Белорусско-Российский университет
Кафедра «Программное обеспечение информационных технологий»

Защита информации

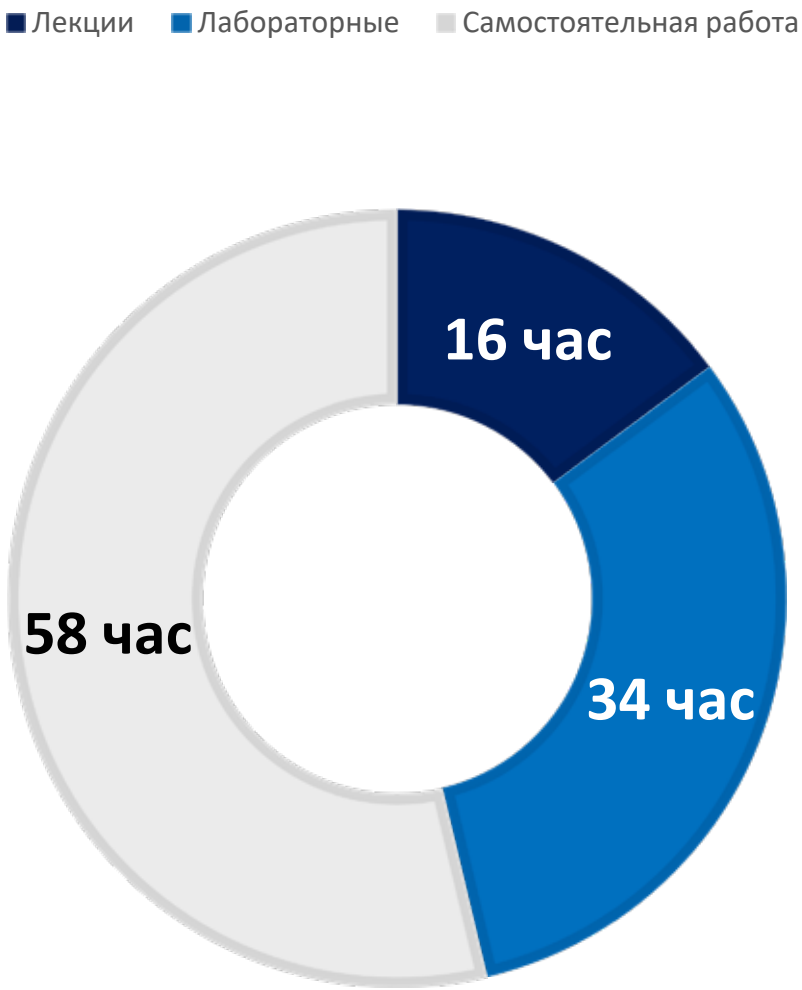
Основы информационной безопасности, методов и средств защиты информации

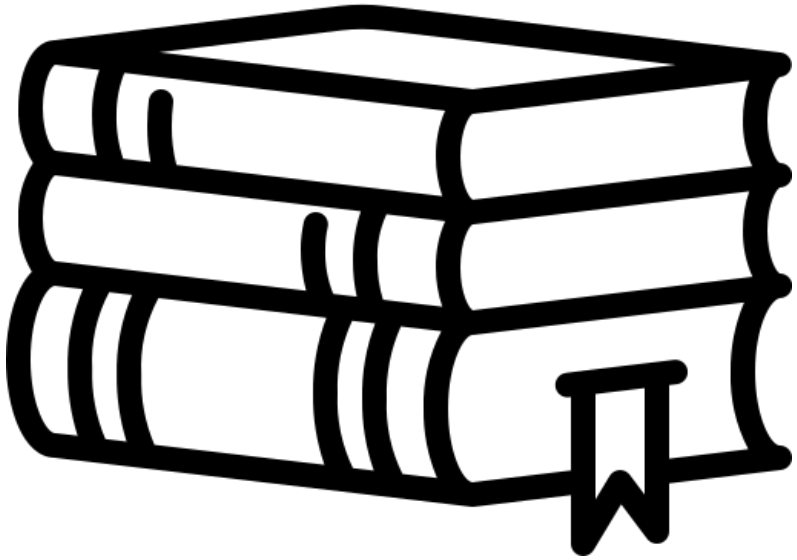
КУТУЗОВ Виктор Владимирович

Республика Беларусь, Могилев, 2024

Защита информации

Курс	**3**
Семестр	**6**
Лекции, часы	**16**
Лабораторные работы, часы	**34**
Экзамен, семестр	**6**
Самостоятельная работа, часы	**58**
Всего часов / зачетных единиц	**108/3**





Рекомендуемая литература

Рекомендуемая литература

Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с.

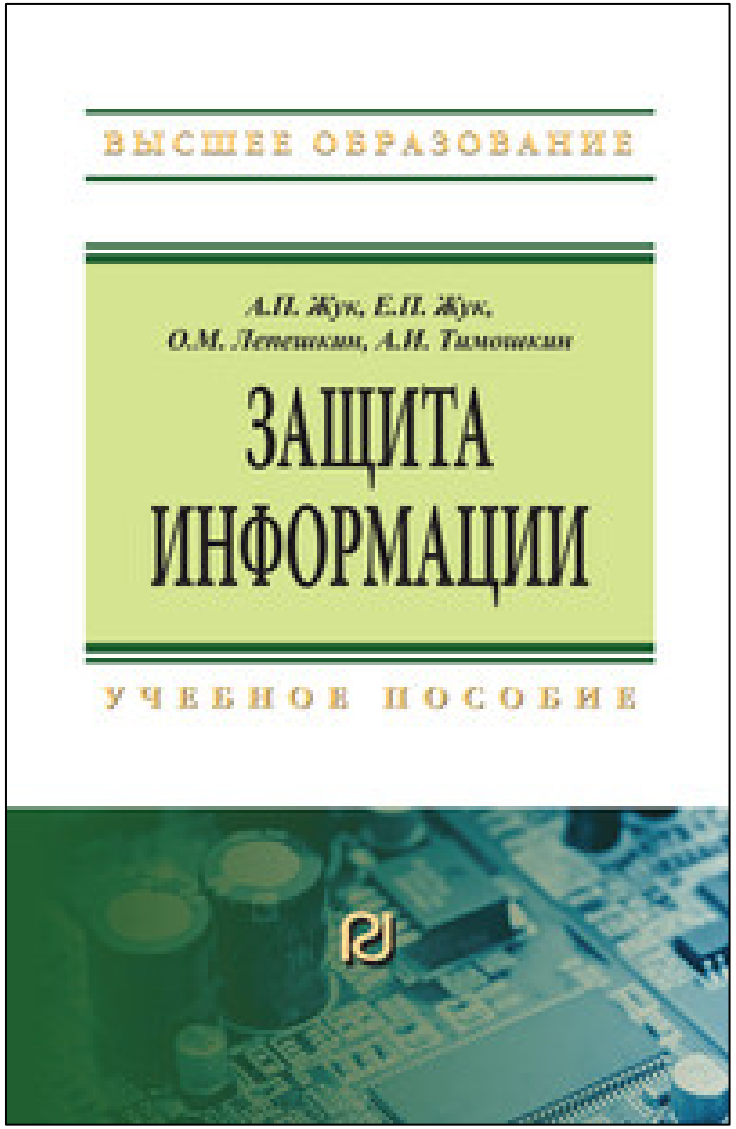
https://urait.ru/bcode/537247

Рекомендуемая литература

Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2024. — 309 с.

https://urait.ru/bcode/537000

Рекомендуемая литература



Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2023. — 400 с.

https://znanium.com/catalog/product/1912992

znanium
электронно-библиотечная система

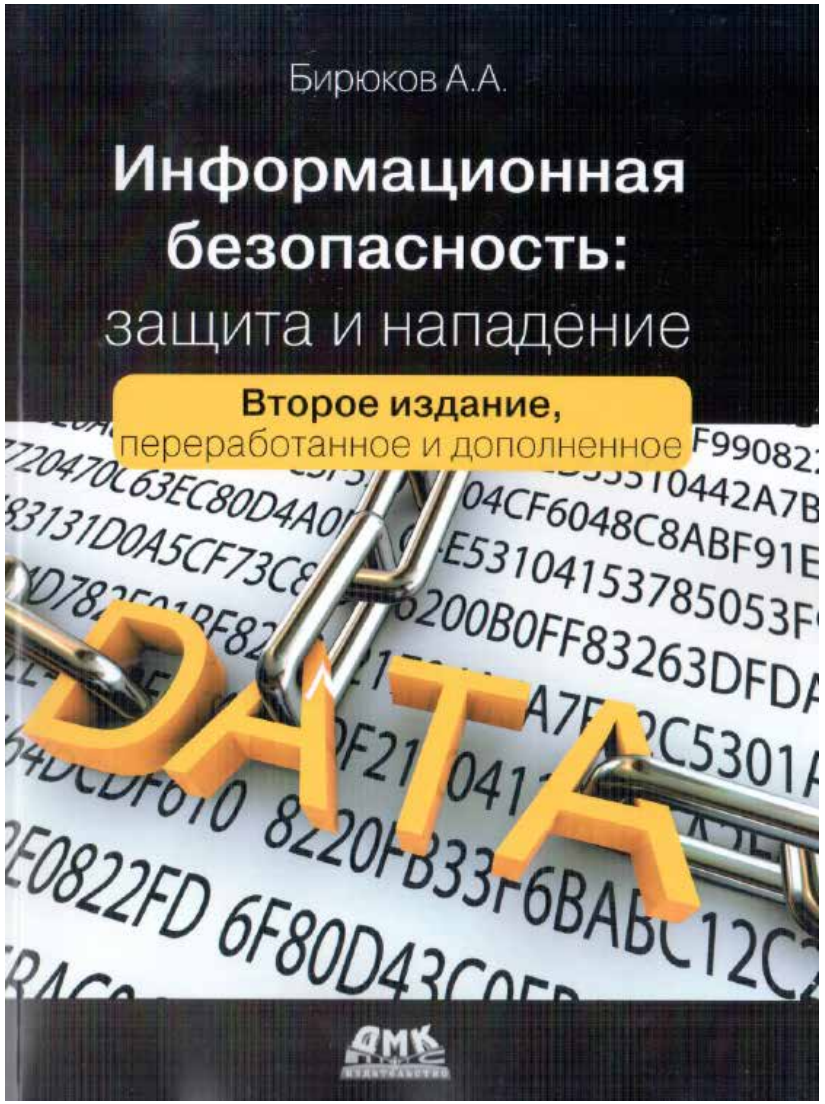
Рекомендуемая литература по теме

Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2022. — 336 с.

https://znanium.ru/catalog/product/1861657

znanium
электронно-библиотечная система

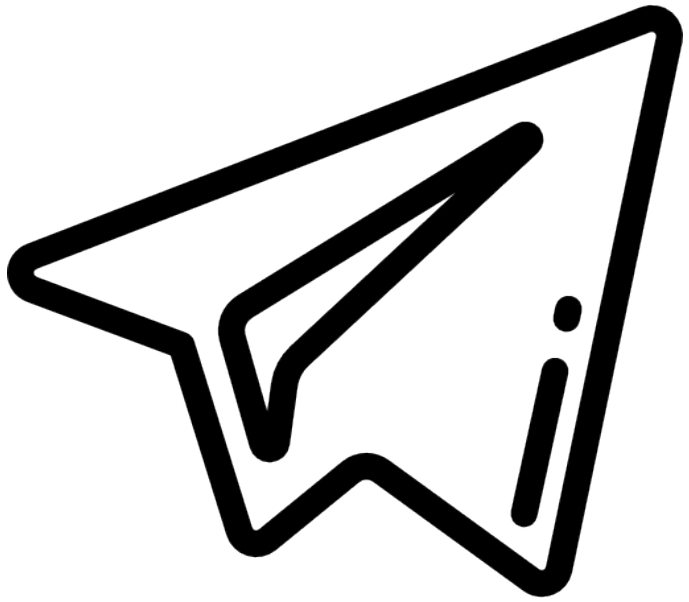
Рекомендуемая литература



Бирюков А. А.

Информационная безопасность: защита и нападение. - Москва: ДМК Пресс, 2017. - 434 с.: ISBN 978-5-97060-435-9

https://nnmclub.to/forum/viewtopic.php?t=1114555



Дополнительные источники информации по теме

Telegram каналы

Telegram **каналы**

https://t.me/SecLabNews

Новости ведущего портала по информационной безопасности SecurityLab.ru

https://t.me/alukatsky

Канал Алексея Лукацкого – специалиста по Информационной Безопасности (ИБ) с большим количеством авторских материалов и репостов по ИБ

https://t.me/dataleak

Утечки информации. Информация по утечкам информации и мониторингу даркнета.

https://t.me/news_infosecurity

ИБшнику. Площадка актуальных новостей и событий в сфере информационной безопасности.

Telegram **каналы**

https://t.me/forensictools

Investigation & Forensic TOOLS Инструментарий для проведения расследований, криминалистических исследований, корпоративной разведки, и исследований в области безопасности.

https://t.me/freedomf0x

Авторский канал Паши Ситникова - этического хакера, специалиста по ИБ и osint. Статьи, уникальные советы, книги, курсы.

https://t.me/tomhunter

T.Hunter - канал повещен информационной безопасности и пентесту. Будь в курсе всех последних новостей мира ИБ.

https://t.me/coursmax

Max Open Source - полезные статьи и бесплатные курсы по пентесту и информационным технологиям, программированию и IT.

Telegram **каналы**

https://t.me/searchinform

SearchInform. Информационная безопасность как она есть. Новости и тенденции отрасли. Разбор инцидентов. Практика, экспертный опыт и реальные кейсы.

https://t.me/true_secator

Secator. Канал делает обзоры на хакерские группировки, пишет про участившиеся в этом году атаки вирусов-вымогателей

https://t.me/irozysk

Интернет-Розыск. Шерлоки Холмсы цифровой эпохи

https://t.me/Social_engineering

Social Engineering. Делаем уникальные знания доступными

Telegram **каналы**

https://t.me/ShizoPrivacy

0% Privacy – канал посвящен анонимности, osint и информационной безопасности, будь в курсе последних трендов и самых свежих уязвимостей.

https://t.me/tmgroupsecurity

Нетипичный Безопасник – авторский канал специалиста по ИБ и osint, Мефодия Келевра, отборные статьи, уникальная информация, советы.

https://t.me/DigitalIntelligence

Digital-Разведка – Главный агрегатор инноваций, интересных решений и инструментов по OSINT и близким наукам.

https://t.me/it_mega_g

IT MEGA – тут эксклюзивные материалы, курсы по программированию, ИБ "хакингу", osint и IT.

Telegram **каналы**

https://t.me/Blackat_tg

Blackat – канал об IT-технологиях, osint и ИБ.

https://t.me/CyberScoutszametki

Заметки CyberScout'a – канал, обозревающий тематику применения OSINT (и не только) в сфере противодействия киберпреступности и иных разведывательных мероприятий.

https://t.me/GDPRru

Privacy GDPR Russia. Privacy news with Russian soul. Let's share the news and opinions.

https://t.me/zer0daylab

Zer0Day Lab. Information must be flow free, money kill it

Telegram **каналы**

https://t.me/cyberyozh_official

CyberYozh – Создаем лучший бесплатный курс по анонимности и безопасности в сети.

https://t.me/KladovkaPavlu

Кладовка Pavlu – Полезные сайты и сервисы. Безопасные мессенджеры. Опенсорсный софт, .onion сайты. Телеграм боты и каналы.
Все для анонимности в сети.

https://t.me/academy_nsb

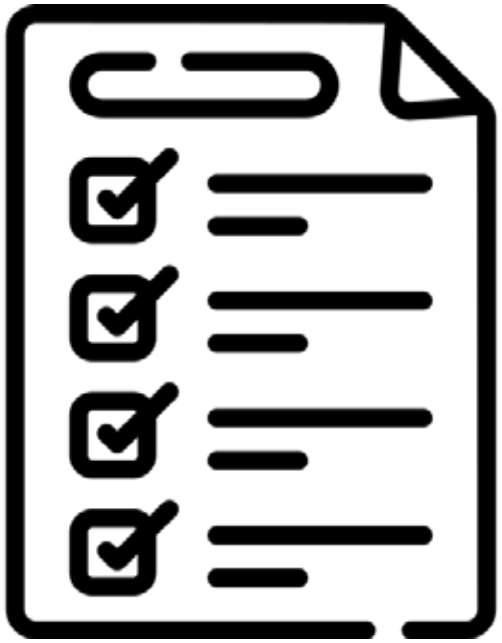
Академия НСБ – Учимся вместе, учимся у профессионалов Негосударственной сферы безопасности

https://t.me/positive_investing

IT's positive investing – В этом канале рассказываем об инвестициях в кибербезопасность

Каталог Telegram-каналов и чатов

Безопасность в Сети	• https://tgstat.ru/tag/it-security
Информационная безопасность	• https://tgstat.ru/tag/cyber_security
Аналитика и исследования	• https://tgstat.ru/tag/analytics
Даркнет	• https://tgstat.ru/darknet



Важные вопросы

Вопросы на которые нужен ответит

1. В какое время мы живем и что сейчас происходит?
2. Что такое информационная безопасность, защита информации?
3. Зачем нужно защищать информацию?
4. От КОГО нужно защищать информацию?
5. От ЧЕГО нужно защищать информацию?
6. Как надо защищаться?
7. Как надо защищаться?
8. Что происходит если мы не занимаемся вопросами информационной безопасности и защиты информации?
9. Как оценить эффективность защиты?

