

# О СПИКЕРЕ

Куличкин Артём Александрович



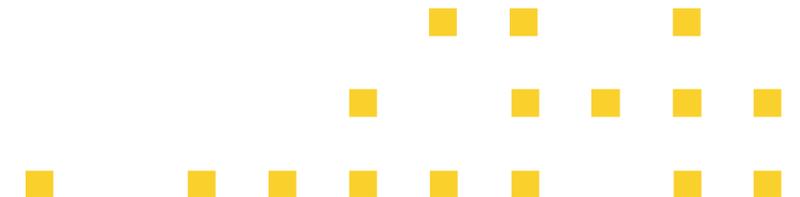
Руководитель ИБ ДЗО группы компаний.

Об опыте:

10 лет опыта в сфере информационной безопасности.

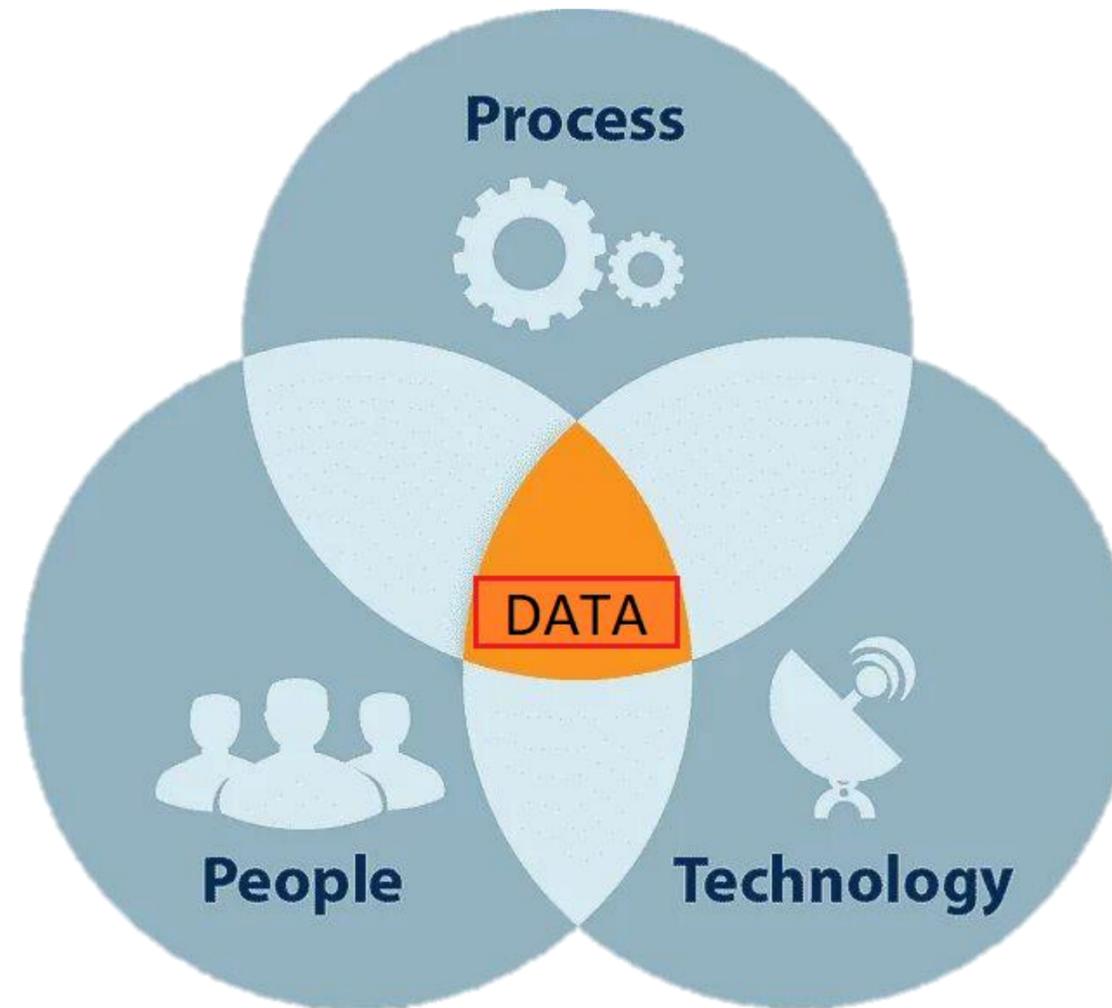
Эксперт по информационной безопасности (Certified Ethical Hacker).

Телефон / эл. почта / соц. сети: +79171110055, [info@kubich.ru](mailto:info@kubich.ru),  
@kulichkin



# Система управления ИБ

1. Технологии
2. Процессы
3. Данные
4. Люди



# Система управления ИБ



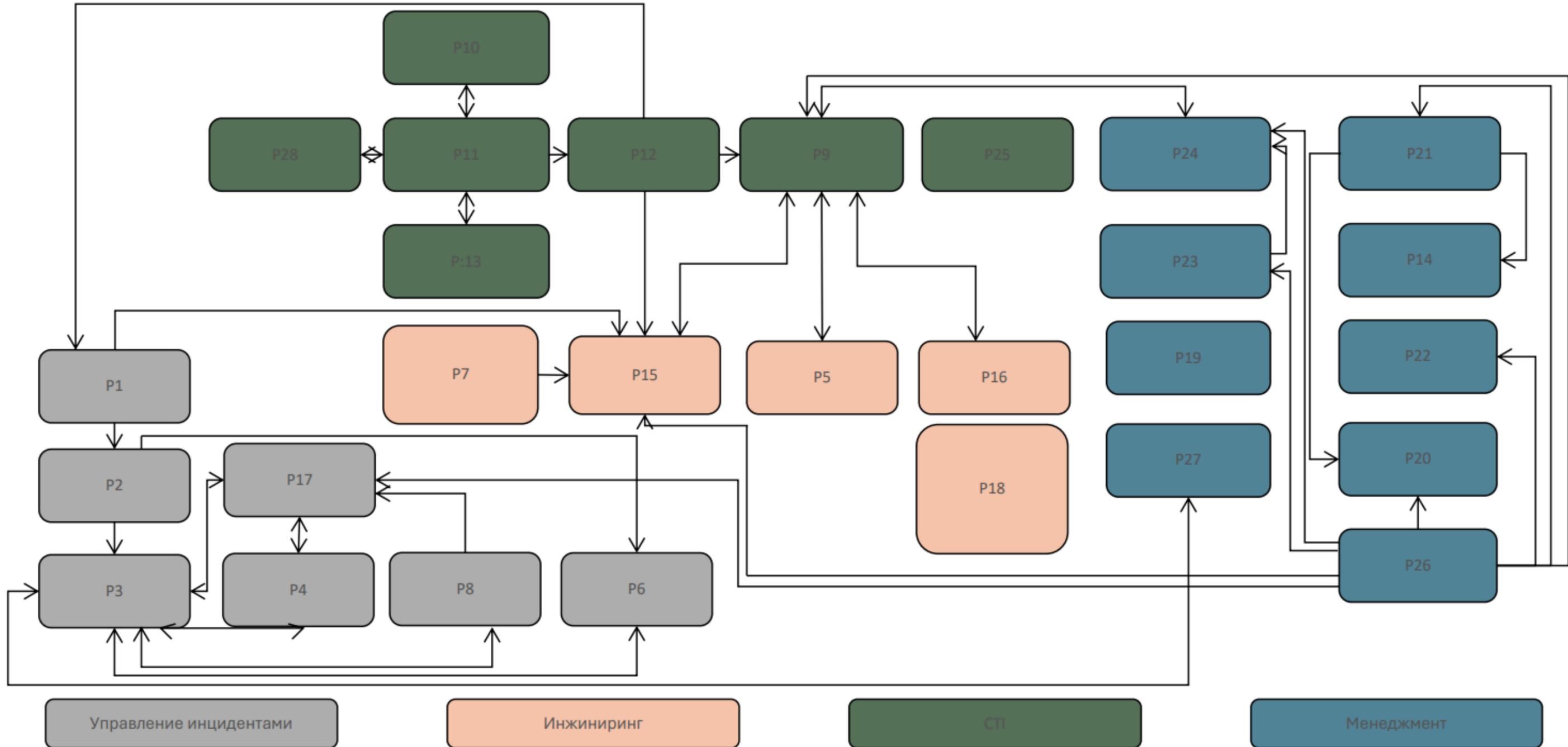
## Нормативная база (пример)

Области управления:

- Управление ИБ
- Управление рисками ИБ
- Защита информации
- Управление доступом
- Защита автоматизированных систем
- Защита инфраструктуры
- Противодействие мошенничеству
- Управление инцидентами и уязвимостями
- Криптозащита
- Непрерывность бизнеса

# Система управления ИБ

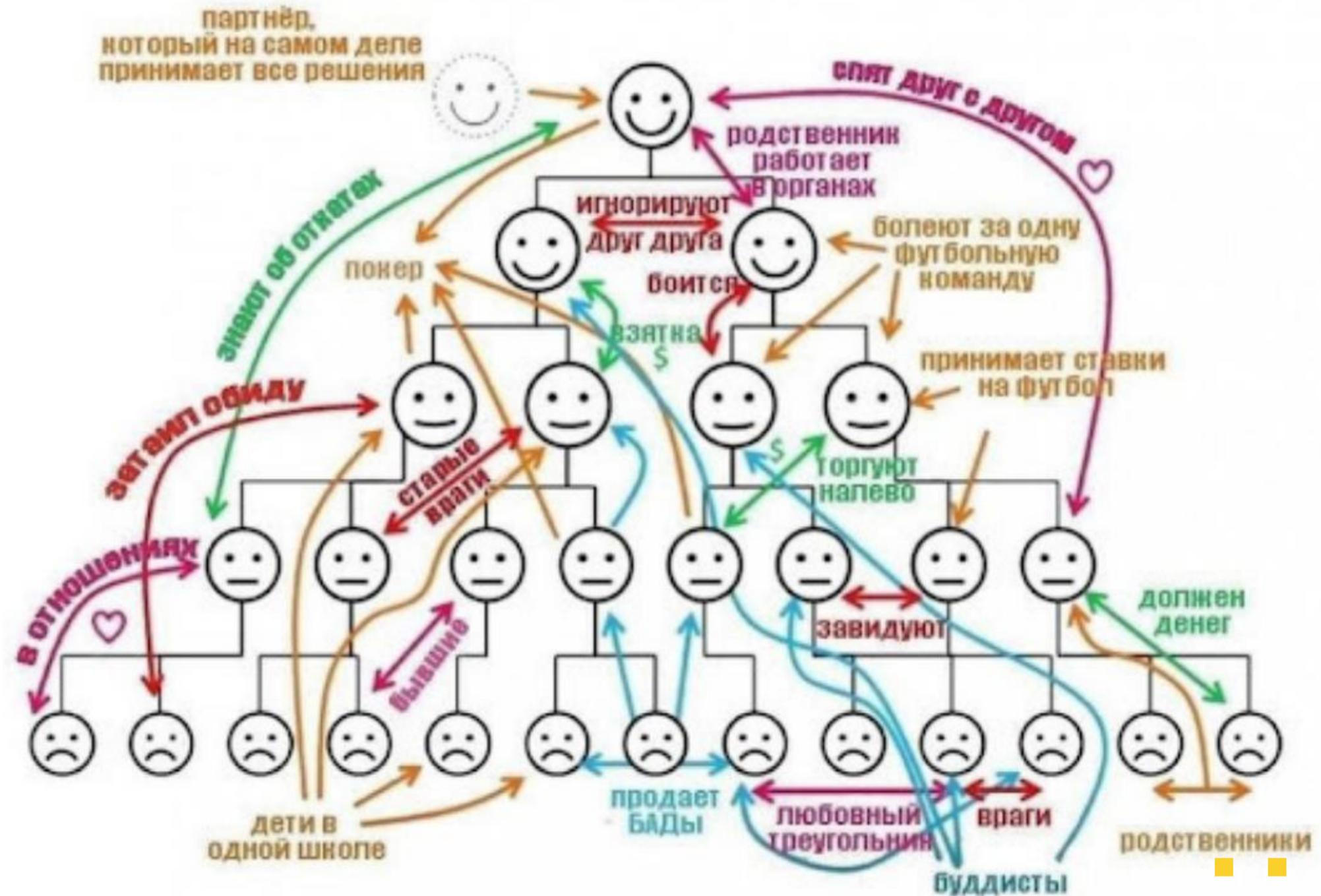
## Процессы



# Система управления ИБ

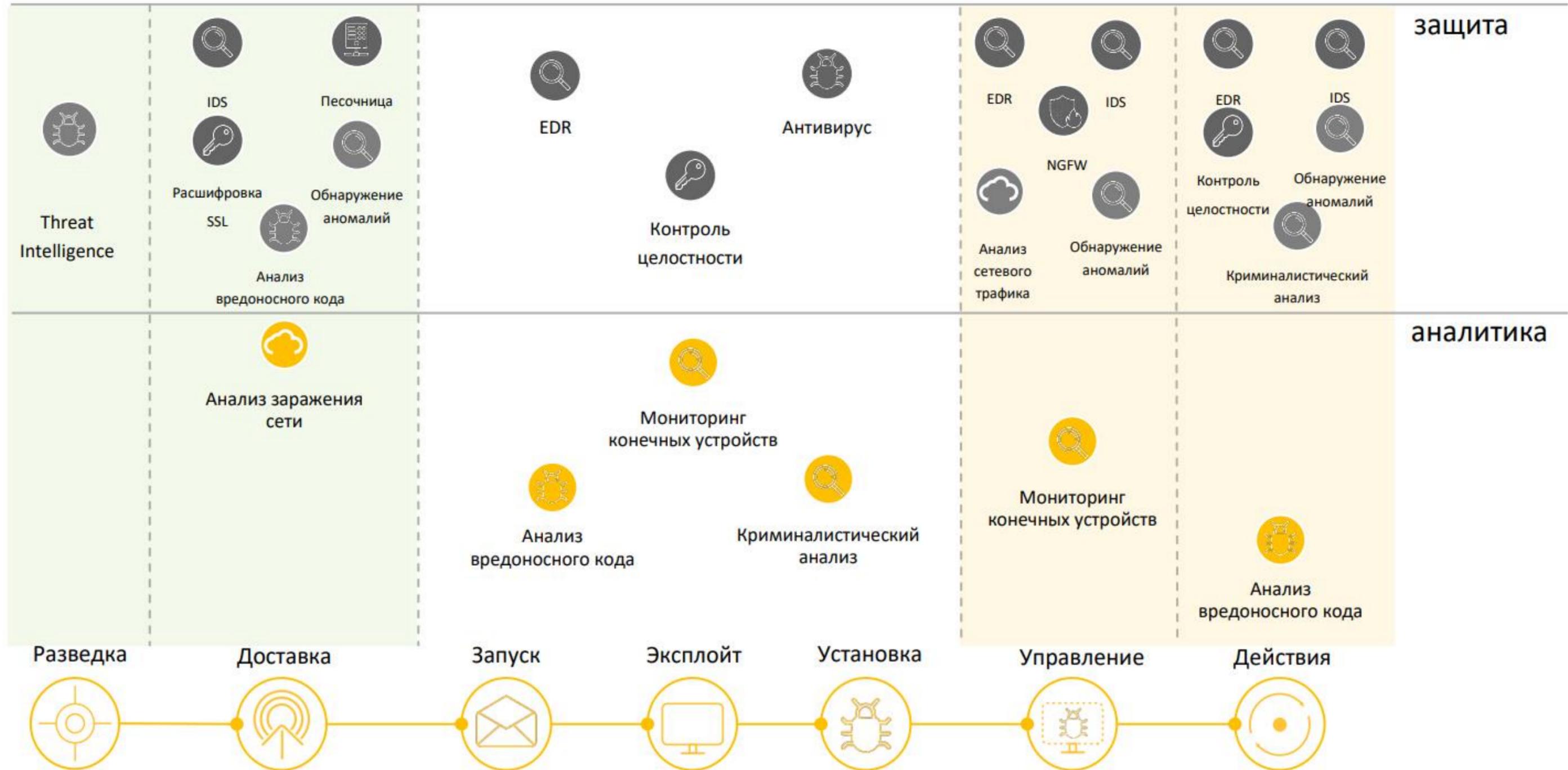
## Люди

- Гибкая организационная структура
- Система материальной и нематериальной мотивации
- Непрерывное обучение и развитие hard и soft skills
- Тренинги коммуникаций и публичных выступлений



