КОДЕБАЙ
АКАДЕМИЯ

Как обеспечить кибербезопасность через призму IT.

ИБ, ориентированная на бизнес!

Спикер: Ануфриев Иван (Руководитель экспертного центра кибербезопасности, куратор образовательных программ по киберрискам и менеджменту ИБ, автор курсов)

«ЭКОСИСТЕМА CODEBY»

Команда Codeby

Сильнейшая Red Team и Purple Team в Российском сегменте, специализирующаяся на аудите информационных и технологических систем, а также ИБ-консалтинге построении систем защиты. Наши клиенты входят в ТОР 20 банков России, компаний энергетического, транспортного, промышленного и других критичных секторов экономики. Наш профессионализм подтвержден множеством проведенных аудитов, закрытых проектов по ИБ-консалтингу и построению систем защиты и победами на крупнейших в России киберучениях на протяжении 4-х лет. (Standoff 365)

- **ТОП №1 СРЕДИ ЭТИЧНЫХ ХАКЕРОВ В РФ (The StandOff) 2021 2022 2023 !**

2015
Год основания экосистемы Codeby

150 000 ++
Крупнейшее в РФ ИТ- киберсообщество, открытая CTF-площадка

300+
Реализованных Проектов по разным направлениям

10+
Ключевых Компетенций. 7 направлений, 4 компании

200+
Специалистов команды Codeby по всему миру,

Россия, СНГ, Мир
Региональные представительства, международная команда,


CODEBY
Your Upgrade
КОДЕБАЙ АКАДЕМИЯ
Академия кибербезопасности
CODEBY.NET
Your InfoSec Upgrade
Крупнейшее в РФ IT-сообщество
КОДЕБАЙ ИГРЫ
CTF площадка
КОДЕБАЙ ПЕНТЕСТ
Информационная безопасность

КОДЕБАЙ
АКАДЕМИЯ

НАПРАВЛЕНИЯ ОБУЧЕНИЯ:

- Информационная безопасность
- Тестирование и аудит ИБ
- Программирование и разработка
- Операционные системы и сети
- Разведка по открытым источникам
- Реверс-инжиниринг
- Менеджмент ИБ, риски, комплаенс

codeby.school

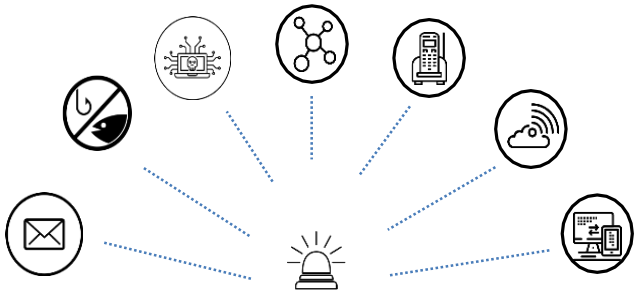
КОМАНДА CODEBY ПО НАПРАВЛЕНИЮ ИБ-КОНСАЛТИНГ И АУДИТ ИБ

Особенности подхода

- Максимальная прозрачность для бизнеса и руководства
- Минимальные неудобства для пользователя
- Достижение стратегических целей в ИБ
- Отсутствие «конвейера» - каждый Заказчик уникален
- Стратегическое сотрудничество с Заказчиком – отсопровождения пилота и создания концепции до сопровождения Заказчика после внедрения систем

Безопасность, которая работает

Любое внедрение – это процесс



- Разработка стандартов ИБ
- Разработка схем процессов ИБ
- Внедрение процессов ИБ
- Тестирование и обучение персонала

Не история, а опытная команда здесь и сейчас

- Опыт реализации сложных консалтинговых комплексных проектов, аудитов ИБ.
- Уникальная проектная экспертиза за последние 4 года
- Экспертиза как в Российских, так и в западных вендорах по ИБ.
- Качество работы в сложных условиях и сжатые сроки

Надежный и квалифицированный партнер

- ТОП-1 рейтинга лучших команд по этичному захакингу в России и СНГ (Standoff 365) по итогам 2019,2020,2021,2022,2023.
- Распределенная команда, специалисты-практики по ИБ в разных отраслях
- Заказчики-лидеры рынка в своих отраслях

Lead Auditor ISO 27001 Information Security Management Systems

CISSP Certified Information Systems Security Professional

CISA Certified Information Systems Auditor An ISACA Certification

CISM Certified Information Security Manager An ISACA Certification

СПИКЕР - АНУФРИЕВ ИВАН.

