“Безопасность есть предотвращение зла”
Платон, определения, стих 415

Основные понятия информационной безопасности и направления деятельности в области защиты информации

Рытов Михаил Юрьевич,
канд. техн. наук, доцент
rmy@tu-bryansk.ru
(4832) 51-13-77

Вопросы:

1. История развития проблемы защиты информации
2. Сущность и основные понятия информационной безопасности
3. Виды угроз информационной безопасности РФ
4. Источники угроз информационной безопасности РФ
5. Задачи обеспечения информационной безопасности в различных сферах деятельности
6. Обзор современных методов и средств защиты информации

1. История развития проблемы защиты информации

Хронология
процесса развития средств и методов защиты информации
(по эволюции видов носителей информации)

П е р в ы й э т а п
(древность – XIX в)

- связан с появлением возможности фиксации информационных сообщений на твердых носителях, то есть **с изобретением письменности.**

- определяется началом создания осмысленных и самостоятельных средств и методов защиты информации таких как как **шифрование и скрытие.**

Второй этап

(примерно с середины XIX в – 40 г.г. XX в)

- характеризуется появлением **технических средств обработки информации** и возможностью сохранения и передачи сообщений с помощью таких носителей, как электрические сигналы и электромагнитные поля (телефон, телеграф, радио)

- возникли проблемы защиты от так называемых технических каналов утечки (побочных излучений, наводок и др.)

- появились способы шифрования сообщений в реальном масштабе времени (в процессе передачи по телефонным и телеграфным каналам связи) и т. д.

- это период активного развития технических средств разведки, многократно увеличивающих возможности ведения промышленного и государственного шпионажа. Огромные, все возрастающие убытки предприятий и фирм способствовали научно-техническому прогрессу в создании новых и совершенствовании старых средств и методов защиты информации.

Третий этап

(середина XX в.-н.в.)

период массовой информатизации общества

- связан с внедрением автоматизированных систем обработки информации
- внимание к проблеме защиты информации в первую очередь было вызвано все возрастающими финансовыми потерями фирм и государственных организаций от преступлений в компьютерной сфере
- выводы западных экспертов показывают, что утечка 20% коммерческой информации в шестидесяти случаях из ста приводит к банкротству фирмы
- все большие финансовые потери приносят вирусные атаки на компьютерные сети. Так, запущенный через электронную Интернет в мае 2000 г. вирус «I love you» вывел из строя свыше 5 млн. компьютеров и нанес ущерб свыше 10 млрд. долларов

Начальный этап
(60-е — начало 70-х гг.)

характеризовался тем, что под защитой информации понималось предупреждение несанкционированного ее получения лицами, не имеющими на то полномочий.

Для этого использовались формальные (то есть функционирующие без участия человека) средства. Наиболее распространенными в автоматизированных системах обработки данных (АСОД) были проверки по паролю прав на доступ к ЭВТ и разграничение доступа к массивам данных. Эти механизмы обеспечивали определенный уровень защиты, однако проблему в целом не решали, поскольку для опытных злоумышленников не составляло большого труда найти пути их преодоления.

Для объектов обработки конфиденциальной информации задачи по ее защите решались в основном с помощью установления так называемого режима секретности, определяющего строгий пропускной режим и жесткие правила ведения секретного документооборота.

Этап развития
(70-е — начало 80-х гг.)

отличается **интенсивными поисками, разработкой и реализацией** способов и средств защиты и определяется следующими характеристиками:

- постепенным осознанием необходимости комплексирования целей защиты

- расширением арсенала используемых средств защиты, причем как по их количеству, так и по их разнообразию. Повсеместное распространение получило комплексное применение технических, программных и организационных средств и методов. Широко стала практиковаться защита информации путем **криптографического ее преобразования**. Стали разрабатываться методы и средства защиты информации на основе **биометрических параметрах человека** (по голосу, почерку, форме руки, отпечаткам пальцев, подписи и т.д.)

- целенаправленным объединением всех применяемых средств защиты в функциональные самостоятельные системы

- нарастание количества средств защиты и принимаемых мер привело в конечном итоге **к проблеме эффективности системы защиты информации**, учитывающей соотношение затраченных на ее создание средств к вероятным потерям от возможной утечки защищаемой информации. Для проведения такой оценки стали применять основные положения теории оценки сложных систем.

- к концу второго периода математически **было доказано**, что обеспечить **полную безопасность информации** в системах ее обработки **невозможно**. Максимально приблизиться к этому уровню можно, лишь решая задачу комплексной защиты информации, опираясь на научно-методологические положения и на хороший инструментарий в виде методов и средств решения соответствующих задач.

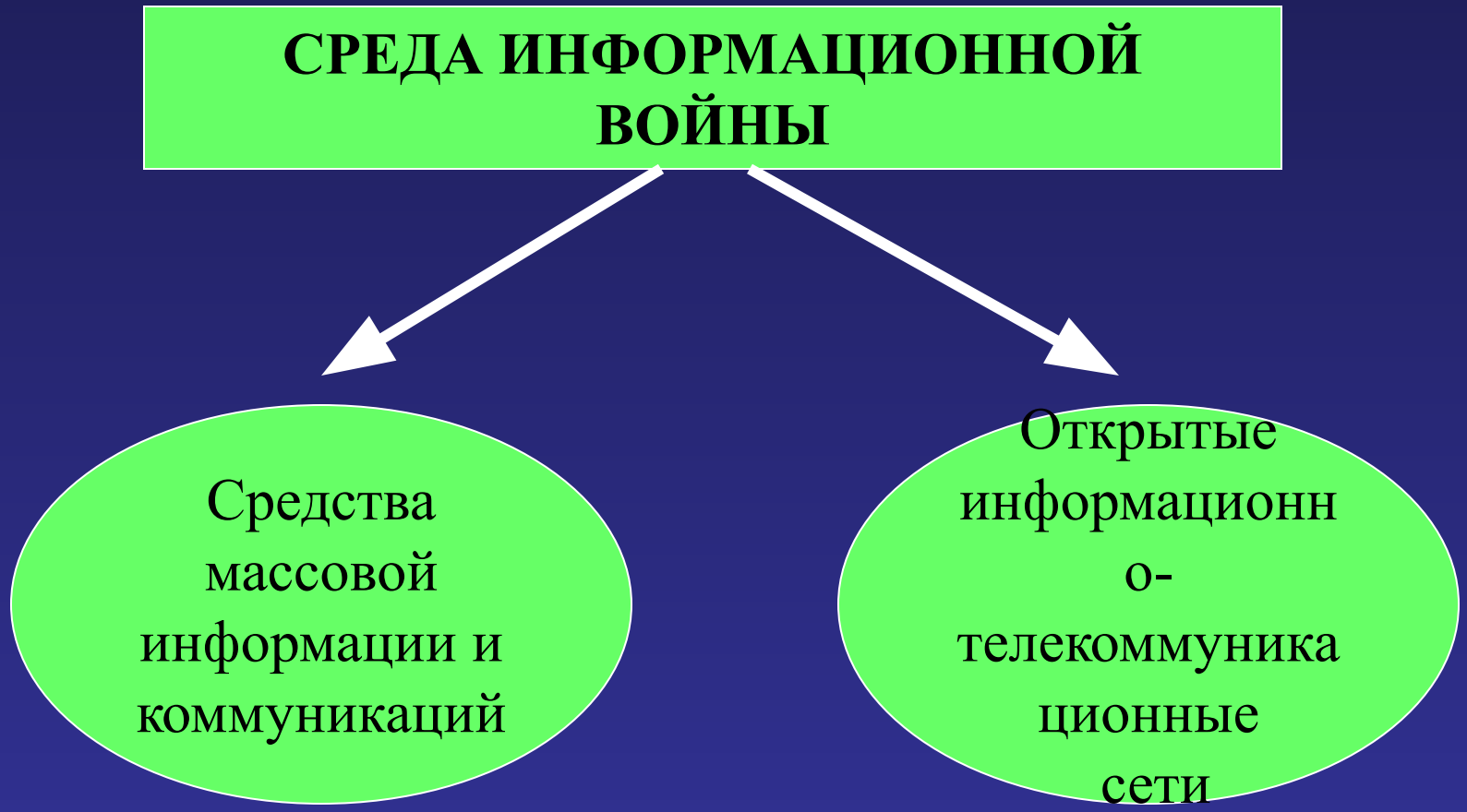
Современный этап
(с середины 80-х гг. по н.в.)