Вопросы на которые нужен ответит

10. Во что обойдется разработка, внедрение, эксплуатация, сопровождение и развитие систем защиты?
11. Кто все это должен делать?
12. Какие требования к специалистам по информационной безопасности настоящее время и каков рынок вакансий в данной сфере?
13. Какие требования к специалистам по информационной безопасности настоящее время?
14. Каков рынок вакансий в сфере информационной безопасности?

В какое время мы живем и что сейчас происходит?

Мы живем в быстроизменяющуюся эпоху, в информационном обществе, где информация стала «нефтью 21 века»

Этапы цифрового развития

1

Компьютеризация – деятельность, предусматривающая оснащение компьютерным оборудованием

2

Автоматизация – внедрение ИТ-решений, повторяющих имеющиеся процессы

3

Информатизация – процесс формирования и использования информационных ресурсов и реализации информационных отношений

4

Цифровизация – улучшение существующих процессов путем внедрения ИТ, реинжиниринг процессов, анализ данных для принятия решений

5

Цифровая трансформация – использование цифровых технологий и данных для обеспечения конкурентоспособности компаний путем изменения стратегии развития, корпоративной культуры, организационной структуры, бизнес моделей, взаимодействия с потребителями, требований к персоналу

Цифровое развитие – процесс последовательной цифровой трансформации экономической деятельности и государственного управления

Цифровая трансформация— процесс внедрения организацией цифровых технологий, сопровождаемый оптимизацией системы управления основными технологическими процессами.

Цифровая трансформация призвана ускорить продажи и рост бизнеса или увеличить эффективность деятельности организаций и т.д.

Цифровая трансформация

Индустрия 4.0

Индустрия 4.0

Адаптация автоматизированных функций к изменениям внешних условий

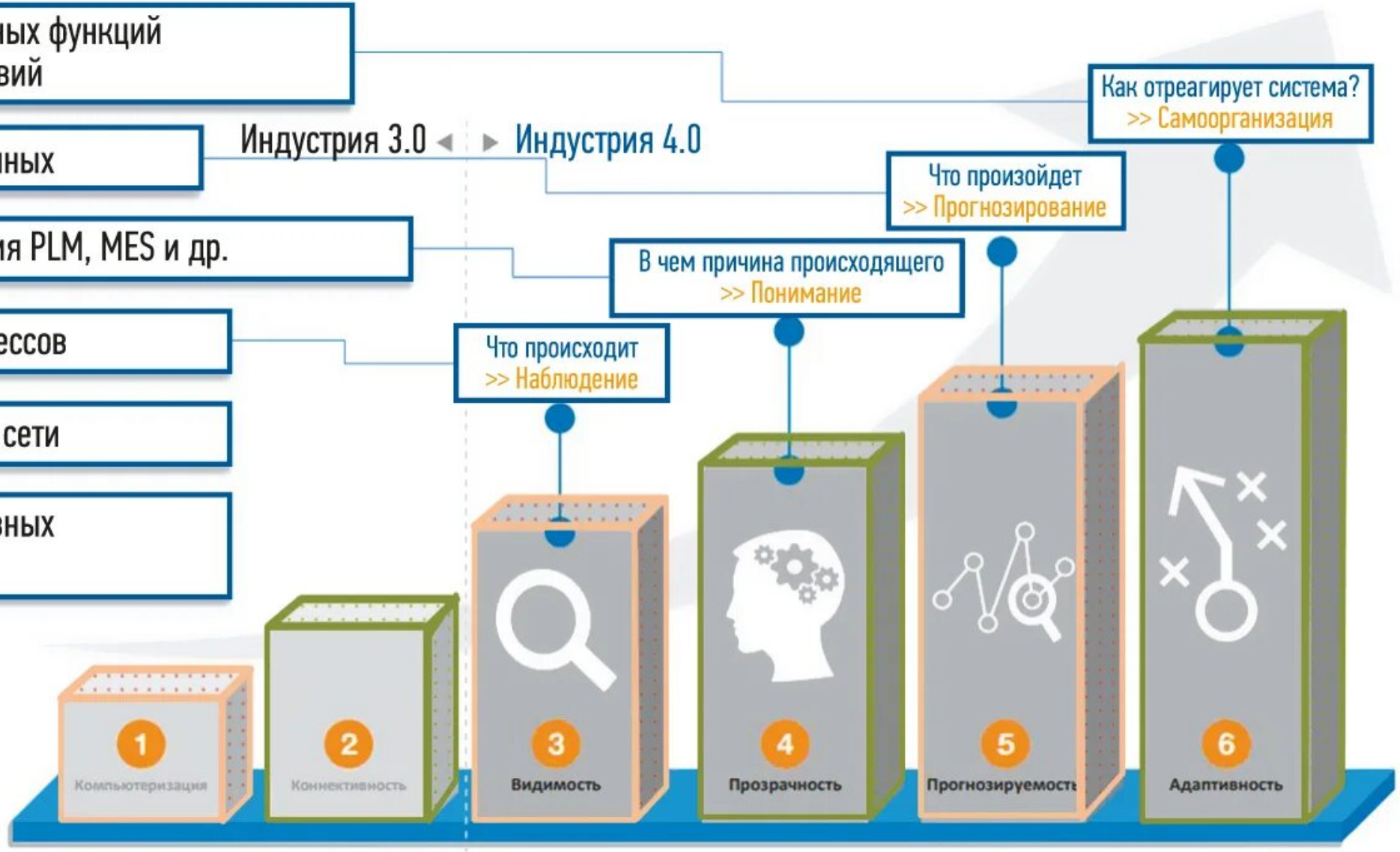
Предиктивная аналитика данных

Анализ в системах управления PLM, MES и др.

Цифровое отображение процессов

Объединение компонентов в сети

Компьютеризация всех основных компонентов производства



Пример цифровой трансформации (такси)

РУЧНОЕ УПРАВЛЕНИЕ
Поиск решения: Человек. **Исполнение решения:** Человек

НУЛЕВОЙ ЭТАП ЦИФРОВОЙ ТРАНСФОРМАЦИИ
ПРОЙДЕН.

0

АВТОМАТИЗАЦИЯ
Поиск решения: Система+человек. **Исполнение решения:** Человек

ПЕРВЫЙ ЭТАП ЦИФРОВОЙ ТРАНСФОРМАЦИИ 2019–2023 гг.
Внедрение действующих технологий, формирующих аппаратную и информационную основу для дальнейшего развития. Частичная цифровизация производственных процессов. Пилотирование перспективных технологий. Акцент на развитие мобильных решений.

1

ЦИФРОВИЗАЦИЯ – НАЧАЛЬНЫЙ ЭТАП
Поиск решения: Система. **Исполнение решения:** Человек

ВТОРОЙ ЭТАП ЦИФРОВОЙ ТРАНСФОРМАЦИИ 2023–2026 гг.
Формирование единой ИТ-платформы, единого источника данных путем интеграции существующих баз данных. Внедрение технологий, показавших эффективность в рамках пилотирования. Продолжение внедрения технологий первого уровня.

2

ПОЛНАЯ ЦИФРОВАЯ ТРАНСФОРМАЦИЯ
Поиск решения: Система. **Исполнение решения:** Система

ТРЕТИЙ УРОВЕНЬ ЦИФРОВОЙ ТРАНСФОРМАЦИИ 2026–2030 гг.
Внедрение технологий работы с Большими данными и технологий машинного обучения. Внедрение технологий, показывающих эффективность в рамках пилотирования. Завершение внедрения технологий второго уровня.

3

Цифровое общество

Цифровая экономика

Цифровая экономика

Цифровая экономика

— это новая парадигма **экономического развития** на основе **обмена данными** в режиме реального времени при помощи

цифровых технологий

институтов

нормативно-правовой базы

навыков

бизнеса

для ускорения **экономического роста** и **производительности труда,** улучшения **качества жизни** и **инвестиционного климата**.

Большие данные (Big Data)

