Введение в информационную безопасность

Управление IT-сервисом и контентом

Юдинцев В. В.

Кафедра математических методов в экономике

29 сентября 2023 г.

САМАРСКИЙ УНИВЕРСИТЕТ
SAMARA UNIVERSITY

Содержание

1. Введение
2. Цели и задачи
3. Меры обеспечения ИБ
4. Сервисы безопасности

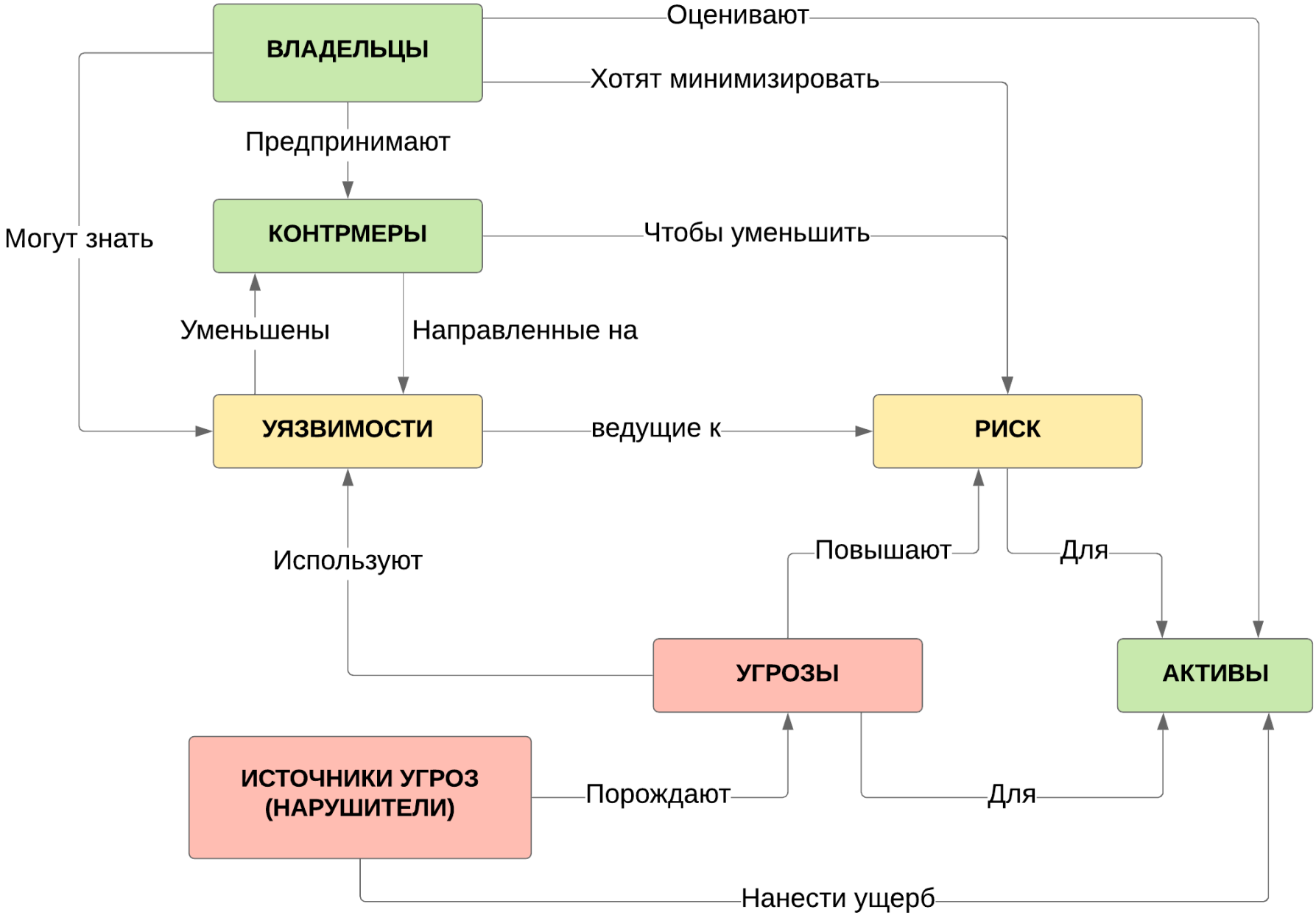
Введение

Безопасность

- Бизнес зависит от информационных систем
- ИТ-инфраструктура имеет связи с глобальной сетью
- ИТ-инфраструктура сложна
- Увеличение сложности ИТ-инфраструктуры $\Rightarrow$ увеличение уязвимости бизнеса

Информационная безопасность

- Под информационной безопасностью (ИБ) организации понимается состояние защищенности интересов (целей) организации в условиях угроз в информационной сфере
- Информационная сфера представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение, хранение и использование информации, а также системы регулирования возникающих при этом отношений


ВЛАДЕЛЬЦЫ
Оценивают
Хотят минимизировать
Предпринимают
КОНТРМЕРЫ
Могут знать
Чтобы уменьшить
Уменьшены
Направленные на
УЯЗВИМОСТИ
ведущие к
РИСК
Используют
Повышают
Для
УГРОЗЫ
АКТИВЫ
ИСТОЧНИКИ УГРОЗ
(НАРУШИТЕЛИ)
Порождают
Для
Нанести ущерб

