ЛЕКЦИЯ № 2

ОСОБЕННОСТИ ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ ОТ АТАК С ИСПОЛЬЗОВАНИЕМ СКРЫТЫХ КАНАЛОВ

ЛЕКЦИЯ № 2
ОСОБЕННОСТИ ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ ОТ АТАК С ИСПОЛЬЗОВАНИЕМ СКРЫТЫХ КАНАЛОВ

Цель занятия: **рассмотреть и проанализировать особенности организации защиты информации от атак с использованием скрытых каналов**

Учебные вопросы:

ВОПРОС 1. Необходимость организации защиты информации от атак с использованием скрытых каналов

ВОПРОС 2. Характеристика доверия к изделиям информационных технологий

ВОПРОС 3. Характеристика ГОСТ Р 53113.1-2008

ВОПРОС 4. Классификация скрытых каналов

ВОПРОС 5. Классификация угроз безопасности, реализуемых с использованием скрытых каналов

ВОПРОС 6. Реализация угроз безопасности, осуществляемых с использованием скрытых каналов

ВОПРОС 7. Классификация активов по степени опасности атак с использованием скрытых каналов

ЛЕКЦИЯ № **2**
ОСОБЕННОСТИ ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ ОТ АТАК С ИСПОЛЬЗОВАНИЕМ СКРЫТЫХ КАНАЛОВ

ВОПРОС 1.

Необходимость организации защиты информации от атак с использованием скрытых каналов

ВОПРОС 1.
Необходимость организации защиты информации от атак с использованием скрытых каналов

Для обеспечения защиты информации, обрабатываемой в АС, необходимо выявить и нейтрализовать все возможные информационные каналы несанкционированного действия — как традиционные, так и скрытые.

Впервые понятие скрытого канала было введено в работе Батлера Лэмпсона «A Note of the Confinement Problem» 10 октября 1973 года, где скрытым называется канал, который не проектировался и не предполагался для передачи информации в электронной системе обработки данных.

Для организации скрытого канала необходимо наличие закладки в программном или аппаратном обеспечении.

ВОПРОС 1.
Необходимость организации защиты информации от атак с использованием скрытых каналов

Для организации скрытого канала необходимо наличие ЗАКЛАДКИ в программном или аппаратном обеспечении.

ЗАКЛАДОЧНОЕ СРЕДСТВО (УСТРОЙСТВО) — техническое средство [устройство] приема, передачи и обработки информации, преднамеренно устанавливаемое на объекте информатизации или в контролируемой зоне в целях перехвата информации или несанкционированного воздействия на информацию и (или) ресурсы автоматизированной информационной системы.

Национальный стандарт Российской Федерации ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

ВОПРОС 1.
Необходимость организации защиты информации от атак с использованием скрытых каналов

Чаще всего скрытый канал является паразитом по отношению к основному каналу: скрытый канал уменьшает пропускную способность основного канала.

Сторонние наблюдатели обычно не могут обнаружить, что помимо основного канал передачи данных есть ещё дополнительный.

Только отправитель и получатель знают это.

Например, в СТЕГАНОГРАФИИ скрытые сообщения кодировались внутри графических изображений или других данных таким образом, что на глаз изменений было не заметить, однако получатель сообщения мог раскодировать зашифрованное сообщение.

ВОПРОС 1.
Необходимость организации защиты информации от атак с использованием скрытых каналов

СКРЫТЫЙ КАНАЛ (covert channel) — непредусмотренный разработчиком системы информационных технологий и автоматизированных систем коммуникационный канал, который может быть применен для нарушения политики безопасности.

Национальный стандарт Российской Федерации ГОСТ Р 53113.1-2008. Информационная технология. Защита ИТ и АС от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения.

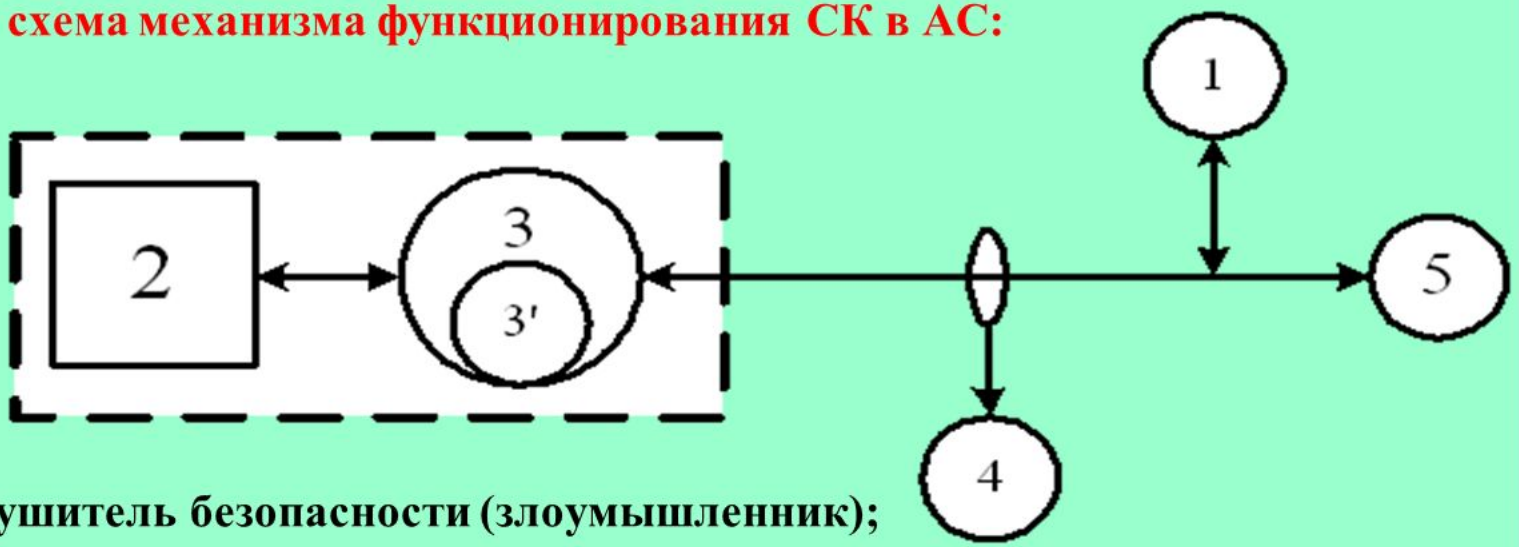
ВОПРОС 1.
Необходимость организации защиты информации от атак с использованием скрытых каналов

КОММУНИКАЦИОННЫЙ КАНАЛ — совокупность носителей информации, доставляющих сообщение от источника к приемнику.

Национальный стандарт Российской Федерации ГОСТ Р 53113.1-2008. Информационная технология. Защита ИТ и АС от угроз ИБ, реализуемых с использованием СК. Часть 1. Общие положения.