Опыт работы в области информационной безопасности в профильных организациях, включая работу как технического руководителя проектов по ИБ и РП по комплексным проектам СНГ и банковской сферы, а также работу на позиции менеджера по работе с ключевыми клиентами системного интегратора (госсектр), а также в качестве коммерческого директора в отраслевом системном интеграторе.

Руководитель научно-технического центра по ИБ при Фонде и работа над проектами по ИБ в Сколково.

Преподавательская и научная деятельность в ведущих университетах на преподавательских позициях а также руководство научно-техническими центрами.

Реализация крупных проектов по ИБ для промышленности, энергетики и банков.

Образование и квалификация:
Диплом с отличием РТУ МИРЭА «Информационная безопасность АС», направление от ПАО «Росатом»; Внутрикорпоративное обучение по управлению ИБ/IT проектами, также по корпоративному управлению и продажам. Во время работы при ФГУП ППП проходил различные технические сертификации.

Научно-методическая работа и преподавательская деятельность:
Являлся преподавателем и куратором проектов развития и экспертом по кибербезопасности и цифровой трансформации при РТУ-МИРЭА, преподавателем в Финансовом университете при Правительстве РФ и директором научно-технического центра. Стратегический консалтинг и операционализация проектов развития в качестве руководителя научно-технического центра для ряда организаций Правительства Москвы. Также сопровождал проекты в рамках программы обучения Master of Public Administration. Являюсь соискателем ученой степени.

Вхожу в некоторые экспертные группы.

МАКСИМАЛЬНО ПОЛЕЗНО КОНЦЕНТРИРОВАННО
ПРЕЗЕНТАЦИЯ БУДЕТ ДОСТУПНА КАК МИНИ-СПРАВОЧНИК =)

1. Риски компаний при слабой ИБ. Актуальность

1.1.Цифры

1.2.Своя проверка

2. Системный подход

Структура и вектора работы

Процессы, функции, системная архитектура

3. Составляем карту рисков и строим систему защиты

3.1.Шаги оценки

3.2.Инструменты

3.3.Проверка безопасности

3.4.Карта рисков

3.5.Регуляторные риски

4. Система защиты

4.1.Построение системы защиты

5. Финансы

Оценка затрат и возврат инвестиций

CODEBY
Your Upgrade

1.1

Риски компаний при слабой ИБ. Актуальность

Всем известные факты по утечкам в РФ в 2022 -2023 г.

В 4 раза с начала специальной военной операции возросло число кибератак против Российской Федерации По данным Positive Technologies

20 мая 2023 г. 61 000 пользователей ИнфоТеКС утекло (логин, фамилия и имя, контактные данные, хеш пароля, место работы и должность, дата регистрации пользователей По данным Positive Technologies

65 млн. данных Россия утекло в 2022 г.
В 2022 по данным Сбербанка

31 миллион строк с информацией, 554 миллиона заказов
ГЕМОТЕСТ - ФИО, дата рождения, адрес, номер телефона, эл.-почта, серия и номер паспорта, результаты анализов

713 тысяч пользователей системы «Умный дом»
РОСТЕЛЕКОМ - ФИО, эл.-почта, телефон, IP-адрес, дата регистрации и последней активности

1,5 млрд строк (3 утечки)
СДЭК - ID клиента, номер телефона, ФИО, адрес эл.-почта, почтовый адрес

49 млн. строк с заказами утекло
27 февраля 2022 архив ЯндексЕда был слит в DarkNet

6 июня 2022 была слита в сеть база данный Ростелекома
Адреса, контактные данные, ФИО сотрудников

