

Национальный исследовательский
ядерный университет "МИФИ"



**Угрозы безопасности информации,
связанные с целенаправленными атаками
на компьютерные системы и
несанкционированным доступом**

Муравьёв С.К.



Кафедра №43
Стратегические информационные исследования

Компьютерная система

ГОСТ Р ИСО/МЭК ТО 10032-2007

Компьютерная система (computer system): Совокупность аппаратных средств, управляемых программным обеспечением (операционной системой) как единый модуль. Компьютерная система может также предоставлять общие услуги, такие как управление доступом, взаимодействие процессоров и графический интерфейс пользователя.

Конвенция о преступности в сфере компьютерной информации

Компьютерная система — любое устройство или группа взаимосвязанных или смежных устройств, одно или более из которых, действуя в соответствии с программой, осуществляет автоматизированную обработку данных.

Компьютерная атака

ГОСТ Р 51275-2006

Компьютерная атака - целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств.

Федеральный закон от 26 июля 2017 г. N 187-ФЗ

Компьютерная атака - целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации

Информационная технология. Методы и средства обеспечения безопасности СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

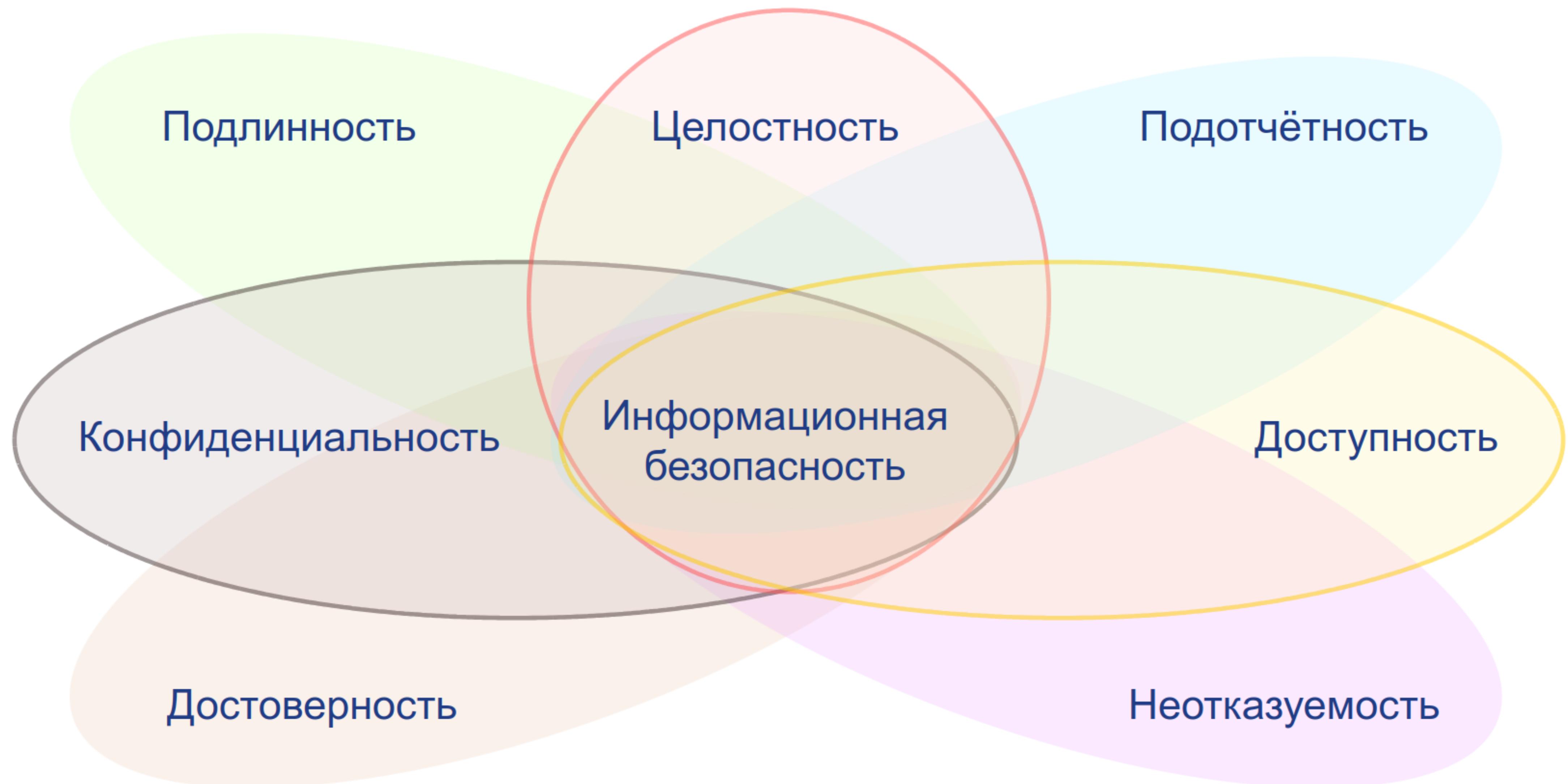
2.4 атака (attack)

Попытка уничтожения, раскрытия, изменения, блокирования, кражи, получения несанкционированного доступа к активу или его несанкционированного использования.

2.3 актив (asset)

Что-либо, что имеет ценность для организации (информация, программное обеспечение, материальные активы, услуги, люди и их квалификация, навыки и опыт, нематериальные активы, такие как репутация и имидж

Информационная безопасность



Основные свойства ИБ

2.9 конфиденциальность (confidentiality)

Свойство информации быть недоступной или закрытой для неавторизованных лиц, сущностей или процессов

2.25 целостность (integrity)

Свойство сохранения правильности и полноты активов

2.7 доступность (availability)

Свойство быть доступным и готовым к использованию по запросу авторизованного субъекта

Другие свойства ИБ

2.6 подлинность (authenticity)

Свойство, гарантирующее, что субъект или ресурс идентичен заявленному

2.2 подотчетность (accountability)

Ответственность субъекта за его действия и решения

2.27 неотказуемость (non-repudiation)

Способность удостоверять имевшее место событие или действие и их субъекты так, чтобы это событие или действие и субъекты, имеющие к нему отношение, не могли быть поставлены под сомнение

2.33 достоверность (reliability)

Свойство соответствия предусмотренному поведению и результатам

Статистика атак



Ущерб для
мирового
бизнеса

400
млрд. \$

Ущерб для
России

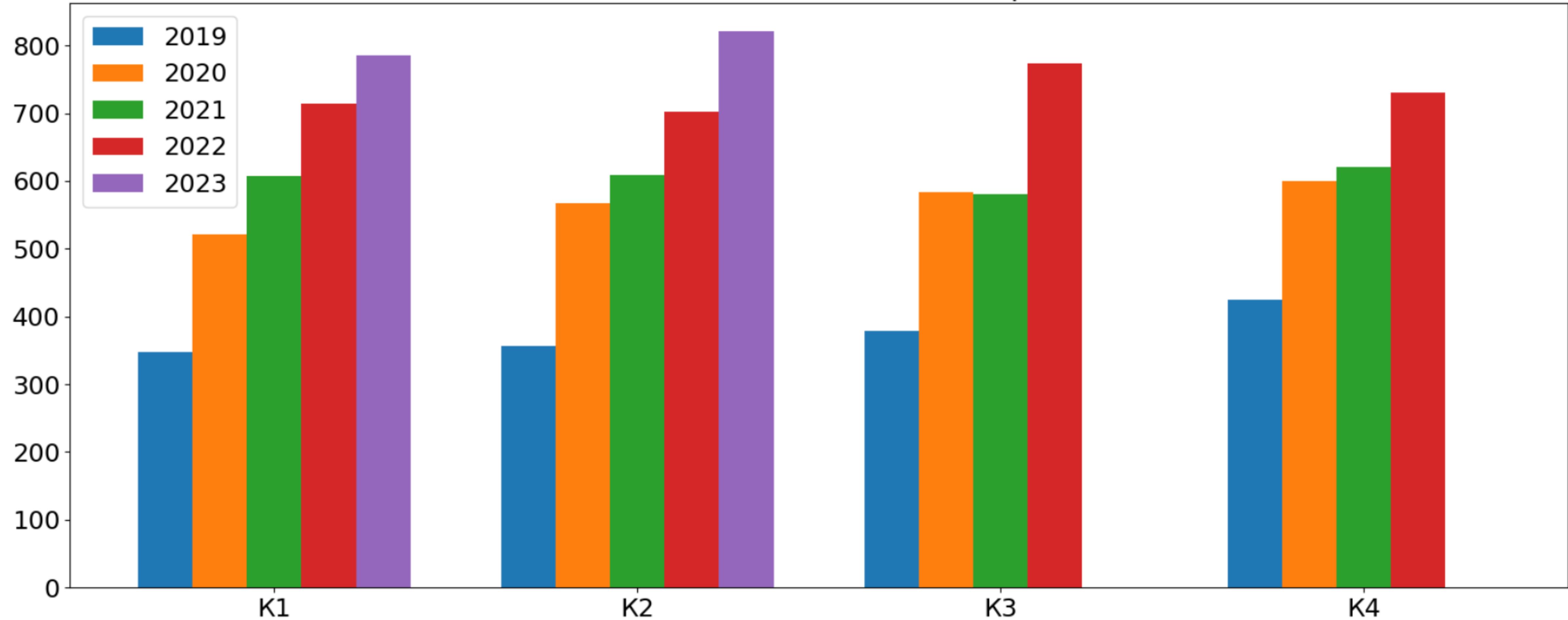
203
млрд. руб.

1
трлн. \$

1,5
трлн. \$

Актуальные киберугрозы

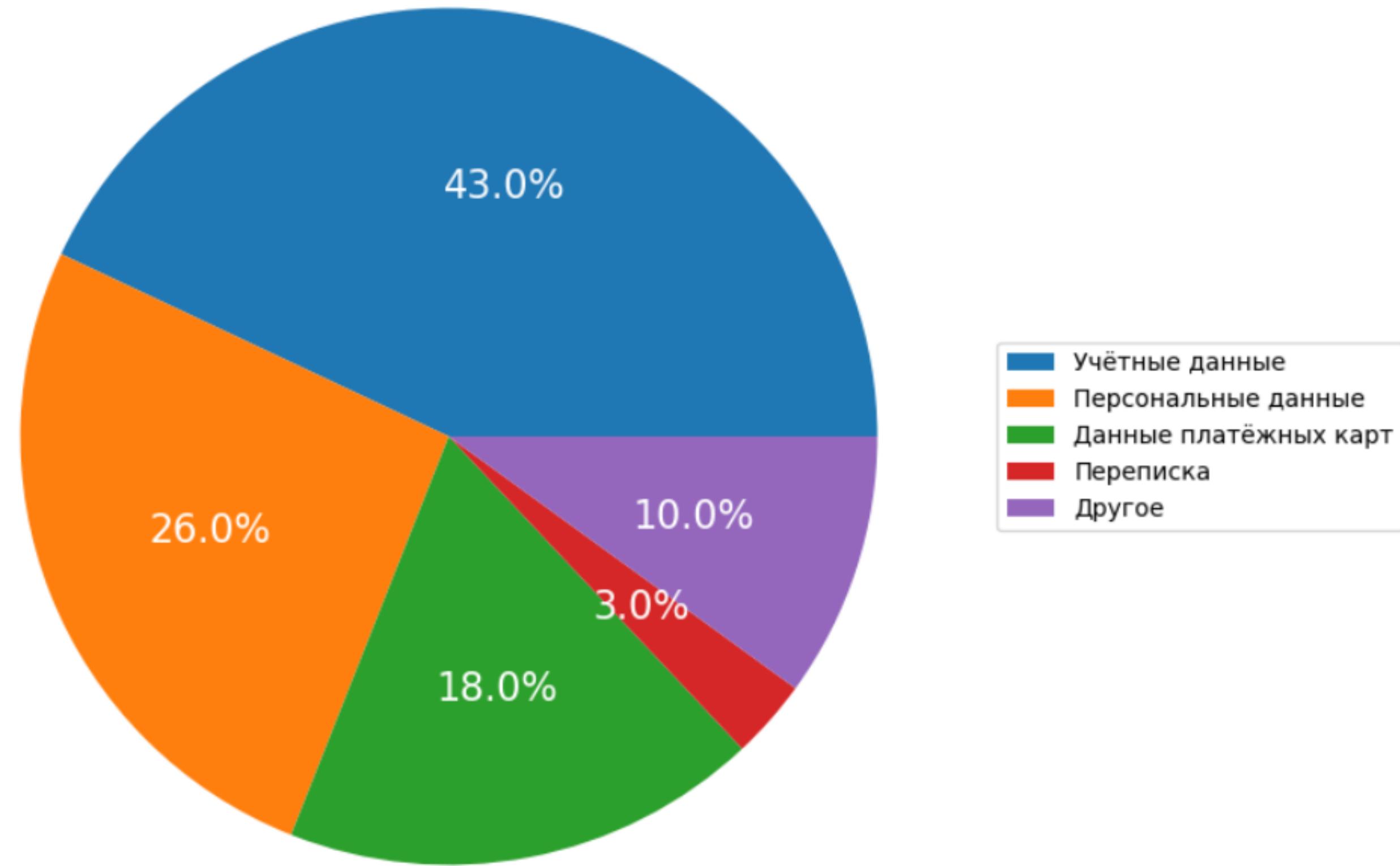
Количество инцидентов по кварталам



Актуальные киберугрозы: 3 квартал 2023 года

Атаки на частных лиц 2023 году

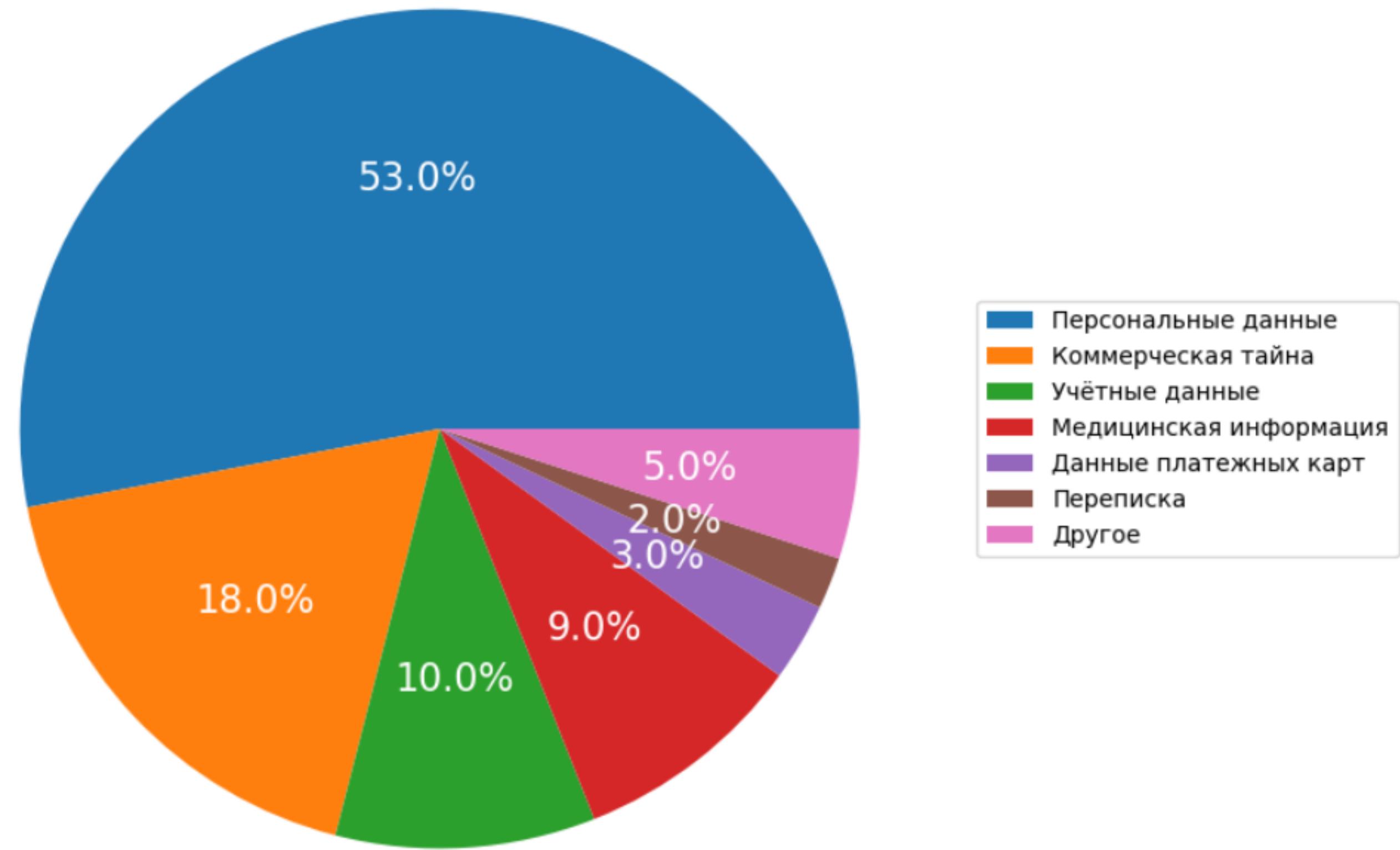
15% атак направлены против частных лиц



Актуальные киберугрозы: 2 квартал 2023 года

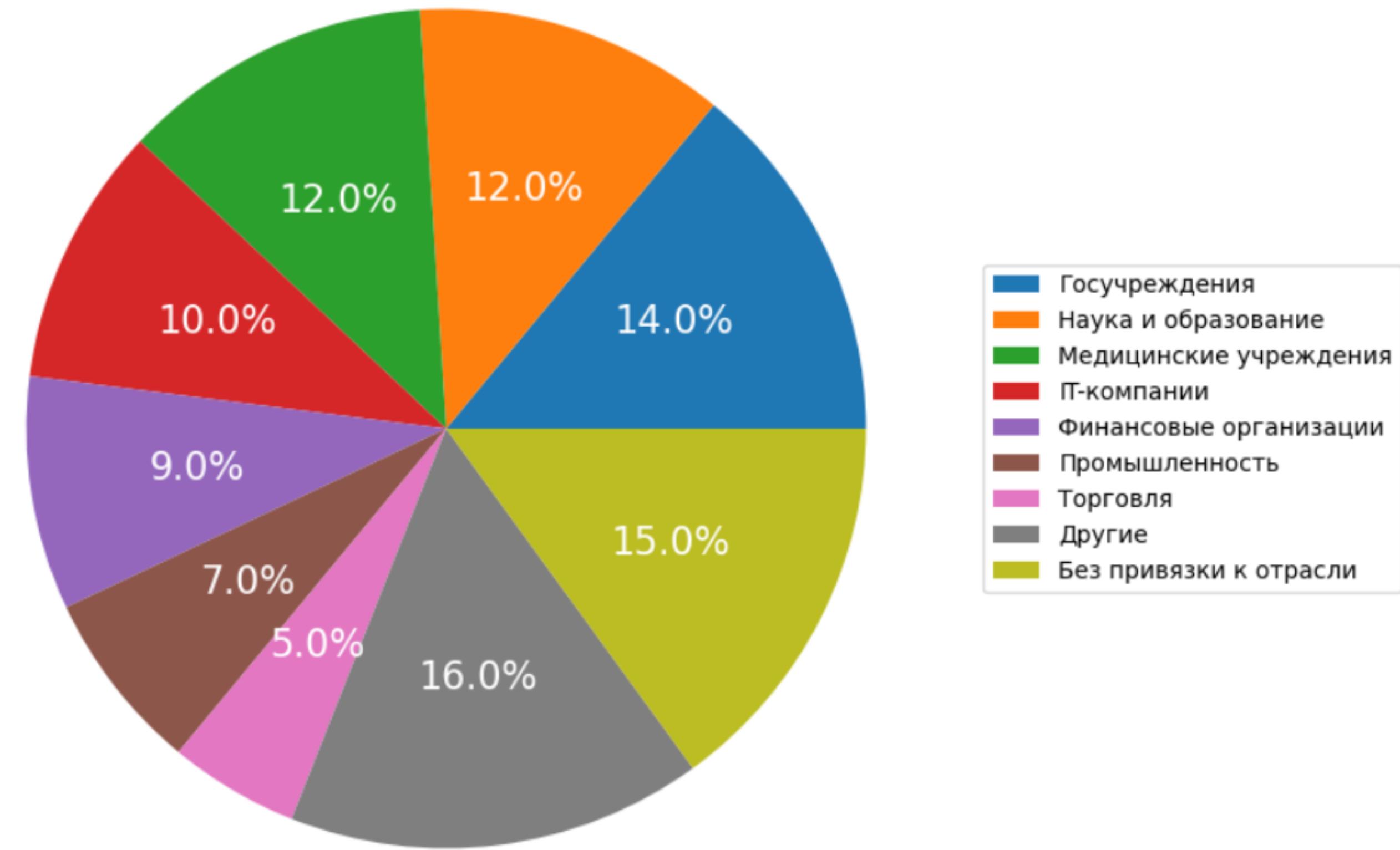
Атаки на организации в 2023 году

78% атак носили целенаправленный характер



Актуальные киберугрозы: 2 квартал 2023 года

Категории жертв среди организаций в 2023 году



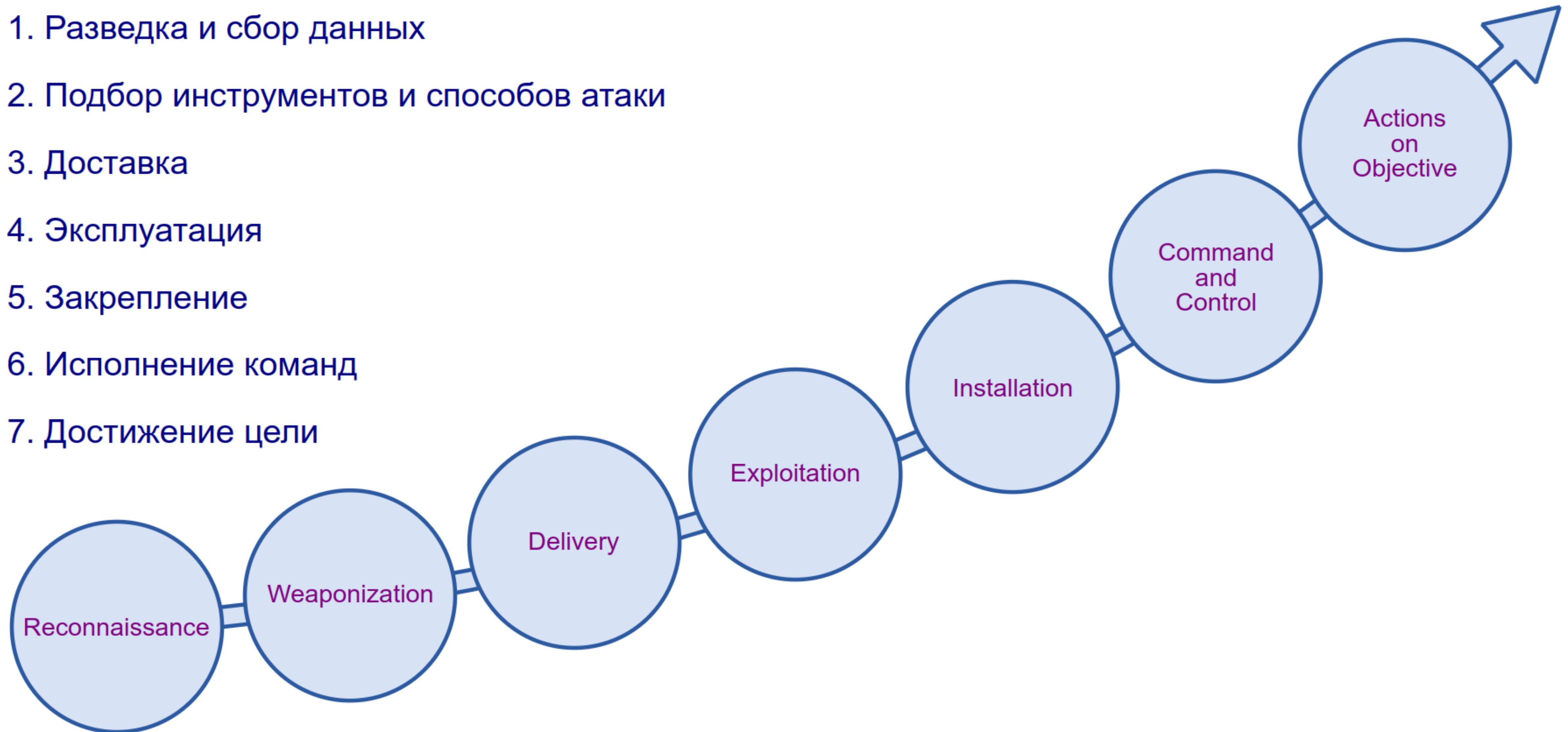
Актуальные киберугрозы: 2 квартал 2023 года

Основные типы атак

- ◆ Криптографические атаки
- ◆ Парольные атаки
- ◆ Атаки отказа в обслуживании
- ◆ Атаки на программный код и приложения
- ◆ Атаки социальной инженерии
- ◆ Сетевые атаки
- ◆ Физические атаки

Жизненный цикл атак (Kill chain)

1. Разведка и сбор данных
2. Подбор инструментов и способов атаки
3. Доставка
4. Эксплуатация
5. Закрепление
6. Исполнение команд
7. Достижение цели

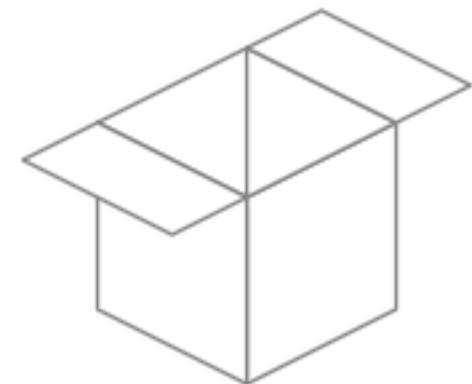


Реагирование на инциденты



Тестирование на проникновение

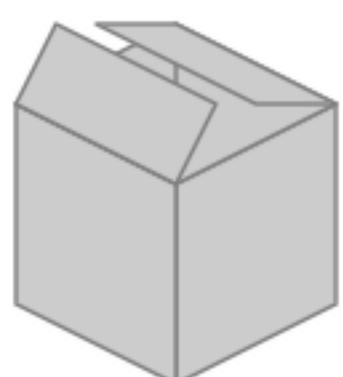
Тестирование на проникновение (Penetration test, pentest) — метод оценки безопасности компьютерных систем или сетей средствами моделирования атаки злоумышленника.