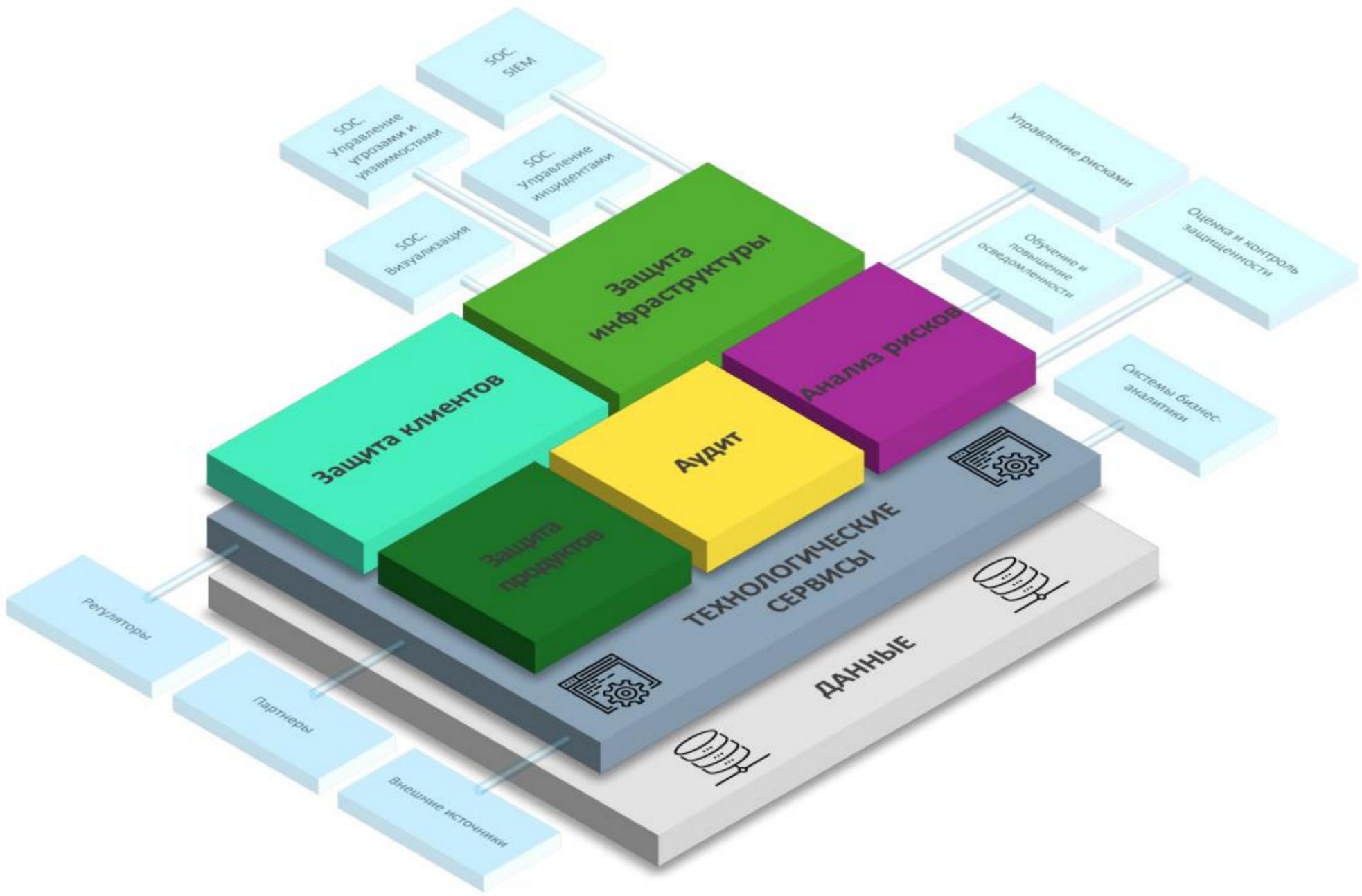
# Система управления ИБ

## Технологии



# Система управления ИБ

Данные



# ИТ vs ИБ



# ИТ vs ИБ

Управление архитектурой	Управление архитектурой организации	Управление персоналом и талантами	Актуализация квалификационных требований Планирование мероприятий по повышению квалификации персонала Мониторинг деятельности и отчетность	Управление рисками	Анализ рисков с точки зрения бизнеса Анализ рисков с точки зрения ИТ Оценка риска Деятельность по предотвращению риска Мониторинг рисков и отчетность
Непрерывное улучшение и управление качеством ИТ	Планирование деятельности Управление улучшениями и качеством Координация процессов Контроль процессов Предоставление отчетности	Управление доступностью	Планирование и мониторинг доступности Тестирование доступности Отчетность о доступности	Управление конфигурацией сервисов	Организация управление конфигурацией Идентификация элемента конфигурации Аудит и отчетность по управлению конфигурацией
Управление информационной безопасностью	Внедрение контролей безопасности Валидация ИТ-безопасности Обзор безопасности и отчетность	Бизнес-аналитика	Бизнес-анализ Управление профилями пользователей Прогнозирование емкости Мониторинг емкости и производительности	Управление непрерывностью обслуживания	Организация управление конфигурацией Идентификация элемента конфигурации Аудит и отчетность по управлению конфигурацией Планирование действий в чрезвычайных ситуациях Тренировки действий в условиях катастрофы Обзор и отчетность по управлению непрерывностью обслуживания
Управление знаниями	Управление знаниями	Управление мощностями и эффективностью деятельности	Отчетность о емкости и производительности	Проектирование услуг	Планирование действий в чрезвычайных ситуациях Тренировки действий в условиях катастрофы Обзор и отчетность по управлению непрерывностью обслуживания Организация проектирования услуг Планирование проектирования услуг Мониторинг проектирования услуг Техническое и организационное проектирование услуг Пересмотр дизайна услуг
Метрики и отчетность	Обзор сервисов Обзор процессов	Управление изменениями	Организация контроля за изменениями Регистрация и классификация изменений Оценка изменений Планирование изменений Оценка изменений до планирования Оценка изменений до реализации Оценка изменений перед развёртыванием Оценка изменений после развёртывания Обзор изменений и отчетность	Служба поддержки	Регистрация инцидентов и заявок Решение на первом уровне Организация управления уровнем сервиса Требования к уровню сервиса Соглашения об уровне сервиса Одобрение уровня сервиса Пересмотр уровня сервиса и отчетность
Управление организационными изменениями	Управление организационными изменениями	Управление инцидентами	Организация управления инцидентами Поиск и устранение неисправностей второго уровня Мониторинг инцидентов и эскалация Управление масштабными инцидентами Отслеживание инцидентов и закрытие Информирование пользователей Отчетность об инцидентах	Управление уровнем сервиса	Требования к уровню сервиса Соглашения об уровне сервиса Одобрение уровня сервиса Пересмотр уровня сервиса и отчетность
Управление портфелем	Подготовка к проектированию услуг Начало проектирования услуг Обзор и обслуживание портфеля услуг Создание проекта	Управление ИТ-активами	Идентификация ИТ-активов Инвентаризация ИТ-активов	Управление запросами на обслуживание	Запрос на услугу Запрос на восстановление резервной копии Включение и исключение из списков Запрос разрешения пользователя Определение процедур тестирования Тестирование компонентов Интеграционное тестирование Приемочное тестирование
Управление проектами	Планирование проекта Контроль над проектом	Мониторинг и управление событиями	Организация мониторинга и управления событиями Мониторинг событий Отслеживание и закрытие событий Регистрация проблемы Решение проблемы Отслеживание и закрытие проблемы Обзор крупных проблем Отчетность о проблемах	Проверка и тестирование услуг	Определение процедур тестирования Тестирование компонентов Интеграционное тестирование Приемочное тестирование
Управление отношениями	Забота о клиентах Прогноз потребностей Контроль потребностей Заключение контракта на стандартное ИТ-услуги Изучение удовлетворенности клиентов Управление отзывами клиентов Мониторинг жалоб клиентов	Управление проблемами	Организация управления выпуском релизов Подготовка релиза Поддержка при запуске и закрытие релизов Окончание срока службы для ИТ-услуг Отчетность о переходе	Управление развертыванием	Развертывание Минорное развертывание Определение портфеля ИТ-технологий Управление портфелем ИТ-технологий Управление ИТ-операциями Непредвиденные действия
Управление финансами	Финансовая организация ИТ Бюджетирование ИТ Прогноз развития ИТ Мониторинг ИТ-расходов Счет-фактуры за ИТ-услуги Анализ прибыльности ИТ Финансовая отчетность ИТ	Управление релизами	Управление каталогом сервисов	Управление инфраструктурой и платформами	Непредвиденные действия Разработка и настройка приложений
Управление стратегией	Оценка стратегии ИТ Концепция стратегии ИТ Внедрение стратегии ИТ	Управление каталогом сервисов	Управление каталогом сервисов	Разработка и управление программным обеспечением	Разработка и настройка приложений
Управление поставщиками	Организация управления поставщиками Оценка поставщиков Подготовка договоров с поставщиками Запрос требований Выбор поставщиков Управление жизненным циклом для контрактов с поставщиками Обзор поставщиков и отчетность				

ключевые с точки зрения ИБ

\* в соответствии с ITIL v 4

ИТ vs ИБ

Диалог



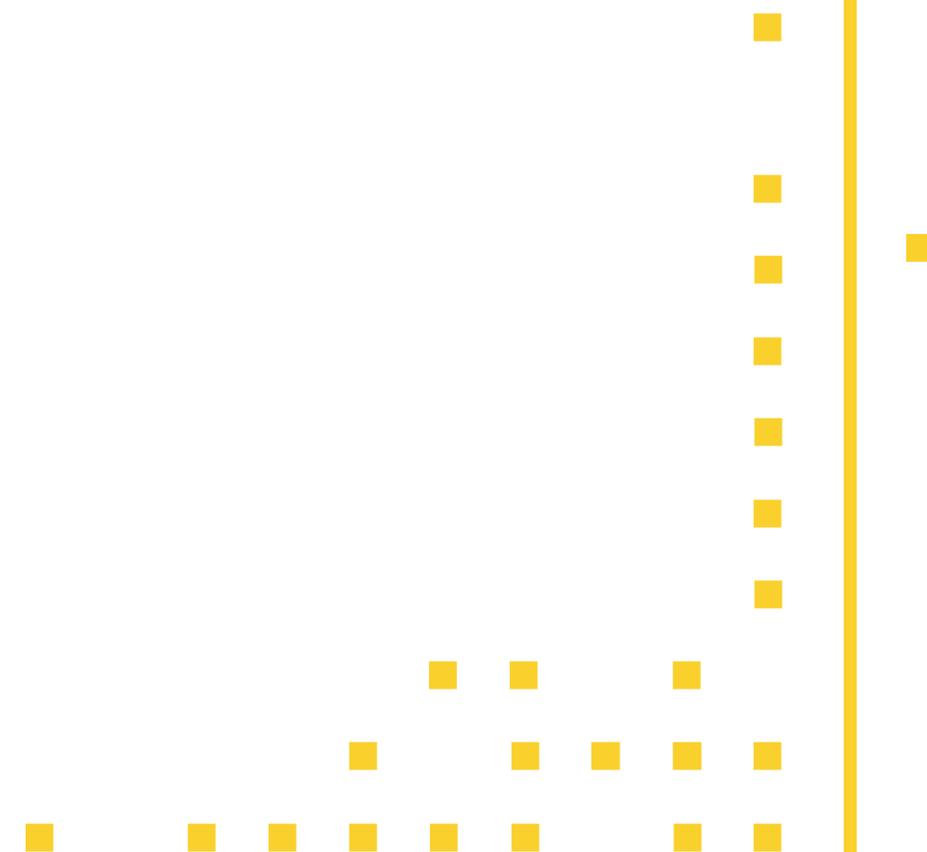
# ИТ vs ИБ

показывает на каком уровне опровержений находится ваш оппонент, позволяет отделить зерна от плевел и сосредоточиться не на словах, а на том, что они собой несут и зачем произнесены

# Пирамида Грэма



# Что такое политика ИБ



# Что такое политика ИБ?

## ChatGPT



### ChatGPT

Политика информационной безопасности (ПИБ) обычно представляет собой документ, который определяет общие принципы, цели, правила и процедуры, которые должны быть соблюдены в организации для обеспечения безопасности информации. Вот примерное содержание, которое может включать политика информационной безопасности:

1. Введение: Осознание важности ИБ.
2. Цели: Защита конфиденциальности, целостности и доступности информации.
3. Область применения: Применение политики ко всей информации и сотрудникам.
4. Принципы: Соблюдение конфиденциальности, целостности и доступности информации.
5. Обязанности: Описать роли и ответственность сотрудников.
6. Политика использования: Правила использования информационных ресурсов.
7. Политика доступа: Управление правами доступа к информации.
8. Обработка информации: Правила обработки, хранения и уничтожения данных.
9. Обучение: Обучение персонала по безопасности.
10. Соблюдение и аудит: Проверка соблюдения политики и аудит безопасности.
11. Разработчики и поставщики: Требования к безопасности при разработке и приобретении продуктов.
12. Исполнение и изменения: Механизмы внедрения и изменения политики.