характерной особенностью третьего, *современного этапа* комплексной защиты, являются попытки аналитической обработки данных всего имеющегося опыта теоретических исследований и практического решения задач защиты и формирования на этой основе научно-методологического базиса защиты информации.

Основной задачей третьего этапа является перевод процесса защиты информации на строго научную основу.

В настоящее время в России традиционно развивается криптографическое направление защиты информации. Кроме того, свыше 60 вузов занимаются разработкой теоретических подходов к решению проблемы защиты информации, практических методов и средств информационной безопасности, а также подготовкой специалистов по защите информации.

Характеристика среды, в которой проводятся операции информационной войны



Историческая справка

Информационно –психологическое воздействие

Объект воздействия XX век

- Территория;
- Экономический
- потенциал;
- ВС;
- Финансы.

Объект воздействия XX I век

Активное развитие ИТ и ТКС

- Человек – личность;
- Информация;
- Технические средства

Термин «информационная война» (ИВ) появился приблизительно в середине семидесятых годов XX века. На Западе отцом термина «информационная война» называют ученого-физика Томаса Рона, который в 1976 (разгар холодной войны) назвал информацию самым слабым звеном вооруженных сил и обороны.

В настоящее время накоплен и систематизирован опыт ведения ИВ, разработаны планы проведения операций и использования средств и методов ИВ.

Государство:

- формирует стратегию и тактику ИВ в соответствии со своими интересами;
- использует средства и методы ИВ для распространения политических, религиозных, военных и экономических взглядов, межличностных отношений;
- осуществляет долговременные широкомасштабные мероприятия в регионах, являющихся территорией других государств;
- проводит информационно-психологические операции по формированию условий принятия зарубежными странами навязываемых политических, военных и экономических решений.
- применяет средства и методы ИВ в политической борьбе и экономической конкуренции.

Определение информационной войны

ИВ рассматривают как новую форму борьбы двух и более сторон, которая состоит в целенаправленном использовании специальных средств и методов влияния на информационные ресурсы противника, а также защиты собственного информационного ресурса для достижения назначенных целей.

В настоящее придерживаются следующего определения: информационная война - **это открытые и скрытые целенаправленные информационные воздействия социальных, политических, этнических и иных систем друг на друга с целью получения определенного выигрыша в материальной сфере.**

ИВ также можно определить как комплекс мероприятий и операций, проводимых ВС государств и другими (как правительственными, так и частными) организациями, направленных на обеспечение информационного превосходства над противником и нанесения ему материального, идеологического или иного ущерба. В ИВ информация является одновременно оружием, ресурсом и целью.

Основные различия между войной информационной и традиционной

- Обычная война обладает четким арсеналом воздействия. Из-за его предсказуемости возможно построение в ответ определенного рода оборонительных систем и проведение защитных мероприятий. В большинстве случаев в ИВ отсутствует возможность предугадать направление и инструментарий возможной атаки.
- В случае обыкновенной войны территория захватывается полностью, тогда как при ИВ возможен поэтапный захват.
- В обыкновенной войне те, кто захватывает территорию, и те, кто потом ее осваивает, являются разными людьми и выполняют разные социальные роли. В случае ИВ эти позиции совпадают. ИВ во многом стирает четкое разграничение типа «друг/враг». Можно считать кого-то союзником, хотя на самом деле он является врагом.
- В отличие от обычной войны, применяемое в которой физическое оружия разрушает в пределах зоны поражения все, информационное оружие действует избирательно, охватывая по-разному различные слои населения.
- **Главной опасностью ИВ** является отсутствие четко видимых признаков разрушительного воздействия, характерного для войн обычных. Население даже не ощущает, что оно подвергается воздействию. В результате общество не приводит в действие имеющиеся в его распоряжении защитные механизмы. Чувство опасности, которое в иных ситуациях действует безотказно, в данном случае не срабатывает.

Классификация видов информационного оружия

1. **Средства борьбы с системами управления противника (command and control warfare - CW);**
2. **Средства борьбы на основе разведывательной технологии (intelligence-based warfare-IBW);**
3. **Электронные средства борьбы;**
4. **Психологические средства ведения войны;**
5. **Экономические средства информационной борьбы (economic information warfare - EW);**
6. **Хакеры как вид информационного оружия.**

Концепции информационных войн в развитых зарубежных странах

На сегодняшний день у большинства развитых стран мира уже сформировались достаточно полные и непротиворечивые собственные системы взглядов в отношении использования информационно-психологической войны в качестве инструмента внешней политики.

Так как в настоящее время информационное общество еще не выработало эффективный способ противодействия информационно-психологической войны и подавления ее источников, использование арсенала сил, средств и методов информационно-психологического воздействия носит агрессивный характер практически повсеместно.

1.1. США

Концепция ИВ США

Государственный уровень

Цель:

- доступ к закрытым информационным ресурсам государства-конкурента и принуждение его принять выгодные США решения;
- защита собственных информационных ресурсов.

Основные формы реализации:

- политические, дипломатические и экономические акции и информационно-психологические операции;
- подрывные и деморализующие пропагандистские действия;
- содействие оппозиционным и диссидентским движениям;
- проникновение в систему государственного управления;
- оказание всестороннего влияния на культурную и политическую жизнь с задачей развала национально-государственных устоев общества;
- защита национальных информационных систем.

Военный уровень

Цель:

- Достижение информационного господства над противником в вооруженном конфликте;
- Защита собственных систем управления от ИО противника

Основные формы ИВ:

- радиоэлектронная борьба;
- психологическая война;
- воина с использованием средств разведки, в т.ч. с использованием Интернет;
- война с использованием потенциала хакеров;
- кибернетическая война.

1.2. Евросоюз

Направления работ по обеспечению ИБ ЕС:

- **Создание спецпдразделений в странах ЕС для отражения информационной агрессии** (функции-выявление и нейтрализация угрозы нападения, защита и восстановление собственных систем);
- **Выявление скрытых методов информационно-психологического воздействия на личность;**
- **Организация безопасного обмена данными в единой ТКС Европы;**
- **Создание системы коллективного контроля и обеспечения ИБ в Европе;**
- **Принятие директив о юридической защите информационных массивов и авторства;**
- **Создание странами Европы международной договорно - правовой базы обеспечения безопасности и создание системы многополюсной системы контроля для ограничения влияния США.**

1.3. Германия

Основные положения концепции ИВ Германии:

- Антимонополизация в сфере информационно-коммуникационных услуг;
- Деятельность ФСБ в сфере информационной техники в направлении оценки риска внедрения ИТ, разработки критериев и методов оценки ИС, выдачи лицензий и сертификатов на виды деятельности в сфере ИБ;
- Разработка технологий надежной защиты от вмешательства спецсплужб противника путем создания и развития собственных независимых от США ТКС, оснащенных средствами национального производства.

1.4. Франция

Основное направление работ по обеспечению ИБ:

- Создание собственных систем управления и космической связи;
- Развитие и эффективное использование методов шифрования для защиты каналов передачи данных.

1.5. КНР

Основные положения политики КНР, направленной на повышение ИБ и подготовки к ИВ:

- Расширение международного сотрудничества с целью максимально возможного ускорения процесса информатизации государства и развития телекоммуникационной инфраструктуры, систем связи, реализации космических проектов;
- Проведение политики “экономической открытости”;
- Оснащение ВС КНР новейшими средствами РЭБ и информационного противодействия, системами управления, связи и разведки;
- Развитие Центра военных стратегических исследований КНР, занимающегося разработкой стратегии и тактики ведения ИВ;
- Разработка международного механизма, норм и правил международного информационного обмена, исключающих проявление сетевого доминирования;
- Организация и лидерство КНР в борьбе развивающихся стран за “справедливый информационный порядок”;
- Защита собственной интеллектуальной собственности, а также блокирование несанкционированного доступа к “чуждой” зарубежной информации;
- Ограничение распространения в ТКС информации о деятельности госструктур и разработка системы правил доступа различных организаций к зарубежным информационным источникам и системы госконтроля за этими процессами.