Метод "белого ящика" - доступна вся информация о системе и имеется доступ ко всем её компонентам.



Метод "черного ящика" - о тестируемой системе ничего не известно. Информация должна быть получена в процессе тестирования.



Метод "серого ящика" - доступна только ограниченная информация, позволяющая провести атаку.

Методология проведения тестирования

- ◆ Руководство по тестированию Open Web Application Security Project (OWASP — открытый проект обеспечения безопасности веб-приложений)
- ◆ Payment Card Industry Data Security Standard (PCI DSS) — стандарт безопасности данных индустрии платёжных карт, разработанный Советом по стандартам безопасности индустрии платежных карт
- ◆ NIST SP 800-115 — техническое руководство по тестированию и оценке информационной безопасности американского национального института стандартизации (National Institute of Standards and Technology, NIST)
- ◆ Руководство по методологии тестирования безопасности с открытым исходным кодом (Open Source Security Testing Methodology Manual, OSSTMM)
- ◆ Стандарт проведения тестов на проникновение (Penetration Testing Execution Standard, PTES)

Подготовка к тестированию

- ◆ Сбор требований
- ◆ Подготовка плана тестирования
- ◆ Ограничения тестирования
- ◆ Определение целей организации
- ◆ Управление проектами и планирование

Сбор требований

- ◆ Основная информация об организации
- ◆ Ключевые цели тестирования
- ◆ Тип тестирования
- ◆ Среда тестирования
- ◆ План аварийного восстановления
- ◆ Ответственные лица
- ◆ Сроки тестирования
- ◆ Другие требования

Подготовка плана тестирования

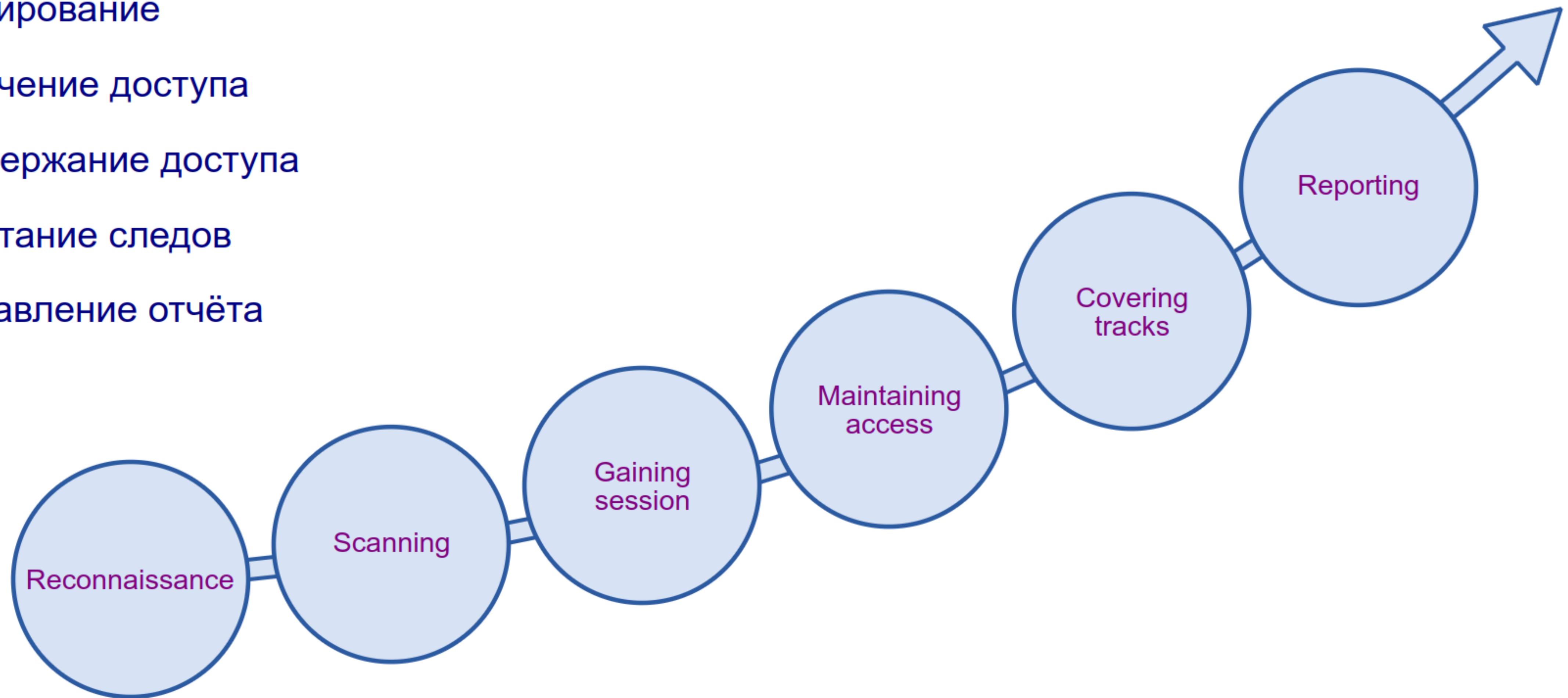
- ◆ Порядок тестирования
- ◆ Распределение ресурсов
- ◆ Анализ затрат
- ◆ Соглашение о неразглашении
- ◆ Контракт на тестирование
- ◆ Правила взаимодействия

Ограничения тестирования

- ◆ Технологические ограничения
- ◆ Ограничения знаний
- ◆ Другие ограничения инфраструктуры

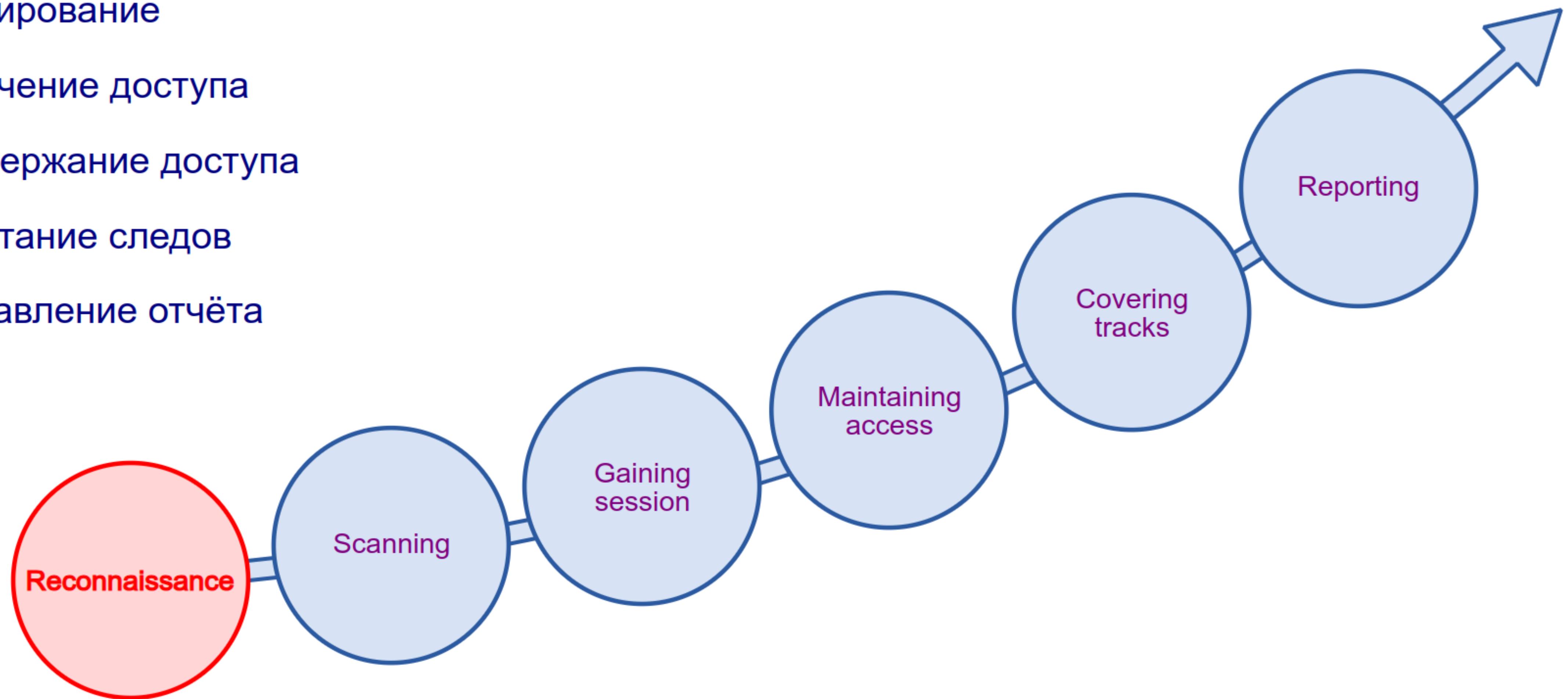
Стандартные этапы тестирования

1. Разведка и сбор данных
2. Сканирование
3. Получение доступа
4. Поддержание доступа
5. Заметание следов
6. Составление отчёта



Разведка и сбор данных

1. Разведка и сбор данных
2. Сканирование
3. Получение доступа
4. Поддержание доступа
5. Заметание следов
6. Составление отчёта



Подходы к разведке и сбору данных

Пассивный сбор

Сбор данных осуществляется во внешних источниках, что делает практически невозможным обнаружение исполнителя.

Активный сбор

Подразумевается взаимодействие с целевой инфраструктурой, которое фиксируется в журналах, может быть обнаружено администраторами или системами обнаружения вторжений.

Также возможно непосредственное взаимодействие со специалистами, взаимодействующими с целевой системой.

Основные методы пассивного сбора данных

- ◆ Использование поисковых систем
- ◆ Сбор данных из социальных сетей
- ◆ Анализ данных на официальном сайте
- ◆ Анализ данных из объявлений о вакансиях
- ◆ Исследование выброшенной документации и носителей информации
- ◆ Использование методов социальной инженерии

Основные методы активного сбора данных

- ◆ Прямое взаимодействие с инфраструктурой
- ◆ Контакты с сотрудниками целевой организации

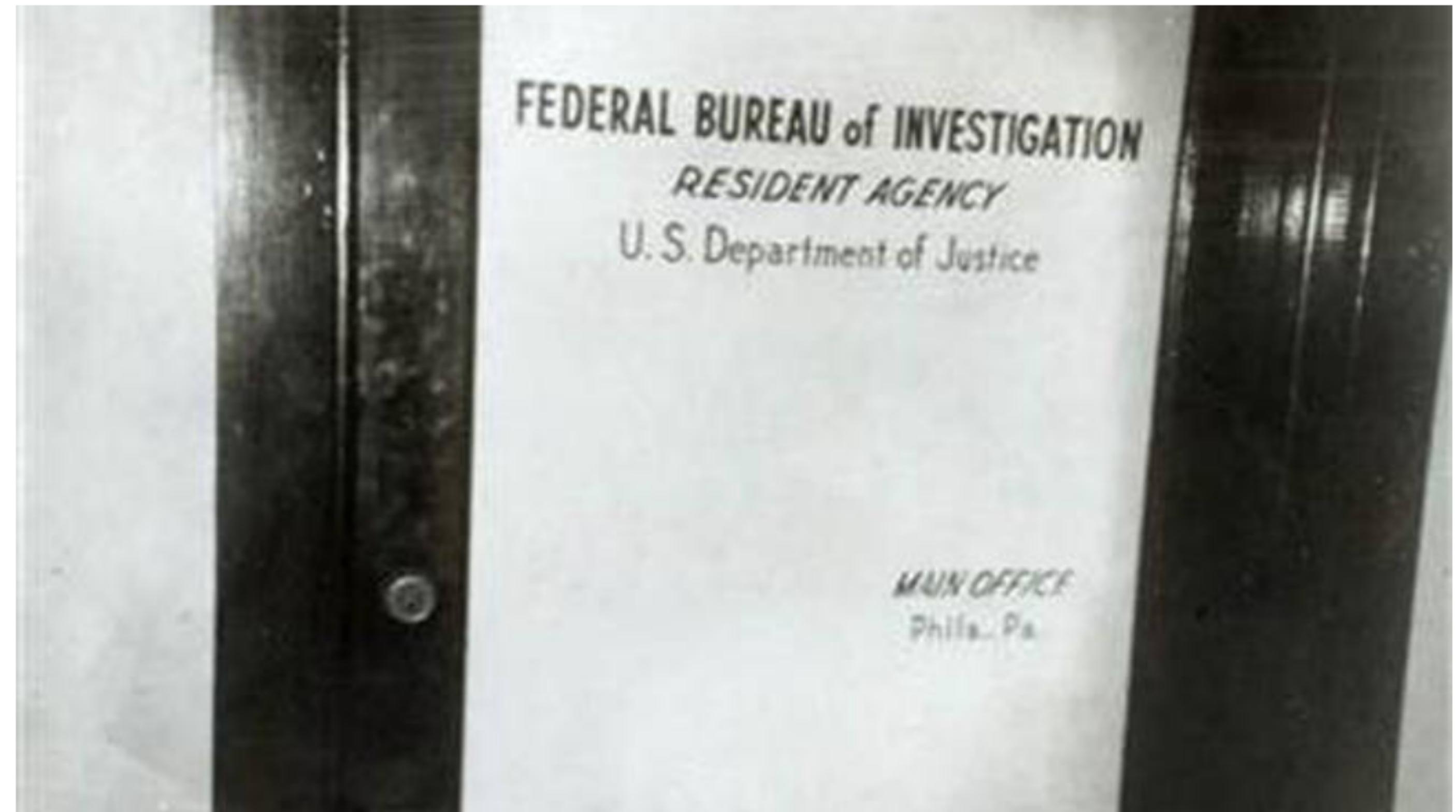
Разведка на основе открытых источников

Open source intelligence (OSINT) — разведывательная дисциплина, включающая в себя поиск, выбор и сбор разведывательной информации из общедоступных источников, а также её анализ.

- ◆ СМИ — газеты, журналы, радио, телевидение.
- ◆ Интернет, социальные сети, видеохостинги, блоги, форумы и другой контент, созданный пользователями
- ◆ Публичные отчёты, официальные данные о бюджетах, материалы пресс-конференций, различные публичные заявления.
- ◆ Наблюдения — радиомониторинг, использование общедоступных данных дистанционного зондирования земли и аэрофотосъемок
- ◆ Профессиональные и академические отчёты, конференции, доклады, статьи и другая специализированная литература

Методы социальной инженерии

- ◆ Подражание
- ◆ Взаимный обмен
- ◆ Влияние авторитета
- ◆ Использование жадности
- ◆ Налаживание социальный взаимоотношений
- ◆ Сила любопытства



Social-engineering the FBI in 1971

Собираемые данные

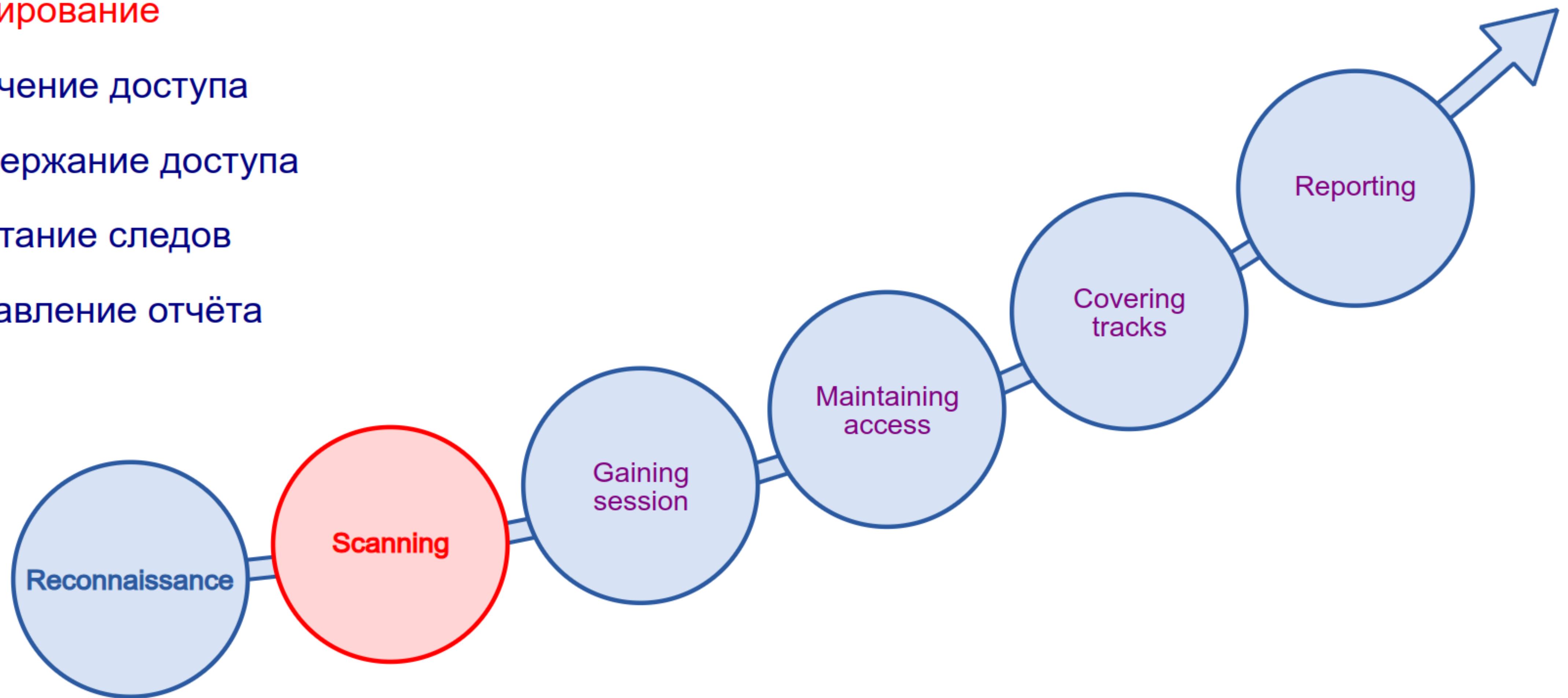
- ◆ Имена контактных лиц организации
- ◆ Адреса электронной почты и телефоны сотрудников организации
- ◆ Организационная структура и функционал подразделений
- ◆ Режим работы ключевых сотрудников и подразделений
- ◆ Резюме действующих и бывших сотрудников, данные о вакансиях
- ◆ Сведения о поставщиках услуг и потребителях
- ◆ Используемое оборудование и программное обеспечение
- ◆ Сведения об используемых доменах и поддоменах

Примеры открытых источников

Ресурс	Описание
archive.org	Просмотр истории изменения сайтов
robtex.com	Информация о домене и сети
reg.ru/whois	Информация о доменах
hh.ru	Сведения о вакансиях и компаниях
egrul.nalog.ru/	Сведения из ЕГРЮЛ/ЕГРИП
spark-interfax.ru/	Сведения о компаниях
e-disclosure.ru	Центр раскрытия корпоративной информации

Сканирование

1. Разведка и сбор данных
2. Сканирование
3. Получение доступа
4. Поддержание доступа
5. Заметание следов
6. Составление отчёта



Задачи сканирования

- ◆ Обнаружение сетевых устройств
- ◆ Определение топологии сети
- ◆ Идентификация операционных систем
- ◆ Перечисление и определение версий сетевых служб
- ◆ Поиск уязвимостей

Виды сканирования

Пассивное сканирование

Осуществляется перехват и анализ передаваемых по сети пакетов, исследование ARP-таблиц.

Активное сканирование

Подразумевает передачу сетевых пакетов и анализ реакции исследуемой системы.

Перерыв

Перерыв

<https://smurav.github.io/ta43/pk23>

Open Systems Interconnection

В 1982 году Международная организация по стандартизации (ISO) начала новый проект в области сетевых технологий, ориентированный на стандартизацию взаимодействия открытых систем, Open Systems Interconnection или OSI.

До OSI сетевые технологии были полностью проприетарными, основанными на несовместимых корпоративных стандартах. Проект OSI сформировал основу для обеспечения совместимости решений разных поставщиков.

Проект OSI свёрнут в 1996 году и большинство протоколов и спецификаций уже не используются.



Сетевая модель OSI

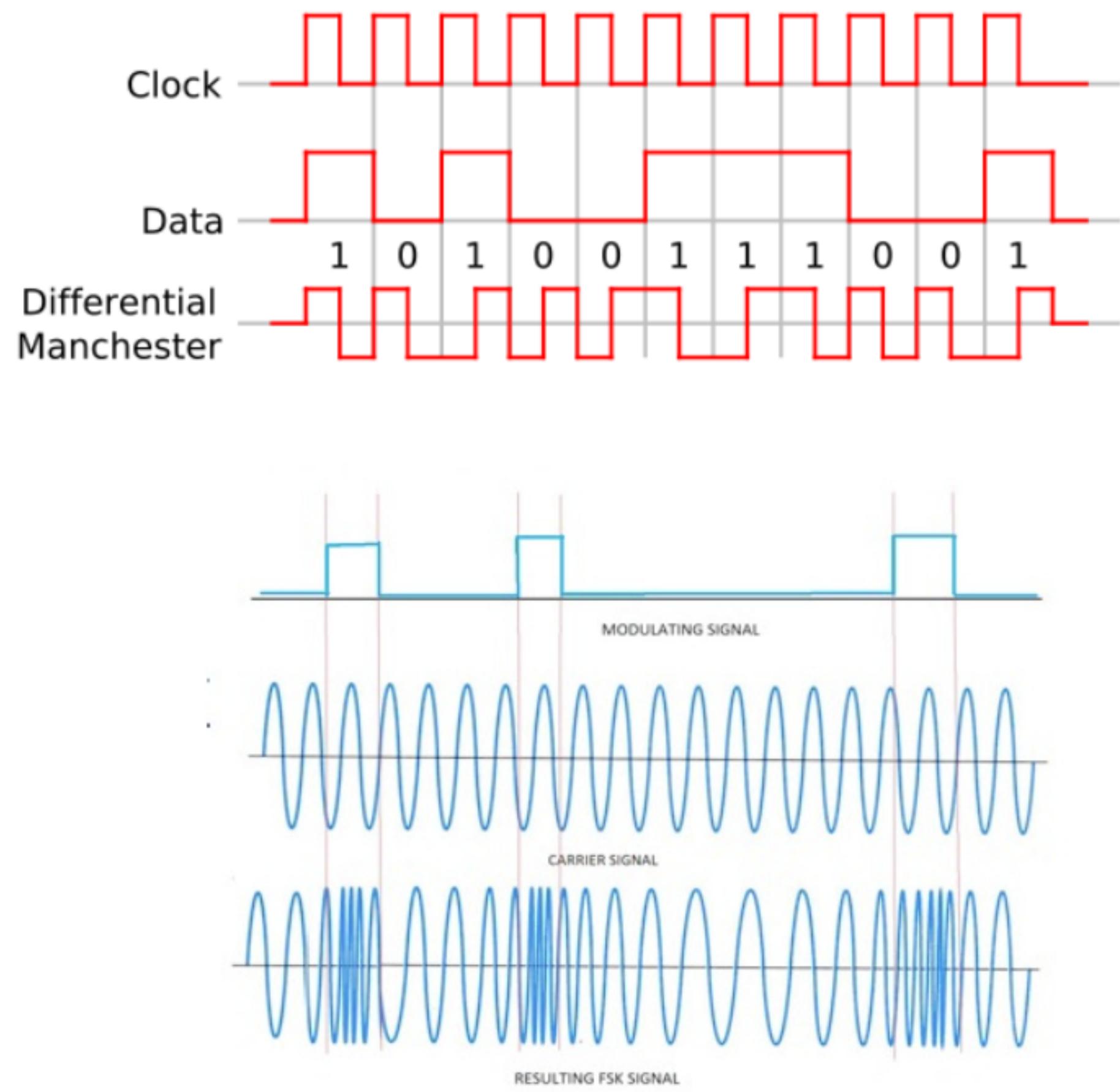
Уровень	Функции	Единица передачи
7. Прикладной	Доступ к сетевым службам	
6. Представления	Преобразование данных и кодирование/декодирование	Сообщение
5. Сеансовый	Управление сеансом связи	
4. Транспортный	Прямая связь между конечными пунктами и надёжность	Сегмент / Датаграмма
3. Сетевой	Определение маршрута и логическая адресация	Пакет
2. Канальный	Физическая адресация	Кадр
1. Физический	Работа со средой передачи и сигналами	Бит

Физический уровень

Физический уровень (physical layer) — нижний уровень модели, который определяет физическую и электрическую среду передачи данных.

