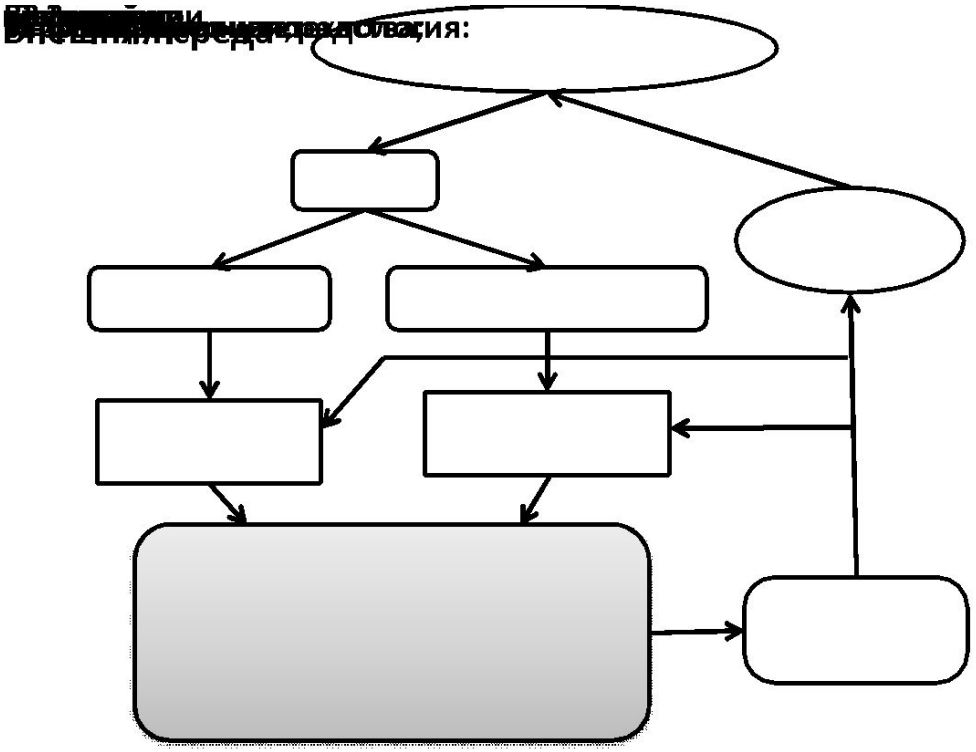
Защита информации – ***процесс перехода к состоянию защищенности информации от вредного воздействия среды***

Защита от информации – ***процесс перехода к состоянию защищенности среды от вредного воздействия информации***

Формирование новой сферы деятельности и области знания «*ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*»

Информационная безопасность – комплексная проблема

Состояние защищенности и среды, и информации от вредных информационных воздействий



Формирование новой сферы деятельности и области знания «*ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*»

Доктрина информационной безопасности Российской Федерации

«Информационная безопасность Российской Федерации – 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 Российской Федерации, оборона и безопасность государства»

Формирование новой сферы деятельности и области знания «*ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*»

Доктрина информационной безопасности Российской Федерации

«Угроза информационной безопасности Российской Федерации – совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере»

Формирование новой сферы деятельности и области знания «*ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*»

Доктрина информационной безопасности Российской Федерации

«Национальные интересы Российской Федерации в информационной сфере – объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития в части, касающейся информационной сферы»

Формирование новой сферы деятельности и области знания «*ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*»

Доктрина информационной безопасности Российской Федерации

«Информационная сфера – совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений»

Формирование новой сферы деятельности и области знания «*ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*»

Доктрина информационной безопасности Российской Федерации

Национальные интересы в информационной сфере

«Обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий, обеспечение информационной поддержки демократических институтов, механизмов взаимодействия государства и гражданского общества, а также применение информационных технологий в интересах сохранения культурных, исторических и духовно-нравственных ценностей многонационального народа Российской Федерации»

Формирование новой сферы деятельности и области знания «*ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*»

Доктрина информационной безопасности Российской Федерации

Национальные интересы в информационной сфере

«Обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации и единой сети электросвязи Российской Феде6рации, в мирное время, в период непосредственной угрозы агрессии и в военное время»

Формирование новой сферы деятельности и области знания «*ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*»

Доктрина информационной безопасности Российской Федерации

Национальные интересы в информационной сфере

«Развитие в Российской Федерации отрасли информационных технологий и электронной промышленности, а также совершенствование деятельности производственных, научных и научно-технических организаций по разработке, производству и эксплуатации средств обеспечения информационной безопасности, оказанию услуг в области обеспечения информационной безопасности»

Формирование новой сферы деятельности и области знания «*ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*»

Доктрина информационной безопасности Российской Федерации

Национальные интересы в информационной сфере

«Доведение до российской и международной общественности достоверной информации о государственной политике Российской Федерации и ее официальной позиции по социально значимым событиям в стране и мире, применение информационных технологий в целях обеспечения национальной безопасности Российской Федерации в области культуры»

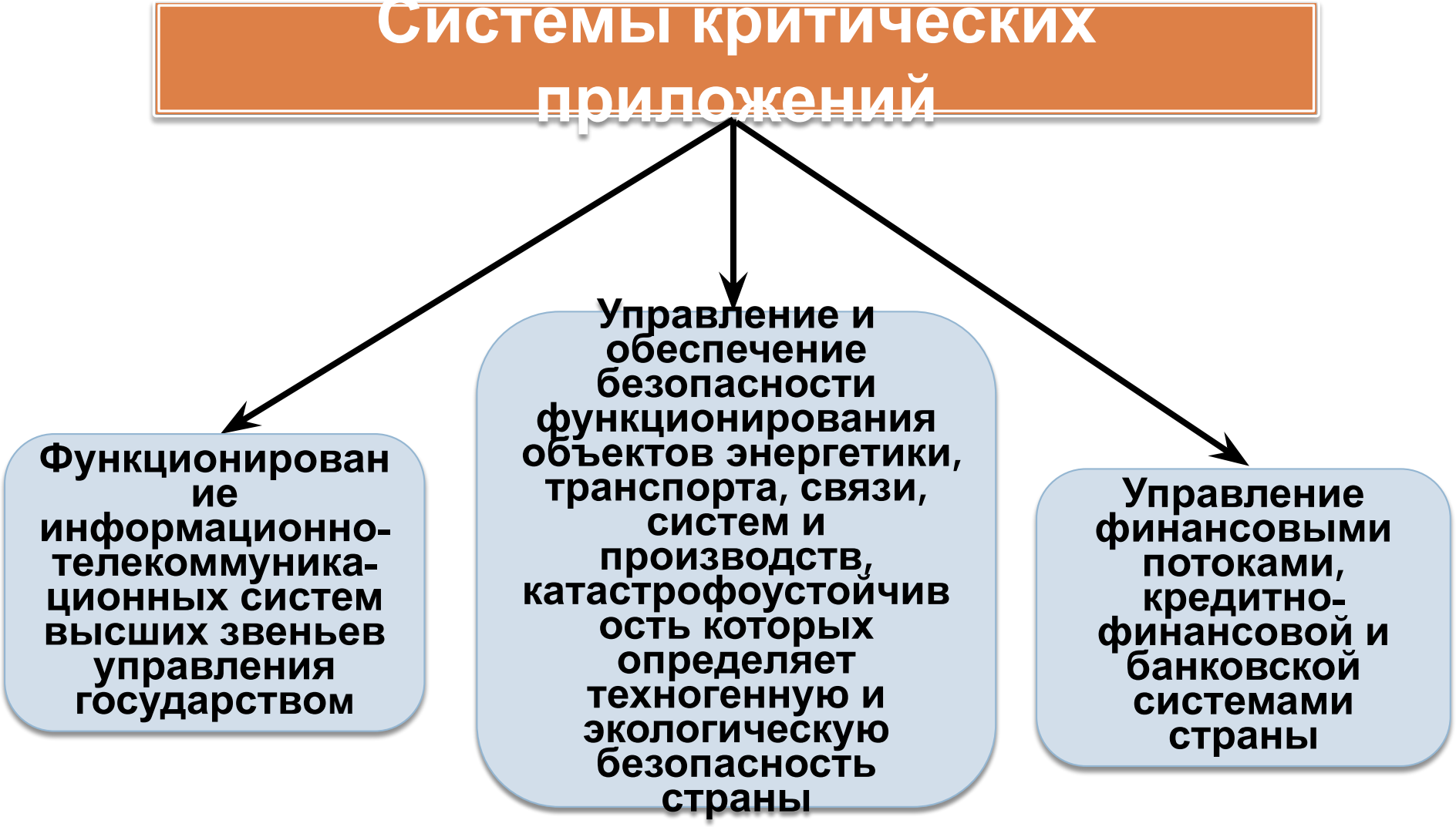
Формирование новой сферы деятельности и области знания «*ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*»

Доктрина информационной безопасности Российской Федерации

Национальные интересы в информационной сфере

«Содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на укрепление равноправного стратегического партнерства в области информационной безопасности, а также на защиту суверенитета Российской Федерации в информационном пространстве»

Формирование новой сферы деятельности и области знания «*ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*»



Формирование новой сферы деятельности и области знания «*ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*»

Определение

Безопасность информации – состояние защищенности информации, хранимой и обрабатываемой в автоматизированной системе, от негативного воздействия на нее с точки зрения нарушения ее физической и логической целостности (уничтожения, искажения) или несанкционированного использования

Формирование новой сферы деятельности и области знания «*ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*»

Определения

Уязвимость информации – возможность возникновения на каком-либо этапе жизненного цикла автоматизированной системы такого ее состояния, при котором создаются условия для реализации угроз безопасности информации

Формирование новой сферы деятельности и области знания «*ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*»

Определения

Защищенность информации – степень поддержания на заданном уровне тех параметров находящейся в автоматизированной системе информации, которые характеризуют установленный статус ее хранения, обработки и использования

Формирование новой сферы деятельности и области знания «*ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*»

Определения

Защита информации **– процесс создания и использования в автоматизированных системах специальных механизмов, поддерживающих установленный статус защищенности информации**

Формирование новой сферы деятельности и области знания «*ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*»

Определение

Комплексная защита информации **–**

целенаправленное регулярное применение в автоматизированных системах средств и методов, а также осуществление мероприятий с целью поддержания заданного уровня защищенности информации по всей совокупности показателей и условий, являющихся существенно значимыми с точки зрения обеспечения безопасности информации

Формирование новой сферы деятельности и области знания «*ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*»

Определение

<u>Автоматизированная система</u> **–**

организованная совокупность средств, методов и мероприятий, используемых для регулярной обработки информации в процессе решения определенного круга прикладных задач

Формирование новой сферы деятельности и области знания «*ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*»

Определение

Изначально защищенная информационная технология – информационная технология, которая, с одной стороны, является унифицированной в широком спектре функциональных приложений, а с другой, – изначально содержит все необходимые механизмы для обеспечения требуемого уровня защиты как основного показателя качества информации

Формирование новой сферы деятельности и области знания «*ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*»

Определения

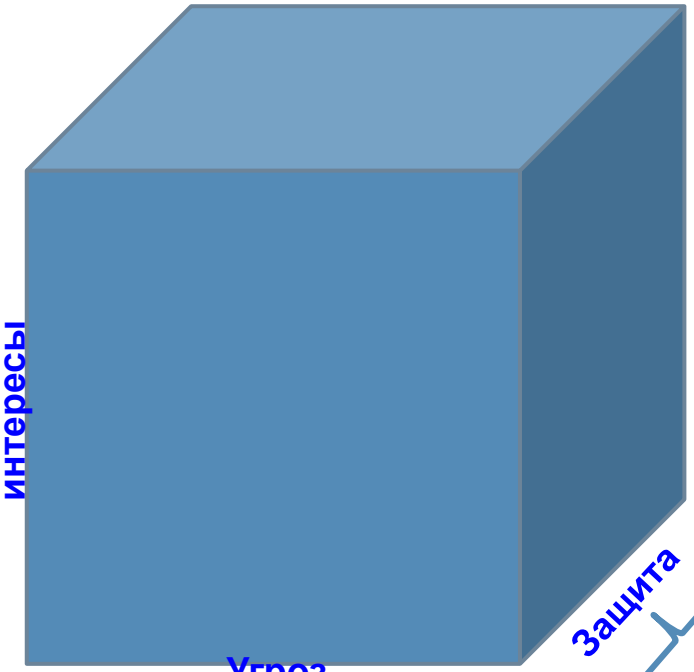
Качество информации **– совокупность свойств, обуславливающих способность информации удовлетворять определенные потребности в соответствии с ее назначением**

Формирование новой сферы деятельности и области знания «*ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*»

Предметная область

- Конституционный строй
- Территориальная целостность
- Суверенитет
- Материальные ценности
- Духовные ценности
- Права
- Свободы

Жизненно важные интересы



Защита

- Устрашение
- Принуждение
- Противодействие
- Соглашение
- Контроль

Угрозы

- Военная
- Экономическая
- Экологическая
- Информационная
- Генетическая
- Социальная
- Интеллектуальная
- Технологическая

Формирование новой сферы деятельности и области знания «*ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*»

Предметная область

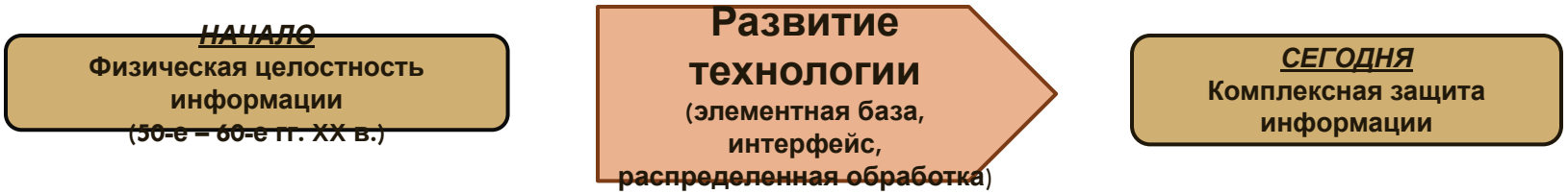
Сечение куба, соответствующее информационным угрозам

Содержание

1. История и современные проблемы информационной безопасности
2. Уязвимость информации
3. Защита информации от несанкционированного доступа
4. Криптографические методы защиты информации
5. Программы-вирусы
6. Защита информации от утечки по техническим каналам
7. Организационно-правовое обеспечение защиты информации
8. Гуманитарные проблемы информационной безопасности
9. Политика информационной безопасности (комплексная система защиты)

История и современные проблемы информационной безопасности

Исторический очерк



Этапы развития подходов к защите информации

Постепенный переход к интенсивным способам защиты

Исторический очерк

Примитивный этап

- Разовое включение в состав автоматизированной системы на этапе ее создания несложных механизмов защиты
- Использование формальных (программно-аппаратных) средств защиты
- Включение программных средств защиты в состав общесистемных компонентов (ОС и СУБД)

Исторический очерк

- Существенное расширение средств защиты, особенно неформальных (организационно-правовых)
- Выделение управляющего элемента (ядра безопасности) и назначение специального профессионально подготовленного лица, ответственного за защиту (администратор безопасности – Россия (СССР), офицер

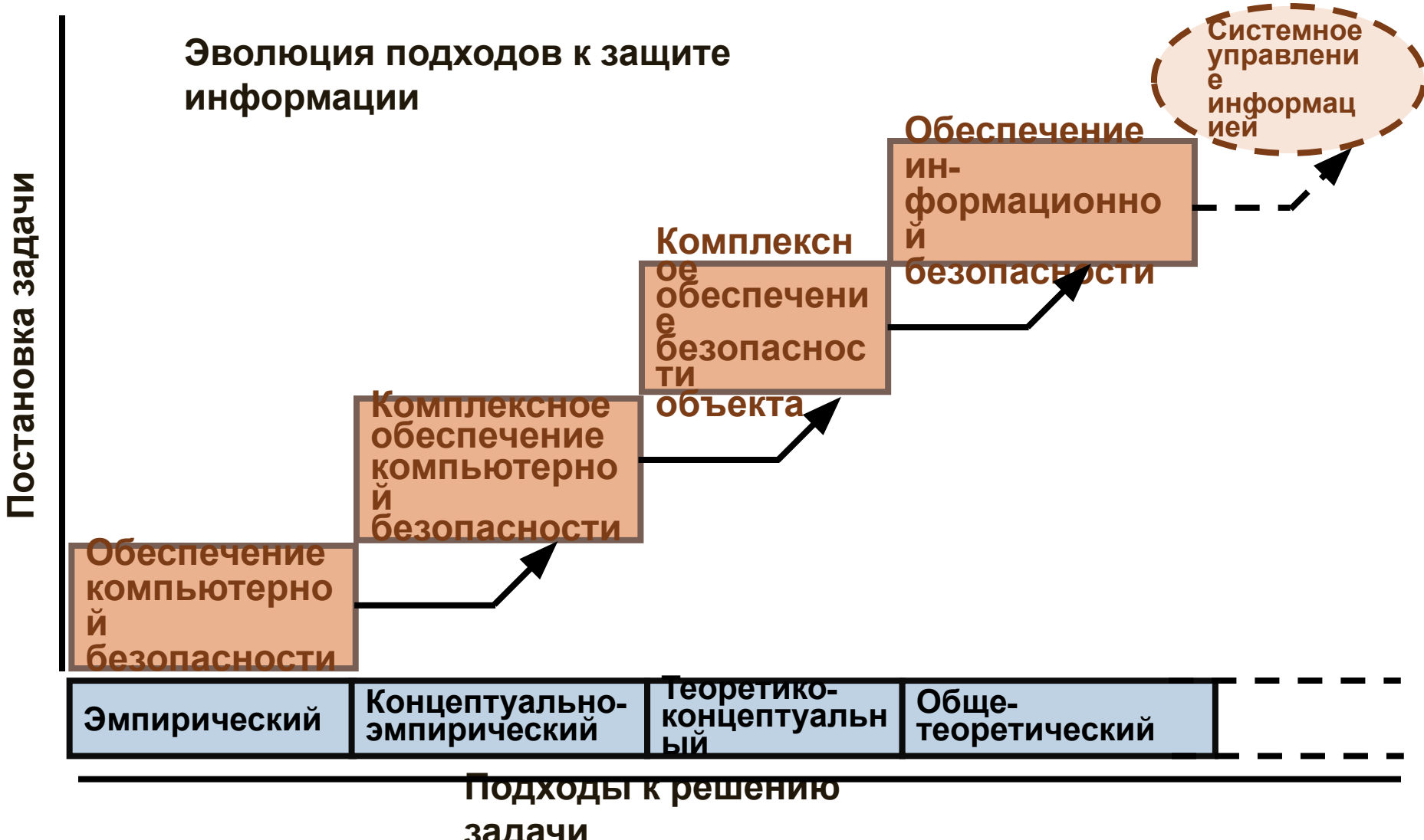
Полусистемный этап

Исторический очерк

Системный этап

- Защита – непрерывный процесс, осуществляемый на всех этапах жизненного цикла автоматизированной системы с помощью комплексного использования всех имеющихся средств защиты
- Основой функционирования средств защиты является созданная нормативно-правовая база

Исторический очерк



Комплексная защита

Тот, кто думает, что может решить проблемы безопасности с помощью технологии, тот не понимает ни проблем безопасности, ни проблем технологии

Брюс Шнайер - президент компании Counterpane Systems

Комплексная защита

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ:
комплексная проблема

Технология

Право

Гуманитарный аспект

Комплексная защита

На систему комплексной защиты возлагается обеспечение:

- **целостности информации**
- **доступности информации**
- **конфиденциальности информации**

Защита от информации

История **Петровны**

Указ Императрицы Елизаветы

(С. Петербургские ведомости, 1750 г., №46)

«Мы с крайним неудовольствием уведомились, что многие как из наших подданных, так и живущих здесь в нашей службе и в нашей протекции иностранцев, разглашая многие лживые ведомости о нынешних статских, политических и воинских делах, присовокупляя к тому развратные толкования и совсем нескладные рассуждения, с столь большею продерзостью, сколь меньшее об оных имеют они сведение и понятие; и для того запотребно рассудили мы чрез сие для известия каждого объявить: что ежели кто отныне, разглашая какие-либо известия или еще и вымышляя оные, о не принадлежащих до него особливо политических и воинских делах превратные толкования и рассуждения делать станет, а нам о том донесется, такой неминуемо всю тягость нашего гнева почувствует»

Защита от информации

Основные проблемы защиты от информации

- обеспечение информационно-психологической безопасности личности и общества
- защита индивидуального, группового и массового сознания общества от деструктивных воздействий средств массовой информации
- противодействие злоупотреблениям свободой распространения информации в сети Интернет
- регулирование использования зарубежными государствами и негосударственными организациями информационных систем других государств для пропаганды политических, религиозных,

Защита от информации

Защита от информации

В основном гуманитарная проблема

Уязвимость информации

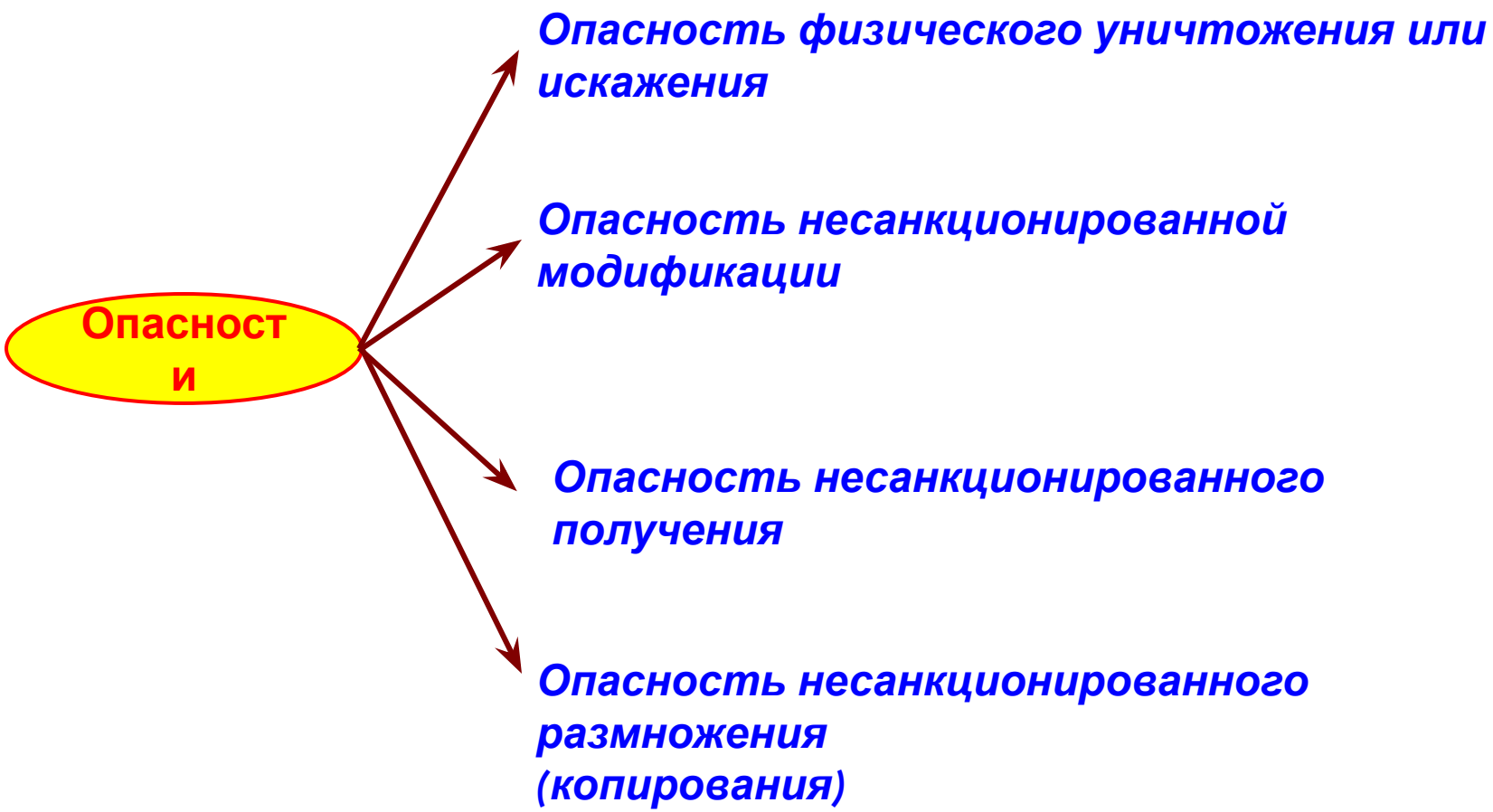
Уязвимость информации

Возможность возникновения на каком-либо этапе жизненного цикла автоматизированной системы такого ее состояния, при котором создаются условия для реализации угроз безопасности информации

Злоумышленник (нарушитель)

Лицо, совершающее несанкционированные действия с целью повышения уязвимости информации

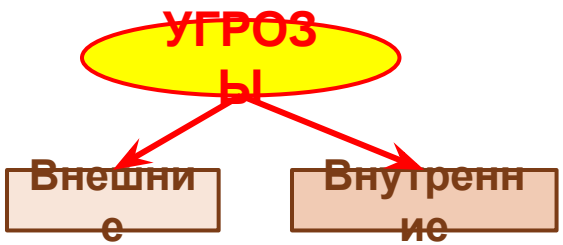
Виды опасностей

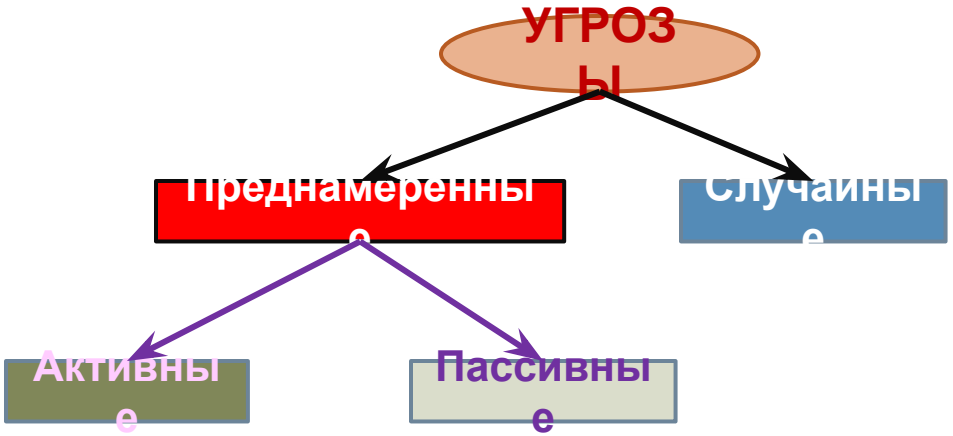


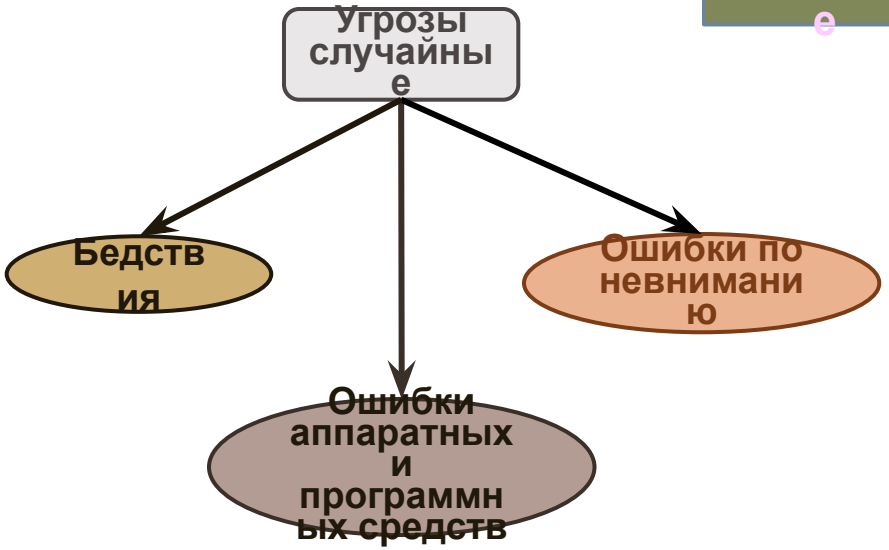
Угрозы безопасности информации

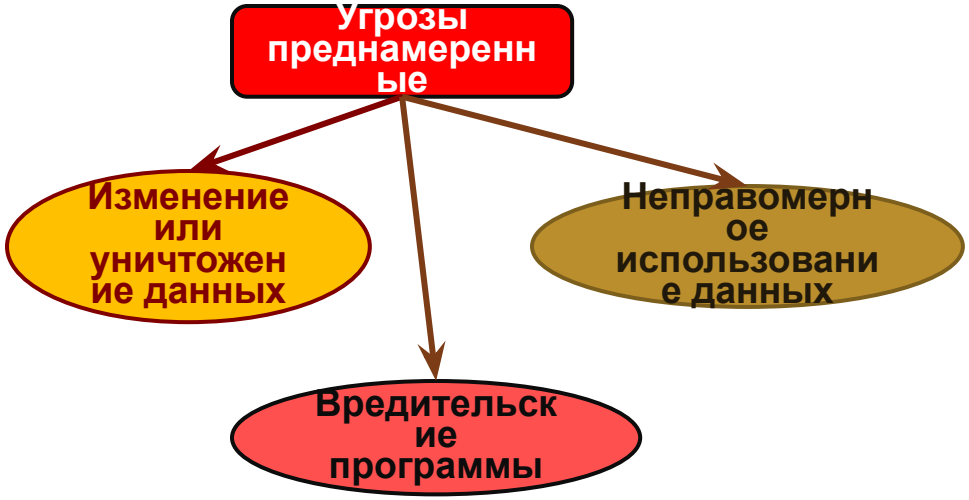
События или действия, которые могут вызвать нарушение функционирования автоматизированной системы, связанное с уничтожением или несанкционированным использованием обрабатываемой в ней информации