21 апреля 2022 действия инсайдера Тинькофф Банка удалось предотвратить благодаря усилиям службы ИБ.
208 Гб. Попытка слива внутренних данных в интересах клиентов Банка

Свежие ссылки на данные по утечкам конец 2022 - 2023

Ссылки на свежие источники, исследования и данные по утечкам которые нам показались наиболее интересными в данном контексте:

13 декабря, 2022
Хакеры обнародовали информацию о московских школьниках и их родителях

https://www.securitylab.ru/news/535250.php

07 марта, 2023
Новая утечка данных: хакеры NLB опубликовали базу данных пользователей 'СберПраво'

Подробнее: https://www.securitylab.ru/news/536800.php

20 мая 2023
«ИнфоТеКС» подтвердила утечку данных о пользователях своего сайта infotecs.ru

' Подробнее Хабр (habr.com)

Data1eaks

Утечки баз данных
«Рыбное место»

Data1eaks | Ут ечки баз данных – Telegram

Информация СМИ

Данные клиентов подвергаются риску после взлома дилерских центров Toyota и Lexus в Японии

Techberg.ru

https://techberg.ru/dannye-klientov-podvergayutsya-risku-posle-vzloma-dilerskih-centrov-toyota-i-lexus-v-yaponii-uprostite-tehnologiyu

CRIME

Hacked car dealer Pendragon defies $60m ransom demand

We won't be held hostage, executive tells LockBit attackers

Pendragon sells brands including Jaguar, Porsche and Aston Martin

PENDRAGON

THE TIMES

https://www.thetimes.co.uk/article/44708586-511d-11ed-b120-ca4f3ffbcdc5

В даркнете стали появляться предложения взломать "умный" автомобиль

НТИ "Автонет": объявления по взлому "умных" автомобилей стали появляться в даркнете

© Depositphotos.com / shmeljov

Люди, занимающиеся интернет-мошенничеством. Архивное фото

РИА

https://ria.ru/20221223/darknet-1840715985.html?ysclid=lj2s9ar1i0431795486

Хакерские атаки в автопроме: страшилка или реальная угроза?