2. Сущность и основные понятия информационной безопасности

Информация - сведения (сообщения, данные) независимо от формы их представления.(ФЗ РФ № 149 “Об информации, информационных технологиях и защите информации ” от 27.07.06 г.)

Информация (И) как объект защиты имеет следующие особенности и свойства:

- Информация нематериальна;
- Информация доступна человеку, если она содержится на материальном носителе;
- Ценность информации оценивается степенью полезности ее для пользователя;
- Учитывая, что информация может быть для получателя полезной или вредной, что она покупается и продается, то информацию можно рассматривать как товар;
- Ценность информации изменяется во времени;
- Невозможно объективно оценить количество информации;
- При копировании, не изменяющем информационные параметры носителя, количество информации не меняется, а цена снижается.

Классификация информации по режиму доступа в РФ

Конфиденциальная информация - документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации. По содержанию конфиденциальная информация может иметь профессиональный, коммерческий, служебный, и другой характер.

Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны.

Защита информации – это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

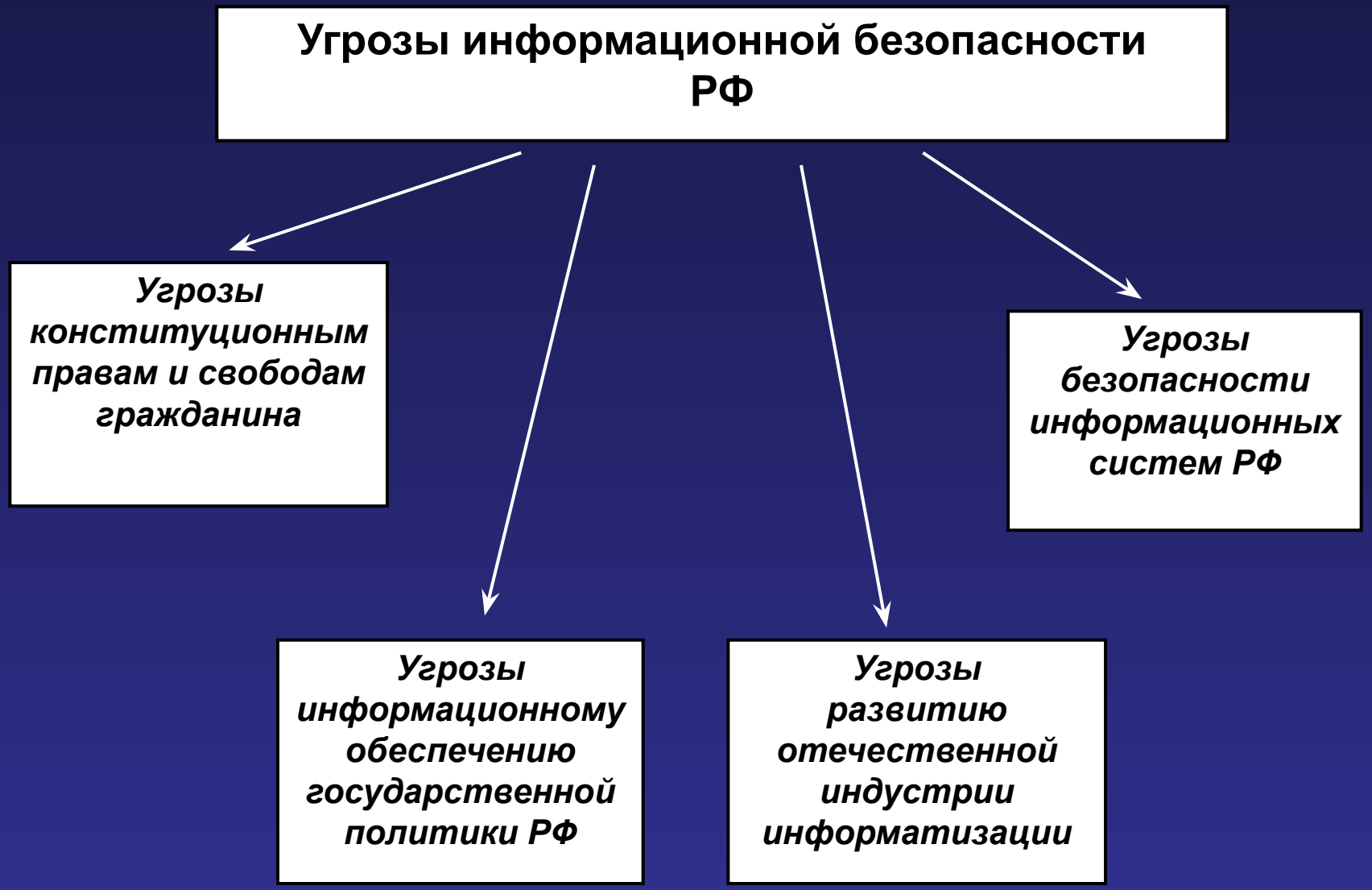
В настоящее время проблема защиты информации рассматривается как проблема **информационной безопасности** – неотъемлемой составной части национальной безопасности РФ. Это определено в Концепции национальной безопасности РФ и Доктриной информационной безопасности РФ.

Информационная безопасность РФ определяется как состояние защищенности её национальных интересов в информационной сфере, определяющихся совокупностью интересов личности, общества и государства.

3. Виды угроз информационной безопасности РФ

Под ***угрозой информационной безопасности*** понимается потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности или секретности информации.

Виды угроз информационной безопасности определены в “Доктрине информационной безопасности Российской Федерации”, утвержденной Президентом РФ 09.09.00. По своей общей направленности угрозы информационной безопасности РФ подразделяются на следующие виды:


Угрозы информационной безопасности РФ
Угрозы конституционным правам и свободам гражданина
Угрозы информационному обеспечению государственной политики РФ
Угрозы развитию отечественной индустрии информатизации
Угрозы безопасности информационных систем РФ

4. Источники угроз информационной безопасности РФ

Источники угроз информационной безопасности РФ подразделяются на внешние и внутренние.

К основным ***внешним источникам*** относятся :