# Что такое политика ИБ?

## Политика ИБ

- Краткий, очень емкий документ, максимум 5 страниц
- Обозначает основные области управления, дает отсылки на другие политики и документы
- Служит основным инструментом в разрешении сложных ситуаций на уровне СХО, часто читается и пересматривается

- Документ «средней тяжести», 10-20 страниц
- Описывает и раскрывает основные области управления, дает отсылки на другие документы
- Служит основным инструментом для разрешения сложных ситуаций в основном между ИБ и ИТ

- «Тяжелый» документ, 50+ страниц
- Описывает все, что автор считает нужным описать
- Используется в случае расследований и наказаний

**GOLD**

**SILVER**

**BRONZE**

# Расскажите про организацию

---

- Название
- Вид деятельности, приносящий основной доход
- Организационная и территориальная структура
- Кто ваши клиенты
- С какими данными работаете
- Характеристики ИТ-инфраструктуры
- Партнеры, контрагенты

... все прочее, что считаете нужным



# Cloud Provider

Наша миссия - предоставление надежных и безопасных облачных решений, которые помогают малым и средним предприятиям эффективно управлять своими цифровыми ресурсами и защищать их от киберугроз.  
Наши клиенты - малые и средние предприятия, которые нуждаются в безопасных облачных решениях для хостинга, онлайн-офисов, дизайна сайтов.



## Ключевые цели:

1. Поддержание высокого уровня удовлетворенности клиентов
2. Обеспечение высокой доступности и отказоустойчивости всех предоставляемых услуг
3. Развитие инновационных технологий для улучшения качества предоставляемых услуг
4. Обеспечение высокого уровня безопасности и защиты данных клиентов
5. Расширение клиентской базы и увеличение доли рынка

## Организационная и территориальная структура:

- Головной офис - отвечает за стратегическое управление, маркетинг, финансы и юридические вопросы. Включает в себя: отдел стратегического планирования, финансовый отдел, юридический отдел, отдел маркетинга и продаж, отдел кадров
- Центр обработки данных (ЦОД) - обеспечивает хостинг, управление серверами и поддержание инфраструктуры. Включает в себя: отдел эксплуатации инфраструктуры, отдел мониторинга и управления инцидентами, отдел поддержки и обслуживания клиентов
- Технический центр - занимается разработкой и поддержкой программного обеспечения, а также исследованиями и разработками (R&D). Включает в себя: отдел разработки программного обеспечения, отдел исследований и разработок, техническая поддержка
- Региональные представительства - обеспечивают местную поддержку клиентов и привлечение новых клиентов. Включают в себя региональных менеджеров по продажам и местную поддержку клиентов

## Данные, с которыми работает компания:

1. Личные данные клиентов (контактная информация, учетные записи, платежные данные)
2. Данные веб-приложений и сайтов клиентов
3. Лог-файлы и данные мониторинга
4. Данные для антивирусной проверки и защиты от DDoS-атак

## Характеристики ИТ-инфраструктуры:

- Серверные мощности: Высокопроизводительные серверы с балансировкой нагрузки и отказоустойчивостью
- Сетевое оборудование: Высокоскоростные маршрутизаторы и коммутаторы с защитой от DDoS-атак
- Системы хранения данных: Надежные и масштабируемые системы хранения данных с резервным копированием
- Информационная безопасность: Продвинутые системы защиты веб-приложений, антивирусные системы, межсетевые экраны (firewalls) и системы обнаружения вторжений (IDS/IPS)
- Системы мониторинга и управления: Инструменты для мониторинга производительности, управления инцидентами и отчетности

## Партнеры и контрагенты:

1. Производители оборудования
2. Поставщики программного обеспечения
3. Интернет-провайдеры
4. Консалтинговые и аутсорсинговые компании
5. Образовательные учреждения

Структура дохода:



■ Хостинг   ■ Офис  
■ Услуги ИБ   ■ Дизайн

# Политика ИБ GOLD

- Миссия, цели и задачи
- Описание объекта защиты
- Основные области управления с отсылками на документы
- Структура управления
- Полномочия участников
- Ключевые технологии
- Соответствие требованиям
- Взаимодействие с внешними сторонами
- Порядок утверждения и пересмотра

... и все, что посчитаете нужным

# Cloud Provider

Наша миссия в информационной безопасности - предоставление надежных и безопасных облачных решений, защищающих данные и информационные ресурсы наших клиентов, обеспечивая их высокую доступность и целостность. Мы стремимся способствовать росту и успеху малого и среднего бизнеса, предоставляя безопасные и инновационные IT-услуги, которые повышают их конкурентоспособность на рынке.

## Цели и задачи информационной безопасности:

1. Обеспечение конфиденциальности, целостности и доступности информации.
2. Защита данных клиентов от несанкционированного доступа и киберугроз.
3. Поддержание высокого уровня информационной безопасности в соответствии с международными стандартами.
4. Содействие бизнес-целям компании, минимизируя риски информационной безопасности.
5. Обеспечение высокой удовлетворенности клиентов через надежные и безопасные сервисы.

## Описание объекта защиты:

- Объектом защиты являются информационные ресурсы компании и ее клиентов, включая данные, программное обеспечение, оборудование и сетевые ресурсы.

## Основные области управления:

- Управление рисками и соответствием: Определение, анализ и снижение рисков.
- Контроль доступа: Управление правами доступа к информации.
- Обучение и осведомленность: Повышение уровня осведомленности сотрудников о вопросах безопасности.
- Управление уязвимостями: Аудит информационных систем на наличие уязвимостей
- Управление инцидентами: Процедуры реагирования на инциденты безопасности
- Защита приложений, инфраструктуры, сети и данных

## Структура управления:

- Комитет по информационной безопасности: Высший орган, определяющий стратегию и политику безопасности.
- Главный специалист по информационной безопасности (CISO): Ответственен за реализацию политики безопасности и управление процессами безопасности.
- Отдел информационной безопасности: Выполняет оперативные задачи по обеспечению безопасности.

## Полномочия участников:

- Комитет по информационной безопасности: Утверждение и пересмотр политики.
- CISO: Разработка и внедрение мер безопасности, контроль соблюдения политики.
- Сотрудники отдела информационной безопасности: Реализация процедур безопасности, мониторинг и аудит.

## Ключевые технологии:

- Межсетевые экраны (firewalls) и системы обнаружения вторжений (IDS/IPS).
- Антивирусные программы и антиDDoS-защита.
- Системы резервного копирования и восстановления данных.
- Шифрование данных и управление ключами.

## Соответствие требованиям:

- ISO/IEC 27001: Стандарт управления информационной безопасностью.
- GDPR: Общий регламент по защите данных.
- PCI DSS: Стандарт безопасности данных индустрии платежных карт.

## Взаимодействие с внешними сторонами:

- Партнеры и контрагенты: Соглашения о конфиденциальности и требования безопасности.
- Клиенты: Обеспечение безопасности данных клиентов и выполнение их требований.
- Регулирующие органы: Соответствие законодательным и нормативным требованиям.

## Порядок утверждения и пересмотра:

- Политика утверждается Комитетом по информационной безопасности.
- Пересмотр политики осуществляется ежегодно или по мере необходимости при изменении условий.
- Все изменения утверждаются Комитетом и доводятся до сведения всех сотрудников компании.

Дата утверждения: [дата]  
Утверждено: [ФИО, должность]

# Чем отличается риск от угрозы?

## ChatGPT

Угроза информационной безопасности — это потенциальная опасность, которая может причинить вред информационным системам или данным. Угрозы могут исходить от различных источников, включая внутренние и внешние акторы, а также могут быть намеренными или ненамеренными. Вот несколько примеров угроз информационной безопасности:

## ChatGPT

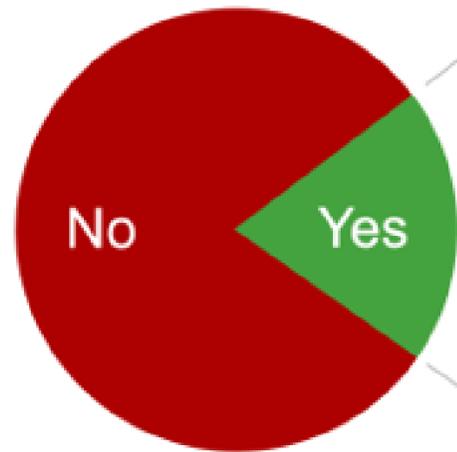
Риск информационной безопасности — это потенциальная возможность возникновения угрозы, которая может привести к ущербу или потере информации в результате воздействия на информационные системы или сети. Этот риск связан с вероятностью того, что угроза реализуется и причинит вред, а также с последствиями, которые этот вред может иметь для организации, индивидуума или системы.

В контексте информационной безопасности учитываются различные типы угроз, включая:

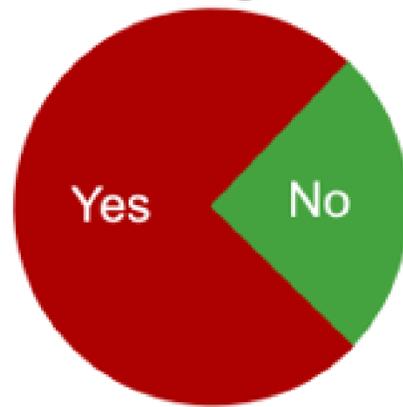
1. **Киберпреступность:** Включает атаки, такие как взлом, вирусы, троянские программы, фишинг и распространение вредоносного ПО. Цели таких атак — кража данных, дестабилизация систем или вымогательство.
2. **Инсайдерские угрозы:** Действия сотрудников или контрагентов, которые могут привести к несанкционированному доступу к данным или системам, утечке информации или другому вреду из-за недосмотра или намеренных действий.
3. **Физические угрозы:** Включают угрозы физической безопасности оборудования или данных, такие как кража оборудования, пожары или стихийные бедствия.
4. **Технические сбои:** Сбои оборудования или программного обеспечения, которые могут привести к потере данных или временному прекращению функционирования системы.
5. **Социальная инженерия:** Методы обмана или манипуляции, направленные на получение конфиденциальной информации.

1. **Кибератаки:** Взломы, вирусы, троянские программы, фишинг и другие формы кибернетической агрессии, направленные на несанкционированное извлечение, изменение или уничтожение данных.
2. **Технические сбои:** Отказ оборудования, программного обеспечения или ошибки в настройке систем безопасности могут прив

Clients That Have  
a **Risk** Register



**Risk** Registers  
That Are Actually  
**Threat** Registers



But  
you may say  
aren't  
**Risks**  
and  
**Threats**  
the same thing?

**Threats** cannot be controlled

**Risks** can  
or rather  
they can be mitigated

*Угроза* просто описывает нам что-то плохое, в то время как *Риск* еще сообщает из-за чего это плохое может произойти.

Несколько примеров рисков, сформулированных по такой конструкции:

- *Раскрытие ключей (паролей) доступа из-за возможности атаки SMB Relay в ОС Windows*  
Тут у нас
  - *Угроза* – Раскрытие ключей (паролей) доступа
  - *Уязвимость* – Возможности атаки SMB Relay
  - *Актив* – ОС Windows
- *Боковое перемещение злоумышленника по локальной сети из-за возможности удаленного подключения через RDS Shadow в ОС Windows*
- *Закрепление злоумышленника в ОС из-за возможности распространения скриптов через Network Logon Scripts в доменных службах Active Directory*
- *Заражение вредоносным программным обеспечением из-за реагирования на мошеннические, фишинговые письма работником*  
// В качестве актива выступает человек
- *Неработоспособность серверного оборудования из-за нарушения температурного режима в серверном помещении*  
// классический ИТ риск на доступность активов