Яндекс

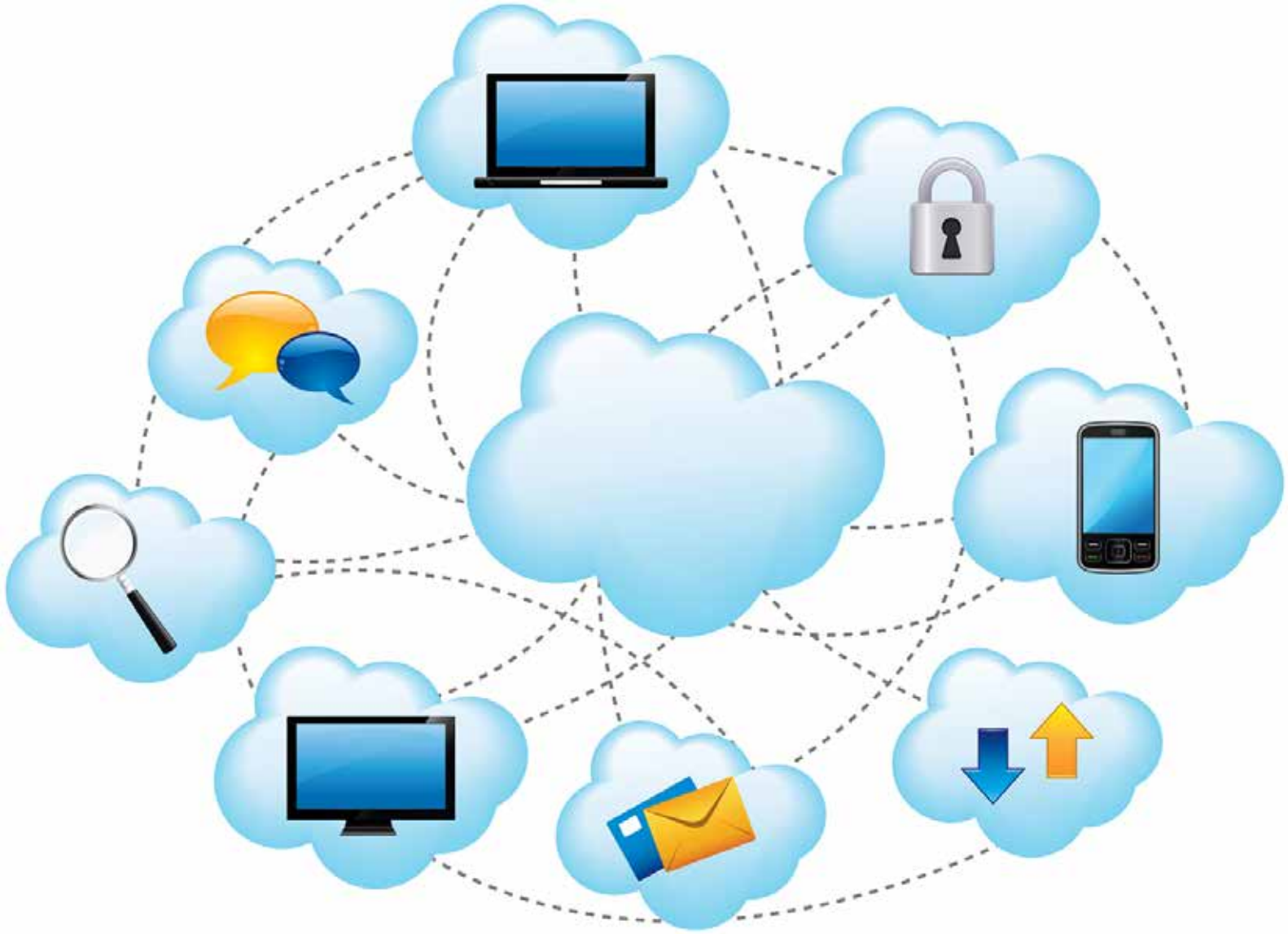
Google

NETFLIX

Сбербанк

YouTube

Облачные технологии

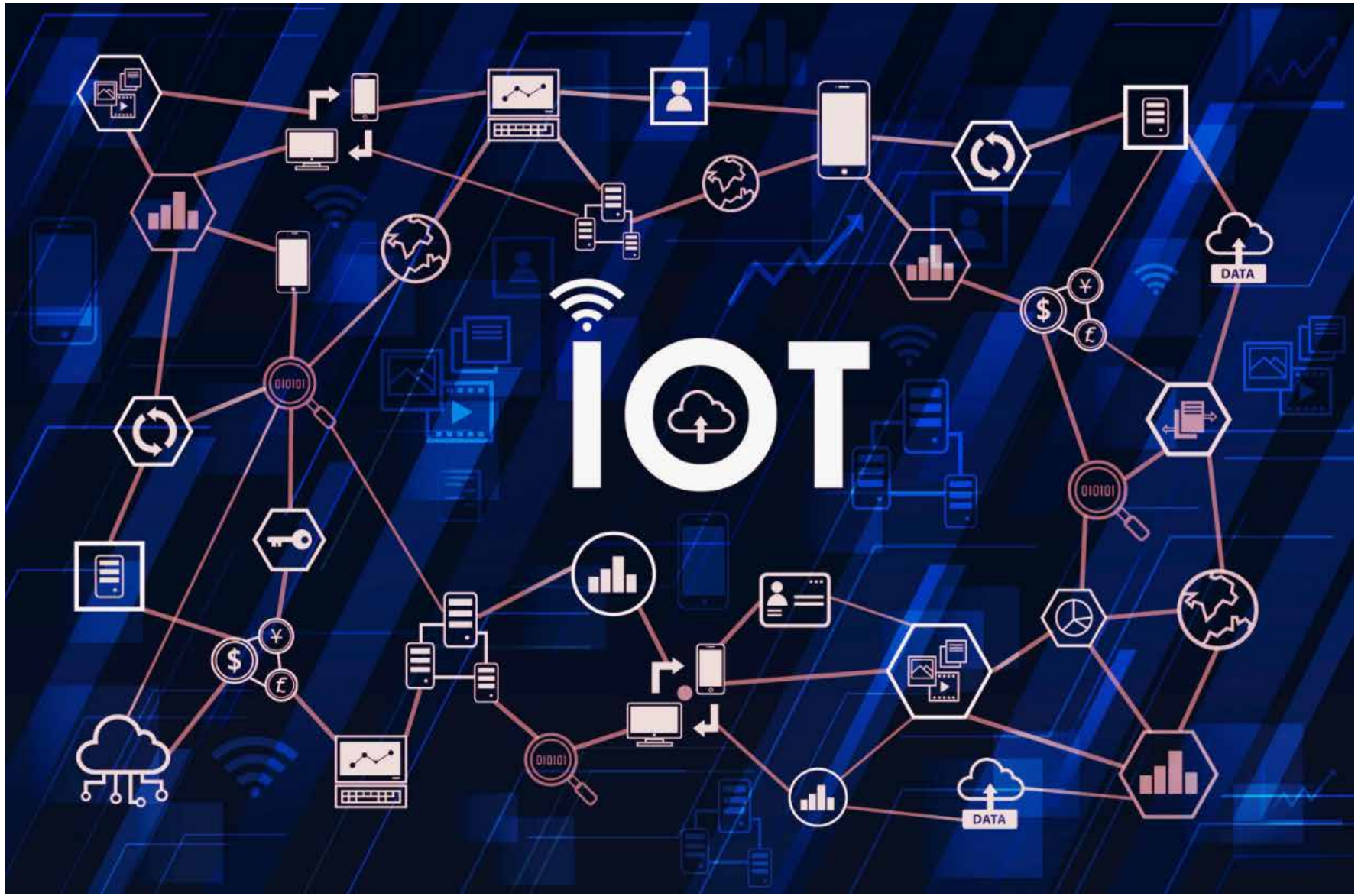


Яндекс

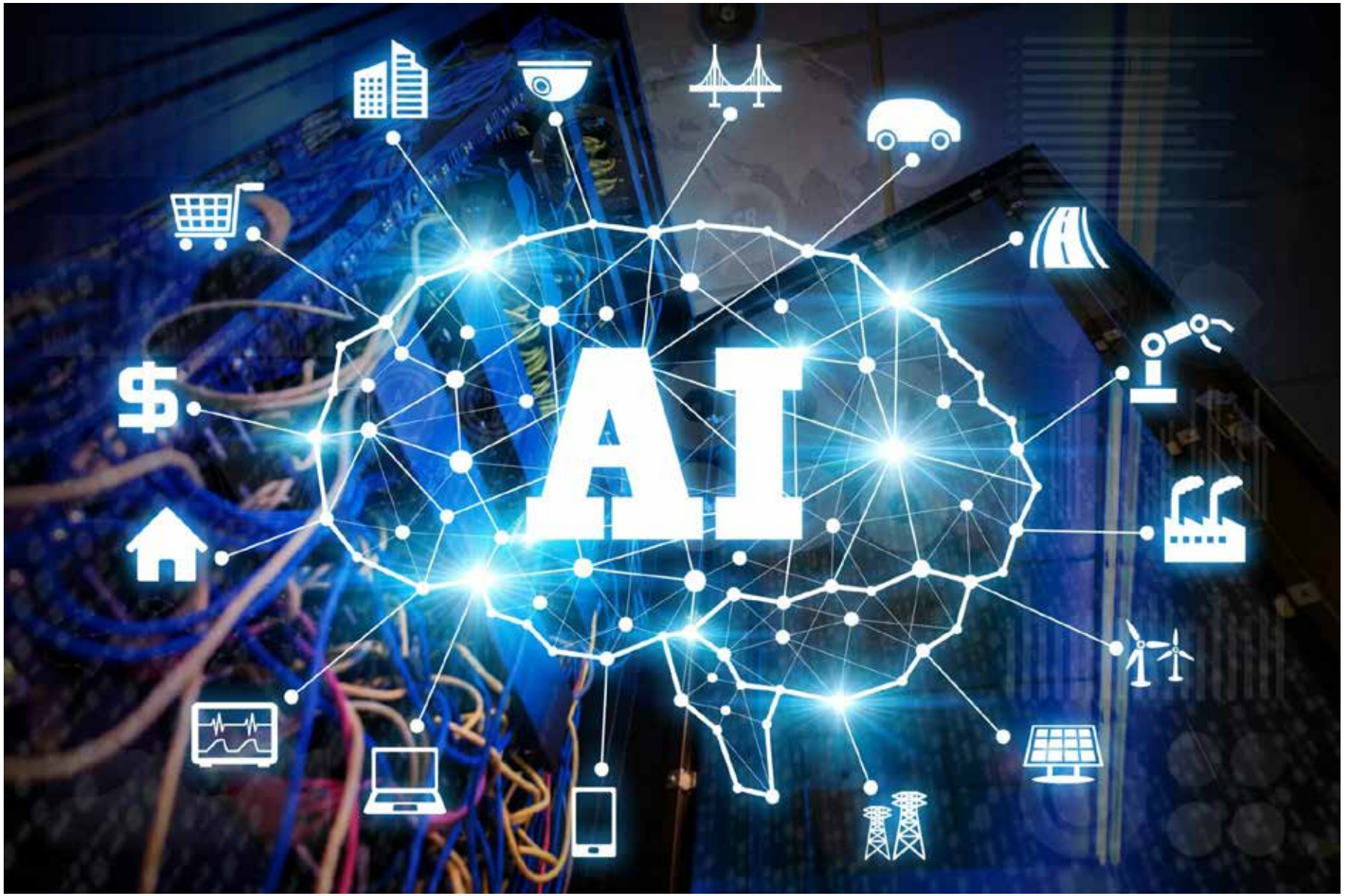
Google

amazon

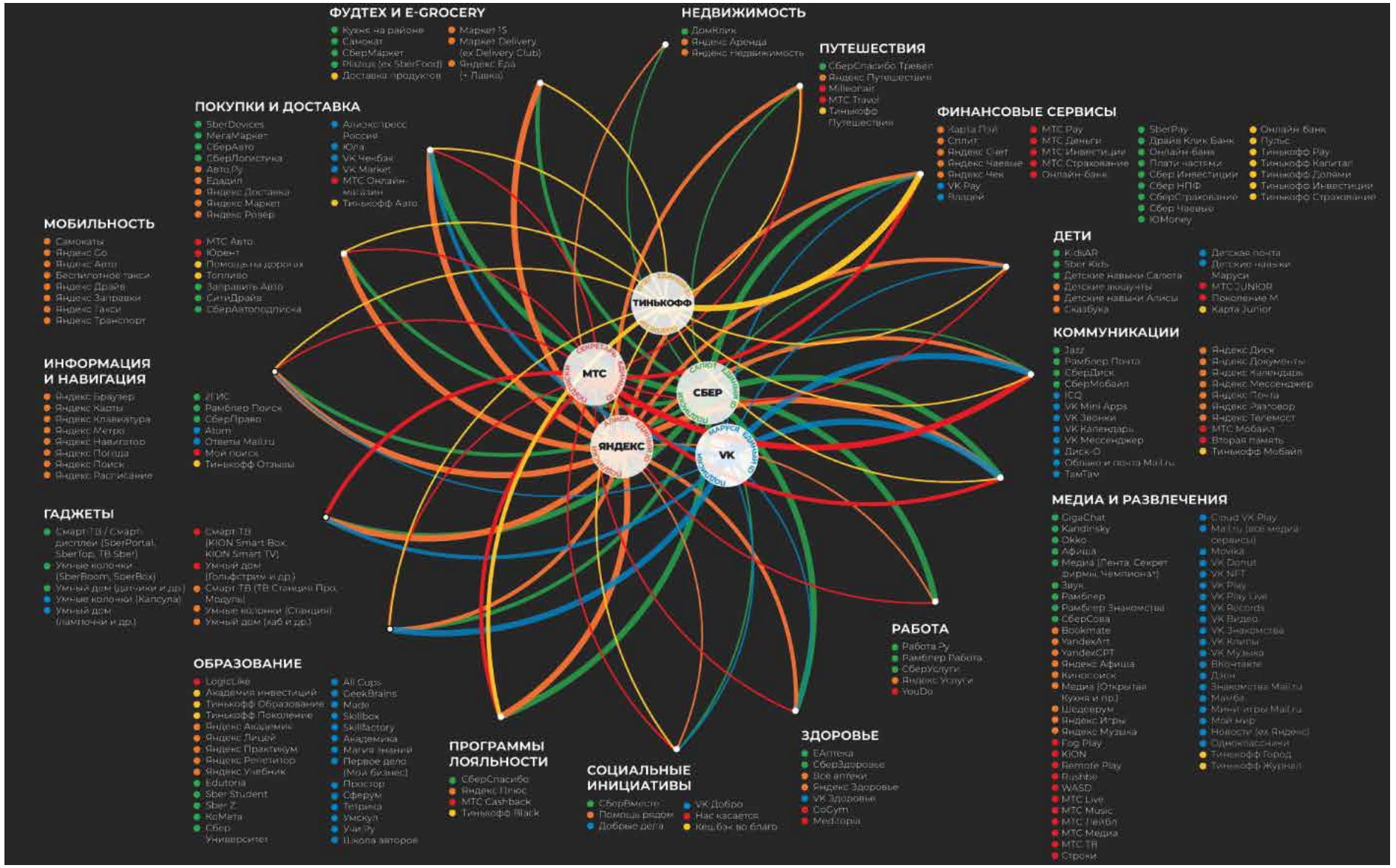
IoT **Интернет вещей**



Искусственный интеллект

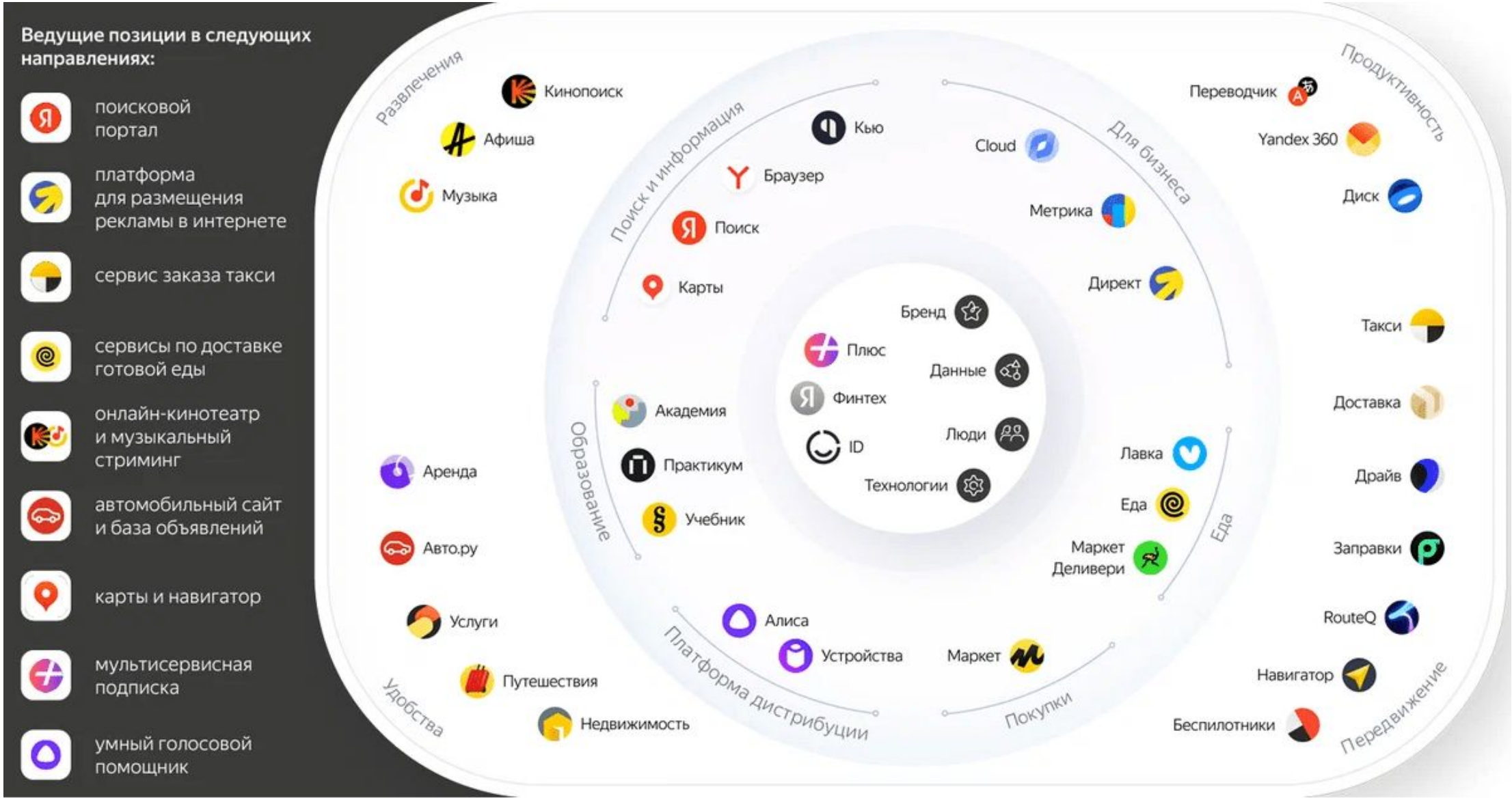


Экосистемы



Крупнейшие Российские экосистемы 2023-2024 https://assets-global.website-files.com/654b88d46d88c15f2b58ee8f/658aa80edd7c62ee2cc11fcc_Spektr%20Экосистемы%202023-2024.pdf

Пример: экосистема Яндекса



Экосистемы

СБЕР

Самый сфокусированный на AI-технологиях

Сбер — одна из самых масштабных экосистем, которая активно развивается и запускает новые сервисы

Одним из первых попал под санкции — они ограничили его потенциал, вынудив отказаться от ряда проектов (например, SberGames или банков в Европе). Но быстро адаптировался, усилив фокус на развитии технологий

Самый сфокусированный на медиа

VK входит в топ-3 экосистем по охвату и присутствию в вертикалях — вместе со Сбером и Яндексом

У экосистемы VK появился четкий медийный фокус (как и у тандемной экосистемы Газпромбанка) — она отказалась от мобильности, фудтеха и даже экосистемной подписки

Самый активный на новых рынках

Яндекс — один из экосистем-лидеров с фокусом на цифровых технологиях

Не попал под прямые санкции, но был вынужден уйти из новостного и USG-сегмента. Активнее других адаптирует свои технологии (райдшеринг, доставка) на внешних рынках

МТС

Самый активный претендент на лидерство

МТС пока уступает экосистемным лидерам по охвату аудитории и разнообразию сервисов

Однако, будучи мало затронут санкциями, активно развивается, выходит в новые вертикали и усиливает конкуренцию с лидерами — например, в медиа и путешествиях

ТИНЬКОФФ

Самый сфокусированный на супераппе

Тинькофф также уступает лидерам по масштабу экосистемы, хотя постепенно расширяет ее (например, в вертикали образования)

Фокусируется на развитии базовой вертикали (финансы) и создании супераппа по примеру WeChat

Крупнейшие Российские экосистемы 2023-2024 https://assets-global.website-files.com/654b88d46d88c15f2b58ee8f/658aa80edd7c62ee2cc11fcc_Spektr%20Экосистемы%202023-2024.pdf

Экспоненциально развивающиеся технологии

Искусственный интеллект

Машинное обучение

Предсказательная аналитика

Интернет вещей

Высокопроизводительные вычислительные системы

Цифровые двойники

Большие данные

Роботизация

Секвенирование генома


10101
01001
11010
10101
01001
11010

Безопасность

Безопасность в цифровом пространстве становится важнейшим вопросом, требующим постоянного внимания и анализа.

С ростом числа цифровых технологий также возрастает и уровень угроз информационной безопасности, с которыми сталкиваются организации и частные лица.

Безопасность

Что такое информационная безопасность, защита информации?

Защита информации (ЗИ)

- **Защита информации** – комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации;

  Концепция информационной безопасности РБ. Постановление Совета Безопасности РБ 18.03.2019 № 1

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

- **Защита информации** – комплекс мероприятий, направленных на обеспечение важнейших аспектов информационной безопасности (целостность, доступность и, если нужно, конфиденциальность информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных).

Информационная безопасность (ИБ)

- **Информационная безопасность** – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере.

  Концепция национальной безопасности РБ, утвержденная Указом Президента РБ от 9 ноября 2010 г. № 575

- **Информационная безопасность** – это набор методик и практик по защите информации от внешних и внутренних воздействий на объекте информатизации.

- **Информационная безопасность** – состояние сохранности информационных ресурсов и защищённости законных прав личности и общества в информационной сфере.

Информация

- **Информация** – это сведения (сообщения, данные) независимо от формы их представления.

- **Информация** может существовать в виде бумажного (электронного) документа, физических полей и сигналов (электромагнитных, акустических, тепловых и т.д.), биологических полей (память человека) и в других видах.

- **Информация (в области обработки информации)** – любые данные, представленные в электронной форме, написанные на бумаге, высказанные на совещании или находящиеся на любом другом носителе, используемые финансовым учреждением для принятия решений, перемещения денежных средств, установления ставок, предоставления ссуд, обработки операций и т.п., включая компоненты программного обеспечения системы обработки.

  стандарт ISO/IEC 2382:2015 «Информационные технологии»

Данные

- **Данные** – это записанная (зафиксированная) информация.

- **Данные** – поддающееся многократной интерпретации представление информации в формализованном виде, пригодном для передачи, связи, или обработки (по ISO/IEC 2382-1:1993).

- **Данные** – информация, фиксированная в определенной форме, пригодной для последующей обработки, хранения и передачи.

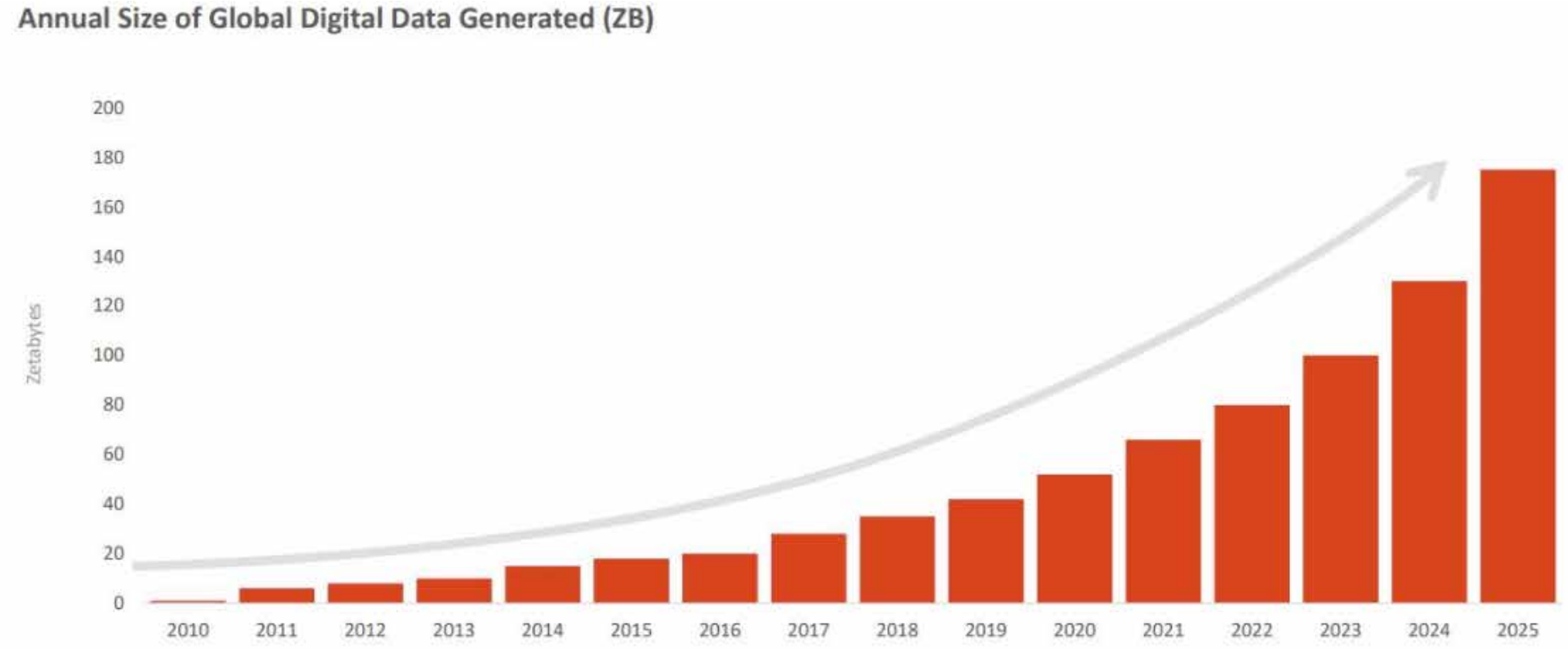
Информация и данные

Информация = данные + смысл

- **Информация не является статичным объектом** – она динамически меняется и существует только в момент взаимодействия данных и методов.
- Информация существует только в момент протекания информационного процесса.
- **Все остальное время информация содержится в виде данных.**