На этом уровне описываются параметры сигналов, такие как амплитуда, частота, фаза, используемая модуляция. Решаются вопросы, связанные с синхронизацией, избавлением от помех, скоростью передачи данных.

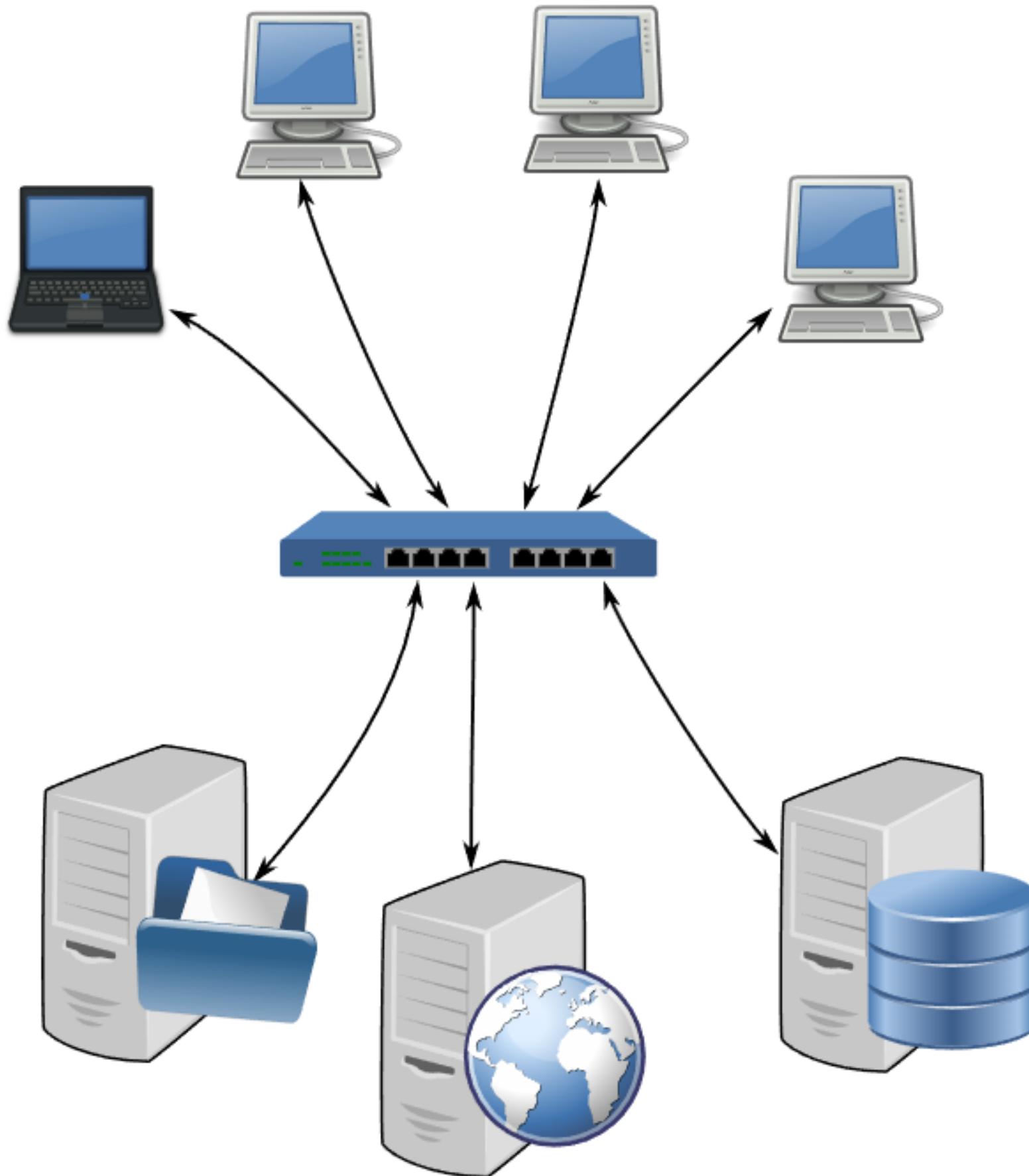
Физический уровень описывает способы передачи бит через физические среды линий связи, соединяющие сетевые устройства.



Канальный уровень

Канальный уровень (data link layer) — второй уровень сетевой модели OSI, предназначенный для обмена данными между узлами находящимися в том же сегменте локальной сети, путем передачи специальных блоков данных, которые называются кадрами (frame).

В процессе формирования кадров данные снабжаются служебной информацией (заголовком), необходимой для корректной доставки получателю, и, в соответствии с правилами доступа к среде передачи, отправляются на физический уровень.



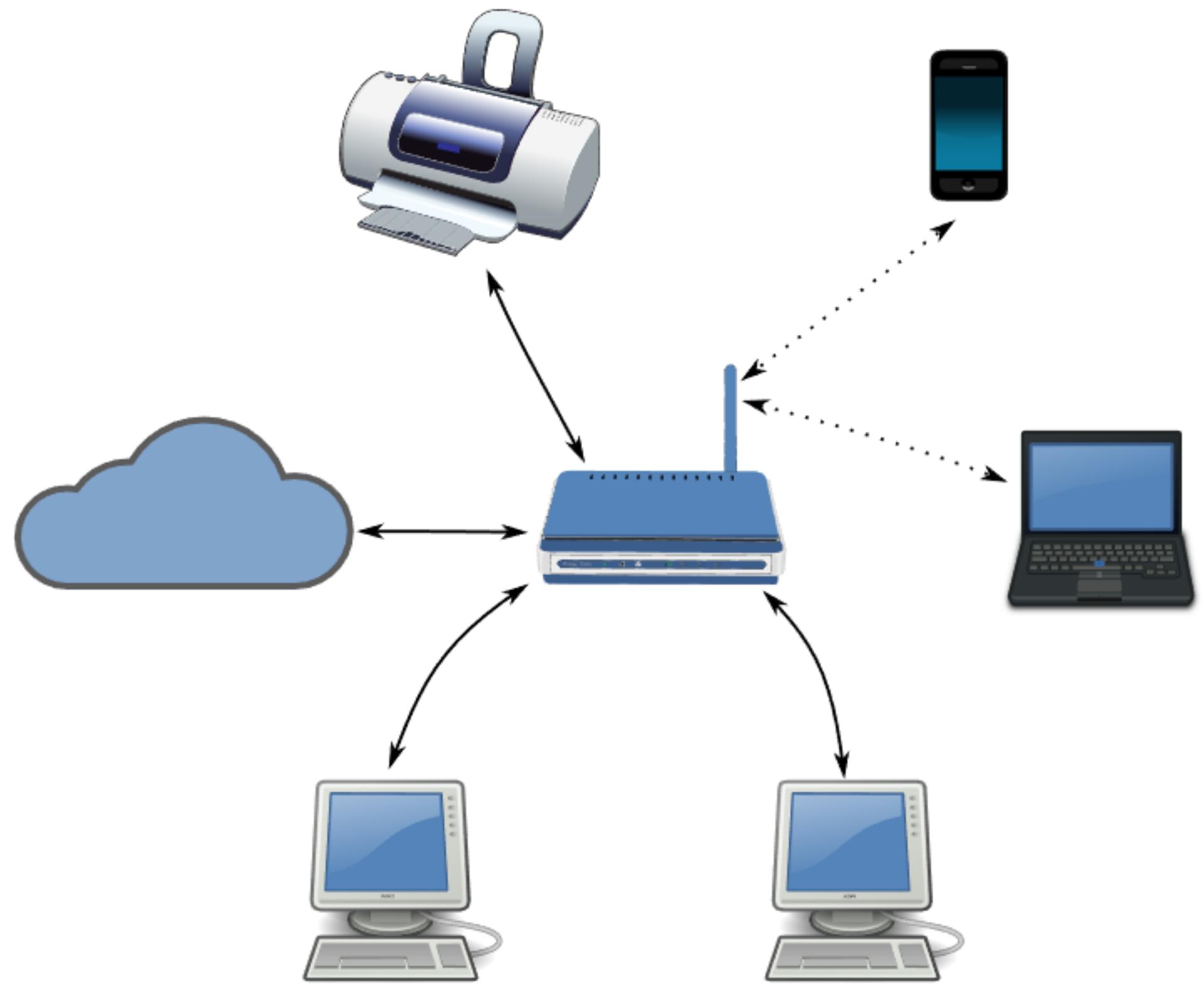
Сетевой уровень

Сетевой уровень (network layer) — 3-й уровень сетевой модели OSI, предназначается для определения пути передачи данных.

Отвечает за трансляцию логических адресов и имён в физические, определение кратчайших маршрутов, коммутацию и маршрутизацию, отслеживание неполадок и заторов в сети.

На этом уровне работает такое сетевое устройство, как маршрутизатор.

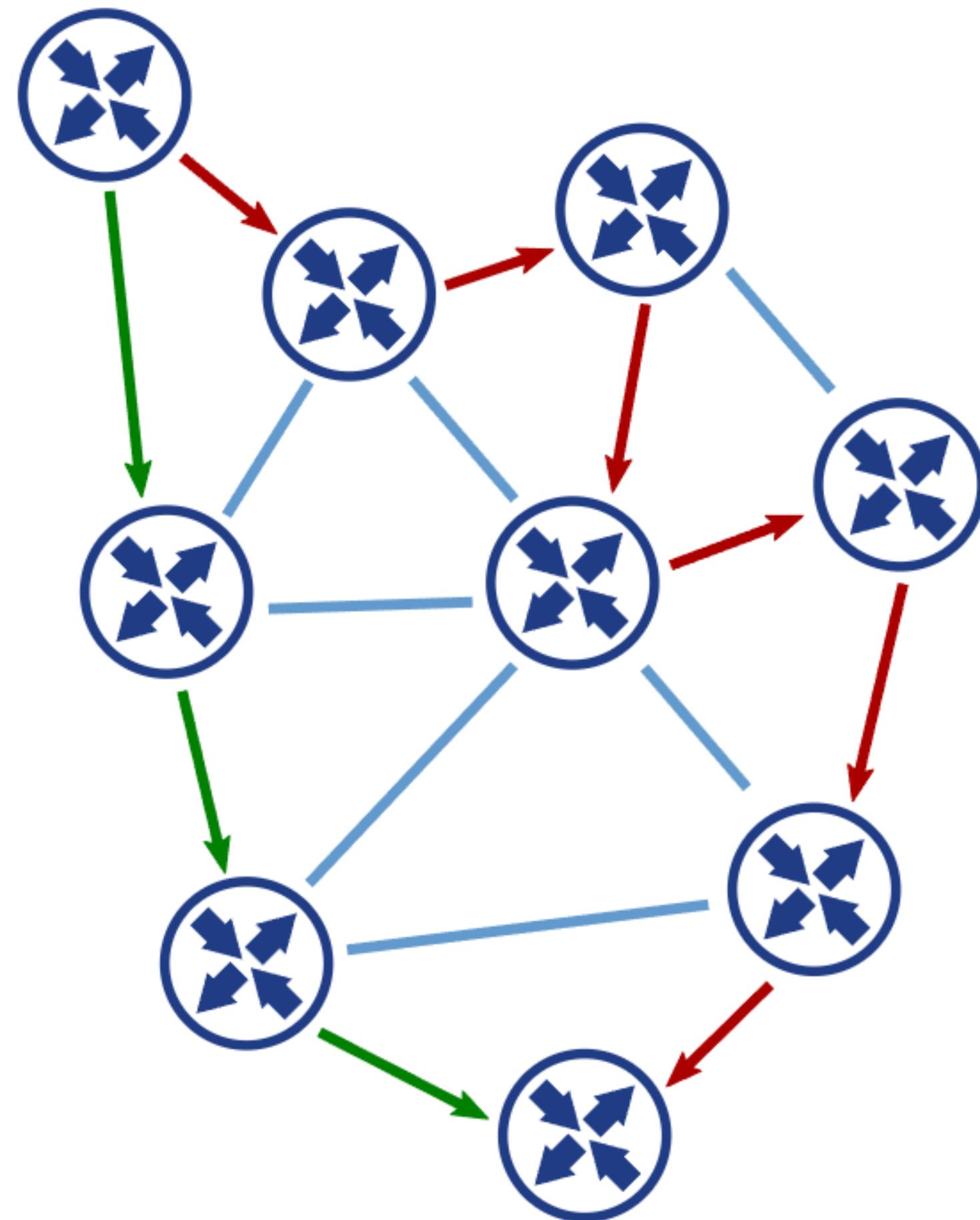
Маршрутизатор — специализированный компьютер, который пересыпает пакеты между различными сегментами сети на основе правил и таблиц маршрутизации.



Транспортный уровень

Транспортный уровень (transport layer) предназначен для обеспечения надёжной передачи данных от отправителя к получателю. Чтобы гарантировать доставку используется подтверждение. Если через определенное время не пришло подтверждение, то тот же самый пакет отправляется снова.

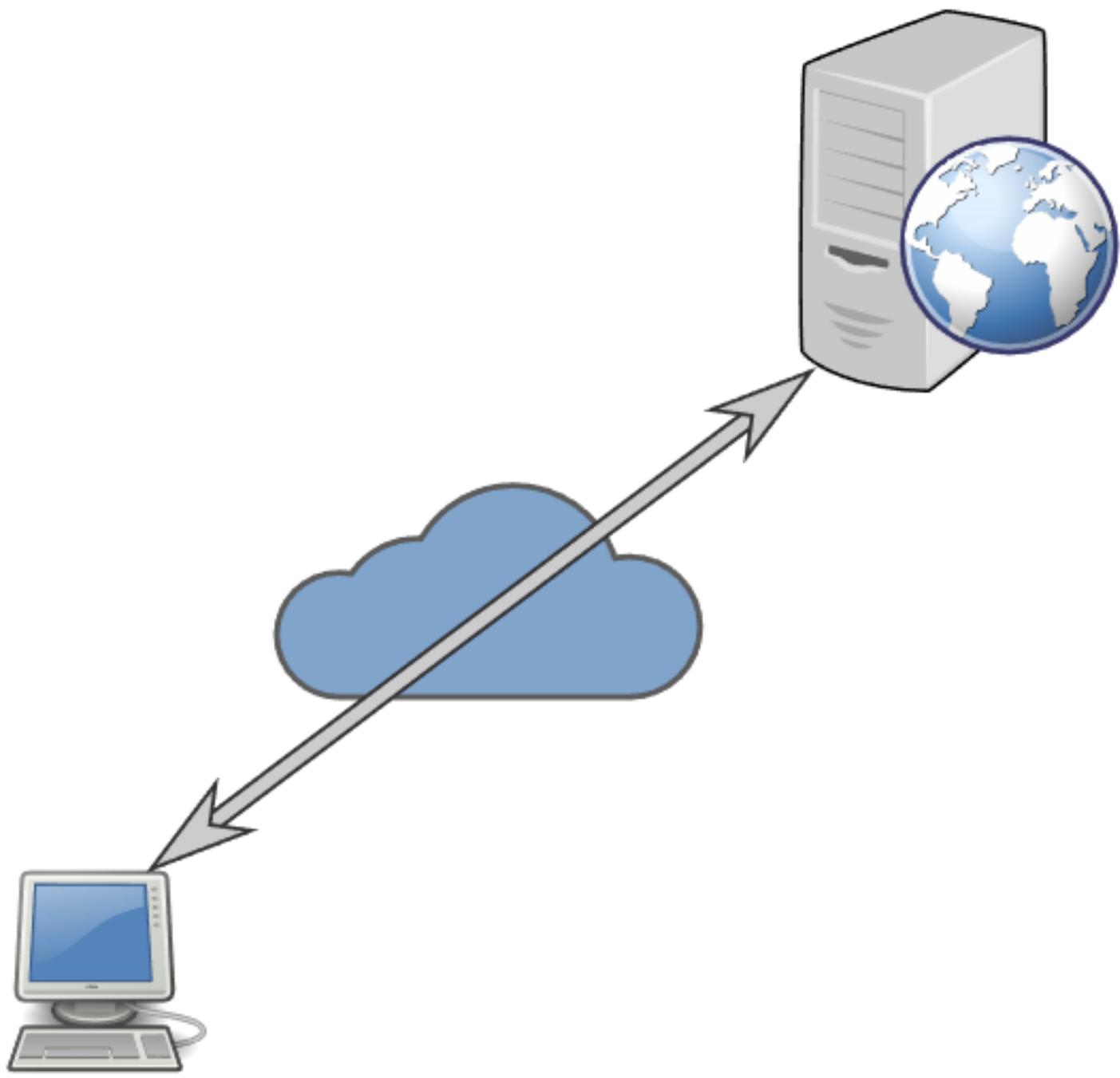
Также на транспортном уровне может обеспечиваться порядок следования сообщений за счёт нумерации сообщений.



Сеансовый уровень

Сеансовый уровень (session layer) модели обеспечивает поддержание сеанса связи, позволяя приложениям взаимодействовать между собой длительное время. Уровень управляет созданием/завершением сеанса, обменом информацией, синхронизацией задач, определением права на передачу данных и поддержанием сеанса в периоды неактивности приложений.

Сеансы передачи составляются из запросов и ответов, которые осуществляются между приложениями. Службы сеансового уровня обычно используются в средах приложений, в которых требуется использование удалённого вызова процедур.



Уровень представления

Уровень представления (presentation layer) отвечает за преобразование протоколов и кодирование/декодирование данных.

Запросы приложений, полученные с прикладного уровня, преобразуются в формат для передачи по сети, а полученные из сети данные преобразуются в формат, понятный приложениям.

На этом уровне может осуществляться сжатие/распаковка или кодирование/декодирование данных, а также перенаправление запросов другому сетевому ресурсу, если они не могут быть обработаны локально.



Прикладной уровень

Протокол прикладного уровня (application layer) — протокол верхнего уровня сетевой модели OSI, обеспечивает взаимодействие сети и пользователя.

Уровень разрешает приложениям пользователя иметь доступ к сетевым службам, таким, как обработчик запросов к базам данных, доступ к файлам, пересылке электронной почты.

Также отвечает за передачу служебной информации, предоставляет приложениям информацию об ошибках и формирует запросы к уровню представления.



Стек протоколов TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) — это концептуальная модель и набор коммуникационных протоколов, используемых в Интернете и подобных компьютерных сетях.

Стек был разработан по инициативе Министерства обороны США в 1972 году для построения сети ARPANET, которая легла в основу сети Интернет.

Развитием архитектуры Интернета и протоколов в модели TCP/IP занимается открытое международное сообщество проектировщиков IETF.



Канальный уровень TCP/IP



Протокол Ethernet

Ethernet – наиболее распространённая технология пакетной передачи данных в компьютерных и промышленных сетях.



- 1973 Разработка первой версии протокола в компании Xerox
- 1980 Компании Xerox, DEC, Intel принимают общий стандарт Ethernet II
- 1983 Публикация международного стандарта IEEE 802.3

Стандарты Ethernet

Название	Скорость	Кабель	Стандарт
Ethernet	10 Мб/с	Коаксильный, витая пара, оптика	802.3
Fast Ethernet	100 Мб/с	Витая пара, оптика	802.3u
Gigabit Ethernet	1 Гб/с	Витая пара, оптика	802.3z, 802.3ab
5G Ethernet	5 Гб/с	Витая пара	802.3bz
10G Ethernet	10 Гб/с	Витая пара, оптика	802.3ae 802.3an
100G Ethernet	100 Гб/с	Оптика	802.3ba
400G Ethernet	400 Гб/с	Оптика	802.3bs

Типы Ethernet

Классический Ethernet

Разделяемая среда

Ethernet - Gigabit Ethernet

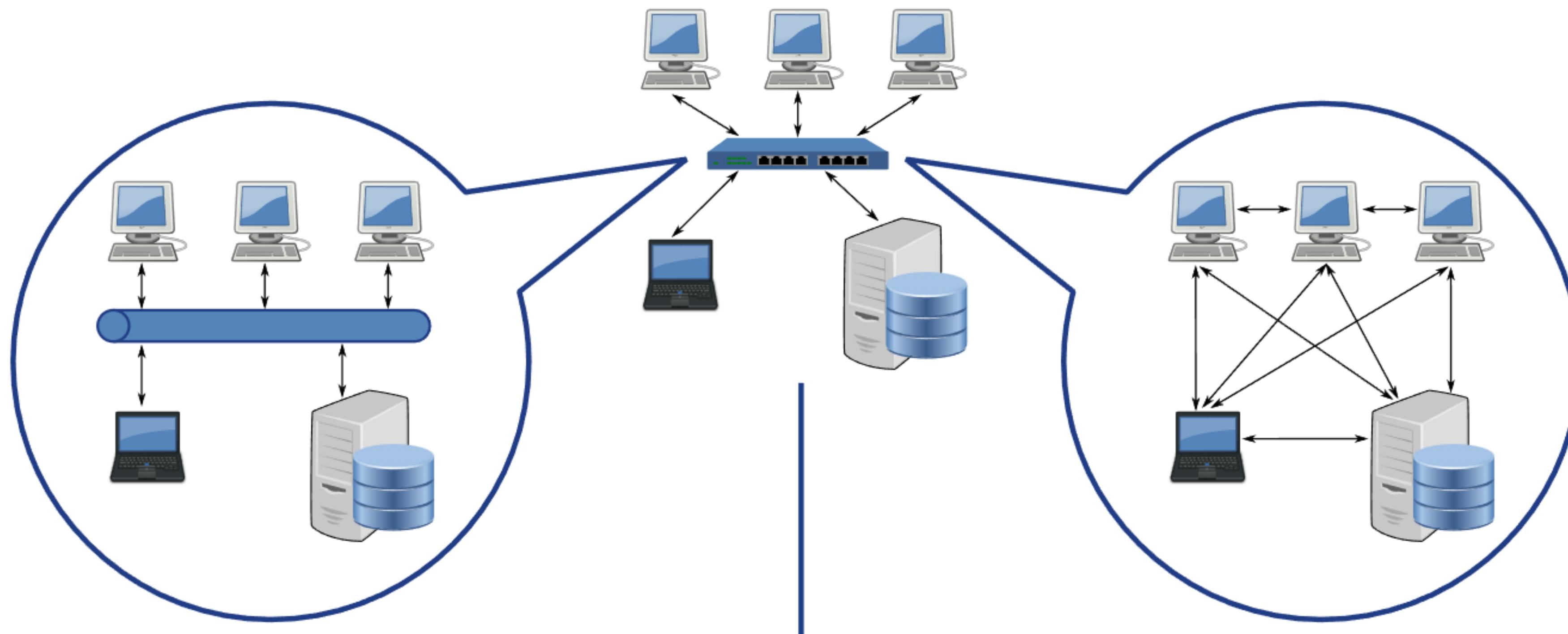
Концентратор (Hub)