## Реестр рисков

Модель наруу

Риски / Реестр

**Текущий риск**  
Данные отсутствуют  
[Авторизуйтесь](#)

КЦД

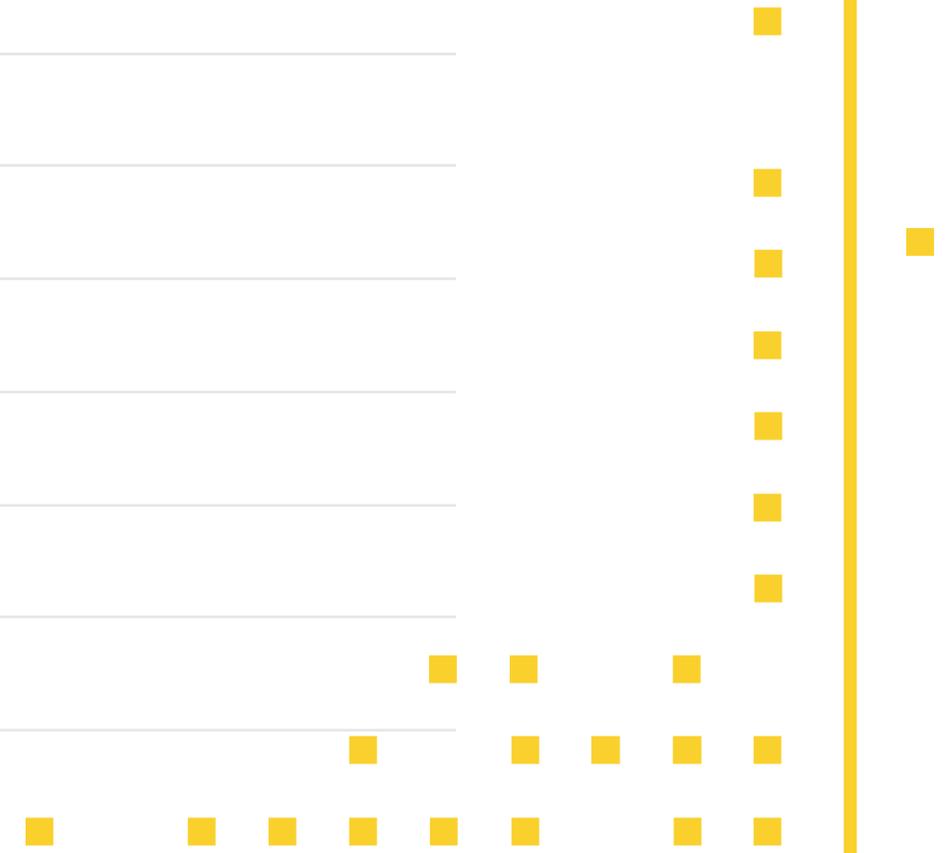
STRIDE

**Риск**  
Данные отсутствуют  
[Авторизуйтесь](#)

**Риск-аппетит**  
Данные отсутствуют  
[Авторизуйтесь](#)

### Риск

Закрепление злоумышленника в ОС из-за возможности изменения программы по умолчанию для открытия файла в ОС Windows Повышение привилегий НСД	
Повышение привилегий в ОС из-за возможности изменения программы по умолчанию для открытия файла в ОС Windows Повышение привилегий Целостность	
Раскрытие ключей (паролей) доступа из-за возможности поиска учетных данных в истории Bash в ОС Linux Конфиденциальность Повышение привилегий Раскрытие информации Подмена пользователя	
Раскрытие ключей (паролей) доступа из-за возможности поиска учетных данных в истории Bash в ОС macOS Конфиденциальность Повышение привилегий Раскрытие информации Подмена пользователя	
Неработоспособность информационной системы из-за возможности удаления учетных записей в доменных службах Active Directory Доступность Отказ в обслуживании	
Раскрытие ключей (паролей) доступа из-за возможности автоматической аутентификации в ОС Windows Конфиденциальность Повышение привилегий Раскрытие информации Подмена пользователя	
Утечка информации из-за возможности доступа к некорпоративным облачным хранилищам в локальной сети Конфиденциальность Раскрытие информации	
Несанкционированное подключение к локальной сети из-за наличия доверительного (неконтролируемого) доступа в ИТ инфраструктуру у контрагента Конфиденциальность Повышение привилегий НСД	



Угроза

### Закрепление злоумышленника в ОС

из-за уязвимости

### Возможность изменения программы по умолчанию для открытия файла

в Активе

### ОС Windows

#### Описание угрозы

После получения доступа к операционной системе злоумышленник может закрепиться в ней и продолжить получать доступ к системе вне зависимости от прерываний доступа.

#### Описание уязвимости

При открытии файла проверяется программа по умолчанию, используемая для открытия файла (так называемая ассоциация файлов). Выбранные ассоциации файлов хранятся в реестре Windows и могут быть отредактированы пользователями, администраторами или программами, имеющими доступ к реестру, или администраторами с помощью встроенной утилиты assoc.

Например, ассоциации системных файлов перечислены в разделе реестра:

```
HKEY_CLASSES_ROOT\[extension]
```

Обработчики указаны по пути:

```
HKEY_CLASSES_ROOT\[handler]
```

Значения перечисленных ключей реестра являются командами, которые выполняются, когда обработчик открывает расширение файла:

```
HKEY_CLASSES_ROOT\[extension]\shell\open\command
```

[Подробнее](#) ↓

Область действия: Вся организация

Объекты атаки [Операционная система](#)

Классификация

STRIDE: [Повышение привилегий](#) ?

Иное: [НСД](#) ?

Источники угрозы

Внутренний нарушитель - Низкий потенциал

#### Описание типа актива

Microsoft Windows любых версий

#### Каталоги

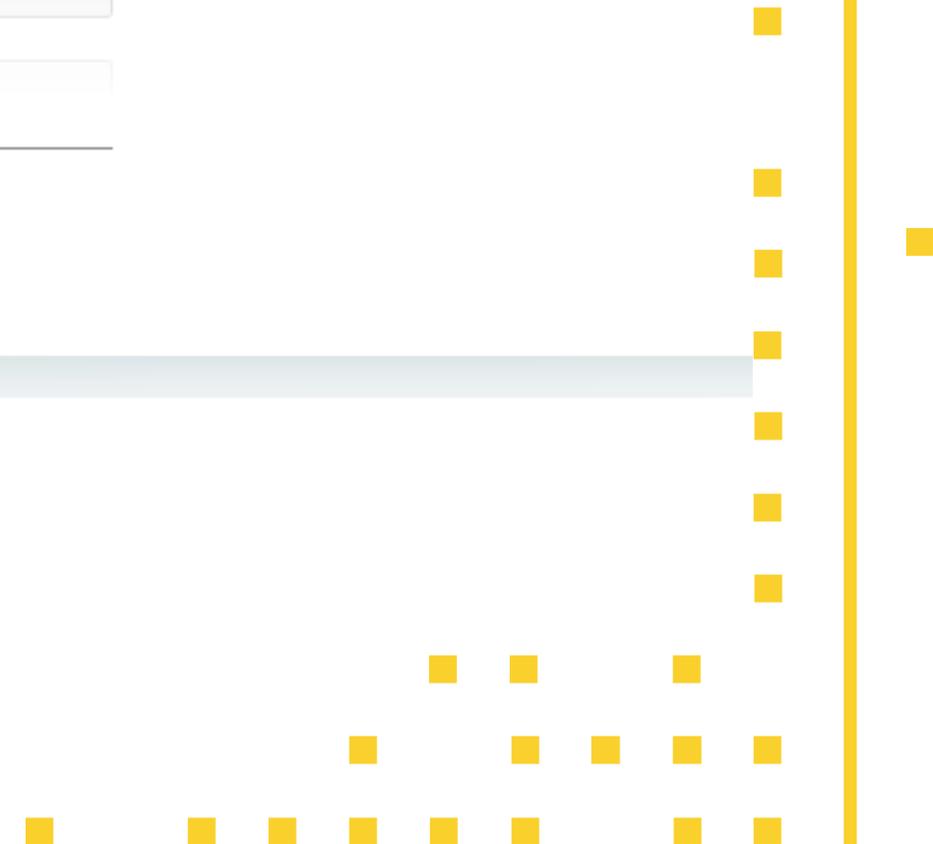
##### БДУ ФСТЭК:

УБИ.015 Угроза доступа к защищаемым файлам с использованием обходного пути ?

Угроза заключается в возможности получения нарушителем доступа к скрытым/защищаемым каталогам или файлам посредством различных в...

##### Техники ATT&CK:

T1546.001 Event Triggered Execution: Change Default File Association



# Что делают с угрозами

## Моделируют

**Threat modeling** — это процесс систематического идентификации, оценки и управления потенциальными угрозами информационной безопасности. Он начинается на ранних этапах разработки системы или приложения и направлен на выявление возможных уязвимостей, а также на разработку стратегий для их снижения или устранения. Этот процесс обеспечивает фундаментальное понимание атакующих поверхностей и потенциальных векторов атак, что служит основой для дальнейших действий по обеспечению безопасности.

## Разведывают

**Threat Intelligence (разведка угроз)** — это процесс сбора, анализа и интерпретации данных о киберугрозах для предсказания, предотвращения и реагирования на атаки. Он включает использование различных источников для получения информации, её анализ для выявления актуальных угроз и создание отчетов с рекомендациями. Основные виды Threat Intelligence включают стратегическую, тактическую, оперативную и техническую разведку. Основная цель — помочь организациям улучшить безопасность, быть проактивными и эффективно защищаться от кибератак.

## Охотятся

**Threat hunting** — это активный поиск скрытых угроз, которые уже могут присутствовать в сети или системе организации. Этот процесс использует информацию из threat intelligence для формирования гипотез о возможных атаках и эксплуатации уязвимостей, которые были выявлены в процессе threat modeling. Threat hunting помогает выявить и устранить реальные угрозы до того, как они причинят ущерб, и обеспечивает ретроспективное понимание уязвимостей, что может стимулировать дополнительные корректировки в threat modeling.

# Уровни моделирования



# Клиентоцентричная безопасность

## Сценарии и контроли (пример)

### Ключевые сценарии риска ИБ\*



Мошеннический вывод денежных средств со счетов клиентов (пользователей).



Утрата или искажение информации в базах данных, масштабное уничтожение контента из медиа сервисов.



Искажение публикуемого контента с целью дестабилизации социально-политической обстановки или работы компании.



Перебои в работе или недоступность платформ и клиентских сервисов, корпоративной инфраструктуры



Утрата исходного кода или внедрение уязвимостей и программных закладок в исходный код разрабатываемых продуктов.



Утечка критичных данных сотрудников, пользователей и клиентов (персональные, финансовые, аутентификационные данные), исходного кода разрабатываемого ПО и иной конфиденциальной информации, представляющей ценность для компании.

### Ключевые контроли риска ИБ\*\*

#### Защита приложений

Влияет на **90%** выявленных сценариев риска

#### Защита данных

Влияет на **84%** выявленных сценариев риска

#### Обучение

Влияет на **80%** выявленных сценариев риска

#### Защита инфраструктуры

Влияет на **84%** выявленных сценариев риска

#### Управление рисками ИБ

Влияет на **69%** выявленных сценариев риска

#### Защита клиентов

Влияет на **49%** выявленных сценариев риска

# Cloud Provider. Модель нарушителя

Нарушитель	Мотивация	Ресурсы	Цели	Методы	Потенциал
Государственные и полугосударственные организации	Шпионаж, национальная безопасность	Высокий уровень технических знаний, значительные финансовые и материальные ресурсы	Кража данных, мониторинг и контроль за деятельностью компании и ее клиентов	Использование сложных техник проникновения, целевые атаки (APT), внедрение вредоносного ПО	Высокий. Значительные ресурсы и технические возможности
Киберпреступники (хакеры)	Финансовая выгода, кража данных, вымогательство	Высокий уровень технических знаний, доступ к специализированным инструментам и эксплойтам	Нарушение работы сервисов, кража конфиденциальной информации, компрометация систем безопасности	Вредоносное ПО, фишинг, эксплойты уязвимостей, DDoS атаки	Высокий. Значительные технические знания и ресурсы
Внутренние нарушители (инсайдеры)	Недовольство, финансовая выгода, шантаж	Легитимный доступ к системам, знание внутренней структуры и процессов	Саботаж, кража данных, передача конфиденциальной информации конкурентам	Злоупотребление правами доступа, кража данных, саботаж	Средний. Доступ к внутренним системам и информации
Конкуренты	Получение конкурентного преимущества, доступ к коммерческой тайне	Финансовые и технические средства, привлечение хакеров	Нарушение работы сервисов, кража коммерческих данных, дискредитация компании	Взлом систем, социальная инженерия, инсайдерская информация	Средний. Привлечение внешних специалистов
Активисты (хактивисты)	Идеологические убеждения, политические или социальные цели	Организованные группы, умеренный уровень технических знаний	Нарушение работы сервисов, дискредитация компании, привлечение внимания к своей идеологии	DDoS атаки, взломы веб-сайтов, распространение пропаганды	Низкий. Ограниченные ресурсы и технические навыки

# Cloud Provider. Модель угроз

Угроза	Описание	Источник (нарушитель)	Способ реализации	Потенциальные последствия	Методы защиты	Уровень угрозы
<b>Кибератаки (DDoS)</b>	Атаки, направленные на перегрузку серверов компании с целью их отключения или снижения производительности	Киберпреступники (хакеры)	Отправка большого объема трафика на сервер	Нарушение доступности услуг, финансовые потери, снижение доверия клиентов	Использование DDoS-защит, настройка фильтров трафика	Высокая степень угрозы
<b>Взлом и несанкционированный доступ</b>	Атаки хакеров с целью получения доступа к конфиденциальным данным клиентов или системы компании	Киберпреступники (хакеры)	Взлом паролей, использование уязвимостей	Утечка данных клиентов, юридические последствия, снижение репутации компании	Двухфакторная аутентификация, регулярные проверки безопасности	Высокая степень угрозы
<b>Вредоносное ПО (вирусы, трояны, шифровальщики)</b>	Внедрение вредоносного программного обеспечения для кражи данных или вымогательства	Киберпреступники (хакеры)	Рассылка вредоносного ПО через почту или зараженные сайты	Потеря данных, нарушение работы сервисов, финансовые потери	Антивирусные программы, обучение сотрудников	Высокая степень угрозы
<b>Фишинг и социальная инженерия</b>	Атаки, направленные на получение конфиденциальной информации путем обмана сотрудников или клиентов	Киберпреступники (хакеры)	Фишинговые письма, телефонные звонки	Утечка данных, компрометация учетных записей	Обучение сотрудников, фильтрация почтового трафика	Средняя степень угрозы
<b>Внутренние угрозы</b>	Злоупотребление доступом или ошибки сотрудников компании	Внутренние нарушители (инсайдеры)	Злоупотребление правами доступа, ошибки в настройках	Утечка данных, нарушение работы систем	Мониторинг действий сотрудников, контроль доступа	Средняя степень угрозы
<b>Уязвимости программного обеспечения</b>	Использование хакерами уязвимостей в программном обеспечении компании	Киберпреступники (хакеры)	Эксплуатация известных уязвимостей	Неавторизованный доступ, компрометация данных, нарушение работы систем	Регулярное обновление ПО, использование средств защиты от уязвимостей	Средняя степень угрозы
<b>Физические угрозы (пожары, наводнения, кражи оборудования)</b>	Физические угрозы, которые могут повредить или уничтожить оборудование и данные компании	Случайные события	Пожары, наводнения, кражи оборудования	Нарушение доступности услуг, финансовые потери	Физическая охрана, резервное копирование данных	Низкая степень угрозы
<b>Отказ оборудования</b>	Поломка серверов или другого критически важного оборудования	Технические причины	Износ оборудования, сбой в электроснабжении	Нарушение доступности услуг, финансовые потери	Регулярное техническое обслуживание, резервные системы	Низкая степень угрозы
<b>Ошибки конфигурации</b>	Неправильная настройка систем безопасности или сетевого оборудования	Внутренние нарушители (инсайдеры)	Ошибки в настройках безопасности	Уязвимость перед атаками, утечка данных, нарушение работы сервисов	Регулярные проверки конфигурации, обучение сотрудников	Низкая степень угрозы