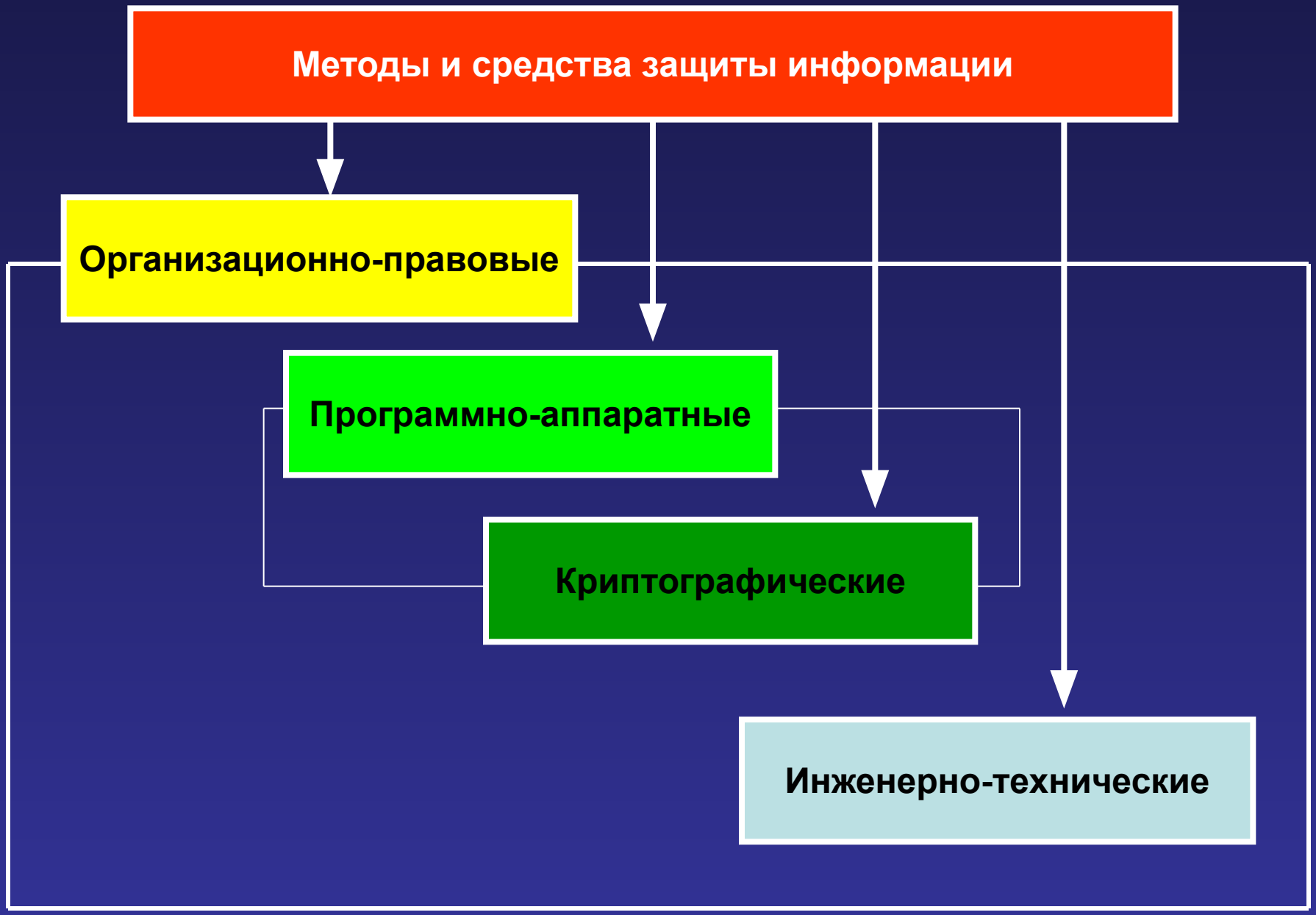
- деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;
- стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;
- увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;
- разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

К наиболее опасным ***внутренним источникам*** относятся :

- критическое состояние отечественных отраслей промышленности;
- неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере;
- недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;
- неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;
- недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;
- недостаточная экономическая мощь государства;
- снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;
- отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

5. Задачи обеспечения информационной безопасности в различных сферах деятельности

6.Обзор современных методов и средств защиты информации


Методы и средства защиты информации
Организационно-правовые
Программно-аппаратные
Криптографические
Инженерно-технические

Правовое регулирование в области защиты информации в РФ

Конституция РФ

Фундаментальная проблема информационного права:

СТАТЬЯ 29 п.4.

Каждый имеет право *свободно искать*, получать, передавать, производить и распространять информацию любым законным способом.

Перечень сведений, составляющих государственную тайну, определяется федеральным законом.

Законодательная база информатизации РФ

ФЗ РФ «О безопасности» от 5.03.92г.

Закрепляет правовые основы обеспечения безопасности личности, общества и государства, определяет систему безопасности и ее функции, устанавливает порядок организации и финансирования органов обеспечения безопасности, а также контроля и надзора за законностью их деятельности.

ФЗ РФ “О государственной тайне” от 21.07.93 г.

Определяет уровни (грифы) секретности государственной тайны и соответствующую степень важности, регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности РФ.

ФЗ РФ “О коммерческой тайне” от 29.07.04 г.

Предусматривает правовое регулирование основных вопросов отнесения информации к коммерческой тайне, оборота такой информации и охраны ее конфиденциальности.

ФЗ РФ «О лицензировании отдельных видов деятельности» от 25.09.98г.

Регулирует отношения, возникающие в связи с осуществлением лицензирования отдельных видов деятельности, и направлен на обеспечение единой государственной политики при осуществлении лицензирования, при регулировании и защите прав граждан, защите их законных интересов, нравственности и здоровья, обеспечении обороны страны и безопасности государства, а также на установление правовых основ единого рынка.

ФЗ РФ “О персональных данных” от 27.07.06 г.

ФЗ РФ «Об цифровой подписи» от 28.06.14 г.

Определяет правила использования электронной подписи в электронных документах, которая признается равноподлинной собственноручной подписью на бумажном носителе.

ФЗ РФ
N 149-ФЗ “Об информации, информационных технологиях и о защите информации” от 27 июля 2006г.

регулирует отношения, возникающие при:
1) осуществлении права на поиск, получение, передачу, производство и распространение информации;
2) применении информационных технологий;
3) обеспечении защиты информации.

Статья 16. Защита информации

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

*4. **Обладатель информации**, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:*

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации.

Ответственность за компьютерные преступления в информационной сфере

Глава № 28 Уголовного кодекса РФ от 1.01.97 г. определяет ответственность за компьютерные преступления

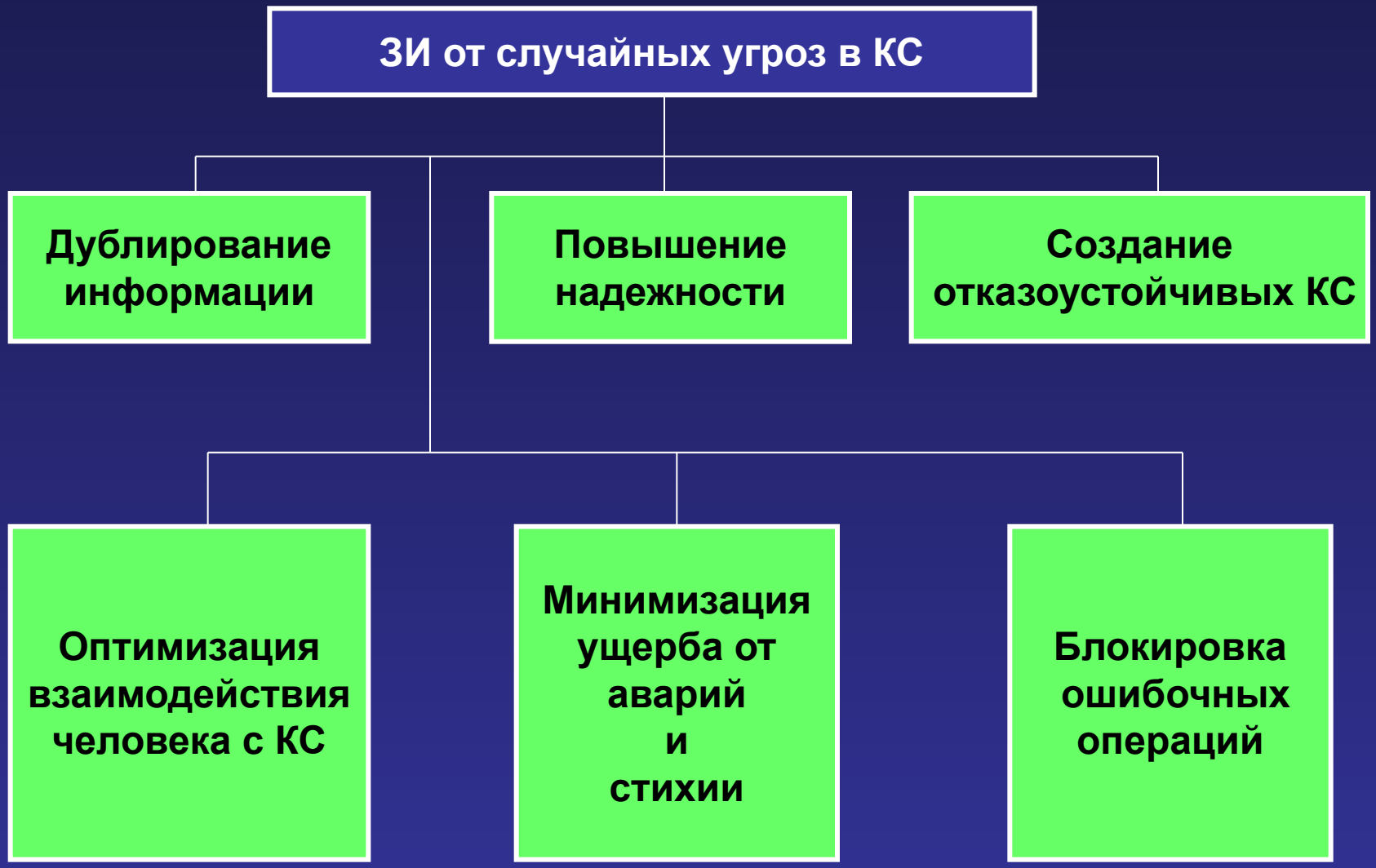
Статья 272 предусматривает наказание за неправомерный доступ к компьютерной информации. Наказание – от штрафа 200 МРОТ до 5 лет лишения свободы.