Коммутируемый Ethernet

Точка-точка

Fast Ethernet >

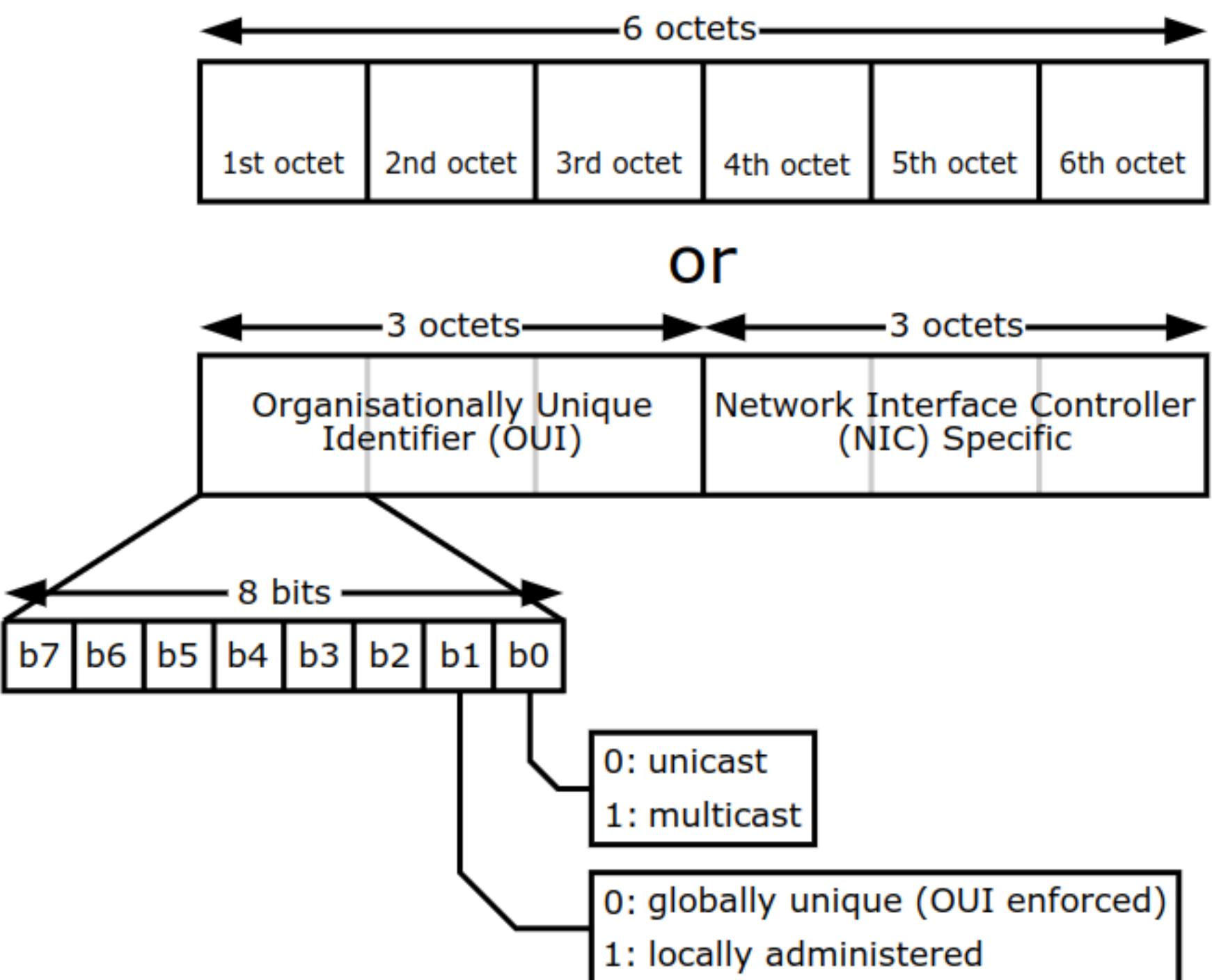
Коммутатор (Switch)



MAC-адрес

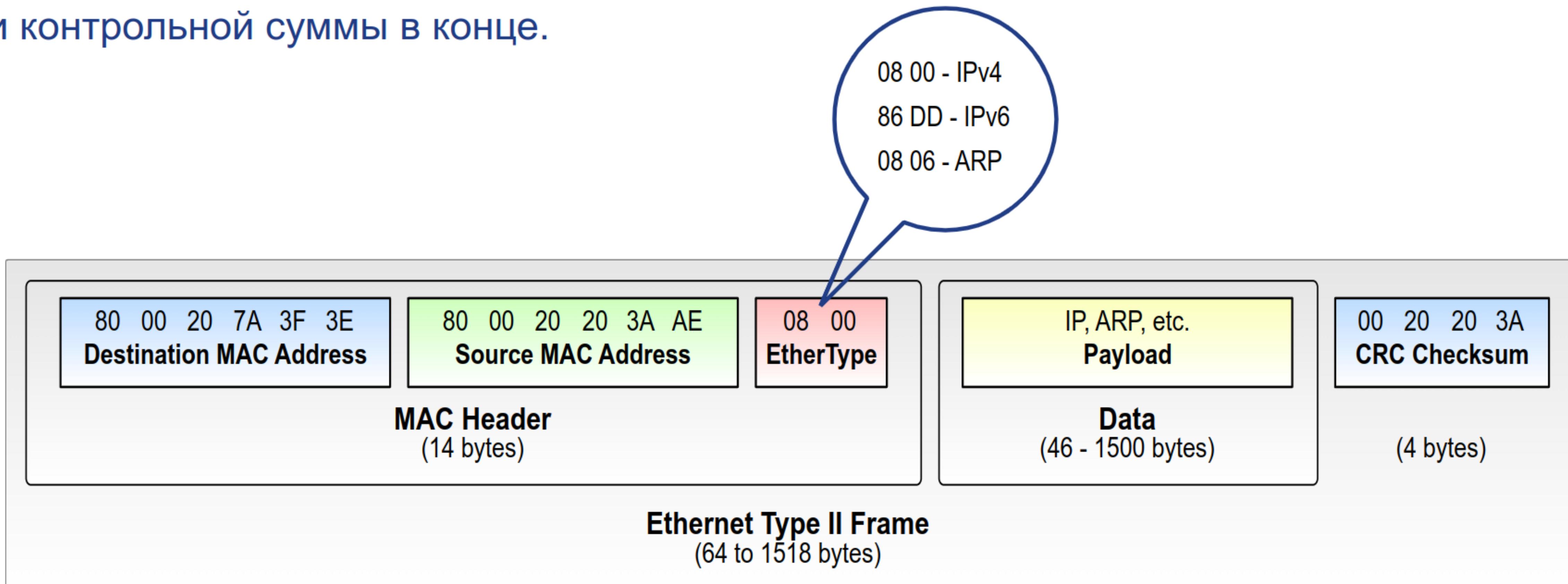
MAC-адрес (Media Access Control — управление доступом к среде, также Hardware Address или физический адрес) — уникальный идентификатор, присваиваемый каждой единице активного оборудования или некоторым их интерфейсам в компьютерных сетях Ethernet.

Поставщику или производителю оборудования IEEE присваивает глобально уникальный идентификатор организации (OUI), и таким образом за этой организацией резервируется блок всевозможного рода производных идентификаторов.



Кадр Ethernet

В Ethernet данные передаются блоками, называемыми фреймами. Каждый фрейм состоит из заголовка, в котором указаны MAC-адрес отправителя, MAC-адрес назначения и тип вышестоящего протокола, полезных данных и контрольной суммы в конце.



Сетевой уровень TCP/IP

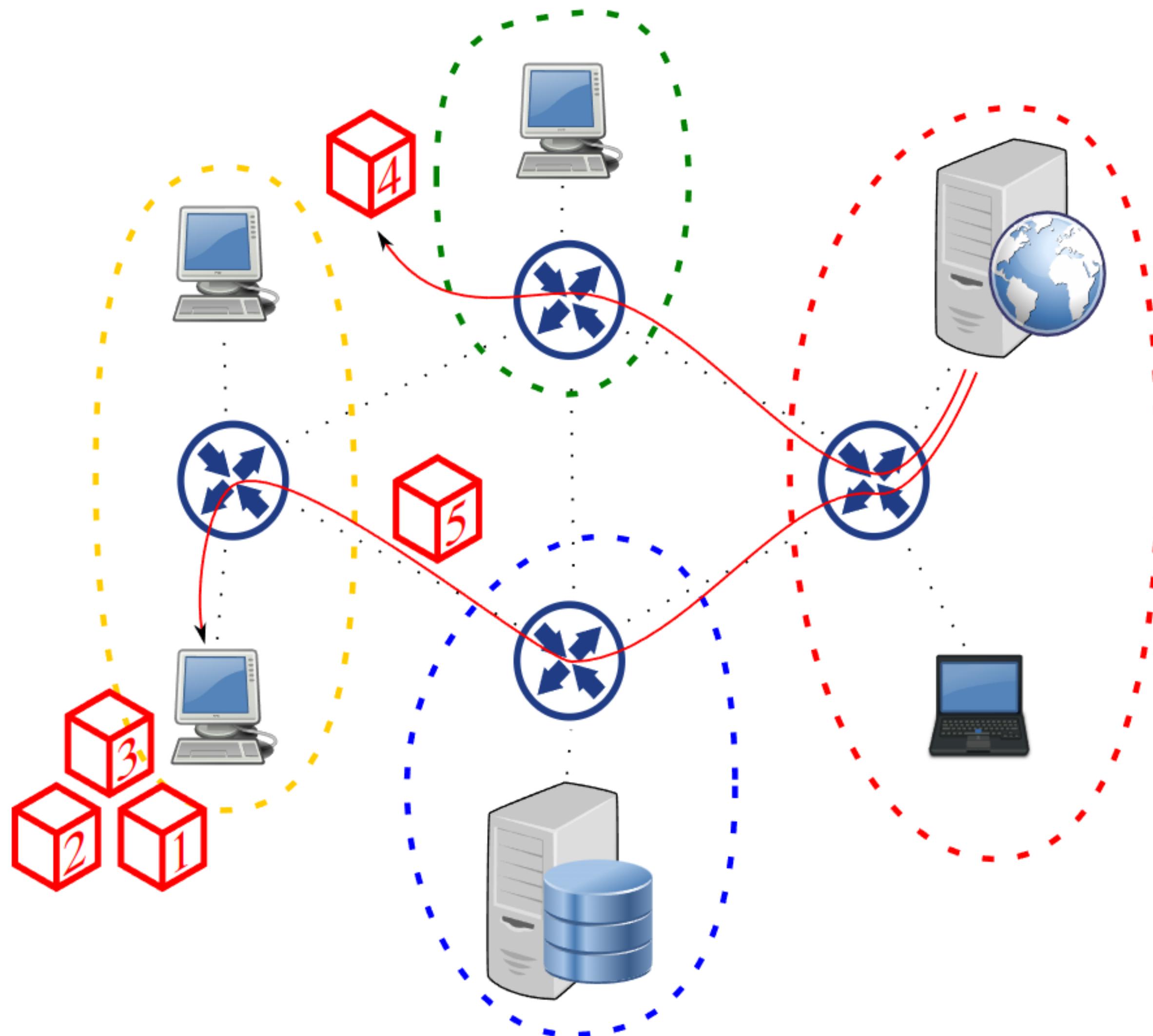


Internet Protocol

Internet Protocol (IP) — межсетевой протокол, объединяющий сегменты сети в единую сеть.

Особенности:

- 1 Доставка пакетов не гарантируется
- 2 Порядок передачи пакетов не гарантируется
- 3 Возможно дублирование пакетов
- 4 Возможна фрагментация пакетов



IP-адрес

Параметр	IPv4	IPv6
Длина адреса	4 байта	16 байт
Адресное пространство	4294967296	79228162514264337593543950336
Структура адреса	4 группы по 8 бит	8 групп по 16 бит
Размер группы	256	65536
Запись адреса	10.0.2.4	2001:0db8:11a3:09d7:1f34:8a2e:07a0: 765d
Неопределённый адрес	0.0.0.0	::
Loopback адрес	127.0.0.1	::1

Классовая адресация IPv4



Бесклассовая адресация IPv4

CIDR (Classless Inter-Domain Routing) - метод бесклассовой адресации, где маска подсети определяет число бит на кодирование адресов сети и узла

IP-адрес в CIDR-формате: 192.168.1.2/23

IP-адрес: 192.168.1.2

Маска подсети: 255.255.254.0

Адрес сети: 192.168.0.0

1	1	0	0	0	0	0	0
---	---	---	---	---	---	---	---

1	0	1	0	1	0	0	0
---	---	---	---	---	---	---	---

0	0	0	0	0	0	0	1
---	---	---	---	---	---	---	---

0	0	0	0	0	0	1	0
---	---	---	---	---	---	---	---

1	1	1	1	1	1	1	1
---	---	---	---	---	---	---	---

1	1	1	1	1	1	1	1
---	---	---	---	---	---	---	---

1	1	1	1	1	1	1	0
---	---	---	---	---	---	---	---

0	0	0	0	0	0	0	0
---	---	---	---	---	---	---	---

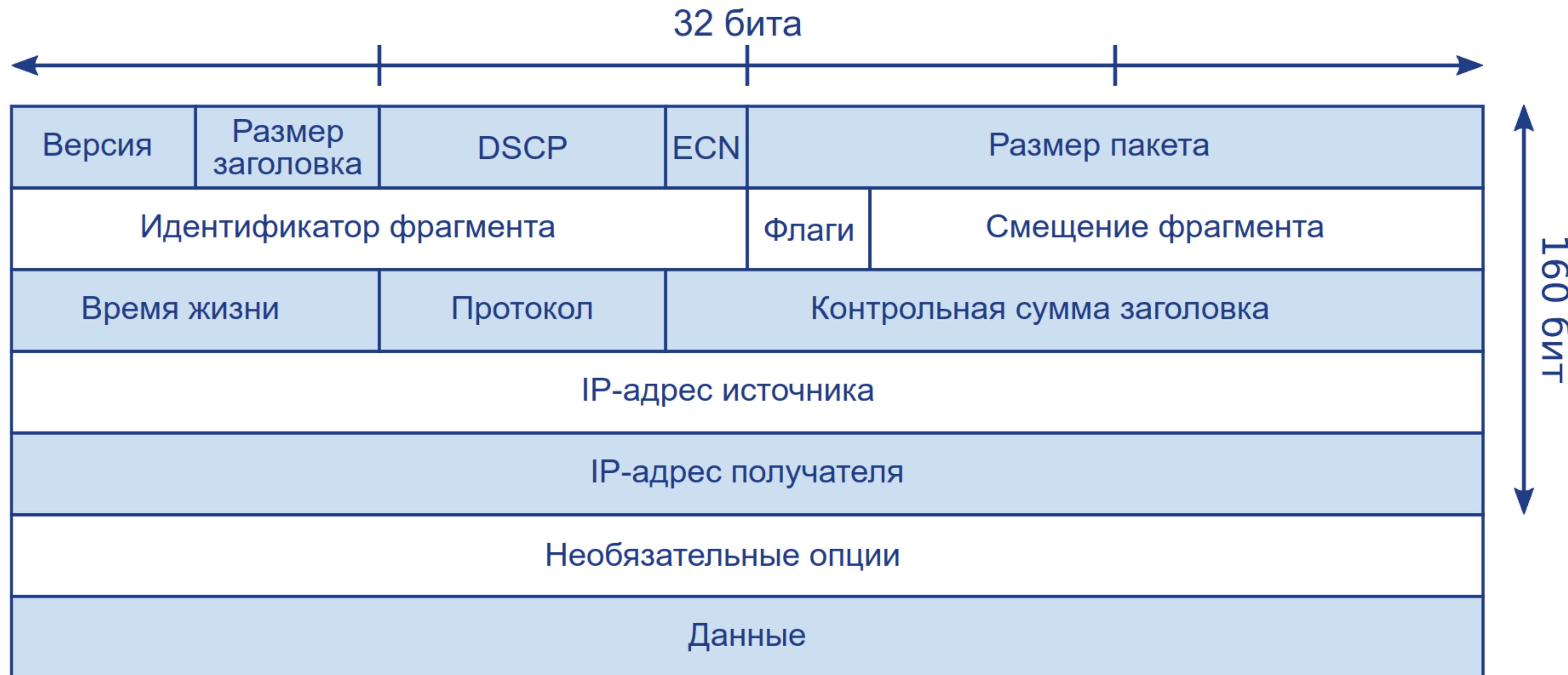
1	1	0	0	0	0	0	0
---	---	---	---	---	---	---	---

1	0	1	0	1	0	0	0
---	---	---	---	---	---	---	---

0	0	0	0	0	0	0	0
---	---	---	---	---	---	---	---

0	0	0	0	0	0	0	0
---	---	---	---	---	---	---	---

Заголовок IPv4



Адресация IPv6

128 бит



Адреса **Unicast** (один получатель) и **Anycast** (один получатель из группы)



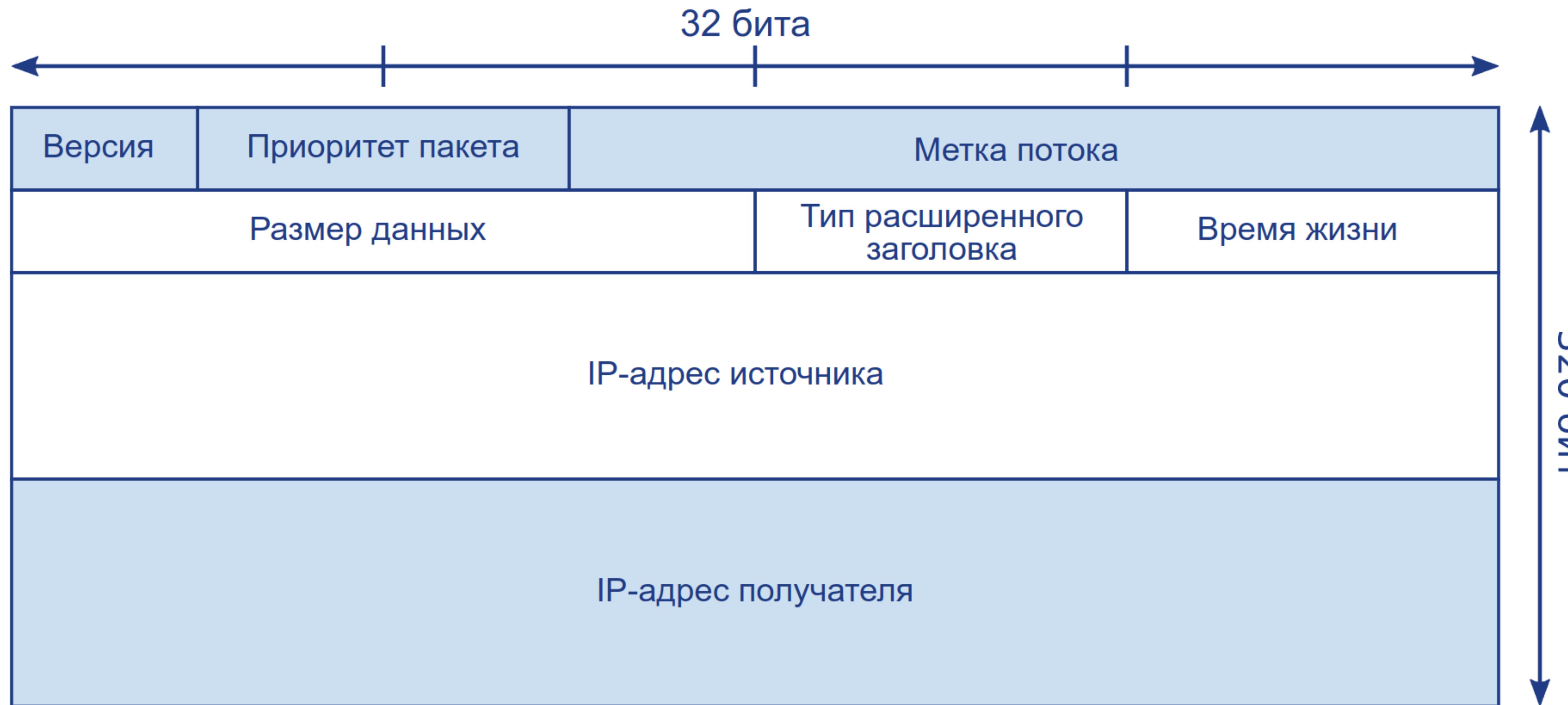
Link-local (Локальный адрес)



Multicast (все получатели группы)



Заголовок IPv6



Протокол DHCP

DHCP (Dynamic Host Configuration Protocol) — протокол динамической настройки узла, позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети.

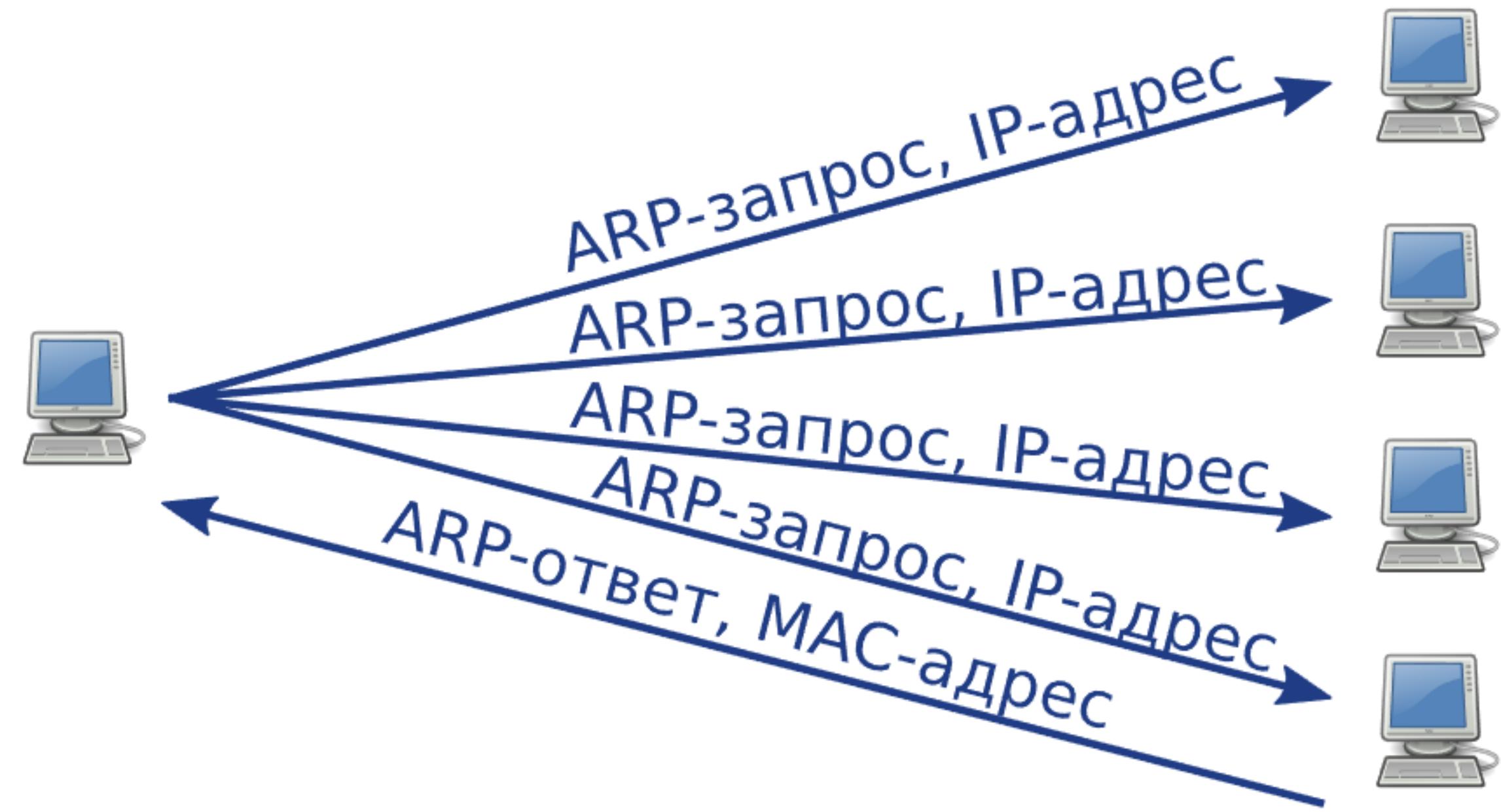


Сообщение	Описание
DISCOVER	Поиск DHCP-сервера
OFFER	Предложение адреса
REQUEST	Запрос адреса
ACK	Подтверждение назначения адреса
NACK	Запрет использования адреса
RELEASE	Освобождение адреса
INFORM	Дополнительные параметры

Протокол ARP

ARP (Address Resolution Protocol) — протокол, предназначенный для определения MAC-адреса по IP-адресу узла.