# Cloud Provider. Реестр рисков\*

Описание	Последствия для бизнеса	Уровень угрозы	Вероятность реализации	Ущерб	Уровень риска	
Кибератаки (DDoS)	Недоступность инфраструктуры ЦОД для клиентов более 30% в течение более 60 минут (ежемесячно) приводит к штрафу со стороны клиентов на сумму 1,5% месячного дохода	Высокий	Высокая	\$360,000 / год	Критический	
Взлом и несанкционированный доступ к данным клиентов	Утечка конфиденциальной информации клиента ТОП-10 приводит к снижению темпов роста клиентской базы за счет снижения репутации и дополнительным издержкам в 0,5% бюджета PR на ее восстановление	Высокий	Высокая	\$60,000 / год	Критический	
Вредоносное ПО (вирусы, трояны, шифровальщики)	Недоступность более 30% инфраструктуры ЦОД для клиентов в течение более 60 минут (ежемесячно) приводит к штрафу со стороны клиентов на сумму 1,5% месячного дохода	Высокий	Средняя	\$360,000 / год	Высокий	
Фишинг и социальная инженерия	Утечка данных, компрометация учетных записей. Является причиной реализации рисков ИБ высокого уровня	Средний	Высокая	\$520,000 / год	Высокий	
Внутренние угрозы	Утечка данных, нарушение работы систем. Является причиной реализации рисков ИБ высокого уровня	Средний	Средняя	\$520,000 / год	Средний	
Уязвимости программного обеспечения	Неавторизованный доступ, компрометация данных, нарушение работы систем. Является причиной реализации рисков ИБ высокого уровня	Средний	Средняя	\$520,000 / год	Средний	
Физические угрозы (пожары, наводнения, кражи оборудования)	Недоступность инфраструктуры ЦОД для клиентов более 30% в течение более 60 минут (ежемесячно) приводит к штрафу со стороны клиентов на сумму 1,5% месячного дохода	Низкий	Низкая	\$360,000 / год	Низкий	
Отказ оборудования систем защиты	Недоступность системы защиты от DDoS атак более 5 минут (ежедневно) приводит к снижению выручки на 2% за счет оттока пользователей	Высокий	Средняя	\$100,000 / год	Критический	Новая угроза
Ошибки конфигурации	Уязвимость перед атаками, утечка данных, нарушение работы сервисов. Является причиной реализации рисков ИБ высокого уровня	Низкий	Средняя	\$520,000 / год	Средний	

Конкретные формулировки  
(где возможно)

\* Стратегия управления, ответственное подразделение и контрольные мероприятия со статусом не влезли на слайд

# CIS Benchmark



# CIS Benchmark

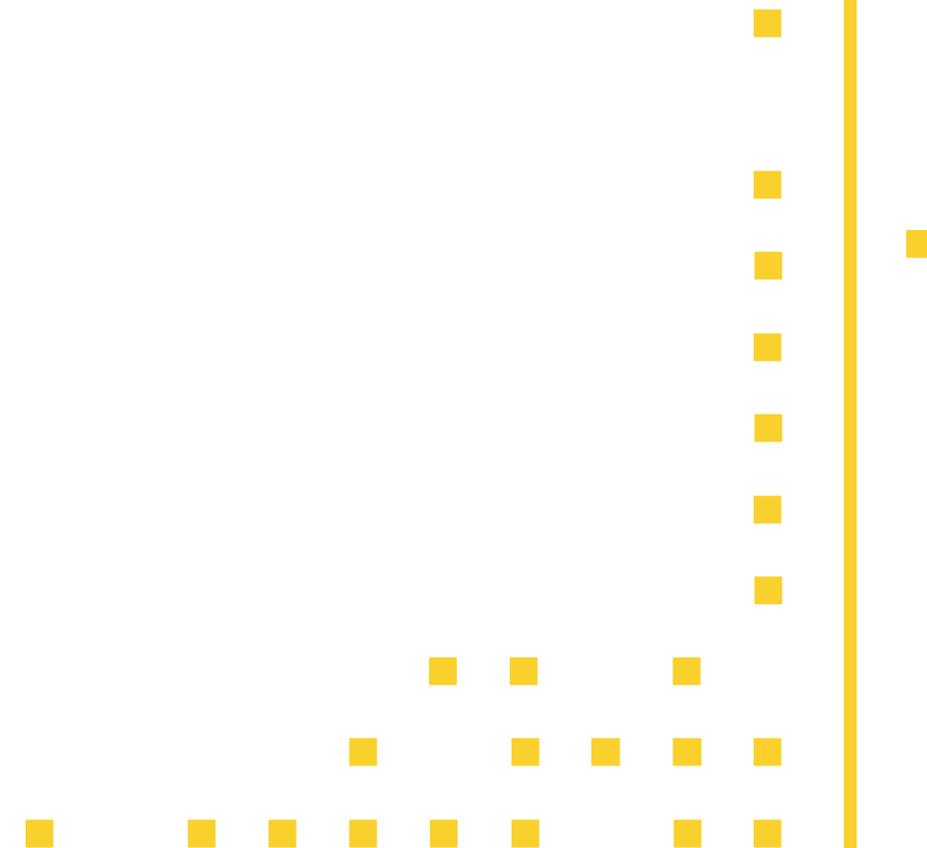
1 Меры защиты	Что делаем?	Тактика	ДЗО 1
2 <b>Защита продуктов</b>			
Безопасные конфигурации устройств и программного обеспечения.	Проводим усиление защищенности (Hardening) ПО, АРМ, серверов, сетевых и портативных устройств.	<ul style="list-style-type: none"> <li>Наладить и поддерживать процесс настройки безопасности для ПО и устройств.</li> <li>Наладить и поддерживать процесс настройки безопасности для сетевой инфраструктуры.</li> <li>Настроить автоматическую блокировку сеанса на корпоративных устройствах.</li> <li>Установить и настроить межсетевой экран на серверах.</li> <li>Установить и настроить межсетевой экран на конечных устройствах пользователей.</li> <li>Внедрить лучшие практики безопасного управления устройствами и ПО.</li> <li>Внедрить лучшие практики безопасного управления устройствами и ПО.</li> <li>Удалить или заблокировать неиспользуемые сервисы и модули на корпоративных устройствах и ПО.</li> <li>Настроить доверенные DNS-серверы на корпоративных устройствах.</li> <li>Внедрить практику автоблокировки на портативных устройствах пользователей.</li> <li>Внедрить удаленную очистку корпоративных данных на портативных устройствах пользователей.</li> <li>Создать выделенные рабочие пространства на мобильных устройствах пользователей.</li> </ul>	<ul style="list-style-type: none"> <li>1 Выполняется</li> <li>1</li> <li>1</li> <li>1</li> <li>1</li> <li>1</li> <li>1 Выполняется</li> <li>2 Выполняется</li> <li>2 Выполняется</li> <li>3</li> <li>2</li> <li>3</li> </ul>
4			
Разработка безопасных приложений	Выстраиваем процесс безопасной разработки ПО.	<ul style="list-style-type: none"> <li>Наладить и поддерживать процесс безопасной разработки ПО.</li> <li>Наладить и поддерживать процесс обнаружения и устранения уязвимостей в ПО.</li> <li>Проводить анализ уязвимостей прикладного ПО.</li> <li>Создать и поддерживать реестр компонентов ПО от сторонних производителей.</li> <li>Использовать последние версии компонентов ПО от доверенных сторонних производителей.</li> <li>Создать и поддерживать классификацию уязвимостей ПО по степени критичности.</li> <li>Использовать стандартные шаблоны конфигураций аппаратной защиты для инфраструктуры прикладного ПО.</li> <li>Отделять продакшен-окружение.</li> <li>Обучить разработчиков практикам безопасной разработки ПО.</li> <li>Использовать принципы безопасного проектирования в архитектуре приложений.</li> <li>Использовать проверенные модули или службы для компонентов безопасности приложений.</li> <li>Использовать проверки безопасности на уровне кода.</li> <li>Проводить тестирование на проникновение для приложений.</li> <li>Проводить моделирование угроз.</li> </ul>	<ul style="list-style-type: none"> <li>2 Выполняется</li> <li>2 Выполняется</li> <li>2 Выполняется</li> <li>2 Выполняется</li> <li>2</li> <li>2</li> <li>2</li> <li>2 Выполняется</li> <li>2 Выполняется</li> <li>2 Выполняется</li> <li>2 Выполняется</li> <li>3</li> <li>3</li> <li>3 Выполняется</li> </ul>
6 <b>Проактивное противодействие угрозам</b>			
Тестирование на проникновение	Проводим тестирования на проникновение, определять уязвимости и расследовать их причины, устранять.	<ul style="list-style-type: none"> <li>Создать и поддерживать программу тестирования на проникновение.</li> <li>Проводить регулярные внешние тесты на проникновение.</li> <li>Устранять уязвимости, найденные в результате тестов на проникновение.</li> <li>Подтвердить эффективность мер безопасности по итогам пентеста.</li> <li>Проводить регулярные внутренние тесты на проникновение.</li> </ul>	<ul style="list-style-type: none"> <li>2</li> <li>2 Выполняется</li> <li>2 Выполняется</li> <li>3 Выполняется</li> <li>3</li> </ul>
8			
		<ul style="list-style-type: none"> <li>Создать и поддерживать программу повышения грамотности в области кибербезопасности.</li> <li>Обучить сотрудников распознавать атаки с использованием социальной инженерии.</li> </ul>	<ul style="list-style-type: none"> <li>1</li> <li>1</li> </ul>

# CIS Benchmark

1	Меры защиты	Что делаем?	Тактика	ДЗО 1	
1	Тестирование на проникновение	Проводим тестирования на проникновение, определять уязвимости и расследовать их причины, устранять.	Проводить регулярные внешние тесты на проникновение.	2	
			Устранять уязвимости, найденные в результате тестов на проникновение.	2	
			Подтвердить эффективность мер безопасности по итогам пентеста.	3	
			Проводить регулярные внутренние тесты на проникновение.	3	
8					
8	Информированность и обучение сотрудников	Обучать работников правилам информационной безопасности, цифровой гигиене и социальной инженерии.	Создать и поддерживать программу повышения грамотности в области кибербезопасности.	1	
			Обучить сотрудников распознавать атаки с использованием социальной инженерии.	1	
			Обучить сотрудников лучшим практикам аутентификации.	1	
			Обучить сотрудников лучшим практикам обращения с корпоративными данными.	1	
			Ознакомить сотрудников с кейсами непреднамеренной утечки данных.	1	
			Обучить сотрудников распознавать инциденты безопасности и сообщать о них.	1	
			Обучить сотрудников, как проверить наличие важных обновлений безопасности на собственных рабочих устройствах.	1	
			Информировать сотрудников о рисках незащищенных сетевых соединений для обмена данными.	1	
			Провести тренинги по информационной безопасности в соответствии с ролями в организации.	3	
10					
10	Защита инфраструктуры	Инвентаризация и учет всех устройств, и программного обеспечения	Контролируем актуальность активов сети и программное обеспечение. Создаём реестр всех устройств и ПО поддерживаем, обнаруживаем нарушения, реагируем.	Создать и поддерживать детальный реестр всех устройств	1
				Реагировать на неавторизованные устройства	1
				Использовать инструменты для активного обнаружения.	2
				Вести журнал DHCP (протокол динамической настройки узла) для обновления реестра.	2
				Использовать инструменты для пассивного обнаружения устройств.	3
				Создать и поддерживать реестр используемого ПО.	1
				Проверять, что авторизованное ПО из реестра поддерживается вендором.	1
				Реагировать на неавторизованное ПО.	1
				Использовать инструменты для автоматического учета ПО.	2
				Использовать белые списки авторизованного ПО.	2
				Использовать белые списки авторизованных библиотек.	2
				Использовать белые списки авторизованных скриптов.	3
				11	
11			Наладить и поддерживать процесс управления журналами аудита.	1	
			Собирать журналы аудита.	1	
			Использовать надежное хранилище для журналов аудита.	1	
			Стандартизировать синхронизацию времени.	2	
			Собирать детализированные журналы аудита.	2	
			Собирать журналы DNS-запросов.	2	
			Собирать журналы URL-запросов.	2	
			Собирать журналы командной строки.	2	
			Централизовать ведение журналов аудита.	2	



**Как бы вы написали  
стратегию по ИБ?**



# Стратегия информационной безопасности



## Цели и задачи стратегии ИБ:

- ▶ Ноль публичных утечек персональных данных клиентов и сотрудников.
- ▶ Сохранение коммерческой тайны, критичных бизнес-данных.
- ▶ Ноль инцидентов ИБ, приводящих к простоем критичных систем.
- ▶ Соответствие требованиям законодательства.
- ▶ Зрелость процессов ИБ на уровне топ-10 аналогичных компаний.
- ▶ Интегрировать технологии, процессы с ГО на ДЗО.
- ▶ Оптимизировать существующие процессы ИБ.

## Минимизация рисков компании:

- Нарушение функционирования информационных систем и ИТ сервисов из-за вируса шифровальщика.
- Утечки персональных данных клиентов.
- Несоответствия требованию законодательства.
- Реализации угроз информационной безопасности в отношении КСПД.
- Реализации угроз информационной безопасности критически важных систем.