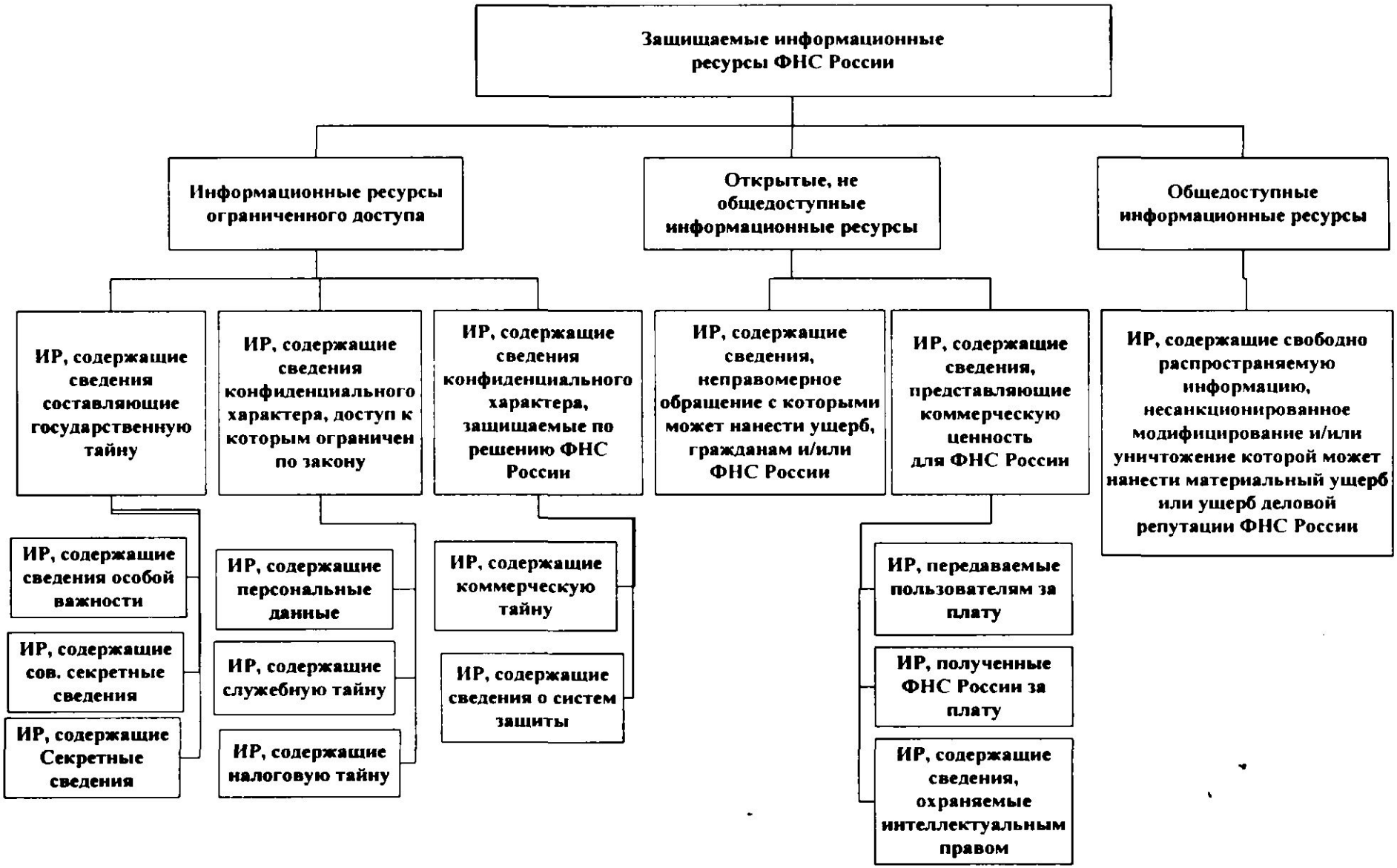
ВОПРОС 1.
Необходимость организации защиты информации от атак с использованием скрытых каналов

Общая схема механизма функционирования СК в АС:

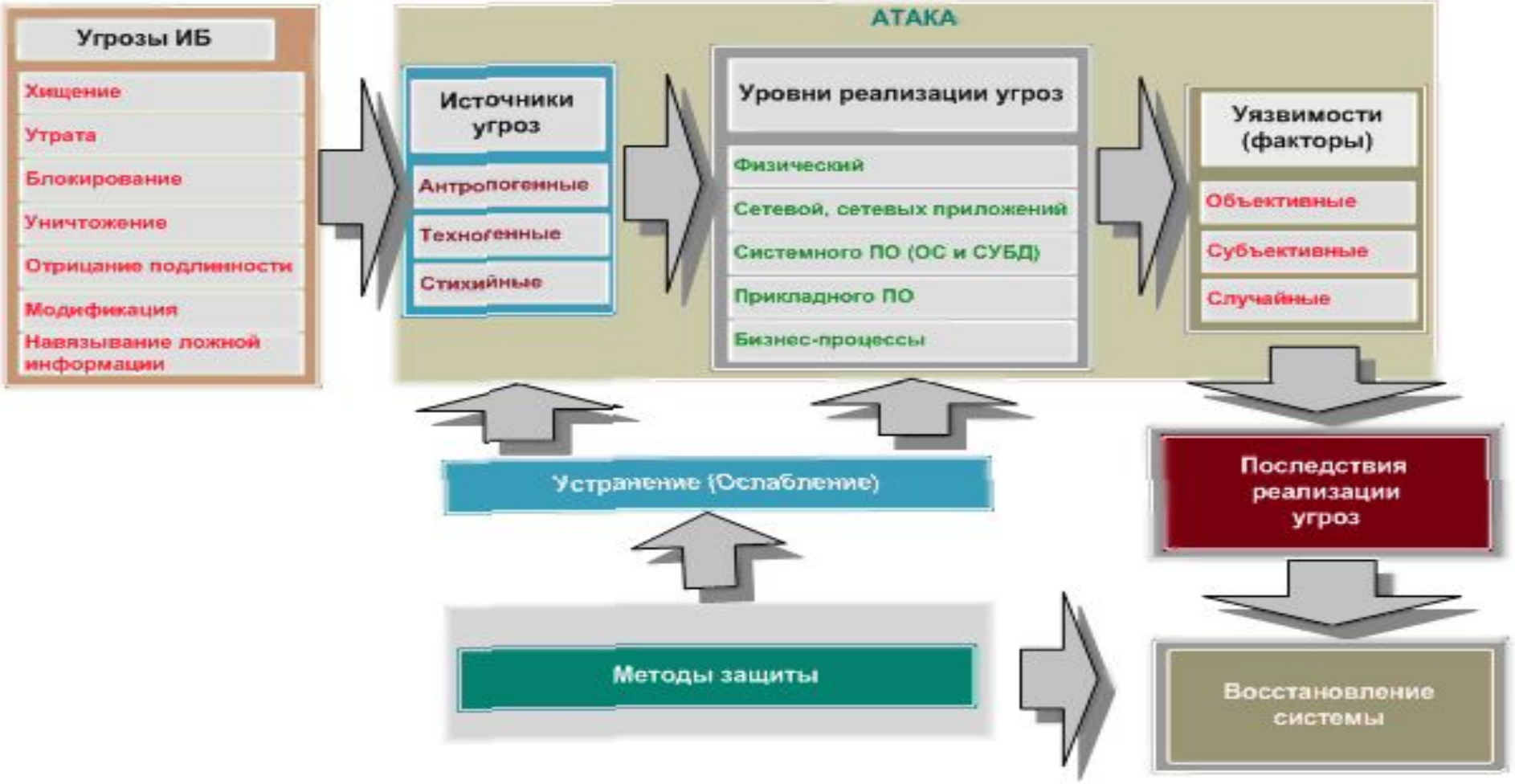


1 – нарушитель безопасности (злоумышленник);
2 - информация ограниченного доступа либо критически важная функция,
3 — субъект, имеющий санкционированный доступ к 2 и 5;
3/ — агент нарушителя безопасности, находящийся в замкнутом контуре с 2 и взаимодействующий с 2 от имени субъекта 3;
4 — инспектор (программное, программно-аппаратное, аппаратное средство или лицо), контролирующий (ее) информационное взаимодействие 3, пересекающее замкнутый контур, отделяющий объект информатизации от внешней среды;
5 — субъект, находящийся вне замкнутого контура, с которым 3 осуществляет санкционированное информационное взаимодействие.