Угроза ИБ

Угрозы безопасности информации – события или действия, которые могут привести к искажению, несанкционированному использованию или разрушению информационных ресурсов управляемой системы, а также программных и аппаратных средств

Классификация угроз

Угроза непосредственно информационной безопасности:

- Доступность
- Целостность
- Конфиденциальность

Цели угроз:

- Данные
- Программы
- Аппаратура
- Поддерживающая инфраструктура

Классификация угроз

По способу осуществления:

- Случайные или преднамеренные
- Природного или техногенного характера

По расположению источника угрозы:

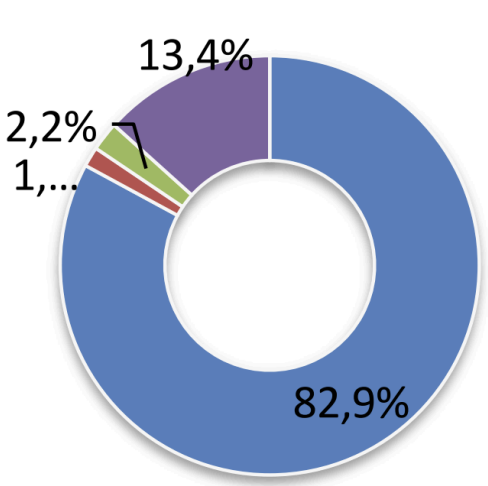
- Внутренние
- Внешние

Риски информационной безопасности

- Риск утечки конфиденциальной информации
- Риск потери или недоступности важных данных
- Риск использования неполной или искаженной информации
- Риск неправомочной скрытой эксплуатации информационно-вычислительных ресурсов
- Риск распространения во внешней среде информации, угрожающей репутации организации

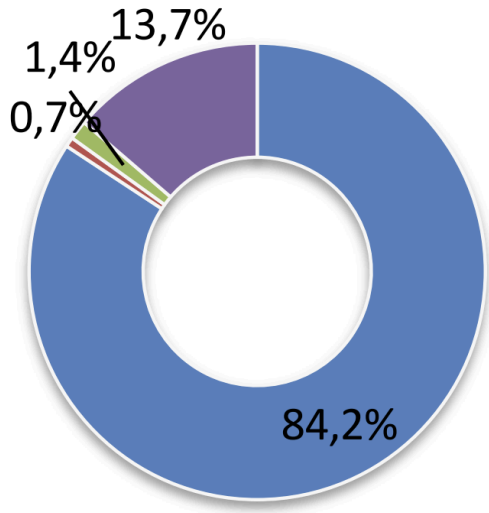
Распределение утечек по типам

Мир 1H 2022



- Персональные данные
- Платежная информация
- Государственная тайна
- Коммерческая тайна, ноу-хау