# Стратегия на 3 года

Направление	Цели	Действия
Защита конфиденциальности данных	Число утечек данных в течение года (целевой ноль).	Установка Антивирус/антиспам для почты (KSMG + KATA, правила Outlook) Установка Прокси-сервера (McAfee) Мониторинг/фильтрация сетевого трафика NGFW (Checkpoint, VipNet и др.) Защита от потери данных Data Loss Protection (Zecurion, DeviceLock) Шифрование данных Data Encryption (VeraCrypt, S/MIME, BitLocker? и др.)
Обеспечение целостности данных	Количество инцидентов ИБ, связанных с изменением данных (целевой ноль).	Защита веб-приложений Web Application Firewall (PT WAF) Управление межсетевыми экранами Firewall Management (Check Point Manager) Управление данными Data Governance (Varonis) Управление цифровыми активами в одном месте Digital Assets Management (IBM Guardium, Fleet)
Доступность систем и услуг	Количество инцидентов ИБ, приводящих к простою систем (целевой ноль).	Выявление целевых атак и сложных угроз EDR (Kaspersky KATA EDR)
Управление уязвимостями	Процент уязвимостей, устраненных в течение установленного срока (100% критических уязвимостей должны быть устранены в течение 30 дней, внедрены и применены компенсирующие меры в течении 3 дней).	Управление уязвимостями Vulnerability Management (Сканер + DefectDojo + Jira +Fleet) Анализ конфигураций Configuration Analysis (Fleet) Аудит безопасности Security Auditing (Fleet, OpenVAS и др.) Тестирование на проникновение Penetration Testing (Metasploit, Burp Suite и др.)
Соответствие нормативным требованиям	Процент соответствия стандартам и нормативам (100% соответствия). Количество выявленных значимых замечаний в ходе регулярных проверок (целевой ноль).	Разработать и внедрить внутренние и внешние ОРД.
Управления инцидентами	Среднее время реагирования на инциденты (менее 1 часа). Процент успешно разрешенных инцидентов (95% инцидентов должны быть разрешены в установленные сроки). Число повторных инцидентов (цель: снижение на 30% по сравнению с прошлым годом).	Установка системы управления информацией и событиями безопасности SIEM + SOAR (IBM QRadar, IBM Resilient) Аналитика поведения пользователей и сущностей (например, Exabeam, HP, IBM) Установка системы симуляции атак Breach & Attack Simulation (Red Canary, Atomic Red Team)
Защита от вредоносного ПО	Процент устройств, защищённых антивирусным ПО 100% рабочих станций. Процент успешных обновлений антивирусных баз (99% обновлений должны выполняться автоматически).	Установка антивируса/фаервола для ПК/серверов (KES, ClamAV, EDR, Wazuh) Установка Sandbox для анализа вредоносного ПО (KATA)
Управление доступом и аутентификацией	Процент многофакторной аутентификации для критичных систем 100%. Количество случаев несанкционированного доступа снижение на 30% по сравнению с прошлым годом.	Управлять доступом к сети Network Access Control (Cisco AnyConnect) Установка системы проверки подлинности при идентификации 2FA (Keycloak, Totp) Управление идентификацией пользователей Identity Management (Forefront Identity Manager, GPO AD) Управление привилегированным доступом Privileged Access Management (IBM Secret Server, Teleport, OVH-Bastion)
Управление безопасной разработкой	Среднее количество ошибок в выпускаемой версии ПО (PROD среда) не превышает 25 на тысячу строк кода (KLOC);	Управление процессами безопасной разработки ПО (SAST, GitLab Runner, SonarQube, Sentry) • Выстраивание процессов, таких как развитие SSDLC, автоматизация DevSecOps, обучение программистов • Составить реестр всех публикаций сервисов Страхователя в сеть интернет с указанием IP и FQDN адреса, формализованный и выполняемый процесс SAST/DAST (Static/Dynamic Application Security Testing) проведения аудита сервисов перед их публикацией в сети интернет.
Повышение осведомлённости работников ИБ	Количество случаев перехода по фишинговым ссылкам снижение на 30% по сравнению с прошлым годом.	Обучение и повышение осведомленности пользователей Security Awareness Training (Gophish, СДО WebTutor).

# Оценка уровня зрелости ДЗО

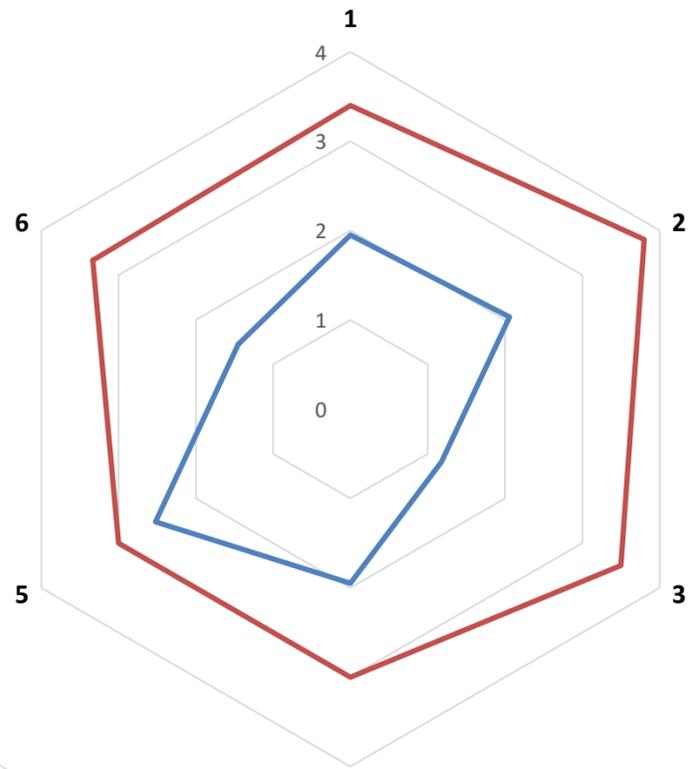
Домены КБ	ДЗО-1	ДЗО-2	ДЗО-3	ДЗО-4	ДЗО-5	Целевой уровень по домену
Управление отношениями	3	3	3	4	4	3,40
Защита продуктов	3	3	3	4	5	3,80
Защита инфраструктуры	3	3	3	4	3	3,50
Проактивное противодействие угрозам	3	3	3	3	3	3,00
Взаимодействие с гос. органами и внешними организациями	3	3	3	3	3	3,00
Процессы и организационная модель	3	3	3	3	3	3,33
Итоговый уровень зрелости	3	3	3	3	3	3,34

# Оценка уровня зрелости ДЗО

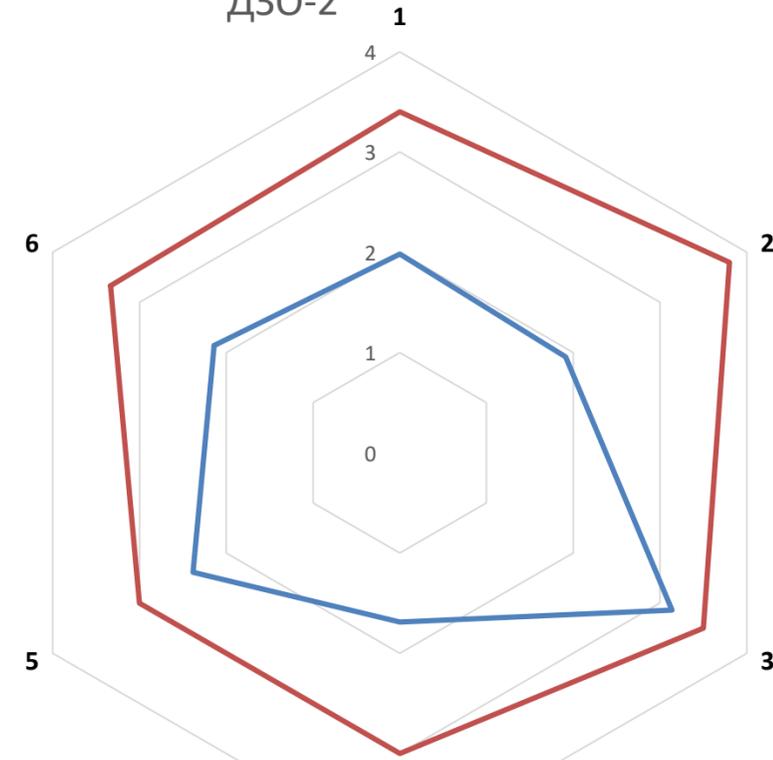
Домены КБ	Направления ИБ	ДЗО-1	ДЗО-2	ДЗО-3	ДЗО-4	ДЗО-5	Целевой уровень по домену
Управление отношениями	Стратегия ИБ	■	■	■	■	■	4,00
	Архитектура ИБ	■	■	■	■	■	3,00
	Коммуникации в области ИБ	■	■	■	■	■	3,00
	Отчетность и метрики	■	■	■	■	■	4,00
	Риск-ориентированный подход	■	■	■	■	■	3,00
Защита продуктов	Безопасность разработки	■	■	■	■	■	4,00
	Защита приложений в процессе эксплуатации	■	■	■	■	■	4,00
	Управление доступом	■	■	■	■	■	4,00
	Управление информационными активами	■	■	■	■	■	3,00
	Противодействие кибермошенничеству	■	■	■	■	■	4,00
Защита инфраструктуры	Сетевая безопасность	■	■	■	■	■	4,00
	Безопасность конечных устройств	■	■	■	■	■	3,00
	Безопасность данных	■	■	■	■	■	3,00
	Управление уязвимостями	■	■	■	■	■	4,00
	Мониторинг ИБ	■	■	■	■	■	4,00
	Управление инцидентами ИБ	■	■	■	■	■	3,00
Проактивное противодействие угрозам	Тесты на проникновение	■	■	■	■	■	3,00
	Расследования	■	■	■	■	■	2,00
	Культура ИБ	■	■	■	■	■	4,00
	Обучение работников службы ИБ	■	■	■	■	■	3,00
Взаимодействие с гос. органами и внешними организациями	Управление комплаенсом	■	■	■	■	■	3,00
	Взаимодействие с третьими сторонами	■	■	■	■	■	3,00
	Защита персональных данных	■	■	■	■	■	3,00
Процессы и организационная модель	Организационная структура	■	■	■	■	■	4,00
	Политики и стандарты в области ИБ	■	■	■	■	■	3,00
	Непрерывность бизнеса	■	■	■	■	■	3,00
<b>Итоговый уровень зрелости</b>						<b>3,34</b>	

# Оценка уровня зрелости ДЗО

ДЗО-1

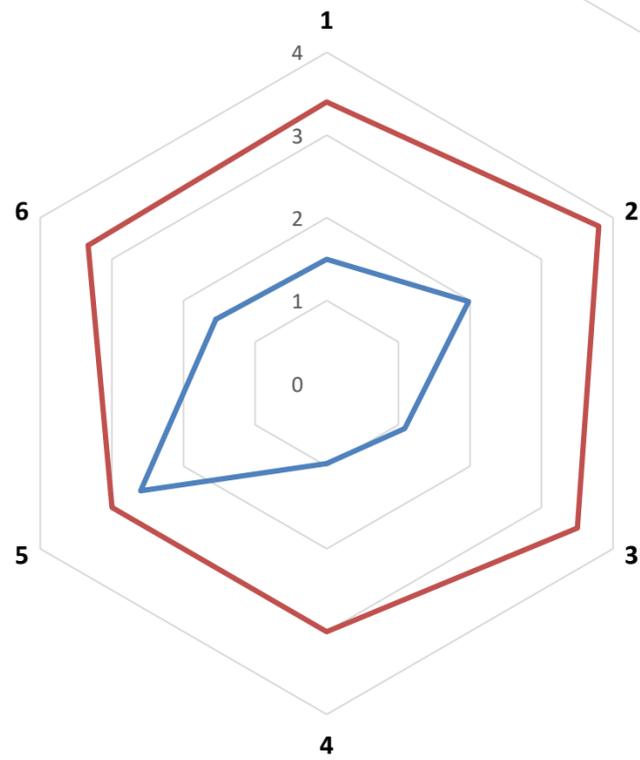


ДЗО-2

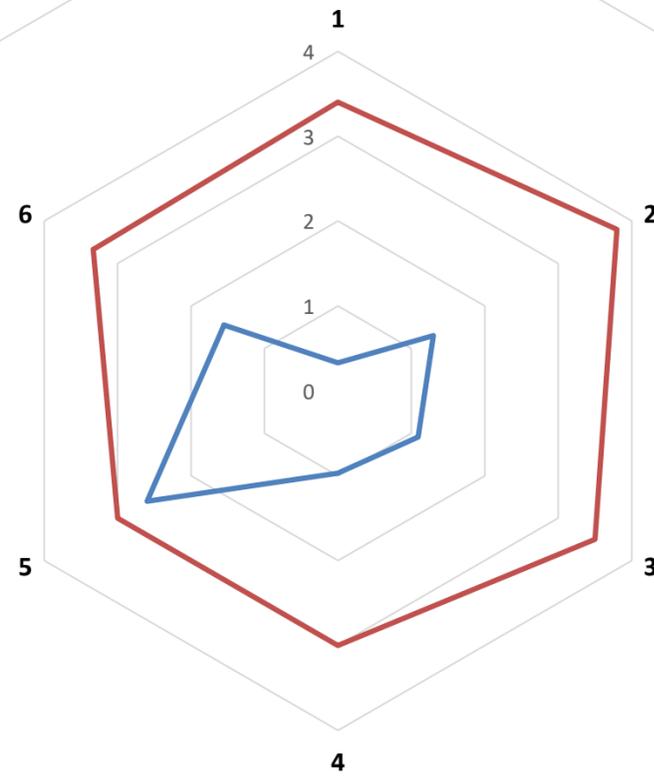


1	Управление отношениями
2	Защита Продуктов
3	Защита инфраструктуры
4	Проактивное противодействие угрозам
5	Взаимодействие с гос. органами и внешними организациями
6	Процессы и организационная модель