Статья 273 устанавливает ответственность за создание, использование и распространение вредоносных программ для ЭВМ. Наказание – до 7 лет лишения свободы.

Статья 274 определяет ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Наказание – до 5 лет лишения свободы

Угрозы безопасности информации ИС

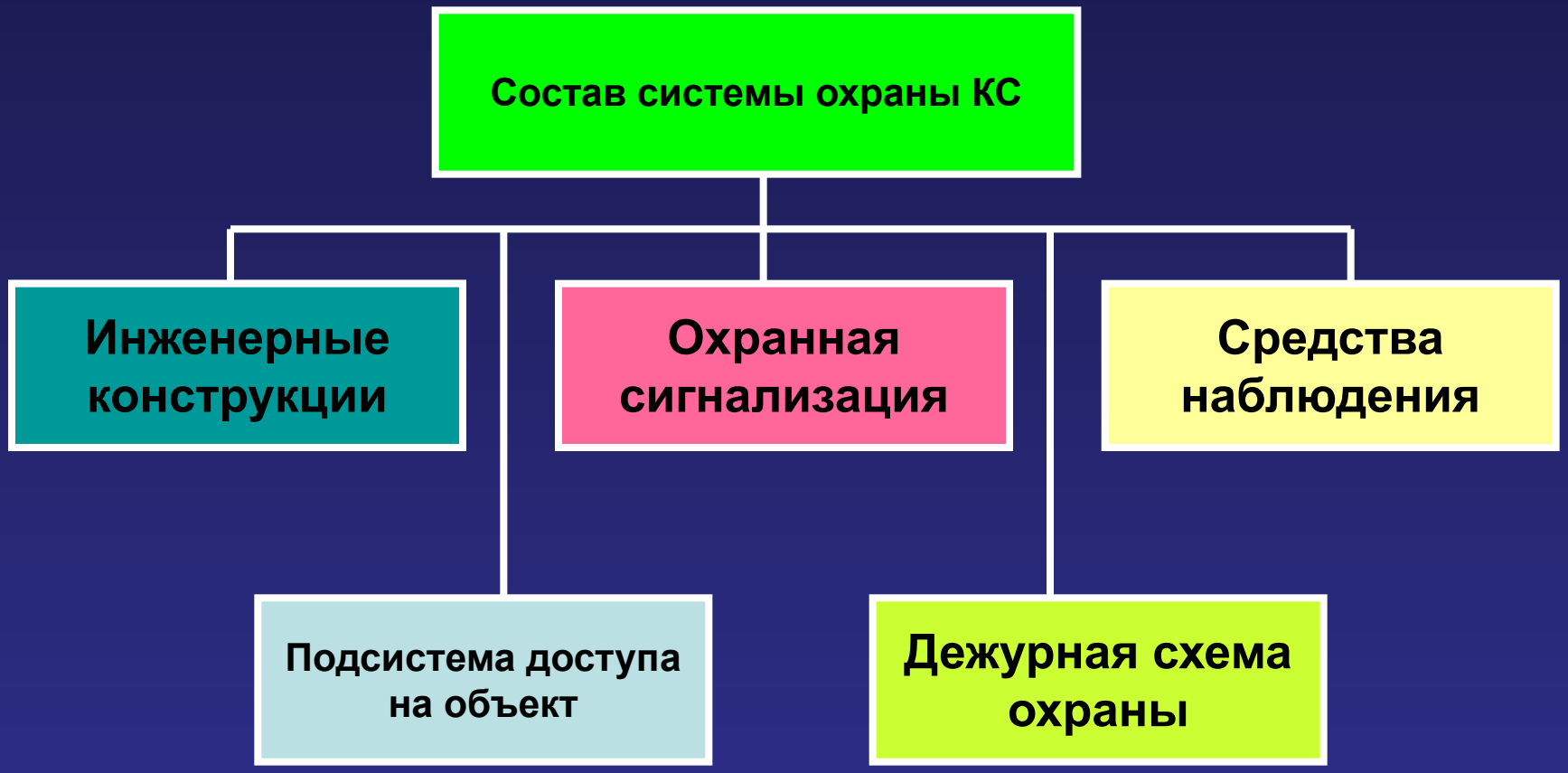
Задачи защиты информации ИС от случайных угроз



*

Задачи защиты информации в ИС от преднамеренных угроз

Обеспечение охраны объектов информатизации



*

Защита информации ИС от НСД

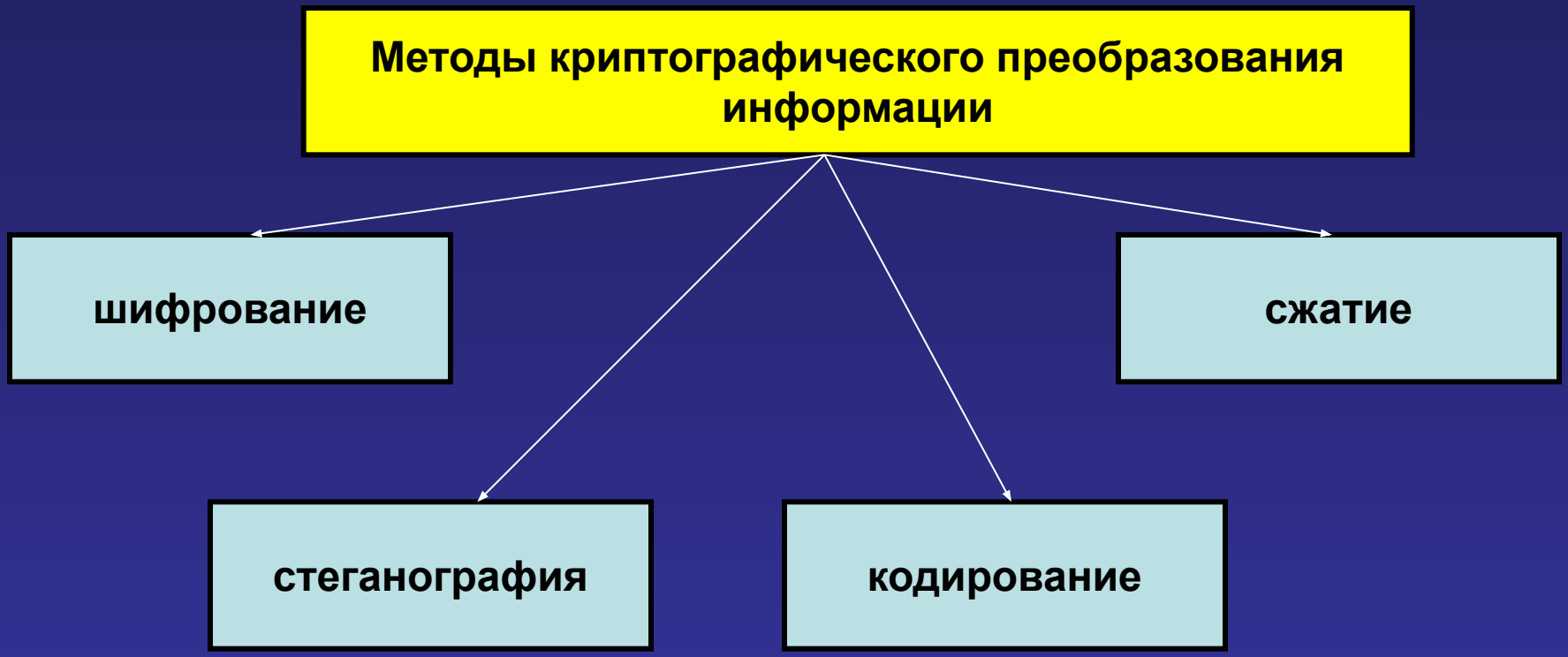
Для защиты информации в ИС от НСД применяют отечественные **программные системы** защиты ПЭВМ “Снег - 1”, “Кобра”, “Страж” и др, и **программно - аппаратные средства** защиты “Аккорд”, “SecretNET”, “VipNET”, “Спектр”, “Рубеж” и др.

