Введение в криптографию

Обязательный курс для студентов I курса магистерских программ «Открытые информационные системы» и «Программное обеспечение вычислительных сетей», для студентов II курса РКТ

Введение

- Основные понятия и определения
- Модель сетевой безопасности
  - Классификация сетевых атак
  - Сервисы безопасности
  - Механизмы безопасности
  - Модель сетевого взаимодействия
- Модель безопасности информационной системы

Основные понятия и определения

Источники:

- ISO (International Organization for Standardization) **Common Criteria for Information Technology Security Evaluation** (CC:2022)
- NIST (National Institute of Standards and Technology) **Glossary of Key Information Security Terms** (2013)
- **ФСТЭК** (ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ)

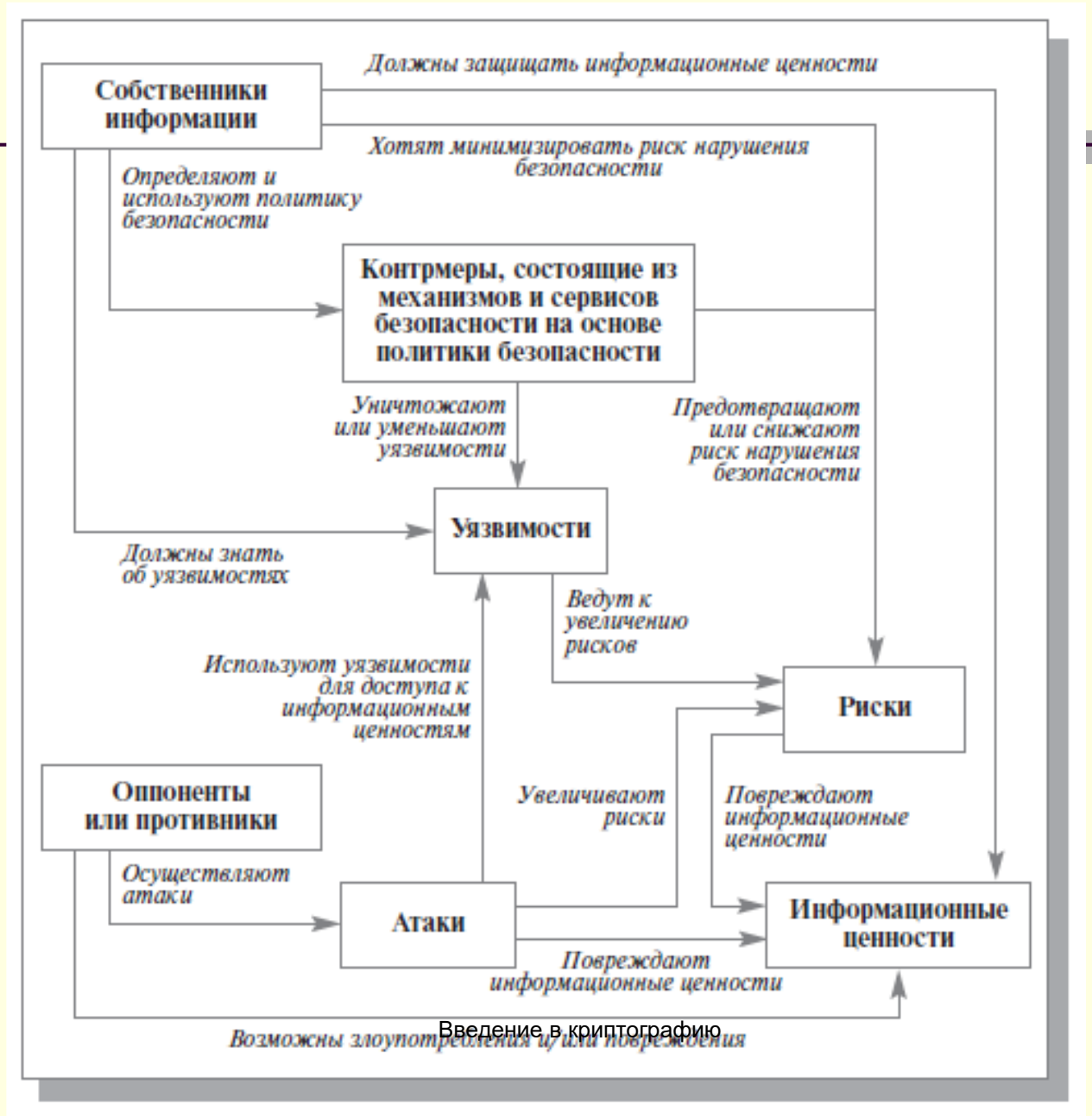
Основные понятия и определения

- Common Criteria (CC) - сравнивать результаты независимых оценок безопасности
  - Hardware
  - Firmware
  - Software

Общая модель:

Безопасность означает защиту активов в операционной среде.