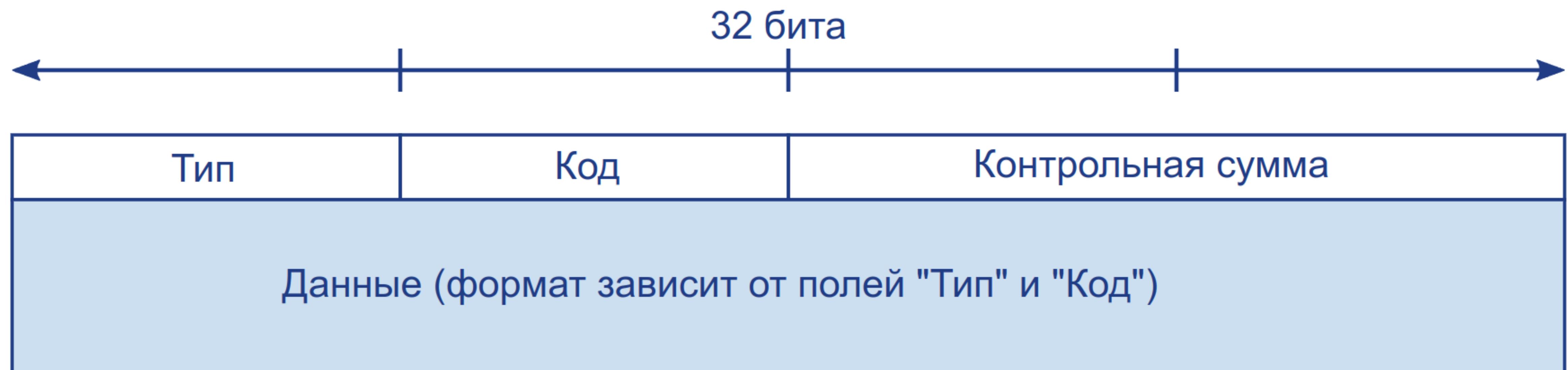
Соответствие MAC-адресов и IP-адресов представляются в ARP-таблице



IP-адрес	MAC-адрес	Тип
10.0.2.4	08:00:27:08:7f:ec	Статический
10.0.2.5	08:00:27:71:26:e9	Динамический

Протокол ICMP

ICMP (Internet Control Message Protocol) — протокол межсетевых управляющих сообщений, используемый для передачи сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных, а также выполнения некоторых сервисных функций.



Транспортный уровень TCP/IP



Адресация на транспортном уровне

Все сетевые процессы, работающие на сетевом узле, разделяют общий IP-адрес.

Для их разделения используются порты, которые представляют собой десятичное число от 0 до 65 535

Порты делятся на диапазоны:

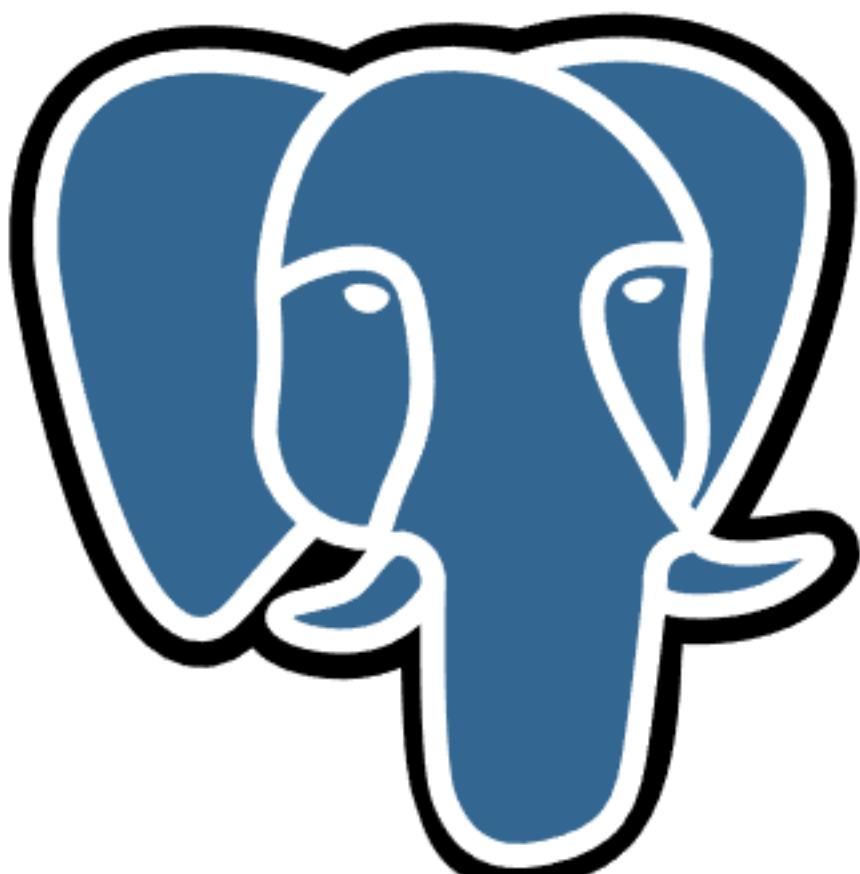
- 1 общезвестные (или системные, 0—1023)
- 2 зарегистрированные (или пользовательские, 1024—49151)
- 3 динамические (или частные, 49152—65535)



25



80



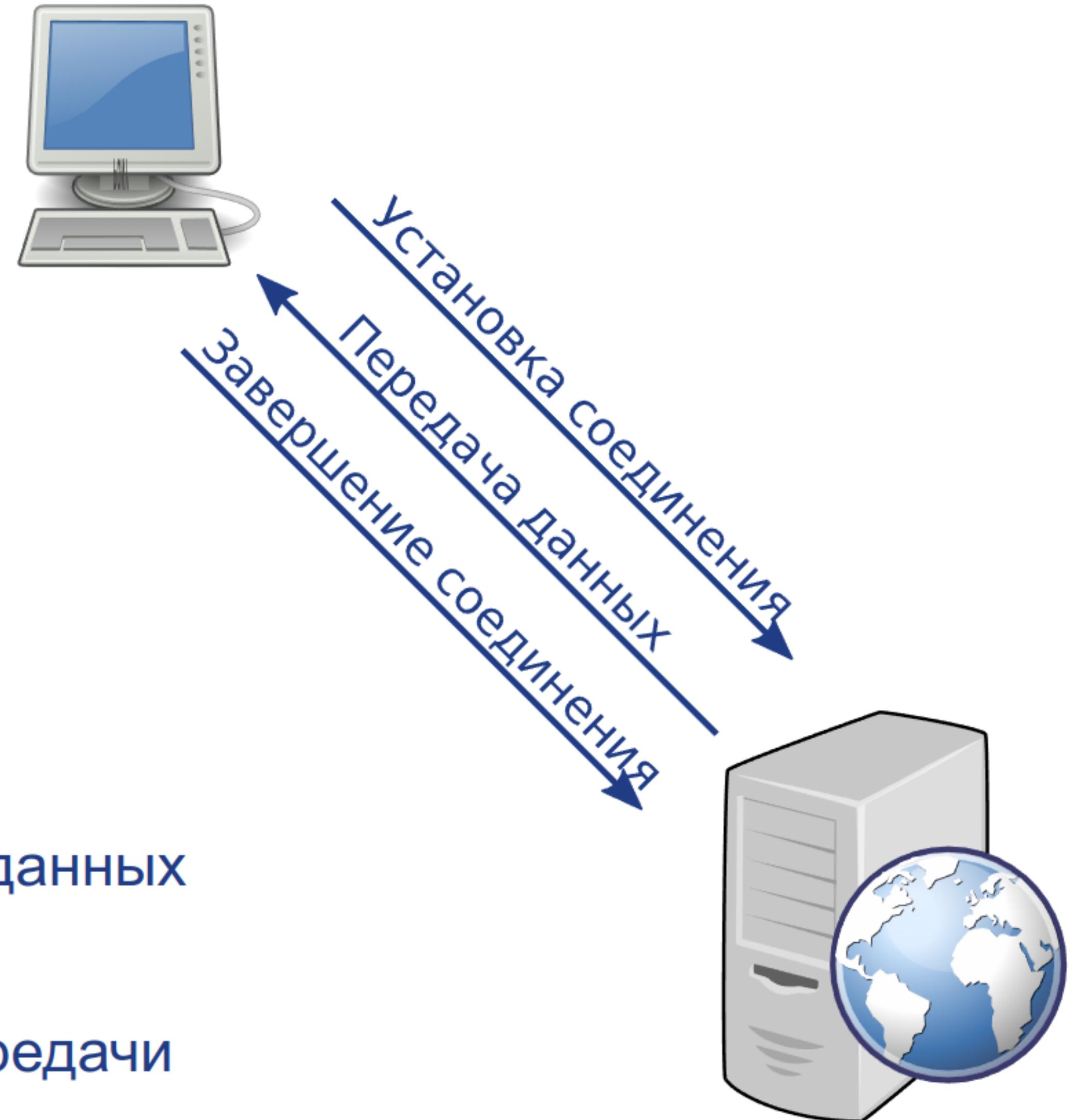
5432

Протокол TCP

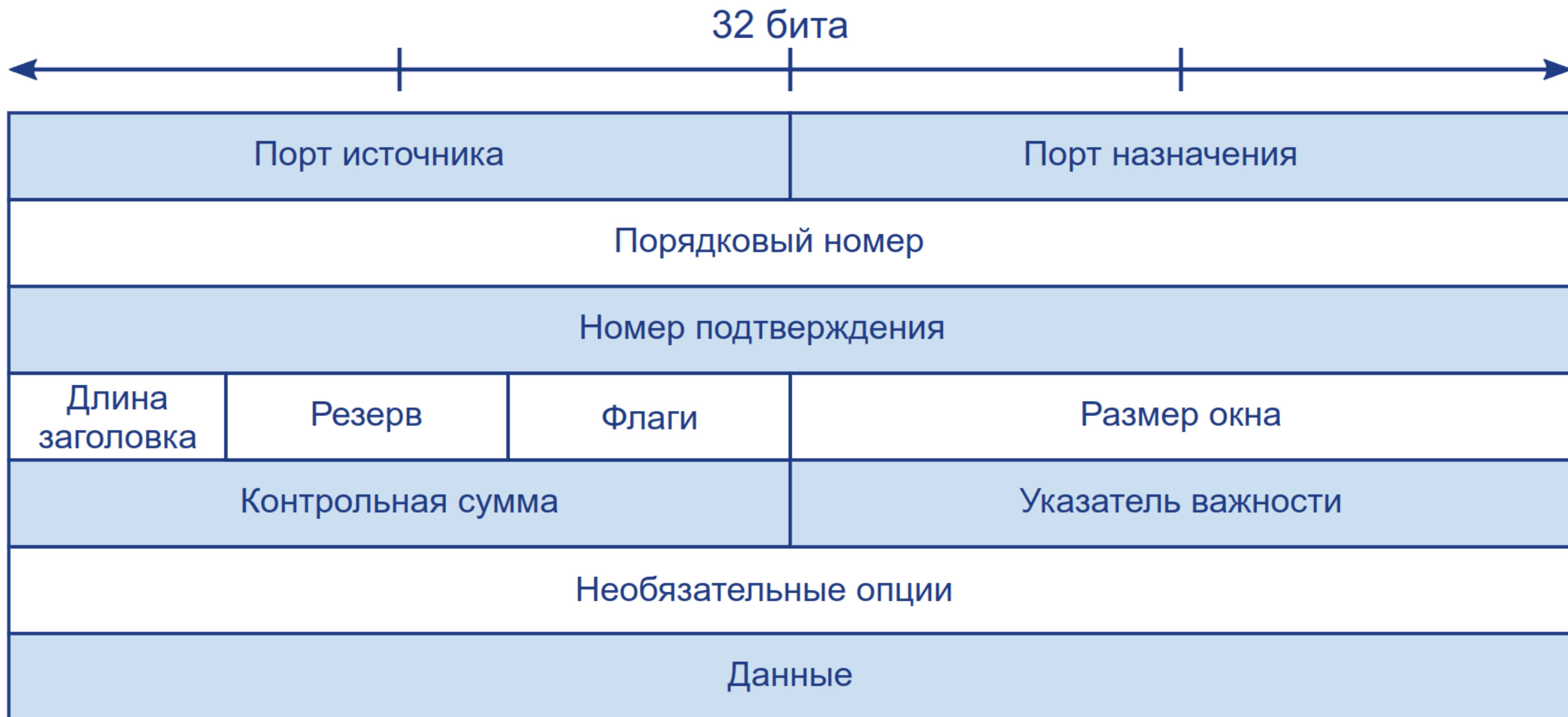
Transmission Control Protocol (TCP) — протокол для управления передачей данных между процессами.

Особенности:

- 1 Устанавливается соединение
- 2 Устранение дублирования пакетов
- 3 Выполняется повторный запрос потерянных данных
- 4 Отправитель уведомляется о результатах передачи



Заголовок сегмента TCP

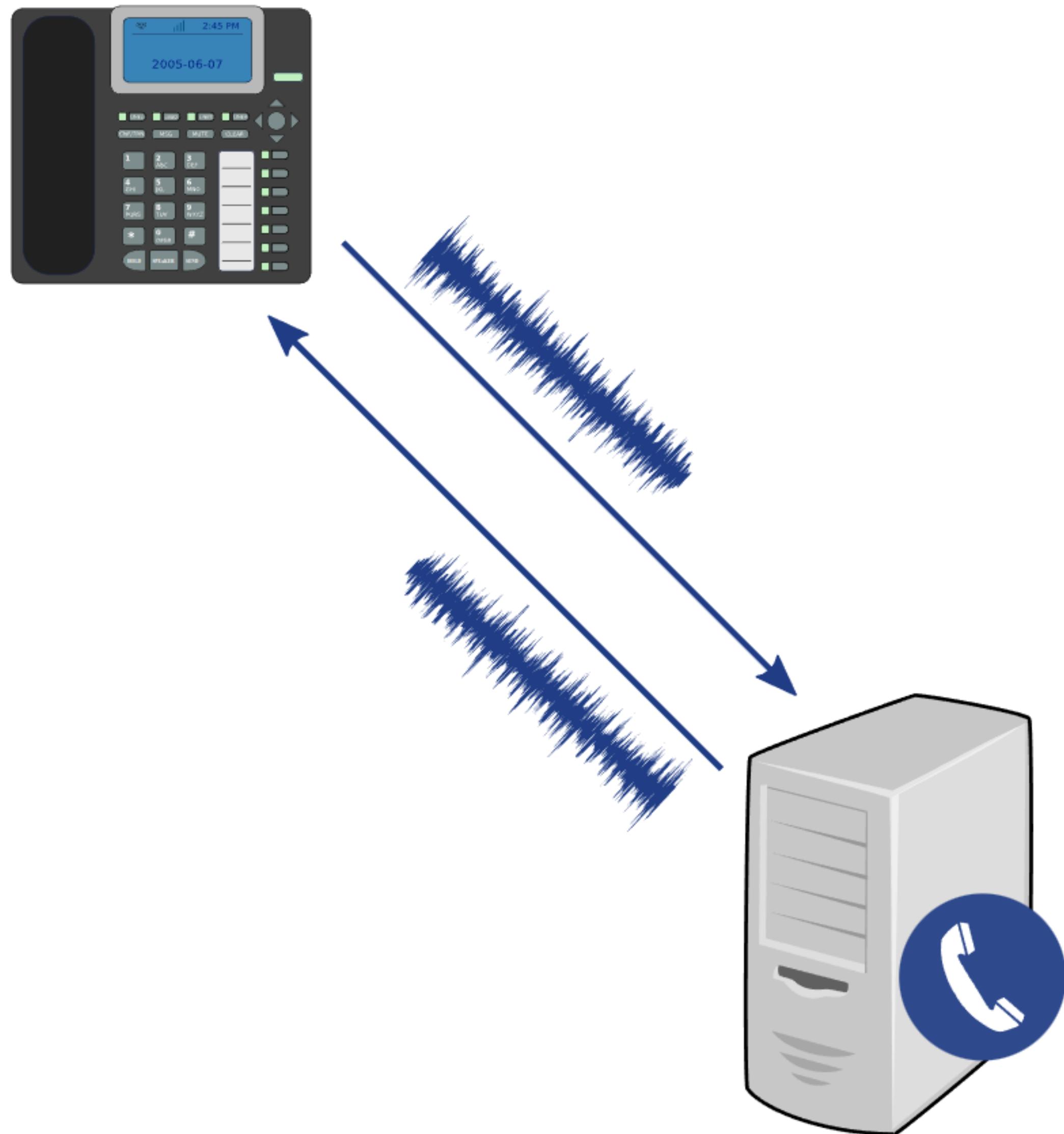


Протокол UDP

UDP (User Datagram Protocol) —
протокол пользовательских датаграмм.

Особенности:

- 1 Соединение не устанавливается
- 2 Доставка данных не гарантируется
- 3 Сохранение порядка не гарантируется
- 4 Перегрузка сети не контролируется
- 5 Более высокая скорость, чем у TCP



Заголовок датаграммы UDP



Прикладной уровень TCP/IP



Прикладной уровень в моделях OSI и TCP/IP

OSI	TCP/IP
 HyperText Transfer Protocol	HyperText Transfer Protocol Secure
 Transport Level Security	
 HTTP keep-alive	

Протокол HTTP

HTTP (HyperText Transfer Protocol) — протокол передачи гипертекста, основанный на технологии "клиент-сервер".

Особенности:

- 1 Использует 80 TCP-порт
- 2 Использует TCP в качестве транспортного протокола
- 3 HTTP используется в качестве "транспорта" для других протоколов прикладного уровня (SOAP, XML-RPC, и др.)
- 4 Широко применяется для передачи данных (XML, JSON и др.)



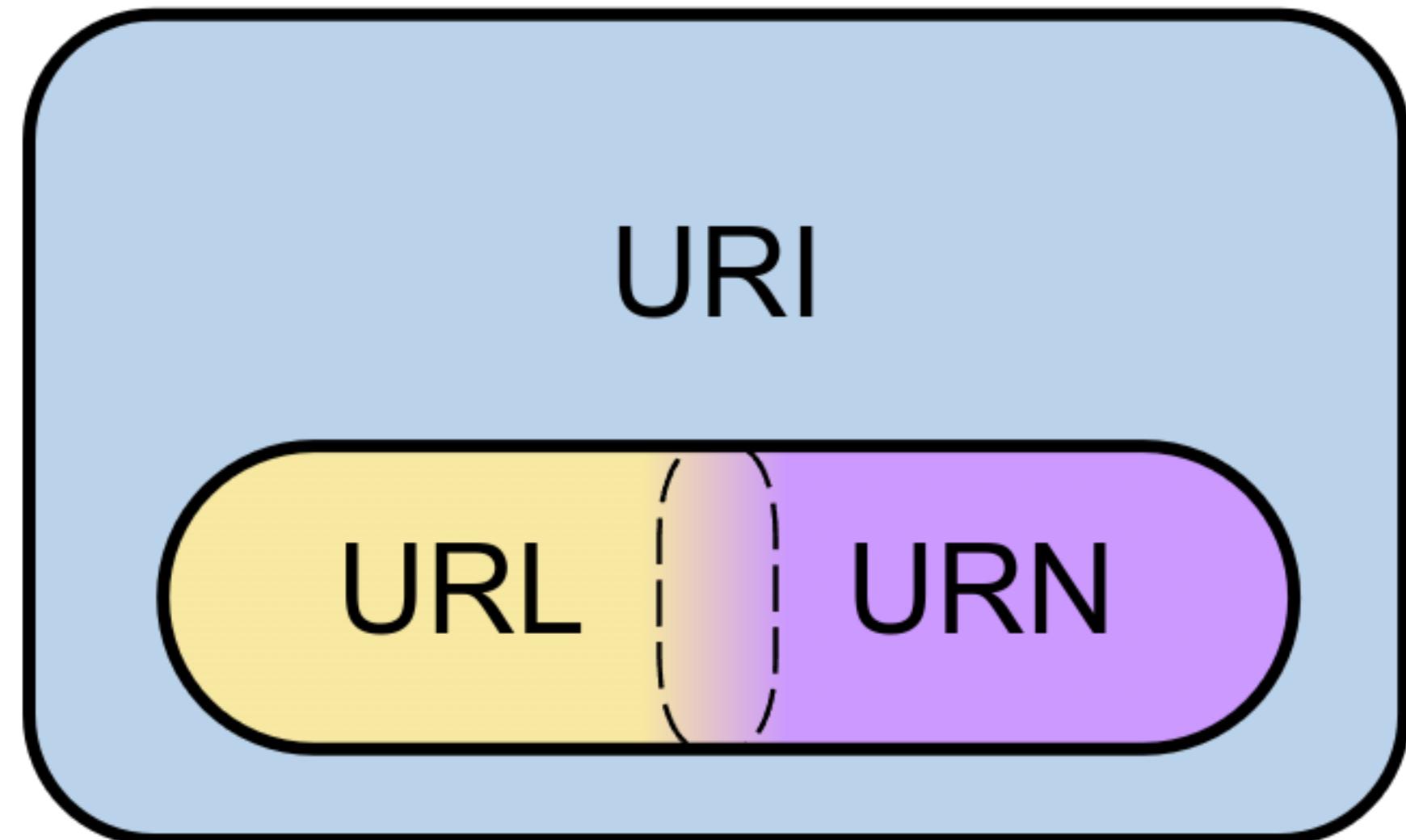
Идентификация ресурсов

URI (Uniform Resource Identifier) — унифицированный (единообразный) идентификатор ресурса.

URL (Uniform Resource Locator) — единообразный определитель местонахождения ресурса.

URN (Uniform Resource Name) — единообразное название (имя) ресурса. URN указывает неизменное имя ресурса без указания его местонахождения и способа обращения.

URI = [схема ":"] путь ["?" запрос] ["#" фрагмент]



Гипертекст

Гипертекст (hypertext) — термин, обозначающий систему из текстовых страниц, имеющих перекрёстные ссылки.

HTML (HyperText Markup Language) — стандартизованный язык разметки гипертекстовых документов во Всемирной паутине.

JavaScript — язык программирования, часто применяемый как язык сценариев для придания интерактивности веб-страницам.

```
<!DOCTYPE html>
<html>
<!-- created 2010-01-01 -->
<head>
  <title>sample</title>
</head>
<body>
  <p>Voluptatem accusantium
    totam rem aperiam.</p>
</body>
</html>
```

HTML

Пакет HTTP

	Запрос	Ответ
Стартовая строка	Метод URI HTTP/Версия	HTTP/Версия КодСостояния Пояснение
Заголовки	Набор пар имя:значение	Набор пар имя:значение
Тело сообщения	Тело объекта, связанного с запросом	Тело объекта, связанного с ответом
Пример	GET /wiki/1.html HTTP/1.1 Host: ru.wikipedia.org User-Agent: Mozilla/5.0 Accept: text/html Connection: close (пустая строка)	HTTP/1.1 200 OK Date: Wed, 11 Feb 2009 11:20:59 GMT Server: Apache Last-Modified: Wed, 11 Feb 2009 11:20:59 GMT Content-Language: ru Content-Type: text/html; charset=utf-8 Content-Length: 1234 Connection: close (пустая строка) (запрошенная страница в HTML)

Методы HTTP

GET	Запрос содержимого указанного ресурса.
POST	Передача пользовательских данных заданному ресурсу.
HEAD	Запрос заголовка страницы.
PUT	Отправка содержимого запроса на указанный URI.
DELETE	Удаление указанного ресурса
TRACE	Трассировка запроса
OPTIONS	Запрос возможностей веб-сервера или параметров соединения для ресурса.
CONNECT	Преобразует соединение запроса в прозрачный TCP/IP-туннель

Коды состояния HTTP

Код состояния HTTP позволяет клиенту определить результаты выполнения запроса и его дальнейшую реакцию.