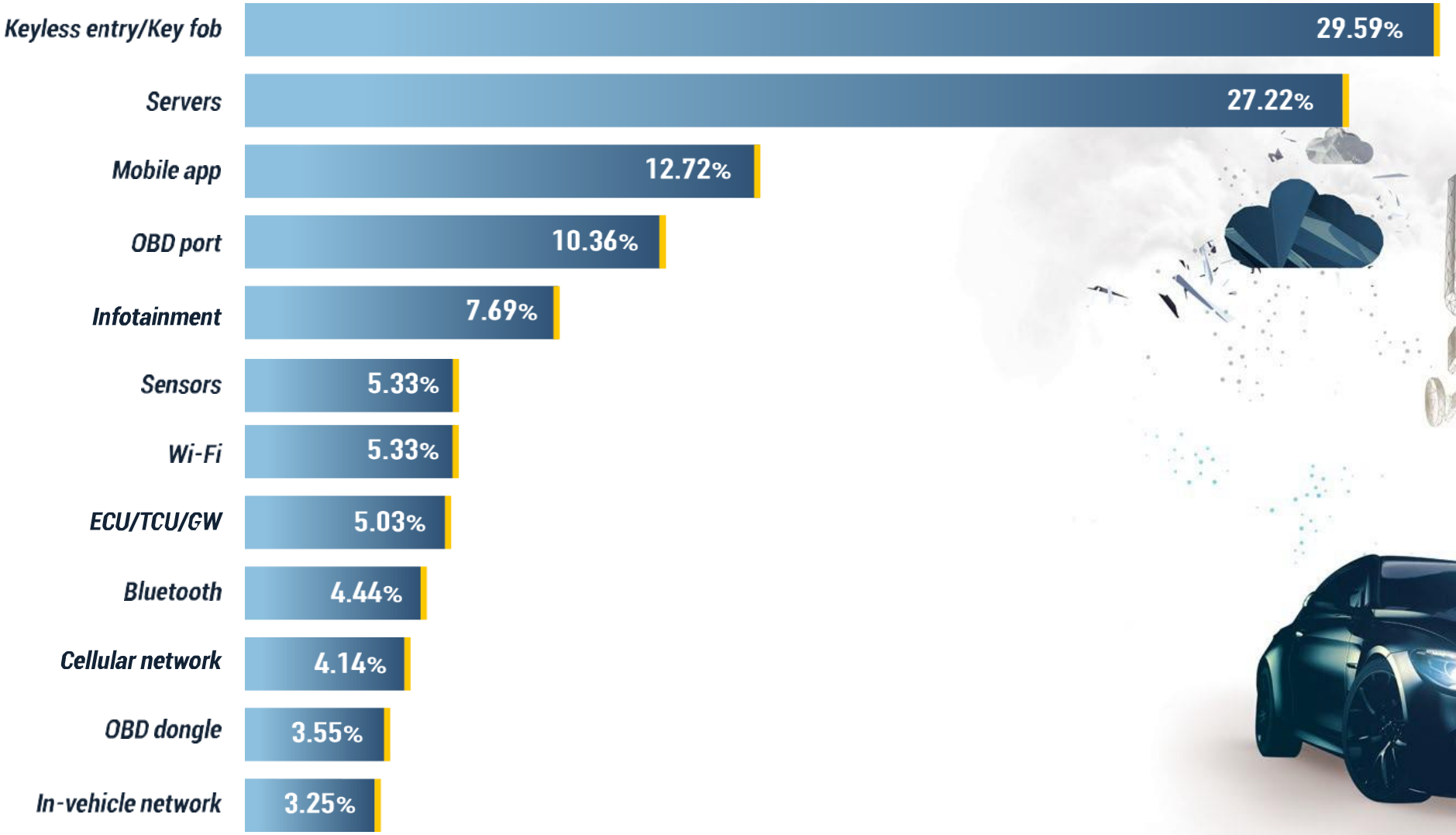
От перехвата управления до кражи информации о миллионах клиентов. Насколько опасны киберпреступления в автомобильной сфере

Autonews.ru

https://www.autonews.ru/news/6315d8829a79473e41167946

Сейчас тенденция: черные хакеры стали взламывать автодилеров и в принципе стал интерес автомобиль как объект взлома

РАСПРЕДЕЛЕНИЕ ОСНОВНЫХ ВЕКТОРОВ АТАК, СТРЕМИТЕЛЬНЫЙ РОСТ КИБЕРИНЦИДЕНТОВ В АВТОМОБИЛЬНОЙ ПРОМЫШЛЕННОСТИ – 7 РАЗ



Целевые атаки

«В 2023 целью хакеров станет не только финансовая, но и политическая выгода»

APT = (Advanced Persistent Threat) persistent. (иногда более 12 мес. внутри сети)

Крупные утечки данных 2022 года в России (fbkcs.ru)