Основные понятия и определения



Основные понятия и определения

Английский термин	Русский термин	Описание
Entity	Сущность	**Идентифицируемый элемент**, который описывается множеством **свойств**. Сущностями являются субъекты, пользователи, ИТ продукты (включая внешние), объекты, сессии, ресурсы. [CC] Это либо **субъект** (активный элемент, который выполняет операции над информацией или над состояние системы), либо **объект** (пассивный элемент, который содержит или получает информацию). [CC] Любой **участник аутентификационного обмена**; такой участник может как быть человеком, так и не быть, и может выполнять роль заявителя и/или проверяющего. [NIST]

Основные понятия и определения

Английский термин	Русский термин	Описание
Object	Объект	Сущность, которая является целью оценки с точки зрения безопасности и которая содержит или получает информацию и над которой субъект может выполнять операции. [CC] **Пассивная сущность** (например, устройства, файлы, записи, таблицы, процессы, программы, домены), которая содержит или получает информацию. Доступ к объекту предполагает доступ к информации, которая в нем содержится. [NIST]

Основные понятия и определения

Английский термин	Русский термин	Описание
Asset	Актив	Объект, представляющий **ценность для заинтересованных сторон**. Актив может быть материальным (например, физический объект, такой как аппаратное обеспечение, встроенное ПО, вычислительная платформа, сетевое устройство или другой технологический компонент) или нематериальным (например, люди, данные, информация, программное обеспечение, возможности, функции, услуги, товарные знаки, авторские права), патент, интеллектуальная собственность, имидж или репутация). Стоимость актива определяется заинтересованными сторонами с учетом потерь на протяжении всего жизненного цикла системы. [NIST]

Основные понятия и определения

Английский термин	Русский термин	Описание
Subject	Субъект	Сущность, которая **выполняет операции над объектами**. [CC] Обычно человек, процесс или устройство выполняют обмен информацией между объектами или изменение состояния системы. [NIST]
Information System Owner	Собственник информационной системы	Лицо, ответственное за закупку, разработку, интеграцию, модификацию или эксплуатацию и обслуживание информационной системы. [NIST]
Operation	Операция	Определенный тип действия, выполняемый субъектом над объектом. [CC]

Основные понятия и определения

Английский термин	Русский термин	Описание
Attack	Атака	Любой вид **вредоносной деятельности**, направленной на сбор, разрушение, предотвращение доступа, ухудшение качества или уничтожение ресурсов информационной системы или самой информации. Попытка получить **несанкционированный доступ** к системным службам, ресурсам или информации или попытка поставить под угрозу **целостность**, **доступность** или **конфиденциальность** системы. [NIST]
Attack surface	Поверхность атаки	Совокупность **логических или физических интерфейсов** к цели атаки, с помощью которых можно попытаться получить доступ к цели атаки и ее функциям. [CC] Набор точек на границе системы, системного элемента или среды, в которые злоумышленник может попытаться проникнуть, оказать воздействие или извлечь данные из этой системы, системного элемента или среды. [NIST]

Основные понятия и определения

Английский термин	Русский термин	Описание
Vulnerability	Уязвимость	**Слабое место в системе** (в объекте оценки), которое может быть использовано для нарушения требований безопасного функционирования оцениваемого объекта в некотором окружении. [CC] Слабое место в информационной системе, в системных процедурах безопасности, системах внутреннего управления или их реализации, которое используется или инициируется источником угрозы. Слабое место в системе, приложении или сети, которая может быть использована не по назначению, которое может стать источником угроз. [NIST]
Potential vulnerability	Потенциальная уязвимость	Предполагаемое, но не подтвержденное слабое место. [CC]

Основные понятия и определения

Английский термин	Русский термин	Описание
Attack signature	Сигнатура атаки	**Определенная последовательность событий**, указывающая на попытку несанкционированного доступа. [NIST]
Attack tree	Дерево атаки	Разветвленная иерархическая структура данных, которая представляет собой **совокупность потенциальных подходов к наступлению события**, при котором безопасность системы нарушена или скомпрометирована определенным образом. [NIST]