Данные средства реализуют максимальное число защитных механизмов:

- Идентификация и аутентификация пользователей
- Разграничение доступа к файлам, каталогам, дискам
- Шифрование информации
- Защита процесса загрузки ОС путем блокирования устройств в/вывода и каналов связи
- Блокировка КС на время отсутствия персонала
- Регистрация событий
- Защита информации от копирования
- Очистка памяти

Криптографические методы защиты информации

Под **криптографической защитой** понимают такое преобразование информации, в результате которого она становится недоступной для преобразования и использования лицами, не имеющими на то прав.



*


Методы шифрования
Методы шифрования с симметричным ключом
Методы замены
Методы перестановки
Аналитические методы
Методы гаммирования
Методы шифрования с открытым ключом
В таких системах используется два ключа. И шифруется открытым ключом, а расшифровывается секретным.
Криптосистемы RSA
Криптосистемы Эль-Гамаля
Криптосистемы Мак-Элиса

Конфиденциальность и безопасность при работе с электронной почтой

Методы обеспечения информационной безопасности при работе с электронной почтой

Анонимность

- Использование бесплатных анонимных Web почтовых ящиков *www.rambler.ru* *www.narod.ru*
- Системы переадресовки (*www.iname.com*)

Шифрование

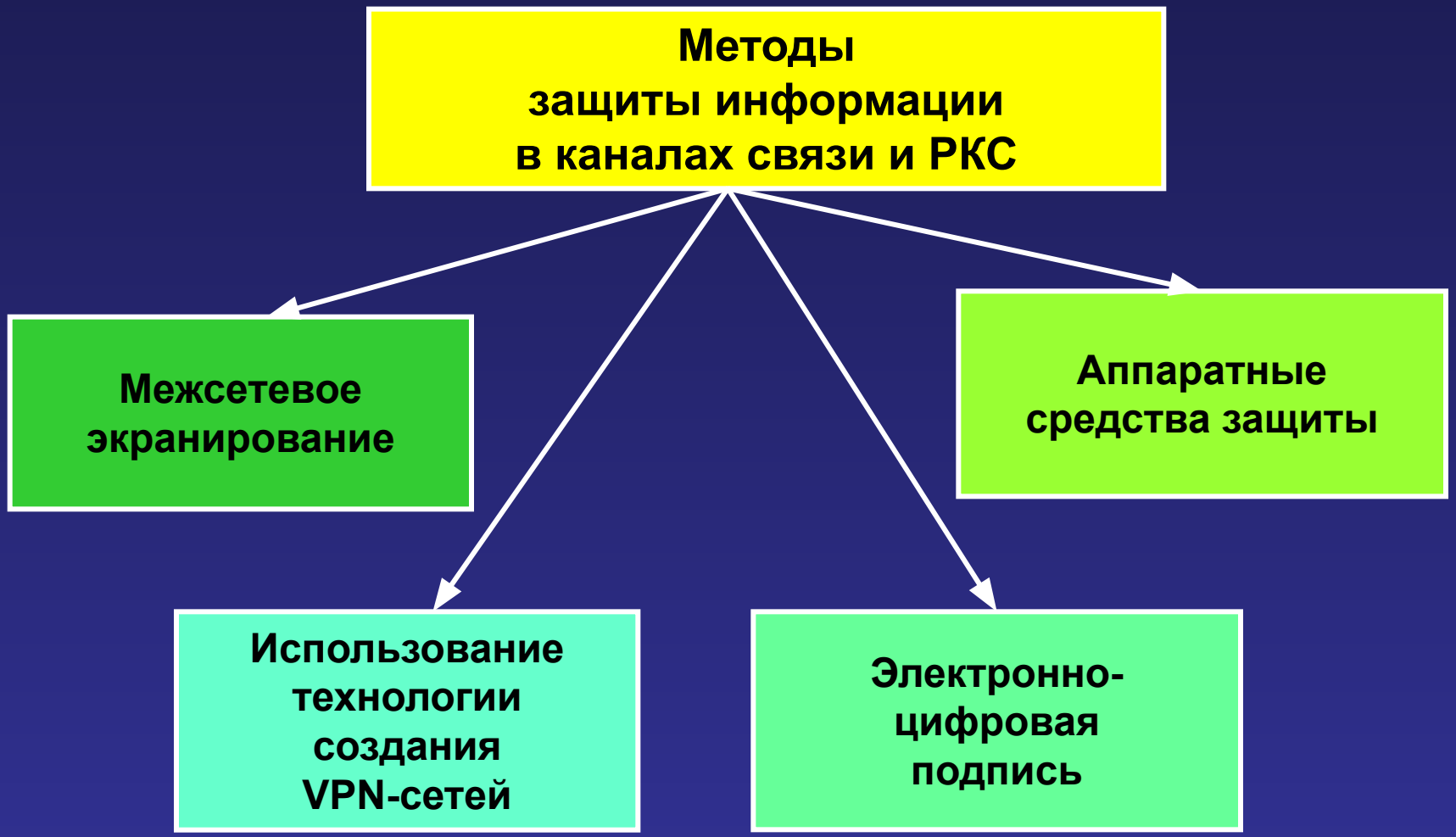
- Настройка стандартных почтовых программ(*The Bat, Outlook Express*)
- ЭЦП (*www.pgpi.com*)
- Спецпрограммы для шифрования информации типа SaveDisk

Антивирусная и антиспамная защита

Межсетевые экраны *ZoneAlarm* *www. zonelabs.com* *Outpost* *www.outpost.agnitum.com*