Пример недопустимого события

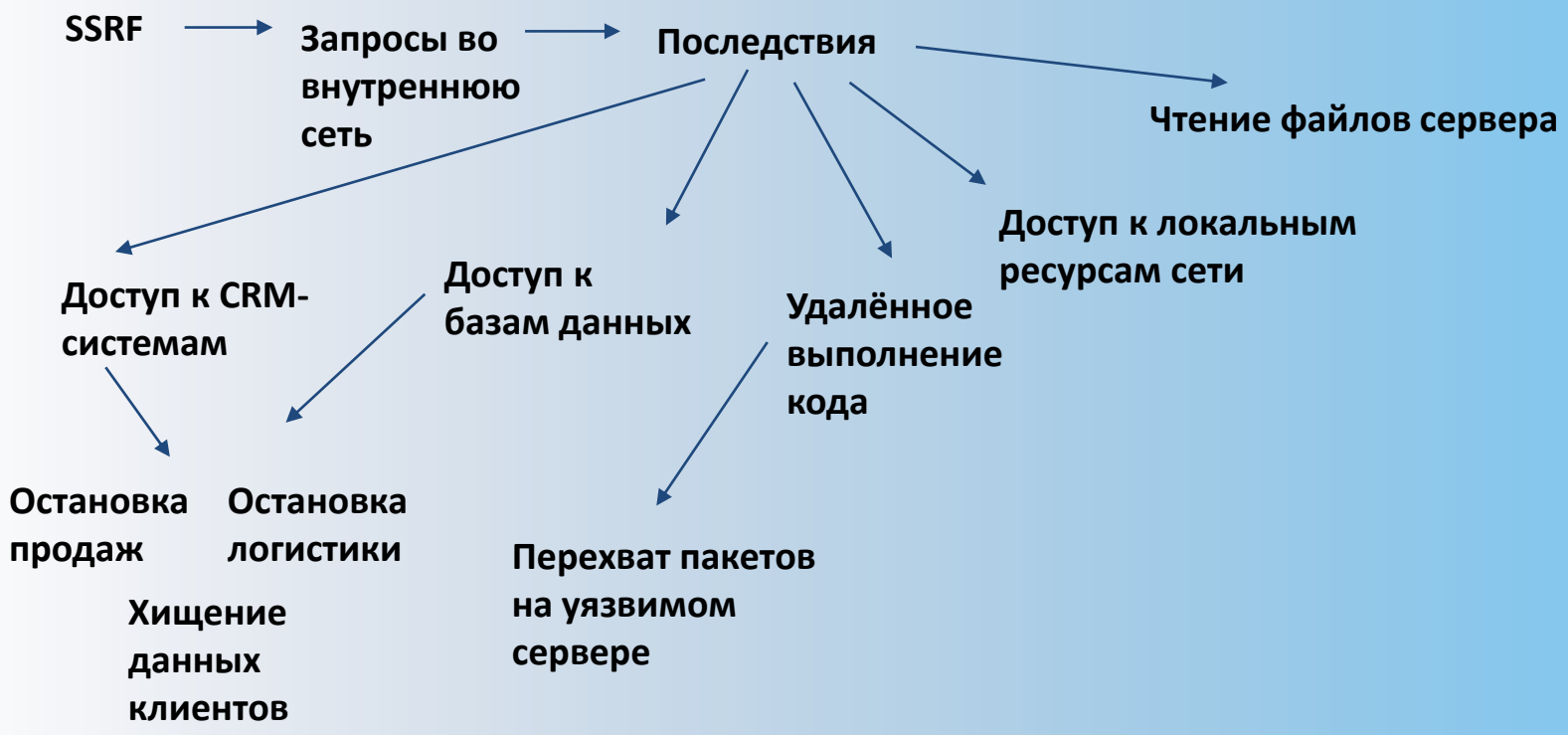
SSRF - подделка запроса на стороне сервера – это атака, которая позволяет отправлять запросы от имени сервера к внешним или внутренним ресурсам.

Вектор эксплуатации:

1)Злоумышленник находит уязвимость на веб-ресурсе

2)Отправляет вредоносный запрос

3)Получает доступ к внутренней сети



МОТИВЫ

1. Продажа в Dark Web
2. Конкурентная борьба
3. Шантаж
4. Обида
5. Странные мотивы

CODEBY
Your Upgrade

№ 2.1

Структура и вектора работы. Системный подход.

Вырабатываем кибериммунитет !