Россия 1H 2022

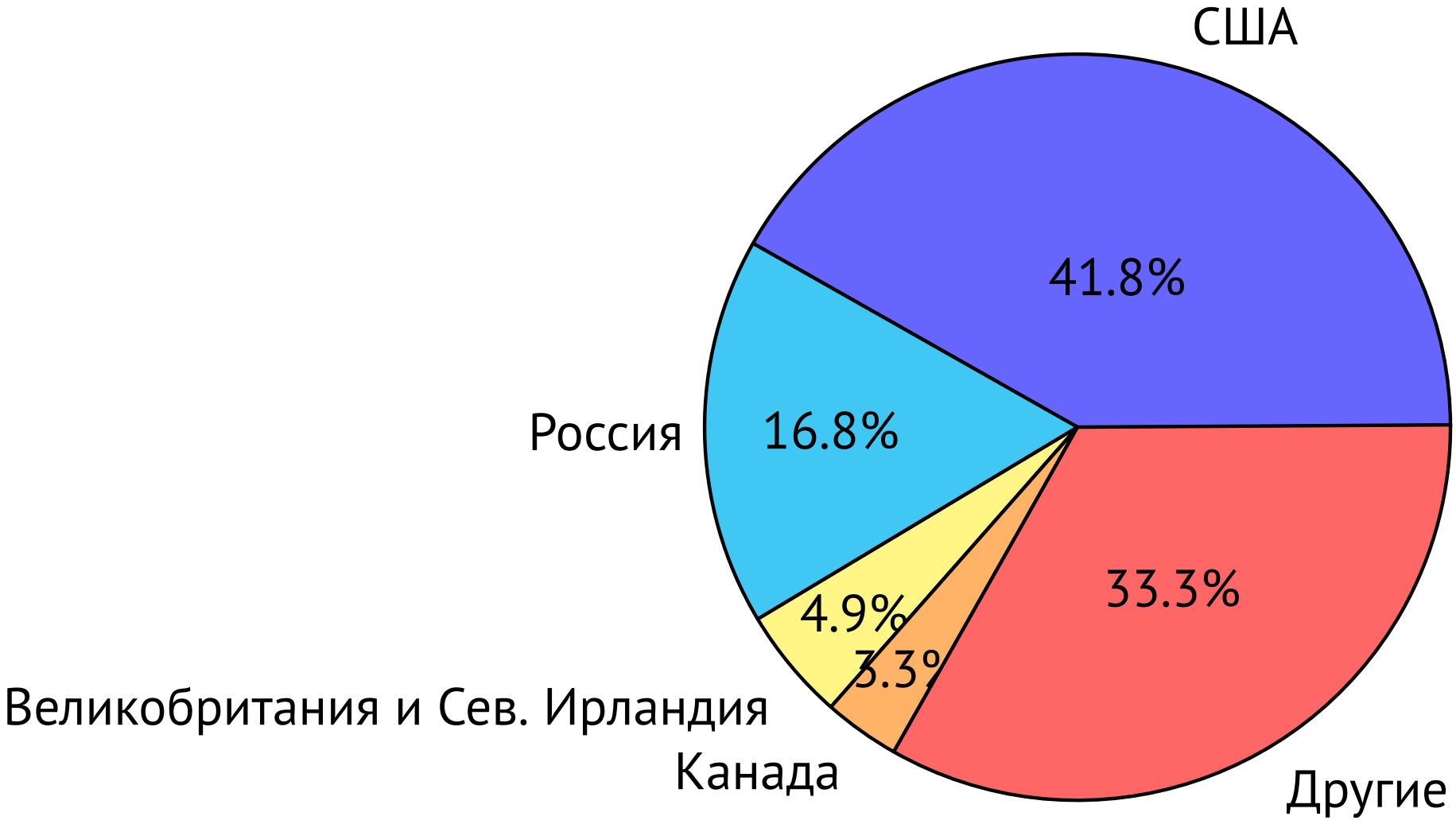


- Персональные данные
- Платежная информация
- Государственная тайна
- Коммерческая тайна, ноу-хау

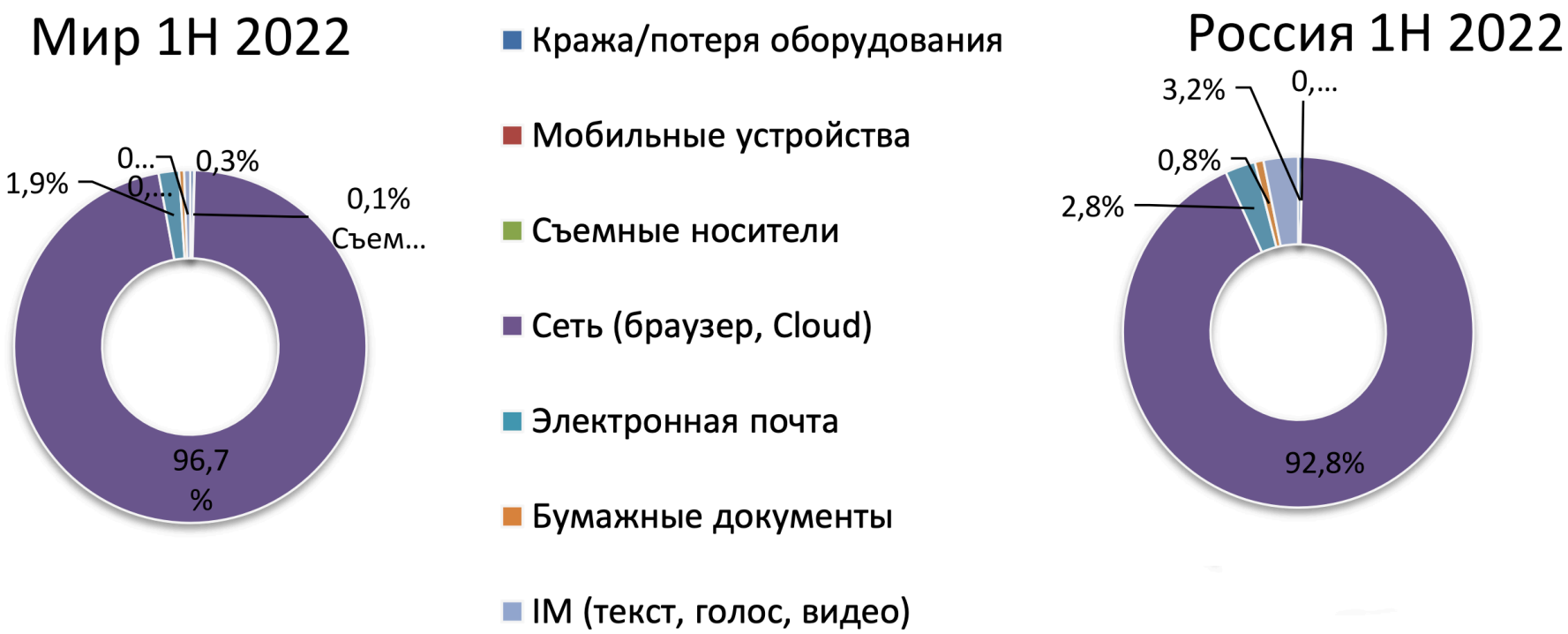
Штрафы

- **$148 млн – Uber**
  утечка персональных данных более 57 млн клиентов и водителей такси в 2016 г
- **$50 млн – Yahoo**
  Компрометированы более 3 млрд аккаунтов (2013-2014 годы).
- **$20.9 млн – Tesco Bank**
  Кража киберпреступниками 2.26 млн фунтов в 2016 году