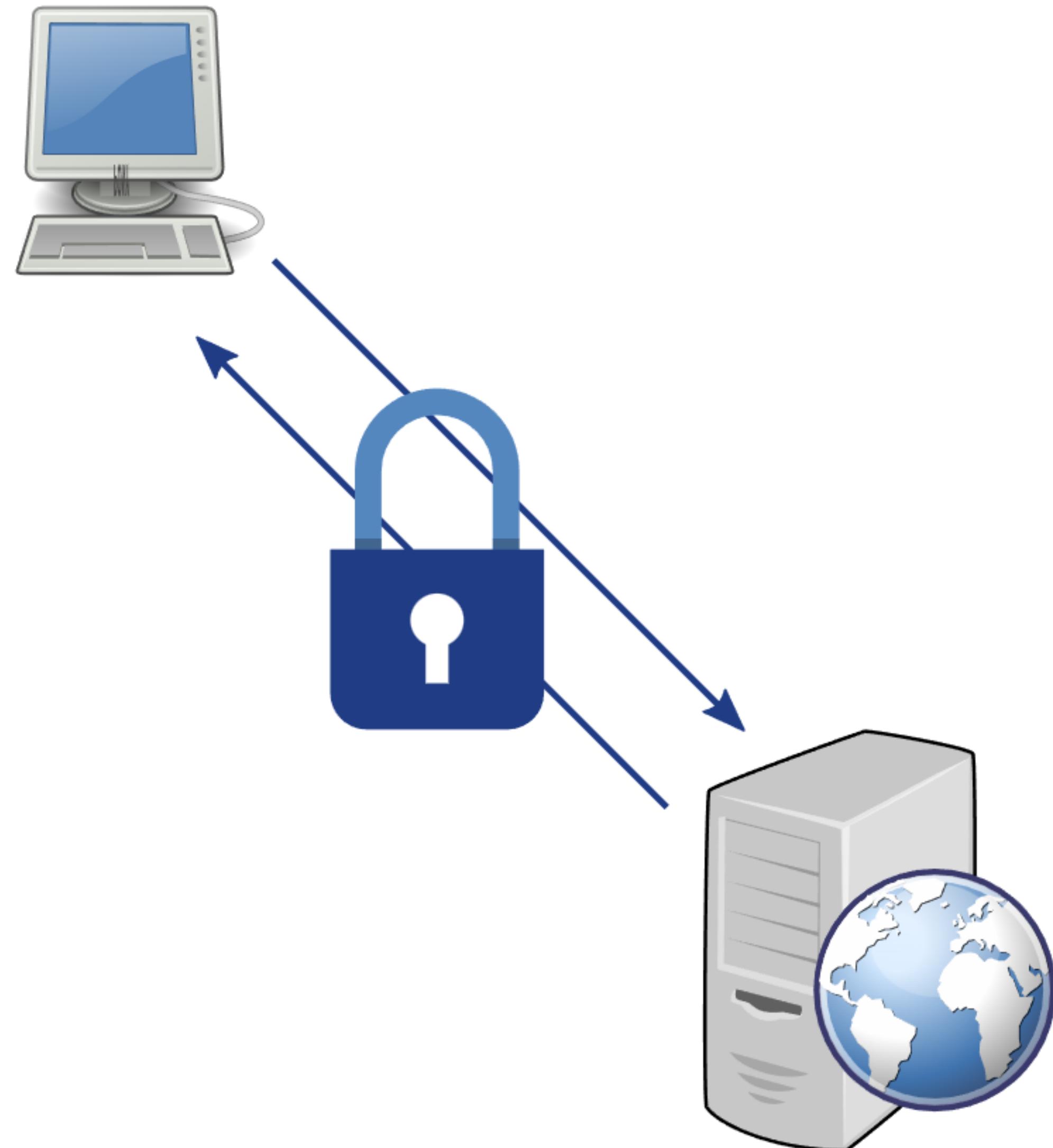
Класс	Описание	Примеры
1XX	Информация	100 - продолжай, 102 - идёт обработка
2XX	Успешное выполнение	200 - хорошо, 201 - создано, 202 - принято
3XX	Преренаправление	301 - перемещено навсегда, 302 - перемещено временно
4XX	Ошибка клиента	403 - доступ запрещён, 404 - страница не найдена
5XX	Ошибка сервера	500 - внутренняя ошибка сервера

Протокол HTTPS

HTTPS (HyperText Transfer Protocol Secure) — расширение протокола HTTP для поддержки шифрования в целях повышения безопасности. Данные в протоколе HTTPS передаются поверх криптографического протокола TLS.

Особенности:

- 1 Использует 443 TCP-порт
- 2 Использует асимметричное шифрование для выработки общего секретного ключа
- 3 Использует симметричное шифрование для обмена данными



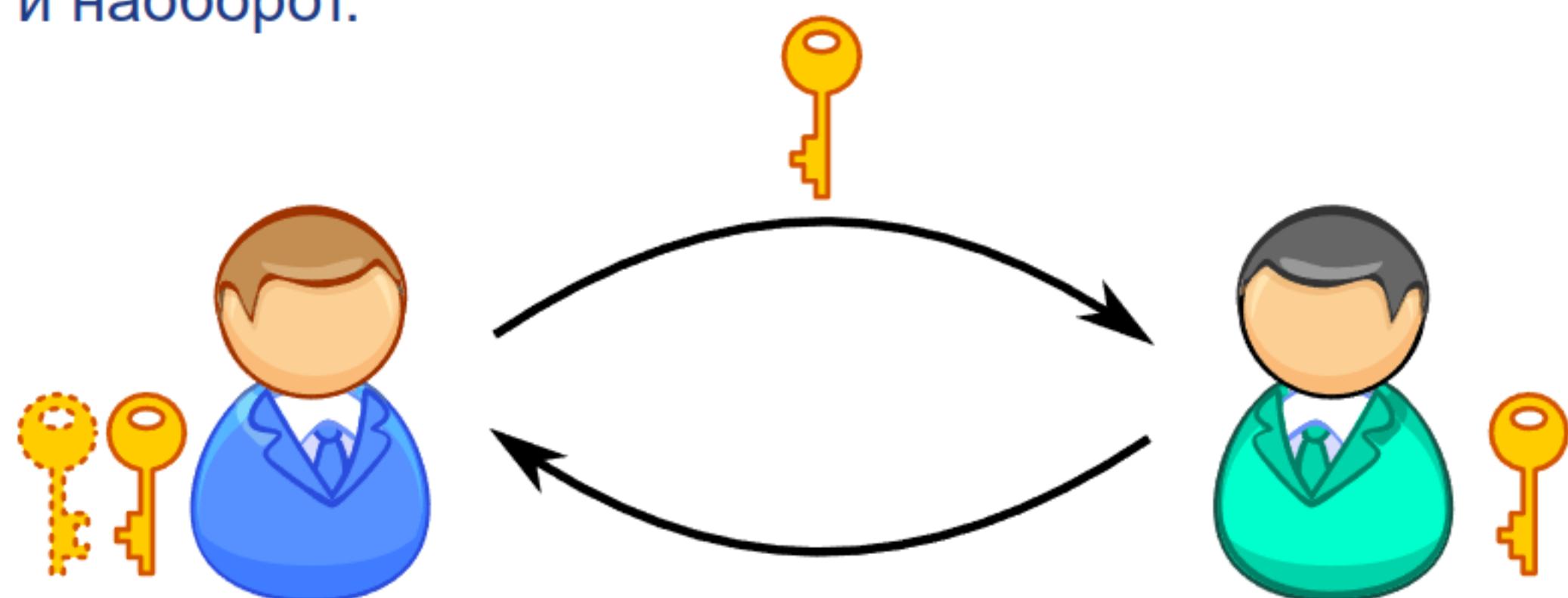
Асимметричное шифрование

Принципы:

- 1 Используется пара ключей (открытый и закрытый).
- 2 Владелец ключей не сообщает никому закрытый ключ и свободно распространяет открытый.
- 3 По открытому ключу невозможно восстановить закрытый за разумное время
- 4 Зашифрованное открытым ключом, дешифруется открытым, и наоборот.

Преимущества:

- 1 Открытый ключ можно распространять по открытым каналам



Недостатки:

- 1 Низкая скорость шифрования/десифрования.

Симметричное шифрование

Принципы:

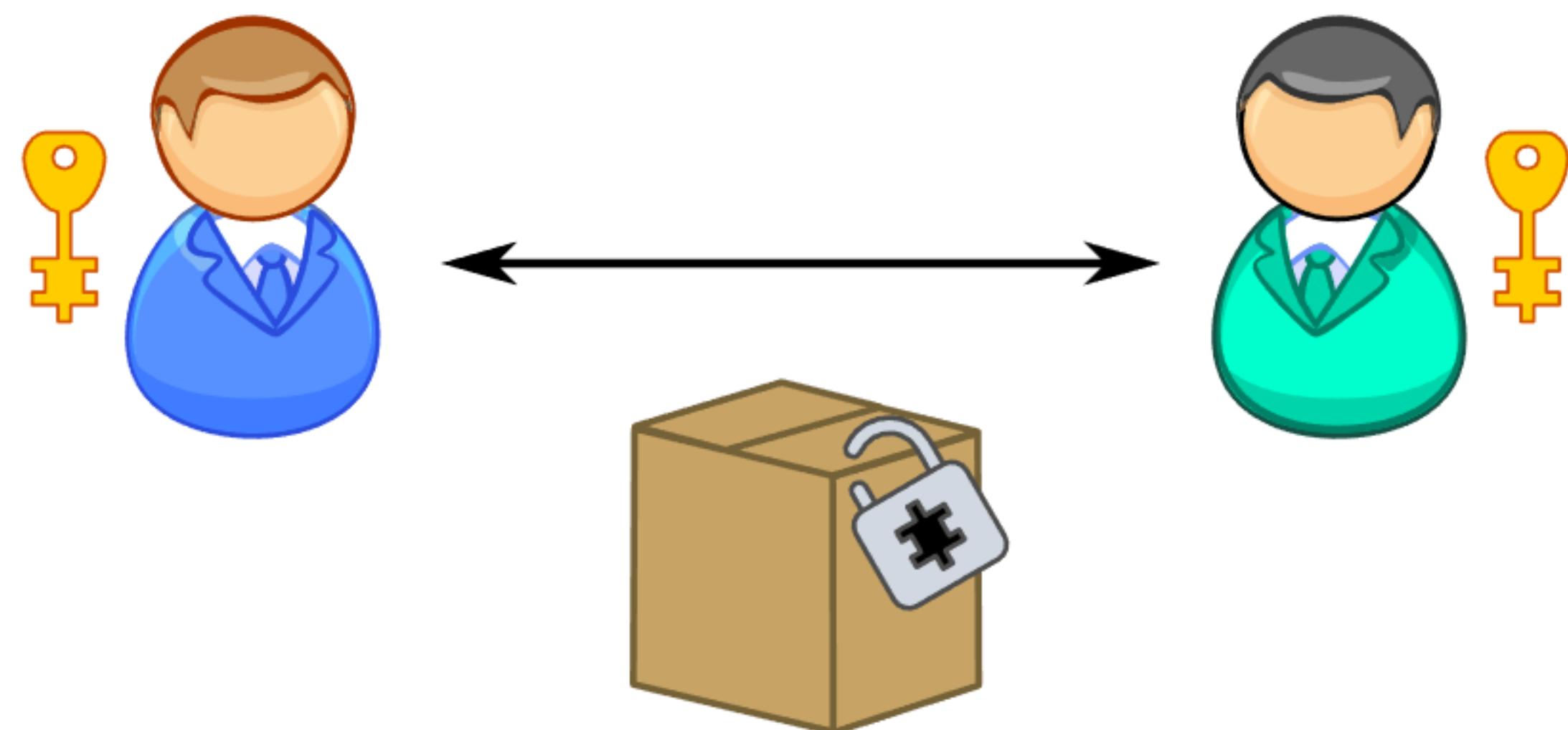
- 1 Отправитель и получатель заранее знают используемый алгоритм шифрования
- 2 Для шифрования и дешифрования используется один и тот же ключ

Преимущества:

- 1 Высокая скорость шифрования/десифрования
- 2 Меньшая длина ключа при сопоставимой стойкости

Недостатки:

- 1 Сложно обмениваться ключами
- 2 Сложно управлять ключами в большой сети



Протокол TLS

TLS (Transport Layer Security) — криптографический протокол, обеспечивающий защищённую передачу данных между узлами в сети Интернет.

Решаемые задачи:

-  Конфиденциальность
-  Целостность
-  Аутентификация



TLS

История TLS

Протокол	Публикация	Состояние
SSL 1.0	не публиковался	устарел
SSL 2.0	1995	устарел
SSL 3.0	1996	устарел
TLS 1.0	1999	устарел
TLS 1.1	2006	устарел
TLS 1.2	2008	
TLS 1.3	2018	

Хэширование

Хэширование - преобразование массива входных данных произвольной длины в (выходную) битовую строку установленной длины, выполняемое определённым алгоритмом.

Принципы:

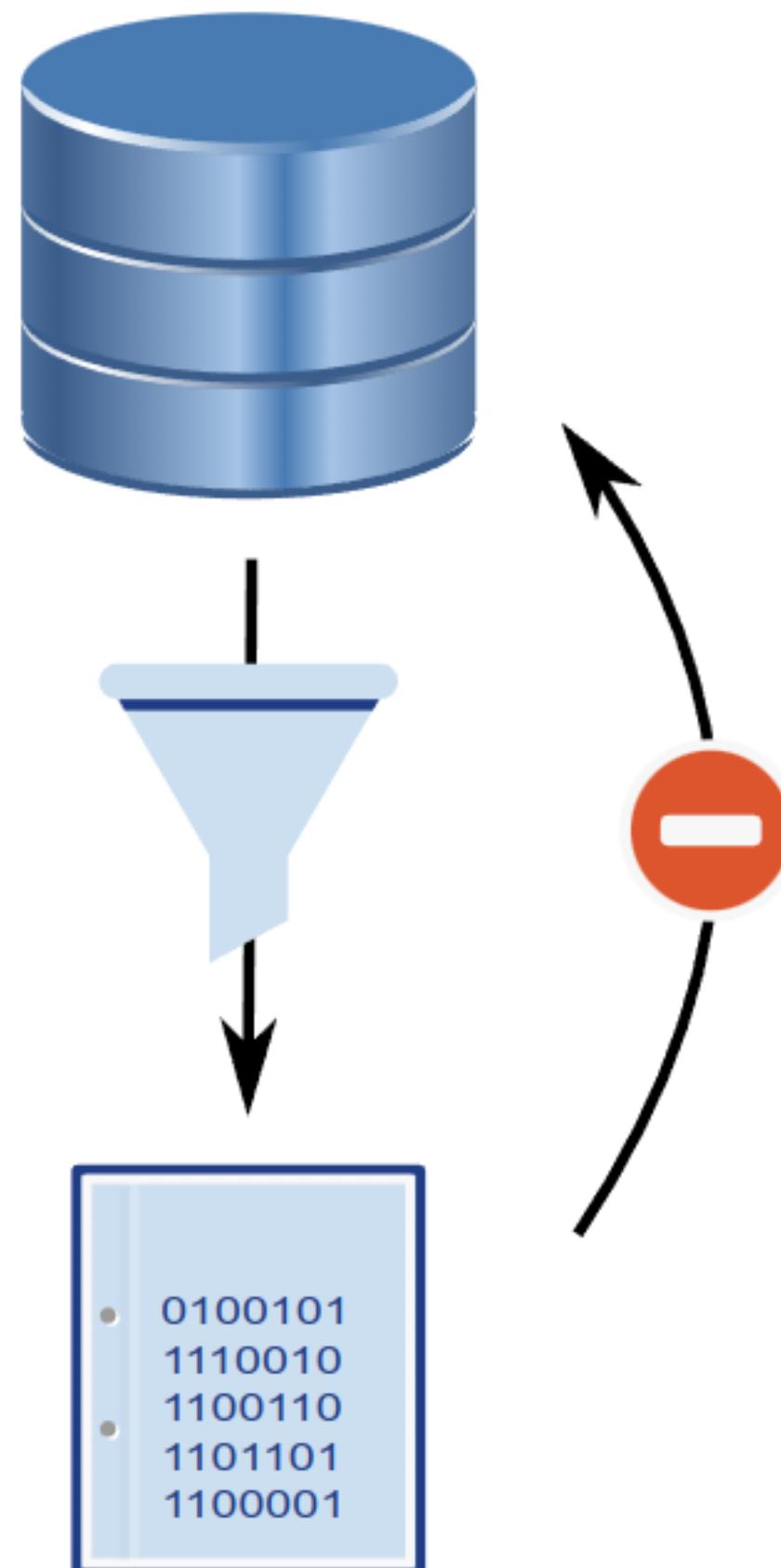
- 1 Выходные данные (хэш) менее разнообразны, чем входные данные.
- 2 Восстановление исходных данных по хэшу в разумное время затруднено.
- 3 Однаковые хэши для разных входных данных называются "коллизией"

Преимущества:

- 1 Хранить и обрабатывать хэши проще и безопаснее

Недостатки:

- 1 Возможность коллизий



Обеспечение целостности

Принципы:

- 1 Отправитель хэширует передаваемые данные
- 2 Хэш шифруется закрытым ключом и полученный результат (цифровая подпись) передаётся получателю
- 3 Получатель самостоятельно вычисляет хэш принятых данных
- 4 Получатель расшифровывает цифровую подпись с помощью открытого ключа отправителя и получает хэш переданных данных.
- 5 Целостность обеспечена при совпадении хэшей.



Обеспечение аутентичности

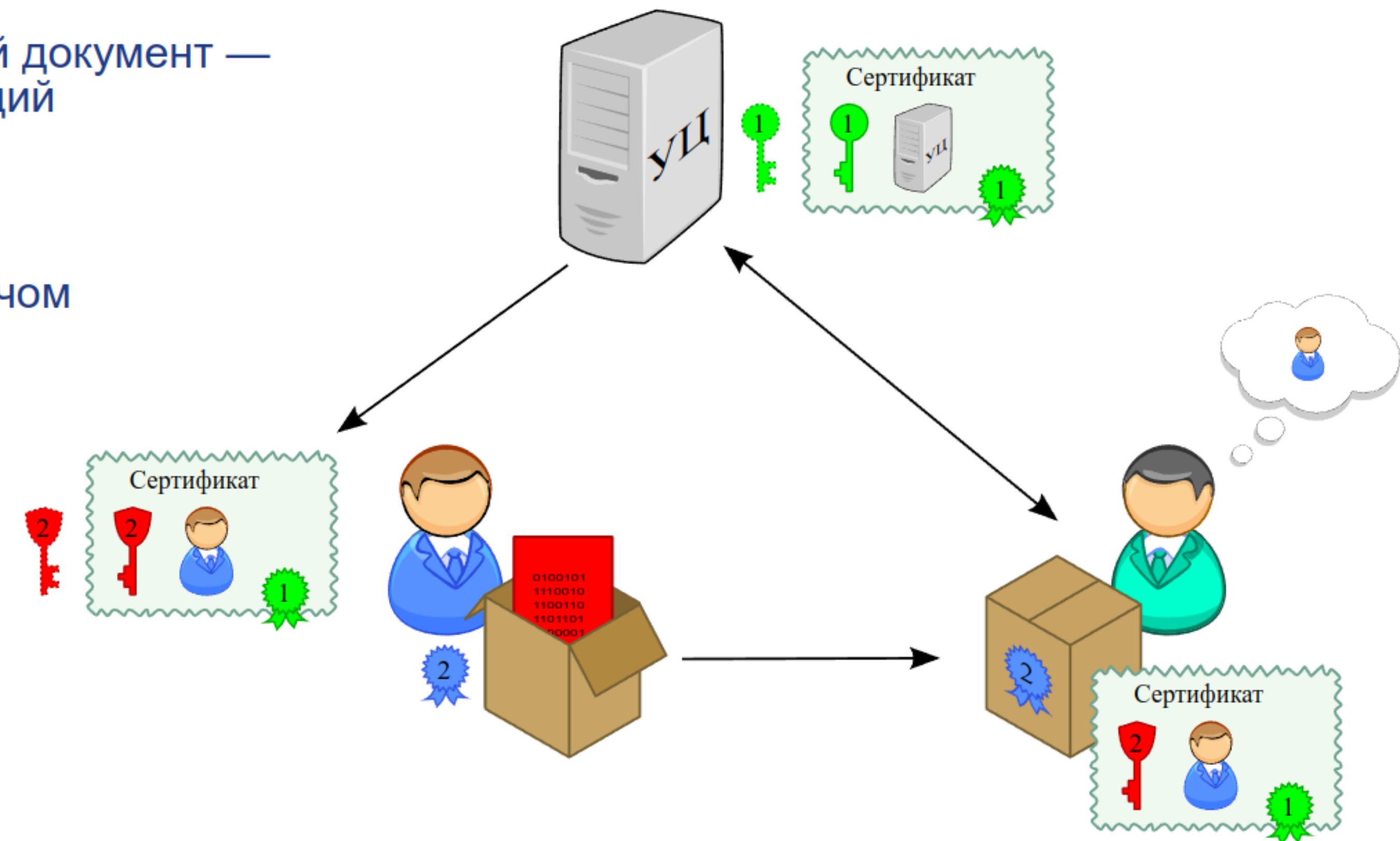
Принципы:

1 Все не доверяют друг другу, но доверяют удостоверяющему центру

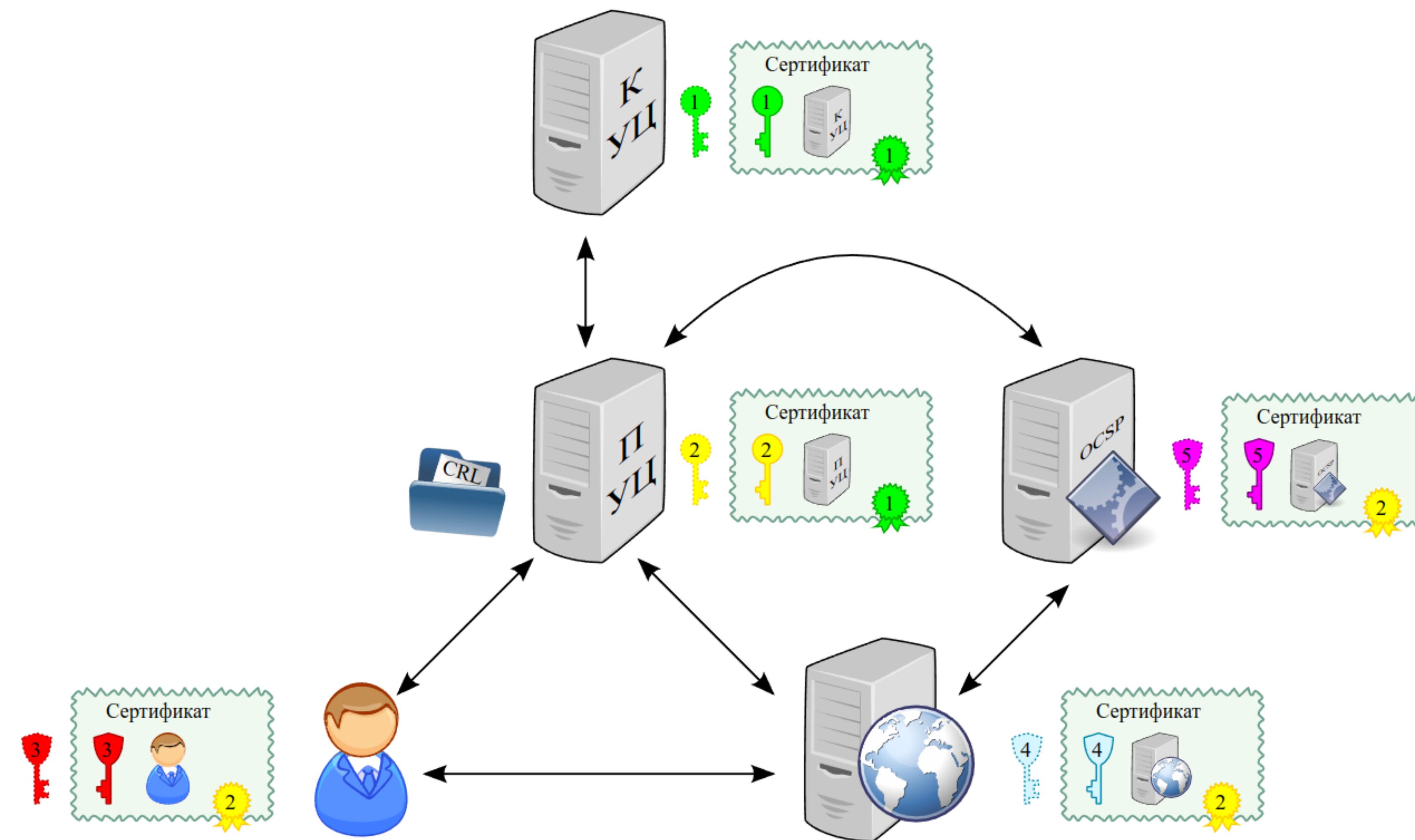
2 Удостоверяющий центр создает электронный документ — сертификат открытого ключа, подтверждающий принадлежность закрытого ключа владельцу этого сертификата

3 Сертификаты подписываются закрытым ключом удостоверяющего центра.

4 Открытый ключ УЦ, позволяющий проверять сертификаты, доступен всем пользователям инфраструктуры



Инфраструктура открытых ключей



Анализ сетевого окружения

<https://smurav.github.io/ta43/pk23>

Уязвимости компьютерных систем

ГОСТ Р 56546-2015

Уязвимость — недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации.