- **В компьютерах все данные хранятся в виде файлов**

Объём генерируемых цифровых данных в мире

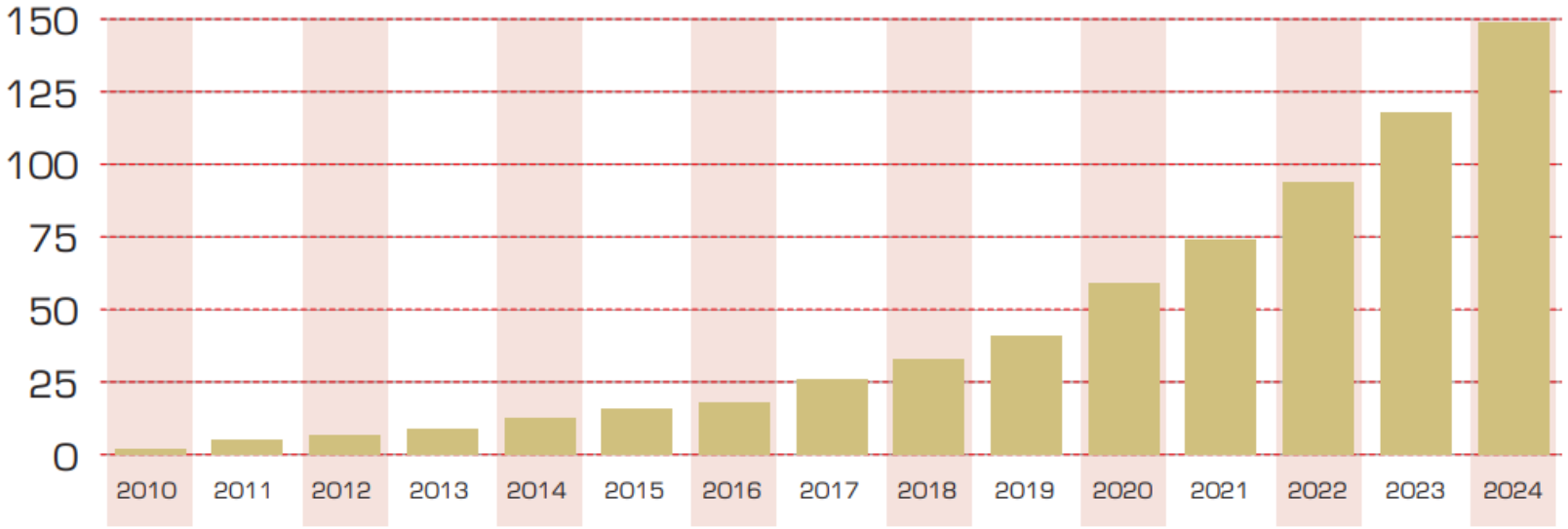


- **В 2020 году в мире было создано 64,2 зеттабайт данных**, однако к 2021 году было сохранено менее 2% новых данных, то есть большая часть из них была временно создана или реплицирована для использования, а затем удалена или перезаписана новыми данными. Об этом свидетельствуют результаты исследования IDC.

Поток данных в глобальном Интернете

Источник: UNCTAD Digital economy report 2019

Рост протокола данных в глобальном Интернете, единица измерения – один зитабайт – 1 000 000 000 000 000 000 000 байт информации. Вы используете 10 байт данных в одном напечатанном слове



Безопасность информации (данных)

- **Безопасность информации (данных)** – состояние защищенности информации (данных), при котором обеспечиваются ее (их) конфиденциальность, доступность и целостность.

- **Безопасность информации (данных)** определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые при применении информационной технологии

Зачем нужно защищать информацию?

Цели защиты информации

- Основными **целями защиты информации являются:**
  - предотвращение утечки, хищения, искажения, подделки;
  - предотвращение безопасности личности, общества, государства;
  - предотвращение несанкционированных действий по уничтожению, искажению, блокированию информации;
  - защиту конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных;
  - сохранение государственной тайны, конфиденциальности документированной информации.

Три фундаментальных свойства Информации

- **1. Конфиденциальность** - это уверенность создателя или владельца информации в том, что никто не сможет получить к ней доступ без его ведома.
  - Пример: вы написали записку вашей подруге и не хотите, чтобы с её содержанием ознакомились посторонние. В этом случае вам важна именно конфиденциальность информации.

- **2. Целостность** - это признак того, что информация не будет изменена без ведома автора.
  - Например, вы заключили с кем-то договор на 1 тысячу рублей и не хотите, чтобы в договоре появилась какая-то другая сумма. Вам важна целостность этого договора, его неизменность.

- **3. Доступность** - это свойство информации, означающее вашу уверенность в том, что вы найдете ваши данные там, где вы их оставили.
  - Например, если вы положили важный документ в ящик стола и не хотите, чтобы его кто-то брал, значит, для вас важна доступность этой информации.

- **Эти примеры отражают суть защиты информации - обеспечение конфиденциальности, целостности, доступности информации - и являются главной целью и задачей информационной безопасности.**

Ущерб

- **Средний размер ущерба** в результате одного инцидента в области информационной безопасности в 2020 году для компаний **среднего бизнеса РФ** составляет **1,6 млн**. рублей, а для **крупного бизнеса** он в десять раз выше – **16,1 млн. рублей**.

- В целом, защита информации необходима для обеспечения конфиденциальности, целостности, доступности данных, соблюдения законодательства, защиты репутации и поддержания доверия.
- Это помогает предотвратить финансовые потери, вредоносные действия, ущерб для бизнеса и нарушение прав и интересов людей.

А что именно защищать?

А что именно защищать?

- Информацию
- Данные
- Секреты
- Репутацию
- Права
- Себя
- Организацию
- и т.д.

Объекты защиты

- Различие в субъектах порождает различия в объектах защиты.
- **Основные группы объектов защиты:**
  - **информационные ресурсы всех видов** (под ресурсом понимается материальный объект: жесткий диск, иной носитель, документ с данными и реквизитами, которые помогают его идентифицировать и отнести к определенной группе субъектов);
  - **права граждан, организаций и государства на доступ к информации**, возможность получить ее в рамках закона; доступ может быть ограничен только нормативно-правовыми актами, недопустима организация любых барьеров, нарушающих права человека;
  - **система создания, использования и распространения данных** (системы и технологии, архивы, библиотеки, нормативные документы);
  - **система формирования общественного сознания** (СМИ, интернет-ресурсы, социальные институты, образовательные учреждения).

- **Каждый объект предполагает особую систему мер защиты от угроз ИБ и общественному порядку.** Обеспечение информационной безопасности в каждом случае должно базироваться на системном подходе, учитывающем специфику объекта.

Информация как товар

- В настоящее время **информация рассматривается в качестве одного из важнейших ресурсов развития общества наряду с материальными, энергетическими и людскими**. С помощью информации потребитель имеет возможность удовлетворять потребность в новых сведениях и знаниях.

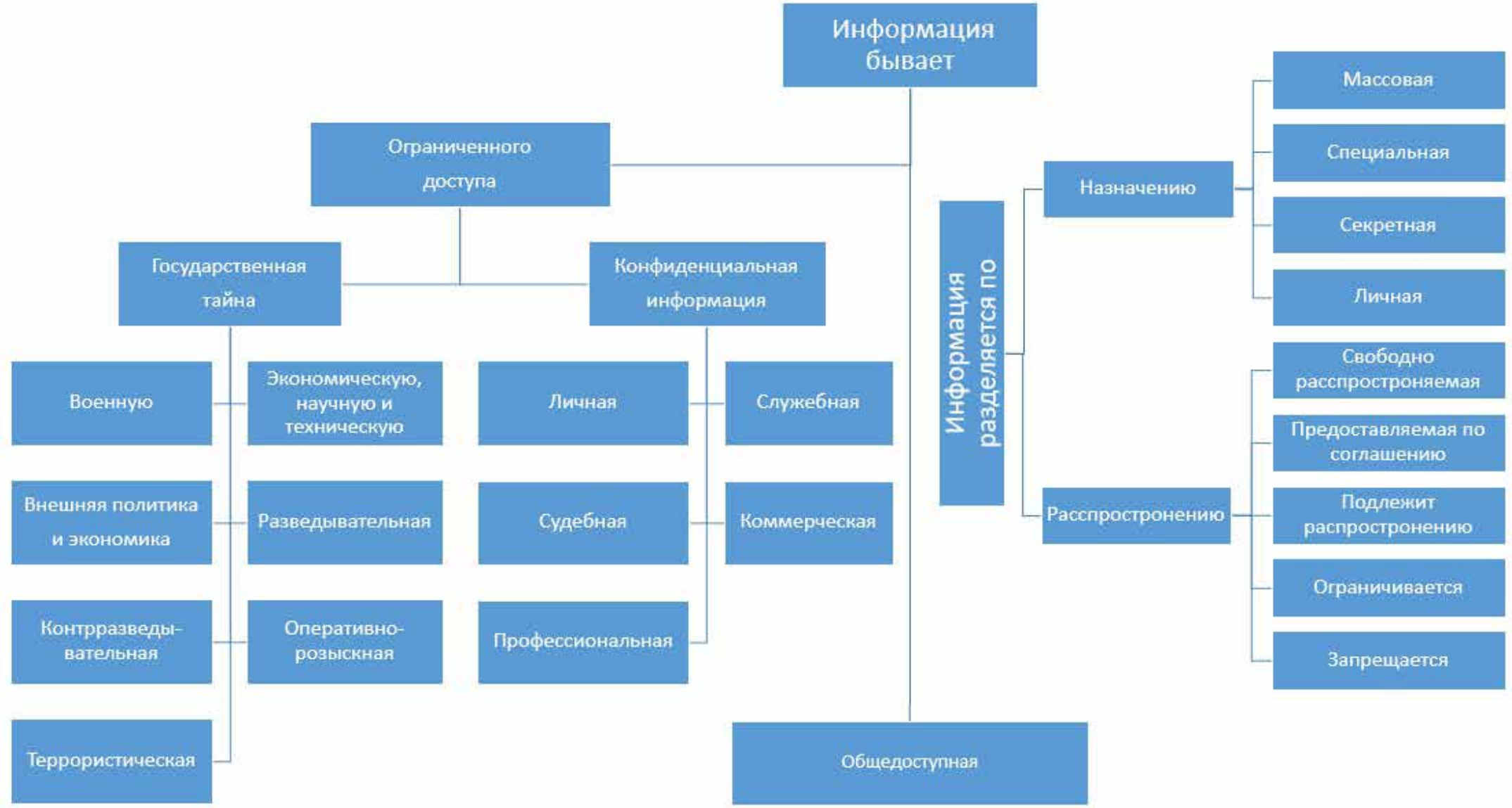
- **Информация** как вид ресурсов и фактор общественного развития **становиться особым видом продукта с присущими ему всеми свойствами товара**. Информация в качестве экономического ресурса предназначается для обмена, имеется в ограниченном количестве, при этом на нее предъявляется платежеспособный спрос. Ценность, или полезность, информации заключается в возможности дать дополнительную свободу действий потребителю

Систематизация последствий с точки зрения 6 свойств информации

Конфиденциальность	Целостность	Доступность	Подотчетность	Аутентичность	Достоверность
•Потеря общественного доверия •Снижение имиджа •Ответственность перед законом •Отрицательное влияние на политику организации •Создание угрозы безопасности персонала •Финансовые потери	•Принятие неправильных решений •Обман •Прерывание коммерческих операций •Потеря общественного доверия •Снижение имиджа •Финансовые потери •Ответственность перед законом	•Принятие неправильных решений •Неспособность выполнять важные поставленные задачи •Потеря общественного доверия •Снижение имиджа •Финансовые потери •Ответственность перед законом •Большие затраты на восстановление	•Манипулирование системой со стороны пользователей •Обман •Промышленный шпионаж •Неконтролируемые действия •Ложные обвинения •Ответственность перед законом	•Обман •Использование достоверных процессов с недостоверными данными •Манипулирование организацией извне •Промышленный шпионаж •Ложные обвинения •Ответственность перед законом	•Обман •Потеря доли рынка •Снижение мотивации в работе персонала •Ненадежные поставщики •Снижение доверия клиентов •Ответственность перед законом

ГОСТ Р ИСО/МЭК ТО 13335-4-2007 «Методы и средства обеспечения безопасности. Выбор защитных мер»

Классификация видов информации

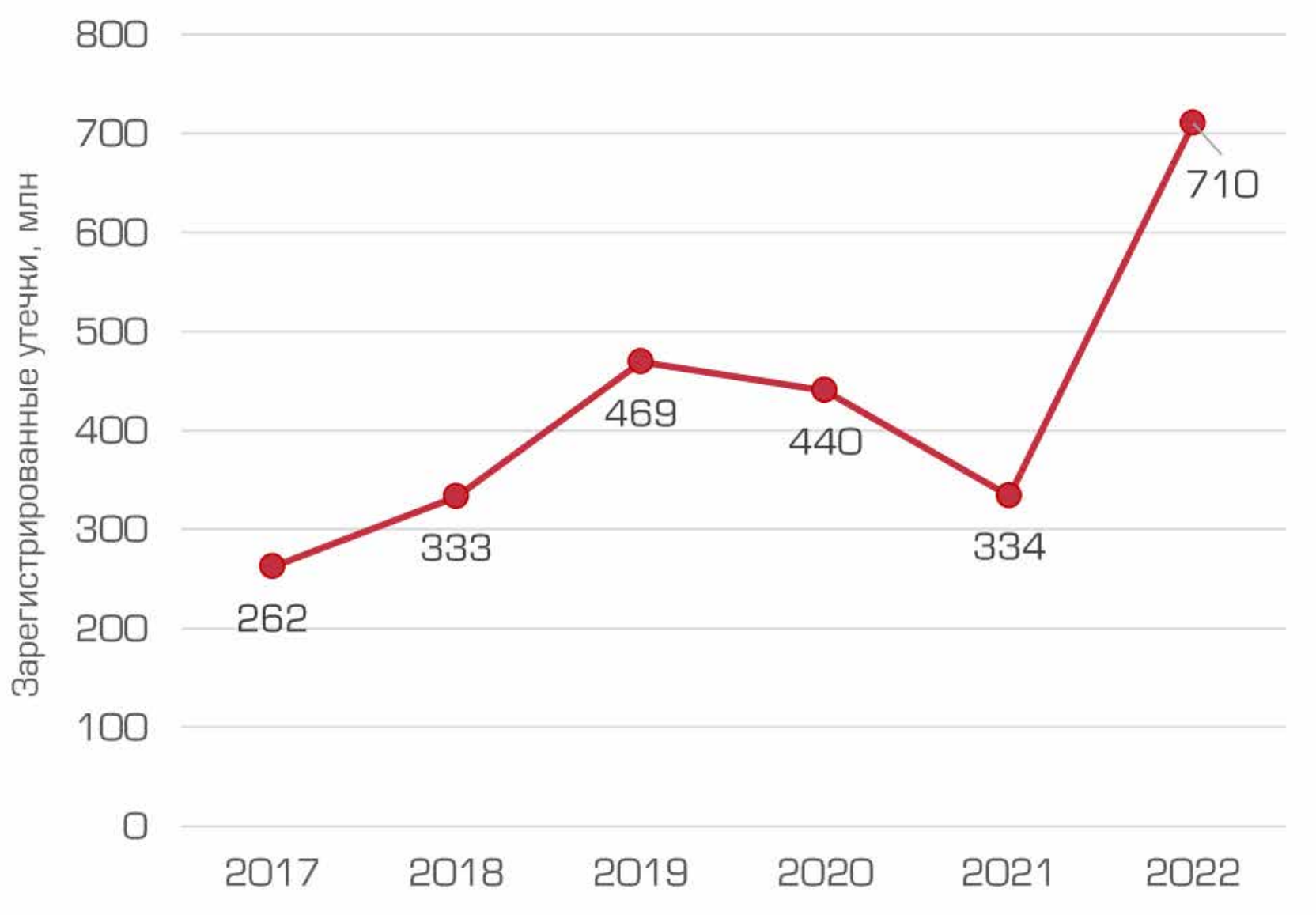


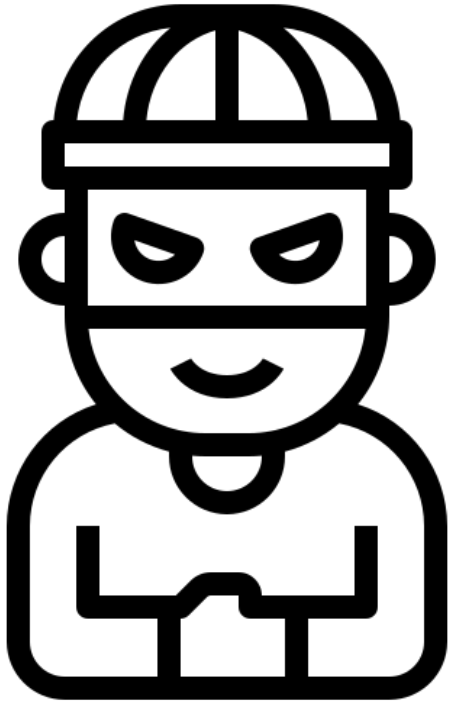
Виды информации

- Информация по назначению бывает следующих видов:
  - **Массовая** — содержит тривиальные сведения и оперирует набором понятий, понятным большей части социума.
  - **Специальная** — содержит специфический набор понятий, которые могут быть не понятны основной массе социума, но необходимы и понятны в рамках узкой социальной группы, где используется данная информация.
  - **Секретная** — доступ, к которой предоставляется узкому кругу лиц и по закрытым (защищённым) каналам.
  - **Личная (приватная)** — набор сведений о какой-либо личности, определяющий социальное положение и типы социальных взаимодействий.