Классификация угроз

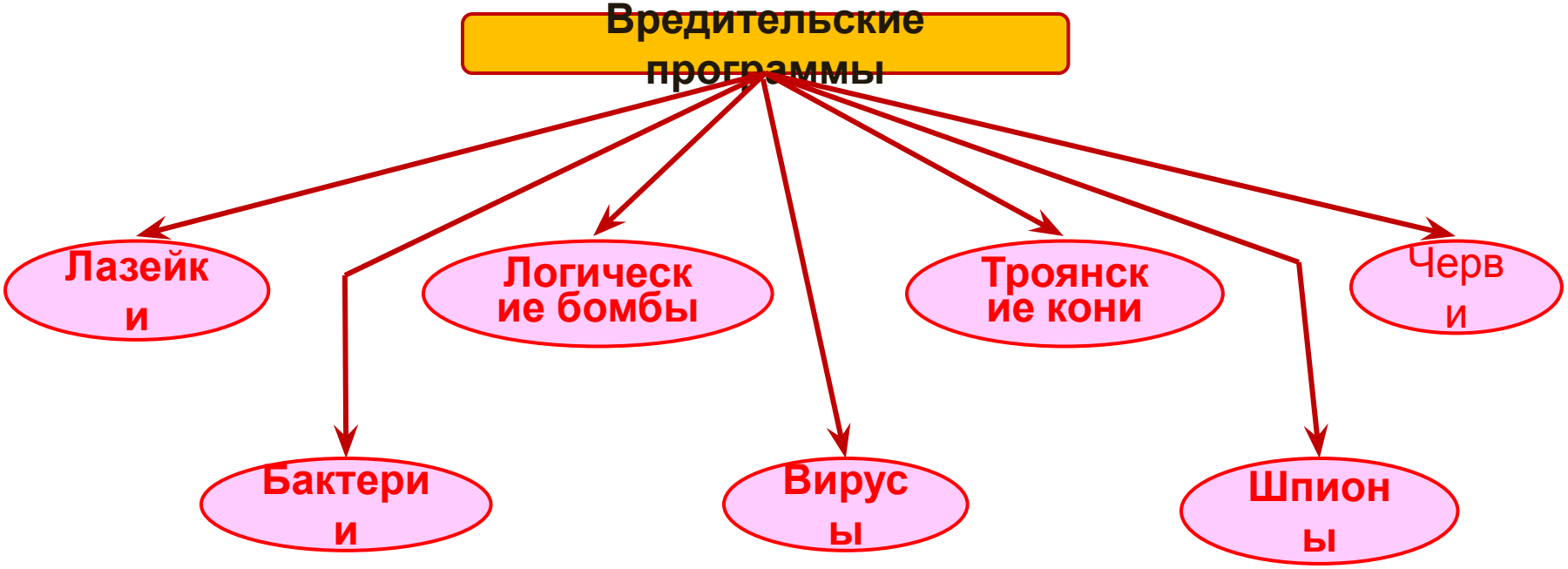








Классификация угроз



Вирус (определение доктора Фредерика Коэна): «Компьютерный вирус
представляет собой программу, которая способна заражать другие
программы, модифицируя их так, чтобы они включали в себя копию вируса

Классификация угроз

Системная классификация угроз

Виды угроз

Нарушение физической целостности

→ **Уничтожение (искажение)**

Нарушение логической структуры

→ **Искажение структуры**

Нарушение содержания

→ **Несанкционированная модификация**

Нарушение конфиденциальности

→ **Несанкционированное получение**

Нарушение права собственности

→ **Присвоение чужого права**

Классификация угроз

Системная классификация угроз

Природа происхождения угроз

Случайная

- → Отказы
- → Сбои
- → Ошибки
- → Стихийные бедствия
- → Побочные влияния

Преднамеренная

- → Злоумышленные действия людей

Классификация угроз

Системная классификация угроз

Предпосылки появления угроз

Объективные

→ **Количественная недостаточность элементов системы**

→ **Качественная недостаточность элементов системы**

Субъективные

→ **Разведорганы иностранных государств**

→ **Промышленный шпионаж**

→ **Уголовные элементы**

→ **Недобросовестные сотрудники**

Классификация угроз

Системная классификация
Источники угроз

Люди
- → Посторонние лица
- → Пользователи
- → Персонал

Технические устройства
- → Регистрации
- → Передачи
- → Хранения
- → Переработки
- → Выдачи

Модели, алгоритмы, программы
- → Общего назначения
- → Прикладные
- → Вспомогательные

Технологические схемы обработки
- → Ручные
- → Интерактивные
- → Внутримашинные
- → Сетевые

Внешняя среда
- → Состояние атмосферы
- → Побочные шумы
- → Побочные сигналы

Классификация угроз

Угрозы информационной безопасности Российской Федерации
(материал Совета Безопасности Российской Федерации)

Информационные угрозы:

- **нарушение адресности и своевременности информационного обмена, противозаконный сбор и использование информации**
- **осуществление несанкционированного доступа к информационным ресурсам и их противоправное использование**
- **манипулирование информацией (дезинформация, сокрытие или искажение информации)**
- **хищение информационных ресурсов из библиотек, архивов, банков и баз данных**
- **нарушение технологии обработки информации**

Классификация угроз

Угрозы информационной безопасности Российской Федерации
(материал Совета Безопасности Российской Федерации)

Программно-математические угрозы:

- **внедрение в аппаратные и программные изделия компонентов, реализующих функции, неописанные в документации на эти изделия**
- **разработка и распространение программ, нарушающих нормальное функционирование информационных систем или их систем защиты информации**

Классификация угроз

Угрозы информационной безопасности Российской Федерации

(материал Совета Безопасности Российской Федерации)

Физические угрозы:

- **уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи**
- **уничтожение, повреждение, разрушение или хищение машинных и других носителей информации**
- **хищение программных или аппаратных ключей и средств криптографической защиты информации**
- **перехват информации в технических каналах связи и телекоммуникационных системах**
- **внедрение электронных устройств перехвата информации в технические средства связи и телекоммуникационные системы, а также в служебные помещения органов государственной власти и других юридических**

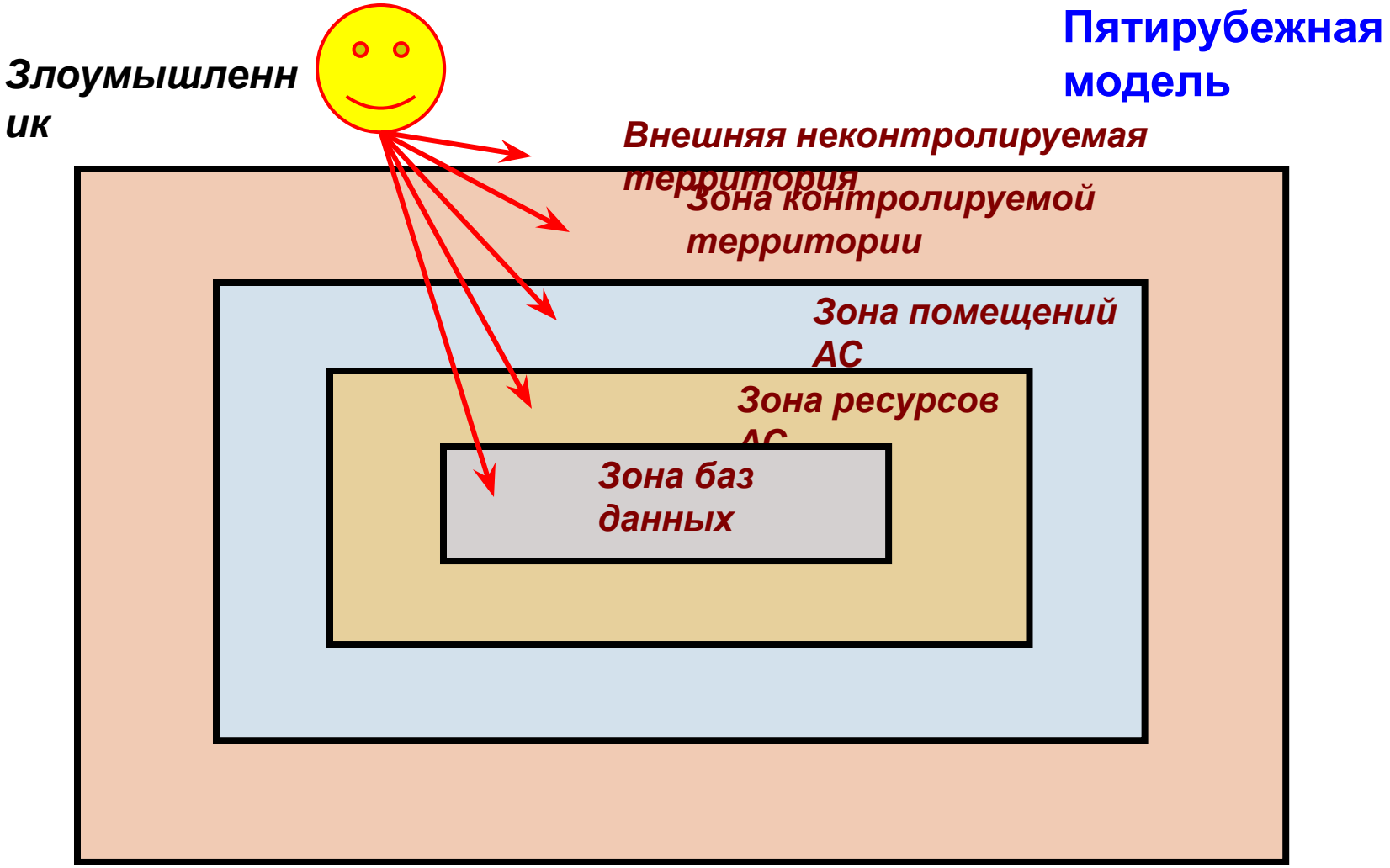
Классификация угроз

Угрозы информационной безопасности Российской Федерации
(материал Совета Безопасности Российской Федерации)

Организационные угрозы:

- **невыполнение требований законодательства в информационной сфере**
- **неправомерное ограничение конституционных прав граждан на информационную деятельность и доступ к открытой информации**
- **противоправная закупка за рубежом несовершенных или устаревших информационных технологий, средств информатизации, телекоммуникации и связи**

Оценка уязвимости информации



Оценка уязвимости информации

Несанкционированный доступ может быть реализован при одновременном наступлении следующих событий:

- **нарушитель получил доступ в соответствующую зону;**
- **в зоне должен проявиться соответствующий канал несанкционированного получения информации;**
- **канал должен быть доступен нарушителю;**
- **в канале должна находиться**

Оценка уязвимости информации

$$P_{jkl} = P_{kl}^{(д)} P_{jl}^{(к)} P_{jkl}^{(н)} P_{jl}^{(и)}$$

P_{jkl} – вероятность несанкционированного получения информации нарушителем k-й категории по j-ому каналу в l-ой зоне;

$P_{kl}^{(д)}$ – вероятность доступа нарушителя k-й категории в l-ую зону;

$P_{jl}^{(к)}$ – вероятность наличия (проявления) j-ого КНПИ в l-ой зоне;

$P_{jkl}^{(н)}$ – вероятность доступа нарушителя k-й категории к j-ому каналу в l-ой зоне;

$P_{jl}^{(и)}$ – вероятность наличия защищаемой информации в j-ом канале в l-ой зоне в момент доступа туда нарушителя.

Понятие информационного риска

Целью применения мер обеспечения безопасности информации является уменьшение риска либо за счет уменьшения вероятности осуществления угрозы, либо за счет уменьшения эффекта воздействия угрозы.

С экономической точки зрения мера защиты оправдана, если эффект от ее применения, выраженный через уменьшение ожидаемого экономического ущерба, превышает затраты на ее реализацию.

Основные характеристики угроз:
вероятность появления и величина ущерба, который они наносят

Понятие информационного риска

Модель оценки риска (IBM)

Вероятность проявления угрозы

Ранг, P	Частота появления	Частота появления в год	Множитель потерь, PL
1	Раз в 300 лет	1/300	0,0033
2	Раз в 30 лет	1/30	0,0333
3	Раз в 3 года	1/3	0,333
4	Раз в 100 дней	365/100	3,65
5	Раз в 10 дней	365/10	36,5
6	Раз в день	365/1	365,0
7	10 раз в день	365/0,1	3650
8	100 раз в день	365/0,01	36500

Понятие информационного риска

Модель оценки риска (IBM)

Размеры ущерба

Условная стоимость (в денежных единицах)	Ранговая константа, Q
0 – 10	1
10 – 100	2
100 – 1 000	3
1 000 – 10 000	4
10 000 – 100 000	5
100 000 – 1 000 000	6
1 000 000 – 10 000 000	7
10 000 000 – 100 000 000	8

Понятие информационного риска

Модель оценки риска (IBM)

Формула определения величины риска:

$$R = \frac{\sqrt{10^{P-3}}}{3^{10^{Q}}}$$

Эффект защиты (уменьшение риска):

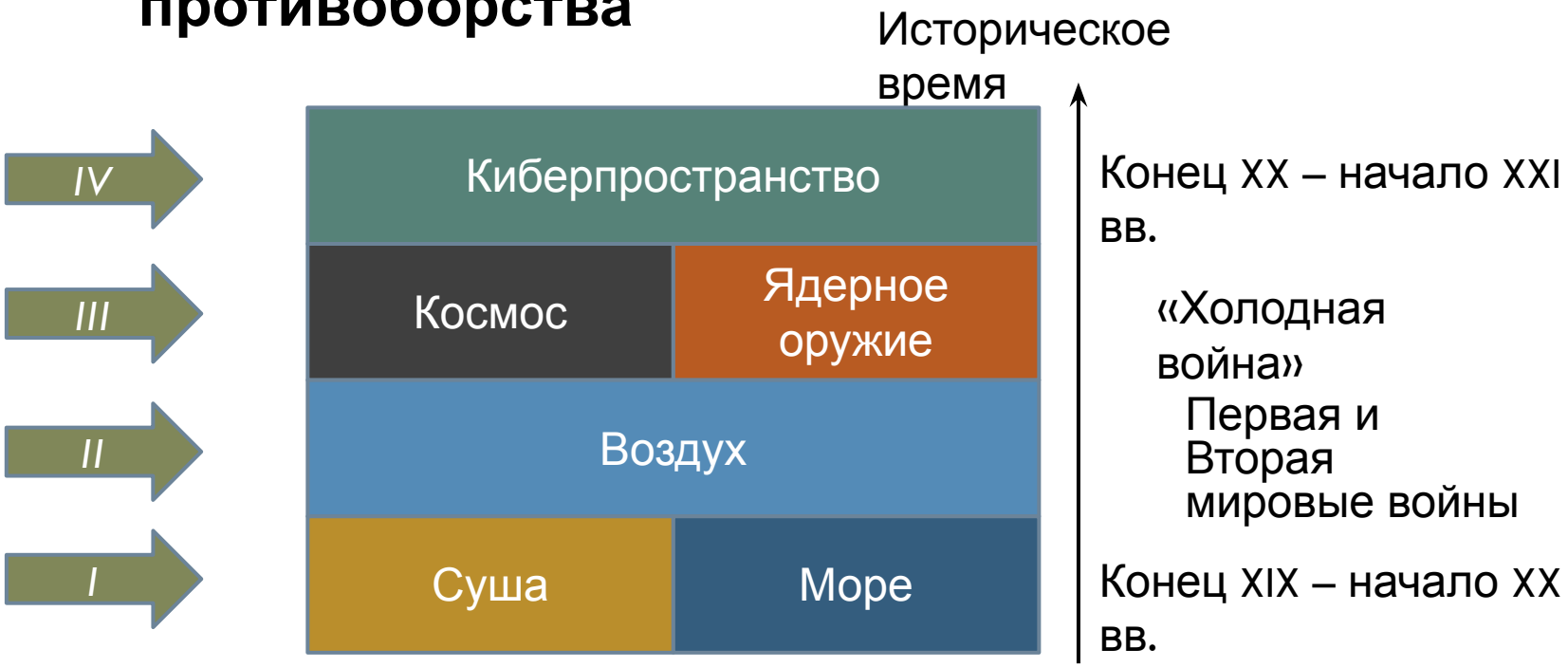
$$\Delta R = R_1 - R_2$$

R_1 – риск без защиты

R_2 – риск с защитой (либо уменьшение вероятности угрозы, либо снижение ущерба)

Информационная война

Пространство военно-силового противоборства



Информационная война

Информационное общество → *Чрезвычайный рост информационной зависимости всех сфер жизнедеятельности общества и государства*

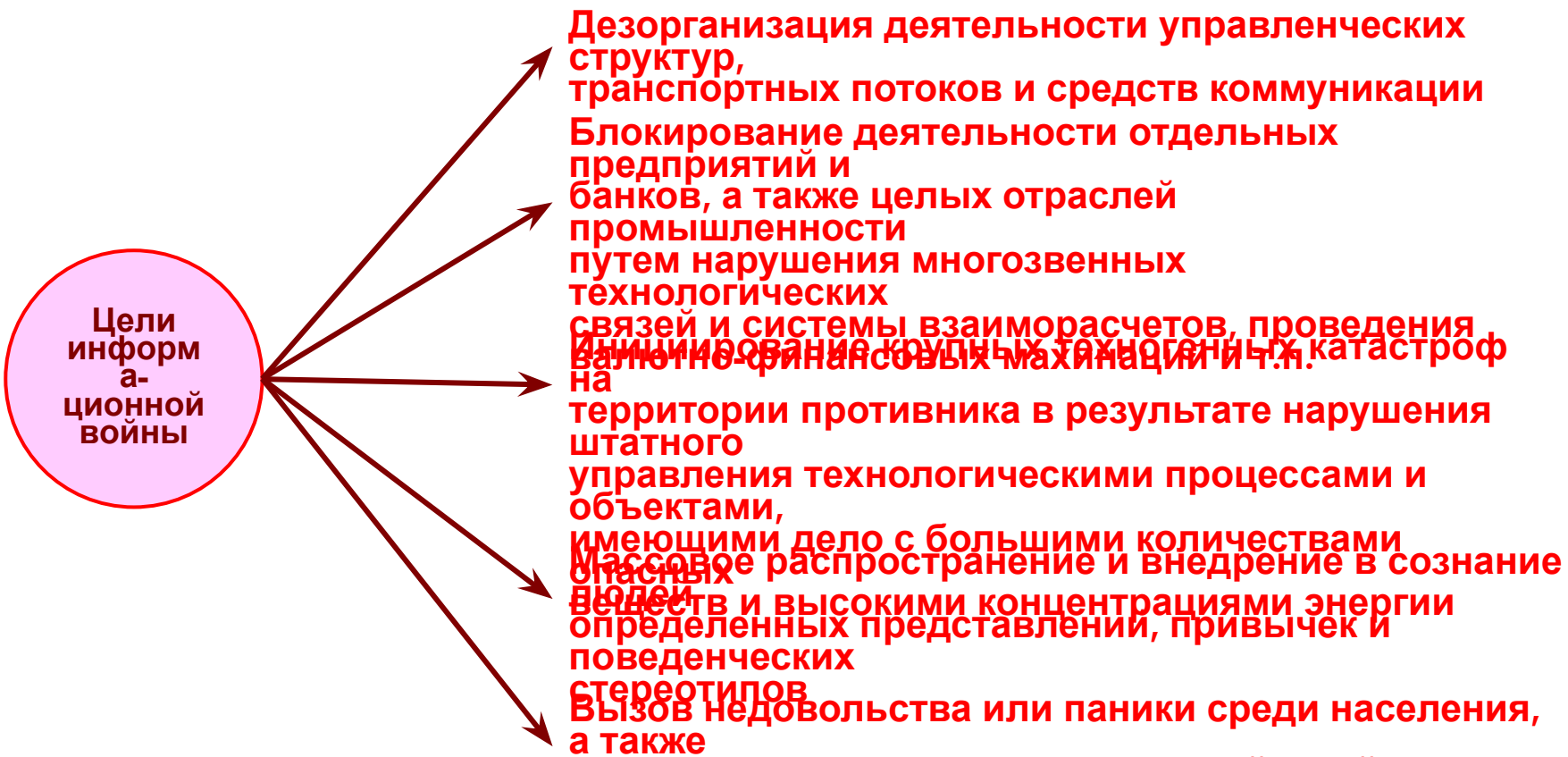
Оценка американских экспертов:

«Нарушение работы компьютерных сетей, используемых в системах управления государственными и банковскими структурами США, путем вывода из строя вычислительных и связных средств или уничтожения хранящейся в сетях информации способно нанести экономике страны настолько серьезный ущерб, что его можно сравнивать с ущербом от применения против США ядерного оружия»

Информационная война

«… Суть информационной войны состоит в достижении какой-либо страной (или группой стран) подавляющего преимущества в информационной области, позволяющего с достаточно высокой степенью достоверности моделировать поведение «противника» и оказывать на него в явной или скрытой форме выгодное для себя влияние. … Страны, проигравшие информационную войну, проигрывают ее «навсегда», поскольку их возможные шаги по изменению ситуации, которые сами по себе требуют колоссальных материальных и интеллектуальных затрат, будут контролироваться и нейтрализовываться победившей стороной. …»

Информационная война



Информационная война

Основные объекты применения информационного оружия

- Компьютерные и связные системы, используемые государственными и правительственными организациями при выполнении своих управленческих функций
- Военная информационная инфраструктура, решающая задачи управления войсками и боевыми средствами, сбора и обработки информации в интересах вооруженных сил
- Информационные и управленческие структуры банков, транспортных и промышленных предприятий
- Средства массовой информации, и в первую очередь электронные (радио, телевидение, Интернет и т.д.)

Информационная война

Возможности США (Министерство обороны)

В видах вооруженных сил введены должности офицеров по информационной войне (infowar officers)

Информационная война

Основные направления исследований в области критических (для создания информационного оружия) технологий

- **Исследование возможности создания принципиально новых вирусов и средств их внедрения в компьютерные системы «противника»**

- **Разработка технологии создания специальных электронных ловушек в микросхемах, которые в качестве элементной базы или в составе систем оружия или систем гражданского назначения поставляются «противнику»**

Информационная война

ВЫВОДЫ

- Ряд стран стремится получить преимущество в создании систем и средств ведения информационной войны, что представляло бы серьезную угрозу национальной безопасности России.
- Создание целостного комплекса средств и методов ведения информационной войны будет осуществляться постепенно, по мере развития в мире базовых информационных технологий, что позволяет осуществлять мониторинг этого процесса.
- Тема информационного оружия и информационной войны, в силу своей чрезвычайной важности для безопасности страны, требует

Задания для самостоятельной работы

1. Были ли в вашей практике случаи попыток несанкционированного получения информации, обрабатываемой в АС? Охарактеризуйте проявившийся в каждом конкретном случае канал несанкционированного доступа и оцените возможную уязвимость информации.

2. Какие вам известны подходы к классификации угроз безопасности информации? Сравните их между собой с точки зрения наибольшего соответствия практическим потребностям создания систем защиты информации.

3. Охарактеризуйте основные принципы системной классификации угроз безопасности информации.

Задания для самостоятельной работы

4. В чем, с вашей точки зрения, состоит опасность разработки и применения информационного оружия? Какие необходимо было бы применить меры международного характера в целях предотвращения информационных войн?

5. Охарактеризуйте процесс развития проблемы защиты информации в современных системах ее обработки.

6. Охарактеризуйте проблему определения предметной области информационной безопасности и дайте определения основным понятиям, используемым в этой сфере.

7. Раскройте содержание исторических этапов развития подходов к защите информации и обеспечению информационной безопасности.