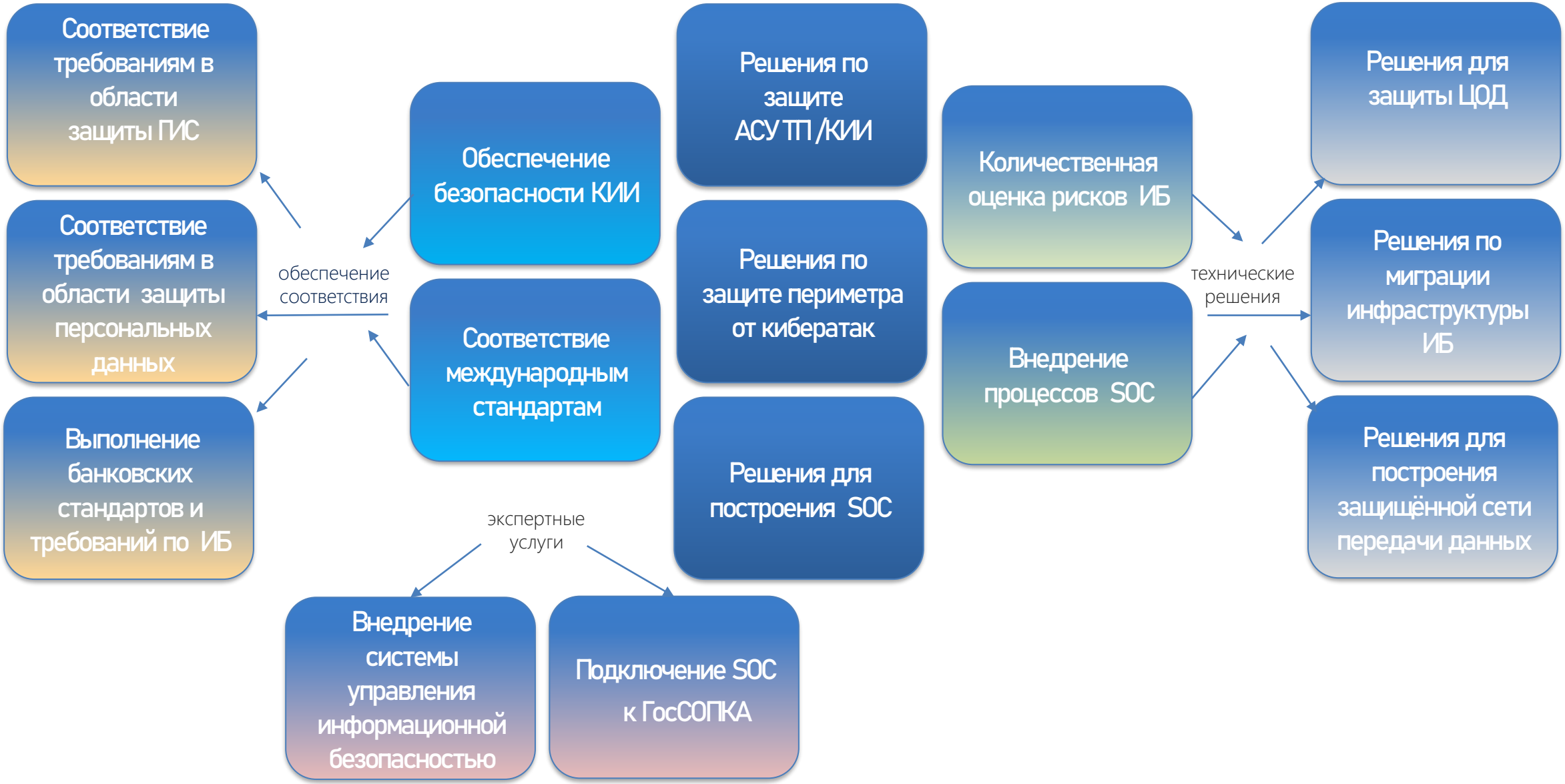
ВЫДЕРЖАТЬ БАЛАНС

Риски ИБ

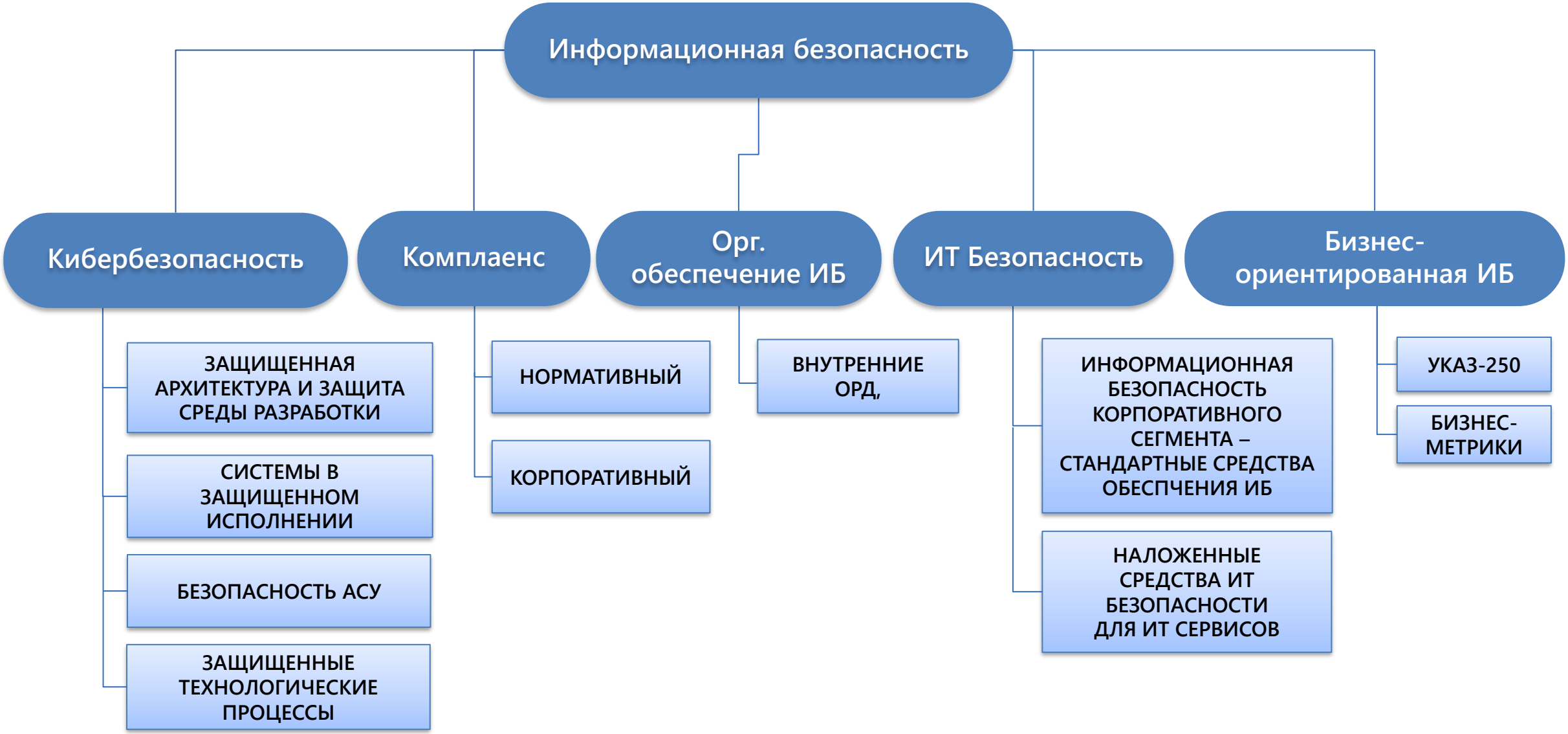
Затраты на систему ИБ

Обоснованный и сбалансированный бюджет на ИБ

ЗОНЫ ВНИМАНИЯ РУКОВОДИТЕЛЯ СЛУЖБЫ ИБ



СОСТАВЛЯЮЩИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
«ТО КАК МЕТОДИЧЕСКИ НЕПРАВИЛЬНО, НО В ЖИЗНИ ИМЕННО ТАК»



CODEBY
Your Upgrade

№2.2

Процессы, функции и системная архитектура

ВЕРХНЕУРОВНЕВАЯ АРХИТЕКТУРА КСИБ

КСИБ состоит из трех ключевых элементов:

Процессы управления и обеспечения ИБ	Риск-ориентированная модель ИБ	Сервисная модель обеспечения ИБ