Классификация информационных ресурсов

Количество утечек данных: Россия, 2017-2022 гг.





От КОГО нужно защищать?

От КОГО нужно защищать информацию?

Внутри

1. Недобросовестные сотрудники, вредительство
2. Ошибки человека, некомпетентность
3. Технические сбои и выход из строя оборудования
4. Несанкционированный физический доступ
5. Естественные бедствия
6. и др.

Снаружи

1. Конкуренты
2. Злоумышленники и хакеры, киберпреступность
3. Государственные организации и кибершпионы, киберпреступность
4. Вредоносное ПО
5. Физические угрозы
6. Технические сбои и выход из строя оборудования, аварии
7. Естественные бедствия
8. и др.

Мотивы нарушений информационной безопасности

От ЧЕГО нужно защищать?

Угрозы и Риски

- Информацию **необходимо защищать от различных угроз и рисков**, чтобы обеспечить ее конфиденциальность, целостность и доступность.

Угрозы / Риски / Уязвимости / Атаки

- Под **угрозой** информационной безопасности объекта будем понимать возможные воздействия на него, приводящие к ущербу.

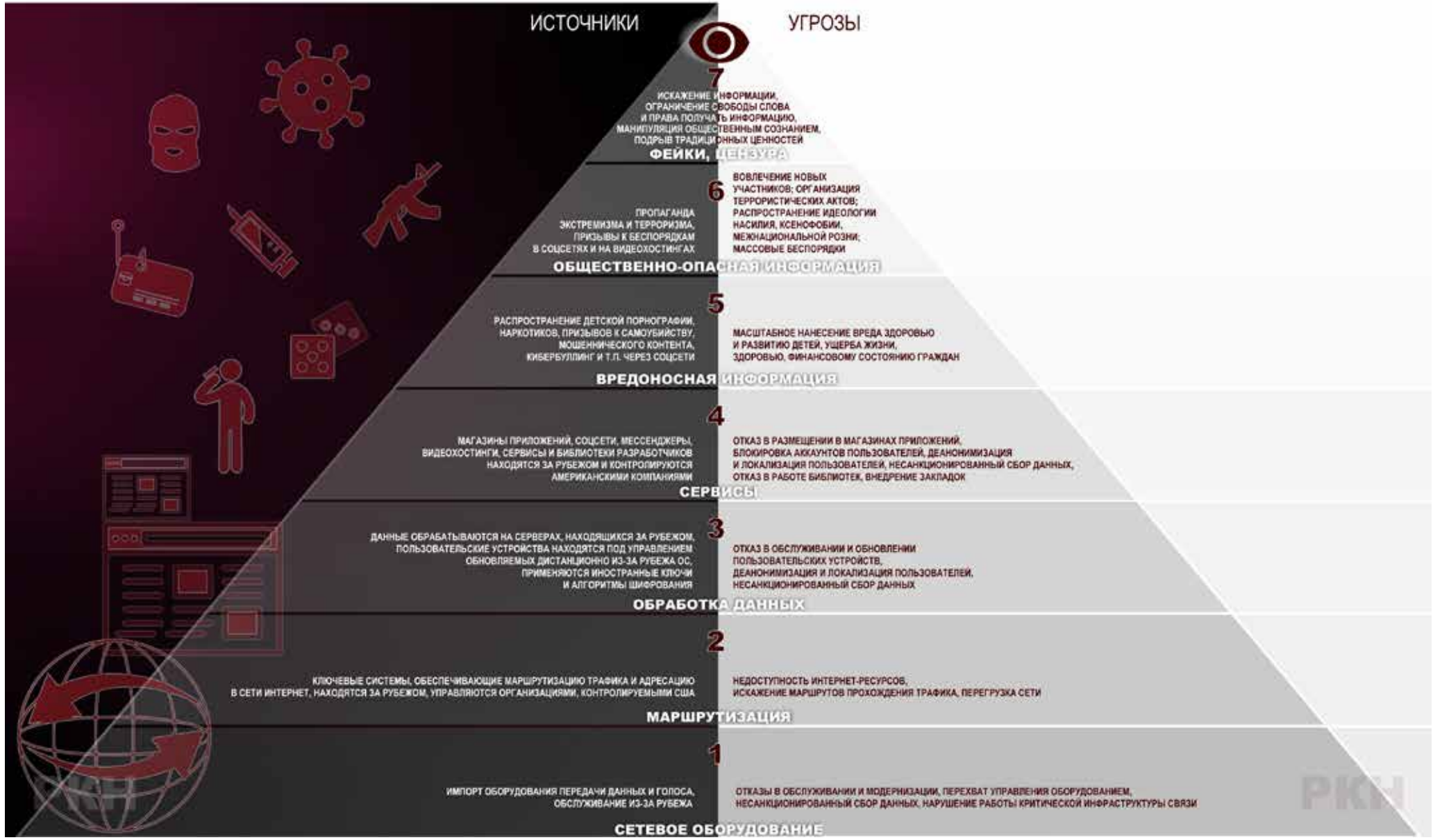
- Некоторое свойство объекта, делающее возможным возникновение и реализацию угрозы, будем называть **уязвимостью**.

- Действие злоумышленника, заключающееся в поиске и использовании той или иной уязвимости, будем называть **атакой**.

- **Риск** – способность конкретных угроз использовать уязвимости одного или нескольких видов активов для нанесения ущерба.

Области проблем ИБ и пути их решения

Пирамида цифровых угроз



Пирамида цифровых угроз

Пирамида цифровых угроз

Каналы утечки информации

- На данный момент выделяют 8 самостоятельных каналов утечки (далее - классификаторы):

1. **Оборудование (сервер, СХД, ноутбук, ПК)**, – компрометация информации в ходе обслуживания, в результате кражи или потери оборудования.
2. **Мобильные устройства** – утечка информации вследствие нелегитимного использования мобильного устройства/кражи мобильного устройства (смартфоны, планшеты). Использование данных устройств рассматривается в рамках парадигмы BYOD.
3. **Съемные носители** – потеря/кража съемных носителей (CD, DVD, USB, карты памяти и др.).

Каналы утечки информации

- На данный момент выделяют 8 самостоятельных каналов утечки (далее - классификаторы):

4. **Сеть (сетевой канал)** – утечка через браузер (отправка данных через вебинтерфейс в личную почту, формы ввода в браузере), нелегитимное использование внутренних ресурсов сети, FTP, облачных сервисов, нелегитимная публикация информации на веб-сервисе.
5. **Электронная почта** – утечка данных через корпоративную электронную почту.
6. **Бумажные документы** – утечка информации вследствие неправильного хранения/утилизации бумажной документации, через печатающие устройства (отправка на печать и кража/вынос конфиденциальной информации на бумаге).

Каналы утечки информации

- На данный момент выделяют 8 самостоятельных каналов утечки (далее - классификаторы):

7. **IM–сервисы мгновенных сообщений** – утечка информации при передаче ее голосом, в текстовом виде, а также через видео - при использовании мессенджеров.
8. **Не определено** – категория, используемая в случае, когда сообщение об инциденте в СМИ не позволяет точно определить канал утечки.

Как надо защищаться?

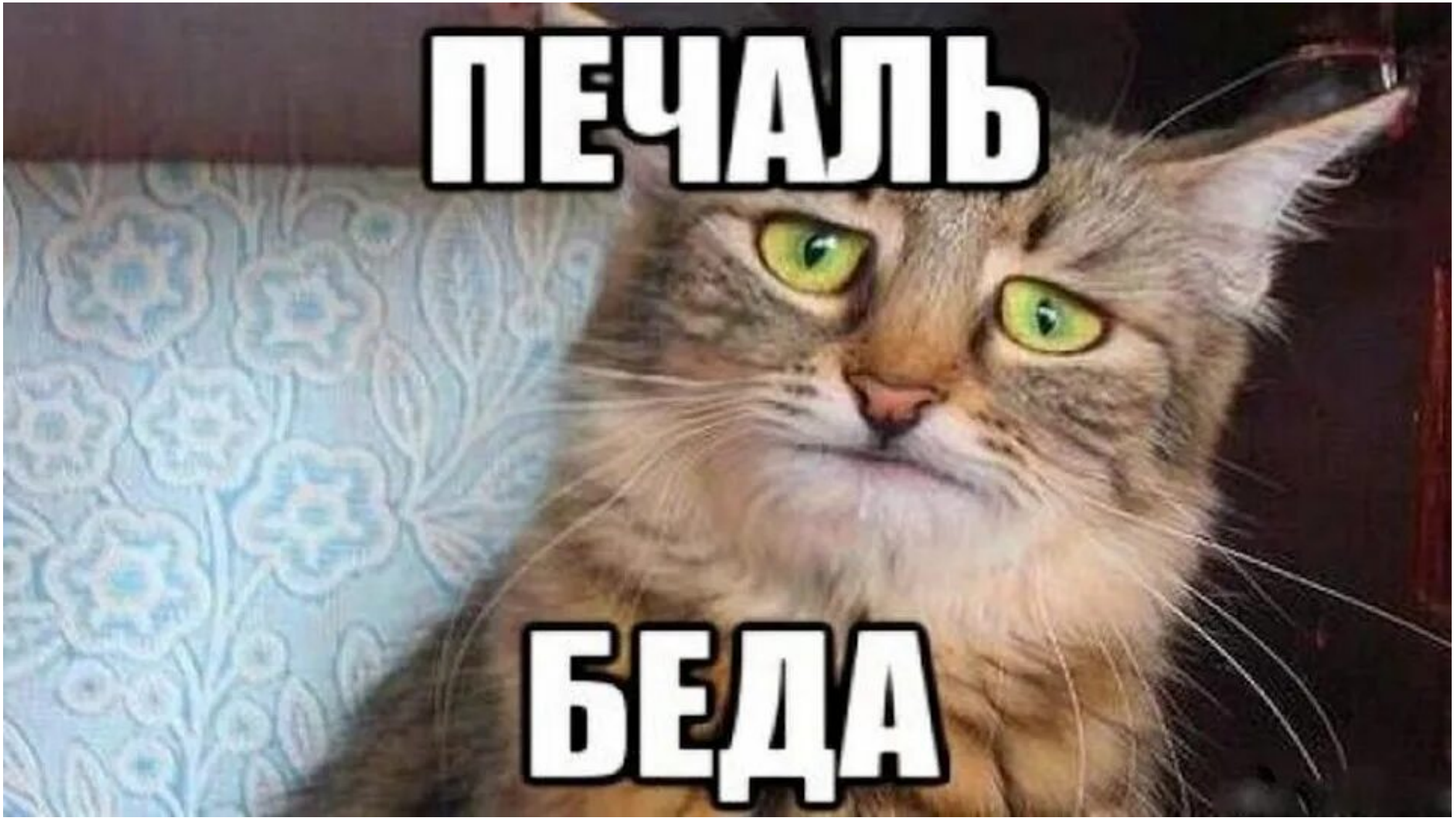

ИНТЕРНЕТ-АДРЕСА,
ЛОГИНЫ И ПАРОЛИ
Информационная безопасность 80 lvl

Что применяем для защиты?

1. Обучение сотрудников
2. Регулярное обновление программного обеспечения, включая операционную систему и приложения
3. Использование сложных и уникальных паролей
4. Установка надежного антивируса и ежедневное его обновление
5. Применение файрволла
6. Применение криптографии, шифрования
7. Построение SOC (Security operations center) - ситуационных центров информационной безопасности
8. Применение DLP (Data Leak Prevention) систем предотвращения от утечек
9. SIEM (Security Information and Event Management) системы управления информацией о безопасности и событиях ИБ
10. и многое, многое другое

Средства защиты информации

Что происходит если мы не занимаемся вопросами информационной безопасности и защиты информации?


ПЕЧАЛЬ
БЕДА

Ущерб

- Согласно последним данным из отчета «Cost of a Data Breach Report 2023», **средний ущерб после утечки составил $4,5 млн**, что на 15% выше, чем три года назад. При этом ущерб от утечки по вине внутреннего нарушителя выше — сумма потерь в таком случае составила $4,9 млн. В совместном отчете компаний Proofpoint и Ponemon Institute отмечается, что для пострадавшей организации на Западе **средняя стоимость кражи учетных данных в результате действий внутреннего нарушителя составила $4,6 млн, а утечка из-за халатности работника (неумышленная) — $6,6 млн.**
- При этом ущерб от инцидентов информационной безопасности может затрагивать не только отдельные организации, но и целые города. Так, недавно городской совет Далласа США выделил из бюджета города $8,6 млн на оплату услуг ИБ-компаний, участвовавших в восстановлении информационной инфраструктуры города после кибератаки. Используя программу-вымогатель, злоумышленники украли персональные данные 26 тыс. человек.

Нерезультативная безопасность

1. American Medical Collection Agency (03’19) – банкротство после утечки данных
2. Утечка 143 млн записей из Equifax (07’17) – ущерб составил 700 млн долларов
3. Взлом штаба демпартии США и утечка почты Хиллари Клинтон (2016) – влияние на результаты выборов (возможно)
4. Утечка 100 млн записей из Capital One – ущерб от 100 до 150 млн долларов
5. Утечка из Marriot / Starwood (03’20) – штраф 123 млн долларов
6. Target (05’14) – 61 млн долларов потерь от утечки данных в результате взлома, 100 млн долларов на изменение инфраструктуры и 18,5 млн долларов штрафа
7. Vastaamo Psychotherapy Centre (02’21) – банкротство после кражи данных пациентов и обвинений с их стороны

https://www.ptsecurity.com/upload/corporate/ru-ru/webinars/ics/uvedomlenie-ob-utechkah.pdf

Кто все это должен делать?

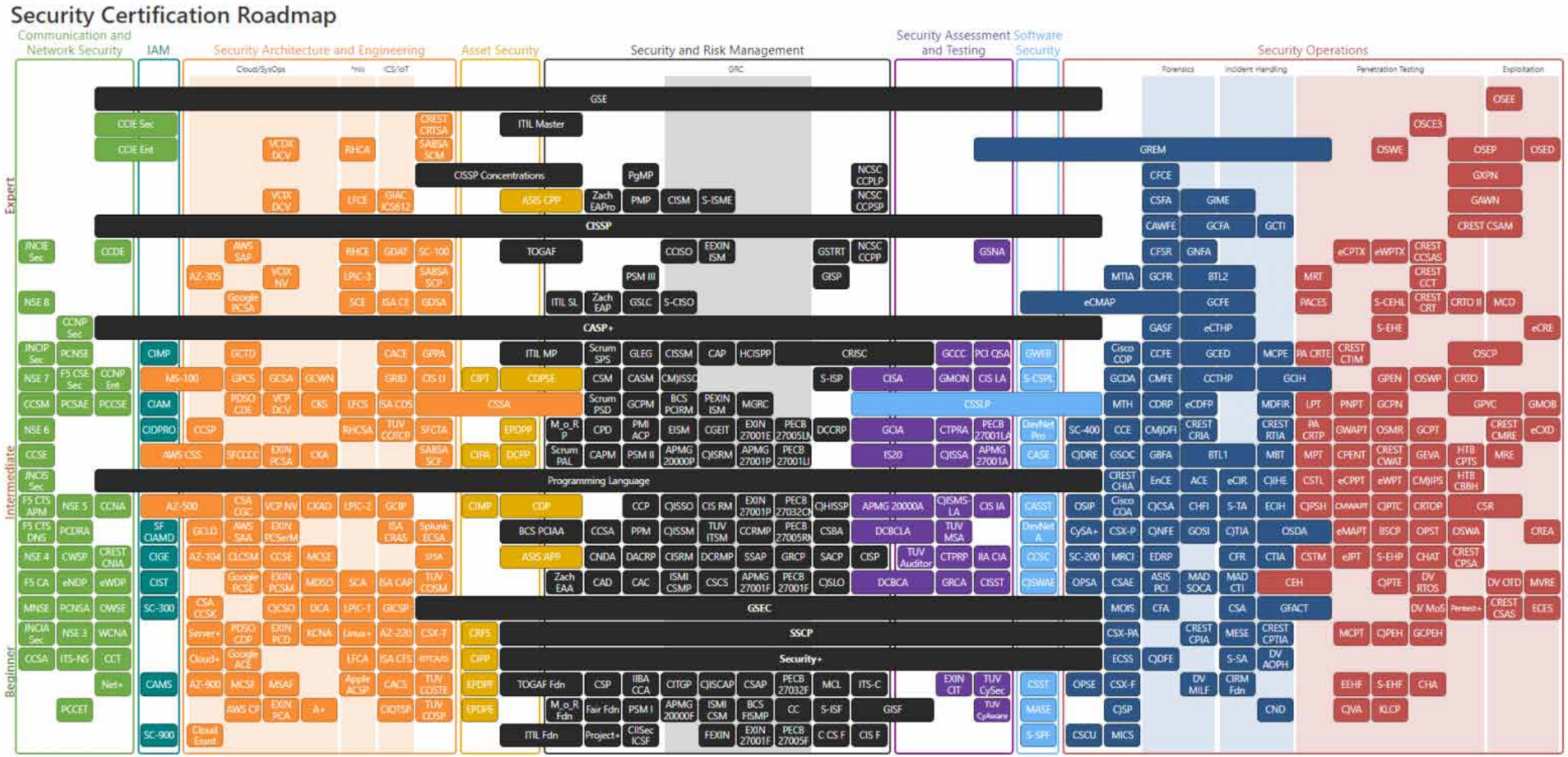
Кто все это должен делать?