Обобщенная структура защищаемых информационных ресурсов на примере ФНС России

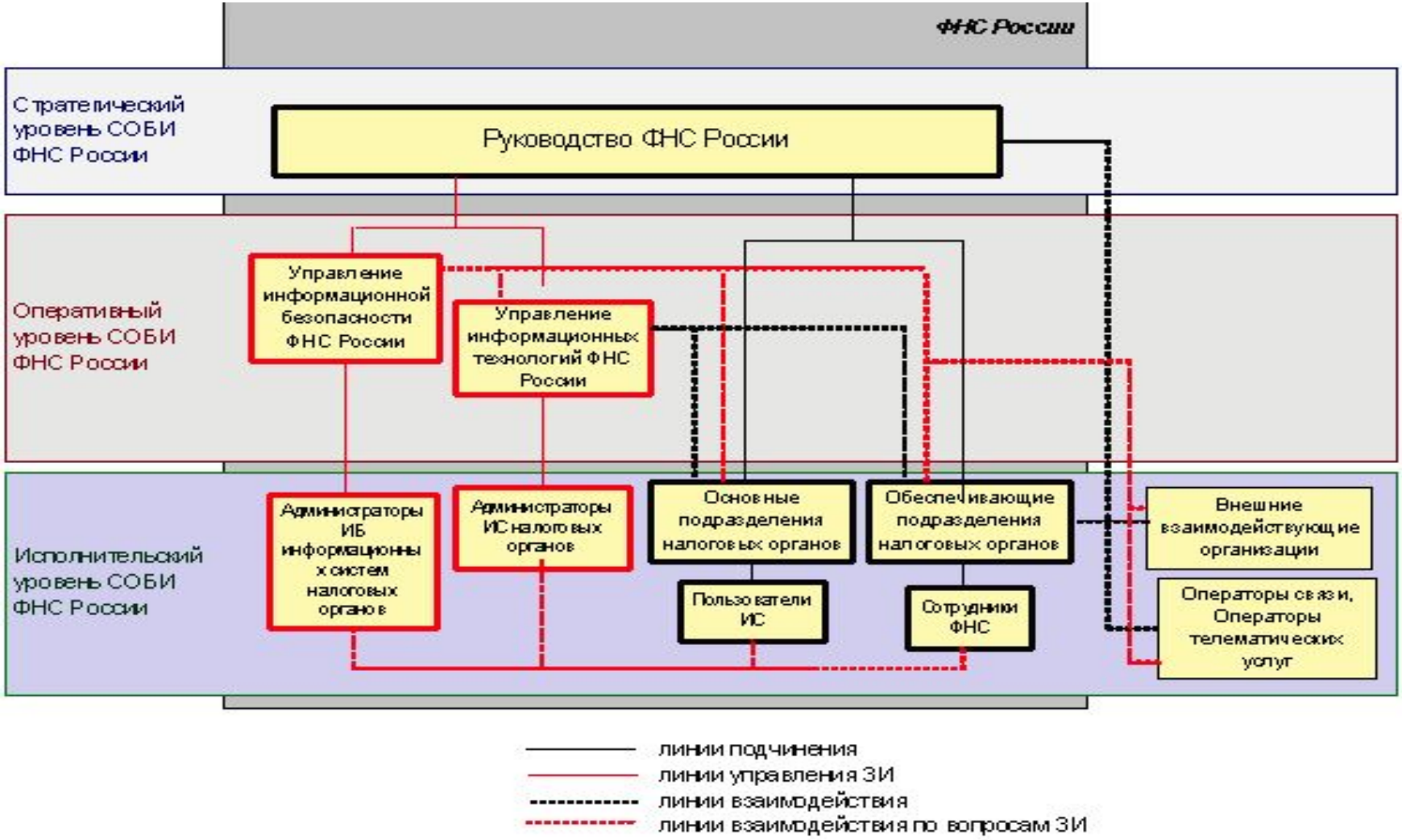


ВОПРОС 1.
Необходимость организации защиты информации от атак с использованием скрытых каналов



Модель реализации угроз информационной безопасности

ВОПРОС 1.
Необходимость организации защиты информации от атак с использованием скрытых каналов

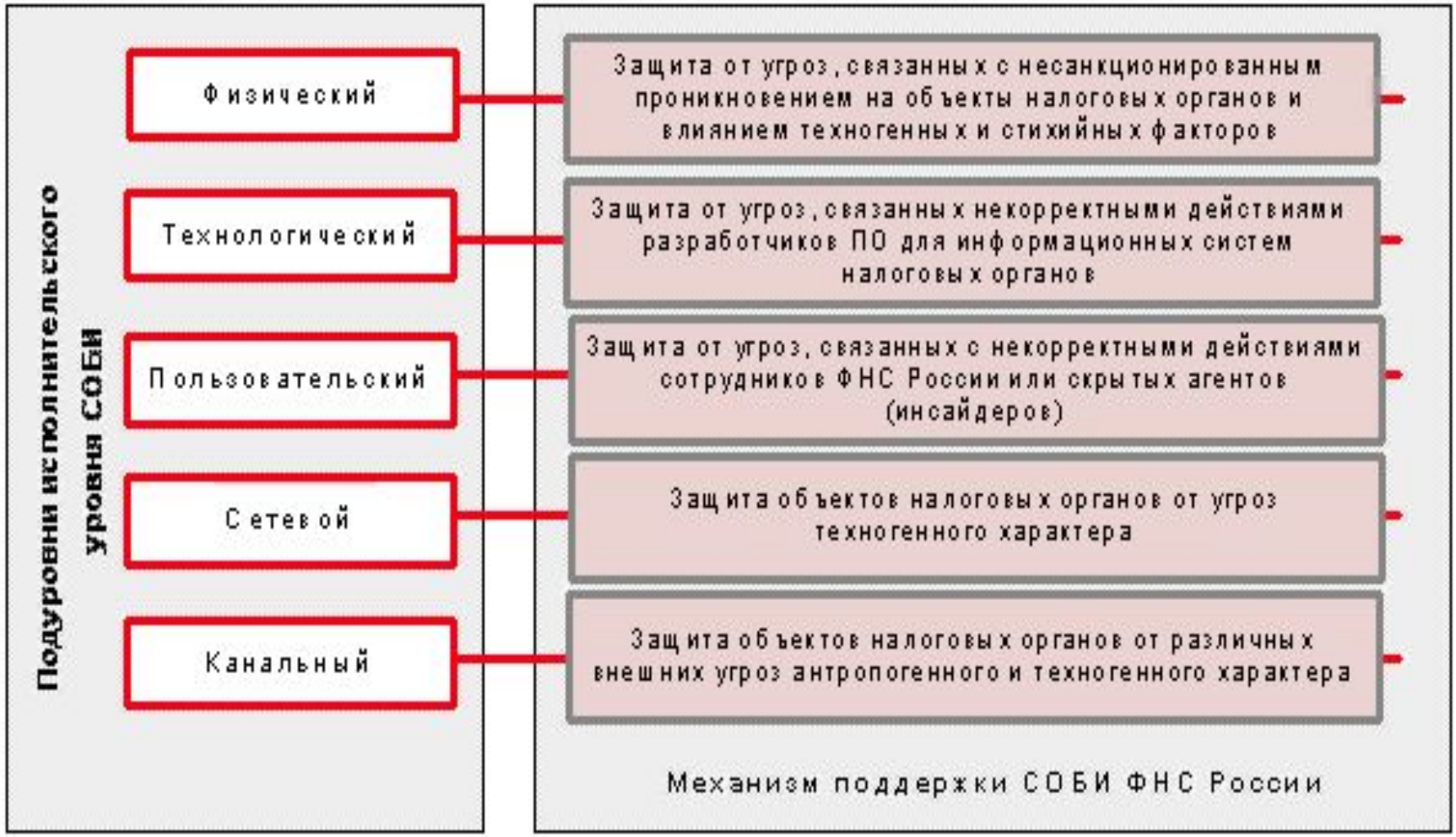


Общая архитектура организационной базы по уровням СОБИ и их взаимосвязь

ВОПРОС 1.
Необходимость организации защиты информации от атак с использованием скрытых каналов

Укрупненная структура Политики безопасности информации органа власти

ВОПРОС 1.
Необходимость организации защиты информации от атак с использованием скрытых каналов



Уровни системы обеспечения безопасности информации

ЛЕКЦИЯ № 2
ОСОБЕННОСТИ ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ ОТ АТАК С ИСПОЛЬЗОВАНИЕМ СКРЫТЫХ КАНАЛОВ

ВОПРОС 2.