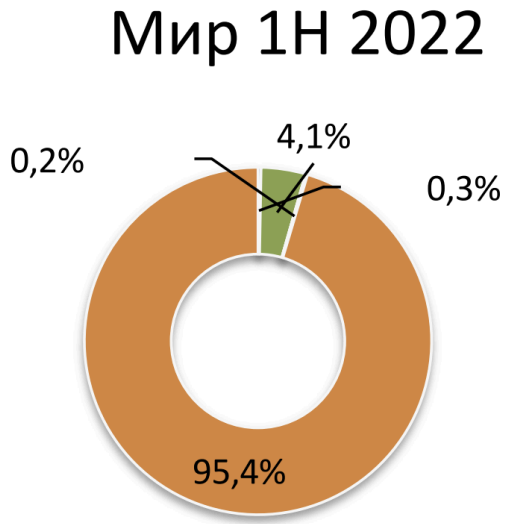
Распределение утечек по странам (2021)

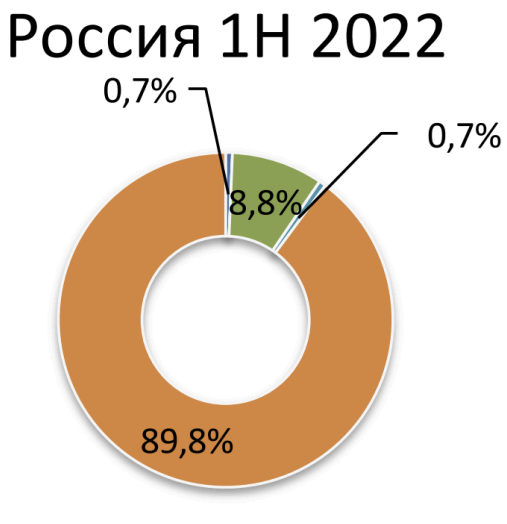


Каналы утечек



Распределение утечек по источнику





- Руководитель
- Системный администратор
- Непривилегированный сотрудник
- Бывший сотрудник
- Подрядчик
- Внешний злоумышленник

- Руководитель
- Системный администратор
- Непривилегированный сотрудник
- Бывший сотрудник
- Подрядчик
- Внешний злоумышленник

Факторы, влияющие на ИБ

http://habrastorage.org

- расширение сотрудничества предприятия с партнерами
- автоматизация бизнес-процессов на предприятии
- расширение кооперации исполнителей при построении и развитии информационной инфраструктуры предприятия
- рост объемов информации предприятия, передаваемой по открытым каналам связи
- рост компьютерных преступлений

Цели и задачи

Аспекты информационной безопасности

Основой безопасной ИТ-инфраструктуры является следующие три принципа

- **Конфиденциальность**
  защита информации от несанкционированного доступа и использования
- **Целостность**
  точность, полнота и своевременность информации
- **Доступность**
  информация должна быть доступна в любой момент предварительного согласованного временного интервала.

Основные сервисы ИБ

Для реализации базовых принципов ИБ необходимо выполнение следующих сервисов

- Идентификация
- Аутентификация
- Подотчетность
- Невозможность отказа
- Авторизация

Меры обеспечения ИБ

Меры обеспечения ИБ

Для обеспечения информационной безопасности необходим комплексный подход сочетающий следующие меры обеспечения информационной безопасности:

- Законодательные
- Административные
- Процедурные
- Программно-технические

Законодательный уровень

- Конституция
  Статьи 23, 24, 41, 42
- Гражданский кодекс
  Баковская, служебная, коммерческая тайна
- Уголовный кодекс (Глава 28)
  Статья 272, 273, 274
- Закон о государственной тайне
- Об электронной цифровой подписи
- О Персональных данных

Административный уровень

- Политика информационной безопасности – совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов
- Политика ИБ определяет стратегию предприятия в области ИБ, ресурсы, затрачиваемые на ИБ
- Политика безопасности предприятия определяется Концепцией обеспечения ИБ, а также другими нормативными и организационно-распорядительными документами предприятия, разрабатываемыми на основе концепции

Документы, определяющие политику ИБ

http://1cstart.kz

- Политика защиты от несанкционированного доступа к информации
- Политика предоставления доступа пользователей в ИС
- Политика управления паролями
- Политика резервного копирования и восстановления данных
- Политика предоставления доступа к ресурсам сети Интернет
- Должностные инструкции для операторов, администраторов и инженеров

Процедурный уровень

- Управление персоналом
- Физическая защита
- Поддержание работоспособности
- Реагирование на нарушения режима безопасности
- Планирование восстановительных работ

Программно-технические меры

https://digital.report

- Программно-технические меры направлены на контроль компьютерных сущностей оборудование, программы, данные
- Программно-технические меры образуют последний и самый важный рубеж информационной безопасности

Сервисы безопасности

Сервисы безопасности

- идентификация и аутентификация
- управление доступом
- протоколирование и аудит
- шифрование
- контроль целостности
- экранирование
- анализ защищенности
- обеспечение отказоустойчивости
- обеспечение безопасного восстановления
- туннелирование
- управление

Аутентификация и идентификации

- Чтобы исключить неправомерный доступ к информации применяют такие способы, как идентификация и аутентификация
- Идентификация – это механизм присвоения собственного уникального имени или образа пользователю, который взаимодействует с информацией.
- Аутентификация – это система способов проверки совпадения пользователя с тем образом, которому разрешен допуск.