8. Охарактеризуйте «вредительские» программы как один из видов

Защита информации от несанкционированного доступа

Основные принципы защиты от НСД

1 ***Принцип обоснованности доступа***

✔ Пользователь должен иметь достаточную «форму допуска»
для доступа к информации данного уровня конфиденциальности

✔ Пользователю необходим доступ к данной информации
для выполнения его производственных функций

Основные принципы защиты от НСД

2 ***Принцип достаточной глубины контроля доступа***

Средства защиты информации должны включать механизмы

контроля доступа ко *всем* видам информационных и программных ресурсов, которые в соответствии с принципом

обоснованности доступа следует разделять между пользователями

Основные принципы защиты от НСД

3 ***Принцип разграничения потоков информации***

Потоки информации должны разграничиваться в зависимости
от уровня ее конфиденциальности
(для реализации принципа все ресурсы, содержащие конфиденциальную
информацию, должны иметь соответствующие метки, отражающие уровень конфиденциальности)

Основные принципы защиты от НСД

4 ***Принцип чистоты повторно используемых ресурсов***

Должна быть предусмотрена очистка ресурсов, содержащих конфиденциальную информацию, до перераспределения этих ресурсов другим пользователям

Основные принципы защиты от НСД

5 ***Принцип персональной ответственности***

✔ **Индивидуальная идентификация пользователей и инициируемых ими процессов**

(идентификаторы должны содержать сведения о форме допуска пользователя и его прикладной области)

✔ **Проверка подлинности пользователей и их процессов по предъявленному идентификатору (аутентификация)**

✔ **Регистрация (протоколирование) работы механизмов контроля доступа к ресурсам системы с указанием даты и времени, идентификаторов запрашивающего и**

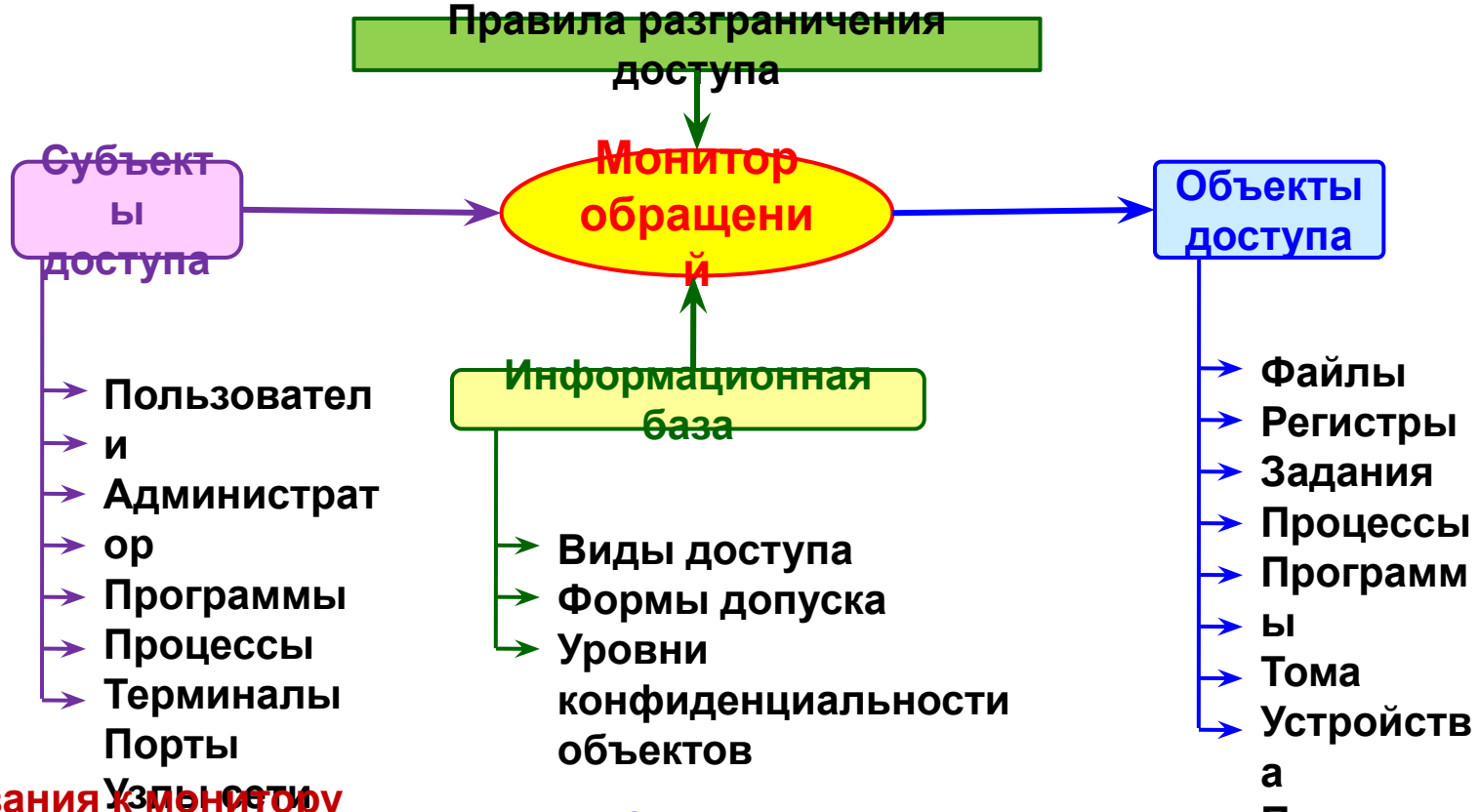
Основные принципы защиты от НСД

6 *Принцип целостности средств защиты*

Система защиты информации должна точно выполнять свои функции в соответствии с основными принципами и быть изолированной от пользователей

(построение средств защиты проводится в рамках отдельного монитора обращений, контролирующего любые запросы на доступ к данным или программам со стороны пользователей)

Монитор обращений



Требования к монитору обращений:

Механизмы контроля

- Защищены от постороннего вмешательства в их работу
- Всегда присутствуют и работают надлежащим образом
- Достаточно малы по своему размеру

Классические модели разграничения доступа

1 Вербальное описание правил разграничения доступа

Модель разграничения доступа защищенной ОС ADEPT-50 (разработана по заказу МО США)

1. **Пользователю разрешен доступ в систему, если он входит в множество известных системе пользователей**
2. **Пользователю разрешен доступ к терминалу, если он входит в подмножество пользователей, закрепленных за данным терминалом**
3. **Пользователю разрешен доступ к файлу, если:**

   а) **уровень конфиденциальности пользователя не ниже уровня конфиденциальности файла;**

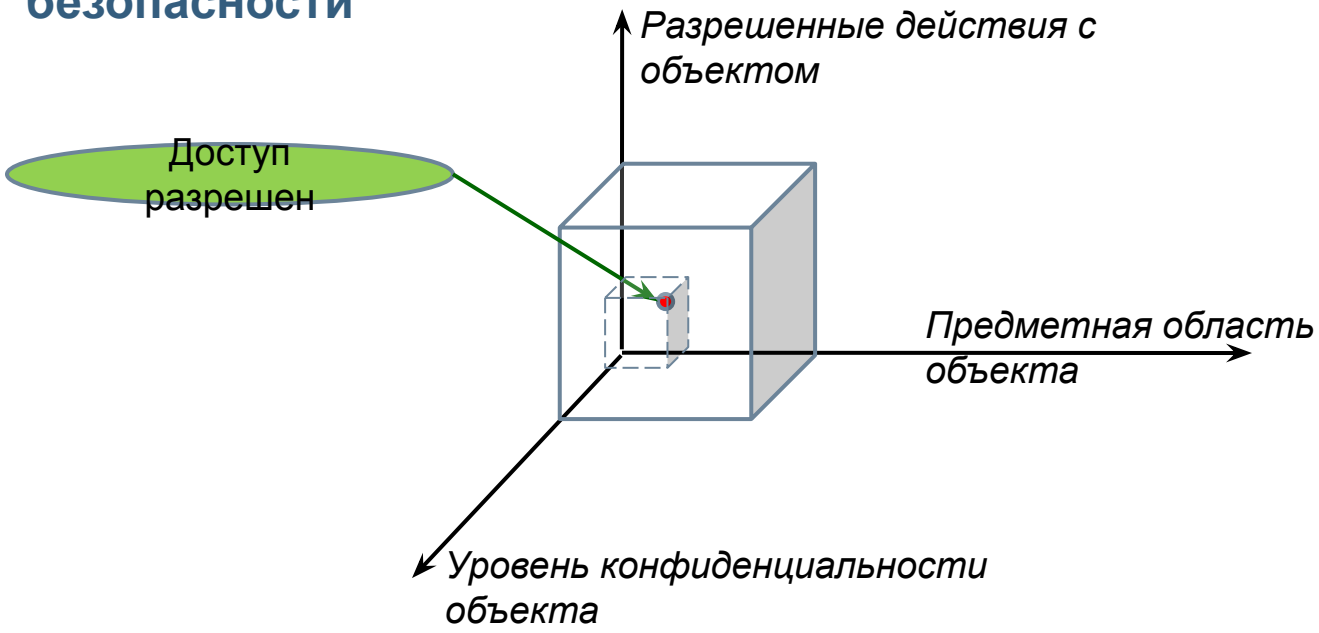
   б) **прикладная область файла включается в прикладную область задания пользователя;**

   в) **режим доступа задания пользователя включает режим доступа к файлу;**

   г) **пользователь входит в подмножество допущенных к файлу**

Классические модели разграничения доступа

2 Построение пространства безопасности



Модель Хартсона (пятимерное пространство безопасности):

- ***установленные полномочия;***
- ***пользователи;***
- ***операции;***
- ***ресурсы;***
- ***состояния***

Классические модели разграничения доступа

3 Модель Лэмпсона – Грэхема – Деннинга (построение матрицы доступа)

Объекты доступа

Субъекты доступа

	O_1	O_2	…	O_n
S_1	T_{11}	T_{12}	…	T_{1n}
S_2	T_{21}	T_{22}	…	T_{2n}
…	…	…	…	…
S_m	T_{m1}	T_{m2}	…	T_{mn}

Элемент T_{ij} определяет привилегии субъекта доступа S_i по отношению к объекту доступа O_i

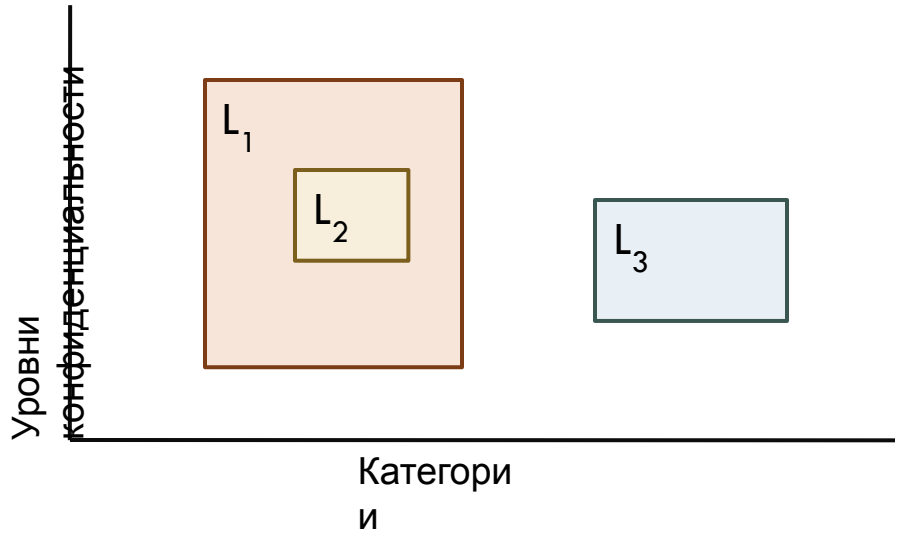
Виды доступа: выполнение, выделение (памяти),
чтение, запись

Когда субъект S_i инициирует доступ вида T_k к объекту O_i, монитор обращений разрешает доступ, если $T_k \le T_{ij}$

Классические модели разграничения доступа

4 Модель Белла – Ла Падула

Объекты и субъекты доступа характеризуются уровнями конфиденциальности
и категориями (предметной областью)



L – уровни безопасности

L_1 доминирует над L_2; L_1 и L_3 (L_2 и L_3) несравнимы

Классические модели разграничения доступа

4 Модель Белла – Ла Падула

Виды доступа

Только чтение → Уровень безопасности субъекта должен доминировать над уровнем безопасности объекта

Только запись → Уровень безопасности объекта должен доминировать над уровнем безопасности субъекта

Чтение и запись → Уровень безопасности объекта должен быть равен уровню безопасности субъекта

Ни чтение, ни запись → Уровни безопасности субъекта и объекта несравнимы

Идентификация и аутентификация пользователей

Определения

Идентификация пользователя – установление и закрепление за каждым пользователем уникального идентификатора в виде номера, шифра, кода и т.д.

Аутентификация пользователя – проверка подлинности

Идентификация и аутентификация пользователей

Аутентификация по типу «Пользователь знает»

Основа – использование парольной системы доступа

Недостаток – многие пароли легко вскрываются или обходятся

Повышение надежности:

- **хранение списков паролей пользователей в зашифрованном виде**
- **использование паролей однократного применения**
- **использование для формирования пароля выборки символов**
- **использование взаимной аутентификации пользователя и системы (процедура «запрос – ответ»)**

Необходимость взаимной аутентификации сетевых процессов подтверждена международным стандартом взаимодействия открытых систем

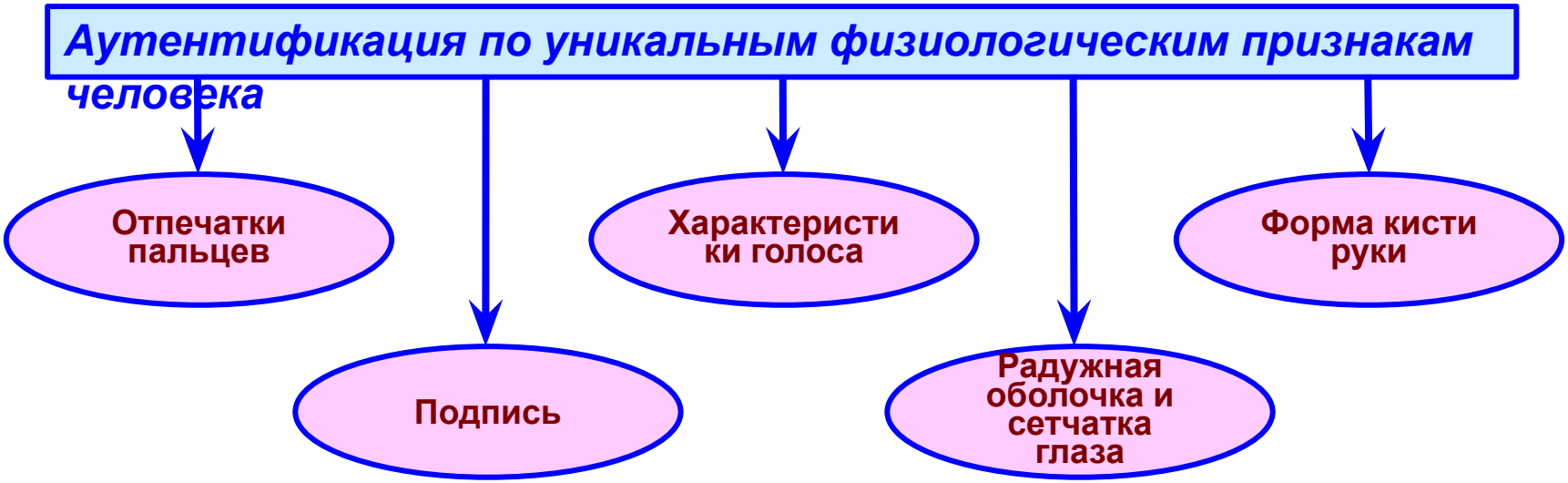
Аутентификация по типу «Пользователь имеет»

В качестве предмета, имеющегося у пользователя, применяются карты идентификации (КИ)

Способы записи и считывания информации с карты (возможна комбинация нескольких способов):

1. Информация записывается на магнитной полосе
2. В КИ встраивается микросхема, содержащая секретный код. Питание схемы и обмен информацией с опознающим устройством осуществляются, как правило, с применением индуктивной связи
3. На поверхность наносится покрытие, позволяющее видеть изображение или текст только в инфракрасном или ультрафиолетовом диапазоне
4. Над текстом или изображением располагают жидкокристаллическую матрицу, прозрачную только при определенной ориентации кристаллов
5. На КИ наносится микротекст или микроузор, который не может быть воспроизведен обыкновенным оборудованием

Аутентификация по типу «Пользователь есть»



Проблема «социальной приемлемости» – процедура опознавания не должна быть слишком хлопотной и занимать много времени, не должна унижать человеческое достоинство и причинять дискомфорт

Аутентификация по типу «Пользователь есть»

Аутентификация по отпечаткам пальцев

1. **Непосредственное сравнение изображений отпечатков пальцев, полученных с помощью оптических устройств, с отпечатками из архива**

2. **Сравнение характерных деталей отпечатка в цифровом виде, которые получают в процессе сканирования изображения отпечатка**

Аутентификация по типу «Пользователь есть»

Аутентификация по подписи

Визуальное сканирование

Анализ динамических характеристик (ускорение, скорость, давление, длительность пауз)

Аутентификация по типу «Пользователь есть»

Аутентификация по характеру голоса

Анализ кратковременных сегментов речи (длительностью до 20 мсек)

Контурный анализ речи

Статистическая оценка голоса (длительность речи около 12 сек)

Аутентификация по типу «Пользователь есть»

Аутентификация по радужной оболочке и сетчатке глаза

Фиксация с помощью специальных видеокамер ряда уникальных характеристик радужной оболочки и сетчатки глаза и сравнение их с данными из архива

Аутентификация по типу «Пользователь есть»

Аутентификация по кисти руки

Анализ ряда характеристик, уникальных для кисти руки каждого человека: длина пальцев, прозрачность кожи, закругленность кончиков пальцев и т.д.

Основные характеристики устройств аутентификации

- Частота ошибочного отрицания законного пользователя
- Частота ошибочного признания постороннего
- Среднее время наработки на отказ
- Число обслуживаемых пользователей
- Стоимость
- Объем информации, циркулирующей между считывающим устройством и блоком сравнения
- Приемлемость со стороны пользователей

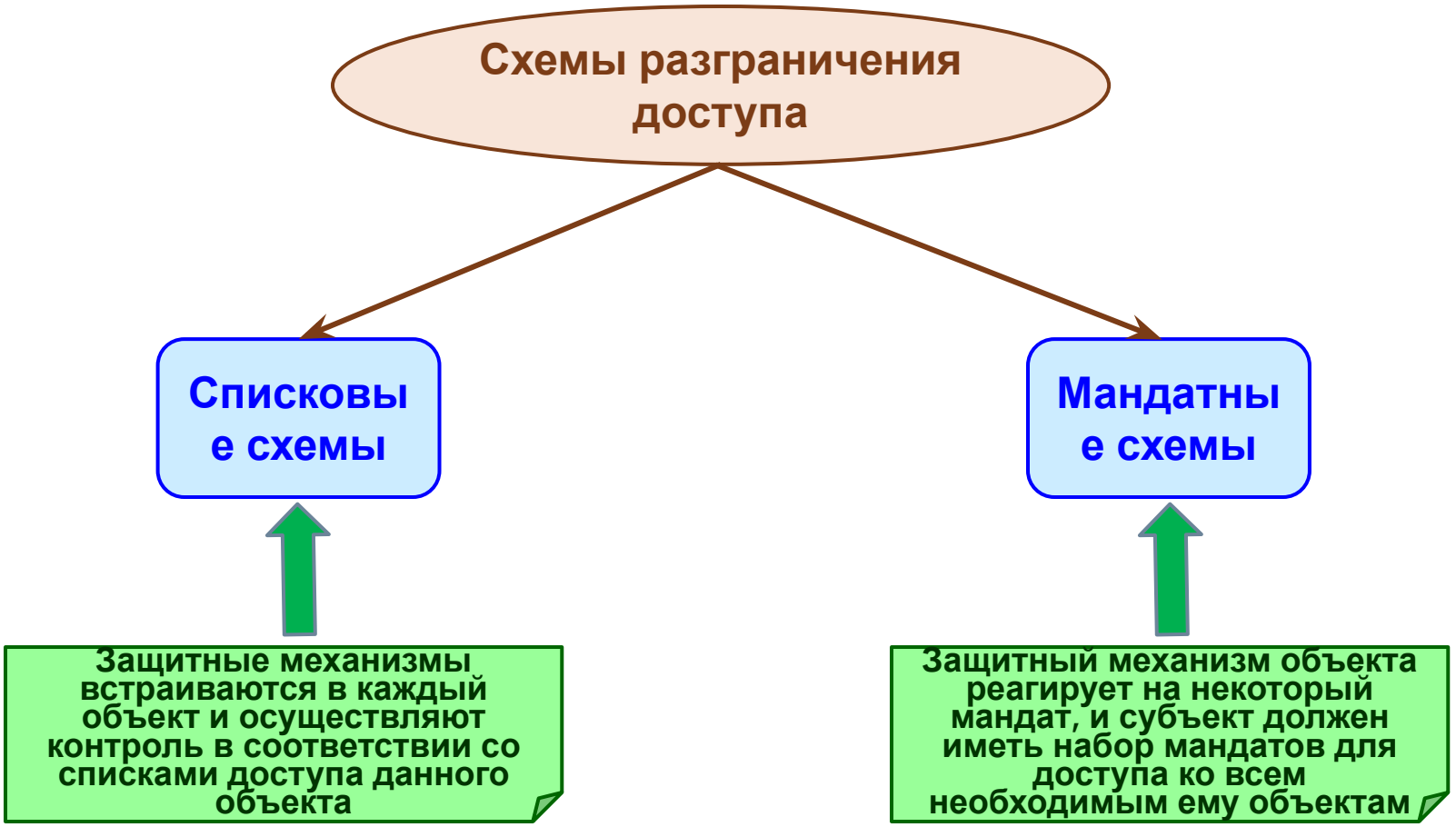
Примечание: 1. Частота ошибочного отрицания обычно несколько превышает частоту ошибочного признания («бей своих, чтобы чужие боялись»)

2. Получение высокой точности аутентификации возможно только при сочетании различных методов

Основные характеристики устройств аутентификации

Методы аутентификации в случае не подтверждения
подлинности должны осуществлять временную
задержку перед обслуживанием следующего запроса на аутентификацию.
Все неуспешные попытки должны

Методы контроля доступа



Методы контроля доступа

Задания для самостоятельной работы

1. Рассмотрите возможности несанкционированного получения информации
   в следующем случае:
   в рассматриваемой АС возможны нарушители двух категорий:
   внешние, не имеющие отношения к системе, и внутренние,
   входящие в состав персонала, обслуживающего АС;
   в качестве компонентов, являющихся объектами несанкционированных действий,
   рассматриваются магнитные носители информации (дискеты),
   видеотерминалы ввода-вывода информации и принтеры;
   каналами несанкционированного получения информации являются
   непосредственное хищение носителей, просмотр информации на экране дисплея
   и выдача ее на печать.
   Каковы, с вашей точки зрения, в этом случае вероятности
   несанкционированного получения информации?

Задания для самостоятельной работы

2. Каковы основные принципы защиты информации от несанкционированного доступа? В чем заключается суть каждого из них?

3. Представьте следующую ситуацию: министры внутренних дел и экономики имеют одинаковую (наивысшую) форму допуска и пытаются с помощью автоматизированной системы получить строго конфиденциальную информацию по вопросу расследования экономических преступлений. Каковы, на ваш взгляд, должны быть возможности их доступа к этой информации? Рассмотрите все возможные ситуации и последствия, к которым приведут принимаемые решения по доступу с точки зрения обеспечения безопасности информации.

Задания для самостоятельной работы

4. Сравните различные известные вам модели защиты от несанкционированного доступа к информации.

5. Что можно сказать о взаимодействии уровней безопасности субъектов и объектов доступа для различных видов доступа, с которыми оперирует модель Белла – Ла Падула?

6. Дайте определения идентификации и аутентификации пользователей. В чем разница между этими понятиями?

7. Назовите основные способы аутентификации. Какой из этих способов является, по-вашему, наиболее эффективным?

8. Приведите примеры известных вам систем аутентификации, построенных по принципу «пользователь имеет».

Задания для самостоятельной работы

9. Что вы можете сказать о преимуществах и недостатках методов аутентификации пользователей пластиковых карт, широко используемых в банковской сфере?

10. Каковы основные характеристики устройств аутентификации? Сравните известные вам устройства по каждой из этих характеристик.

11. Какие основные методы контроля доступа используются в современных автоматизированных системах? Охарактеризуйте эти методы и рассмотрите их возможности для реализации автоматизированной системы ведения текущих счетов клиентов банка.

12. Раскройте содержание разграничения доступа к информации с помощью монитора обращений.

Задания для самостоятельной работы

14. Раскройте содержание принципов обоснованности доступа и персональной
ответственности как основных
принципов защиты от несанкционированного доступа.

15. В чем состоит суть принципов достаточной глубины контроля и разграничения
потоков информации как основных принципов защиты
информации от несанкционированного доступа?

16. Раскройте содержание принципов чистоты повторно используемых ресурсов и
целостности средств защиты как основных принципов
защиты информации от несанкционированного доступа.

17. Раскройте основные особенности известных вам методов аутентификации
с использованием
индивидуальных физиологических характеристик пользователей.

Тестовый контроль 1

1. В чем заключается смысл интенсификации процессов защиты информации?

1) Ускорение решения задач защиты информации.
2) Использование наступательной стратегии защиты информации.
3) Организация защиты информации на основе использования аппаратных и программных средств.
4) Обеспечение комплексной защиты информации с опорой на научно обоснованные прогнозы возможных проявлений дестабилизирующих факторов.

Ответ: 4

2. Какой из приведенных ниже способов аутентификации является наиболее надежным?

1) Аутентификация по предъявленному паролю.
2) Аутентификация по пластиковой карте.
3) Аутентификация по геометрии руки.
4) Аутентификация по подписи.

Ответ: 3

Тестовый контроль 1

3. Какой из основных принципов защиты информации от несанкционированного доступа
требует наличия у пользователя определенной формы допуска?

1) Принцип обоснованности доступа.
2) Принцип достаточной глубины контроля доступа.
3) Принцип разграничения потоков информации.
4) Принцип чистоты повторно используемых ресурсов.
5) Принцип персональной ответственности.
6) Принцип целостности средств защиты.

Ответ:
1

4. Реализация принципа чистоты повторно используемых ресурсов предполагает:

1) Очистку ресурсов, содержащих конфиденциальную информацию, в конце рабочего дня.
2) Очистку ресурсов, содержащих конфиденциальную информацию, после окончания сеанса
связи с пользователем.
3) Очистку ресурсов, содержащих конфиденциальную информацию, до их перераспределения другим пользователя.;
4) Очистку ресурсов, содержащих конфиденциальную информацию, при их

Ответ:
3

Тестовый контроль 1

5. Защита информации – это:

1) Состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере.
2) Состояние защищенности жизненно важных интересов личности, общества и государства от внешних и внутренних информационных угроз.
3) Обеспечение защищенности информации, обрабатываемой в автоматизированной системе, от внешних и внутренних угроз.
4) Состояние защищенности информации, обрабатываемой в автоматизированной системе, от внешних и внутренних угроз.

Ответ: 3

Тестовый контроль 1

6. Какие из перечисленных вредительских программ относятся к классу саморепродуцирующихся?

1) «Логические бомбы».
2) «Троянские кони».
3) «Лазейки».
4) «Вирусы».
5) «Бактерии».
6) «Черви».
7) «Шпионы».

Ответ:
4

Тестовый контроль 1

7. Какую роль играет PIN-код, используемый в банковской пластиковой карте?

1) Персональный номер пользователя.
2) Пароль в системе аутентификации.
3) Ключ к расшифровке личного счета пользователя.

Ответ: 2

8. Представьте следующую ситуацию: министры внутренних дел и экономики имеют одинаковую (наивысшую) форму допуска и пытаются с помощью автоматизированной системы получить строго конфиденциальную информацию по вопросу расследования экономических преступлений. Какой из основных принципов защиты информации от несанкционированного доступа должен быть положен в основу принятия решения в данной ситуации?

1) Принцип обоснованности доступа.
2) Принцип достаточной глубины контроля доступа.
3) Принцип разграничения потоков информации.

Ответ:

Тестовый контроль 1

**9. Выполнение каких условий из перечисленных ниже обеспечивает реализацию принципа
целостности средств защиты?**

1) Система защиты информации должна точно выполнять свои функции.
2) Система защиты информации должна содержать средства идентификации и аутентификации пользователей.
3) Система защиты информации должна быть изолированной от пользователей.
4) Система защиты информации не должна существенно влиять на время реализации
прикладных программ пользователей.
5) Система защиты информации должна позволять осуществлять контроль эффективности
защиты.

Ответ: 1,3.

Тестовый контроль 1

10. Безопасность информации – это:

1) Состояние защищенности жизненно важных интересов личности, общества и государства
в информационной сфере.
2) Состояние защищенности жизненно важных интересов личности, общества и государства от
внешних и внутренних информационных угроз.
3) Обеспечение защищенности информации, обрабатываемой в автоматизированной системе,
от внешних и внутренних угроз.
4) Состояние защищенности информации, обрабатываемой в автоматизированной системе,
от внешних и внутренних угроз.
5) Обеспечение защищенности жизненно важных интересов личности, общества и государства
в информационной сфере.