Основные понятия и определения

Английский термин	Русский термин	Описание
Threat	Угроза	Любое обстоятельство или событие, которое **потенциально может отрицательно повлиять** на деятельность организации (включая миссию, функции, имидж или репутацию), активы организации, отдельных лиц, другие организации с использованием информационной системы посредством несанкционированного доступа, уничтожения, раскрытия, изменения информации и/или отказ в обслуживании. Потенциальный источник нежелательного события. Вероятность того, что источник угрозы успешно воспользуется определенной уязвимостью информационной системы. [NIST]

Основные понятия и определения

Английский термин	Русский термин	Описание
Threat Analysis	Анализ угроз	**Исследование источников угроз** на предмет уязвимостей системы для определения угроз для конкретной системы в конкретной операционной среде. [NIST]
Threat Scenario	Сценарий угроз	**Совокупность дискретных событий**, связанных с конкретным источником угрозы или несколькими источниками угроз, частично упорядоченных во времени. [NIST]

Основные понятия и определения

Английский термин	Русский термин	Описание
Threat agent	Агент угроз	**Сущность**, которая потенциально может совершить **нежелательные действия** в отношении защищаемых активов. [CC] Примеры агентов угроз включают хакеров, злонамеренных пользователей, незлонамеренных пользователей, которые иногда допускают ошибки, компьютерные процессы и несчастные случаи. Владельцы активов могут воспринимать подобные угрозы как потенциальный источник обесценения активов, приводящий к снижению их стоимости. Нарушение, связанное с безопасностью, обычно включает, помимо прочего, потерю конфиденциальности активов, потерю целостности активов и потерю доступности активов.

Основные понятия и определения

Английский термин	Русский термин	Описание
Threat agent	Агент угроз	Таким образом, эти **угрозы порождают риски для активов**, основанные на вероятности реализации угрозы и воздействии на активы в случае реализации этой угрозы. Вследствие этого вводятся **меры обеспечения безопасности** для снижения рисков для активов. Эти меры обеспечения безопасности могут состоять из средств контроля, связанных с **ИТ** (например, МСЭ и смарт-карты) и **не-ИТ** средств контроля (например, охранники и процедуры входа). См. ISO/IEC 27001 и ISO/IEC 27002 для более общего обсуждения мер безопасности, а также того, как их внедрять и управлять ими. [NIST]
Adverse action	Вредоносное действие	**Действие**, выполняемое **агентом угроз над активом**. [CC]
Hacker	Хакер	Неавторизованный пользователь, который пытается получить или получает доступа к информационной системе. [NIST]

Основные понятия и определения

Английский термин	Русский термин	Описание
Security Goals	Цели безопасности	Пятью целями безопасности являются **конфиденциальность**, **доступность**, **целостность**, **подотчетность** и **гарантированность**. [NIST]
Security Service	Сервис безопасности	Сервис, который реализует **одну или несколько целей безопасности** или одно или несколько требований безопасности (например, конфиденциальность, целостность, доступность). Примерами сервисов безопасности являются управление ключами, управление доступом и аутентификация. [NIST] Для сервиса безопасности необходимо продемонстрировать, что: — Меры обеспечения безопасности **достаточны**, т.е. применяемые сервисы **минимизируют угрозы активам**. — Меры обеспечения безопасности **корректны**, т.е. применяемые сервисы делают то, что заявляют.

Основные понятия и определения

Английский термин	Русский термин	Описание
Risk	Риск	**Уровень воздействия на операции организации** (включая миссию, функции, имидж или репутацию), активы организации или отдельных лиц в результате работы информационной системы с учетом потенциального воздействия угрозы и вероятности возникновения этой угрозы.
IT-Related Risk	Риски, относящиеся к ИТ	**Вероятность** того, что конкретный источник угрозы воспользуется ею или использует конкретную уязвимость информационной системы Риски безопасности, связанные с информационными системами, — это те риски, которые возникают в результате потери конфиденциальности, целостности или доступности информации или информационных систем и учитывают неблагоприятное воздействие на операции организации (включая цели, функции, имидж или репутацию), активы организации. [NIST]