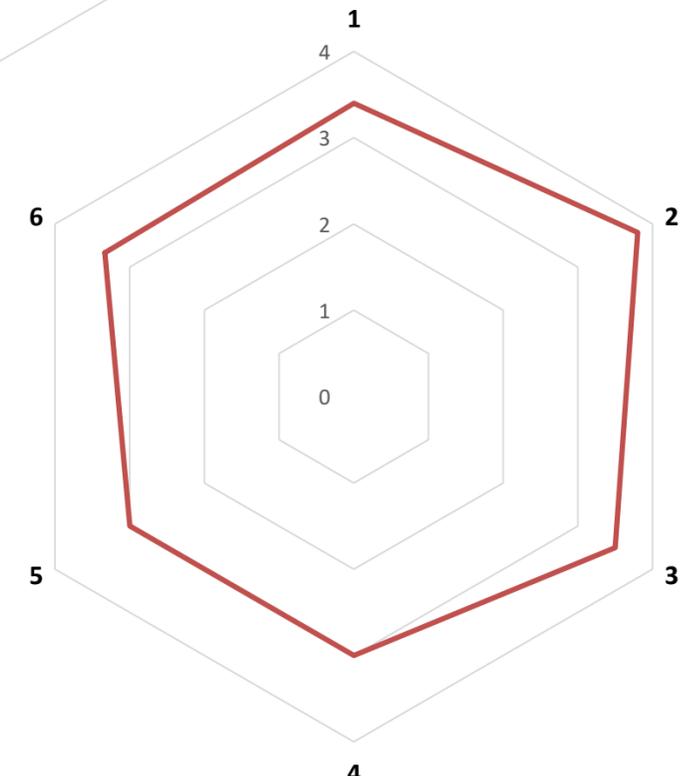
— Текущая — Целевая



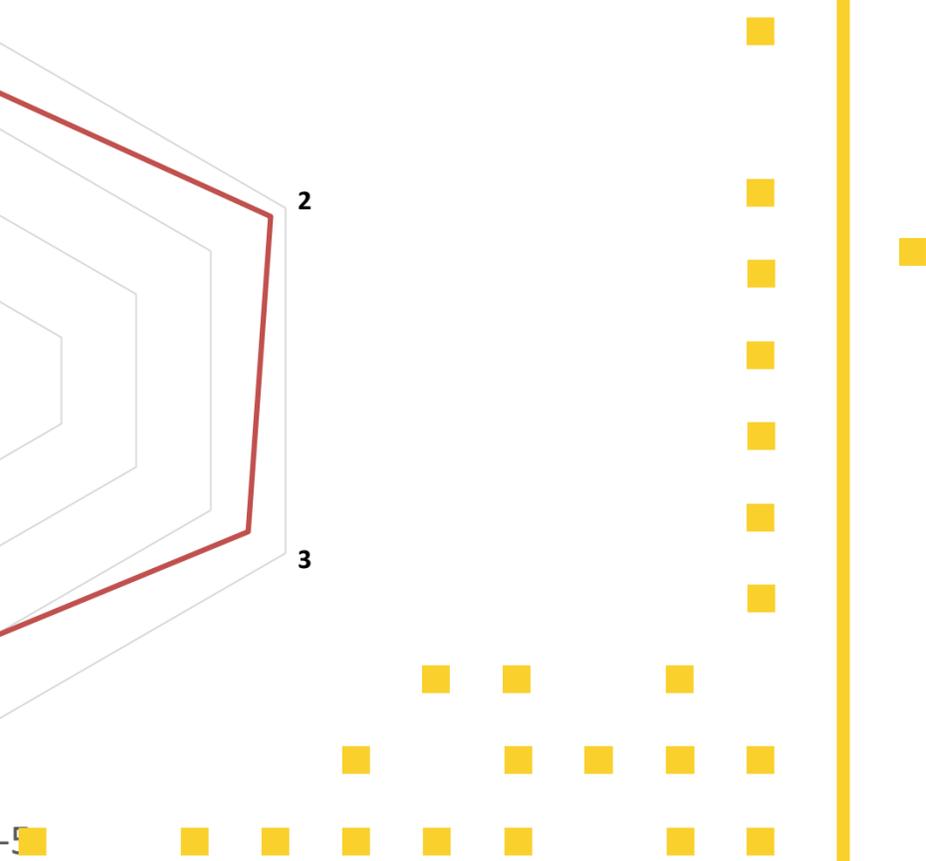
ДЗО-3



ДЗО-4



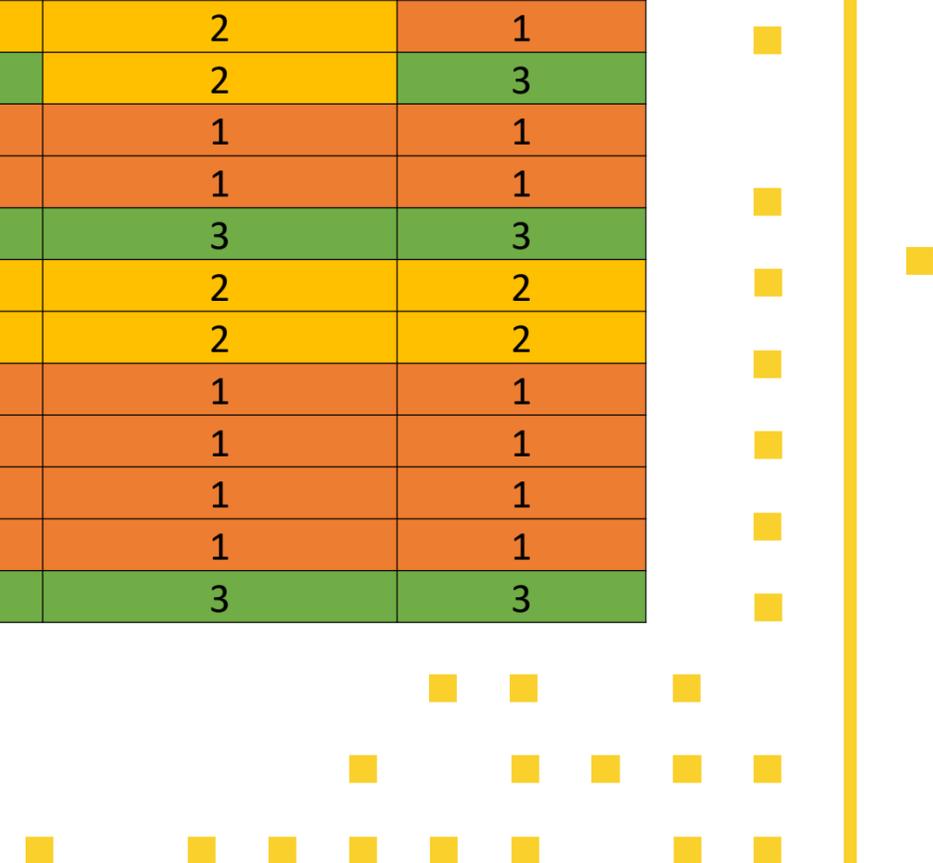
ДЗО-5



# Внедрённые процессы / технологии

Процессы   Технологии	ДЗО-1	ДЗО-2	ДЗО-3	ДЗО-4	ДЗО-5
Проксирование через промежуточный сервер	3	2	2	2	3
Мониторинг/фильтрация сетевого трафика	2	2	2	2	2
Защита от потери данных	1	1	1	1	1
Шифрование данных	1	1	1	1	1
Защита веб-приложений	1	1	1	1	1
Управление межсетевыми экранами	1	1	3	3	3
Управление данными	1	1	1	1	1
Управление цифровыми активами в одном месте	2	1	2	2	2
Выявление целевых атак и сложных угроз	3	3	3	2	3
Управление уязвимостями	1	3	1	1	1
Анализ конфигураций	1	1	1	1	1
Аудит безопасности	1	1	1	1	1
Тестирование на проникновение	3	1	1	1	1
Внутренние и внешние ОРД	2	2	2	2	1
Установка системы управления информацией и событиями безопасности	1	1	3	2	3
Система поведения пользователей и сущностей	1	1	1	1	1
Системы симуляции атак	1	1	1	1	1
Антивирус для ПК/серверов	2	3	3	3	3
Sandbox для анализа вредоносного ПО	2	2	2	2	2
Управлять доступом к сети	3	1	2	2	2
Система проверки подлинности при идентификации	1	1	1	1	1
Управление идентификацией пользователей	1	1	1	1	1
Управление привилегированным доступом	1	1	1	1	1
Управление процессами безопасной разработки ПО	1	1	1	1	1
Обучение и повышение осведомленности пользователей	3	3	3	3	3

Не внедрено	1	Требует доработок	2	Внедрено, работает	3
-------------	---	-------------------	---	--------------------	---



# SWOT анализ

**(S) Сильные стороны**

**(W) Слабые стороны**

и ПО.  
ентами.

ентами.

ентами.

**(O) Возможности**

**(Т) Угрозы**

безопасности.  
мацию.

фраструктуры.  
замеченными.

и системы.  
ям и штрафам.

ния данных.  
стей.  
к критическим ресурсам.

потерям.

вность бизнеса.

# План мероприятий

Цели
Число утечек данных в течение года (целевой ноль).
Количество инцидентов ИБ, связанных с изменением данных (целевой ноль).
Процент уязвимостей, устраненных в течение установленного срока
Процент соответствия стандартам и нормативам
Среднее время реагирования на инциденты (менее 1 часа)
Процент успешно разрешенных инцидентов в установленные сроки
Число повторных инцидентов, снижение на 30% по сравнению с прошлым годом.
Процент устройств, защищённых антивирусным ПО 100% рабочих станций.
Процент 2FA для критичных систем 100%
Снижение случаев несанкционированного доступа снижение на 30% год к году
Среднее количество ошибок в выпускаемой версии ПО не превышает 25 на тысячу строк кода
Случаи перехода по фишинговым ссылкам снижение на 30% год к году

Люди
Работник 1

Процессы
Повышение защиты конфиденциальных данных
Обеспечение целостности данных
Доступность систем и услуг
Управление уязвимостями
Соответствие нормативным требованиям
Управления инцидентами
Защита от вредоносного ПО
Управление доступом и аутентификацией
Управление безопасной разработкой
Повышение осведомлённости работников ИБ

Технологии
Kaspersky Secure Mail Gateway
Kaspersky Anti Targeted Attack
Microsoft Outlook rules
Mcafee Web Gateway
Check Point NGFW
VipNet, S-terra, Континент
Zecurion, DeviceLock, InfoWatch
VeraCrypt, S/MIME, BitLocker
PT Application Firewall
Check Point Manager
Varonis Data Governance
IBM Guardium Database Activity Monitoring
Fleet
DefectDojo
OpenVAS
Burp Suite, Metasploit, Nuclei
IBM QRadar, IBM Resilient
Exabeam, HP, IBM
Red Canary, Atomic Red Team
Kaspersky Endpoint Security, ClamAV
Cisco AnyConnect
Keycloak, Totp
Forefront Identity Manager, GPO AD
IBM Secret Server, Teleport, OVH-Bastion
GitLab Runner, SonarQube, Sentry
Gophish, СДО WebTutor

Проекты
Система защиты для электронной почты
Контроль сетевого трафика
Контроль конфигурациями устройств
Аудит безопасности
Тестирование на проникновение
Разработка, внедрение внутренних и внешние ОРД
Управление идентификацией пользователей и доступом
Выявления целевых атак и сложных угрозы
Выявление и устранение уязвимостей
Защита бизнеса от потери данных
Защита веб-приложений
Защита цифровых активов и данных
Система проверки подлинности
Система управления информацией и событиями безопасности
Аналитика поведения пользователей
Систему симуляции атак
Безопасная разработка
Повышение осведомленности работников ИБ