Ответ: 4

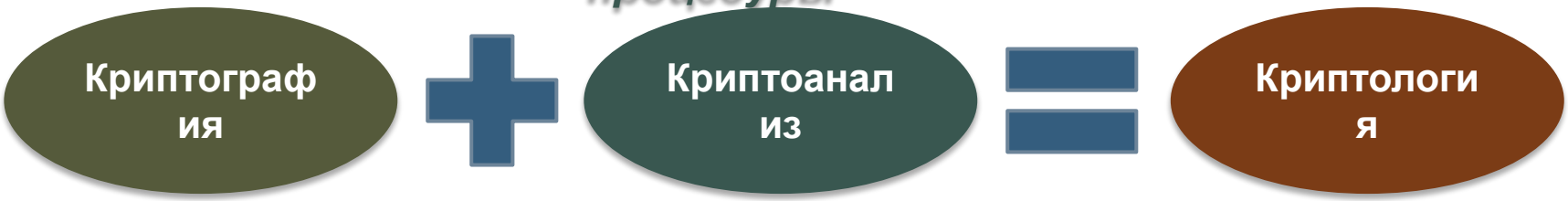
Криптографические методы защиты информации

Общие сведения

Основная цель ››› ***Преобразование информации в форму, непонятную для постороннего***

Криптография → ***Научная дисциплина, изучающая способы обеспечения конфиденциальности информации при передаче ее по незащищенным каналам***

Криптоанализ → ***Научная дисциплина, изучающая способы восстановления исходной информации из преобразованной с помощью криптографической процедуры***



Общие сведения

Стеганография → ***Сокрытие самого факта передачи сообщения***

Общие сведения

СТЕГАНОГРА
ФИЯ

Оплаченный левыми протест ошибочно лишен гневной огласки. Воровство и откаты урадываются сражу. Нужно оживить работу Лены Столыпиной и устроит Ляшенко очную смену. Баржа пришвартуется – стоп удово.
Чао.

Если выписать вторую букву каждого слова, получится:
«Першина отаружается 4 марта»

Общие сведения

Классификация стеганографии:

- Классическая стеганограф
- Компьютерная стеганограс
- Цифровая стеганография

Общие сведения

Классическая стеганография

Симпатические чернила.

Одним из наиболее распространенных методов классической стеганографии является использование симпатических (невидимых) чернил. Текст, записанный такими чернилами, проявляется только при определенных условиях (нагрев, освещение, химический проявитель и т. д.)

Другие стенографические методы

- микроточки

- запись на боковой стороне колоды карт, расположенных в условленном порядке;

- запись внутри варёного яйца;

- «жаргонные шифры», где слова имеют другое обусловленное значение;

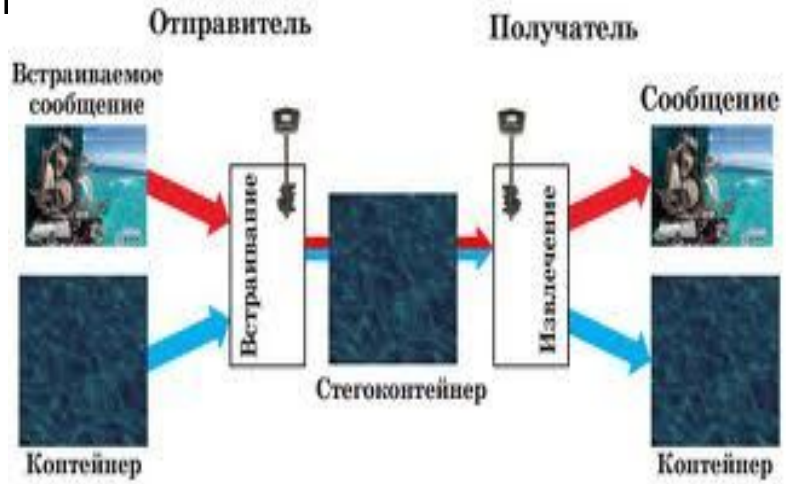
- трафареты, которые, будучи положенными на текст, оставляют видимыми только значащие буквы;

- узелки на нитках и т. д.

Общие сведения

Компьютерная стеганография

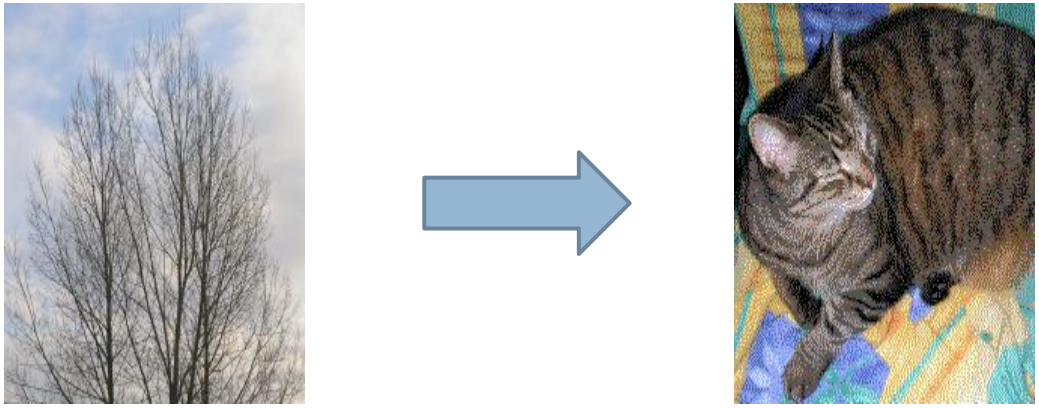
Компьютерная стеганография — направление классической стеганографии, основанное на особенностях компьютерной платформы. Примеры — стеганографическая файловая система StegFS для Linux, скрытие данных в неиспользуемых областях форматов файлов, подмена символов в назв[illegible]ографии и т. д.



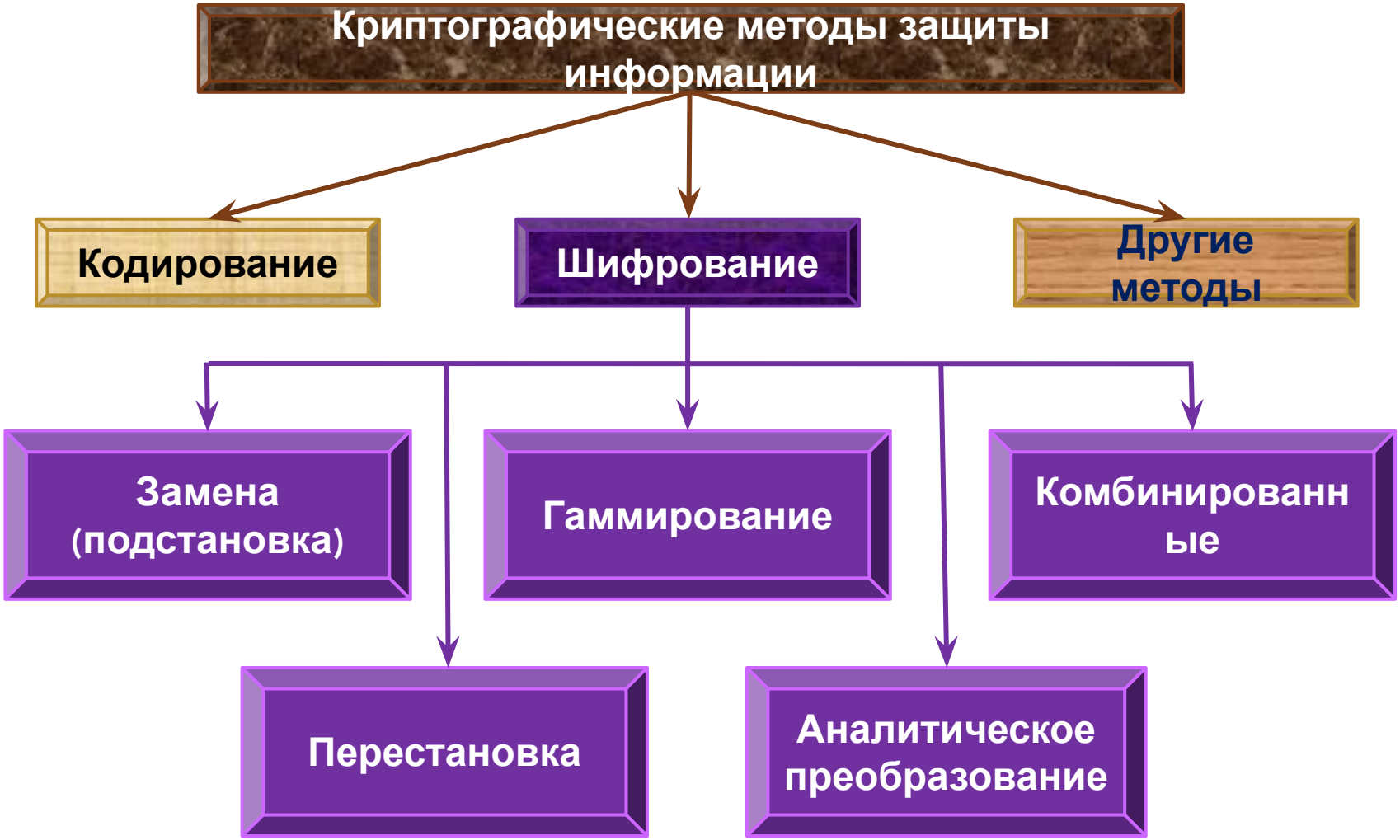
Общие сведения

Цифровая стеганография

Цифровая стеганография — направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов. Обычно данные объекты являются мультимедиа-объектами и внесение искажений, которые находятся ниже порога чувствительности среднестатистического человека, не приводит к заметным изменениям этих объектов.



Общие сведения



Общие сведения

Кодирование

Использование системы условных обозначений элементов информации (кодов)

✔ **Кодирование проводится с помощью специальных кодовых таблиц, которые должны быть у всех участников информационного обмена.**

✔ **Кодирование используется в системах военной, разведывательной и дипломатической связи**

Общие сведения

Шифрование

Преобразование исходного сообщения с помощью специальной процедуры (с использованием ключа)

Симметричные системы шифрования → **Для шифрования и расшифрования используются одинаковые ключи**

Несимметричные системы шифрования → **Для шифрования и расшифрования используются разные ключи**

Шифрование + Расшифрование = Криптосистема

Общие сведения

Шифрование

Симметричная система

Отправитель

Исходный код:
10110

Шифрование

Замена: **01001**

Перестановка:
11000

Получатель

Полученное сообщение:
11000

Расшифрование

Замена:
00111

Перестановка:

10110 = 10110

Несимметричная система

Отправитель

Исходный код: 10110

Шифрование

Замена: **01001**

Серия перестановок: 10001 – 10001 – 10001 – 10010

Получатель (незаконный)

Полученное сообщение: 10010

Расшифрование

Замена: **01101**

Серия перестановок: 10101 – 11001 – 11001 – 11010

Результат: 11010

11010 ≠ 10110

Общие сведения

Другие методы криптографической защиты

Использование различных физических принципов для преобразования информации в форму, непонятную для постороннего

Новое направление – квантовая криптография

Защита информации основана на принципе неопределенности и других
законах квантовой физики.
Наиболее эффективно квантовая криптография может быть реализована
в волоконно-оптических линиях связи.

Замена (подстановка)

Идея метода: **один алфавит заменяется другим**

Пример 1

А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я

Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я А Б В Г Д Е

Ключ: *число символов, на которое сдвигается алфавит (- 6)*

Исходная фраза: ***будьте осторожны с представителем фирмы феникс***

Зашифрованная фраза: ***зщкевшл фчшфцфмуб ч хцлкчшжиошлслт ъоцтб ълуорч***

Недостаток: **легко дешифровать с помощью частотного анализа текста**

Замена (подстановка)

Оценки вероятности появления букв русского языка и пробела

А	Б	В	Г	Д	Е,Ё	Ж	З	И	Й	К
0,069	0,013	0,038	0,014	0,024	0,071	0,007	0,016	0,064	0,010	0,029
Л	М	Н	О	П	Р	С	Т	У	Ф	Х
0,039	0,027	0,057	0,094	0,026	0,042	0,046	0,054	0,023	0,003	0,008
Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	пробел
0,005	0,012	0,006	0,004	0,001	0,015	0,013	0,002	0,005	0,017	0,146

Повышение надежности: каждый символ шифруется с помощью нового алфавита

(таблицы Вижинера)

Перестановка

Идея метода: **шифруемый текст разбивается на блоки, которые перемешиваются между собой**

Пример 2

Исходная фраза: ***будьте осторожны с представителем фирмы феникс***

Ключ:
58137462

Шифрование

5	8	1	3	7	4	6	2
Б	У	Д	Ь	Т	Е	@*	О
С	Т	О	Р	О	Ж	Н	Ы
@	С	@	П	Р	Е	Д	С
Т	А	В	И	Т	Е	Л	Е

* - пробел

Зашифрованная фраза:
до@вфноысе@@ьрпииежеемсбс@тмф@ндлы@тортркутса@е

Ф	Е	Н	И	К	С	@

Перестановка

Расшифрование

Зашифрованная фраза:
до@вфноысе@@ьрпииижеемсбс@тмф@ндлы@тортркутса@е

Ключ:
58137462

Зашифрованная фраза разбивается на блоки. Длина каждого блока равна числу символов в сообщении, деленному на длину ключа

до@вфн - оысе@@ - ьрпии - ижеемс - бс@тмф - @ндлы@ - тортрк - утса@е

5	8	1	3	7	4	6	2
Б	У	Д	Ь	Т	Е	@	О
С	Т	О	Р	О	Ж	Н	Ы
@	С	@	П	Р	Е	Д	С
Т	А	В	И	Т	Е	Л	

Расшифрованная фраза: ***будьте осторожны с представителем фирмы феникс***

Гаммирование

***Идея метода*: символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, которая**

Процедура наложения гаммы:

$t_ш = (t_u + t_г)_{mod(k)}$, $t_ш$, t_u , $t_г$ – символы соответственно зашифрованного, исходного текста и гаммы;

k – число символов в алфавите

Гамма – любая последовательность случайных символов, например, последовательность цифр числа π, числа e и т.д.

Пример

Исходная фраза: ***будьте осторожны с … (01010010 10000010 11001011 …)***

Шифрование

	Б	У	Д	
	Ь …			
Гамма →	01010010	10000010	11001011	…
	00000111	00000100	00100000	…
	01010101	10000110	11101011	…

Зашифрованная фраза: ***01010101 10000110 11101011 …***

Гаммирование

Расшифрование – вычитание той же гаммы

Зашифрованная фраза: *01010101 10000110 11101011 …*

Расшифрование

Гамма →

01010101	10000110	11101011	
…			
00000111	00000100	00100000	…
01010010	10000010	11001011	…
… Б	У	Д	
…			

Расшифрованная фраза: *будьте осторожны с … (01010010 10000010 11001011 …)*

Аналитическое преобразование

Идея метода: **использование методов алгебры матриц**

Пример 4

Умножение матрицы на вектор

$| a_{ij} | b_j = \sum a_{ij} b_j = c_i,\ i = 1,2,\ldots;\ | a_{ij} |$ - ***ключ***

Шифрование ***Ключ*** :

$$|a_{ij}| = \begin{vmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{vmatrix}$$

А – 1, Б – 2, В – 3, Г – 4, Д – 5, Е – 6, Ж – 7, З – 8, И – 9, К – 10, Л – 11,
М – 12, Н – 13, О – 14, П – 15, Р – 16, С – 17, Т – 18, У – 19, Ф – 20, Х – 21,
Ц – 30,
Я - 31

Исходная фраза: ***будьте …*** → ***2 19 5 28 18 6***

$$\begin{vmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{vmatrix} \times \begin{vmatrix} 2 \\ 19 \\ 5 \end{vmatrix} = \begin{vmatrix} 28 + 152 + 15 \\ 16 + 95 + 10 \\ 6 + 38 + 5 \end{vmatrix} = \begin{vmatrix} 195 \\ 121 \\ 49 \end{vmatrix}$$

$$\begin{vmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{vmatrix} \times \begin{vmatrix} 28 \\ 18 \\ 6 \end{vmatrix} = \begin{vmatrix} 392 + 144 + 18 \\ 224 + 90 + 12 \\ 84 + 36 + 6 \end{vmatrix} = \begin{vmatrix} 554 \\ 326 \\ 126 \end{vmatrix}$$

Зашифрованная фраза: ***195 121 49 554 326 126 …***

Аналитическое преобразование

Расшифрование

Умножение на обратную матрицу

Правило: обратная матрица образуется из присоединенной делением всех элементов на определитель. Присоединенная матрица составляется из алгебраических дополнений A к элементам данной матрицы.

$$A_{ij} = (-1)^{i+j} D_{ij}, \quad D_{ij} - \textit{определитель матрицы},$$
$$D = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31}$$

Обратная матрица

$$\overline{|a_{ij}|} = \begin{vmatrix} 1 & -2 & 1 \\ -2 & 5 & -4 \\ 1 & -4 & 6 \end{vmatrix}$$

Зашифрованная фраза: *195 121 49 554 326 126 …*

$$\begin{vmatrix} 1 & -2 & 1 \\ & 28 & \\ -2 & 5 & -4 \\ & 504 & \\ 1 & -4 & 6 \\ & 756 & \end{vmatrix} \times \begin{vmatrix} 195 \\ 121 \\ 49 \\ 554 \\ 326 \\ 126 \end{vmatrix} = \begin{vmatrix} 195 - 242 + 49 \\ -390 + 605 - 196 \\ 195 - 484 + 294 \\ 554 - 652 + 126 \\ -1108 + 1630 - \\ 554 - 1304 + \end{vmatrix} = \begin{vmatrix} 2 \\ 19 \\ 5 \\ 28 \\ 18 \\ 6 \end{vmatrix}$$

Расшифрованная фраза: *2 19 5 28 18 6 будьте …*

Комбинированные методы

Идея методов: **комбинирование различных элементарных методов шифрования**

Все реальные алгоритмы используют только комбинированные методы!!!

Пример 5

Алгоритм DES

Наиболее распространенная криптосистема **– стандарт США на шифрование информации DES (Data Encription Standard). Разработан фирмой IBM, длина ключа 64 бита (российский аналог: ГОСТ – 28147 – 89, длина ключа 256 бит)**

Особенность алгоритма DES

Шифруются 64-битовые блоки с применением ключа длиной 64 бита.

Из основного ключа образуются 16 вспомогательных 48-битовых ключей.

Комбинированные методы

Последовательность работы алгоритма DES

Усовершенствованный алгоритм DES: длина ключа 128 бит

Несимметричные системы шифрования

Теоретическая основа **– понятие «односторонней функции с потайной дверью»**

Определение. ***Функция называется односторонней, если легко может быть вычислено значение f(x), но по известному значению функции крайне трудно вычислить x.***

Пример – умножение простых чисел

$$\underbrace{367589023156\ldots}_{100\text{ знаков}} \times \underbrace{64379021345\ldots}_{100\text{ знаков}} = \underbrace{\ldots\ldots\ldots\ldots\ldots}_{200}$$

Разложение на множители 200-значного числа потребует десятков лет непрерывной работы мощной ЭВМ

Для расшифрования односторонняя функция должна иметь как бы «потайную дверь», т.е. способ эффективного вычисления функции в обоих направлениях

Криптографические алгоритмы с общедоступным ключом

Ключи шифрования пользователей известны всем, а ключи расшифрования все пользователи хранят в тайне

Стойкость криптосистемы

Определения

На основе классической теории информации

Криптосистема является стойкой, если у криптоаналитика отсутствует возможность получения необходимого количества информации для восстановления зашифрованного

На основе теории вычислительной сложности

Криптосистема является стойкой, если даже при наличии всей необходимой информации криптоаналитик не может восстановить зашифрованное сообщение в заданный срок из-за большого объема

Вскрытие современных криптоалгоритмов требует от 5 до 20 человеколет

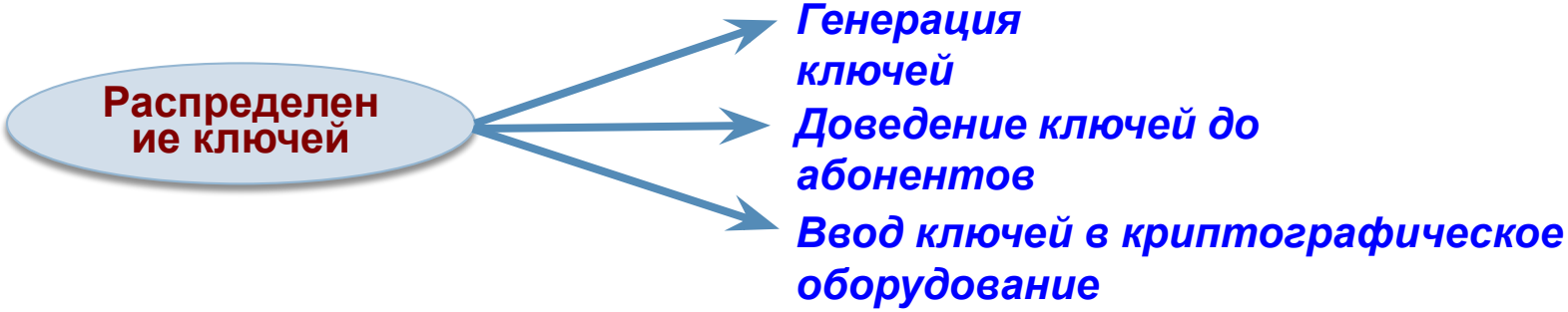
Стойкость криптосистемы

Стойкость криптосистем зависит от следующих основных свойств криптоалгоритмов:

- ***Сложность*** → **Более сложные криптоалгоритмы труднее поддаются дешифрованию**
- ***Симметричность*** → **Несимметричные криптоалгоритмы труднее поддаются дешифрованию**
- ***Длина ключа*** → **Длинные ключи обеспечивают большую стойкость**
- ***Метод реализации*** → **Аппаратный метод реализации обеспечивает большую стойкость по сравнению с программным**

Основное требование к криптосистеме **– наличие очень большого числа возможных ключей, чтобы не допустить восстановления исходного сообщения путем их**

Распределение ключей шифрования



ГЕНЕРАЦИЯ КЛЮЧЕЙ

Распределение ключей шифрования

ДОВЕДЕНИЕ КЛЮЧЕЙ ДО АБОНЕНТОВ

Небольшое число абонентов → **Ключи поставляются потребителям традиционным способом (спецпочтой или курьерской службой) на бумажных или машинных носителях**

Большое число абонентов → **Системы автоматизированного распределения ключей по каналам связи (децентрализованные и централизованные)**

Распределение ключей шифрования

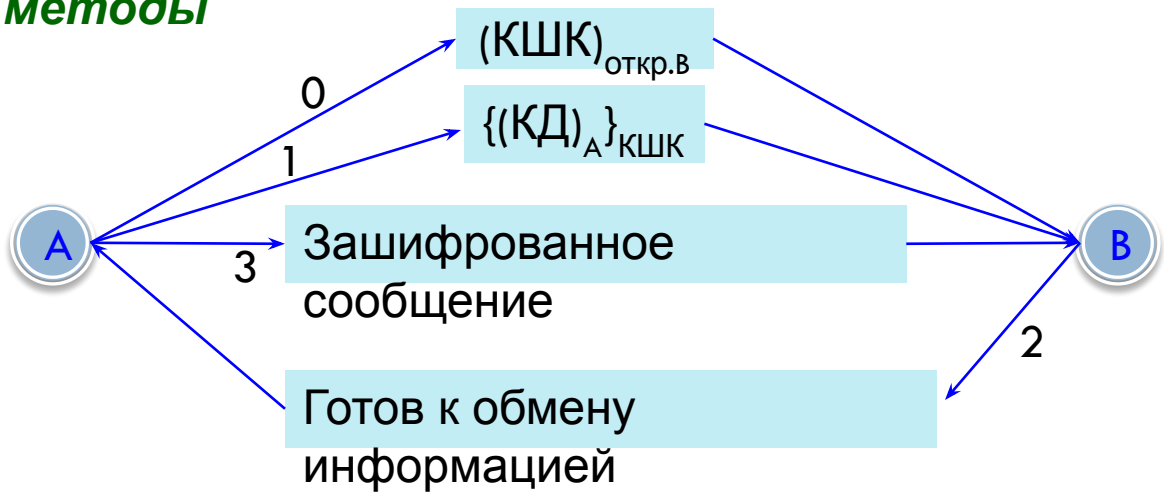
ДОВЕДЕНИЕ КЛЮЧЕЙ ДО АБОНЕНТОВ

Децентрализованные системы → **2 ключа:**

- **ключ данных (КД)**
- **ключ шифрования ключей (КШК)**

Период замены КШК >> периода замены КД

Доведение КШК до абонентов – традиционные методы



Для передачи КШК по каналам связи может использоваться криптосистема
с общедоступным ключом (ОК).
Получается трехключевая система (ОК, КШК,КД)

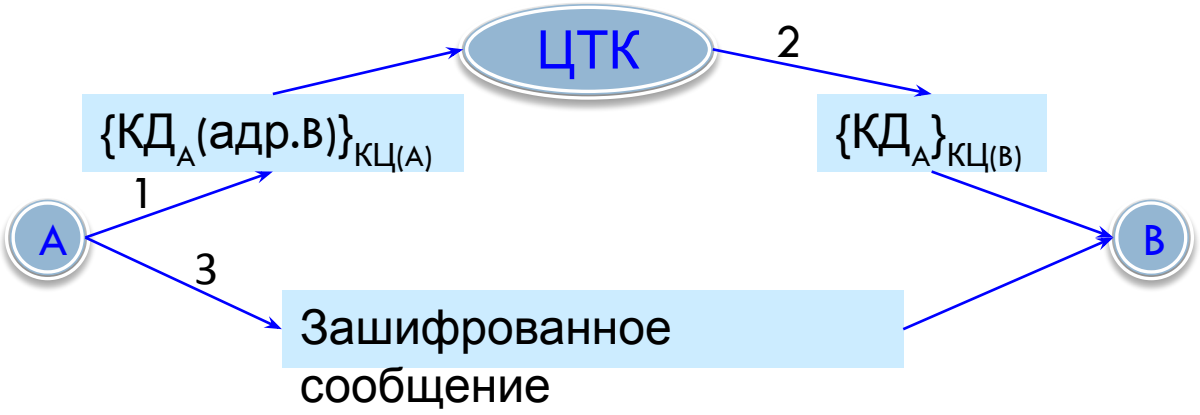
Распределение ключей шифрования

ДОВЕДЕНИЕ КЛЮЧЕЙ ДО АБОНЕНТОВ

Централизованные системы

- ***С центром трансляции ключей (ЦТК)***
- ***С центром распределения ключей (ЦРК)***

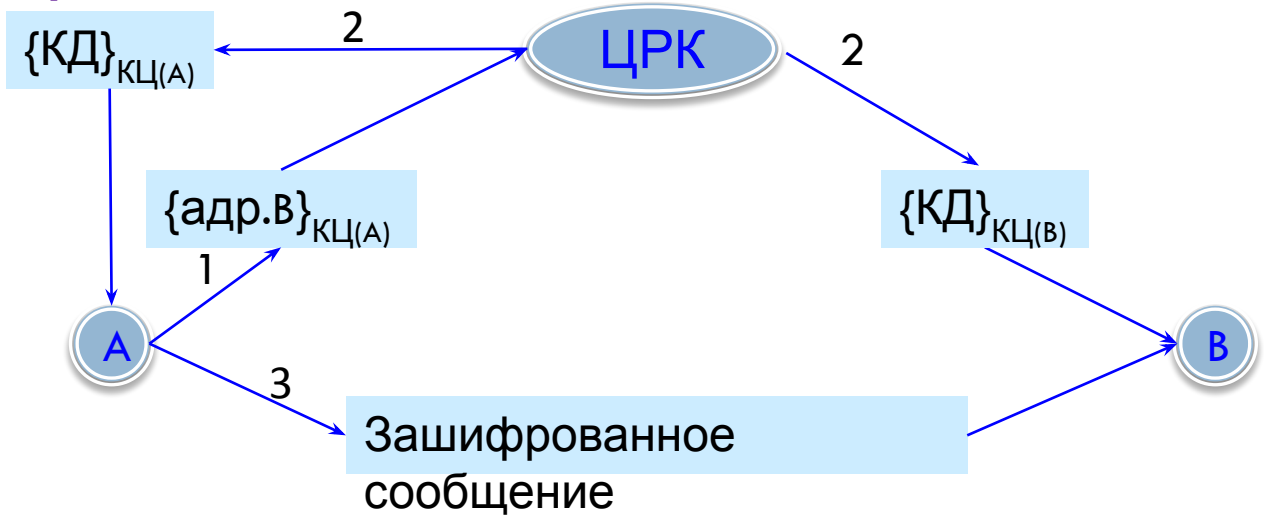
Система ЦТК (каждый абонент имеет ключ для связи с центром – КЦ)