Способы аутентификации

https://www.rutoken.ru

- Имя и пароль
- Двухфакторная аутентификация при помощи смарт-карты, USB-токенов, приложений, одноразовых паролей
- Биометрические данные

Повышение надежности парольной защиты

KeePassXC

`https://keepassxc.org`

- технических ограничения (минимальная длина, сложность)
- ограничение срока действия
- ограничение числа неудачных попыток входа
- использование программных генераторов паролей (KeePassXC, PasswordSafe)
- ограничение использования одинаковых паролей для разных сервисов

Управление доступом

- Средства управления доступом позволяют специфицировать и контролировать действия, которые субъекты (пользователи и процессы) могут выполнять над объектами (информацией и другими компьютерными ресурсами)
- Управление доступом – основной механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность объектов

Управление доступом

- **Избирательное управление доступом**
  Access Control List или ACL — список управления доступом, который определяет, кто или что может получать доступ к объекту (программе, процессу или файлу), и какие именно операции разрешено или запрещено выполнять субъекту
- **Управление доступом на основе ролей**
  Права доступа субъектов системы на объекты группируются с учётом специфики их применения, образуя роли

Протоколирование и аудит

- **Протоколирование** – сбор и накопление информации о событиях, происходящих в информационной системе
- **Аудит** – анализ накопленной информации, проводимый оперативно, в реальном времени или периодически

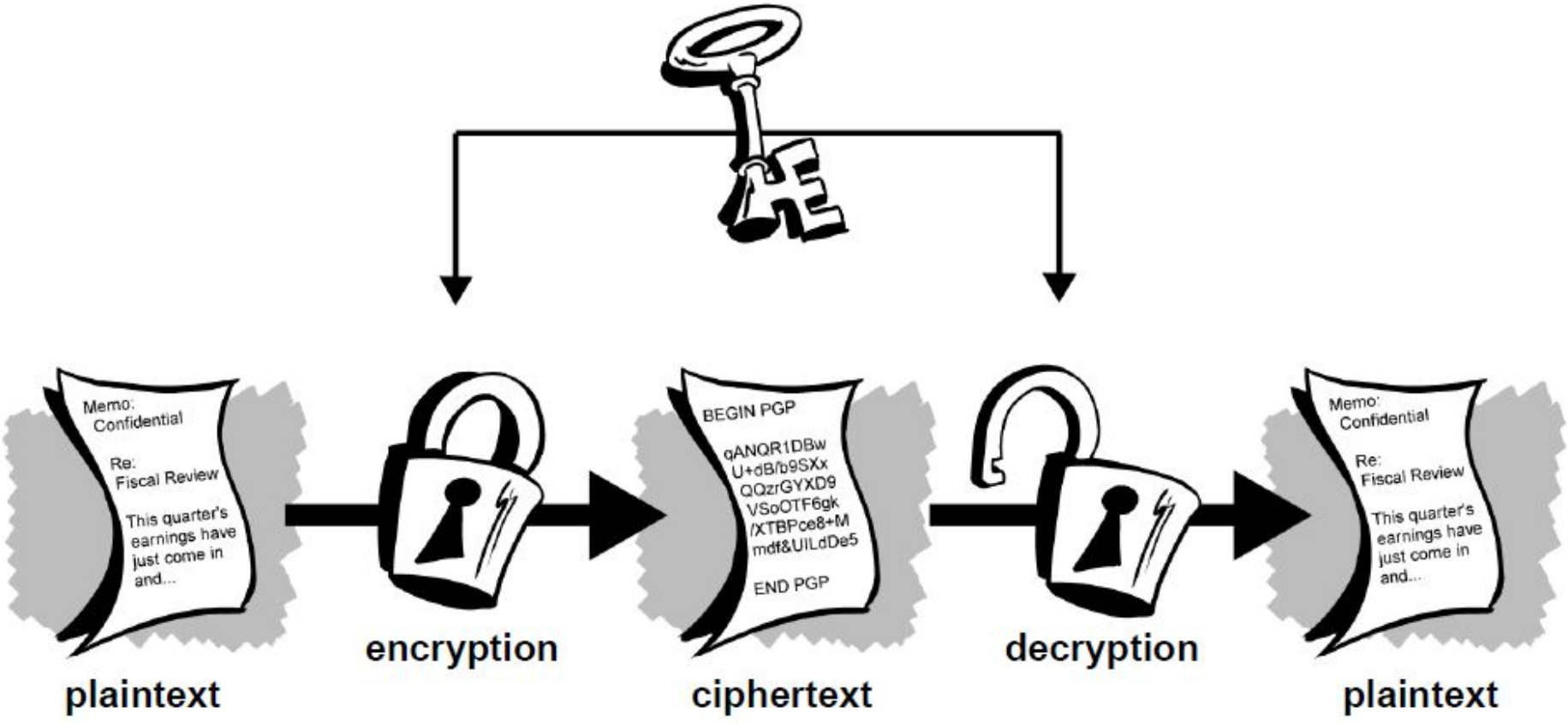
Криптография

https://digital.report

Криптография необходима для реализации трех сервисов безопасности:

- шифрование
- контроль целостности
- аутентификация

Симметричная криптография



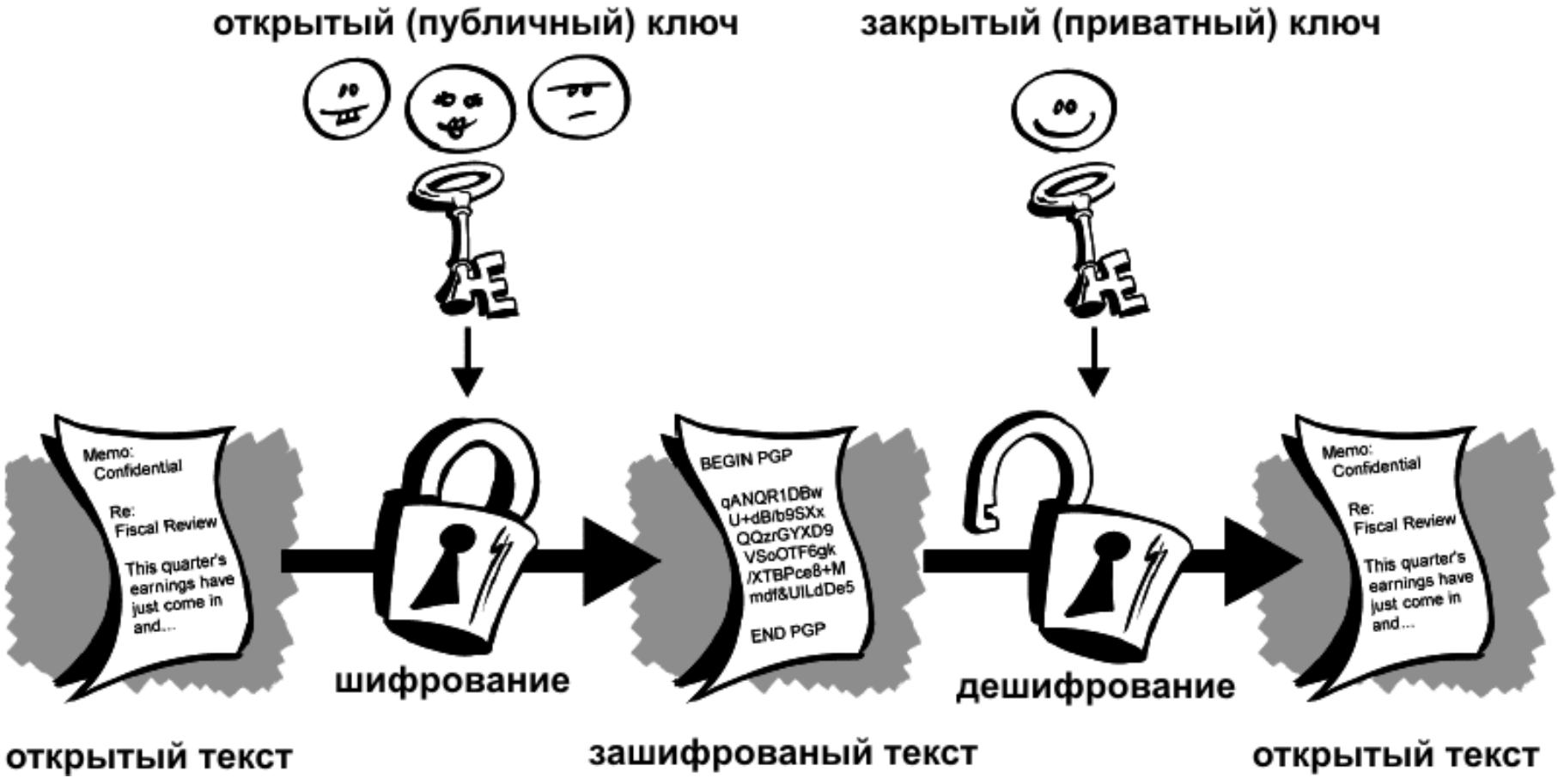
Один ключ для шифрования и расшифровки

https://chrispacia.files.wordpress.com/2013/09/symmetric-key-cyrptography.jpg

Симметричные алгоритмы

- DES
  блок: 64 бит, ключ 56 бит
- 3DES
  блок: 64 бит, ключ 168 бит
- AES
  блок: 128 бит, ключ 128/192/256 бит
- Blowfish
  блок 64 бита / ключ от 32 до 448 бит
- Serpent
  блок 128 бит / 128/192/256 бит
- ГОСТ Р 34.12-2015 (Кузнечик)
  блок 128 бит / ключ 256 бит