Характеристика доверия к изделиям информационных технологий

ВОПРОС 2.
Характеристика доверия к изделиям информационных технологий

Существенным моментом защищенности систем ИТ и АС является доверие к системам защиты.

ДОВЕРИЕ — основание для уверенности в том, что объект соответствует целям безопасности.

Национальный стандарт Российской Федерации ГОСТ Р 53113.1-2008. Информационная технология. Защита ИТ и АС от угроз ИБ, реализуемых с использованием СК. Часть 1. Общие положения.

ВОПРОС 2.
Характеристика доверия к изделиям информационных технологий

Угрозу государственной и общественной безопасности составляют сайты насильственной, экстремистской и иной противоправной направленности, использование сети Интернет и мобильной телефонии для организации СКРЫТЫХ КАНАЛОВ связи и пропаганды террористической деятельности.

Государственная программа Российской Федерации «Информационное общество (2011 - 2020 годы)» Подпрограмма "Безопасность в информационном обществе"

ВОПРОС 2.
Характеристика доверия к изделиям информационных технологий

ЦЕЛЬ БЕЗОПАСНОСТИ — изложенное намерение противостоять установленным угрозам и/или удовлетворять установленной политике безопасности организации и предположениям.

Национальный стандарт Российской Федерации
ГОСТ Р ИСО/МЭК 15408-1-2008
«Информационная технология.
Методы и средства обеспечения безопасности.
Критерии оценки безопасности информационных технологий.
Часть 1.
Введение и общая модель»

ВОПРОС 2.
Характеристика доверия к изделиям информационных технологий

ПОЛИТИКА БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ (*organisational security policies*) — одно или несколько правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности.

Национальный стандарт Российской Федерации
ГОСТ Р ИСО/МЭК 15408-1-2008
«Информационная технология.
Методы и средства обеспечения безопасности.
Критерии оценки безопасности информационных технологий.
Часть 1.
Введение и общая модель»

ВОПРОС 2.
Характеристика доверия к изделиям информационных технологий

ПОЛИТИКА БЕЗОПАСНОСТИ ИНФОРМАЦИИ (*information security policy*) — совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Национальный стандарт Российской Федерации ГОСТ Р 53113.1-2008. Информационная технология. Защита ИТ и АС от угроз ИБ, реализуемых с использованием СК. Часть 1. Общие положения.

ВОПРОС 2.
Характеристика доверия к изделиям информационных технологий

Обеспечение доверия осуществляется путем глубокого анализа или экспертизы программно-аппаратных продуктов с точки зрения их защищенности.

Характеристики защищенности относятся к трем типам нарушения безопасности информации:

— несанкционированного раскрытия информации — нарушение конфиденциальности;

— модификации информации — нарушение целостности;

— потеря возможности использования информации — нарушение доступности.

ВОПРОС 2.
Характеристика доверия к изделиям информационных технологий

Защищенность — атрибуты программного обеспечения, относящиеся к его способности предотвращать несанкционированный доступ, случайный или преднамеренный, к программам и данным.

Государственный стандарт Российской Федерации
ГОСТ Р 9126-94
«Информационная технология.
Оценка программной продукции.
Характеристики качества и руководства по их применению»

ЛЕКЦИЯ № 2
ОСОБЕННОСТИ ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ ОТ АТАК С ИСПОЛЬЗОВАНИЕМ СКРЫТЫХ КАНАЛОВ

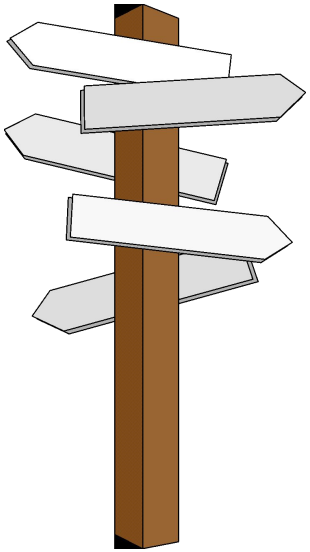
ВОПРОС 3.

Характеристика ГОСТ Р 53113.1-2008

Стандарт определяет следующий ПОРЯДОК ДЕЙСТВИЙ по определению степени опасности СК для активов организации, выявлению и противодействию СК:

1 Проведение классификации активов в зависимости от степени опасности атак с использованием СК с учетом возможных угроз безопасности активам

ОПРЕДЕЛЕНИЕ необходимой **2 глубины анализа СК** в зависимости от типа



3 Проведение анализа СК, включающее в себя выполнение следующих задач:

А) идентификация (выявление) СК;

Б) оценка пропускной способности СК;

В) оценка опасности, которую несет скрытое функционирование СК.

Мероприятия по защите от угроз, реализуемых с использованием СК, и включающие в себя выполнение следующих задач:

4 А) принятие решений о внедрении защитных мер для противодействия указанным угрозам безопасности;

ВОПРОС 3.
Характеристика ГОСТ Р 53113.1-2008

ГОСТ Р 53113.1-2008 «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения» разработан с целью организации и проведения мероприятий по противодействию угрозам ИБ, реализуемым с использованием СК при формировании семейств профилей защиты.

ВОПРОС 3.
Характеристика ГОСТ Р 53113.1-2008

В стандарте ГОСТ Р 53113.1-2008 определяются следующие основные положения:

— устанавливается классификация СК;

— определяются задачи, решаемые при проведении анализа СК, что является необходимой составляющей для определения дальнейшего порядка организации защиты информации от атак с использованием СК;

— устанавливается порядок проведения анализа СК для продуктов и систем ИТ и АС, результаты которого используются при оценке доверия к мерам защиты информационных систем и ИТ.

ВОПРОС 3.
Характеристика ГОСТ Р 53113.1-2008

Стандарт используется заказчиками, разработчиками и пользователями ИТ при формировании ими требований к разработке, приобретению и применению важных продуктов и систем ИТ.

Эти продукты и системы предназначаются

для обработки, хранения или передачи информации,

подлежащей защите в соответствии с требованиями нормативных документов

или требованиями, устанавливаемыми собственником информации.

ВОПРОС 3.
Характеристика ГОСТ Р 53113.1-2008

Также положения стандарта ГОСТ Р 53113.1-2008 используются:

— органами сертификации и испытательных лабораторий при проведении оценки безопасности и сертификации безопасности ИТ и АС,

— а также аналитическими подразделениями

— и службами безопасности для сопоставления угроз ценным информационным активам с потенциальной возможностью ущерба через СК.

ВОПРОС 3. Характеристика ГОСТ Р 53113.1-2008

Характеристика ГОСТ Р 53113.1-2008

В настоящем стандарте использованы НОРМАТИВНЫЕ ССЫЛКИ на следующие стандарты:

— ГОСТ Р ИСО/МЭК15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

— ГОСТ Р ИСО/МЭК 17799-2006 Информационная технология. Практические правила управления информационной безопасностью

ВОПРОС 3.
Характеристика ГОСТ Р 53113.1-2008

Характеристика ГОСТ Р 53113.1-2008
НОРМАТИВНЫЕ ССЫЛКИ

ГОСТ Р ИСО/МЭК15408-3-2008

Информационная технология.