Распределение ключей шифрования

ДОВЕДЕНИЕ КЛЮЧЕЙ ДО АБОНЕНТОВ

Система ЦРК (каждый абонент имеет ключ для связи с центром – КЦ)



Для повышения надежности процесс соединения абонентов состоит из двух фаз:

- ✔ ***взаимный обмен абонентов сеансной и идентификационной информацией;***
- ✔ ***передача зашифрованных сообщений***

Распределение ключей шифрования

ВВОД КЛЮЧЕЙ В КРИПТОГРАФИЧЕСКОЕ ОБОРУДОВАНИЕ

При вводе ключей обязателен двойной контроль:

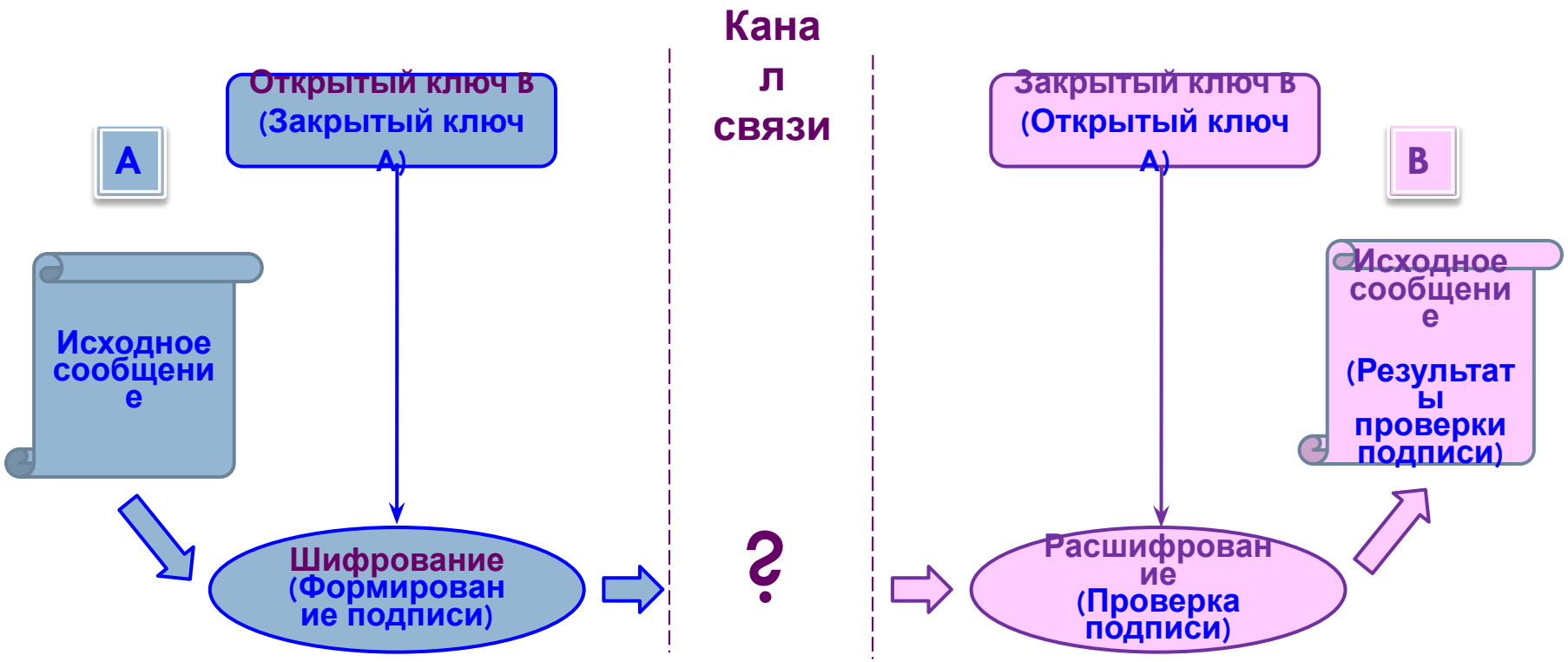
- ***два замка, ключи от которых у двух разных лиц (ввод возможен только при их совместном открытии);***
- ***раздельный ввод ключей (по частям)***

Электронная цифровая подпись

Определение

**ЭЦП – некоторая информация со специальной структурой,
которая на основе выполнения определенных математических
соотношений между подписанным сообщением и открытым
ключом позволяет с очень высокой степенью достоверности
проверить целостность этого сообщения и сделать вывод о том,
была ли цифровая подпись выработана с**

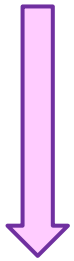
Электронная цифровая подпись



Электронная цифровая подпись

Формирование ЭЦП (несимметричная система RSA)

Определение эталонной характеристики подписываемого сообщения (специальная криптографическая функция – ХЭШ-функция)



Вычисление дополнительных параметров, зависящих от секретного ключа и эталонной характеристики, и формирование математического равенства (ЭЦП)

Хэш-функция – итеративная функция, которая позволяет вычислить для сообщения произвольной длины ХЭШ-код фиксированного размера (128 бит)

Итеративные функции – стойкие функции блочного симметричного шифрования

Электронная цифровая подпись

Проверка подписи

Проверка справедливости математического равенства

⇨

В качестве параметров алгоритма проверки выступают цифровая подпись и текущая характеристика сообщения, а также открытый ключ предполагаемого отправителя сообщения (криптосистема Эль-Гамаля)

Технология «блокчейн»

Блокчейн (цепочка блоков) – это распределенная база данных,
у которой устройства хранения данных не подключены
к общему серверу. Эта база данных хранит постоянно растущий список упорядоченных записей, называемых блоками. Каждый блок содержит метку времени и ссылку
на предыдущий блок.

Технология «блокчейн»

Технология «блокчейн»

Роль шифрования

Шифрование гарантирует, что пользователи могут изменять только те части блоков, которыми они «владеют»
в том смысле, что у них есть ключи, без которых запись
в файл невозможна (симметричная система).

Шифрование

Доступ к блокам может получить другой пользователь, который
получил ключ от пользователя-создателя блоков (несимметричная система)

Технология «блокчейн»

Истори

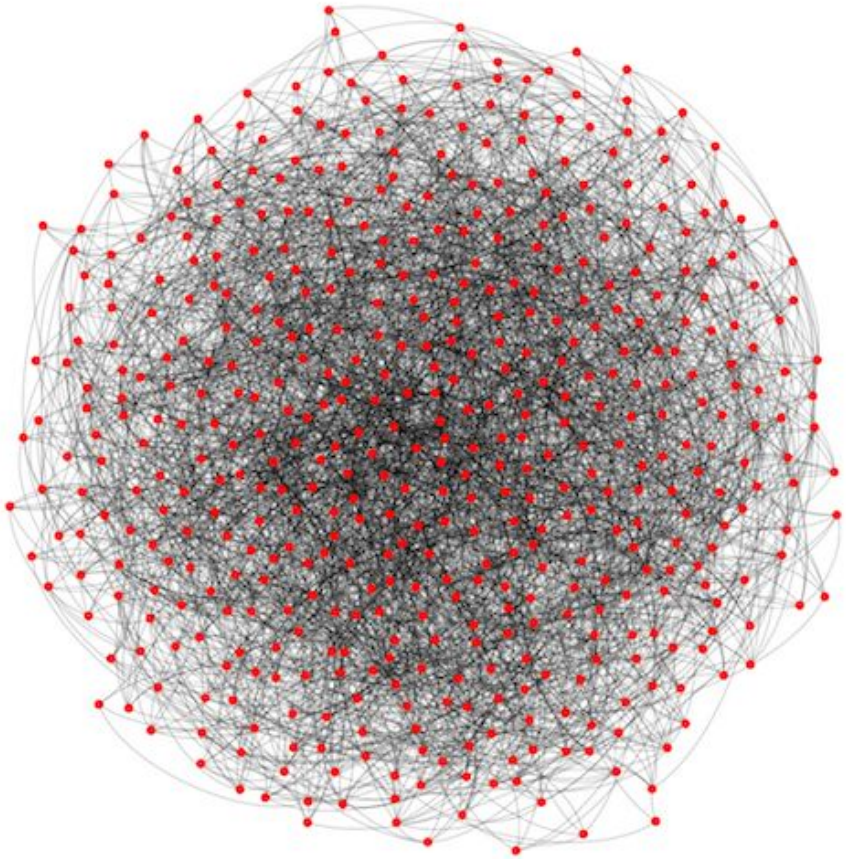
Концепция предложена в 2008 году. Автор Сатоши Накамото.
Впервые реализована в 2009 году как компонент цифровой валюты – биткойна.

Другое возможное применение

Медицинская база данных. Каждая запись – блок. У записи
есть метка: дата и время внесения. Обязателен запрет на изменение записей задним числом. Доступ к записи имеет
только врач (у него ключ). Ключ для расшифровки врач с помощью несимметричной системы

Технология «блокчейн»

Виртуальное отображение децентрализованного биткойн сервера



Криптографические методы защиты информации в ЭВМ

Защита паролей и информации, записанной в долговременной памяти
(жесткий диск, CD и т.п.)

- ***Алгоритм шифрования паролей*** **использует встроенный неизменяемый ключ (дешифровать пароль в обычных условиях не может даже администратор системы). Перед шифрованием к паролю добавляется еще несколько символов для обеспечения уникальности зашифрованного пароля (даже если два пользователя выберут одинаковый пароль). Такая система защиты паролей принята в ОС UNIX.**
- ***Шифрование данных в долговременной памяти*** **– эффективный способ предотвращения несанкционированного доступа к ним с целью копирования или хищения**

Задания для самостоятельной работы

1. Что изучают криптография, криптоанализ и криптология?
   Дайте определения этим наукам.

2. Какие методы криптографического закрытия информации вы знаете?
   В чем разница между шифрованием и кодированием?

3. Объясните, что представляет собой стеганография?

4. Объясните, почему основными требованиями,
   предъявляемыми к криптосистемам, являются наличие очень большого числа
   возможных ключей и равная вероятность их генерации.

5. От каких основных свойств криптографических алгоритмов зависит, на ваш взгляд,
   стойкость криптосистемы?

Задания для самостоятельной работы

6. В чем принципиальное различие оценки стойкости криптосистемы с использованием теории информации и теории вычислительной сложности?

7. Какие основные способы шифрования вы знаете? Каковы их преимущества и недостатки?

8. Опишите наиболее известный алгоритм шифрования DES. Какие из основных методов шифрования использованы в этом алгоритме?

9. Каковы основные особенности криптосистем с общедоступным ключом?

10. Раскройте основное содержание алгоритма электронной цифровой подписи.

11. Опишите последовательность установления связи и передачи

Задания для самостоятельной работы

12. В каких случаях применяются криптографические методы защиты информации
непосредственно в ЭВМ?

Программы-вирусы

История

60-е годы XX века – ***МО США рассматривает возможность применения программ-вирусов в целях выведения из строя средств***

80-е годы XX века – ***начало широкого распространения программ-вирусов***

Первая масштабная эпидемия – 1988 год, США:

Заражены 4 сети ЭВМ под общим названием «Интернет»:

- **«Арпанет» – ДАРПА МО (60 тыс. ЭВМ)**
- **сеть ННФ (университеты, участвующие в оборонных исследованиях)**
- **«Милнет» - несекретная информация подрядчиков МО США**
- **локальные вычислительные сети учреждений**

Изоляция и ликвидация вируса заняли четверо суток

Определения

- ***Компьютерный вирус представляет собой программу,***
  которая способна заражать другие программы,
  модифицируя их так, чтобы они включали в себя копию
  вируса (или его разновидность).
- ***Компьютерный вирус – самокопирующаяся программа,***
  заражающая другие программы, разрушающая данные,
  носители информации и даже оборудование

Фазы существования вируса

- ***Спячка*** — Используется автором вируса для создания у пользователя уверенности в правильной
- ***Распространение*** — В результате загрузки и выполнения зараженной программы происходит заражение других программ
- ***Запуск*** — Осуществляется после наступления некоторого события
- ***Разрушение*** — Разрушение программ, данных, аппаратуры или другое деструктивное действие, предусмотренное автором вируса

Программа-вирус на псевдоязыке


```
VIRUS
{
VIRUS; // Признак наличия вируса в программе
ЗАРАЗИТЬ_ПРОГРАММУ;
Если УСЛОВИЕ_СРАБАТЫВАНИЯ то МАНИПУЛЯЦИИ;
Передать управление программе;
}
ЗАРАЗИТЬ_ПРОГРАММУ
{
Выбрать программу, не содержащую строку “VIRUS”;
Присоединить вирус к программе;
}
УСЛОВИЕ_СРАБАТЫВАНИЯ
{
// Определение наличия условий для наступления фазы разрушения
}
МАНИПУЛЯЦИИ
{
// Осуществление специальных манипуляций, связанных с визуальными эффектами,
// разрушением системы и т.п.
}
```

Основные классы антивирусных программ

Копии → *Копирование программ является методом защиты, однако оно не гарантирует отсутствия вирусов*

Программы проверки целостности программного обеспечения → *Не могут препятствовать заражению, однако дают пользователю ценную информацию о зараженных или измененных программах*

Программы контроля → *Прерывают работу ЭВМ, если замечают что-либо подозрительное, и выдают пользователю рекомендацию о дальнейших действиях*

Программы удаления вирусов → *Проверяют наличие только известных вирусов. Обнаружив вирус, сообщают об этом пользователю или удаляют вирус*

Наиболее эффективны антивирусные программы смешанного типа, сочетающие свойства программ всех классов

Перспективные методы защиты

Универсальные → *Противостояние абсолютно всем вирусам*

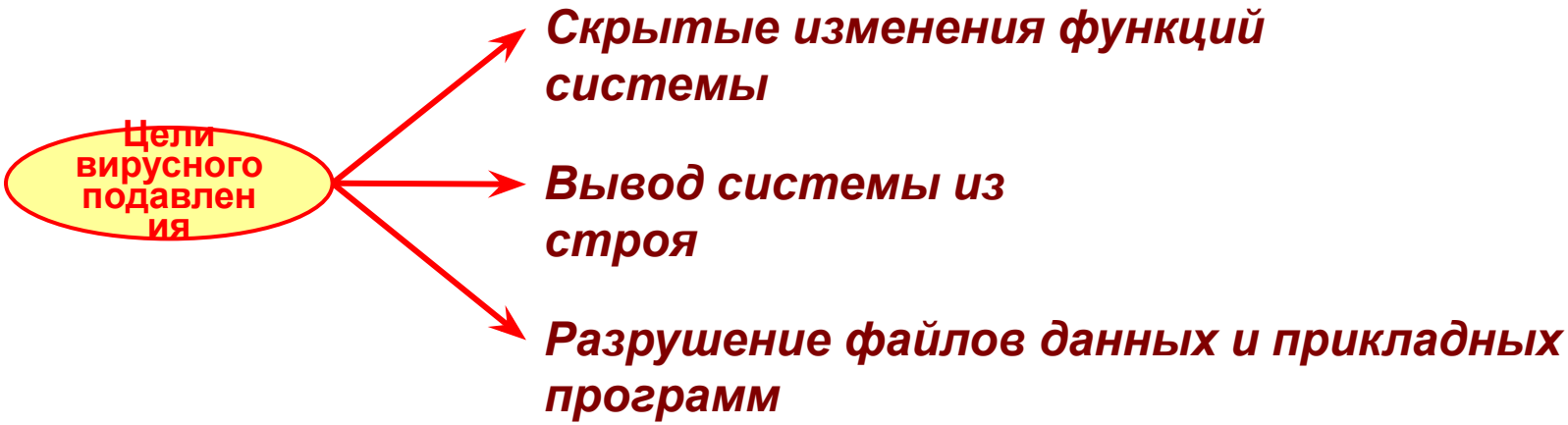
Адаптивные и самообучающиеся → *Автоматическое расширение списка вирусов, которым противостоят*

Интеллектуальные → *Базируются на системах логического вывода*

Аппаратные → *Дополнительное усиление системы защиты*

Наибольший интерес представляют адаптивные и интеллектуальные средства

Вирусное подавление как вид информационного оружия



Характерная черта современных АС – возрастание уязвимости для компьютерных вирусов

- Расширение применения распределенной цифровой обработки информации → Более доступны различные компоненты АС
- Использование перепрограммируемых встроенных ЭВМ и сетей связи → Большая доступность перепрограммируемых ЗУ и сетей обмена (поражение – изменение маршрутов обмена)
- Стандартизация ЭВМ, программного обеспечения, форматов сообщений и процедур передачи да ых → Создаются благоприятные условия для использования стандартных программ вирусного подавления

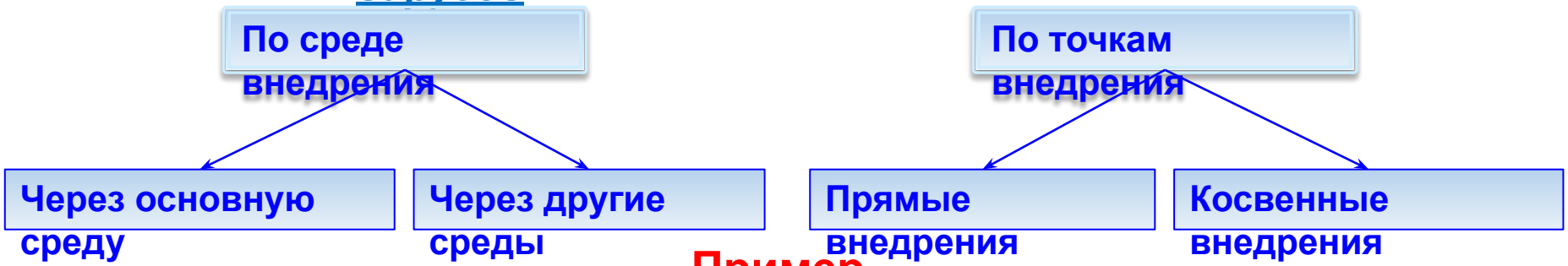
Вирусное подавление как вид информационного оружия

Примеры

- **Усовершенствованные авиационные радиоэлектронные системы (цифровая обработка, интеграция функций, применение модульной конструкции и мультиплексорных шин высокоскоростной**
- **Интегрированные системы командования и управления военного назначения (объединение систем связи тактических и стратегических подразделений – общие аппаратные и программные средства, к тому же коммерчески доступные)**

Вирусное подавление как вид информационного оружия

Механизмы внедрения компьютерных вирусов



Примеры

Основная среда **– цифровая радиосвязь (вирус внедряется в радиоприемное устройство вместе с принимаемым им сигналом)**

Другая (вспомогательная среда) **– воздействие вируса на подсистемы электропитания, стабилизации, термоконтроля и т.д. (эти подсистемы связаны с системными процессорами).**

Прямое внедрение **– непосредственное введение вируса в поражаемую систему (например, Другой способ – физическое внедрение в процессора путем непрерывной передачи его кода, когда система принимает полезную информацию).**

Косвенное внедрение **– точка канала внедрения – самая незащищенная из доступных точек (как правило, это средства обслуживания и диагностики)**

Вирусное подавление как вид информационного оружия

Комплексная стратегия защиты

1. ***Запрет доступа*** (препятствие проникновению вирусных программ в систему)
2. ***Обнаружение*** (обнаружение присутствия в системе вирусных программ)
3. ***Сдерживание*** (изоляция пораженной части системы от непораженной)
4. ***Ликвидация*** (уничтожение вирусов до того, как они произведут свое разрушительное действие)
5. ***Восстановление*** (восстановление разрушенных файлов с использованием резервных файлов)
6. ***Альтернативные меры*** (меры, не допускающие вывода системы из строя даже в случае поражения особо сложными и оригинальными вирусными

Задания для самостоятельной работы

1. Дайте определение компьютерного вируса как саморепродуцирующейся программы. Приведите примеры известных вам случаев заражения компьютеров вирусами.

2. Попробуйте изобразить структуру компьютерного вируса в виде программы, написанной на псевдоязыке.

3. Охарактеризуйте основные фазы, в которых может существовать компьютерный вирус.

4. Охарактеризуйте известные вам основные классы антивирусных программ. В чем смысл комплексного применения нескольких программ?

5. Каковы, на ваш взгляд, должны быть основные правила работы с компьютером, предупреждающие возможное заражение его вирусами?

Задания для самостоятельной работы

6. Охарактеризуйте перспективные методы защиты компьютеров от программ-вирусов.

7. Рассмотрите возможности вирусного подавления как одной из форм радиоэлектронной борьбы.

8. Каковы основные механизмы внедрения компьютерных вирусов в поражаемую систему?

9. Раскройте содержание комплексной стратегии защиты, ориентированной на противодействие возможному вирусному подавлению.

Защита информации от утечки по техническим каналам

Определения

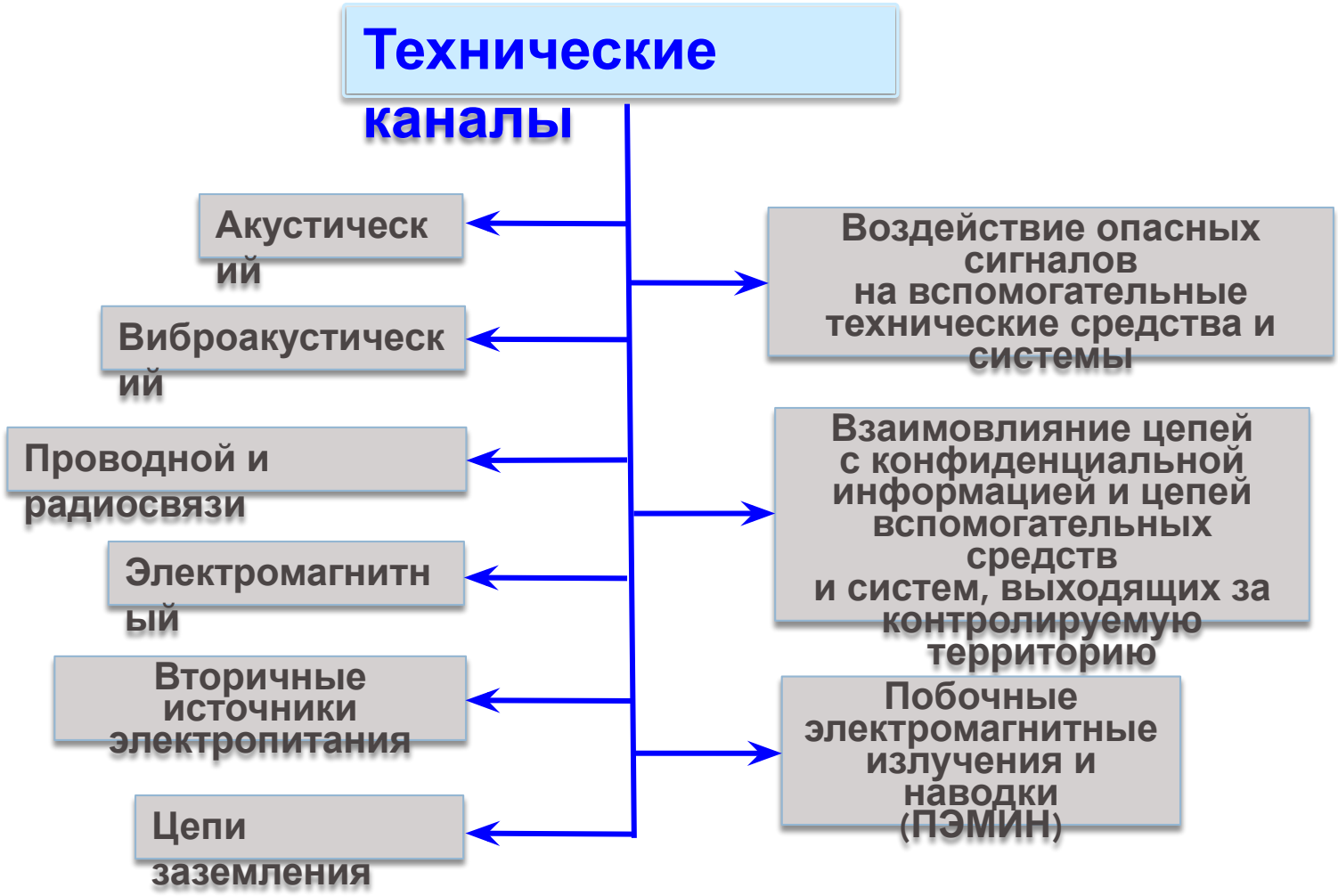
Технический канал утечки информации

Совокупность физических полей, несущих конфиденциальную информацию, конструктивных элементов, взаимодействующих с ними, и технических средств злоумышленника для регистрации поля и снятия информации

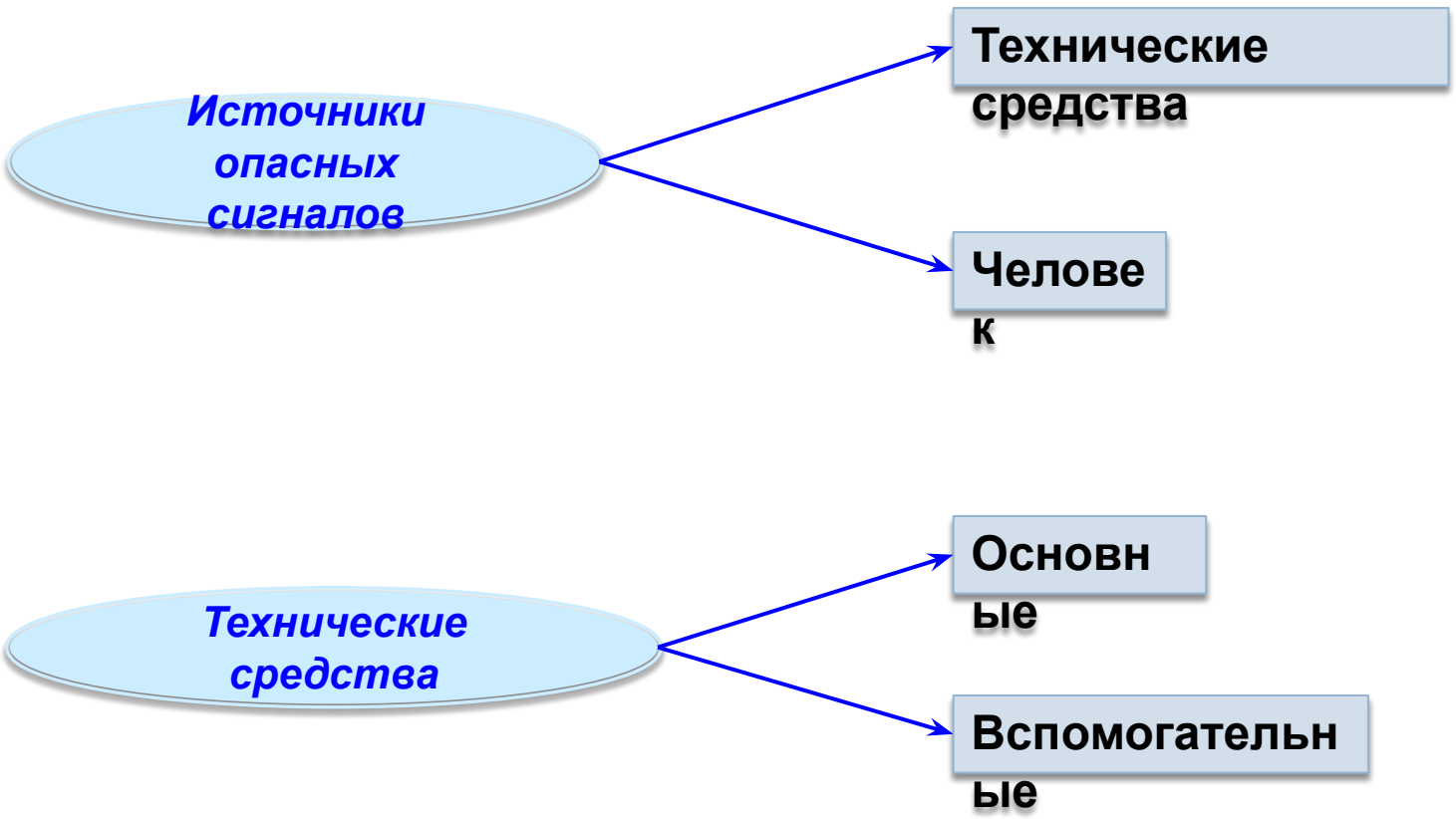
Опасные сигналы

Акустические, виброакустические, электрические и электромагнитные сигналы, представляющие конфиденциальную информацию