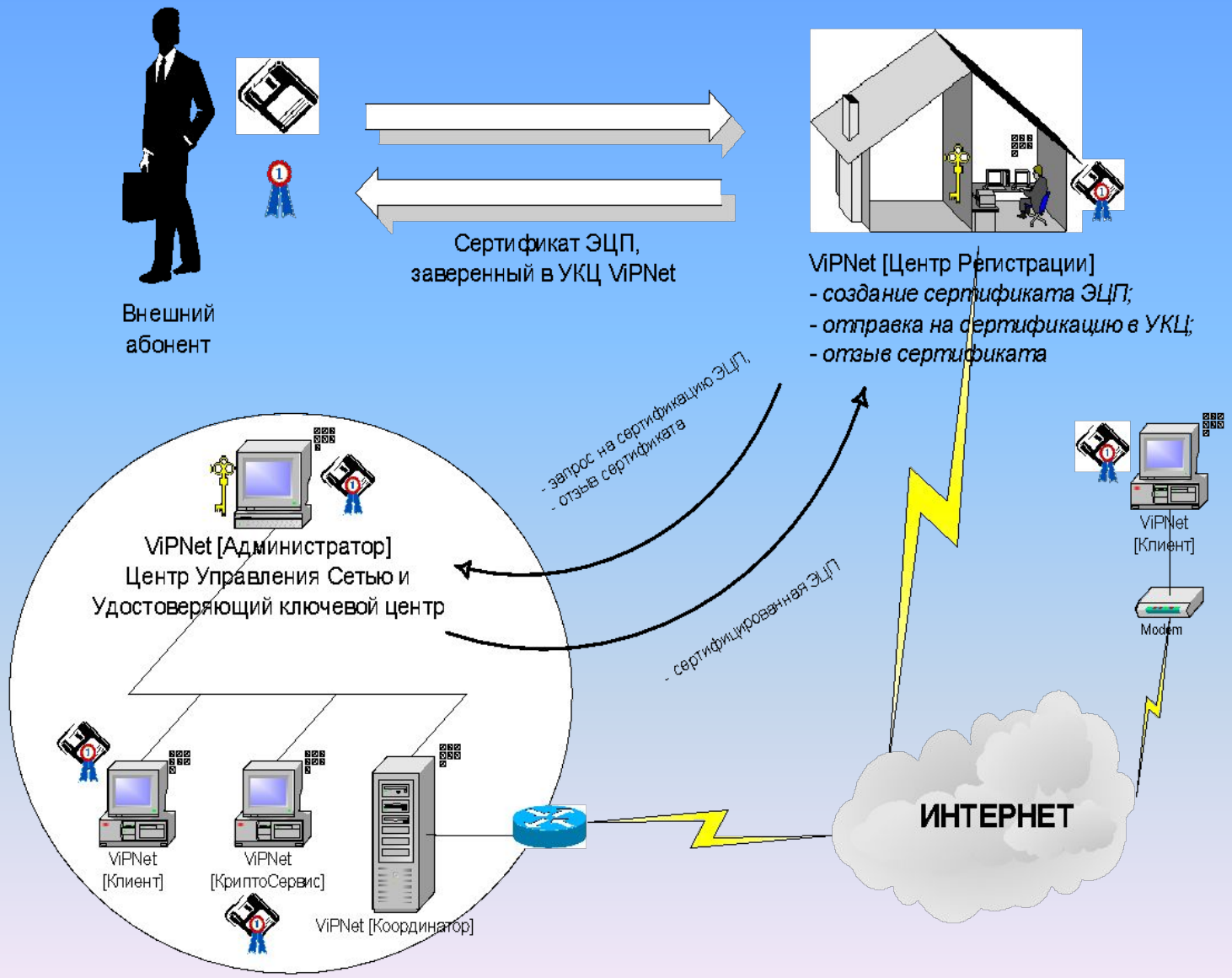
- Антивирусные программы
- Утилиты

Защита информации в каналах связи и РКС

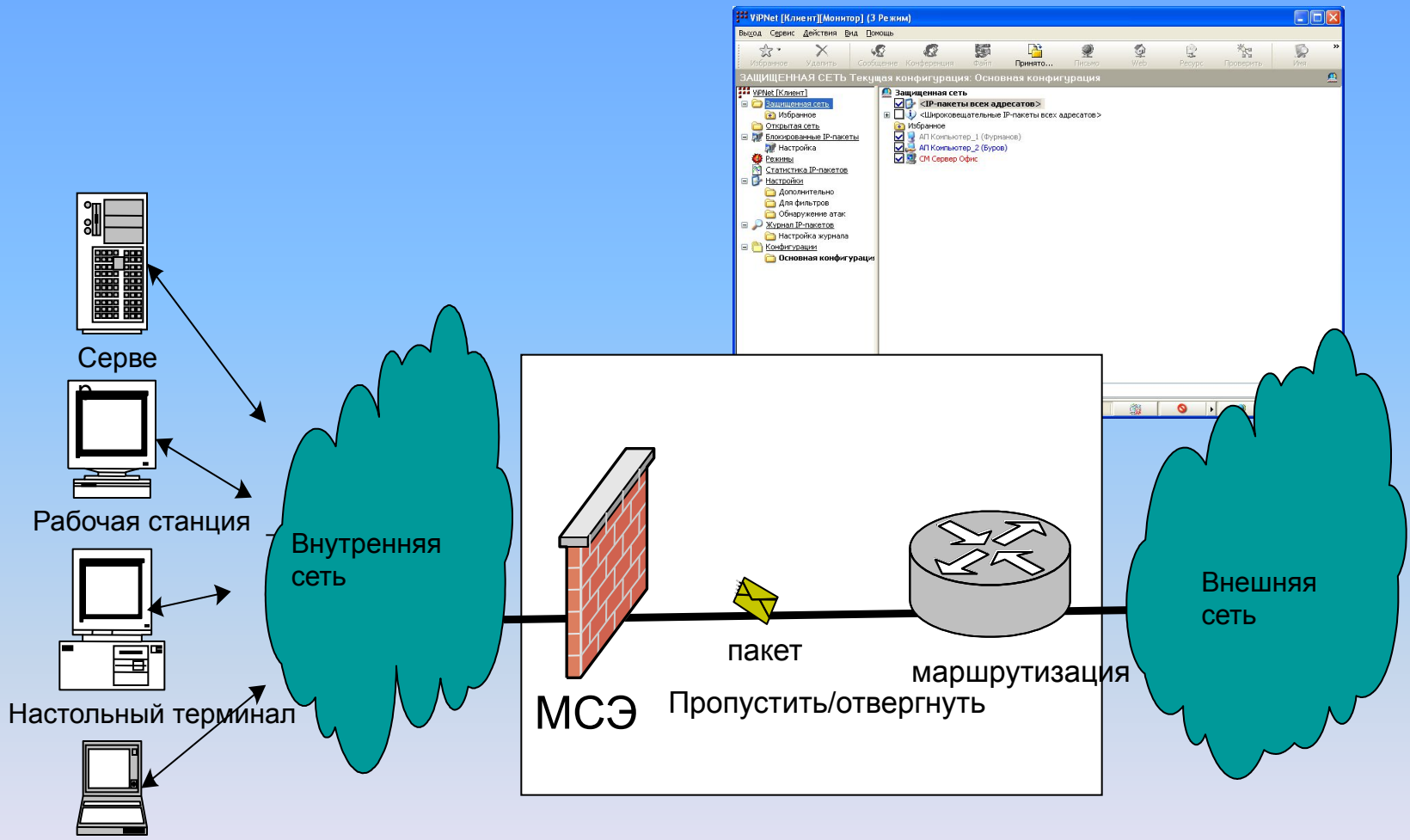


*

Структура VPN -сети

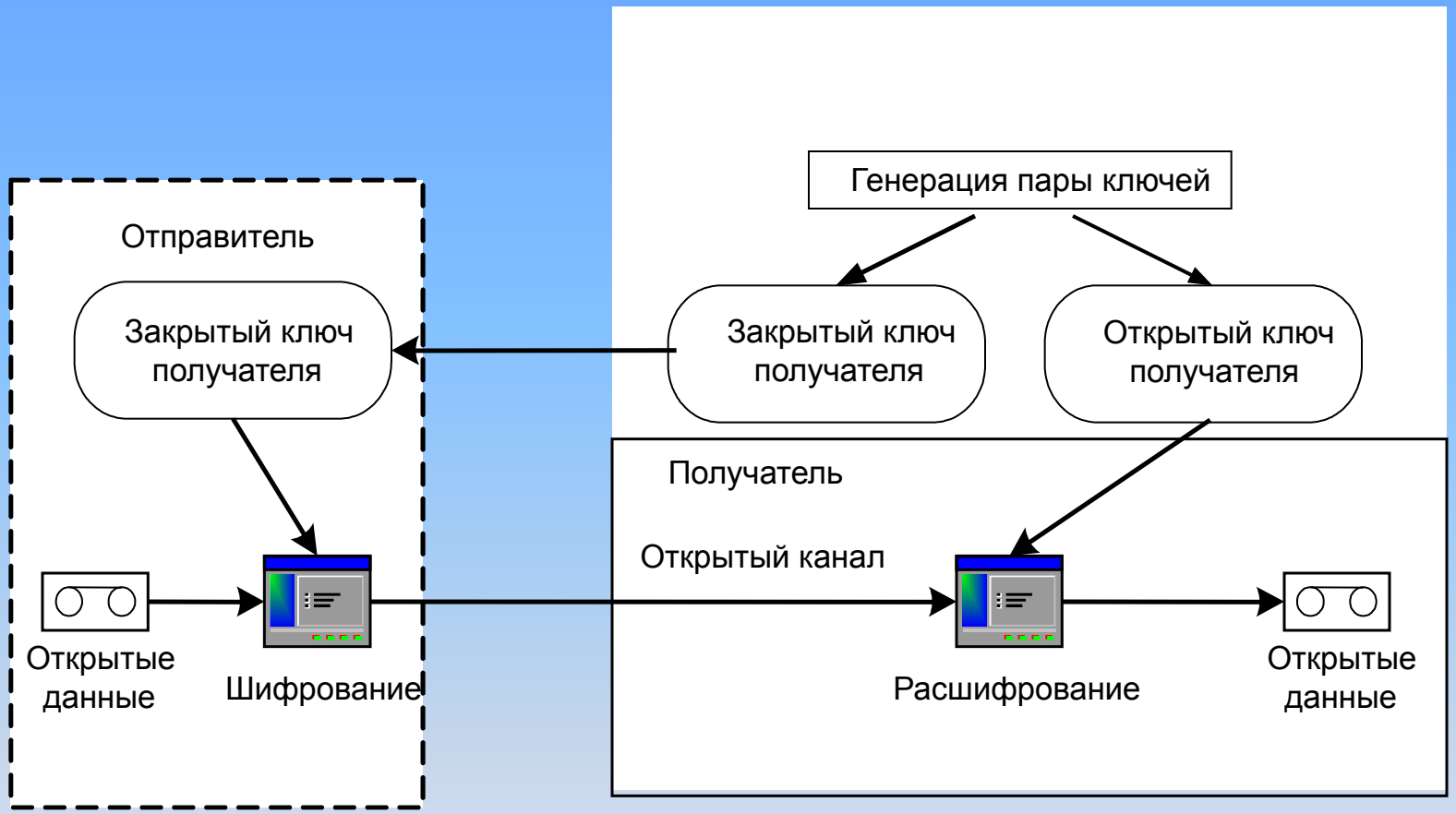


Межсетевое экранирование



*

Технология применения ЭЦП



*

Антивирусная борьба

Компьютерные вирусы – это небольшие исполняемые программы, обладающие свойством распространения и самовоспроизведения в КС.

Вирусы могут выполнять ***изменение*** или ***уничтожение*** ПО или данных, хранящихся в КС.

Основные источники вирусов

- глобальные сети - электронная почта, электронные конференции; файл-серверы ftp;
- локальные сети;
- пиратское программное обеспечение;
- персональные компьютеры «общего пользования»;
- съемные носители информации – дискеты, RW/DVD-диски, энергонезависимая память;
- ремонтные службы.


Классификация компьютерных вирусов
По среде обитания
По способу заражения
По алгоритму функционировани я
сетевые
файловые
загрузочные
комбинированные
резидентные
нерезидентные
след. слайд
По способу опасности вредительских воздействий
безвредные
опасные
очень опасные

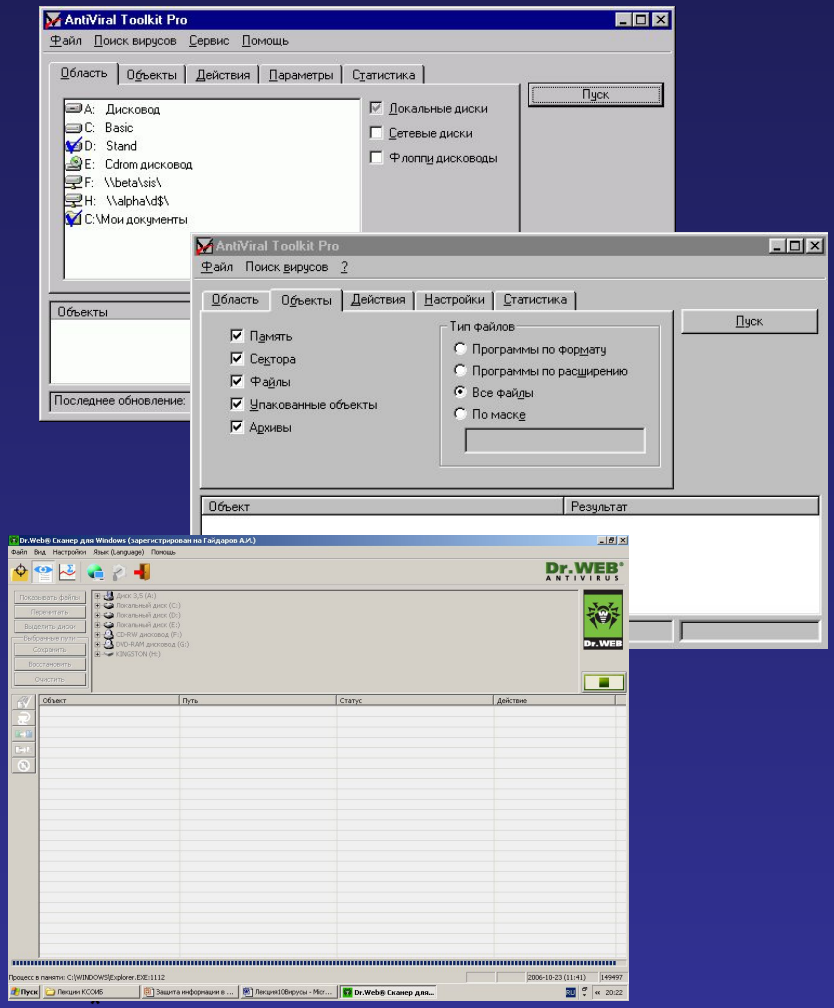

По алгоритму функционирования
Вирусы, не изменяющие среду обитания при распространении
Вирусы, изменяющие среду обитания при распространении
Вирусы – “спутники”
Вирусы – “черви”
студенческие
“стелс”-вирусы
полиморфные

Признаки проявления вируса

1. Прекращение работы или неправильная работа ранее успешно функционировавших программ;
2. Медленная работа компьютера;
3. Невозможность загрузки операционной системы;
4. Исчезновение файлов и каталогов или искажение их содержимого;
5. Изменение даты и времени модификации файлов;
6. Изменение размеров файлов;
7. Неожиданное значительное увеличение количества файлов на диске;
8. Существенное уменьшение размера свободной оперативной памяти;
9. Вывод на экран непредусмотренных сообщений или изображений;