Методы и средства обеспечения безопасности.

Критерии оценки безопасности информационных технологий.

Часть 3.

Требования доверия к безопасности

ВОПРОС 3.
Характеристика ГОСТ Р 53113.1-2008

Характеристика ГОСТ Р 53113.1-2008
Приложение С к 15408-1-2008
(справочное)

Сведения
о соответствии национальных стандартов Российской Федерации ссылочным международным стандартам

Таблица С.1

№ п/п	Обозначение ссылочного международного стандарта	Обозначение и наименование соответствующего национального стандарта
1	ИСО/МЭК 15408-1:2005	ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
2	ИСО/МЭК 15408-2:2005	ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
3	ИСО/МЭК 15408-3:2005	ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

ВОПРОС 3.
Характеристика ГОСТ Р 53113.1-2008

Характеристика ГОСТ Р 53113.1-2008

НОРМАТИВНЫЕ ССЫЛКИ

ГОСТ Р ИСО/МЭК 17799-2006

Информационная технология.

Практические правила управления

информационной безопасностью

ВОПРОС 3.
Характеристика ГОСТ Р 53113.1-2008

Характеристика ГОСТ Р ИСО/МЭК 17799-2005

СВЕДЕНИЯ О СТАНДАРТЕ

1 Подготовлен Федеральным государственным учреждением "Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю"

2 Внесен Управлением технического регулирования и стандартизации Федерального агентства по техническому регулированию и метрологии

3 Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2005 г. N 447-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 17799:2000 "Информационная технология. Практические правила управления информационной безопасностью" (ISO/IEC 17799:2000 "*Information technology. Code of practice for security management*")

5 Введен впервые 1 января 2007 г.

ВОПРОС 3.
Характеристика ГОСТ Р 53113.1-2008

Характеристика ГОСТ Р ИСО/МЭК 17799-2005

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ - механизм защиты, обеспечивающий:

- **КОНФИДЕНЦИАЛЬНОСТЬ: доступ к информации только авторизованных пользователей;**
- **ЦЕЛОСТНОСТЬ: достоверность и полноту информации и методов ее обработки;**
- **ДОСТУПНОСТЬ: доступ к информации и связанным с ней активам авторизованных пользователей по мере необходимости.**

Информационная безопасность достигается путем реализации соответствующего КОМПЛЕКСА МЕРОПРИЯТИЙ по управлению информационной безопасностью, которые могут быть представлены ПОЛИТИКАМИ, методами, процедурами, организационными структурами и функциями программного обеспечения.

ВОПРОС 3.
Характеристика ГОСТ Р 53113.1-2008

Характеристика ГОСТ Р ИСО/МЭК 17799-2005

Отдельные мероприятия по управлению информационной безопасностью могут рассматриваться как руководящие принципы для управления информационной безопасностью и служить отправной точкой для ее внедрения.

Такие мероприятия либо основываются на ключевых требованиях законодательства, либо рассматриваются как общепринятая практика в области информационной безопасности.

Ключевыми мерами контроля с точки зрения законодательства являются:

- **обеспечение конфиденциальности персональных данных (12.1.4);**
- **защита учетных данных организации (12.1.3);**
- **права на интеллектуальную собственность (12.1.2).**

ВОПРОС 3.
Характеристика ГОСТ Р 53113.1-2008

Характеристика ГОСТ Р ИСО/МЭК 17799-2005

3.1 ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Как минимум, политика должна включать следующее:

а) определение информационной безопасности, ее общих целей и сферы действия, а также раскрытие значимости безопасности как инструмента, обеспечивающего возможность совместного использования информации;

б) изложение целей и принципов информационной безопасности, сформулированных руководством;

в) краткое изложение наиболее существенных для организации политик безопасности, принципов, правил и требований, например:

1) соответствие законодательным требованиям и договорным обязательствам;

2) требования в отношении обучения вопросам безопасности;

3) предотвращение появления и обнаружение вирусов и другого вредоносного программного обеспечения;

4) управление непрерывностью бизнеса;

5) ответственность за нарушения политики безопасности;

г) определение общих и конкретных обязанностей сотрудников в рамках управления информационной безопасностью, включая информирование об инцидентах нарушения информационной безопасности;

д) ссылки на документы, дополняющие политику информационной безопасности, например, более детальные политики и процедуры безопасности для конкретных информационных систем, а также правила безопасности, которым должны следовать пользователи.

Такая политика должна быть доведена до сведения всех сотрудников организации в доступной и понятной форме.

ВОПРОС 3.
Характеристика ГОСТ Р 53113.1-2008

Характеристика ГОСТ Р 53113.1-2008

4.7. Противодействие опасным СК может осуществляться с помощью следующих средств и методов:

А) построение архитектуры ИТ или АС. позволяющей перекрыть СК или сделать их пропускную способность настолько низкой, что каналы становятся неопасными.
Этот метод применяется на этапе проектирования ИТ или АС;

Б) использование технических средств, позволяющих перекрывать СК или снижать их пропускную способность ниже заданного уровня;

ВОПРОС 3.
Характеристика ГОСТ Р 53113.1-2008

Характеристика ГОСТ Р 53113.1-2008

4.7. Противодействие опасным СК может осуществляться с помощью следующих средств и методов:

В) использование программно-технических средств, позволяющих выявлять работу опасных СК в процессе эксплуатации системы.

Выявление признаков работы СК МОЖЕТ ПОЗВОЛИТЬ БЛОКИРОВАТЬ их воздействие на информационные ресурсы;

Г) применение организационно-технических мер, позволяющих ликвидировать СК или уменьшить их пропускную способность до безопасного значения.

ЛЕКЦИЯ № 2
ОСОБЕННОСТИ ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ ОТ АТАК С ИСПОЛЬЗОВАНИЕМ СКРЫТЫХ КАНАЛОВ

ВОПРОС 4.

Классификация скрытых каналов

ВОПРОС 4.
Классификация скрытых каналов

СК по памяти

СК по памяти основаны на наличии памяти, в которую передающий субъект записывает информацию, а принимающий — считывает ее.

СК по времени

СК по времени предполагают, что передающий информацию субъект модулирует с помощью передаваемой информации некоторый изменяющийся во времени процесс, а субъект, принимающий информацию, в состоянии демодулировать передаваемый сигнал, наблюдая несущий информацию процесс во времени.

Скрытые статистические каналы

Скрытый статистический канал использует для передачи информации изменение параметров распределений вероятностей любых характеристик системы, которые могут рассматриваться как случайные и описываться вероятностно-статистическими моделями.

ВОПРОС 4.
Классификация скрытых каналов

СК по памяти

Скрытость каналов по памяти определяется тем, что сторонний наблюдатель не знает того места в памяти, где записана скрываемая информация.

СК по памяти предполагают использование ресурсов памяти, однако способ использования памяти не учитывается разработчиками системы защиты и поэтому не может выявляться используемыми средствами защиты.

СК по памяти, в свою очередь, подразделяются на:

— СК, основанные на сокрытии информации в структурированных данных.

— СК, основанные на сокрытии информации в неструктурированных данных.

ВОПРОС 4.
Классификация скрытых каналов

СК по памяти

СК по памяти, в свою очередь, поздравляют на:

— СК, основанные НА СОКРЫТИИ ИНФОРМАЦИИ В СТРУКТУРИРОВАННЫХ ДАННЫХ.