Виды технических каналов



Виды технических каналов



Виды технических каналов

Основные технические средства

- ✔ Персональные ЭВМ с периферийным оборудованием, сети ЭВМ
- ✔ Телефонные аппараты городской АТС
- ✔ Телефонные аппараты местной АТС
- ✔ Радиотелефоны и сотовые телефоны
- ✔ Селекторная связь
- ✔ Телефакс
- ✔ Телетайп
- ✔ Средства размножения документов

Виды технических каналов

Вспомогательные технические средства

- ✔ Радиоаппаратура
- ✔ Радиотрансляционный громкоговоритель
- ✔ Датчики охранной и пожарной сигнализации
- ✔ Табельное электрооборудование помещений
- ✔ Кондиционеры

Возможности злоумышленника

Контроль акустической информации

Возможности злоумышленника

Контроль акустической информации

Электронный контроль речи

- Использование радиоканала
- Использование линий электропитания

Радиоканал → ***Закамуфлированные радиопередатчики***

Линии электропитания → ***Передача сигнала с помощью ультразвука***

Возможности злоумышленника

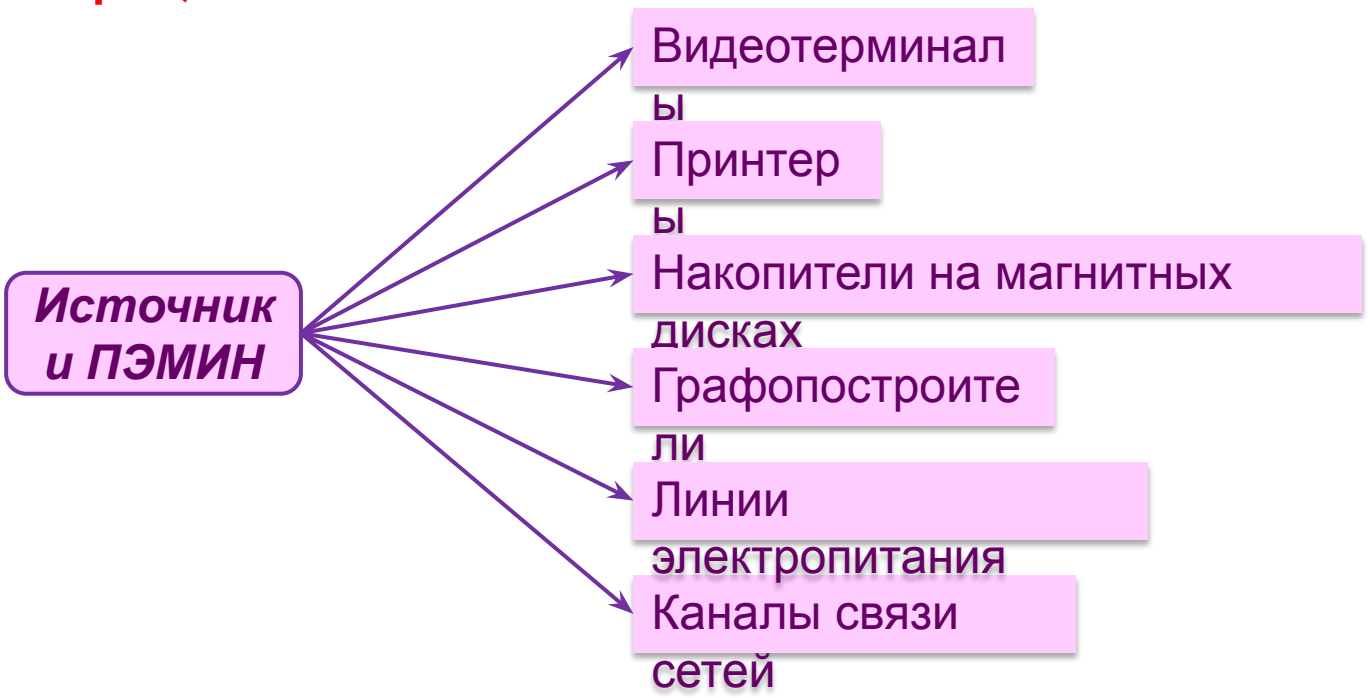
Контроль информации в каналах телефонной связи

- ✔ Непосредственное подключение к телефонной линии
- ✔ Негальваническое подключение к телефонной линии (индуктивное)
- ✔ Использование микропередатчика с питанием от телефонной линии (подключается в любом месте от аппарата до АТС)
- ✔ Прослушивание помещений с помощью кодового микрофонного усилителя (встраивается в телефонный аппарат)
- ✔ Прослушивание помещений с помощью микрофона телефонного аппарата (модуляция высокочастотного сигнала сигналами от микрофона или корпуса телефонного аппарата)
- ✔ Прослушивание помещений с использованием телефонных аппаратов, содержащих электромагнитный звонок(в цепи звонка есть модулированный ток)
- ✔ Прослушивание телефонных разговоров, ведущихся по

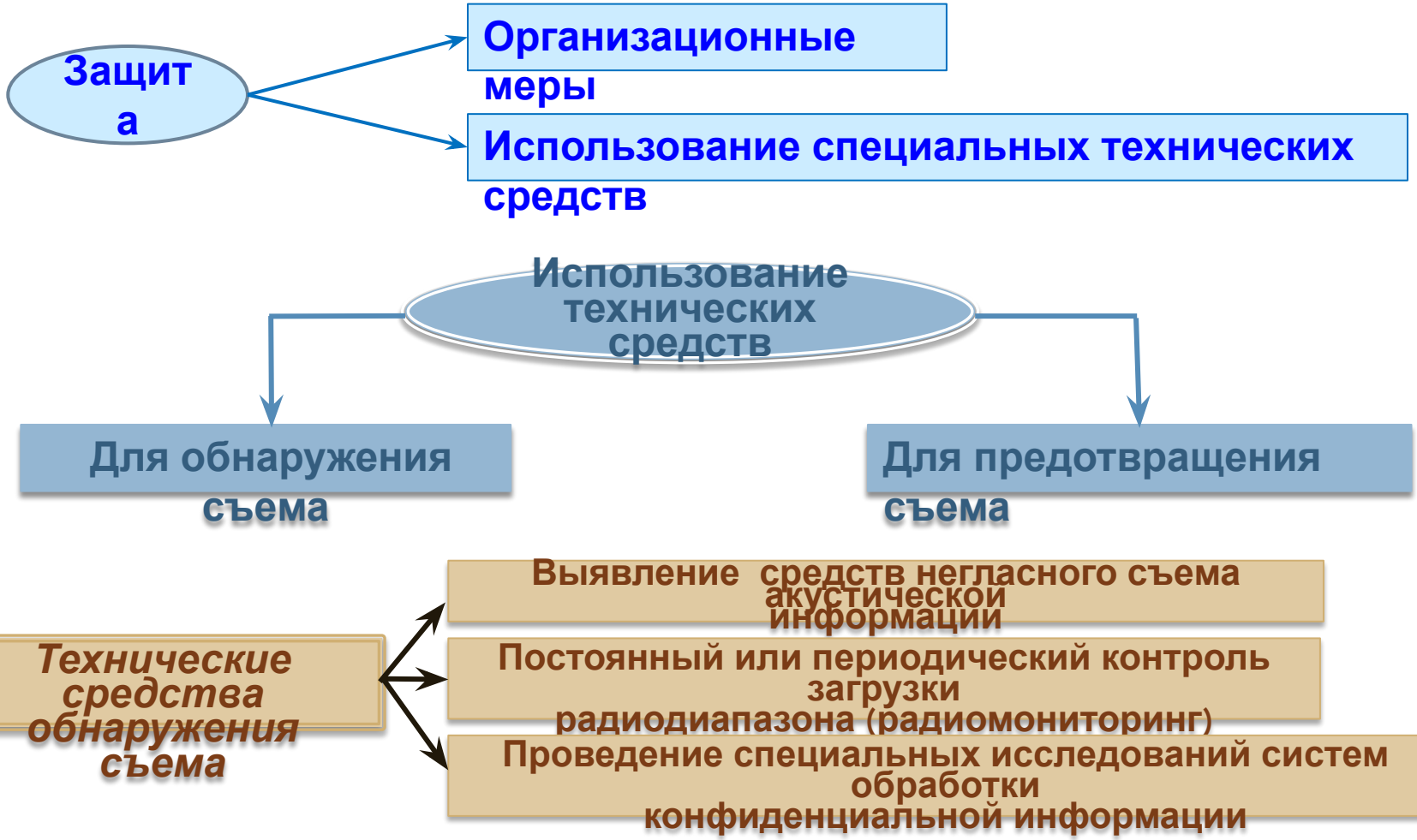
Возможности злоумышленника

Контроль информации, обрабатываемой средствами вычислительной техники

Перехват ПЭМИН (на расстоянии до нескольких сотен метров)



Способы предотвращения утечки информации по техническим каналам



Способы предотвращения утечки информации по техническим каналам

Акустический канал

Обнаружение съема → ***Достаточно сложно (практически можно обнаружить только работающие диктофоны)***

Обнаружение съема (электронный контроль речи)

- ***Поиск и контроль по электромагнитному излучению – работающие устройства***
- ***Аппаратура пассивного обнаружения – независимо от режима работы обнаруживаемых устройств (нелинейные локаторы, эндоскопы, дефектоскопы, металлоискатели, тепловизоры и т.п.)***

Предотвращение съема → ***Генераторы аудиопомех (от миниатюрных до стационарных)***

Способы предотвращения утечки информации по техническим каналам

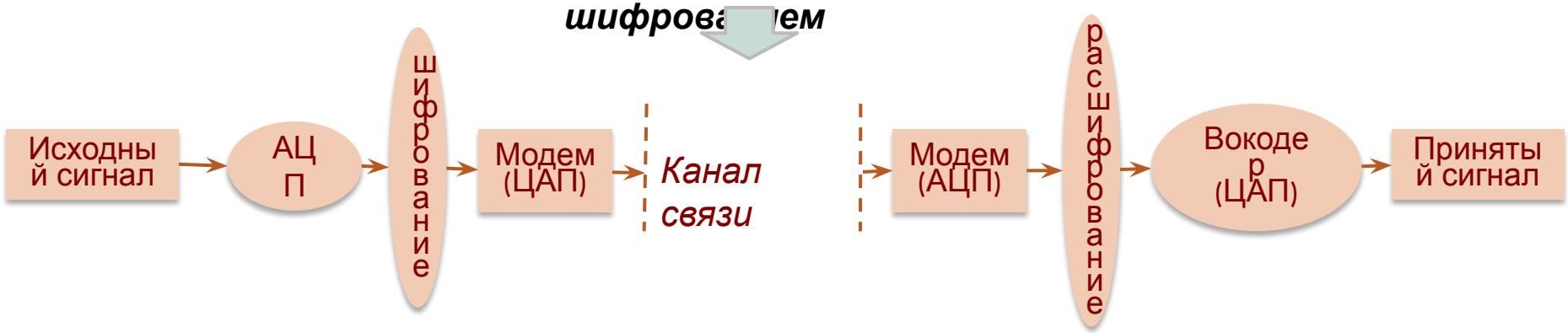
Каналы связи

Обнаружение съема

- ***Установление факта подключения к телефонным каналам подслушивающих устройств***
- ***Спектральный анализ каналов связи***

Предотвращение съема

- ***Аналоговое скремблирование*** → **Изменение характеристик речевого сигнала без изменения полосы частот**
- ***Дискретизация с последующим шифрова[illegible]ем***



Способы предотвращения утечки информации по техническим каналам

Канал ПЭМИН

Обнаружение съема → ***Обнаружение техническими средствами невозможно***

Предотвращение съема → ***Пассивная защита***

Предотвращение съема → ***Активная защита***

Способы предотвращения утечки информации по техническим каналам

Канал ПЭМИН

Пассивная защита

1. *Размещение всего оборудования в экранирующей радиоизлучения среде (применимо только для малогабаритной аппаратуры)*
2. *Экранирование отдельных компонентов защищаемых систем, применение в линиях связи и питания различных фильтров, устройств подавления сигналов и*

Допустимые уровни излучений аппаратуры и меры защиты информации регламентируются специальными стандартами. Стоимость оборудования, отвечающего стандартам, в 3-5 раз выше стоимости соответствующего

Способы предотвращения утечки информации по техническим каналам

Канал ПЭМИН

Активная защита

Сокрытие информационных сигналов за счет шумовой или заградительной помехи с помощью специальных генераторов шума (радиомаскировка)

Энергетическая (экологически опасная)

Широкий спектр Большая мощность

Неэнергетическая (статистическая

Изменение вероятностной структуры сигнала, который может быть принят злоумышленником

Задания для самостоятельной работы

1. Дайте определение понятию «технический канал утечки информации». Назовите основные виды технических каналов.

2. Какой, по вашему мнению, технический канал утечки информации можно отнести к наиболее часто используемым техническими разведками для получения конфиденциальной информации? Раскройте особенности этого канала.

3. Дайте классификацию источников утечки информации по техническим каналам.

4. Что такое основные и вспомогательные технические средства автоматизированной системы? Приведите примеры и рассмотрите возможности их использования в качестве технических каналов утечки информации.

5. Назовите известные вам методы и средства контроля акустической

Задания для самостоятельной работы

7. Назовите методы контроля информации, обрабатываемой средствами вычислительной техники.

8. Охарактеризуйте основные способы предотвращения утечки информации по техническим каналам.

9. Приведите известные вам методы защиты от утечки информации по акустическому каналу. Попробуйте сравнить их, используя критерий «эффективность/стоимость».

10. Охарактеризуйте существующие на сегодняшний день способы защиты информации в каналах связи.

11. Назовите методы и средства защиты информации от утечки по побочному электромагнитному каналу.

Организационно-правовое обеспечение защиты информации

Государственная система защиты информации

Определение

Государственная система защиты информации – совокупность федеральных и иных органов управления и взаимоувязанных правовых, организационных и технических мер, осуществляемых на различных уровнях управления и реализации информационных отношений и направленных на обеспечение

Государственная система защиты информации

Состав государственной системы

- Совет Безопасности Российской Федерации
  - МВК по информационной безопасности
  - Секция НС по информационной безопасности
- МВК по защите государственной тайны

ФСБ | СВР | ФСО | МВД | ФСТЭК | Минкомсвязь

- МВД → Бюро специальных технических мероприятий

Службы, управления, отделы информационной безопасности министерств и ведомств

Концепция правового обеспечения информационной безопасности

Опыт законодательного регулирования информатизации за рубежом

История. **Проблема впервые начала обсуждаться в 60-е годы XX века в США в связи с предложением создать общенациональный банк данных**

Направления законодательного регулирования

Защита прав личности на частную жизнь (защита от бесконтрольного распространения и доступа к персональным данным)

- Установление пределов вмешательства в частную жизнь с использованием компьютерных систем
- Введение административных механизмов защиты граждан от такого вмешательства

Защита государственных интересов

- Установление приоритетов защиты
- Определение исполнительских механизмов и нормативное обеспечение механизмов защиты

Защита предпринимательской и финансовой деятельности

- Введение антимонопольного законодательства
- Создание механизмов добросовестной конкуренции
- Введение механизмов защиты авторских прав

Опыт законодательного регулирования информатизации за рубежом

Исторические примеры национальных законодательств

- ***Великобритания:*** Билль о надзоре за данными (1969)
  Закон о защите информации (1984)

- ***Франция:*** Закон об информатике, картотеках и свободе (1978)

- ***ФРГ:*** Закон о защите данных персонального характера от злоупотреблений
  при обработке данных (1977)
  Закон о защите информации (1978)

- ***США:*** Закон о тайне частной информации (1974)
  Акт о злоупотреблениях в использовании ЭВМ (1986)
  Закон о безопасности компьютерных систем (1987)

- ***Канада:*** Закон о компьютерных и информационных преступлениях (1985)

Опыт законодательного регулирования информатизации за рубежом

Законодательство США
(наиболее развитое – свыше 100 различных актов)

- ***Определение и закрепление государственной политики в области информатизации***
- ***Обеспечение развитого производства, технологий***
- ***Борьба с монополизмом и стимуляция приоритетных направлений***
- ***Организация информационных систем***
- ***Организация систем управления в сфере информатизации***
- ***Защита прав потребителя, особенно прав граждан на информацию, защита информации о гражданах***

Опыт законодательного регулирования информатизации за рубежом

Общее для зарубежных законодательств

- ***Установлена ответственность за нарушение порядка обработки и использования персональных данных***

- ***Компьютерные преступления расцениваются как преступления, представляющие особую опасность для граждан, общества и государства, и влекут значительно более жесткие меры наказания, нежели аналогичные преступления, совершенные без применения компьютерной техники***

- ***Как преступления рассматриваются также действия, создающие угрозу нанесения ущерба (попытка проникновения в систему, внедрение***

Опыт законодательного регулирования информатизации за рубежом

Основные виды компьютерных преступлений

- ***Несанкционированный доступ к информации, хранящейся в компьютере (использование чужого имени, изменение физических адресов технических устройств, использование информации, оставшейся после решения задач, модификация программного и информационного обеспечения, хищение носителей информации, установка аппаратуры записи, подключаемой к каналам передачи данных)***

- ***Ввод в программное обеспечение «логических бомб», которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему***

- ***Разработка и злонамеренное распространение компьютерных вирусов***

- ***Преступная небрежность в разработке, изготовлении и эксплуатации программно-вычислительных комплексов, приведшая к тяжким***

КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ (ИНТЕРПОЛ)

Группа	Вид деятельности
QA – несанкционированный доступ и перехват	
QAH	**Компьютерный абордаж (хакинг): несанкционированный доступ в компьютер или компьютерную сеть;**
QAI	**Перехват: несанкционированный перехват информации при помощи технических средств, несанкционированные обращения в компьютерную систему или сеть как из нее, так и внутри компьютерной системы или сети;**
QAT	**Кража времени: незаконное использование компьютерной системы или сети с намерением неуплаты;**
QAZ	**Прочие виды несанкционированного доступа и перехвата.**
Группа QD – изменение компьютерных данных	
QDL	**Логическая бомба: неправомерное изменение компьютерных данных путем внедрения логической бомбы;**
QDT	**Троянский конь: неправомерное изменение компьютерных данных путем внедрения троянского коня;**
QDV	**Вирус: изменение компьютерных данных или программ без права на то, путем внедрения или распространения компьютерного вируса;**
QDW	**Червь: несанкционированное изменение компьютерных данных или программ путем передачи, внедрения или распространения компьютерного червя в компьютерную сеть;**
QDZ	**Прочие виды изменения данных.**

КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ (ИНТЕРПОЛ)

Группа	Вид деятельности
Группа QF – компьютерное мошенничество	
QFC	**Компьютерные мошенничества с банкоматами: мошенничества, связанные с хищением наличных денег из банкоматов;**
QFF	**Компьютерные подделки: мошенничества и хищения из компьютерных систем путем создания поддельных устройств (карточек и пр.);**
QFG	**Мошенничества с игровыми автоматами: мошенничества и хищения, связанные с игровыми автоматами;**
QFM	**Манипуляции с программами ввода-вывода: мошенничества и хищения посредством неверного ввода или вывода в компьютерные системы или из них путем манипуляции программами;**
QFP	**Компьютерные мошенничества с платежными средствами: мошенничества и хищения, связанные с платежными средствами;**
QFT	**Телефонное мошенничество: доступ к телекоммуникационным услугам путем посягательства на протоколы и процедуры компьютеров, обслуживающих телефонные системы;**
QFZ	**Прочие компьютерные мошенничества.**
Группа QR – незаконное копирование	
QRG/QFS	**Незаконное копирование, распространение или опубликование компьютерных игр и другого программного обеспечения;**
QRT	**Незаконное копирование топологии полупроводниковых изделий: незаконное копирование защищенной законом топологии полупроводниковых изделий или незаконная коммерческая эксплуатация или импорт с этой целью топологии или самого полупроводникового изделия, произведенного с использованием данной топологии;**
QRZ	**Прочее незаконное копирование.**

КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ (ИНТЕРПОЛ)

Группа	Вид деятельности
Группа QS – компьютерный саботаж	
QSH	**Саботаж с использованием аппаратного обеспечения: ввод, изменение, стирание или подавление компьютерных данных или программ или вмешательство в работу компьютерных систем с намерением помешать функционированию компьютерной или телекоммуникационной системы;**
QSS	**Компьютерный саботаж программы: несанкционированное стирание, повреждение, ухудшение или подавление компьютерных данных или программ;**
QSZ	**Прочие виды саботажа.**
Группа QZ – прочие компьютерные преступления	
QZB	**Электронные доски объявлений (BBS): использование BBS для хранения, обмена и распространения материалов, имеющих отношение к преступной деятельности;**
QZE	**Хищение информации, представляющей коммерческую тайну (компьютерный шпионаж): приобретение незаконными средствами или передача информации, представляющей коммерческую тайну без права на то или другого законного обоснования, с намерением причинить экономический ущерб или получить незаконные экономические преимущества;**
QZS	**Материал конфиденциального характера: использование компьютерных систем или сетей для хранения, обмена, распространения или перемещения информации конфиденциального характера;**
QZZ	**Прочие компьютерные преступления.**

Состояние правового обеспечения информатизации в России

История. **Впервые вопрос о правовом обеспечении информатизации был поставлен в 70-х годах XX века в связи с развитием АСУ различных уровней. Серьезно вопросом стали заниматься только в начале 90-х годов**

1 → ***Проблема права на информацию***

- Закрепление общего права граждан на информацию
- Разработка актов, связанных с режимом массовой информации
- Создание общего информационного пространства (в том числе, в общеевропейском контексте)

2 → ***Проблема собственности на некоторые виды информации***

3 → ***Проблема признания информации объектом товарного характера***

Состояние правового обеспечения информатизации в России

Базовый закон

ЗАКОН
об информации, информационных технологиях и о защите информации
2006

- Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации
- Информация как объект правовых отношений
- Обладатель информации
- Общедоступная информация
- Право на доступ к информации
- Ограничение доступа к информации
- Распространение информации или предоставление информации
- Документирование информации
- Государственное регулирование в сфере применения информационных технологий
- Информационные системы
- Государственные информационные системы
- Использование информационно-коммуникационных сетей
- Защита информации
- Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации

Состояние правового обеспечения информатизации в России

Базовый закон

ЗАКОН
об информации, информационных технологиях и о защите информации
2006

В Законе:

- ✔ Закрепляются права граждан, организаций, государства на информацию
- ✔ Устанавливается правовой режим информации на основе применения правил документирования, института собственности, деления информации по признаку доступа на открытую и с ограниченным доступом, правил формирования информационных ресурсов и пользования ими
- ✔ Устанавливаются основные права и обязанности государства, организаций, граждан в процессе создания информационных систем, создания и развития научно-технической, производственной базы информатизации, формирования рынка информационной продукции, услуг в этой сфере
- ✔ Устанавливаются правила и общие требования ответственности в области защиты информации в системах ее обработки
- ✔ Предусматривается порядок включения страны в международные информационные системы

Состояние правового обеспечения информатизации в России

Базовый закон

ЗАКОН
об информации, информационных технологиях и о защите информации
2006

Защита информации:

- **Предотвращение утечки, хищения, утраты, искажения, подделки, несанкционированных действий по уничтожению, копированию, блокированию информации и других форм незаконного вмешательства в информационные системы**
- **Сохранение полноты, достоверности, целостности информации**
- **Сохранение возможности управления процессом обработки, пользования информацией в соответствии с условиями, установленными собственником или владельцем информации**
- **Обеспечение конституционных прав на сохранение личной тайны и конфиденциальности персональной информации, накапливаемой в информационных системах**
- **Защита прав субъектов правоотношений в информационных процессах**
- **Сохранение секретности, конфиденциальности информации в соответствии с правилами, установленными базовым законом и другими законодательными актами**

Состояние правового обеспечения информатизации в России

ЗАКОН
о государственной тайне

1993

- ✔ **Закреплено право Российской Федерации на государственную тайну (установление прав собственности государства на определенную часть информации, относящуюся к обеспечению национальной безопасности)**
- ✔ **Определены сферы деятельности государства, в которых допустимо и недопустимо засекречивание информации**
- ✔ **Введены ограничения гражданских прав, а также установлены льготы и компенсации для лиц, привлекаемых к работе с информацией, отнесенной к государственной тайне**
- ✔ **Установлены принципы засекречивания информации, а также система защиты государственной тайны**

Состояние правового обеспечения информатизации в России

ЗАКОН
о коммерческой тайне

2004

- Право на отнесение информации к информации, составляющей коммерческую тайну, и способы получения такой информации
- Сведения, которые не могут составлять коммерческую тайну
- Предоставление информации, составляющей коммерческую тайну
- Права обладателя информации, составляющей коммерческую тайну
- Обладатель информации, составляющей коммерческую тайну, полученной в рамках трудовых отношений
- Порядок установления режима коммерческой тайны при выполнении государственного контракта для государственных нужд
- Охрана конфиденциальности информации
- Охрана конфиденциальности информации в рамках трудовых отношений
- Охрана конфиденциальности информации в рамках гражданско-правовых отношений
- Охрана конфиденциальности информации при ее предоставлении
- Ответственность за нарушение Закона о коммерческой тайне
- Ответственность за не предоставление органам государственной власти, иным государственным органам, органам местного

Состояние правового обеспечения информатизации в России

ЗАКОН
о персональных данных

2006

- Принципы и условия обработки персональных данных
- Права субъекта персональных данных
- Обязанности оператора
- Контроль и надзор за обработкой персональных данных

Состояние правового обеспечения информатизации в России

ЗАКОН
об электронной подписи

2011

- Правовое регулирование отношений в области использования электронных подписей
- Принципы использования электронных подписей
- Виды электронных подписей
- Условия признания электронных документов, подписанных электронной подписью
- Признание электронных подписей, созданных в соответствии с нормами иностранного права и международными стандартами
- Полномочия федеральных органов исполнительной власти в сфере использования электронной подписи
- Использование простой электронной подписи
- Обязанности участников электронного взаимодействия при использовании усиленных электронных подписей
- Признание квалифицированной электронной подписи
- Средства электронной подписи
- Удостоверяющий центр
- Сертификат ключа проверки электронной подписи
- Аккредитованный удостоверяющий центр
- Аккредитация удостоверяющего центра
- Квалифицированный сертификат

Состояние правового обеспечения информатизации в России

ЗАКОН
О безопасности критической информационной инфраструктуры Российской Федерации

2017

- Правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры
- Принципы обеспечения безопасности критической информационной инфраструктуры
- Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
- Полномочия Президента Российской Федерации и органов государственной власти Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры
- Категорирование объектов критической информационной инфраструктуры
- Реестр значимых объектов критической информационной инфраструктуры
- Права и обязанности субъектов критической информационной инфраструктуры
- Система безопасности значимого объекта критической информационной инфраструктуры
- Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры
- Оценка безопасности критической информационной инфраструктуры