Основные понятия и определения

Английский термин	Русский термин	Описание
Security Mechanism	Механизм безопасности	**Программа и/или устройство**, предназначенное для реализации одного или нескольких сервисов безопасности, обычно оцениваемых с точки зрения надежности обслуживания и надежности конструкции. [NIST]
Security Requirements	Требования безопасности	Требования, предъявляемые к информационной системе, которые вытекают из **законов, распоряжений, директив, политик, стандартов, инструкций, правил и процедур, а также бизнес-обоснования организации**, необходимого для обеспечения конфиденциальности, целостности и доступности обрабатываемой, хранимой и передаваемой информации. [NIST]

Основные понятия и определения

Английский термин	Русский термин	Описание
Policy	Политика	Правила или утверждения, которые определяют **правильное или желаемое поведение объекта**. Например, политика авторизации может указывать правильные правила управления доступом для программного компонента. [CC]
Security Policy	Политика безопасности	Формулировка **требований к необходимой защите информационных объектов**. **Набор критериев** для организации сервисов безопасности. Определяет и ограничивает функционирование средств обработки данных, с целью обеспечения выполнения требования безопасности систем и данных. [NIST]

Основные понятия и определения

Английский термин	Русский термин	Описание
IT Security Policy	Политика ИТ-безопасности	**Задокументированные решения по ИТ безопасности** в организации. В NIST SP 800-12 выделены три базовых типа политики ИТ безопасности: 1) **Программная политика организации**— политика высокого уровня, используемая для создания программы ИТ-безопасности организации, определения ее объема внутри организации, распределения обязанностей по реализации, определения стратегического направления и выделения ресурсов для реализации. 2) **Политики решения конкретных проблем** — для решения конкретных вопросов, важных для организации, таких как планирование на случай непредвиденных обстоятельств, использование определенной методологии для управления системными рисками и внедрение новых правил или законов. Эта политика, вероятно, потребует более частого пересмотра по мере изменения технологий и связанных с ними факторов.

Основные понятия и определения

Английский термин	Русский термин	Описание
IT Security Policy	Политика ИТ-безопасности	3) **Политики, касающиеся отдельных систем**, например, создание списков управления доступом или обучение пользователей тому, какие действия в системе разрешены. Эти политики могут различаться от системы к системе в одной и той же организации. Кроме того, политика может относиться к совершенно другим вопросам, например, к конкретным управленческим решениям, определяющим политику электронной почты (электронной почты) организации или политику безопасности факсов. [NIST]

Основные понятия и определения

Английский термин	Русский термин	Описание
Environment, Environment of Operation	Окружение, условия эксплуатации	Совокупность **внешних процедур, условий и объектов**, влияющих на разработку, эксплуатацию и обслуживание информационной системы. [NIST] Физическое окружение, в котором информационная система обрабатывает, хранит и передает информацию. [NIST]

Основные понятия и определения

Английский термин	Русский термин	Описание
IT Security Architecture	Архитектура ИТ-безопасности	Описание **принципов безопасности и общего подхода к соблюдению принципов**, лежащих в основе проектирования системы; т.е. рекомендации по размещению и реализации конкретных сервисов безопасности в различных распределенных вычислительных средах. [NIST]

Основные понятия и определения

Английский термин	Русский термин	Описание
Operations Security (OPSEC)	Операционная безопасность	**Систематический и проверенный процесс**, с помощью которого предотвращаются атаки потенциальных противников путем выявления, контроля и защиты. Процесс включает в себя **пять этапов**: выявление критической информации, анализ угроз, анализ уязвимостей, оценка рисков и применение соответствующих контрмер. [NIST]

Модель сетевой безопасности

- Классификация сетевых атак
- Сервисы безопасности
- Механизмы безопасности
- Модель сетевого взаимодействия

Модель угрозы Долева-Яо

- Модель угрозы Долева-Яо — модель, предложенная в 1981 году Д. Долевым (Danny Dolev) и А. Яо (Andrew Yao), широко используемая в криптографии для описания среды, в которой происходит обмен шифрованными сообщениями, часто используется для формального анализа протоколов.
- Согласно модели, в такой уязвимой сети (например, Интернет) злоумышленник обладает следующими возможностями:

- Злоумышленник может получить любое сообщение, передаваемое по сети.
- Злоумышленник является авторизованным пользователем сети, и поэтому, в частности, имеет право устанавливать соединение с любым другим пользователем.
- Злоумышленник может стать стороной, принимающей сообщения от любой передающей стороны.
- Злоумышленник может посылать любому пользователю сообщения от имени любого другого пользователя.