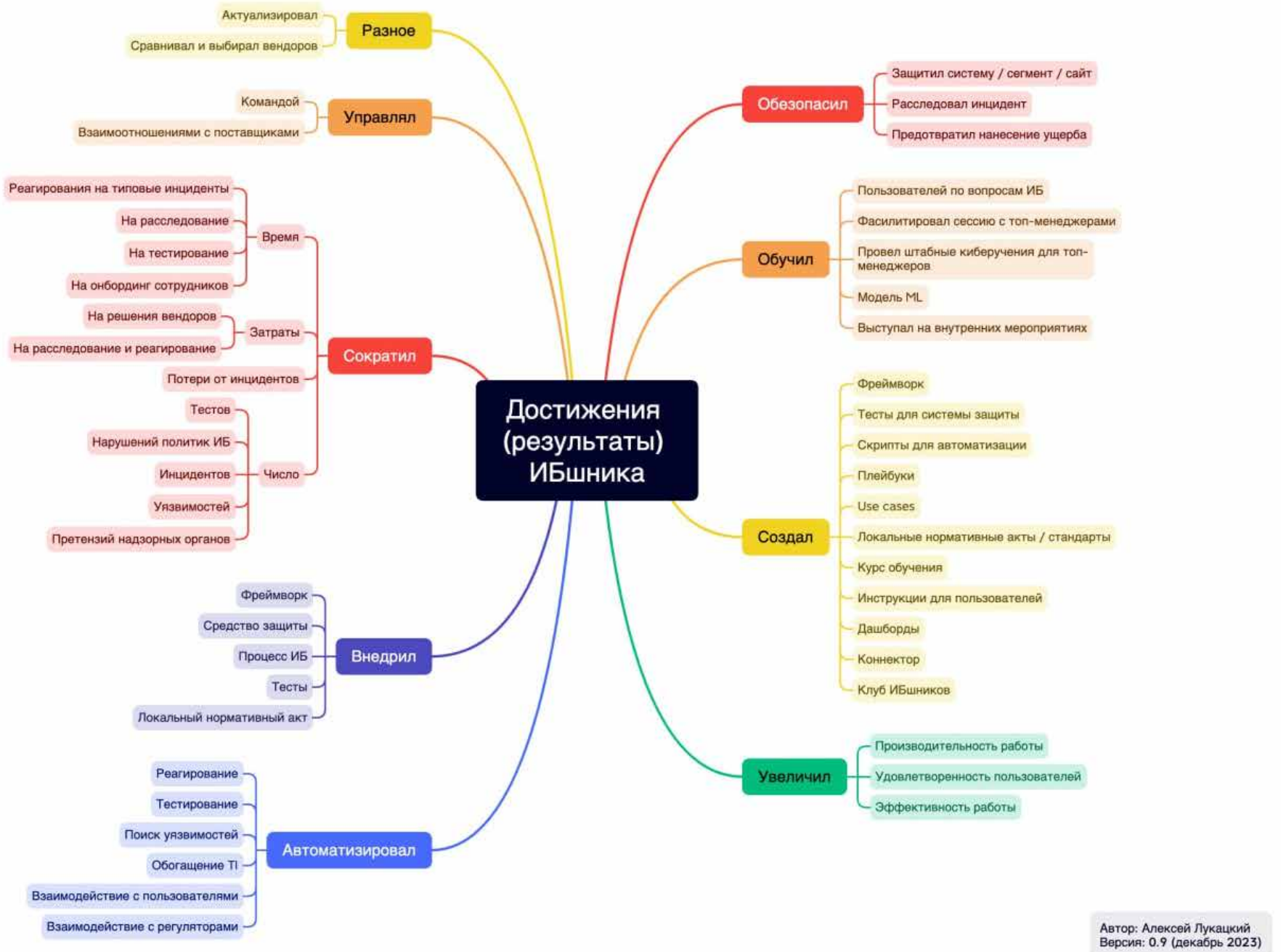
Специалист по ИБ

- **Задача специалиста по кибербезопасности** — создавать защищённую архитектуру пользования данными, предотвращая киберпреступления и исключая кибер-террористические атаки.

- В эпоху, когда массовые «сливы» данных происходят едва ли не каждую неделю, а от кибератак страдают банки, органы власти и глобальные производства, ценность таких профессионалов будет только расти. В число компетенций, необходимых для развития в качестве специалиста по кибербезопасности, входят навыки программирования, умение обрабатывать массивы данных, знание технических аспектов электронных приборов и гаджетов, а также аналитическое мышление, внимательность и аккуратность.

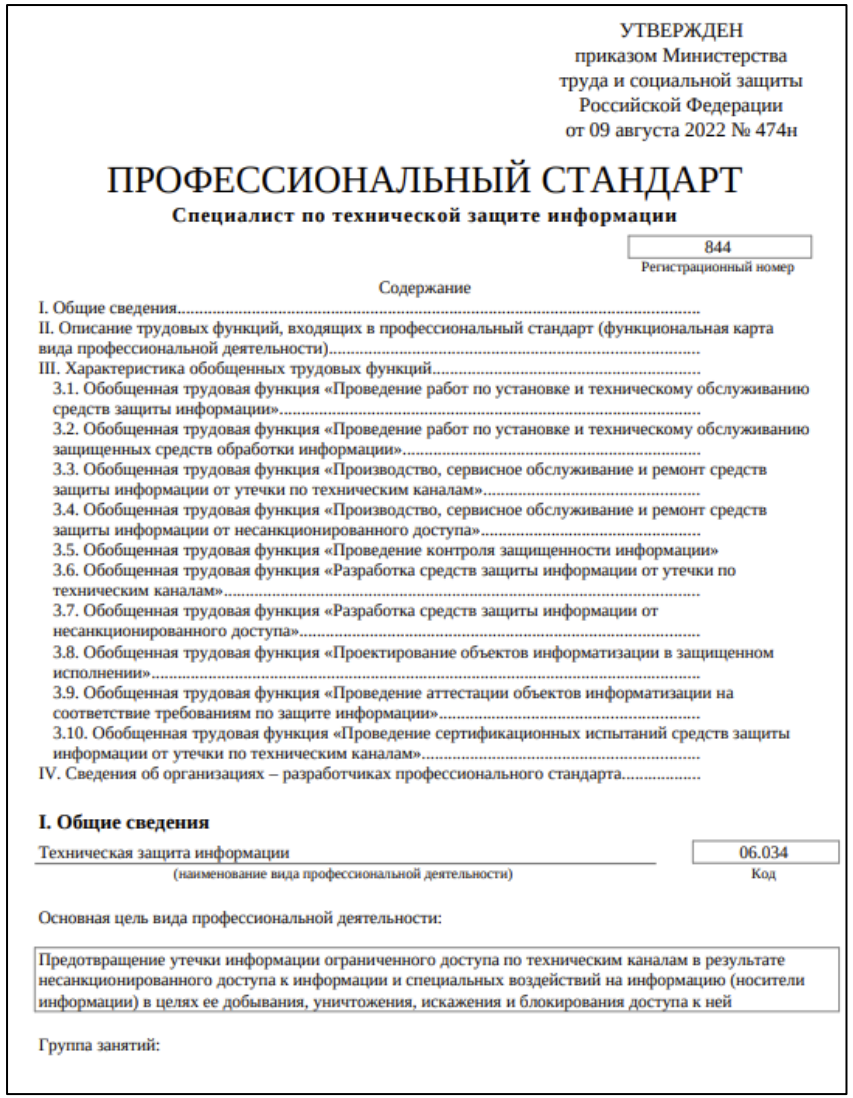
В информационной безопасности 400 с лишним направлений




Достижения (результаты) ИБшника
Разное
Актуализировал
Сравнивал и выбирал вендоров
Управлял
Командой
Взаимоотношениями с поставщиками
Сократил
Время
Реагирования на типовые инциденты
На расследование
На тестирование
На онбординг сотрудников
Затраты
На решения вендоров
На расследование и реагирование
Потери от инцидентов
Число
Тестов
Нарушений политик ИБ
Инцидентов
Уязвимостей
Претензий надзорных органов
Внедрил
Фреймворк
Средство защиты
Процесс ИБ
Тесты
Локальный нормативный акт
Автоматизировал
Реагирование
Тестирование
Поиск уязвимостей
Обогащение TI
Взаимодействие с пользователями
Взаимодействие с регуляторами
Обезопасил
Защитил систему / сегмент / сайт
Расследовал инцидент
Предотвратил нанесение ущерба
Обучил
Пользователей по вопросам ИБ
Фасилитировал сессию с топ-менеджерами
Провел штабные киберучения для топ-менеджеров
Модель ML
Выступал на внутренних мероприятиях
Создал
Фреймворк
Тесты для системы защиты
Скрипты для автоматизации
Плейбуки
Use cases
Локальные нормативные акты / стандарты
Курс обучения
Инструкции для пользователей
Дашборды
Коннектор
Клуб ИБшников
Увеличил
Производительность работы
Удовлетворенность пользователей
Эффективность работы
Автор: Алексей Лукацкий
Версия: 0.9 (декабрь 2023)

Какие требования к специалистам по информационной безопасности настоящее время?

Требования к специалистам по информационной безопасности в России



УТВЕРЖДЕН
приказом Министерства
труда и социальной защиты
Российской Федерации
от 09 августа 2022 № 474н

ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ

Специалист по технической защите информации

844
Регистрационный номер

Содержание

I. Общие сведения

Техническая защита информации — 06.034
(наименование вида профессиональной деятельности) — Код

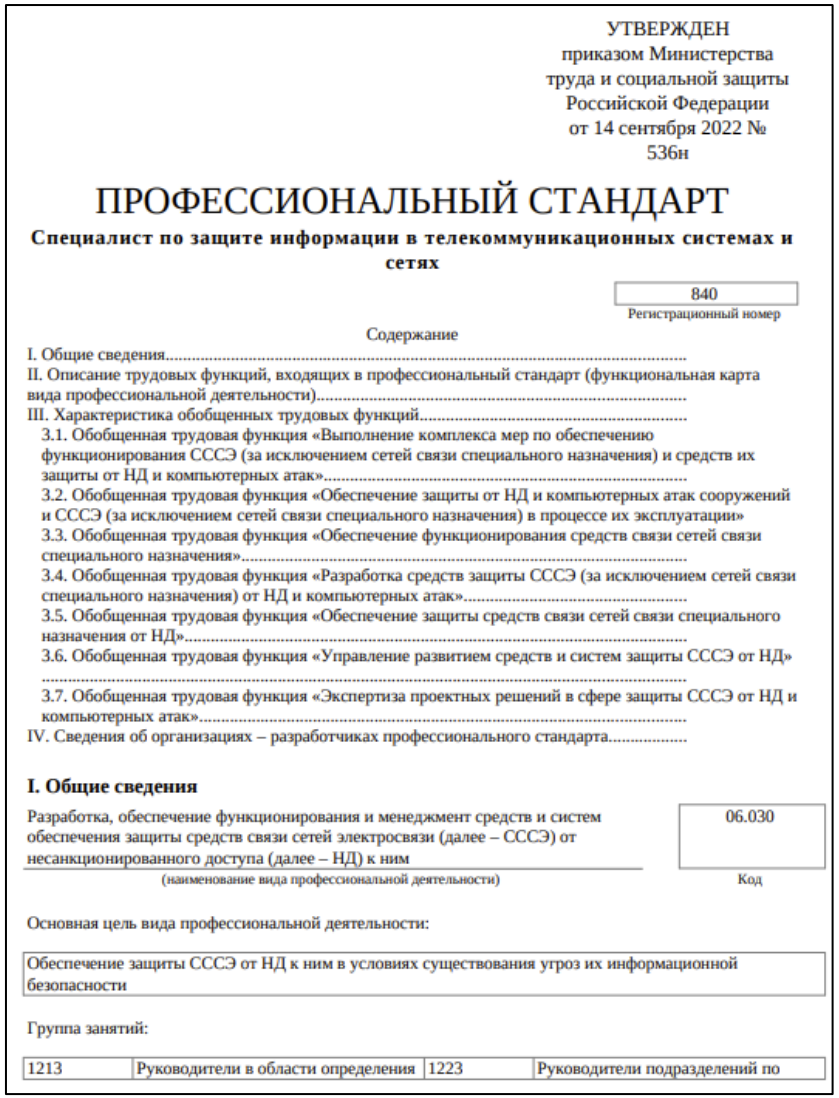
Основная цель вида профессиональной деятельности:

Предотвращение утечки информации ограниченного доступа по техническим каналам в результате несанкционированного доступа к информации и специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней

Группа занятий:

- Профессиональный стандарт «**Специалист по технической защите информации**»
- https://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/reestr-professionalnykh-standartov/index.php?ELEMENT_ID=115980

Требования к специалистам по информационной безопасности в России



УТВЕРЖДЕН
приказом Министерства
труда и социальной защиты
Российской Федерации
от 14 сентября 2022 №
536н

ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ

Специалист по защите информации в телекоммуникационных системах и сетях

840
Регистрационный номер

Содержание

I. Общие сведения

Разработка, обеспечение функционирования и менеджмент средств и систем обеспечения защиты средств связи сетей электросвязи (далее – СССЭ) от несанкционированного доступа (далее – НД) к ним	06.030
(наименование вида профессиональной деятельности)	Код

Основная цель вида профессиональной деятельности:

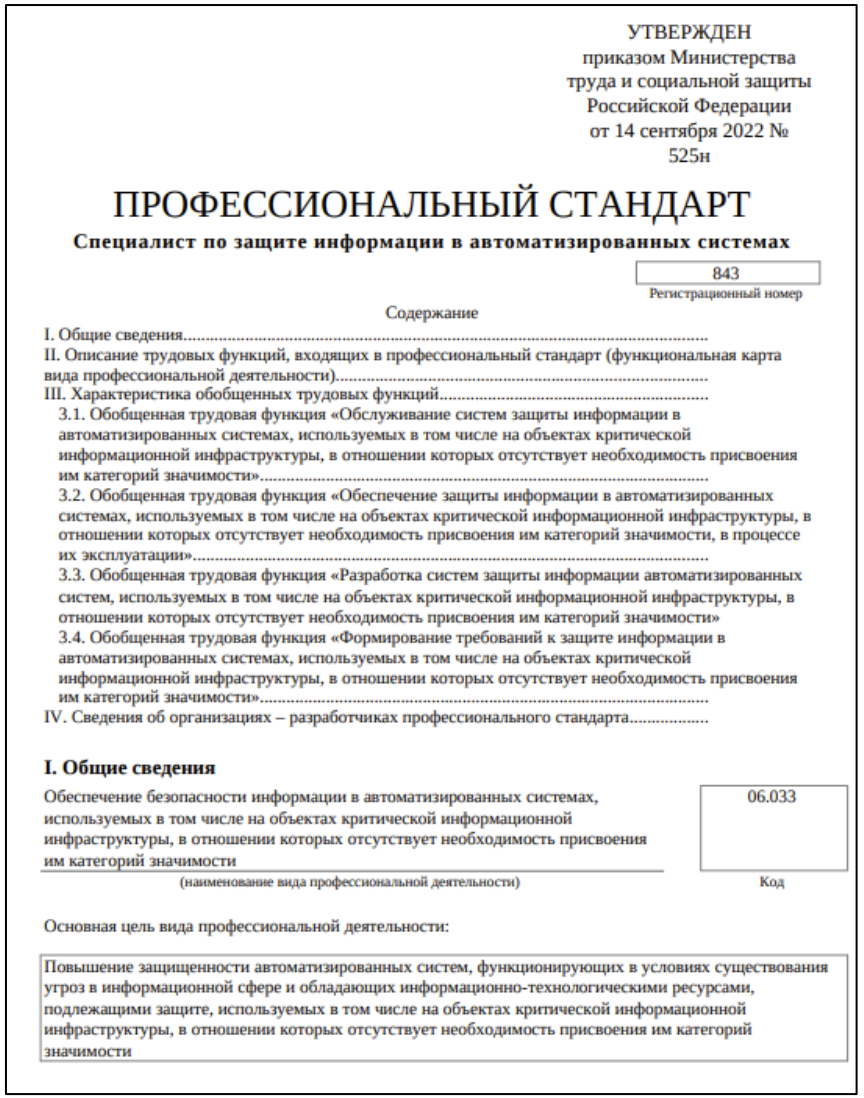
Обеспечение защиты СССЭ от НД к ним в условиях существования угроз их информационной безопасности

Группа занятий:

1213	Руководители в области определения	1223	Руководители подразделений по

- Профессиональный стандарт «**Специалист по защите информации в телекоммуникационных системах и сетях**»
- https://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/reestr-professionalnykh-standartov/index.php?ELEMENT_ID=117320

Требования к специалистам по информационной безопасности в России



УТВЕРЖДЕН
приказом Министерства
труда и социальной защиты
Российской Федерации
от 14 сентября 2022 №
525н

ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ

Специалист по защите информации в автоматизированных системах

843
Регистрационный номер

Содержание

I. Общие сведения

Обеспечение безопасности информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости

(наименование вида профессиональной деятельности)

06.033
Код

Основная цель вида профессиональной деятельности:

Повышение защищенности автоматизированных систем, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно-технологическими ресурсами, подлежащими защите, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости

- Профессиональный стандарт «**Специалист по защите информации в автоматизированных системах**»
- https://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/reestr-professionalnykh-standartov/index.php?ELEMENT_ID=116917

Топ-10 навыков, требуемых в вакансиях ИБ

%, доля от общего числа вакансий в ИБ, Россия, 2022 г.