Стандарты, руководящие нормативно-технические, методические и организационные документы

Истори я

США →

«Критерии оценки гарантированной защищенности вычислительной системы» – «Оранжевая книга» (1985)
Дополнения по оценке защищенности сетей ЭВМ (1987) и
систем управления базами данных (1989)

ЕС →

Франция, Великобритания, ФРГ, Голландия в конце
80-х годов приняли согласованный документ «Критерии
оценки безопасности информационных технологий»

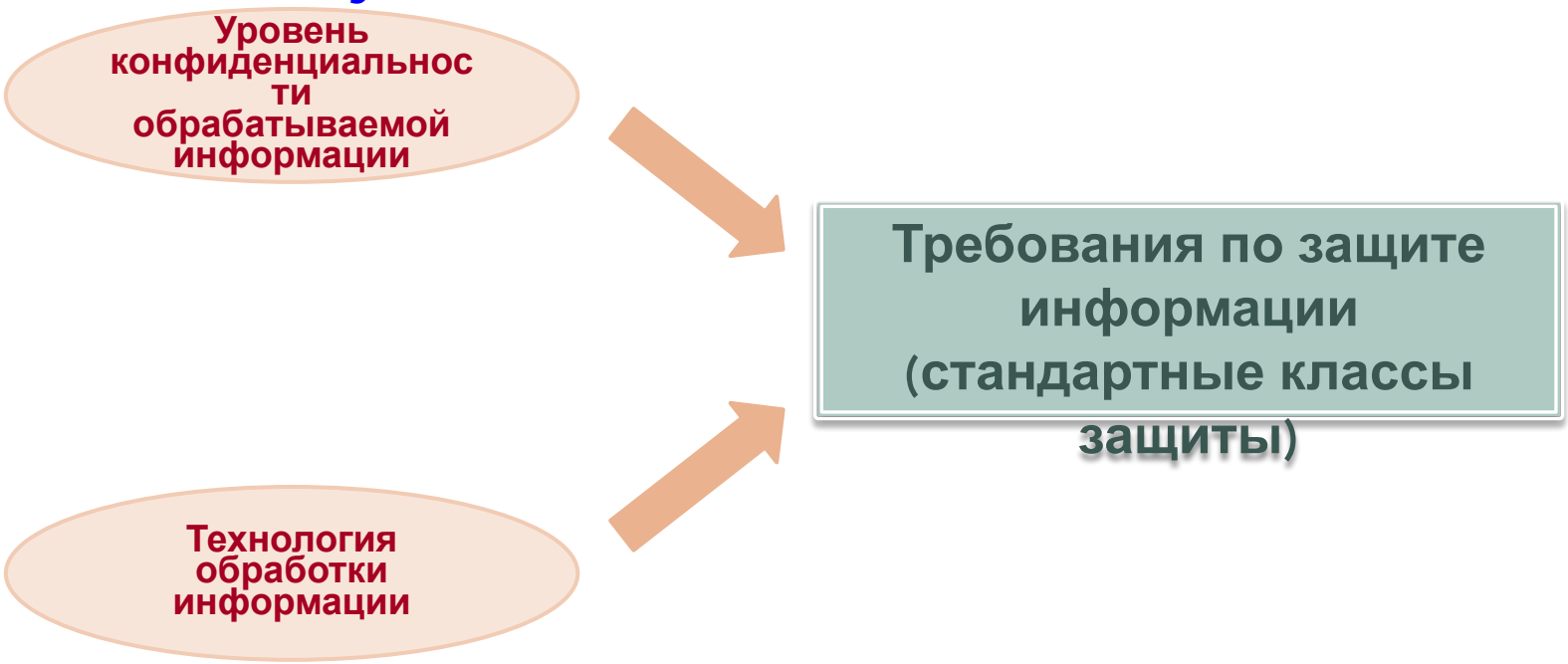
Россия →

В начале 90-х годов приняты руководящие документы по
стандартизации:

- ✔ **«Средства вычислительной техники, Защита от несанкционированного доступа к информации. Показатели защищенности СВТ»**
- ✔ **«Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования**

Стандарты, руководящие нормативно-технические, методические и организационные документы

Структура руководящих документов



Стандарты, руководящие нормативно-технические, методические и организационные документы

Последующие документы Гостехкомиссии России (ФСТЭК)

- **«Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (1997)**
- **«Защита от НСД. Часть I. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (1998)**
- **«Средства защиты информации. Защита информации в контрольно-кассовых машинах и автоматизированных кассовых системах. Классификация контрольно-кассовых машин, автоматизированных кассовых систем и требования по защите информации» (1998)**

Дальнейшее развитие – внедрение «Общих критериев» (с 2004 г.)

(стандарт ISO 15408-99 «Критерии оценки безопасности информационных технологий»)

Задания для самостоятельной работы

1. С чем, по вашему мнению, связана необходимость организационно-правового
обеспечения защиты информации? В чем заключается специфика этого обеспечения применительно к информации, обрабатываемой в автоматизированных системах?

2. Охарактеризуйте задачи, решаемые организационно-правовым обеспечением защиты информации в АС. Выделите особенности, связанные с «электронной» формой представления информации в АС.

3. Сформулируйте основные направления развития организационно-правового
обеспечения защиты информации в зарубежных странах. Назовите известные вам
законодательные акты зарубежных стран в области регулирования процессов
информатизации и обеспечения безопасности информации.

4. Что вы знаете из истории развития организационно-правового

Задания для самостоятельной работы

5. Сформулируйте основные положения Закона Российской Федерации «Об информации, информационных технологиях и защите информации».
Какие еще вы знаете российские законодательные акты в этой области?

6. Сформулируйте основные подходы к разработке организационно-правового
обеспечения защиты информации. Раскройте содержание структуры этого обеспечения.

7. Сформулируйте основные требования, предъявляемые к системе стандартизации
в области защиты информации. Назовите известные вам системы стандартов
в этой области, принятые в России и за рубежом.

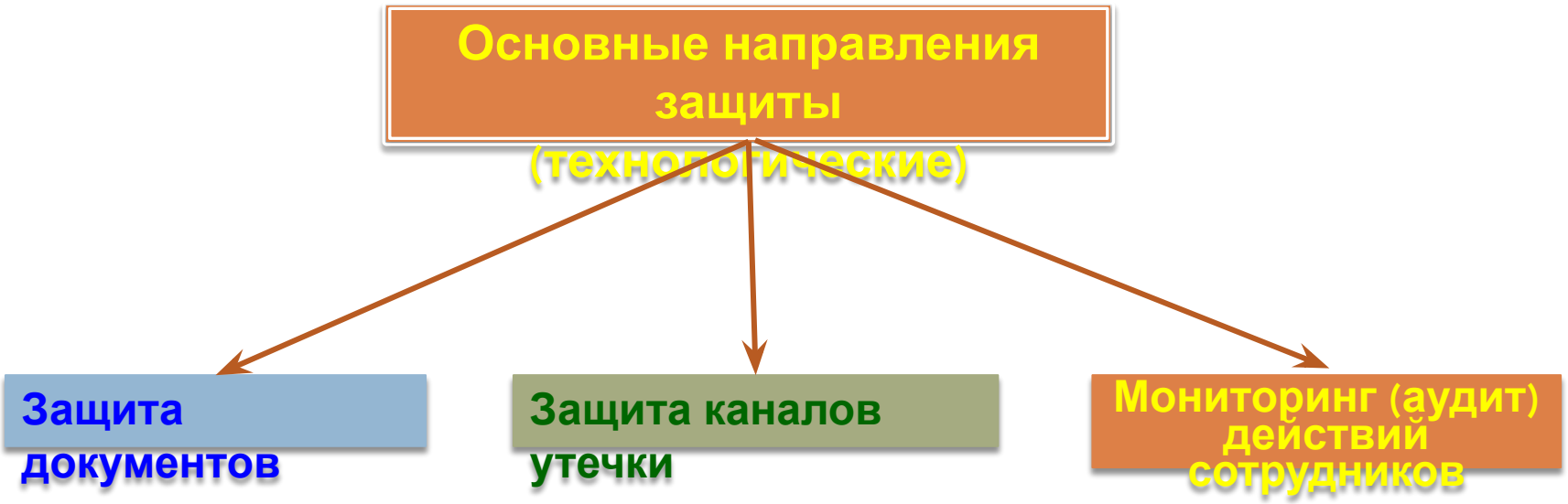
8. Опишите систему органов государственного управления Российской Федерации,
осуществляющих управление и координацию деятельности в области

Гуманитарные проблемы информационной безопасности

Основные проблемы
(утверждены Советом Безопасности РФ)

- Место и роль проблем информационной безопасности в становлении современного информационного общества
- Обеспечение баланса интересов личности, общества и государства в информационной сфере, баланса между потребностью в свободном обмене информацией и допустимыми ограничениями ее распространения
- Национальные интересы России и информационное противостояние в современном мире
- Место и роль СМИ в решении задач информационного обеспечения государственной политики Российской Федерации
- Ценностная ориентация личности, ее информационное обоснование и информационная безопасность
- Информационная безопасность и проблемы информационной культуры и этики
- Сохранение культурно-нравственных ценностей российского народа
- Информационное пространство и проблема целостности российского государства

Защита информации от внутренних угроз



Защита информации от внутренних угроз

Классификация внутренних нарушителей

Тип	Умысел	Корысть	Постановка задачи	Действия при невозможности
Халатный	Нет	Нет	Нет	Сообщение
Манипулируемый	Нет	Нет	Нет	Сообщение
Обиженный	Да	Нет	Сам	Отказ
Нелояльный	Да	Нет	Сам	Имитация
Подрабатывающий	Да	Да	Сам/Извне	Отказ/Имитация/Взлом
Внедренный	Да	Да	Сам/Извне	Взлом

Диаграмма причинно-следственных связей (кража с соучастниками)

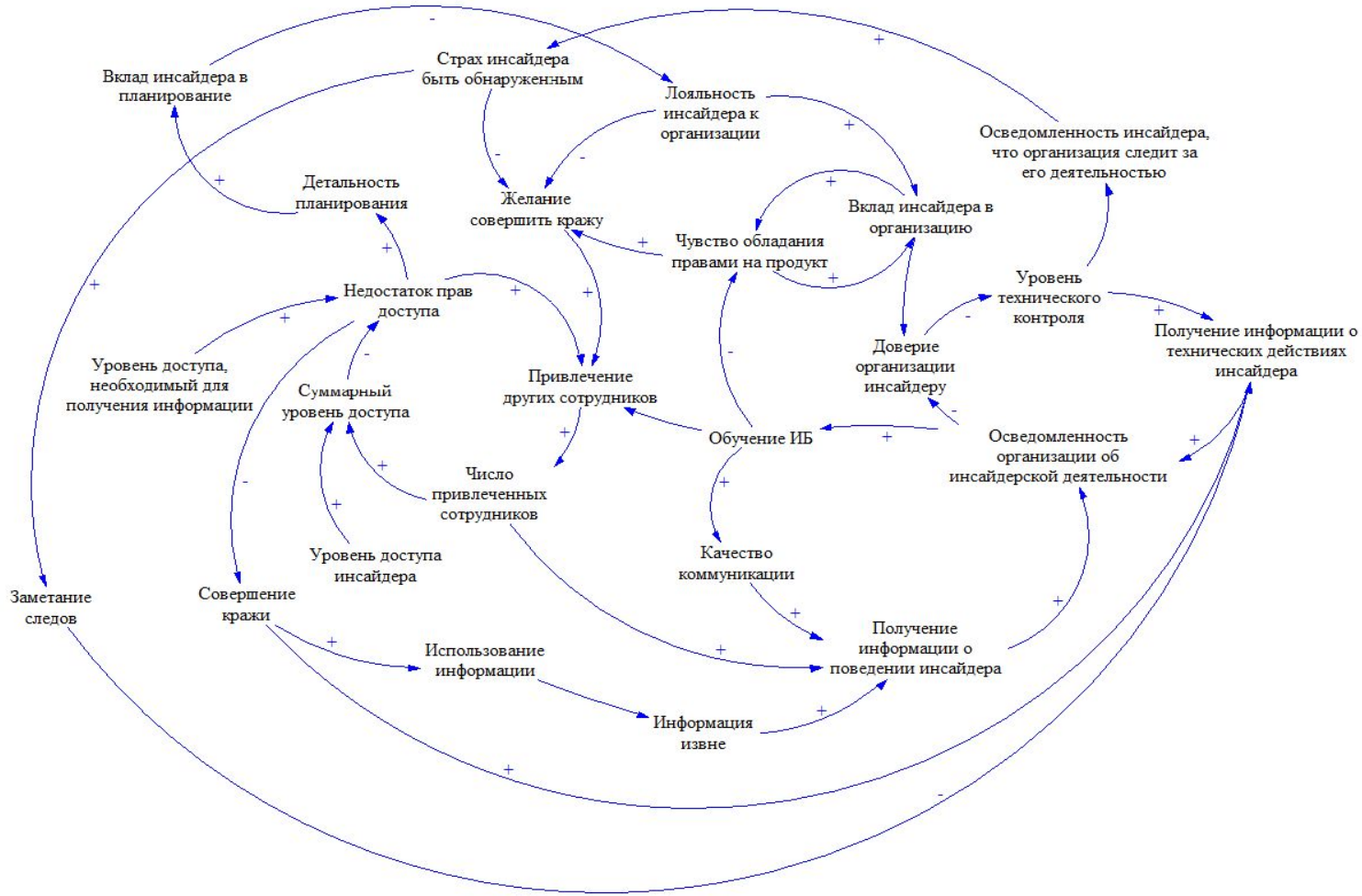
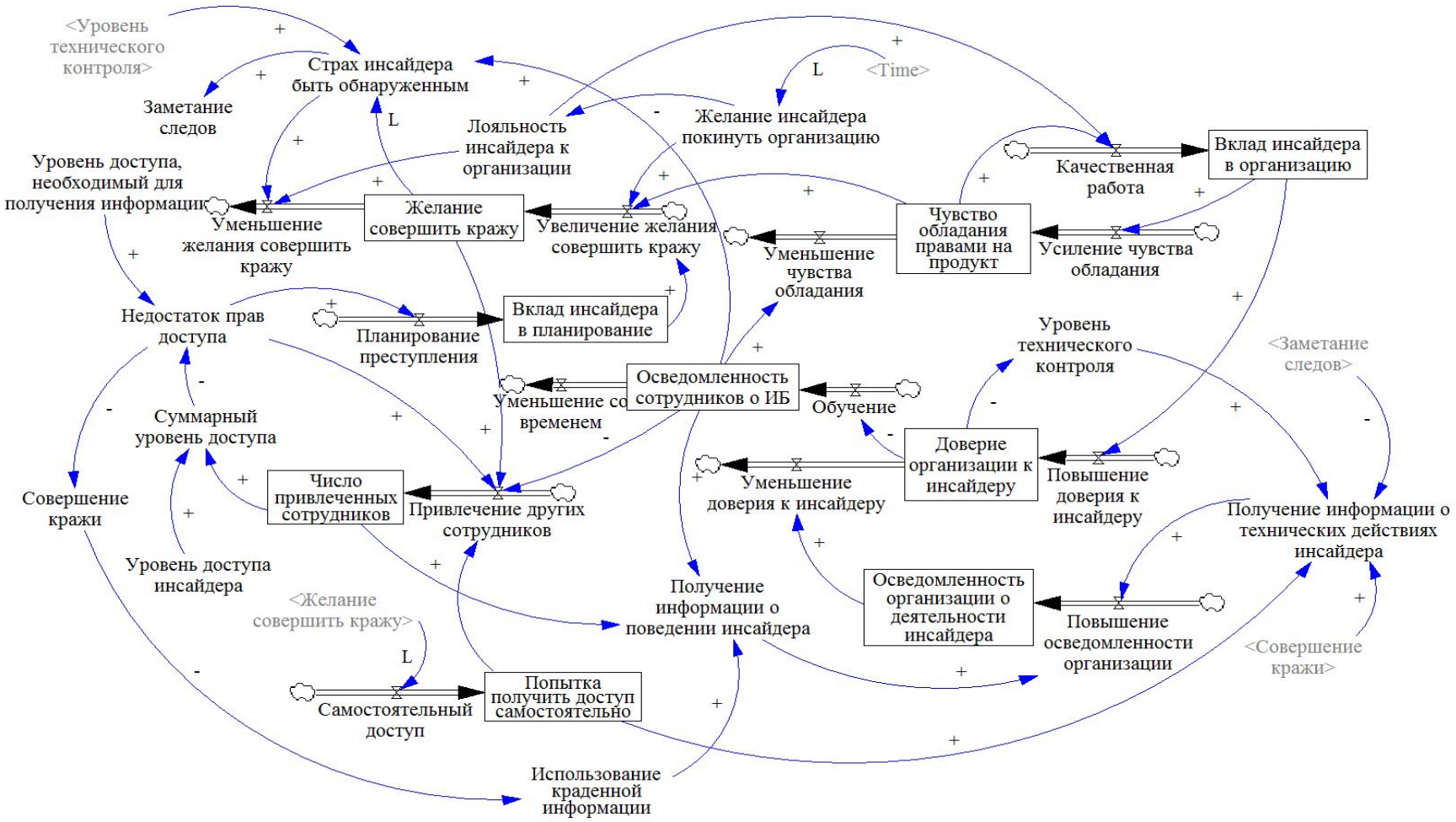
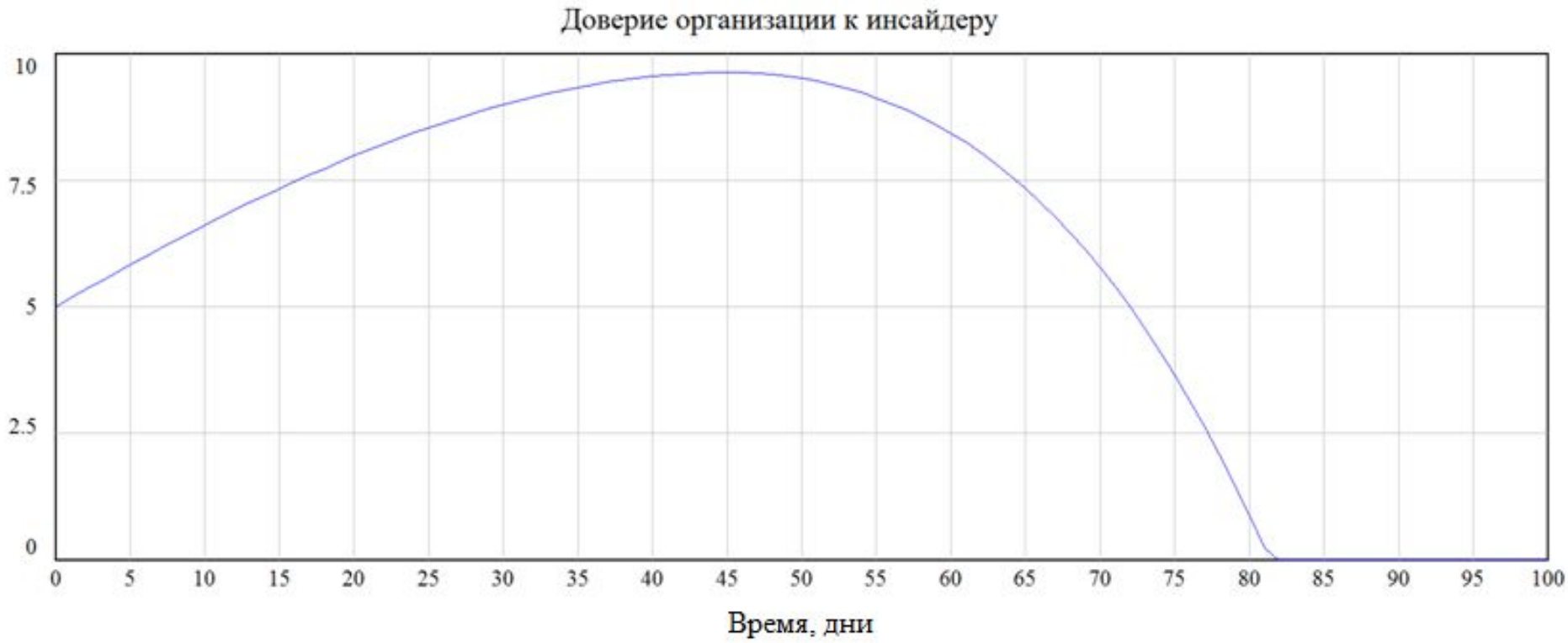


Диаграмма потоков (кража с соучастниками)



Эксперимент: график (кража с соучастниками)



Желание инсайдера покинуть организацию: 30 день моделирования
Попытка получить доступ самостоятельно: 33 день моделирования

Комплексная система защиты информации

Комплексная защита информации

Политика безопасности

1

Стратегия защиты информации

2

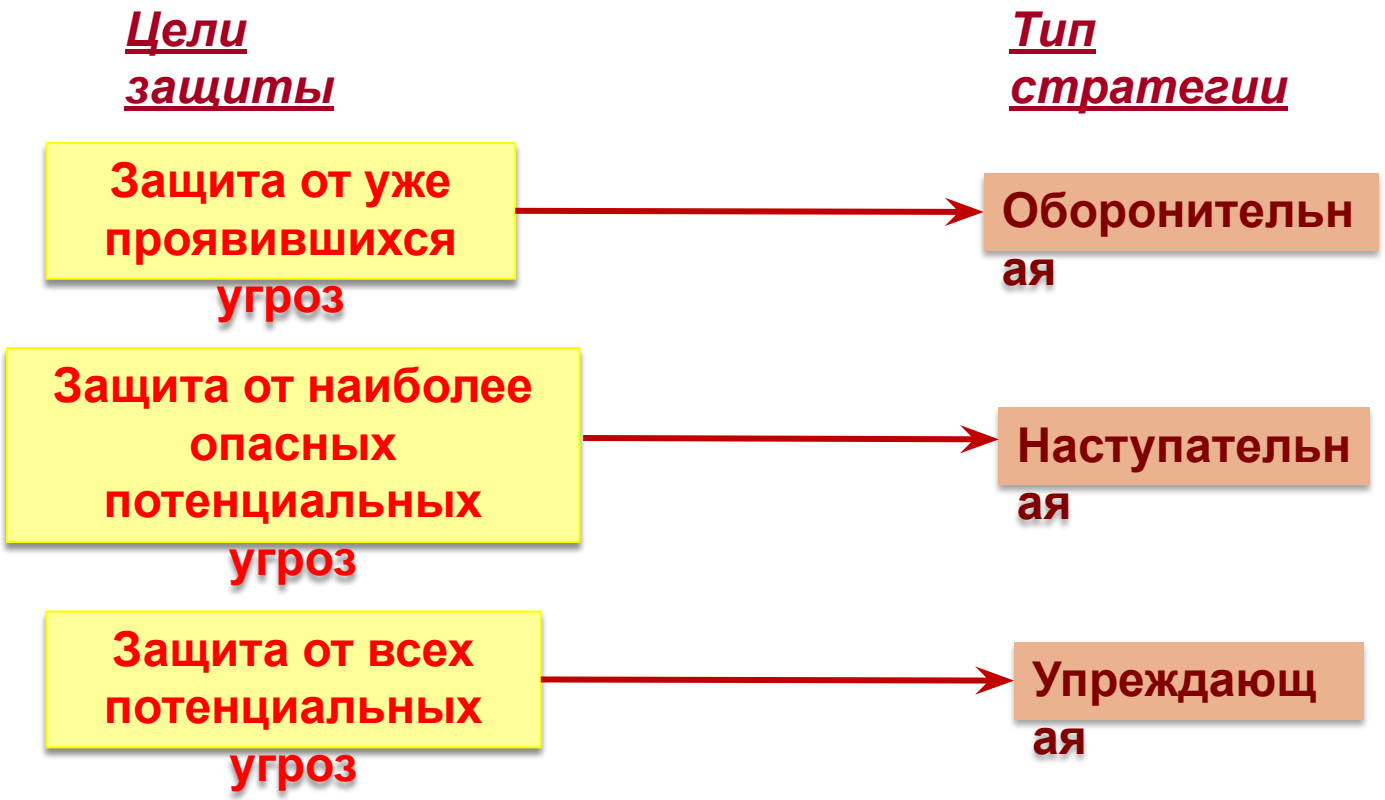
Концепция защиты информации

Стратегия защиты информации

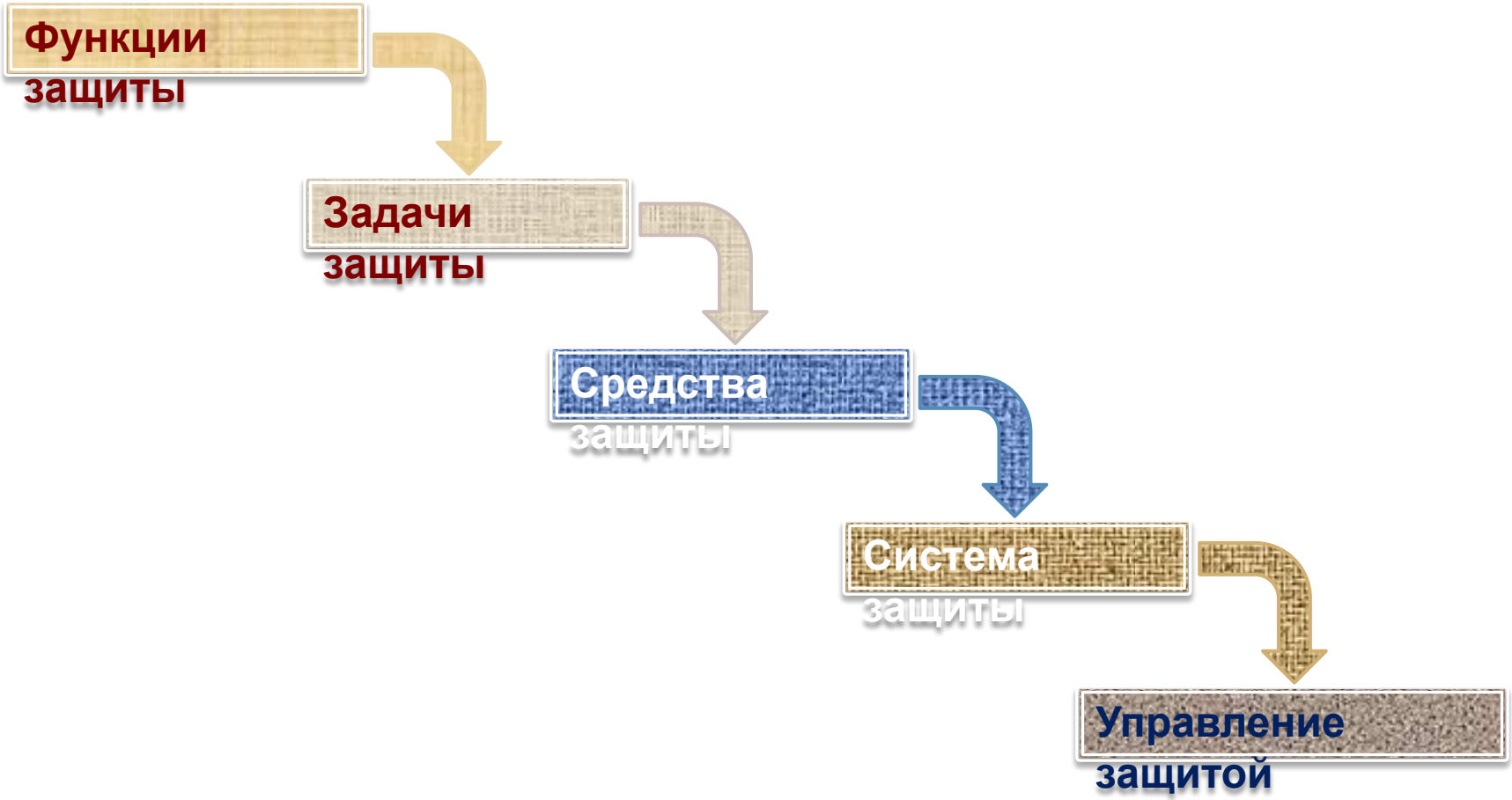
Определение

СТРАТЕГИЯ – общая, рассчитанная на перспективу, руководящая установка при организации и обеспечении соответствующего вида деятельности, направленная на то, чтобы наиболее важные цели этой деятельности достигались при наиболее рациональном расходовании имеющихся ресурсов