10. Подача непредусмотренных звуковых сигналов;
11. Частые зависания и сбои в работе компьютера.

Следует отметить, что вышеперечисленные явления необязательно вызываются присутствием вируса, а могут быть следствием других причин. Поэтому всегда затруднена правильная диагностика состояния компьютера. В целом, подозрение на наличие вируса должно вызывать **любое отклонение от штатной работы вычислительной системы.**

Наиболее используемые антивирусные системы



НАЗВАНИЕ АВС	ПРОИЗВОДИТЕЛЬ
АВС отечественного производства	
AtiViralToolkitPro (AVP)	Лаборатория Касперского
Dr. Web	ЗАО "ДиалогНаука
АВС зарубежного производства	
Norton Antivirus	фирмы Symantec
PC-Cillin	фирмы TrendMicro
F-Prot	Command Software Systems
IBM Antivirus	IBM Corp.
ThunderByte Antivirus	Authentix/ThunderByte
ViruScan	Eliashim

Профилактика заражения вирусами КС

1. Использование лицензированного ПО
2. Дублирование информации
3. Регулярное использование антивирусных программ
4. Обновление баз и версий антивирусных программ
5. Проведение антивирусной проверки внешних носителей информации при их использовании в КС
6. При работе в РКС обязательное использование межсетевых экранов и аппаратных средств защиты
7. Периодические проверки КС специалистами на предмет заражения вирусами.

Порядок действий при заражении ЭВМ вирусами

1. Выключить ЭВМ для уничтожения резидентных вирусов
2. Загрузить эталонную ОС с резервного носителя
3. Сохранить важную информацию на съемных носителях
4. Использовать антивирусные средства для удаления вирусов и восстановления информации. Если работоспособность ЭВМ восстановлена, то следует перейти к пункту 8
5. Осуществить форматирование и новую разметку жесткого диска ЭВМ
6. Восстановить ОС и необходимое ПО на ЭВМ
7. Тщательно проверить информацию, сохраненную после заражения вирусами ЭВМ
8. Завершить восстановление информации проверкой ЭВМ с помощью имеющихся антивирусных программ

Конец занятия !

Желаю всем приятного отдыха !