Модель угрозы Долева-Яо

Модель угрозы Долева-Яо описывает наихудшего злоумышленника:

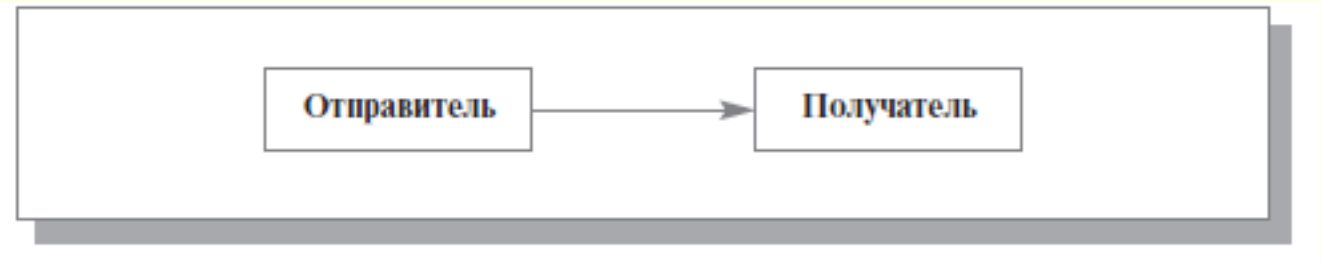
- видит все сетевые коммуникации,
- может читать любое сообщение,
- удалять или задерживать доставку любого сообщения,
- дублировать любое сообщение или
- иным образом синтезировать любое сообщение, для которого у злоумышленника есть доступ к соответствующим криптографическим ключам (если таковые имеются).

Модель угрозы Долева-Яо

- Тем не менее, злоумышленник не является всемогущим. В частности, в модели на него накладываются следующие ограничения:
  - не может угадывать случайные числа, выбранные из достаточно большого множества;
  - не может расшифровать не имея ключа, либо корректно зашифровать сообщение при условии использования некоторого идеального алгоритма шифрования;
  - не может найти закрытый ключ по открытому ключу (при использовании криптосистем с открытым ключом);
  - контролируя средства связи, злоумышленник, тем не менее, не может получить доступ к закрытым, внутренним ресурсам, например, к памяти или жёсткому диску пользователя.

Классификация сетевых атак

Информационный поток



I. Пассивная атака

Классификация сетевых атак

II. Активная атака

1. Отказ в обслуживании – DoS-атака (Denial of Service)

2. Модификация потока данных – атака «man in the middle»

Классификация сетевых атак

3. Создание ложного потока (фальсификация)

4. Повторное использование

Классификация нарушителей

- **Социальный статус** атакующих сильно влияет на силу их атак. Очевидно, что у рядового пользователя Интернета меньше возможностей, чем у целого мошеннического интернет-провайдера (ISP). Рядовой пользователь может использовать свою относительно небольшую пропускную способность для запуска атак, в то время как интернет-провайдер обычно также может отслеживать и изменять связь, злоупотреблять гораздо более широкой полосой пропускания и коррелировать шаблоны трафика.
- Если злоумышленники **объединяют в большие группы** отдельных пользователей/устройств (например, в форме ботнета), их общая мощность увеличивается.
- Злоумышленники также могут контролировать определенные **интернет-сервисы**, маршрутизаторы или любую их комбинацию. Мы также различаем внутренних и внешних злоумышленников, которые находятся либо внутри, либо за пределами доверенного домена соответственно.

Классификация нарушителей

Классификация злоумышленников:

- (i) где могут располагаться злоумышленники,
- (ii) кто они,
- (iii) какими возможностями они обладают.

Сервисы безопасности

- ***Конфиденциальность*** – предотвращение пассивных атак для передаваемых или хранимых данных
- ***Аутентификация*** – подтверждение того, что информация получена из законного источника, и получатель является требуемым
- ***Целостность*** – возможность получателя определить, что информация при передаче или хранении не изменилась