5.6. СК. основанные на сокрытии информации в структурированных данных, используют встраивание данных в информационные объекты с формально описанной структурой и формальными правилами обработки.

НАПРИМЕР, внутренний формат файлов, используемых современными текстовыми процессами, содержит ряд полей, не отображаемых при редактировании файла, поэтому они могут быть использованы для вставки скрытой информации.

ВОПРОС 4.
Классификация скрытых каналов

СК по памяти

СК по памяти, в свою очередь, поздравляют на:

— СК, основанные НА СОКРЫТИИ ИНФОРМАЦИИ В НЕСТРУКТУРИРОВАННЫХ ДАННЫХ.

5.7. СК, основанные на сокрытии информации в неструктурированных данных, используют встраивание данных в информационные объекты без учета формально описанной структуры.

НАПРИМЕР: запись скрытой информации в наименее значимые биты изображения, не приводящая к видимым искажениям изображения.

ВОПРОС 4.
Классификация скрытых каналов

СК по времени

Модулируя время занятости процессора, приложения могут передавать друг другу нелегальные данные.

В многозадачной операционной системе (ОС) центральный процессор является разделяемым информационно-вычислительным ресурсом для прикладных программ.

ВОПРОС 4.
Классификация скрытых каналов

Скрытые статистические каналы

Скрытость таких каналов основана на том. что получатель информации имеет меньшую неопределенность в определении параметров распределений наблюдаемых характеристик системы, чем наблюдатель, не имеющий знаний о структуре СК.

НАПРИМЕР, появление реальной, но маловероятной комбинации в присланном пакете в заданный промежуток времени может означать сигнал к сбою в компьютерной системе.

ВОПРОС 4.
Классификация скрытых каналов

Классификация скрытых каналов по пропускной способности

- Скрытый канал с низкой пропускной способностью
- Скрытый канал с высокой пропускной способностью

СК является каналом с низкой пропускной способностью, если его пропускной способности достаточно для передачи ценных информационных объектов минимального объема (например, криптографические ключи, пароли) или команд за промежуток времени, на протяжении которого данная передача является актуальной.

СК является каналом с высокой пропускной способностью, если его пропускная способность позволяет передавать информационные объекты среднего и большого размера (например, текстовые файлы, изображения, базы данных) за промежуток времени, на протяжении которого да иные информационные объекты являются ценными.

ВОПРОС 5.

Классификация угроз безопасности, реализуемых с использованием скрытых каналов

ВОПРОС 5.
Классификация угроз безопасности, реализуемых с использованием скрытых каналов

УГРОЗА БЕЗОПАСНОСТИ –

СОВОКУПНОСТЬ УСЛОВИЙ И ФАКТОРОВ, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее.

Национальный стандарт Российской Федерации
ГОСТ Р 53113.1-2008.
Информационная технология.
Защита ИТ и АС от угроз информационной безопасности, реализуемых с использованием скрытых каналов.
Часть 1.
Общие положения.

ВОПРОС 5.
Классификация угроз безопасности, реализуемых с использованием скрытых каналов

В современных условиях угрозы безопасности, которые могут быть реализованы с помощью СК, включают в себя следующие виды угроз.

А) ВНЕДРЕНИЕ ВРЕДОНОСНЫХ ПРОГРАММ И ДАННЫХ.

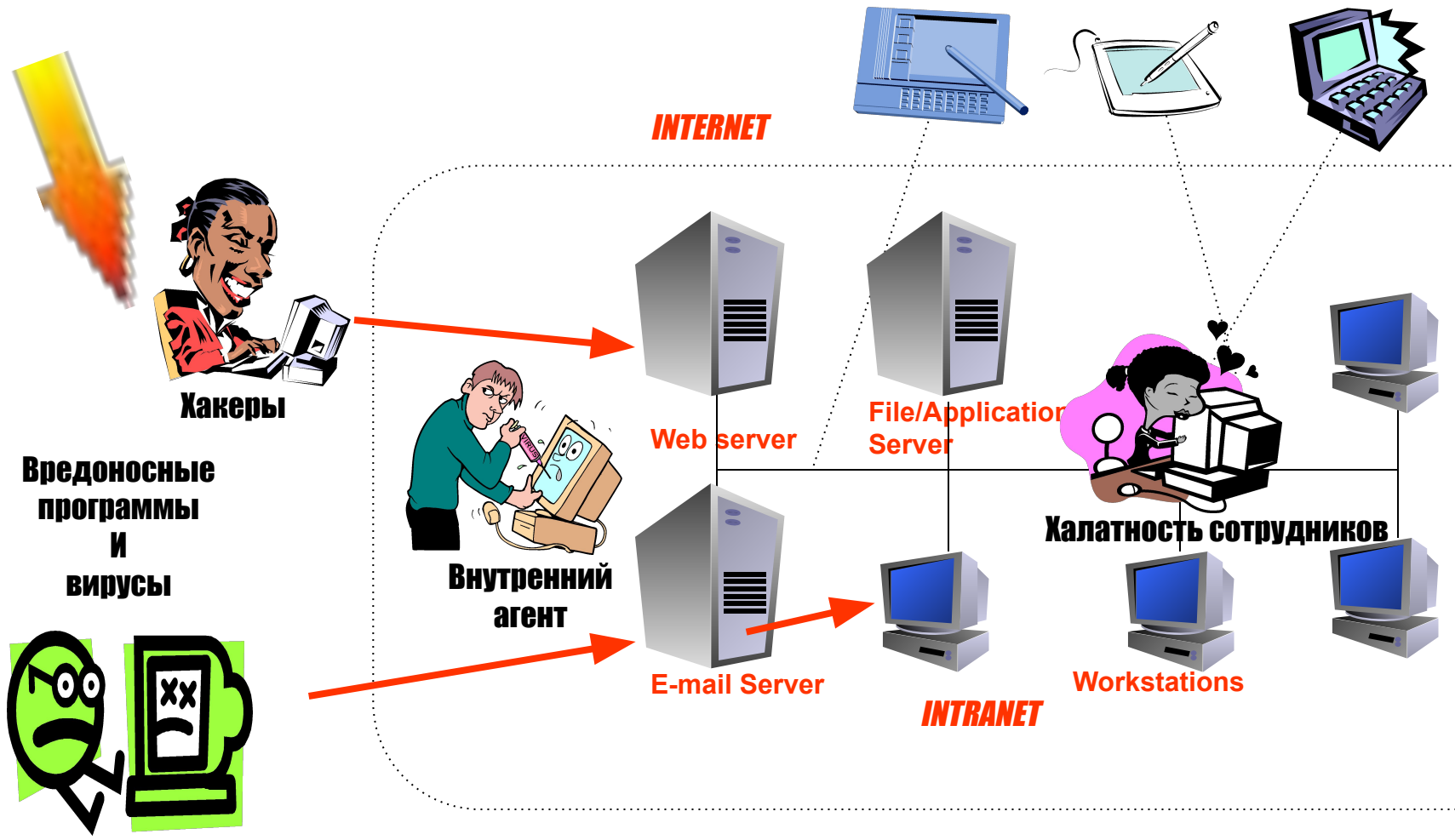
При этом под термином ВРЕДОНОСНАЯ ПРОГРАММА следует понимать программу, предназначенную для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы.

Национальный стандарт Российской Федераци
ГОСТ Р 50922-2006
Защита информации. Основные термины и определения.

Национальный стандарт Российской Федерации
ГОСТ Р 53113.1-2008.
Информационная технология.
Защита ИТ и АС от угроз информационной безопасности, реализуемых с использованием скрытых каналов.
Часть 1. Общие положения.

Каналы внешних атак:

A — внедрение вредоносных программ и данных



ВОПРОС 5.
Классификация угроз безопасности, реализуемых с использованием скрытых каналов

В современных условиях угрозы безопасности, которые могут быть реализованы с помощью СК, включают в себя следующие виды угроз.