Обзор рынка труда в ИТ и ИБ (02.03.2023) https://itm.ranepa.ru/sites/default/files/files/hh-rynok_truda_ib_02.03.2023.pdf

Каков рынок вакансий в сфере информационной безопасности?

Рынок ИБ в России 2023

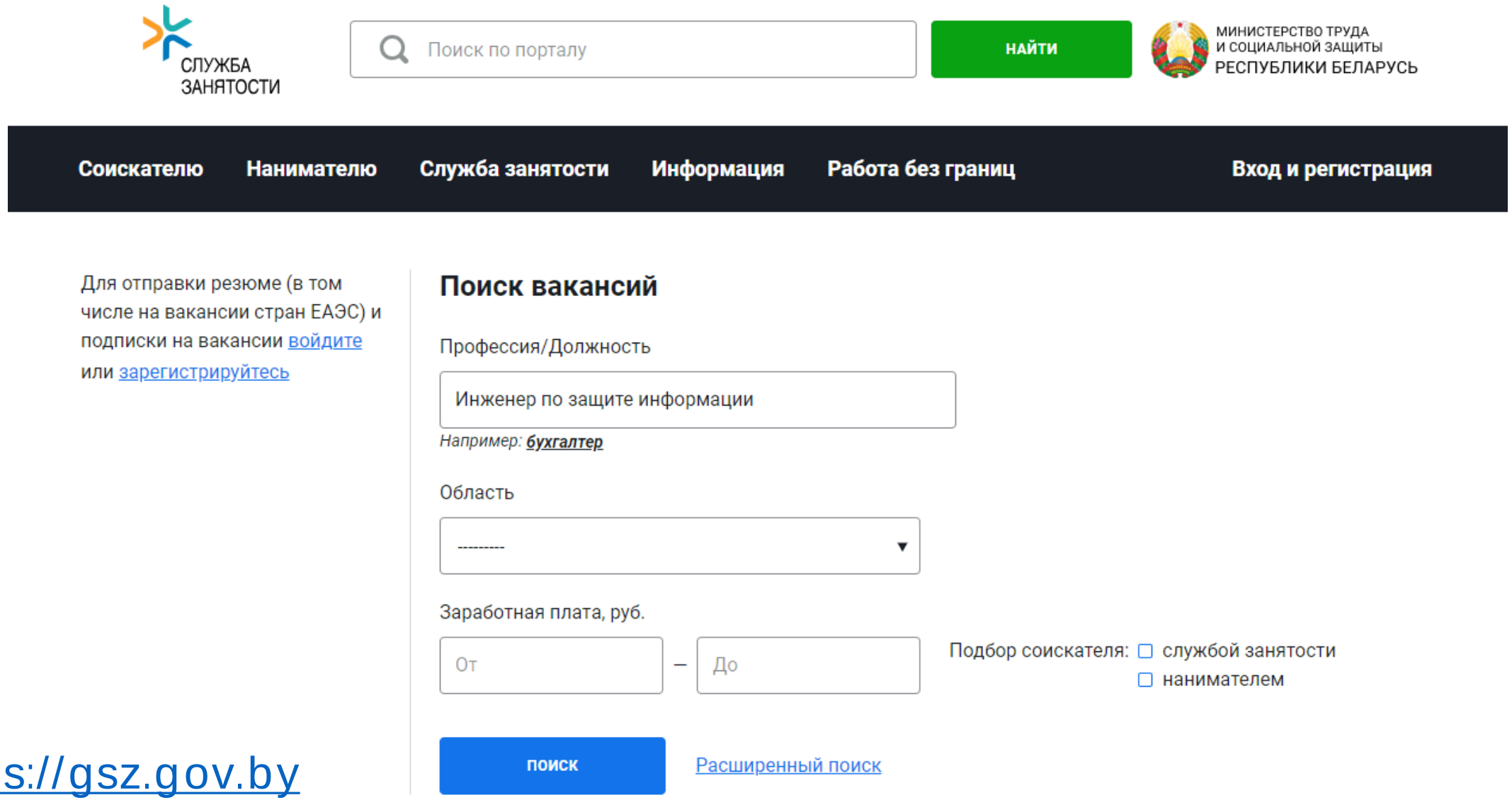
- **По оценкам рекрутеров, на протяжении всего 2023 г. вакансий специалистов по ИБ было стабильно больше, чем за аналогичные периоды прошлого года.** Вероятнее всего, потребность в кадрах будет только увеличиваться. Это может быть связано с ростом объема российского рынка кибербезопасности. По прогнозам Центра стратегических разработок, в 2022 г. он оценивался в 193,3 млрд руб., а к 2027 г. его объем составит 559 млрд.

- **В третьем квартале 2023 года компании-работодатели опубликовали на hh.rub России 7,2 тыс. вакансий в поисках ИБ-специалистов.** Объем предложений работы соответствует уровням первых двух кварталов, при этом находится существенно выше (+26%) показателей аналогичного периода 2022 года, а также в сравнении с динамикой вакансий всего ИТ-сектора, которая показывает рост в 20% в третьем квартале. **Сегмент кибербезопасности наряду с программированием/разработкой является одним из самых сильных драйверов роста спроса.**

Рынок ИБ в России 2023

- **Спрос на ИБ-специалистов осенью 2023 года вырос почти во всех отраслях бизнеса.** По-прежнему лидируют ИТ-компании с 2,7 тыс. вакансий (+35% г/г), финансовый сектор – ровно 1 тыс. (+20%), b2b-услуги – 0,5 тыс. (+40%), телеком – 0,3 тыс. (+6%). Лишь в трех отраслях бизнеса сегодня наблюдается снижение числа вакансий для ИБ: металлургия (-35% г/г), лесная промышленность (-20%), FMCG (-30%).
- **Москва продолжает доминировать по уровню спроса на ИБ-специалистов** в региональном сегменте – ее доля в общем числе вакансий по-прежнему самая высокая (47%), и прибавила еще 1 п. п. по сравнению с прошлым кварталом. Из первой десятки регионов по числу открытых ИБ-вакансий только в двух была зафиксирована отрицательная динамика – в Самарской (-17%) и Московской (-25%) областях.
- **Компании по-прежнему готовы активно рассматривать все без исключения грейды ИБ-специалистов, в том числе сотрудников с опытом от 1 до 3 лет**, но основной прирост спроса приходится на миддл- и сеньор-специалистов, для которых вакансии за год выросли на 36% и 29% соответственно. Минимальный прирост сохраняется на джунов без какого-либо опыта в ИБ – чуть выше 700 вакансий с приростом всего 6%.

Общереспубликанский банк вакансий



https://gsz.gov.by

Вакансии


hh ru
HeadHunter
Вход в личный кабинет
Вакансии
Сотрудникам
Работа в компан
Сбербанк России
Промсвязьбанк
Мобильные ТелеСистемы (МТС)
ИНКОМ-Недвижимость
hh ru
HeadHunter

Вакансии

hh.ru

Дата поиска вакансий: 11.02.2024

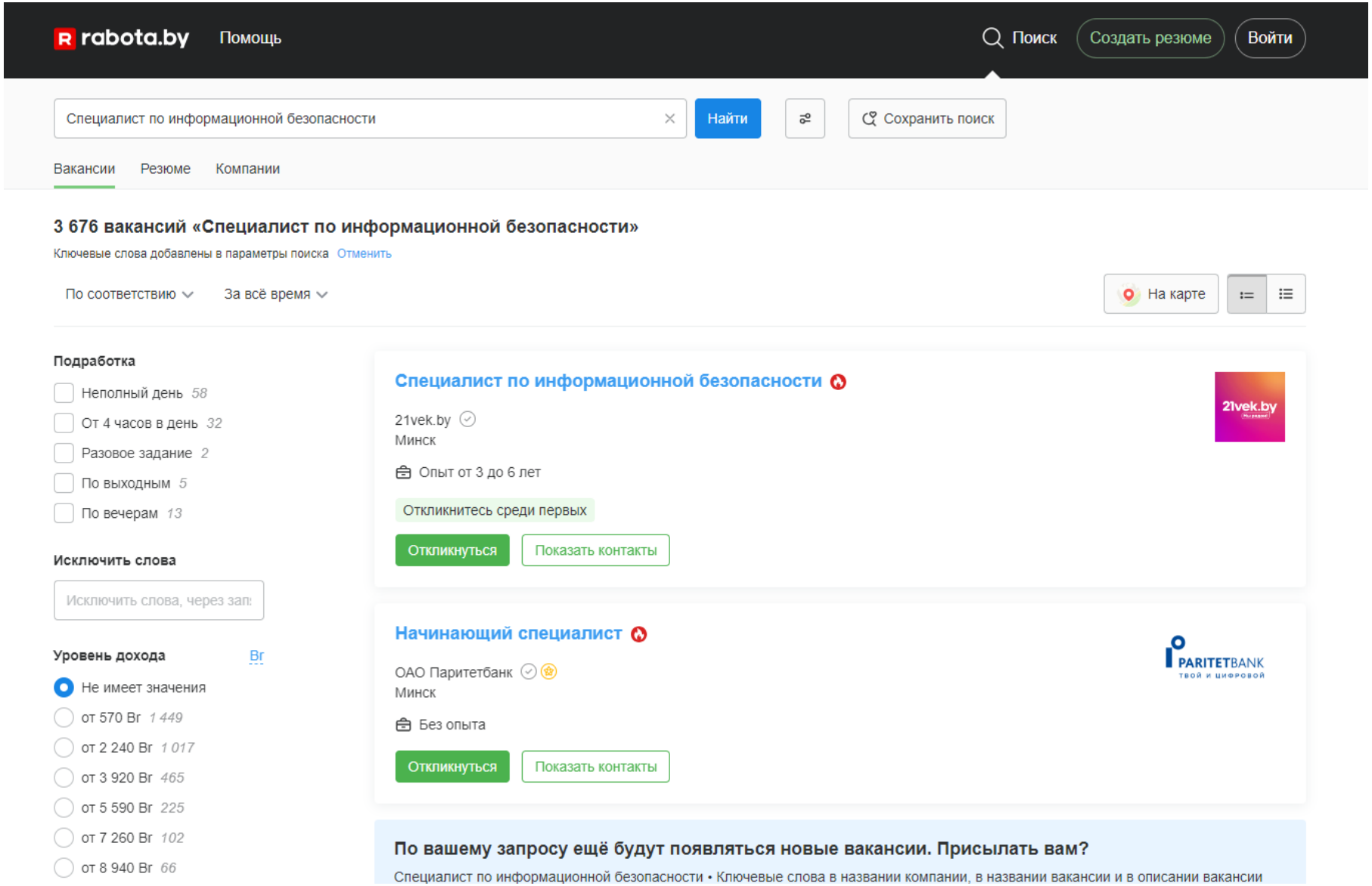
Запрос	Регион	Количество вакансий
Информационная безопасность	Россия целиком	8913
Специалист по ИБ	Россия целиком	1463
Информационная безопасность	Беларусь в целом	138
Специалист по ИБ	Беларусь в целом	19

gsz.gov.by

Дата поиска вакансий: 13.02.2024

Запрос	Количество вакансий
Техник по защите информации	38
Специалист по защите информации	
Инженер по защите информации	

Вакансии rabota.by



Вакансия: Специалист по ИБ

- **Обязанности:**
  - проведение внутренних аудитов информационной безопасности;
  - совершенствование процессов информационной безопасности компании;
  - внедрение и эксплуатация средств защиты информации, разработка архитектуры системы защиты информационной системы;
  - мониторинг событий информационной безопасности;
  - проведение анализа событий и расследований инцидентов информационной безопасности;
  - обучение сотрудников предприятия по вопросам информационной безопасности;
  - контроль выполнения сотрудниками корпоративных требований информационной безопасности;
  - разработка и поддержка в актуальном состоянии регламентов, положений по информационной безопасности.
- **Будет плюсом:**
  - опыт проведения расследований инцидентов информационной безопасности;
  - опыт проектирования, создания и аттестации системы защиты информации;
  - опыт аудита, проектирования, создания и аттестации критически важных объектов информатизации.

Вакансия: Специалист по ИБ

- **Требования:**
  - высшее профессиональное (техническое) образование, квалификация «Специалист» по профилю: "компьютерная безопасность", "организация и технология защиты информации", "информационная безопасность телекоммуникационных систем", "противодействие техническим разведкам"; повышение квалификации по программам информационной безопасности; Группа специальностей 98 01 «ЗАЩИТА ИНФОРМАЦИИ»;
  - знание действующего законодательства РБ в области защиты информации;
  - отличное знание Linux и Windows ОС;
  - практический опыт использования средств защиты информации (NGFW, DLP, WAF, IDS/IPS, AV, SIEM, SOAR и др.);
  - опыт проведения аудитов и оценка эффективности защищенности информационных систем;
  - опыт разработки ЛНПА в области информационной безопасности согласно требованиям законодательства РБ;
  - знание английского языка на уровне B1 (изучение технической документации).

https://web.archive.org/web/20230217211651/https://hh.ru/vacancy/75554840

Хабр.Карьера

Хабр Карьера • Кем работать в IT: Информационная безопасность

Intern

Понимание принципов SIEM, сетевых протоколов и построения сетей. Навык работы с Windows\Linux системами;
Будет плюсом знание основ программирования, PowerShell и Python;
Умение формировать SQL-запросы.

Без опыта\ 3-4 курса (ИБ)

- Построение аналитических отчетов по результатам реагирования на инциденты КБ;
- Обработка данных;
- Визуализирование информации.

Зарплата по договоренности

Junior

1 линия SOC

Базовые знания IDS\IPS, SIEM, NGFW.

Опыт работы в ИБ от года

- Мониторинг и расследование инцидентов в рамках SOC L1;
- Своевременная эскалация инцидентов ИБ.

до 160 000 ₽

Хабр.Карьера

Middle
2 линия SOC

Углубленные знания IDS\IPS, SIEM, NGFW, ELK Stack, OWASP.

Опыт работы в ИБ от двух лет

- Мониторинг и расследование инцидентов в рамках SOC L2;
- Разработка правил корреляции\сценариев выявления инцидентов ИБ;
- Участие в разработке сценариев реагирования (playbook).

до 180 000 ₽

Senior
3 линия SOC

Экспертные знания IDS\IPS, NGFW, SIEM, AV, Sandbox, Windows\Linux, Network, ELK; Опыт написания скриптов (bash, PowerShell, Python).

Опыт работы в ИБ от двух лет

- Мониторинг и расследование инцидентов в рамках SOC L3;
- Разработка правил корреляции\сценариев выявления инцидентов ИБ;
- Разработка сценариев реагирования (playbook);
- Анализ инцидентов, оценка их последствий и разработка рекомендаций по устранению последствий;
- Разбор сложных и нетиповых инцидентов ИБ.