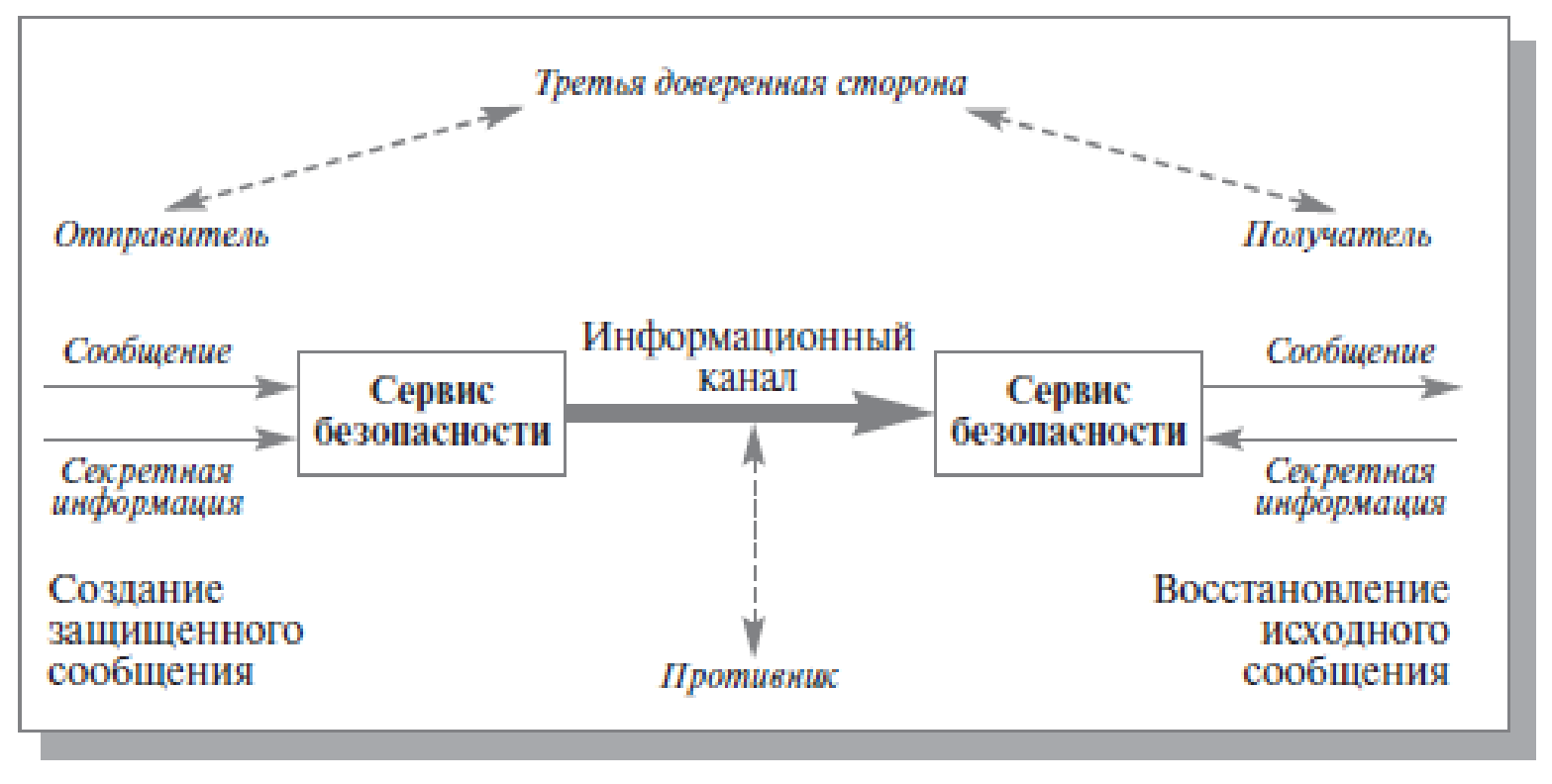
Сервисы безопасности

- ***Невозможность отказа*** – невозможность, как для получателя, так и для отправителя, отказаться от факта передачи
- ***Контроль доступа*** – возможность ограничить и контролировать доступ к системам и приложениям по коммуникационным каналам
- ***Доступность*** – минимизация возможности осуществления DoS-атак