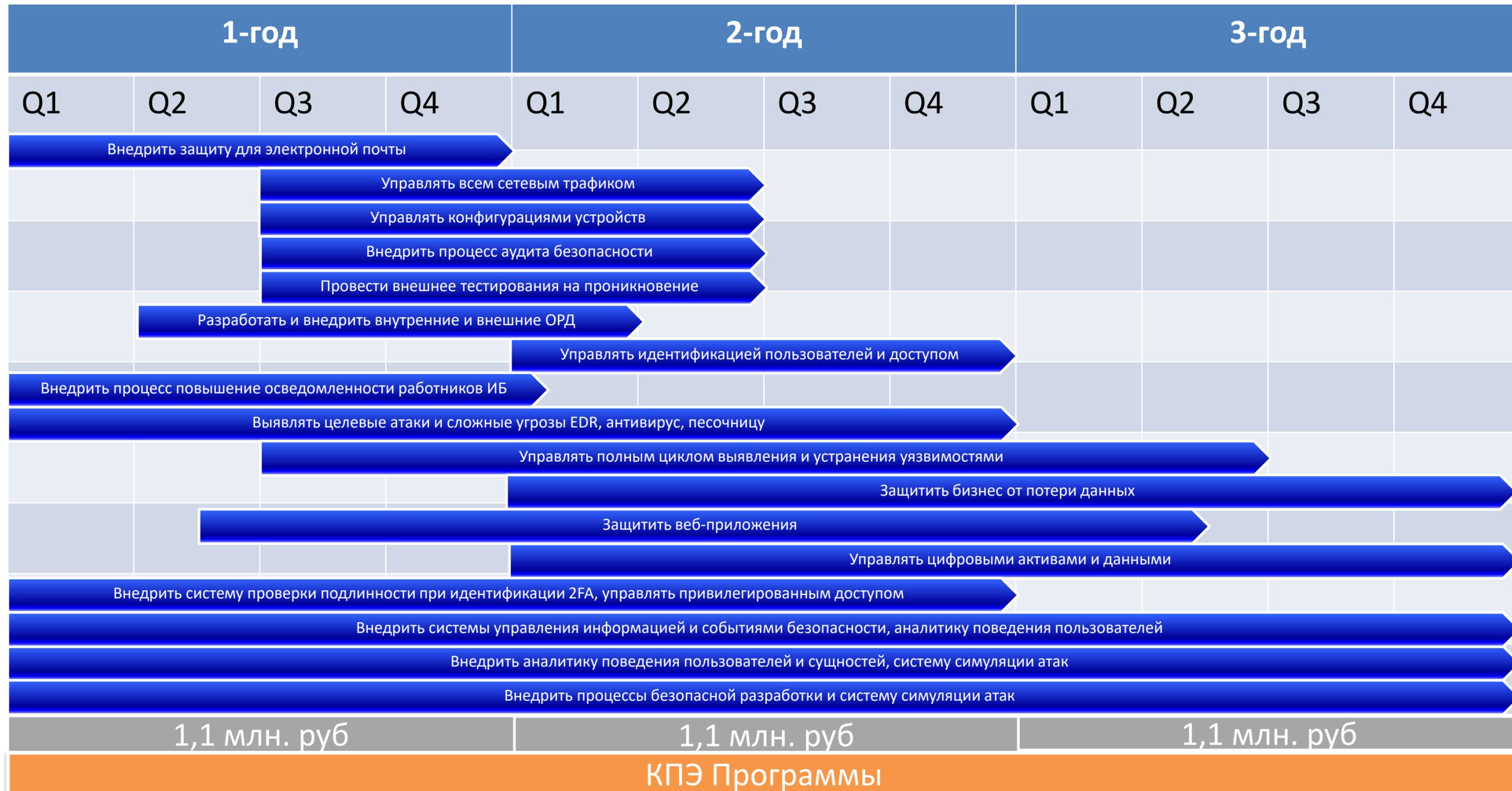
# Задачи

	Сроки	Бюджет
Внедрить антивирус/антиспам для почты (KSMG + KATA, правила Outlook)	1 год	?
Внедрить Прокси-сервер (McAfee)	1 год	?
Настроить мониторинг/фильтрацию сетевого трафика NGFW (Checkpoint, VipNet и др.)	1 год	?
Управлять межсетевыми экранами (Check Point Manager)	1 год	?
Внедрить процесс анализа конфигураций (Fleet)	1 год	?
Внедрить процесс аудита безопасности (Fleet, OpenVAS и др.)	1 год	?
Проводить тестирование на проникновение (Metasploit, Burp Suite и др.)	1 год	?
Разработать и внедрить внутренние и внешние ОРД	1 год	?
Управлять доступом к сети компании (Cisco AnyConnect)	1 год	?
Управлять идентификацией пользователей (Forefront Identity Manager, GPO AD)	1 год	?
Внедрить процесс обучения и повышение осведомленности работников (Gophish, СДО WebTutor).	1 год	?
Выявлять целевые атаки и сложных угроз EDR (Kaspersky KATA EDR)	2 года	?
Управлять уязвимостями (Сканер + DefectDojo + Jira +Fleet)	2 года	?
Внедрить антивирус/фаервол для ПК/серверов (KES, ClamAV)	2 года	?
Защитить бизнес от потери данных (Zecurion, DeviceLock)	2 года	?
Внедрить шифрование данных (VeraCrypt, S/MIME, BitLocker)	2 года	?
Защитить веб-приложения (PT WAF)	2 года	?
Управлять данными Data Governance (Varonis)	2 года	?
Управлять цифровыми активами в одном месте (IBM Guardium, Fleet)	2 года	?
Внедрить Sandbox для анализа вредоносного ПО (KATA, cuckoo)	2 года	?
Внедрить система проверки подлинности при идентификации 2FA (Keycloak, Totp)	2 года	?
Внедрить системы управления информацией и событиями безопасности SIEM + SOAR (IBM QRadar, IBM Resilient)	3 года	?
Внедрить аналитику поведения пользователей и сущностей ( Exabeam, HP, IBM)	3 года	?
Внедрить систему симуляции атак (Red Canary, Atomic Red Team)	3 года	?
Управлять привилегированным доступом (IBM Secret Server, Teleport, OVH-Bastion)	3 года	?
Управлять процессами безопасной разработки ПО (SAST, GitLab Runner, SonarQube, Sentry)	3 года	?
Внедрить процессы, таких как развитие SSDLC, автоматизация DevSecOps, обучение программистов	3 года	?

Бюджет: ? млн. руб.

Целевая численность ИБ: 30 чел.

# План основных мероприятий



- **Снижение числа инцидентов безопасности:** Уменьшение количества успешных атак и инцидентов на 30% в течение 12 месяцев.
- **Увеличение осведомленности сотрудников:** Повышение на 70% уровня осведомленности сотрудников о потенциальных угрозах и методах защиты.
- **Сокращение времени реагирования на угрозы:** Среднее время обнаружения и реагирования на инциденты снизится на 80%
- **Увеличение уровня защищенности данных:** Достижение 95% защиты критически важных бизнес-данных.

# Проект решения

1. Утвердить ИБ-стратегию на 3 года
2. Предварительно одобрить бюджет развития ИБ в размере ??? млн. руб. на 3 года.



# Компоненты стратегии

Компоненты  
стратегии



# Цели бывают разные

## ChatGPT

Ключевые бизнес-цели могут сильно различаться в зависимости от отрасли, поскольку каждая из них имеет уникальные требования и рыночные условия. Вот примеры ключевых бизнес-целей для различных отраслей:

### 1. Финансовый сектор

- **Усиление безопасности транзакций:** защита данных клиентов и предотвращение финансового мошенничества.
- **Соблюдение регуляторных требований:** выполнение требований, предъявляемых финансовыми регуляторами в разных юрисдикциях.
- **Оптимизация рисков:** разработка моделей для управления кредитными и рыночными рисками.

### 2. Здравоохранение

- **Улучшение качества ухода за пациентами:** повышение эффективности диагностики и лечения.
- **Сохранение конфиденциальности медицинской информации:** защита чувствительной информации пациентов.
- **Достижение операционной эффективности:** сокращение издержек и улучшение управления ресурсами в медицинских учреждениях.

### 3. Розничная торговля

- **Увеличение продаж:** оптимизация маркетинговых и продажных стратегий для увеличения оборота.
- **Повышение удовлетворенности клиентов:** предложение высококачественного обслуживания и улучшение пользовательского опыта.
- **Расширение рынка:** вход на новые географические рынки и/или расширение ассортимента продукции.

## ChatGPT

Формулирование стратегических целей для ИТ-компании должно быть конкретным, измеримым и направленным на достижение долгосрочных результатов. Вот примеры четко сформулированных стратегических целей для ИТ-компании:

### 1. Рост доходов:

- Увеличить годовой доход компании на 20% в течение следующих трех лет за счет расширения портфеля облачных услуг и цифровых решений.

### 2. Расширение клиентской базы:

- Привлечь 100 новых корпоративных клиентов в сегменте среднего бизнеса к концу следующего года через усиленные маркетинговые кампании и улучшенное клиентское обслуживание.

### 3. Улучшение клиентского опыта:

- Достичь уровня удовлетворенности клиентов не менее 90% по результатам годовых опросов, улучшив техническую поддержку и времена реакции на запросы клиентов.

### 4. Технологические инновации:

- Разработать и успешно запустить на рынок три новых продукта в области искусственного интеллекта и машинного обучения в течение ближайших двух лет.

### 5. Улучшение безопасности данных:

- Внедрить комплексную систему управления информационной безопасностью, соответствующую стандарту ISO 27001, и получить сертификацию к концу текущего года.

### 6. Оптимизация операционной эффективности:

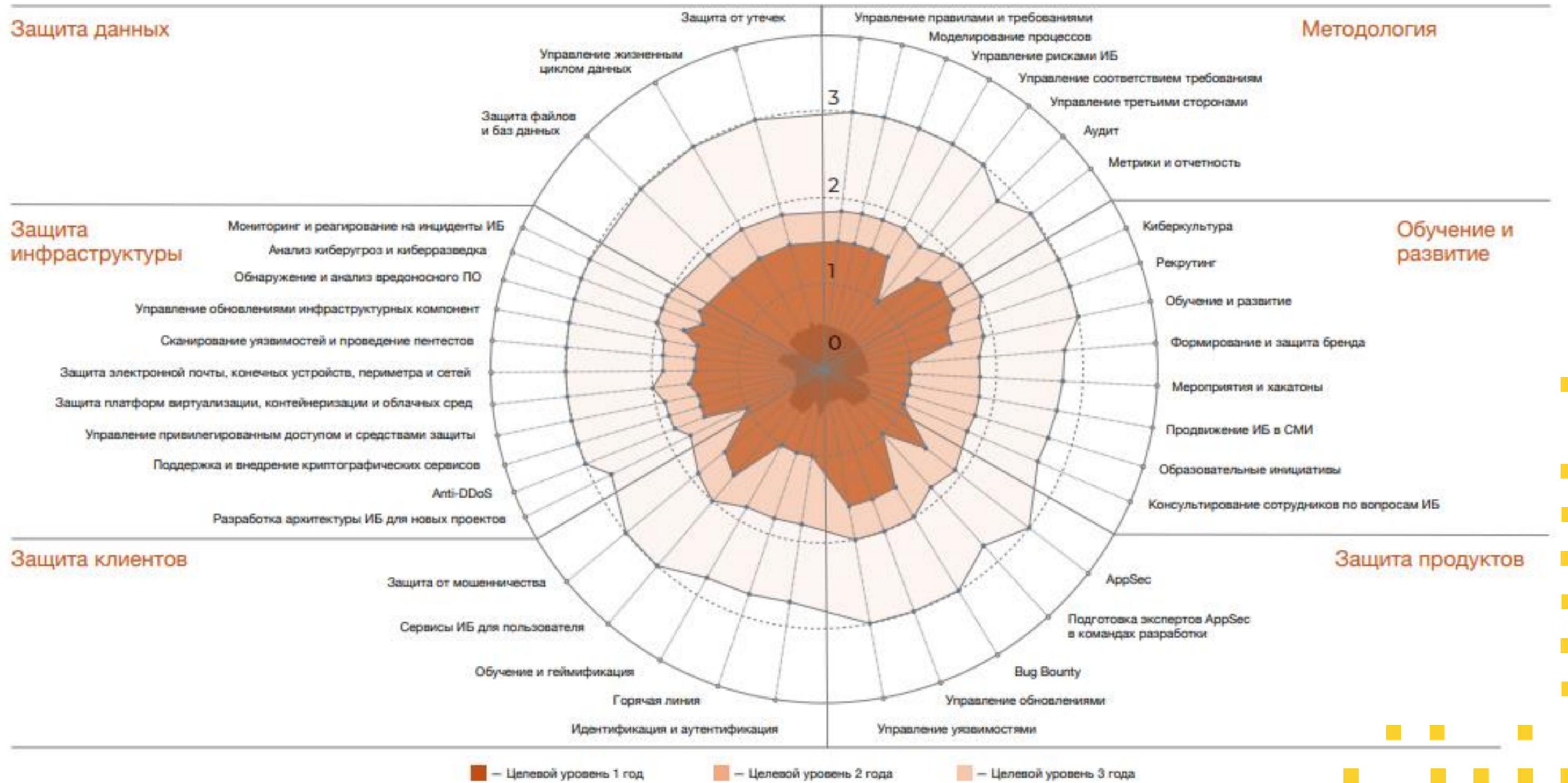
- Сократить операционные расходы на 15% в течение следующих двух лет, оптимизировав процессы управления проектами и автоматизировав рутинные задачи.

### 7. Развитие персонала:

- Повысить уровень квалификации 80% сотрудников компании по ключевым технологическим направлениям через внедрение программы непрерывного обучения и сертификации к концу следующего года.

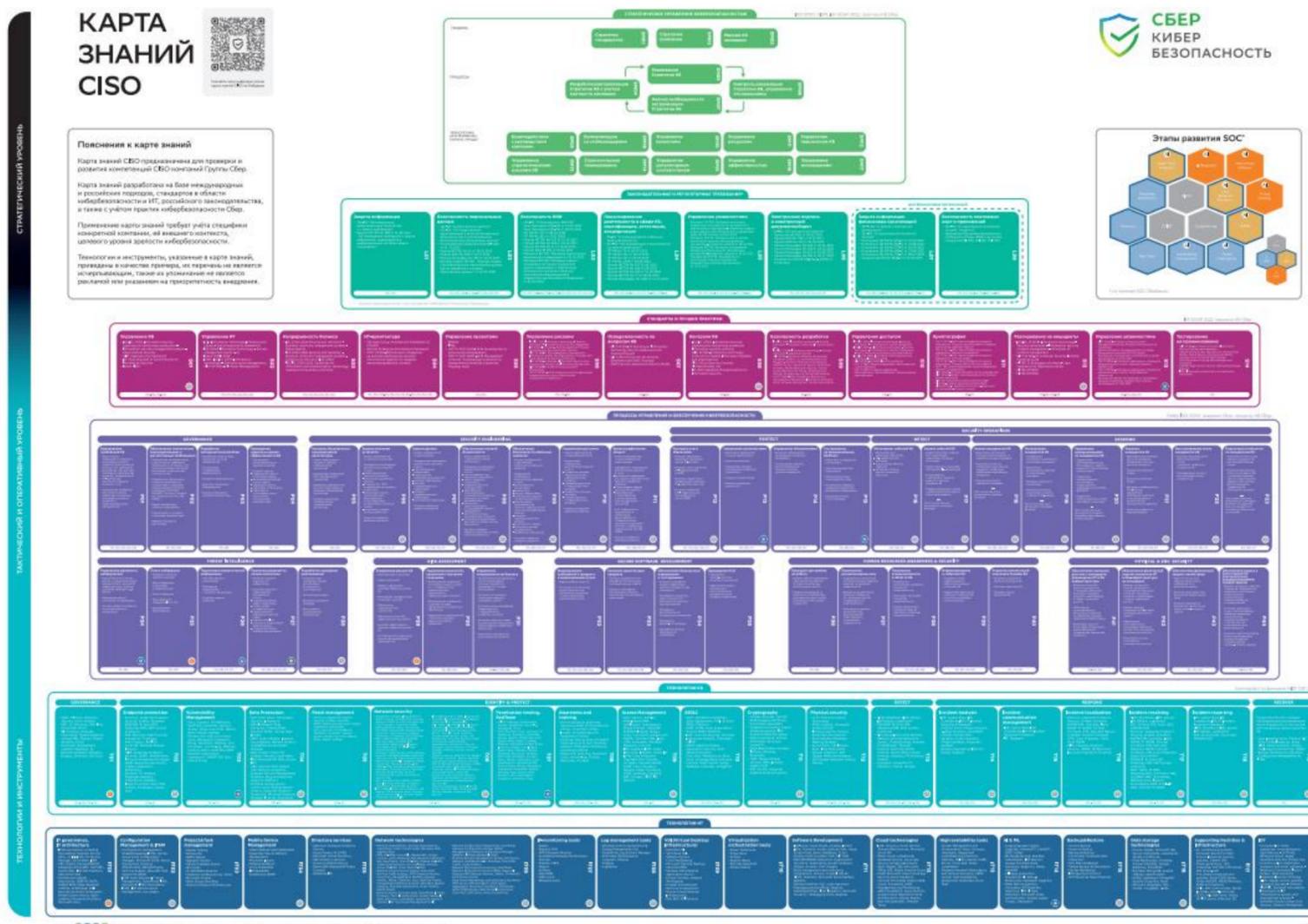
Эти цели помогут ИТ-компании стать более конкурентоспособной, улучшить её финансовые показатели и операционную эффективность, а также укрепить репутацию в качестве лидера в области технологических инноваций.

# Зрелость ИБ (пример)



# Карта знаний CISO

На карте можно ознакомиться со сводом профессиональных знаний в области кибербезопасности, собранным экспертами Сбера, и выявить зоны своего развития. Эти материалы представляют собой квинтэссенцию собственного опыта Группы Сбер и лучших международных и российских практик в области кибербезопасности и информационных технологий.



Сбербанк

<https://www.sberbank.ru> > experts > karta-znaniy-ciso

## Карта знаний CISO. Кибрарий

CISO MindMap — карта знаний охватывает законодательные и регуляторные требования, стандарты управления кибербезопасностью, подробно описывает ...

# КОНТАКТЫ

Куличкин Артём Александрович

TG: @Kulichkin

Тел.: +79171110055