до 300 000 ₽

Ключевые требования работодателей к специалистам по информационной безопасности

	Junior	Middle	Senior	Lead
Стаж работы	до 1 года	1-3 года	3-6 лет	от 6 лет
Образование	Высшее в области ИБ / Высшее техническое + Курсы	Высшее в области ИБ / Другое высшее + переподготовка (ФСТЭК)	Высшее в области ИБ / Другое высшее + переподготовка (ФСТЭК)	Высшее в области ИБ / Другое высшее + переподготовка (ФСТЭК)
Навыки	• Знание основных видов угроз ИБ • Понимание принципов сетевых технологий • Базовые знания операционных систем • Понимание принципов работы основных СЗИ • Опыт работы с системами мониторинга (Zabbix) • Навыки программирования	• Защита от утечек информации (DLP) • Анализ состояния защиты информации • Опыт администрирования Windows/Linux • Опыт расследования инцидентов ИБ • Знание основных НПА в области ИБ • Опыт работы с SIEM	• Знание законодательства в области ИБ • Знание всех процессов обеспечения ИБ • Опыт администрирования и сопровождения СЗИ • Понимание принципов работы SIEM, IPS/IDS, WAF • Написание программ на скриптовых языках • Знание методов форензики	• Опыт проведения аудитов ИБ • Уверенное знание законов и стандартов в области ИБ • Опыт построения и эксплуатации ИС • Опыт разработки технической документации • Глубокое понимание трендов в области ИБ • Управленческие навыки

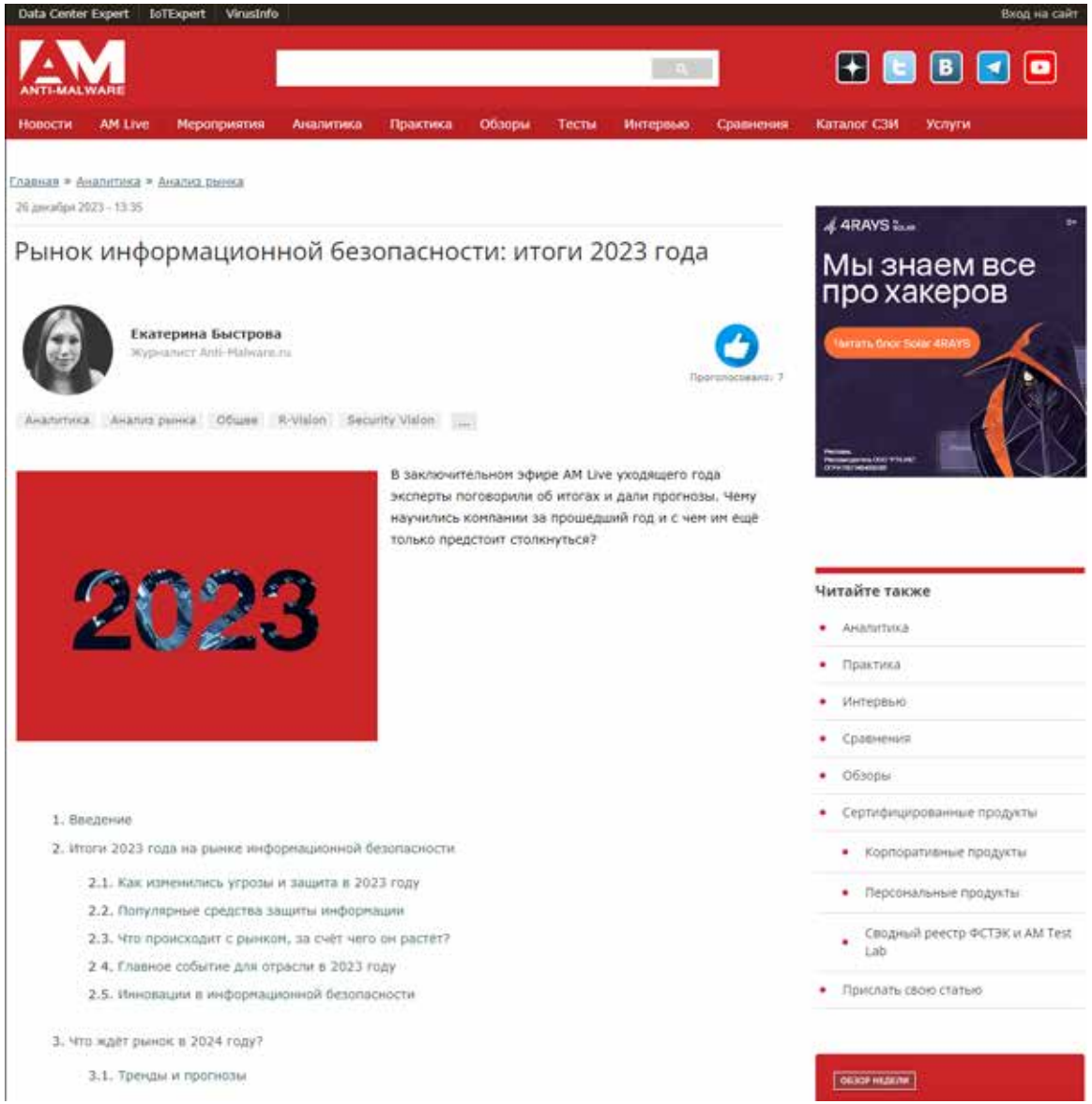
Источник: Код Подбора

Аналитика: Рынок вакансий ИБ 2022

- **Исследование рынка информационной безопасности в России по клиентским сегментам. 2022 год**
- В данном исследовании освещается текущая ситуация на рынке ИБ в России, рассматривается движение сегментов, их объемы и занимаемые доли рынка, а также прогнозируется развитие рынка до 2025 года.

- https://rt-solar.ru/upload/iblock/962/b7wyn7498evdp1jf8t7iccj5239ug4i9/Issledovanie-rynka-IB-RF-2022.pdf

Аналитика: Рынок вакансий ИБ 2023



- **Рынок информационной безопасности: итоги 2023 года**
- В заключительном эфире AM Live уходящего года эксперты поговорили об итогах и дали прогнозы. Чему научились компании за прошедший год и с чем им ещё только предстоит столкнуться?

- https://www.anti-malware.ru/analytics/Market_Analysis/CyberSecurity-2023-Results

Аналитика / Отчеты по информационной безопасности

Как перевернулся мир ИБ в последних несколько лет

Тренды в сфере ИБ

- В 2020 году киберугрозы попали в квадрант наивысшего риска в глобальном ландшафте рисков. Причина – как степень наибольшего влияния, так и самая высокая вероятность наступления рисков
(Global Risks Report 2020, World Economic Forum).
- Предотвращение утечек данных – главный приоритет для ИТ отрасли и второй для безопасности организаций
(2020 Cybersecurity Outlook Report, VMware/Carbon Black).
- Вероятность ареста киберпреступника составляет менее 1% от общего числа ежегодных киберинцидентов в США
(To Catch a Hacker, Third Way).
- Количество утечек данных, о которых публично заявили в 2021 году, на 17% превышает общее количество инцидентов в 2020 году
(2021 Q3 Data Breach Analysis, ITRC).

Тренды в сфере ИБ

- Киберинциденты вошли в тройку главных бизнес-рисков (Allianz Risk Barometer, Allianz).
- Киберпреступники чаще всего атаковали организации из финансового и страхового сектора (X-Force Threat Intelligence Index 2021).
- 18% BEC-атак произошли в компаний, предоставляющих финансовые услуги (Top Industries Targeted by Cyberattacks).
- Мошенничество с похищением учетных записей выросло на 850%, при этом большинство атак были сосредоточены на криптовалютах и цифровых кошельках. В 2020 год ущерб от киберпреступлений, связанных с криптовалютой, составил 1,9 млрд долларов (Q3 2021 Digital Trust & Safety Index).

Ущерб от киберпреступлений

- В 2020 году предполагаемый ущерб от киберпреступлений увеличился больше чем на 50% за два года и превысил 1 триллион долларов (The Hidden Costs of Cybercrime, McAfee).
- В отрасли здравоохранения средняя стоимость взломанной записи в 2020 году составила 499 долларов (Healthcare Breach Report 2021, Bitglass).
- Фишинг был главным киберпреступлением в США в 2020 году, на него пришлось более 30% всех жертв. BEC-атаки привели к финансовым потерям в размере 1,86 млрд долларов (Internet Crime Report 2020, FBI).

Человеческий фактор

- 85% утечек данных происходят из-за «человеческого фактора» (2021 Data Breach Investigations Report, Verizon).
- По данным ежегодного исследования «СёрчИнформ», в 2021 году 66% инцидентов в ИБ были неумышленными.
- Сотрудники знают о своей ответственности в случайных утечках. 43% сотрудников «очень» или «почти» уверены, что они допустили ошибки на работе, которые повлияли на безопасность (The Psychology of Human Error, Tessian).
- 55% ИТ-руководителей ожидают, что сотрудники будут предупреждать их о киберинцидентах. При этом в 89% случаев вовлеченным в инциденты сотрудникам пришлось столкнуться с негативными последствиями этих инцидентов. Только у 54% работников обладают специальными профильными знаниями в области ИБ. (Egress Insider Data Breach Survey 2021).

Человеческий фактор

- С 2016 года число инцидентов, связанных с инсайдерскими угрозами, увеличилось в три раза (Cost of Insider Threats Global Report, Ponemon Institute).
- 59% ИБ-руководителей ожидают, что число инсайдерских рисков вырастет в течение следующих двух лет (2021 Data Exposure Report)
- Ущерб от инсайдеров составляет 11,45 млн долларов США для компаний с численностью сотрудников более 1000 человек (2020 Cost of Insider Threats: Global Report).
- 73% корпоративных устройств содержат конфиденциальные данные (2021: Endpoint Risk Report)
- Только 36% российских компаний оснащены DLP-системами для предотвращения внутренних инцидентов (глобальное исследование «СёрчИнформ», 2021 год)

Утечки данных

- Количество записей, скомпрометированных в результате утечек данных, увеличилось на 141% (2020 Year End Data Breach QuickView Report, RiskBased Security).
- Средняя стоимость утечки данных выросла до 4,24 млн долларов. Это самый высокий показатель за последние 17 лет (Cost of a Data Breach Report 2021, Ponemon Institute и IBM Security).
- Количество утечек данных в сфере здравоохранения увеличилось на 55% в 2020 году по сравнению с предыдущим годом (Healthcare Breach Report 2021, Bitglass).

Утечки данных

- По данным исследования «СёрчИнформ» в 2019 сфера здравоохранения лидировала по количеству утечек – на нее пришлось 69%. При этом половина организаций замалчивали факт происшествия (глобальное исследование «СёрчИнформ», 2019 год).
- Среднее время выявления утечки данных и устранения последствий инцидента составило 280 дней (Cost of a Data Breach Report 2020, Ponemon Group и IBM Security).
- В 2021 году в сфере здравоохранения произошло более 250 утечек данных, в результате которых 17 млн записей с медицинской информацией оказались в открытом доступе (DHS Breach Portal).

Фишинг

- Ежедневно злоумышленники отправляют 3 млрд фишинговых писем (Email Fraud Landscape: Spring 2021, Valimail).
- Каждый четвертый сотрудник на работе открывал фишинговое письмо (Email Fraud Landscape: Spring 2021, Valimail).
- Фишинг был причиной 36% всех утечек данных (2021 Data Breach Investigations Report, Verizon).
- Количество BEC-атак увеличилось на 35% в 2020 году по сравнению с 2019 годом (Statista).

Программы-вымогатели

- Число атак с использованием программ-вымогателей увеличилось на 250% в первой половине 2021 года (Global Security Report: Rapid Increase in Ransomware Threats Drives Need for Security Controls That Speed the Kill Chain, Venafi).

- В 2019 году 32% атак с использованием программ-вымогателей произошло в сфере энергетики и коммунальных услуг, по 14% атак происходили в госорганах и производственных организациях (2020 Cybersecurity Outlook Report, VMware/Carbon Black).

Интернет вещей (IoT)

- Количество вредоносных программ для атак на IoT-устройстваё увеличилось на 700% (Zscaler).

- Кибератаки на IoT-устройства увеличились на 35% в первой половине 2020 года (Microsoft Digital Defense Report 2020: Cyber Threat Sophistication on the Rise)

- Устройствам IoT по-прежнему не хватает средств защиты (2020 Consumer Threat Landscape Report)

Цифровая гигиена

- 63% руководителей высшего звена сообщили, что их сотрудники оставляли конфиденциальные документы в открытом доступе (Data Protection Report 2020, Shred-it).
- 57% сотрудников хранят пароли на стикерах на рабочем столе (Workplace Password Malpractice Report 2021, Keeper Security).
- Почти 24% людей использовали 1 в конце своего пароля (Unmasked: What 10 million passwords reveal about the people who choose them, WP Engine).
- 66% людей в основном или всегда используют один и тот же пароль (Psychology of Passwords, LogMeIn).

Цифровая гигиена

- В пятерку наиболее часто используемых паролей входят: 123456, 123456789, qwerty, password, 12345 (The top 10 most common passwords worldwide, CyberNews).
- 44% сотрудников повторно используют пароли в личных и рабочих учетных записях (Workplace Password Malpractice Report 2021, Keeper Security).
- 51% пользователей и 49% ИТ-специалистов иногда или часто делятся паролями с коллегами (The 2020 State of Password and Authentication Security Behaviors Report, Yubico).
- 55% людей не используют двухфакторную аутентификацию (The 2020 State of Password and Authentication Security Behaviors Report, Yubico).

Удаленка

- 54% опрошенных ИТ-руководителей считают, что удаленная работа увеличивает инсайдерскую угрозу (Egress Insider Data Breach Survey 2021, Egress).
- 20% организаций столкнулись с нарушением правил безопасности сотрудниками, которые работают на удаленке (Enduring from home, Malwarebytes).
- 56% сотрудников используют персональный компьютер при работе из дома; 25% не знают протоколы безопасности; 20% сотрудников заявили, что их ИТ-отдел не давал советов по работе из дома (2020 WFH Employee Cybersecurity Threat Index, Morphisec).
- Три четверти сотрудников сообщили, что распечатывают рабочие документы дома (Data Protection Report 2020, Shred-it).

Предотвращение инцидентов

- Только 29% компаний из списка Fortune 100 обучают сотрудников основам киберграмотности, это на 11% больше, чем в 2018 году (What companies are disclosing about cybersecurity risk, EY).
- 24% руководителей и 54% владельцев малого бизнеса не проходят регулярного обучения основам информационной безопасности (Data Protection Report 2020, Shred-it).
- Меньше половины компаний в России внедряют в свою работу серьезные средства защиты от кибератак, а большинство обходится только антивирусом (глобальное исследование «СёрчИнформ», 2021 год).

Глобальные траты на ИБ в 2021-2023 гг.

Класс решений	Расходы 2021г., $млн	Рост 2021/2020	Расходы 2022г., $млн	Рост 2022/2021	Расходы 2023, $млн	Рост 2023/2022
Класс решений	**Расходы 2021г., $млн**	Рост 2021/2020	**Расходы 2022г., $млн**	Рост 2022/2021	**Расходы 2023, $млн**	Рост 2023/2022
Безопасность приложений	**4 963**	20,8%	**6 018**	21,3%	**7 503**	24,7%
Облачная безопасность	**4 323**	36,3%	**5 276**	22,0%	**6 688**	26,8%
Защита персональных данных	**1 140**	14,2%	**1 264**	10,8%	**1 477**	16,9%
Безопасность данных	**3 193**	6,0%	**3 500**	9,6%	**3 997**	14,2%
Системы идентификации и управления доступом	**15 865**	22,3%	**18 019**	13,6%	**20 746**	15,1%
Защита инфраструктуры	**24 109**	22,5%	**27 408**	13,7%	**31 810**	16,1%
Комплексное управление рисками	**5 647**	15,4%	**6 221**	10,1%	**7 034**	13,1%
Оборудование сетевой защиты	**17 558**	12,3%	**19 076**	8,6%	**20 936**	9,7%
Другое ПО	**1 767**	26,2%	**2 032**	15,0%	**2 305**	13,4%
ИБ-сервисы	**71 081**	9,2%	**71 684**	0,8%	**76 468**	6,7%
Потребительское ПО	**8 103**	13,7%	**8 659**	6,9%	**9 374**	8,3%
Итого:	**157 749**	14,3%	**169 157**	7,2%	**188 338**	11,3%

Источник: Gartner, 2022

Отчет

- **Аналитический отчет о киберугрозах: итоги 2023 года (25.01.2024)**
- Центр информационной безопасности компании «Инфосистемы Джет» представил аналитический отчет о киберугрозах, зафиксированных в течение 2023 года
- https://jetcsirt.su/upload/godovoy_otchet__jet_2023.pdf

Тренды на 2024 год

Тренды 2024

- ИБ-службы будут бояться инцидентов больше, чем регуляторов
- Рынок взрослеет
- Оценка рисков остается в приоритете
- Вместе с утечками персональных данных растут репутационные риски компаний
- Будет развиваться практика оборотных штрафов за утечку персональных данных
- Самым уязвимым звеном ИБ останется человек
- Главные векторы атак: социальная инженерия, рассылка вредоносов, троянов, шифровальщиков
- Единственной панацеей от этого всего могут быть бэкапы бэкапов
- Ожидаем дальнейший рост DDoS-атак
- Инструментарием хакеров станут дипфейки и цифровые личности
- Ботнеты продолжат работать внутри России

Какие темы мы будем рассматривать в данном курсе

Укрупненные тематики

- **Тема 1.** Основы информационной безопасности, методов и средств защиты информации
- **Тема 2.** Правовое и нормативное обеспечение защиты информации
- **Тема 3.** Защита персональных данных
- **Тема 4.** Угрозы информационной безопасности
- **Тема 5.** Управление рисками информационной безопасности
- **Тема 6.** Политика информационной безопасности в организациях
- **Тема 7.** Критическая инфраструктура. Критическая информационная инфраструктура
- **Тема 8.** Идентификация, аутентификация и авторизация
- **Тема 9.** Криптография
- **Тема 10.** Электронная цифровая подпись
- **Тема 11.** Защита информации в операционных системах
- **Тема 12.** Сетевые атаки и защита информации в компьютерных сетях
- **Тема 13.** Защита internet ресурсов, сайтов, OWAPS

Защита информации

Тема: Основы информационной безопасности, методов и средств защиты информации

Благодарю за внимание

КУТУЗОВ Виктор Владимирович

Белорусско-Российский университет, Кафедра «Программное обеспечение информационных технологий»
Республика Беларусь, Могилев, 2024