Классификация уязвимостей осуществляется по:

- ◆ области происхождения уязвимости
- ◆ типу недостатков ИС
- ◆ месту возникновения (проявления) уязвимости ИС

Области происхождения уязвимостей

- ◆ Уязвимости кода
- ◆ Уязвимости конфигурации
- ◆ Уязвимости архитектуры
- ◆ Организационные уязвимости
- ◆ Многофакторные уязвимости

Типы уязвимостей

- ◆ недостатки, связанные с неправильной настройкой параметров ПО
- ◆ недостатки, связанные с неполной проверки входных данных
- ◆ недостатки, связанные с возможностью прослеживания пути доступа к каталогам
- ◆ недостатки, связанные с возможностью перехода по ссылкам
- ◆ недостатки, связанные с возможностью внедрения команд ОС
- ◆ недостатки, связанные с межсайтовым выполнением сценариев
- ◆ недостатки, связанные с внедрением интерпретируемых операторов языков программирования или разметки
- ◆ недостатки, связанные с внедрением произвольного кода

Типы уязвимостей (продолжение)

- ◆ недостатки, связанные с переполнением буфера памяти
- ◆ недостатки, связанные с неконтролируемой форматной строкой
- ◆ недостатки, связанные с вычислениями
- ◆ недостатки, приводящие к утечке/раскрытию информации ограниченного доступа
- ◆ недостатки, связанные с управлением полномочиями (учетными данными)
- ◆ недостатки, связанные с управлением разрешениями, привилегиями и доступом
- ◆ недостатки, связанные с аутентификацией
- ◆ недостатки, связанные с криптографическими преобразованиями (недостатки шифрования)

Типы уязвимостей (продолжение)

- ◆ недостатки, связанные с подменой межсайтовых запросов
- ◆ недостатки, приводящие к "состоянию гонки"
- ◆ недостатки, связанные с управлением ресурсами
- ◆ иные типы недостатков

Места возникновения уязвимостей

- ◆ уязвимости в общесистемном (общем) ПО
- ◆ уязвимости в прикладном ПО
- ◆ уязвимости в специальном ПО
- ◆ уязвимости в технических средствах
- ◆ уязвимости в портативных технических средствах
- ◆ уязвимости в сетевом (коммуникационном, телекоммуникационном) оборудовании
- ◆ уязвимости в средствах защиты информации

Международная классификация уязвимостей

- ◆ Open Web Application Security Project Top 10 (OWASP)
- ◆ Common Weakness Enumeration (CWE)
- ◆ Common Attack Pattern Enumeration and Classification (CAPEC)
- ◆ The Web Application Security Consortium Threat Classification v2.0 (WASC)
- ◆ Seven Pernicious Kingdoms

Базы данных уязвимостей

Имя	Адрес
Банк данных угроз безопасности информации	https://bdu.fstec.ru/vul
Packet Storm	https://packetstormsecurity.com/
National Vulnerability Database	https://nvd.nist.gov/
IBM iSS X-Force	https://exchange.xforce.ibmcloud.com/
Vulnerability Notes Database	https://www.kb.cert.org/vuls/
UC-CERT Alerts	https://us-cert.cisa.gov/ncas/alerts
Bugtraq SecurityFocus	https://www.securityfocus.com/

Базы данных уязвимостей (продолжение)

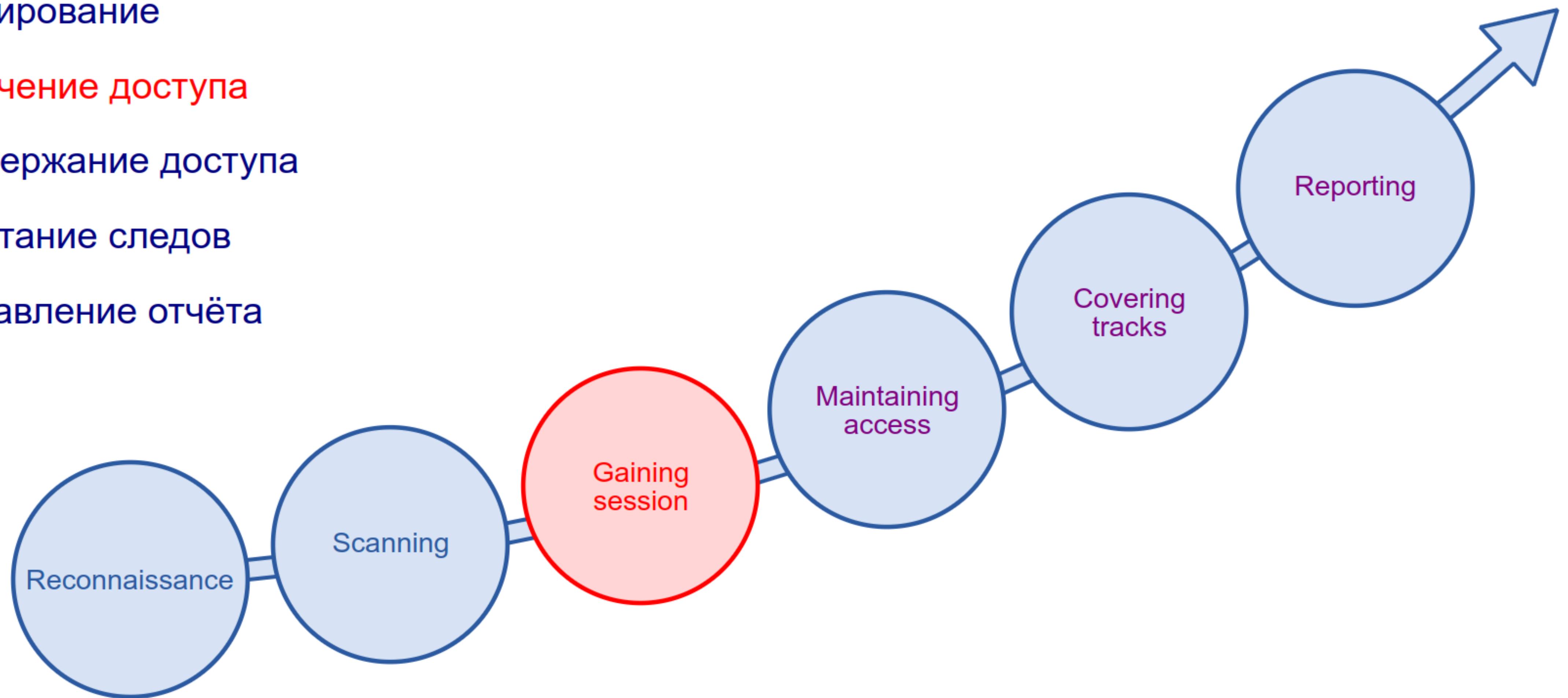
Имя	Адрес
SecuriTeam	https://securiteam.com/
CXSecurity	https://cxsecurity.com/
XSS attacks information	http://xssed.com/
Security Vulnerabilities DB	https://vulners.com/
Common Vulnerabilities and Exposures	http://cve.mitre.org/
Exploit Database	https://www.exploit-db.com/
CVE Details	https://www.cvedetails.com/

Поиск уязвимостей

<https://smurav.github.io/ta43/pk23>

Получение доступа

1. Разведка и сбор данных
2. Сканирование
3. Получение доступа
4. Поддержание доступа
5. Заметание следов
6. Составление отчёта



Исследование выявленных уязвимостей

- ◆ Анализ программного кода
- ◆ Обратный инжиниринг
- ◆ Использование специализированных инструментальных средств
- ◆ Разработка и адаптация полезной нагрузки

Экспloit

Экспloit

Компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему.

- ◆ Удалённый экспloit - работает через сеть и использует уязвимость в защите без какого-либо предварительного доступа к уязвимой системе
- ◆ Локальный экспloit - запускается непосредственно в уязвимой системе, требуя предварительного доступа к ней.

Полезная нагрузка

Полезная нагрузка

Вредоносный код, предназначенных для встраивания в эксплойт.

- ◆ **Singles** - самостоятельные и полностью автономные.
- ◆ **Stagers** - устанавливают сетевое соединение между злоумышленником и жертвой, они компактны и надежны.
- ◆ **Stages** - компоненты полезной нагрузки, которые загружаются модулями Stagers.

Доставка полезной нагрузки

Для доставки полезной нагрузки различные методы:

- ◆ удалённые эксплойты
- ◆ электронная почта
- ◆ разделяемые файловые ресурсы
- ◆ съёмные носители
- ◆ web-ресурсы

Повышение привилегий

Вертикальное повышение привилегий

Получение пользователем с низкими привилегиями доступ к функциям приложений, предназначенных для привилегированных пользователей.

Горизонтальное повышение привилегий

Получение доступа к функциям, предназначенных для других обычных пользователей.

Подходы к повышению привилегий

- ◆ Локальная эксплуатация
- ◆ Использование ошибок конфигурации
- ◆ Парольные атаки
- ◆ Исследование сетевого траффика для захвата учётных данных
- ◆ Имитация сетевых пакетов

Парольные атаки

- ◆ Атаки "грубой силы" (Brute force)
- ◆ Атаки по словарю (Dictionary attacks)
- ◆ Атаки на парольные хэши (Rainbow attacks)
- ◆ Кейлогеры

Подходы к парольным атакам

Автономные атаки (offline)

Атака осуществляется путём анализа хэшей паролей, полученных с целевой системы, без обращения к целевой системе.

Интерактивные атаки (online)

Осуществляются попытки подбора пароля при непосредственном доступе к целевой системе.

Пароли в Linux

Пароли пользователей Linux расположены в файле /etc/shadow

```
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7...
```

1. Имя пользователя (msfadmin)
2. Хэшированный пароль (\$1\$XN10Zj2c\$Rt/zzCW3mLtUWA.ihZjA5/)
3. Дата последнего изменения пароля (14684)
4. Минимальный срок действия пароля (0)
5. Максимальный срок действия пароля (99999)
6. Период предупреждения о необходимости изменения пароля (7)
7. Срок действия просроченного пароля до отключения учётной записи
8. Дата отключения учётной записи
9. Зарезервированное поле

Хэширование паролей в Linux

Структура хэшированного пароля

\$id\$salt\$hashed

id - Алгоритм хэширования

1 - MD5

2a - Blowfish

2y - Blowfish

5 - SHA-256

6 - SHA-512

salt - Соль

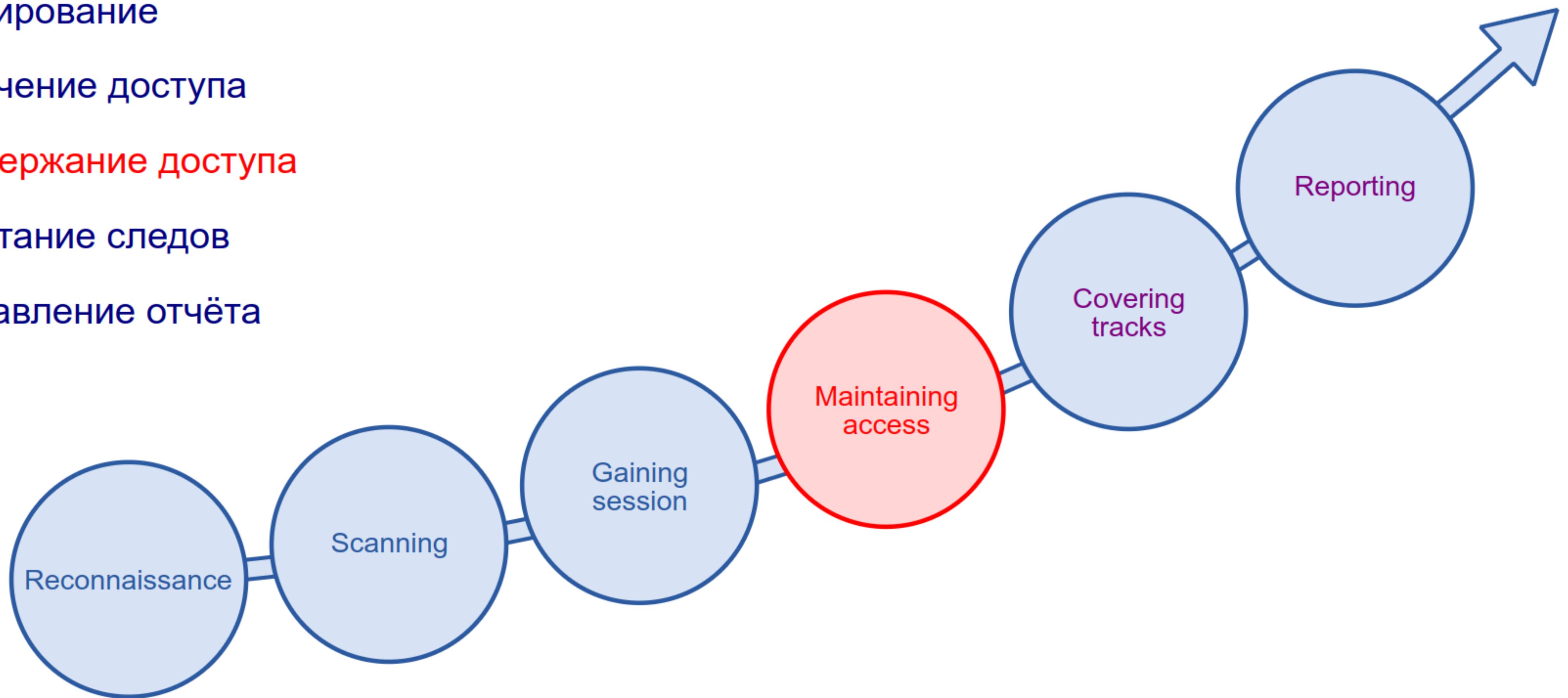
hashed - Хэш

Эксплуатация уязвимостей

<https://smurav.github.io/ta43/pk23>

Поддержание доступа

1. Разведка и сбор данных
2. Сканирование
3. Получение доступа
4. Поддержание доступа
5. Заметание следов
6. Составление отчёта



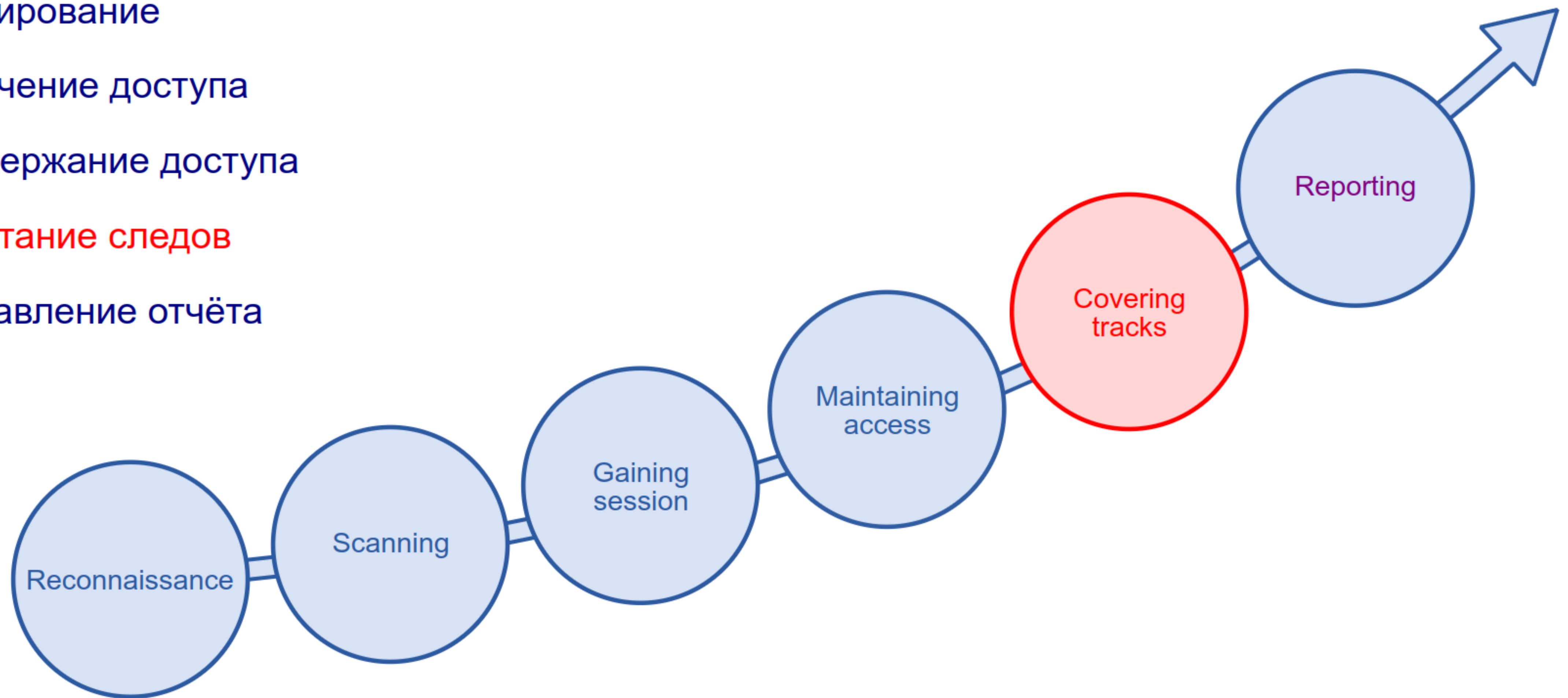
Подходы к поддержанию доступа

На случай устранения уязвимостей, использованных для получения доступа и повышения привилегий необходимо реализовать альтернативные механизмы получения доступа:

- ◆ Бэкдоры
- ◆ Туннелирование
- ◆ Создание пользователей
- ◆ Установка SSH-ключей

Заметание следов

1. Разведка и сбор данных
2. Сканирование
3. Получение доступа
4. Поддержание доступа
5. Заметание следов
6. Составление отчёта

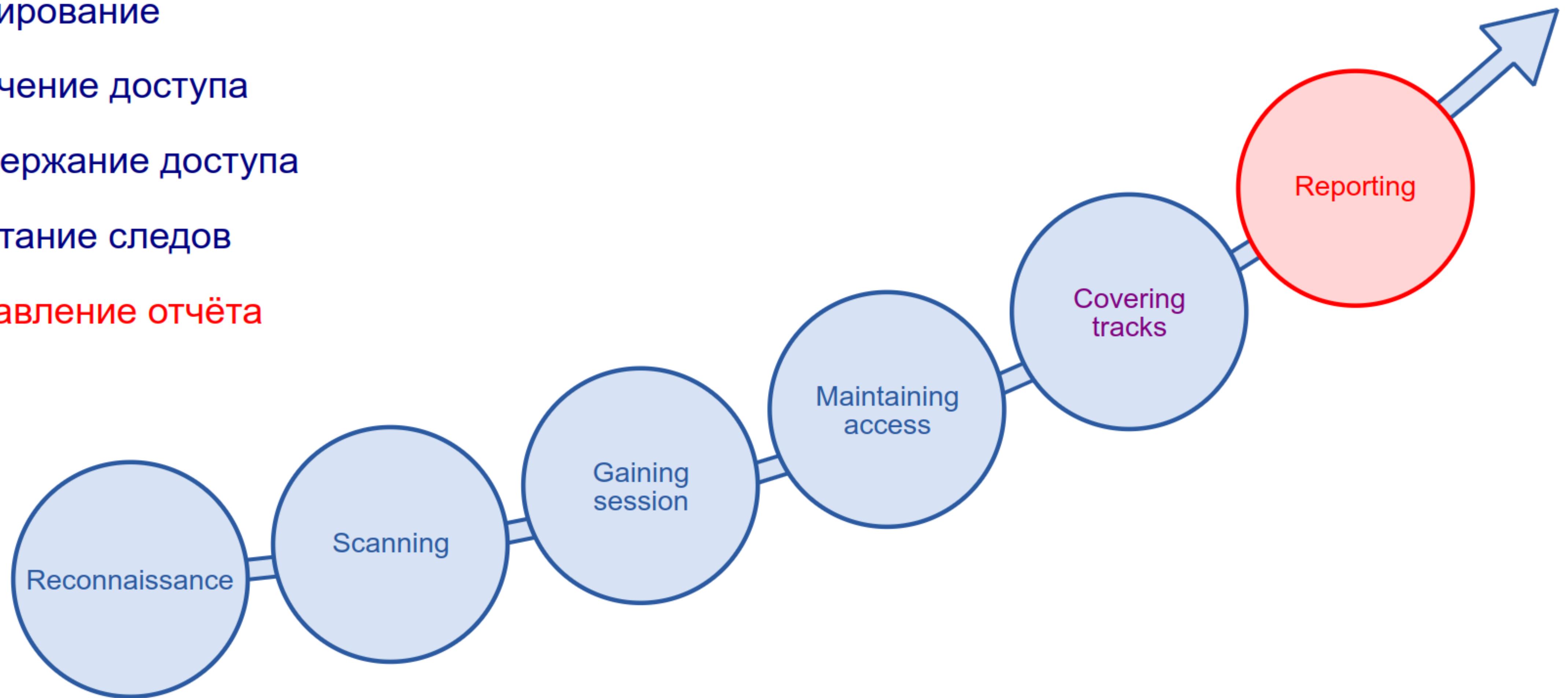


Способы заметания следов

- ◆ Восстановление настроек
- ◆ Восстановление журналов
- ◆ Удаление загруженных файлов
- ◆ Устранение бэкдоров

Подготовка отчётов

1. Разведка и сбор данных
2. Сканирование
3. Получение доступа
4. Поддержание доступа
5. Заметание следов
6. Составление отчёта



Виды подготовляемых отчётов

- ◆ Исполнительный отчёт
- ◆ Отчёт для руководства
- ◆ Технический отчёт

Исполнительный доклад

- ◆ Цель проекта
- ◆ Классификация рисков уязвимости
- ◆ Резюме
- ◆ Статистика
- ◆ Матрица рисков

Отчёт для руководства

- ◆ Достижение соответствия
- ◆ Методология тестирования
- ◆ Предположения и ограничения
- ◆ Управление изменениями
- ◆ Управление конфигурациями

Технический отчёт

- ◆ Вопросы безопасности
- ◆ Карта уязвимостей
- ◆ Карта эксплойтов
- ◆ Передовой опыт

Устранение типовых уязвимостей

- ◆ Управление конфигурациями
- ◆ Управление обновлениями
- ◆ Управление изменениями
- ◆ Управление уязвимостями

Обнаружение атак на компьютерные системы

Honeypot (с англ. — «горшочек с мёдом») — ресурс, представляющий собой приманку для злоумышленников.

Задачи:

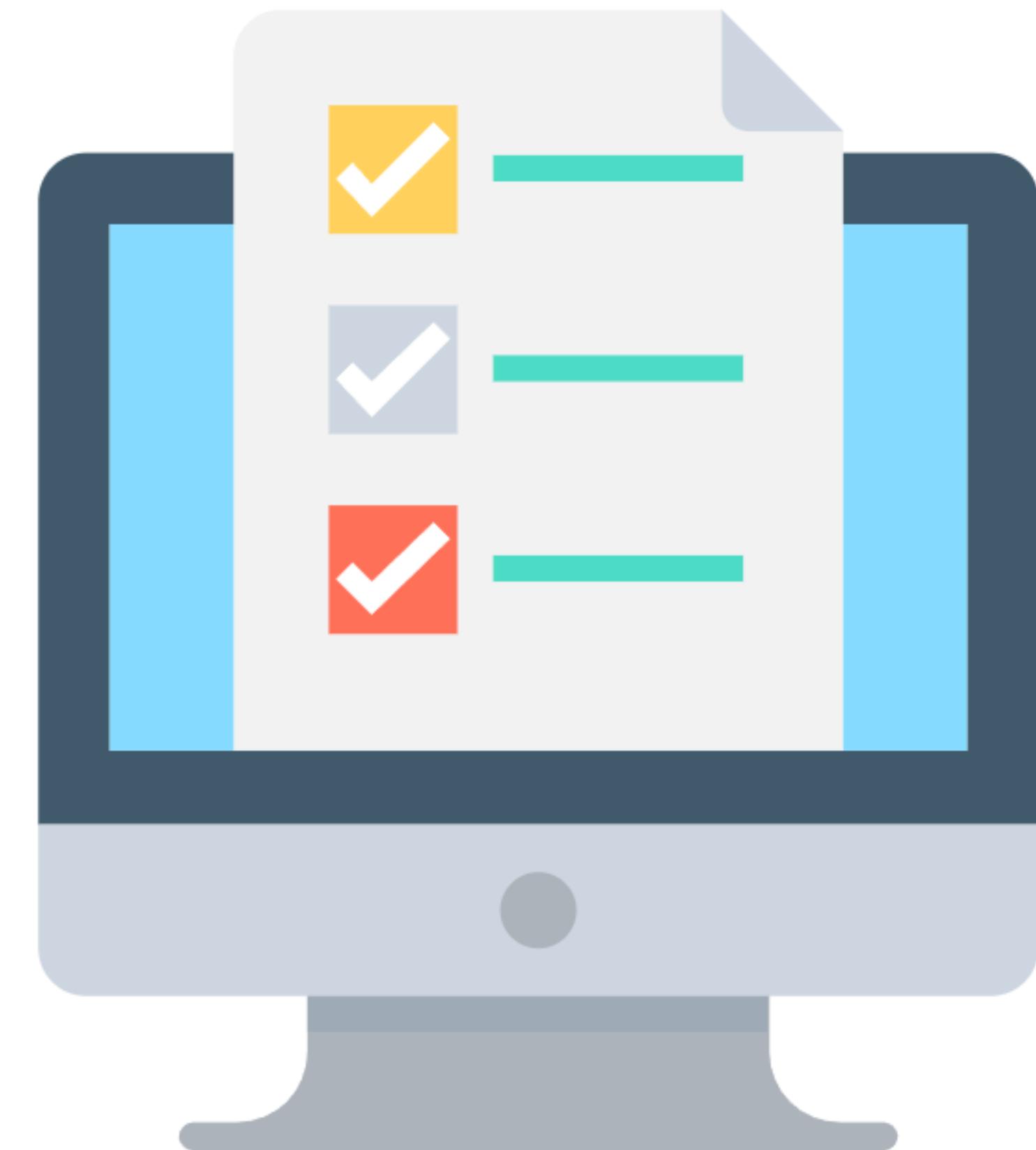
- ◆ обнаружение фактов выполнения атак
- ◆ сбор сведений о стратегиях и методах, используемых злоумышленниками
- ◆ снижение эффективности атак



FIM (File integrity monitoring) — технологии контроля файлов операционной системы, баз данных и прикладного программного обеспечения, для определения их изменений или повреждений.