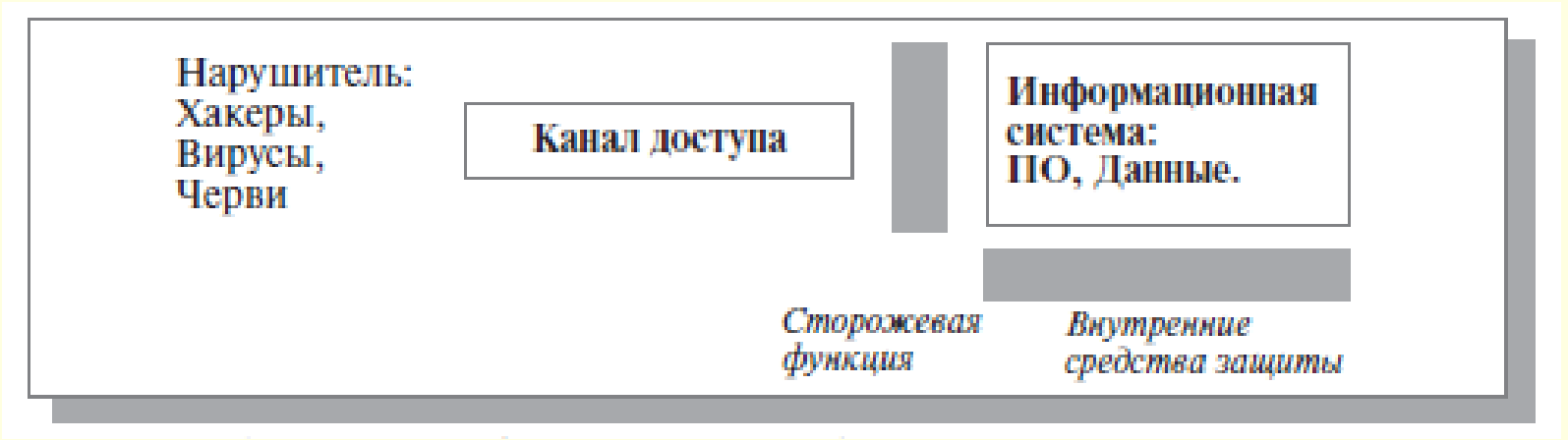
Механизмы безопасности

- ***Алгоритмы симметричного шифрования*** – алгоритмы шифрования, в которых для шифрования и расшифрования используется один и тот же ключ
- ***Алгоритмы асимметричного шифрования*** – алгоритмы шифрования, в которых для шифрования и расшифрования используются два разных ключа, называемые открытым и закрытым ключами, причем, зная один из ключей, вычислить другой невозможно
- ***Хеш-функции*** – функции, входным значением которых является сообщение произвольной длины, а выходным значением – сообщение фиксированной длины

Модель сетевого взаимодействия



Модель безопасности информационной системы



Управление доступом - концепция нулевого доверия (ZeroTrust – ZT)

- В ZT предполагается, что атакующий может присутствовать в среде предприятия, и что эта среда, принадлежащая предприятию, ничем не отличается (т.е. не более безопасна) от любой среды, не принадлежащей предприятию. Эти сервисы должны давать ответы на следующие вопросы:
  - Каков уровень уверенности в **идентификации субъекта**, выполняющего запрос?
  - Является ли **доступ к ресурсу допустимым** при данном уровне уверенности в идентификации субъекта?
  - **Устройство**, используемое для запроса, обладает **достаточными характеристиками безопасности**?
  - Существуют ли **другие факторы**, которые должны быть рассмотрены и которые могут изменить уровень доверия (например, время, расположение субъекта, характеристики безопасности субъекта)?

Управление доступом - концепция нулевого доверия (ZeroTrust)

Базовые принципы ZTA

1. Все источники данных и вычислительные сервисы считаются **ресурсами**.
2. Все **коммуникации должны быть защищены** не зависимо от сетевого местоположения.
3. Доступ к отдельным ресурсам предприятия **предоставляется на сессию**.
4. Доступ к ресурсу **определяется динамической политикой** на основе идентификации клиента, приложения/сервиса и запрашиваемых информационных ценностей, могут также учитываться различные атрибуты клиента, приложения/сервиса и окружения.

Управление доступом - концепция нулевого доверия (ZeroTrust)

Сеть с точки зрения ZT

1. **Не считается**, что вся локальная сеть предприятия находится в неявной зоне доверия.
2. Устройства в сети **могут не быть в собственности предприятия** или не быть им конфигурируемыми (BYOD устройства).
3. **Не все ресурсы** предприятия находятся в его собственности.
4. Удаленные субъекты и активы предприятия **не могут полностью быть доверяемыми** при их присоединении к локальной сети.
5. Активы и потоки, проходящие между инфраструктурами предприятия и не-предприятия, должны иметь **согласованные политику и состояние безопасности**.