Асимметричная криптография



https://cdn-images-1.medium.com/max/1600/0*hgvn-X4rcJbqG7qo.png

Ассимметричные алгоритмы

- **RSA** (Rivest-Shamir-Adleman)
- DSA (Digital Signature Algorithm)
- Elgamal (Шифросистема Эль-Гамаля)
- **Diffie-Hellman** (Обмен ключами Диффи — Хелмана)
- ECDSA (Elliptic Curve Digital Signature Algorithm)
- ГОСТ Р 34.10-2012

Контроль целостности

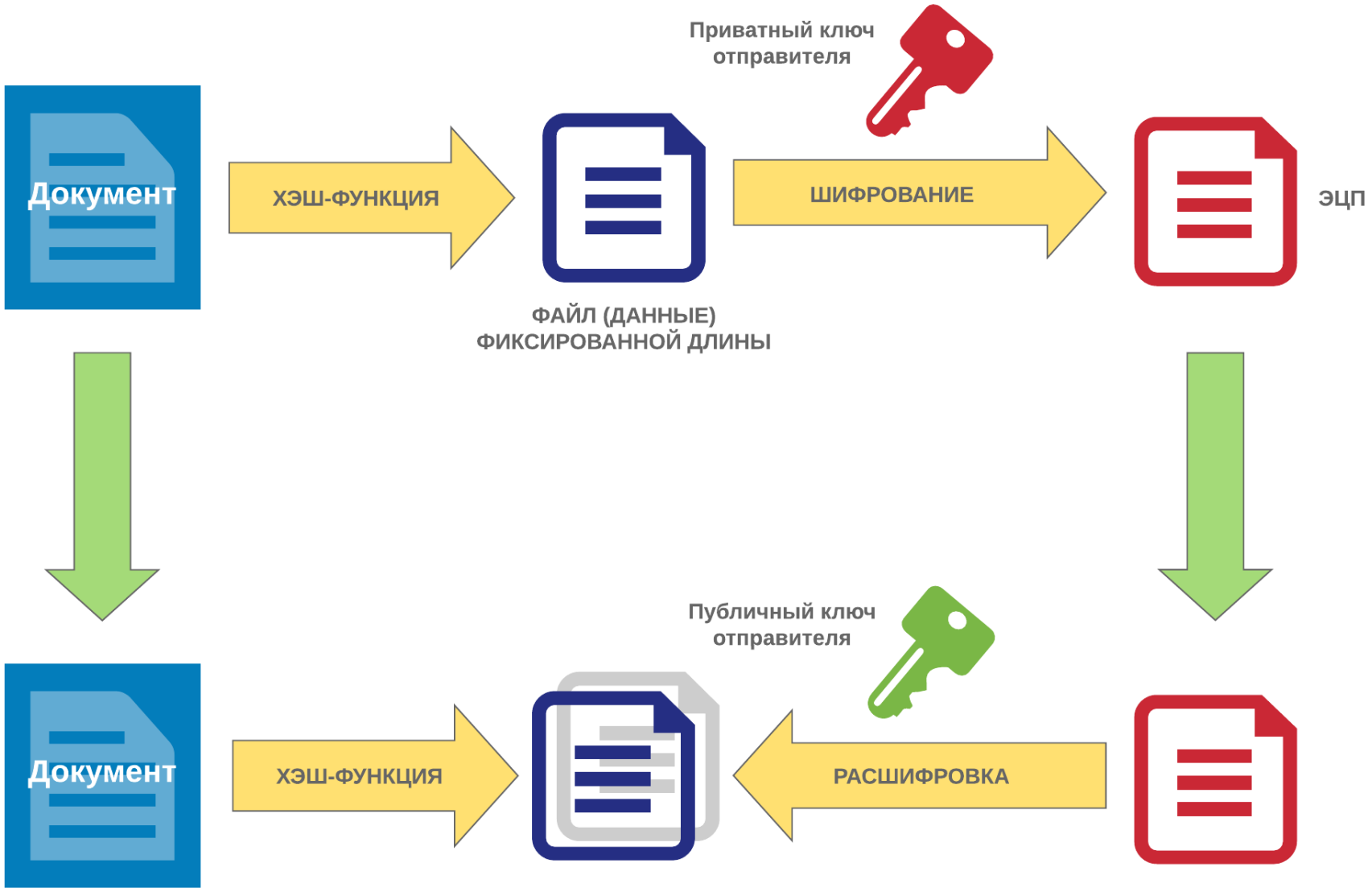
Криптографические методы позволяют

- надежно контролировать целостность данных
- определять подлинность источника данных
- гарантировать невозможность отказаться от совершенных действий

В основе криптографического контроля целостности лежат два понятия:

- хэш-функция
- электронная цифровая подпись (ЭЦП)

Электронная цифровая подпись



Хэш-функция

MD5, SHA-1, SHA-2, Whirlpool, ГОСТ Р 34.11-2012 (Стрибог)

- **От топота копыт пыль по полю летит**
  70DB02FC4A6341322A7FAD83B8DE6FBA
- **От топота копыт пыль по полю летит.**
  A1D32FC54324CE39C26D28DEA40DEAE0

Приложения для шифрования данных

Свободные

- **GnuPG**
- OpenSSL
- **VeraCrypt** (TrueCrypt)
- EncFS
- dm-crypt/LUKS (Linux)