Контролируемые параметры:

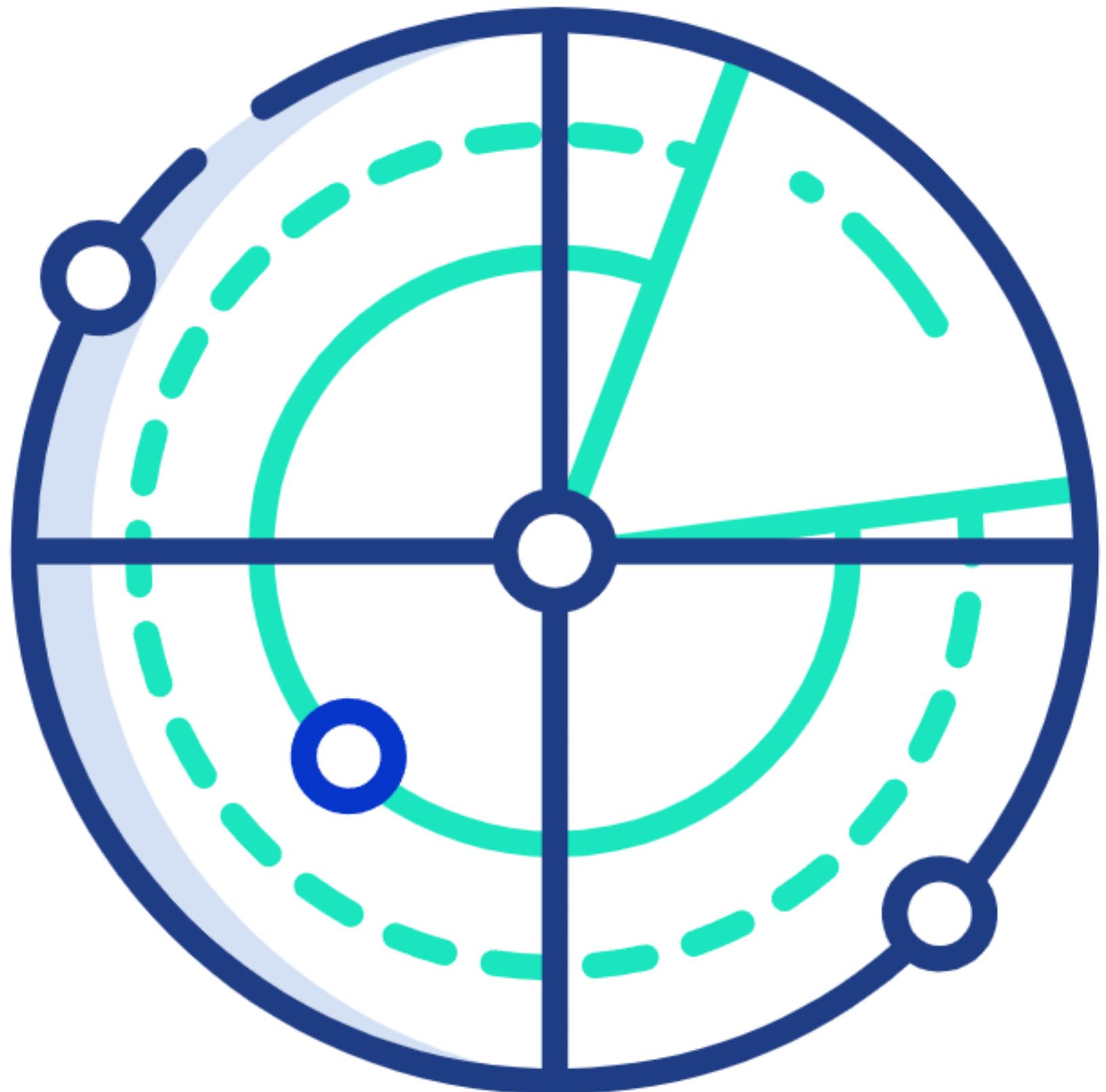
- ◆ наличие
- ◆ содержимое
- ◆ права доступа
- ◆ атрибуты



IDS (Intrusion Detection System) — система обнаружения вторжений (СОВ), предназначенная для выявления фактов неавторизованного доступа в компьютерную систему

Состав:

- ◆ сенсоры
- ◆ подсистема анализа
- ◆ хранилище
- ◆ консоль управления



Виды IDS

- ◆ Network-based IDS (NIDS) — отслеживает вторжения, проверяя сетевой трафик и ведет наблюдение за сетевыми узлами.
- ◆ Protocol-based IDS (PIDS) — отслеживает и анализирует коммуникационные протоколы со связанными системами или пользователями.
- ◆ Application Protocol-based IDS (APIDS) — ведет наблюдение и анализ данных, передаваемых с помощью специфичных для приложений протоколов.
- ◆ Host-based IDS (HIDS) — располагается на хосте и отслеживает вторжения, используя анализ системных вызовов, логов приложений, модификаций файлов (исполняемых, файлов паролей, системных баз данных), состояния хоста и прочих источников.
- ◆ Гибридная СОВ совмещает в себе несколько подходов.

SIEM (Security information and event management) — системы управления информацией о безопасности и событиями безопасности.

Решаемые задачи:

- ◆ сбор, обработка и анализ событий безопасности
- ◆ обнаружение в режиме реального времени атак и нарушений политик безопасности
- ◆ оперативная оценка защищенности ресурсов
- ◆ анализ и управление рисками безопасности
- ◆ проведение расследований инцидентов



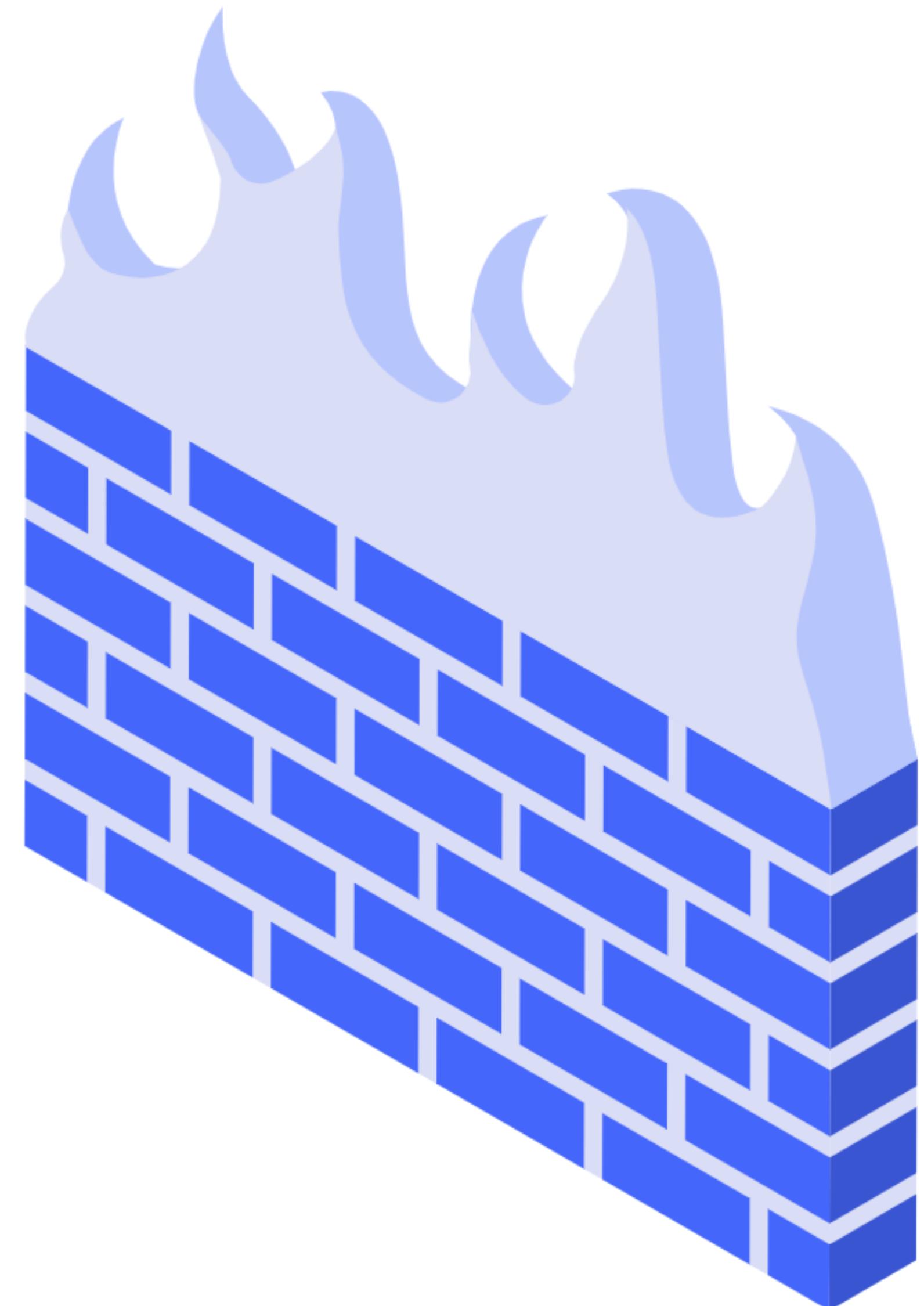
SIEM

Межсетевой экран

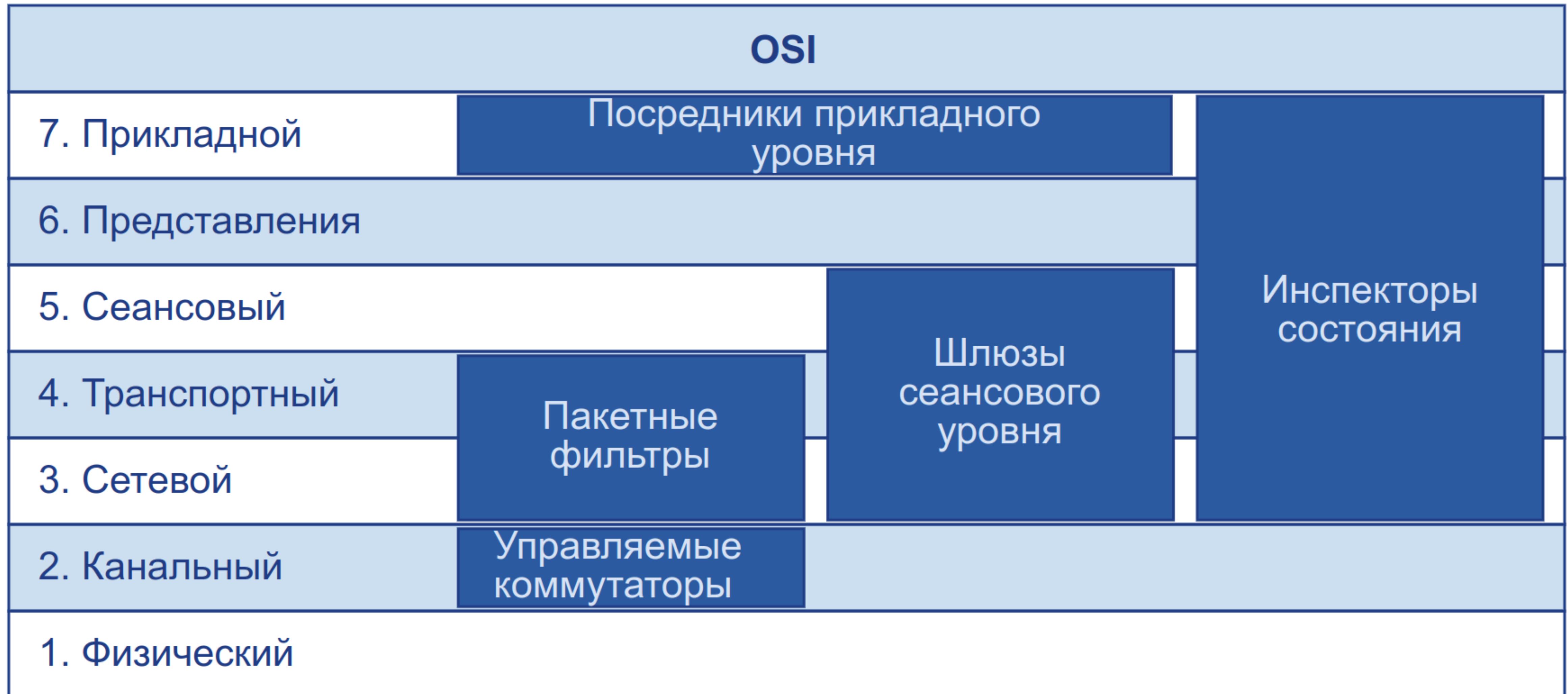
Межсетевой экран — программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него трафика в соответствии с заданными правилами.

Задачи:

- ◆ защита сегментов сети или отдельных хостов внешних потоков
- ◆ предотвращение выхода важных данных во внешнюю среду



Классификация межсетевых экранов

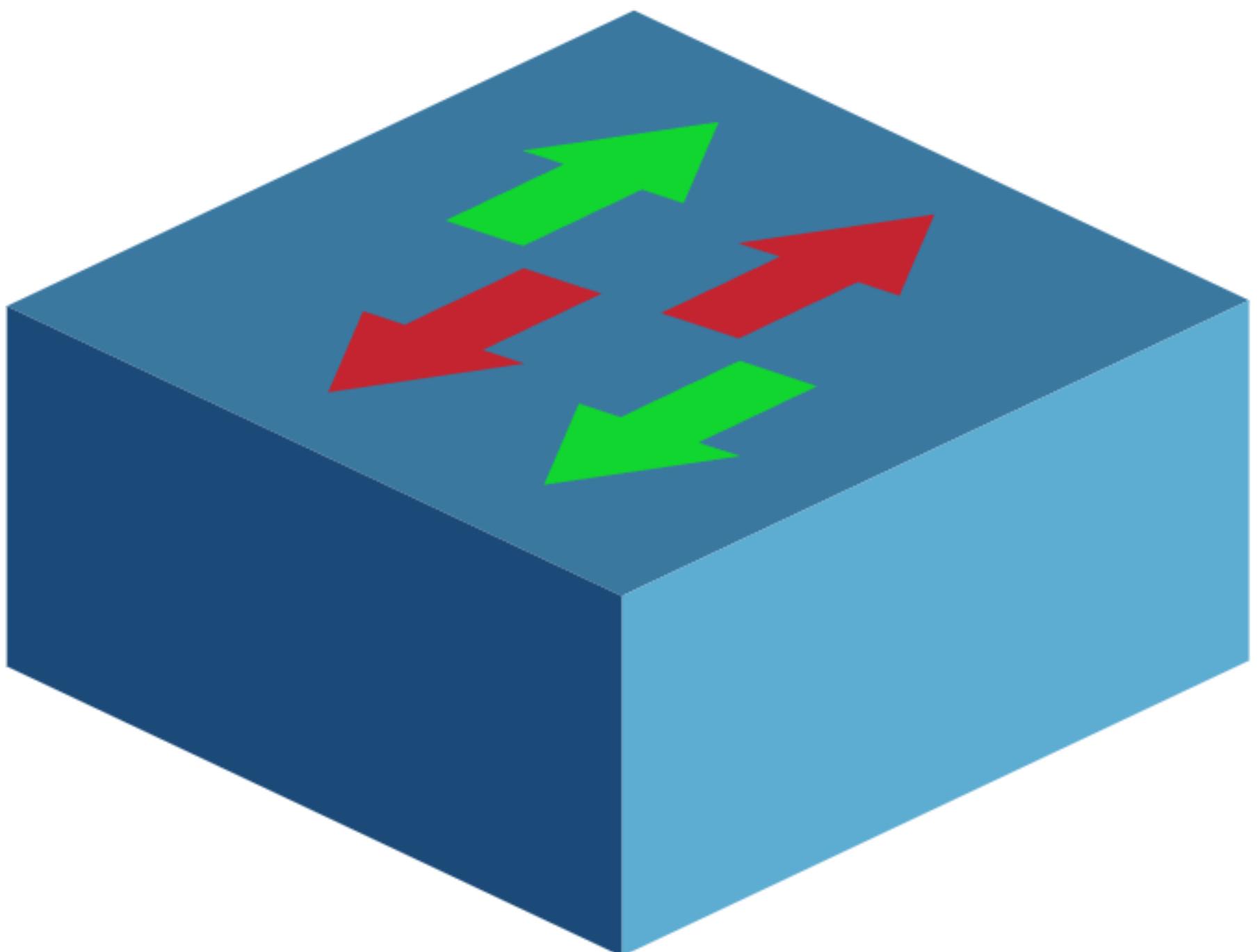


Управляемые коммутаторы

Некоторые управляемые коммутаторы позволяют фильтровать трафик на основе MAC-адресов или VLAN ID.

Особенности:

- ◆ MAC-адреса могут быть подменены программно
- ◆ Очень высокое быстродействие



Пакетные фильтры

Пакетные фильтры контролируют прохождение трафика на основе информации, содержащейся в заголовке пакетов.

Особенности:

- ◆ Анализируются IP-адреса источника и получателя,
- ◆ тип транспортного протокола, поля служебных заголовков, порт источника и получателя
- ◆ Не анализируются протоколы более высокого уровня
- ◆ Фильтрация фрагментированных пакетов затруднена
- ◆ Уязвимы для атак подмены сетевого адреса
- ◆ Высокая скорость работы

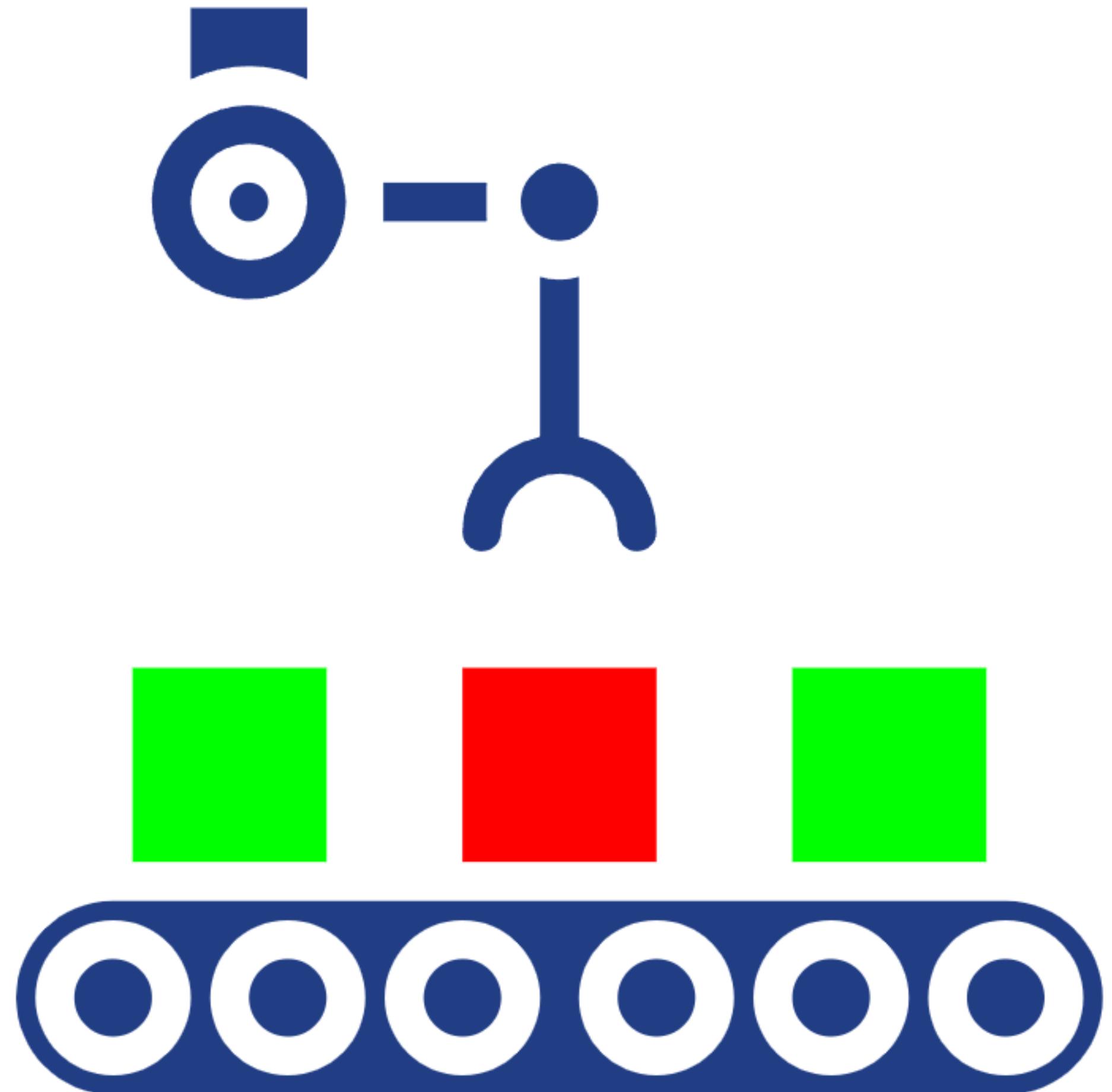


Шлюзы сеансового уровня

Межсетевой экран сеансового уровня исключает прямое взаимодействие внешних хостов с узлом, расположенным в локальной сети, выступая в качестве прокси, который реагирует на все входящие пакеты и проверяет их допустимость на основании текущей фазы соединения.

Особенности:

- ◆ Гарантирует, что ни один сетевой пакет не будет пропущен, если он не принадлежит ранее установленному соединению.
- ◆ Пакеты, «притворяющиеся» пакетами уже завершённого соединения, отбрасываются
- ◆ Скрывает топологию защищаемой сети
- ◆ Защищает от DoS-атак



Посредники прикладного уровня

Межсетевые экраны прикладного уровня определяет тип передаваемой информации в зависимости от контекста отдельного протокола прикладного уровня.

Особенности:

- ◆ Блокирует недопустимые и нежелательные последовательности команд
- ◆ Может проверять аргументы входных данных
- ◆ Способны выполнять аутентификацию
- ◆ Для каждого протокола нужна своя реализация
- ◆ Высокие затраты на анализ сетевых пакетов



Инспекторы состояния

Инспекторы состояния совмещают в себе функционал других видов межсетевых экранов

Особенности:

- ◆ Проверка пакетов на основе таблицы правил
- ◆ Проверка сессий на основе таблицы состояний
- ◆ Способны выполнять аутентификацию
- ◆ Проверка приложений с помощью специализированных посредников
- ◆ Относительно высокая скорость работы



Ссылки

- ◆ ГОСТ Р ИСО/МЭК ТО 10032-2007: Эталонная модель управления данными
- ◆ Конвенция о преступности в сфере компьютерной информации ETS N 185
- ◆ ГОСТ Р 51275-2006 - Защита информации.
Объект информатизации. Факторы, воздействующие на информацию
- ◆ Федеральный закон от 26 июля 2017 г. N 187-ФЗ
О безопасности критической информационной инфраструктуры Российской Федерации
- ◆ Стратегия противодействия целенаправленным атакам
- ◆ Парасрам Ш., Замм А., Хериянто Т. Kali Linux. Тестирование на проникновение и безопасность. - СПб.: Питер, 2020. - 448 с.

Спасибо за внимание

smurav@mail.ru

<https://smurav.github.io/ta43/pk23>