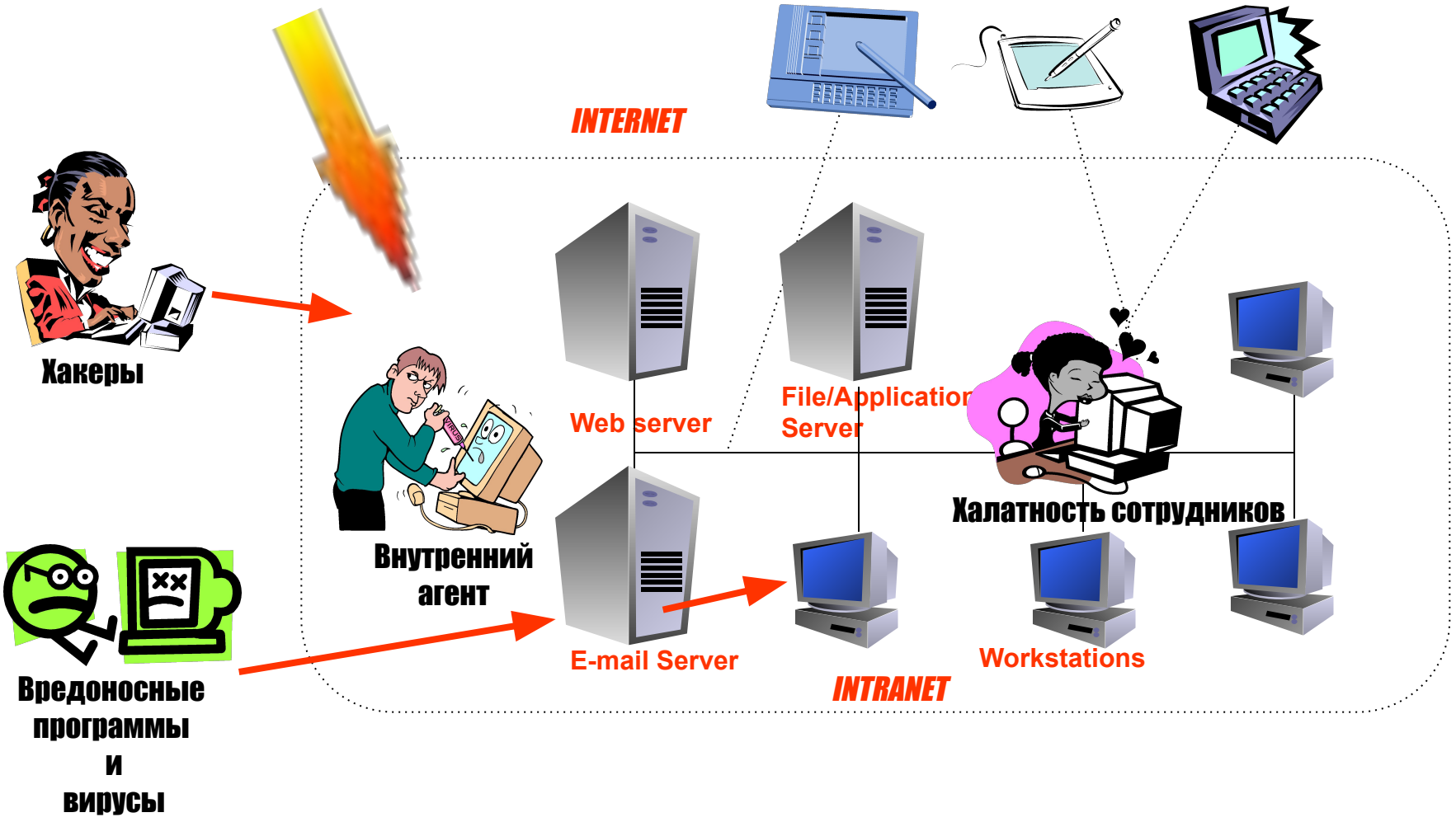
Б) ПОДАЧУ ЗЛОУМЫШЛЕННИКОМ КОМАНД АГЕНТУ ДЛЯ ВЫПОЛНЕНИЯ.

В данном случае агент нарушителя — это лицо, программное, программно-аппаратное или аппаратное средство, действующие в интересах нарушителя.

Национальный стандарт Российской Федерации
ГОСТ Р 53113.1-2008.
Информационная технология.
Защита ИТ и АС от угроз информационной безопасности, реализуемых с использованием скрытых каналов.
Часть 1. Общие положения.

Каналы внешних атак:

Б — подача злоумышленником команд агенту для выполнения



ВОПРОС 5.
Классификация угроз безопасности, реализуемых с использованием скрытых каналов

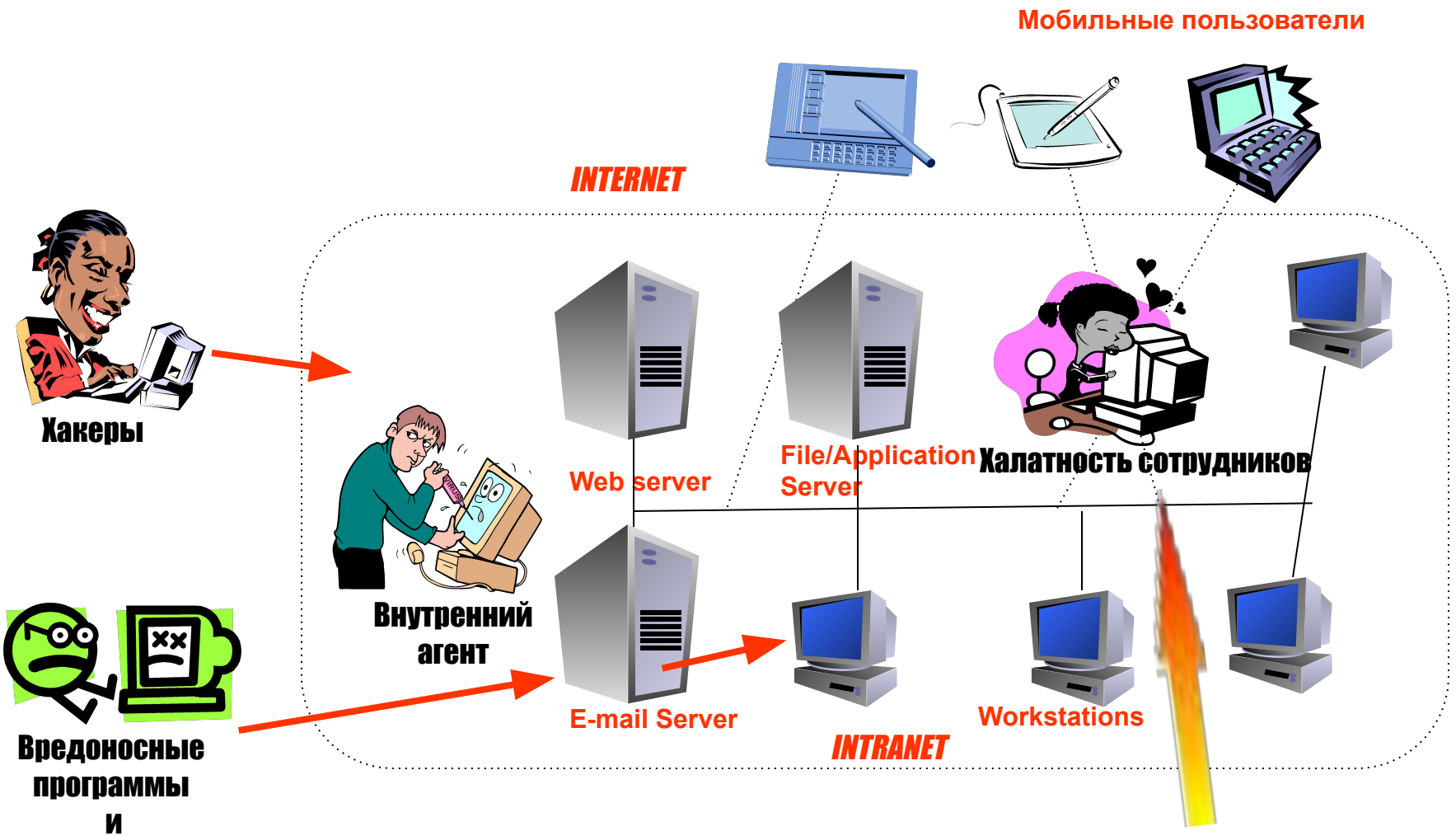
В современных условиях угрозы безопасности, которые могут быть реализованы с помощью СК, включают в себя следующие виды угроз.