Коммерческие

- PGP
- BestCrypt
- BitLocker (Windows)
- FileVault (Mas OS)

Экранирование

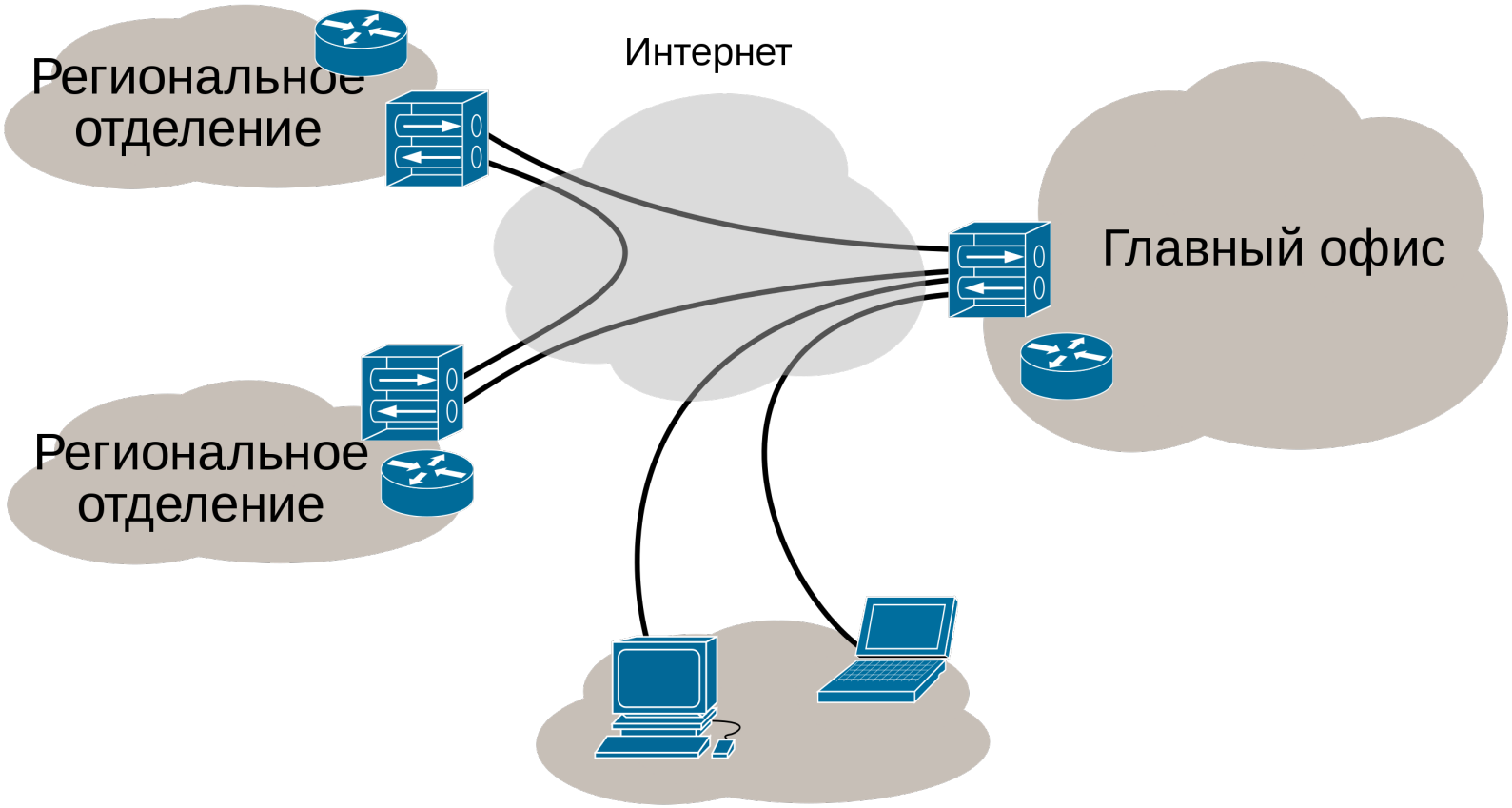
- Экран – это средство разграничения доступа клиентов из одного множества к серверам из другого множества
- Экран осуществляет свои функции, контролируя все информационные потоки между двумя множествами систем

VPN

- **Virtual Private Network** — виртуальная частная сеть — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет)
- Уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии

Сценарии применения

VPN в интернете



https://upload.wikimedia.org

Анализ защищенности

- Сервис анализа защищенности предназначен для выявления уязвимых мест с целью их оперативной ликвидации
- Сервис позволяет выявить ”оперативные”бреши, появившиеся в результате ошибок администрирования или из-за невнимания к обновлению версий программного обеспечения

Список использованных источников

- Артемов А. В. Информационная безопасность: курс лекций.
- Андрианов В. В. Обеспечение информационной безопасности бизнеса 2-е издание, переработанное и дополненное
- http://uskov.info/lektsii-po-informatsionnoj-bezopasnosti/
- http://www.redov.ru/kompyutery_i_internet/it_servis_menedzhment_vvedenie/p17.php
- http://securitypolicy.ru/шаблоны/концепция_обеспечения_иб
- https://fstec.ru/en/component/attachments/download/293