Стратегия защиты информации



Концепция защиты информации

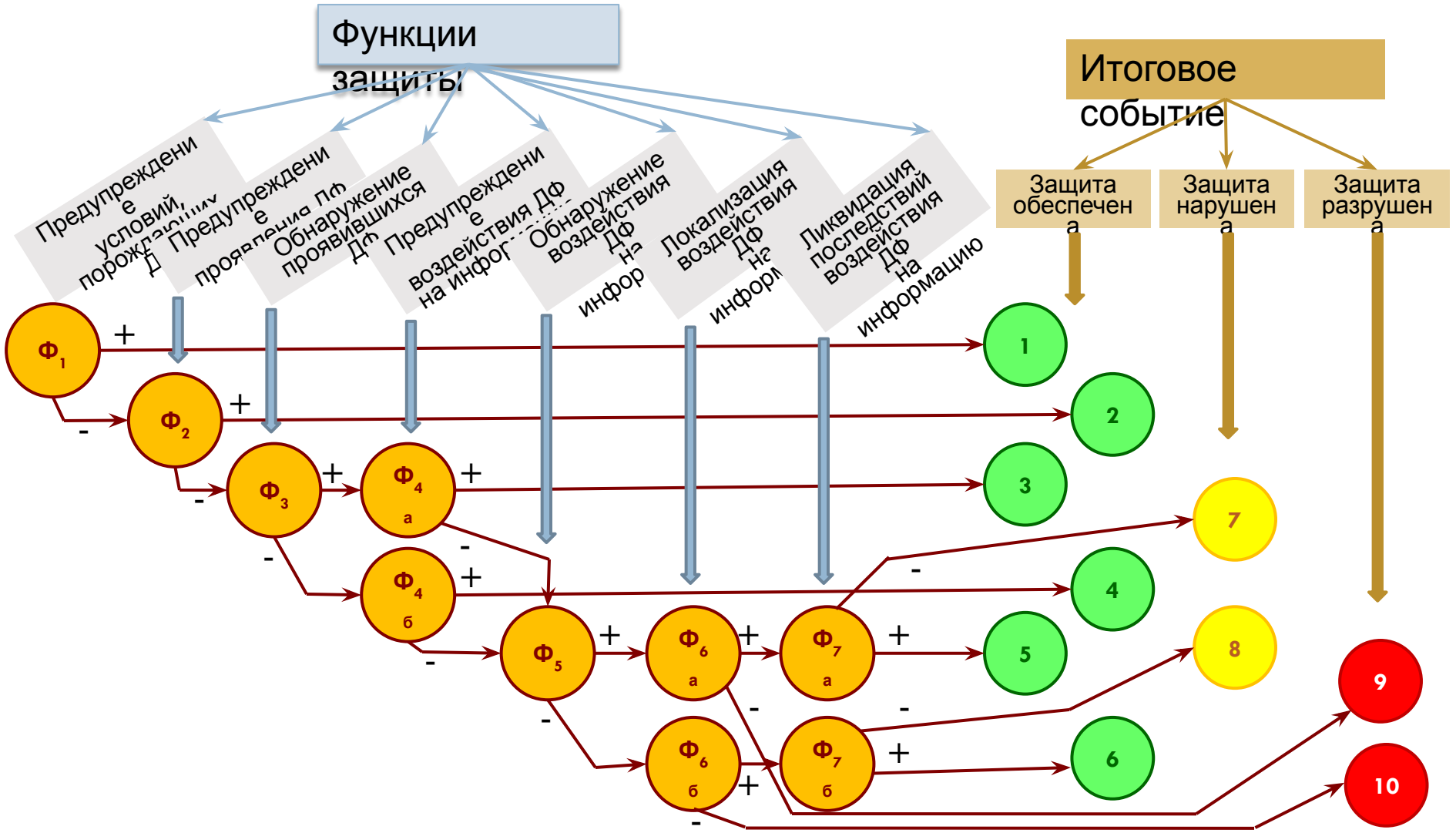


Функции защиты информации

Определение

Функция защиты – совокупность однородных в функциональном отношении мероприятий, регулярно осуществляемых в АС различными средствами и методами, с целью создания, поддержания и обеспечения условий, объективно необходимых для надежной защиты информации

Функции защиты информации



Функции защиты информации

Исходы → Полная группа несовместных событий → $P_u = \sum_{m=1}^{10} P_m^{(u)} = 1$

Благоприятные исходы → Требуемый уровень защиты → $P_з = \sum_{m=1}^{6} P_m^{(u)}$

Функции защиты информации

$$P_1^{(u)} = P_1^{(ф)};$$

$$P_2^{(u)} = (1 - P_1^{(ф)})P_2^{(ф)};$$

$$P_3^{(u)} = (1 - P_1^{(ф)})(1 - P_2^{(ф)})P_3^{(ф)}P_{4а}^{(ф)};$$

$$P_4^{(u)} = (1 - P_1^{(ф)})(1 - P_2^{(ф)})(1 - P_3^{(ф)})P_{4б}^{(ф)};$$

$$P_5^{(u)} = (1 - P_1^{(ф)})(1 - P_2^{(ф)})[P_3^{(ф)}(1 - P_{4а}^{(ф)}) + (1 - P_3^{(ф)})(1 - P_{4б}^{(ф)})](1 - P_5^{(ф)})P_{6б}^{(ф)}P_{7б}^{(ф)};$$

$$P_6^{(u)} = (1 - P_1^{(ф)})(1 - P_2^{(ф)})[P_3^{(ф)}(1 - P_{4а}^{(ф)}) + (1 - P_3^{(ф)})(1 - P_{4б}^{(ф)})P_5^{(ф)}P_{6а}^{(ф)}P_{7а}^{(ф)}]$$

Функции защиты информации

$$P_з = P_1^{(ф)} + (1 - P_1^{(ф)})P_2^{(ф)} + (1 - P_1^{(ф)})(1 - P_2^{(ф)})P_3^{(ф)}P_{4а}^{(ф)} +$$

$$+ (1 - P_1^{(ф)})(1 - P_2^{(ф)})[P_3^{(ф)}(1 - P_{4а}^{(ф)}) +$$

$$+ (1 - P_3^{(ф)})(1 - P_{4б}^{(ф)})P_5^{(ф)}P_{6а}^{(ф)}P_{7а}^{(ф)})] +$$

$$+ (1 - P_1^{(ф)})(1 - P_2^{(ф)})[P_3^{(ф)}(1 - P_{4а}^{(ф)}) +$$

$$+ (1 - P_3^{(ф)})(1 - P_{4б}^{(ф)})](1 - P_5^{(ф)})P_{6б}^{(ф)}P_{7б}^{(ф)}) +$$

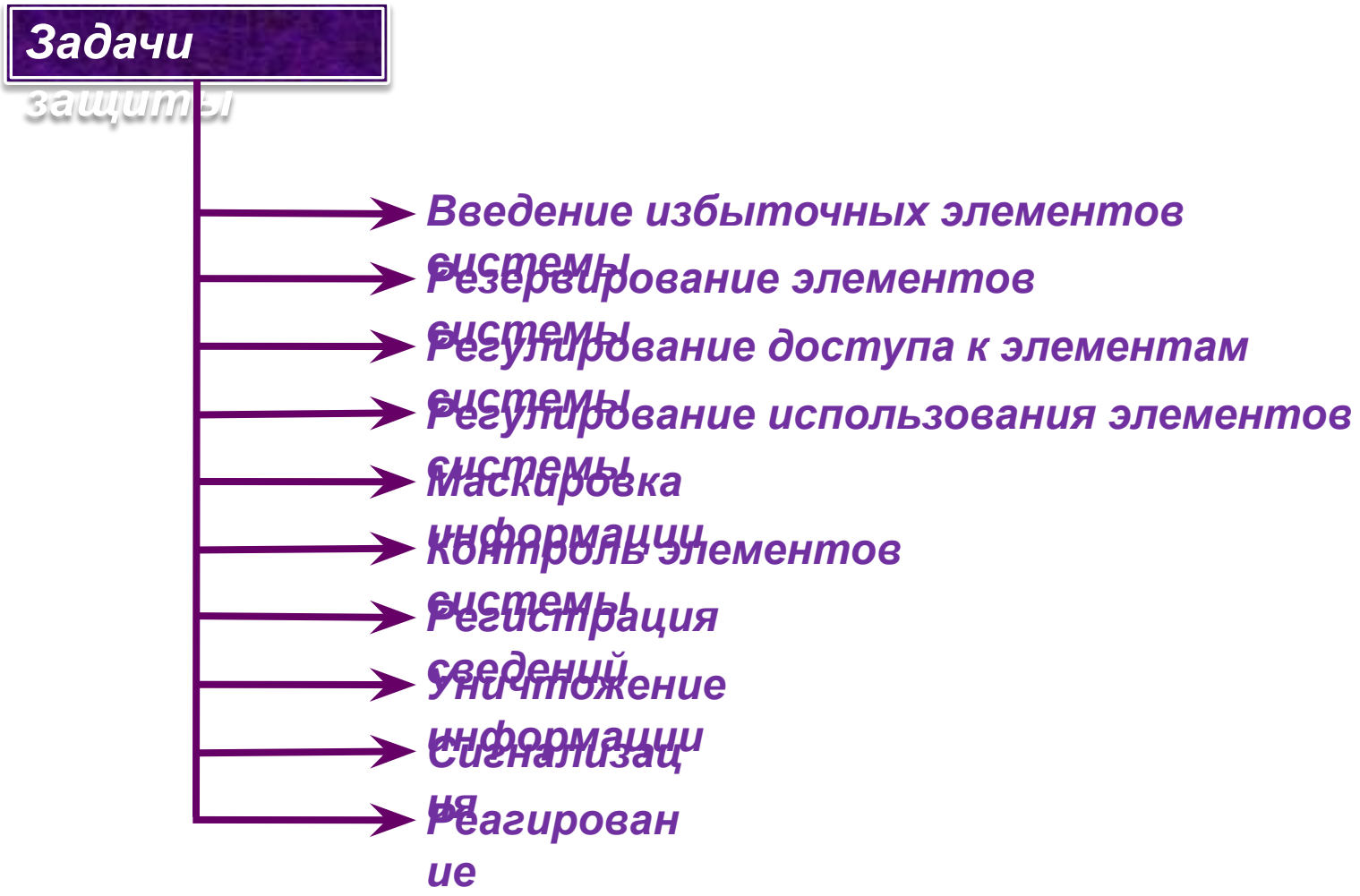
$$+ (1 - P_1^{(ф)})(1 - P_2^{(ф)})(1 - P_3^{(ф)})P_{4б}^{(ф)}$$

Задачи защиты информации

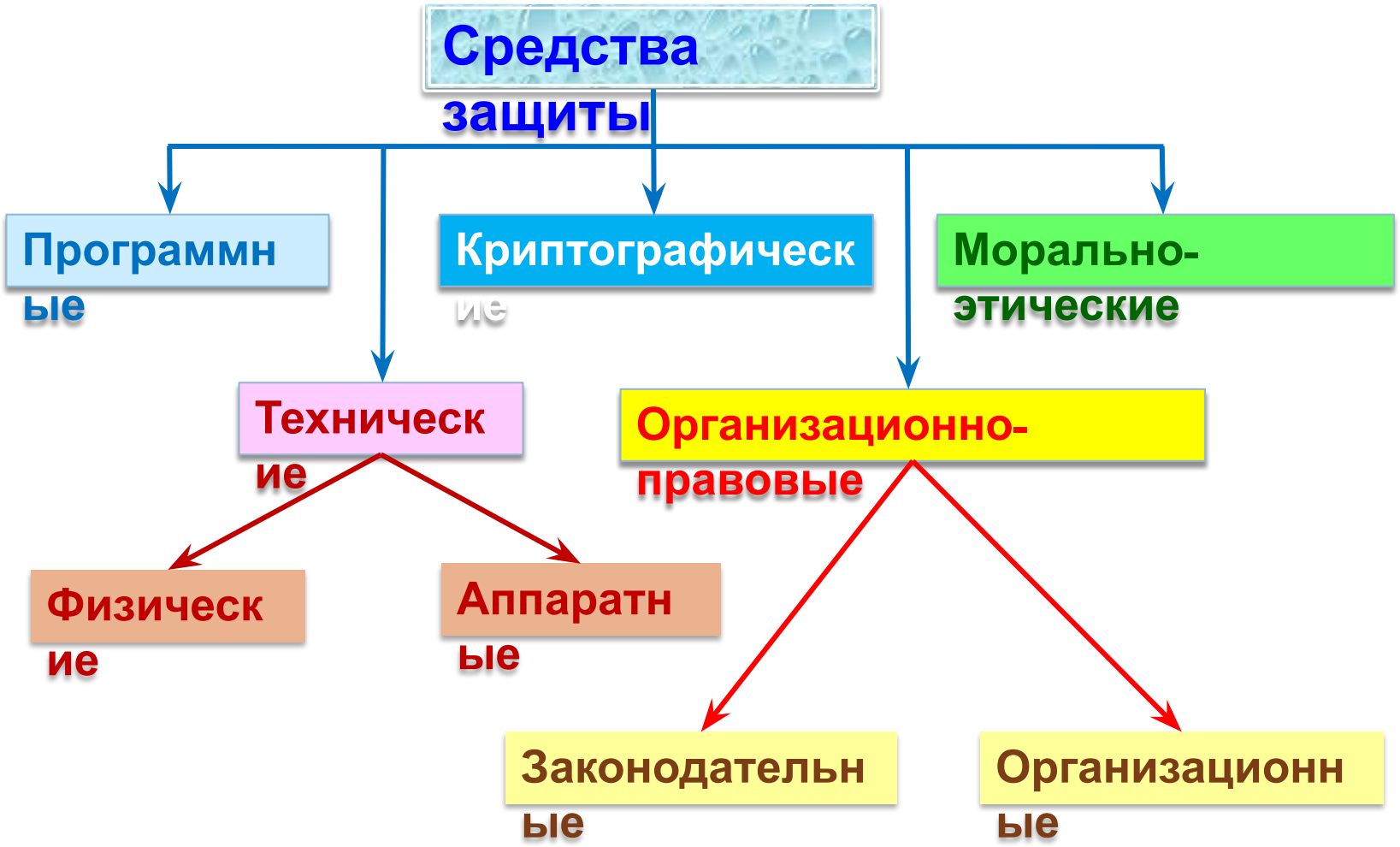
Определение

Задача защиты – организованные возможности средств, методов и мероприятий, осуществляемых в автоматизированной системе с целью полной или частичной реализации одной или нескольких функций защиты

Задачи защиты информации



Средства защиты информации



Система защиты информации

Определение

Система защиты – организованная совокупность всех средств, методов и мероприятий, выделяемых (предусматриваемых) в АС для решения в ней выбранных задач защиты

Система защиты информации

Требования к системе защиты

Концептуальные	**Адаптируемость (способность к целенаправленному приспособлению при изменении структуры, технологических схем или условий функционирования АС)**
Функциональные	**Обеспечение решения требуемой совокупности задач защиты, удовлетворение всем требованиям защиты**
Эргономические	**Минимизация помех пользователям, удобство для персонала системы защиты информации**
Экономические	**Минимизация затрат на систему, максимальное использование стандартных серийных средств**
Технические	**Комплексное использование средств защиты, оптимизация архитектуры**
Организационн	**Структурированность всех компонентов, простота эксплуатации**

Система защиты информации

Проектирование оптимальной системы защиты

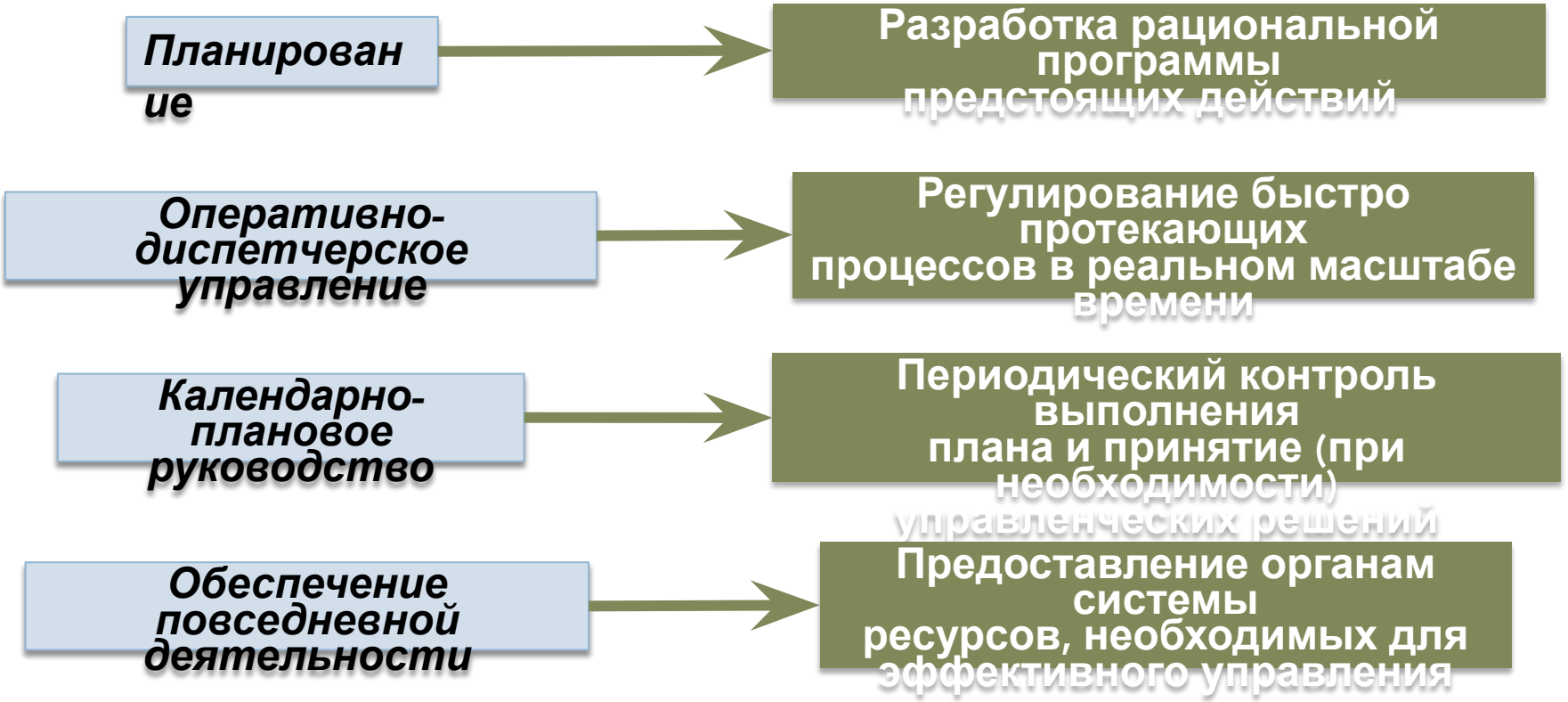
1. **Обеспечение максимального уровня защищенности при ограниченных ресурсах**

ИЛИ

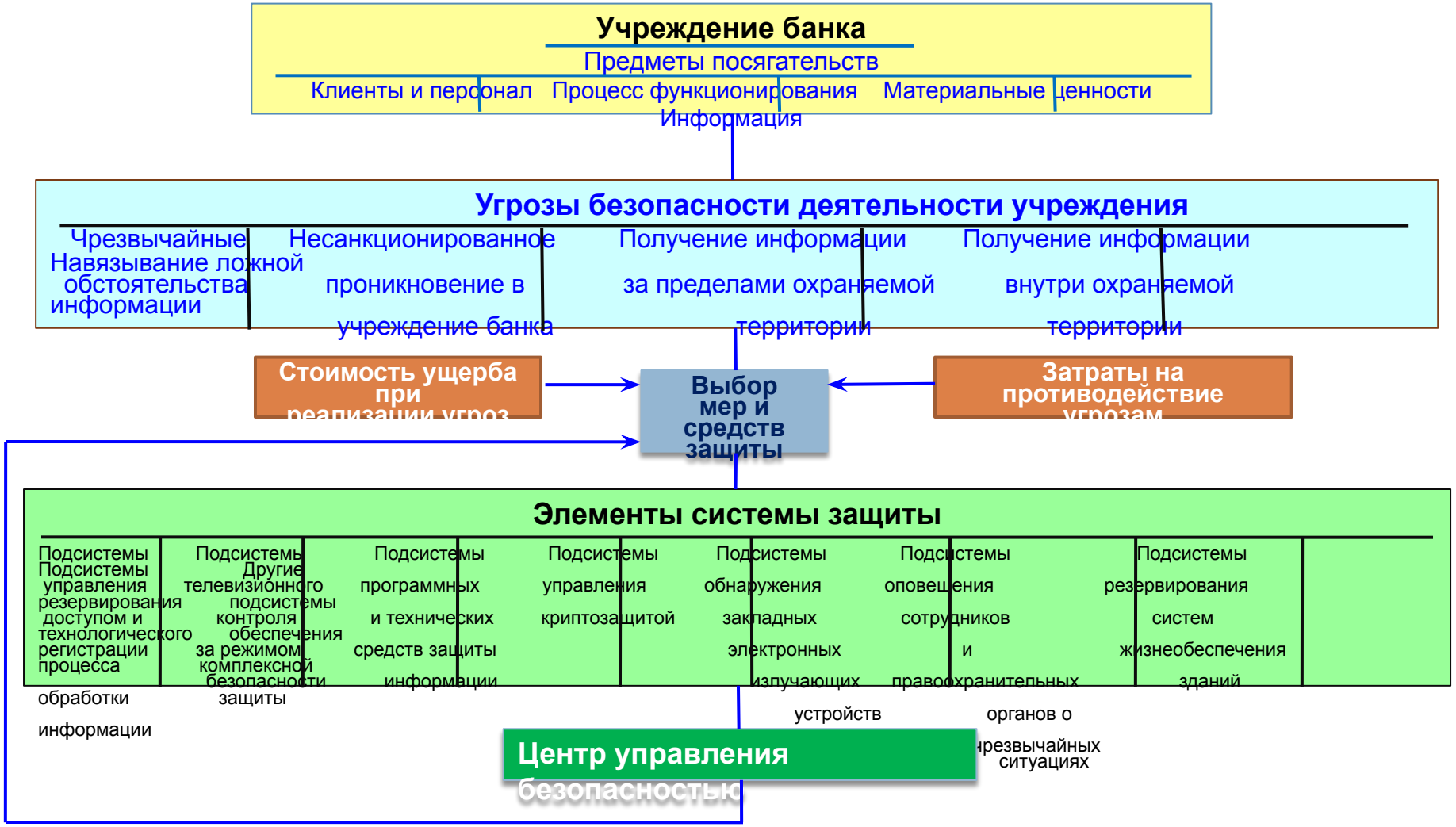
2. **Обеспечение заданного уровня защищенности при минимальных ресурсах**

Управление защитой информации

Макропроцессы управления



Система информационной безопасности банка



Задания для самостоятельной работы

1. Почему, на ваш взгляд, действительно эффективная защита информации может быть обеспечена только при комплексном системном подходе к решению этой проблемы? В чем заключается комплексность? Каким требованиям должна удовлетворять концепция комплексной защиты?

2. Сформулируйте основные концептуальные положения теории защиты информации.

3. Раскройте содержание функции защиты информации. Какие из функций образуют полное множество функций защиты?

4. Сформулируйте определение задачи защиты информации и попытайтесь назвать десять классов задач, образующих репрезентативное множество задач защиты.

5. Приведите наиболее распространенную на сегодняшний день

Задания для самостоятельной работы

6. Дайте определение системы защиты информации и сформулируйте основные концептуальные требования, предъявляемые к ней.

7. Раскройте содержание концепции управления системой защиты информации. Каковы ее особенности по сравнению с общей концепцией управления системами организационно-технологического типа?

Тестовый контроль 2

1. В чем заключается различие систем распределения ключей шифрования с центром
трансляции ключей (ЦТК) и с центром распределения ключей (ЦРК)?
1) В системе ЦРК ключ данных вырабатывает центр, а в системе ЦТК – вызывающий
абонент.
2) В системе ЦТК все абоненты имеют индивидуальные ключи связи с центром,
а в системе ЦРК ключ связи с центром – общедоступный.
3) В системе ЦТК используется один ключ, а в системе ЦРК – два ключа.

Ответ: 1

2. Активная защита – это ... утечки информации по каналу ПЭМИН.
Закончите фразу.
1) Размещение всего оборудования в экранирующей радиоизлучения среде.
2) Экранирование отдельных компонентов защищаемых систем, а также
применение в линиях связи и питания различных фильтров, устройств
подавления сигналов и развязки.
3) Сокрытие информационных сигналов за счет шумовой или заградительной

Ответ: 3

Тестовый контроль 2

3. Одним из основных требований, предъявляемых к системе защиты информации,
являются функциональные требования, сущностью которых является …
Закончите фразу.
1) Обеспечение решения требуемой совокупности задач защиты, удовлетворение
всем требованиям защиты.
2) Комплексное использование средств защиты, оптимизация архитектуры.
3) Структурированность всех компонентов, простота эксплуатации.

Ответ: 1

4. Пассивная защита от утечки информации по каналу ПЭМИН – это …
Закончите фразу.
1) Изменение вероятностной структуры сигнала, который может быть принят
злоумышленником.
2) Сокрытие информационных сигналов за счет шумовой или заградительной
помехи с помощью специальных генераторов шума.
3) Применение в линиях связи и питания различных фильтров, устройств
подавления сигналов и развязки

Ответ: 3

Тестовый контроль 2

5. Кто вырабатывает ключ данных в централизованной системе распределения
ключей шифрования, построенной на основе центра трансляции ключей?

1) Вызывающий абонент.
2) Вызываемый абонент.
3) Центр трансляций ключей.

Ответ:
1

6. Какие из перечисленных ниже устройств могут быть использованы для пассивного обнаружения электронного контроля речи?

1) Генераторы аудиопомех.
2) Электронные стетоскопы.
3) Нелинейные локаторы.
4) Лазерные детекторы.

Ответ:
3

Тестовый контроль 2

7. Технические средства защиты информации – это: …
Закончите фразу.
1) Механические, электрические, электромеханические, электронные, электронно-механические и тому подобные устройства и системы, которые функционируют автономно, создавая различного рода препятствия на пути дестабилизирующих факторов.
2) Различные электронные, электронно-механические и тому подобные устройства, встраиваемые в аппаратуру автоматизированной системы или сопрягаемые с ней специально для решения задач защиты информации.

Ответ:
1,2

8. Кто вырабатывает ключ данных в централизованной системе распределения ключей шифрования, построенной на основе центра распределения ключей?
1) Вызывающий абонент.
2) Вызываемый абонент.
3) Центр распределения ключей.

Ответ:
3

Тестовый контроль 2

9. Какой из перечисленных ниже методов не применяется для защиты
конфиденциальной информации в каналах связи?
1) Использование нелинейных локаторов.
2) Использование аналогового скремблирования.
3) Использование дискретизации с последующим шифрованием.

Ответ:
1

10. Можно ли использовать криптосистему с общедоступным ключом
для доведения до абонентов ключа шифрования ключей в децентрализованной системе распределения ключей?
1) Можно.
2) Нельзя.
3) Можно в отдельных случаях.

Ответ:
1

Успешной сдачи зачета!