В) УТЕЧКА КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ ИЛИ ПАРОЛЕЙ;

При этом под утечкой (информации) по техническому каналу следует понимать неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

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

Каналы внешних атак:



B — утечка криптографических ключей или паролей

ВОПРОС 5.
Классификация угроз безопасности, реализуемых с использованием скрытых каналов

В современных условиях угрозы безопасности, которые могут быть реализованы с помощью СК, включают в себя следующие виды угроз.

В) УТЕЧКА КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ ИЛИ ПАРОЛЕЙ;

Криптографический ключ (криптоключ) — совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.

Приказ ФАПСИ от 13 июня 2001 г. № 152
«Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»

ВОПРОС 5.
Классификация угроз безопасности, реализуемых с использованием скрытых каналов

В современных условиях угрозы безопасности, которые могут быть реализованы с помощью СК, включают в себя следующие виды угроз.

В) УТЕЧКА КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ ИЛИ ПАРОЛЕЙ;

При криптографической защите информации вместо словосочетания криптографический ключ часто используют просто слово ключ.

КЛЮЧ — конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований.

ГОСТ 28147-89
Системы обработки информации.
Защита криптографическая.
Алгоритм криптографического преобразования.

ВОПРОС 5.
Классификация угроз безопасности, реализуемых с использованием скрытых каналов

В современных условиях угрозы безопасности, которые могут быть реализованы с помощью СК, включают в себя следующие виды угроз.

В) УТЕЧКА КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ ИЛИ ПАРОЛЕЙ;

Термин «ПАРОЛЬ» в Российской Федерации также стандартизирован.

ПАРОЛЬ — конфиденциальная информация аутентификации, обычно состоящая из строки знаков.

Государственный стандарт Российской Федерации ГОСТ Р ИСО 7498-2-99 "Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации".

ПАРОЛЬ ДОСТУПА — идентификатор субъекта доступа, который является его (субъекта) секретом.

Национальный стандарт Российской Федерации ГОСТ Р 53113.1-2008. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения

ВОПРОС 5.
Классификация угроз безопасности, реализуемых с использованием скрытых каналов

В современных условиях угрозы безопасности, которые могут быть реализованы с помощью СК, включают в себя следующие виды угроз.

Г) УТЕЧКА ОТДЕЛЬНЫХ ИНФОРМАЦИОННЫХ ОБЪЕКТОВ.

ИНФОРМАЦИОННЫЙ ОБЪЕКТ — элемент программы, содержащий фрагменты информации, циркулирующей в программе.

В зависимости от языка программирования в качестве информационных объектов могут выступать переменные, массивы, записи, таблицы, файлы, фрагменты оперативной памяти и т.п.

Национальный стандарт Российской Федерации ГОСТ Р 53113.1-2008. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения.

ВОПРОС 6.

Реализация угроз безопасности, осуществляемых с использованием скрытых каналов

ВОПРОС 6.
Классификация угроз безопасности, реализуемых с использованием скрытых каналов

Угрозы безопасности, реализуемые с использованием скрытых каналов

могут привести к:

— нарушению конфиденциальности информационных активов;

— нарушению работоспособности ИТ и АС;

— блокированию доступа к ресурсам;

— нарушению целостности данных и ПО.

Национальный стандарт Российской Федерации ГОСТ Р 53113.1-2008. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения.

ВОПРОС 6.
Классификация угроз безопасности, реализуемых с использованием скрытых каналов

6.3 Системами, наиболее подверженным атакам с использованием СК, являются:

- многопользовательские распределенные системы;
- системы с выходом в глобальные сети;
- системы, использующие криптографические средства защиты;
- системы, использующие многоуровневую (мандатную) политику разграничения доступа;
- системы, программно-аппаратные агенты в которых не могут быть обнаружены (в связи с использованием программного и аппаратного обеспечения с недоступным исходным кодом и в связи с отсутствием конструкторской документации).

Национальный стандарт Российской Федерации ГОСТ Р 53113.1-2008. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения.

ВОПРОС 6.
Классификация угроз безопасности, реализуемых с использованием скрытых каналов

Взаимосвязь угроз, реализуемых с помощью скрытых каналов, с типами скрытых каналов в зависимости от их пропускной способности

Угрозы, реализуемые с помощью скрытых каналов	Тип скрытых каналов	
	Скрытые каналы с низкой пропускной способностью	Скрытые каналы с высокой пропускной способностью
Внедрение вредоносных программ и данных	+	+
Подача злоумышленником команд агенту для выполнения	+	+
Утечка криптографических ключей или паролей	+	+
Утечка отдельных информационных объектов	-	+
Примечание — знак «+» — означает, что имеется связь угрозы с соответствующим типом скрытого канала; знак «-» — означает, что связи не существует.		

ВОПРОС 7.

Классификация активов по степени опасности атак с использованием скрытых каналов

ВОПРОС 7.
Классификация активов по степени опасности атак с использованием скрытых каналов

1-й класс

АКТИВЫ, содержащие информацию, степень подверженности которой атакам, реализуемым с использованием СК. определяет собственник

2-й класс

АКТИВЫ, содержащие информацию ограниченного доступа или персональные данные и обрабатываемые в системах, имеющих технические интерфейсы с открытыми сетями или компьютерными системами общего доступа, а также компьютерными системами, не предполагающими защиту от утечки по техническим каналам.

3-й класс

АКТИВЫ, содержащие сведения, составляющие государственную тайну

ВОПРОС 7.
Классификация активов по степени опасности атак с использованием скрытых каналов

Особый класс активов,
которые уязвимы с точки зрения угроз, реализуемых с использованием СК с низкой пропускной способностью

Класс А — активы, связанные с функционированием критически важных объектов.

Например,
передача команды, способной инициализировать деструктивное воздействие на объект такого типа, может быть осуществлена по СК с низкой пропускной способностью.

Класс Б — активы, содержащие ключевую/парольную информацию, в том числе ключи криптографических систем защиты информации и пароли доступа к иным активам.

Например,
утечка ключевой/парольной информации по СК может поставить под угрозу функционирование всей информационной системы.

ВОПРОС 7.
Классификация активов по степени опасности атак с использованием скрытых каналов

КРИТИЧЕСКИ ВАЖНЫЕ ОБЪЕКТЫ —

Объекты, нарушение или прекращение функционирования которых приводит:

— к потере управления, разрушению инфраструктуры,

— необратимому негативному изменению или разрушению экономики страны, субъекта или административно-территориальной единицы

— или к существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях длительный период времени.

Национальный стандарт Российской Федерации ГОСТ Р 53113.1-2008. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения.

СПАСИБО
ЗА ВНИМАНИЕ