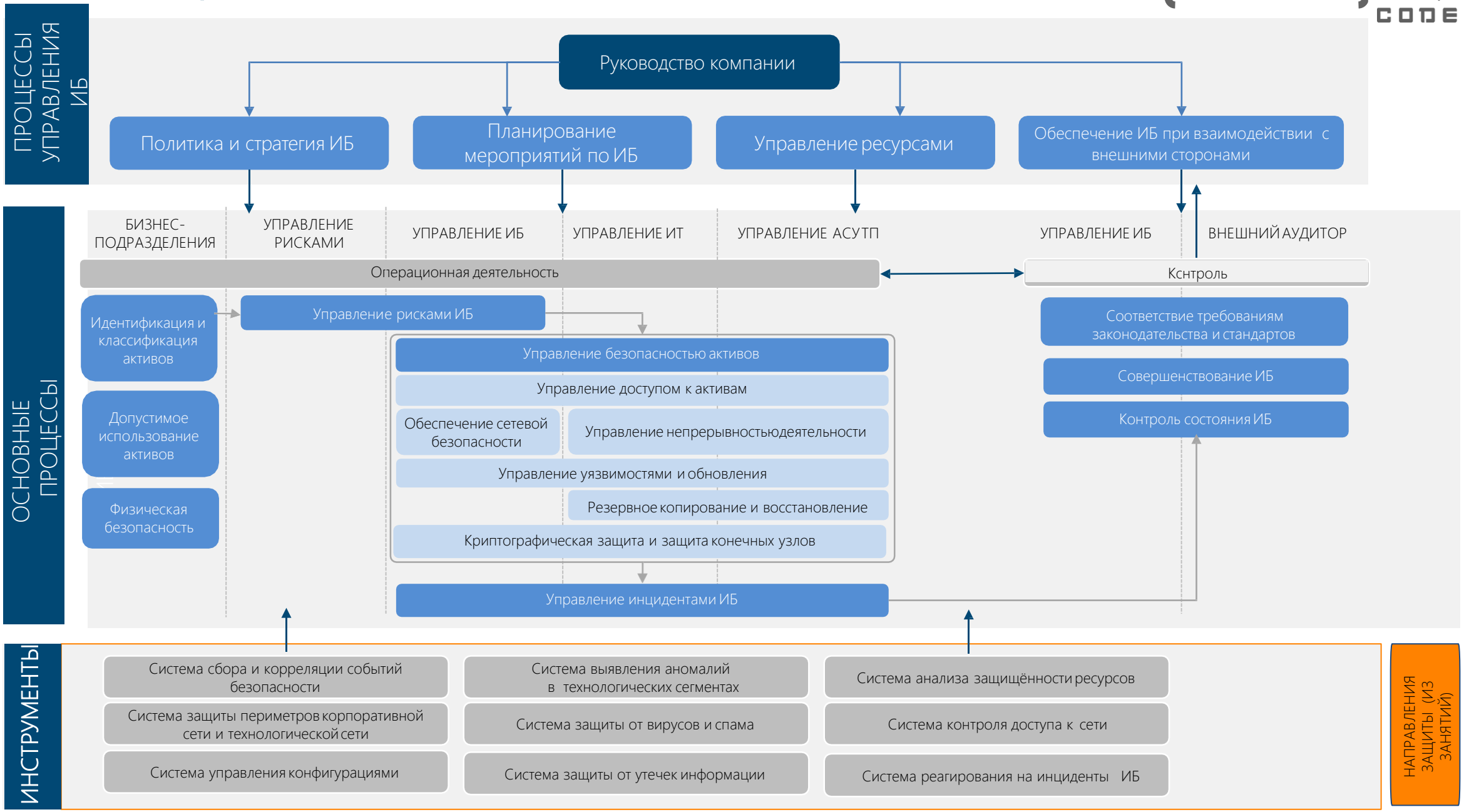
- Технические решения для
- эффективного обеспечения ИБ
- Централизованная техническая архитектура ИБ
- Единый технический стандарт ИБ

- Функции специалистов по ИБ
- Квалификация специалистов по ИБ
- Численность специалистов по ИБ

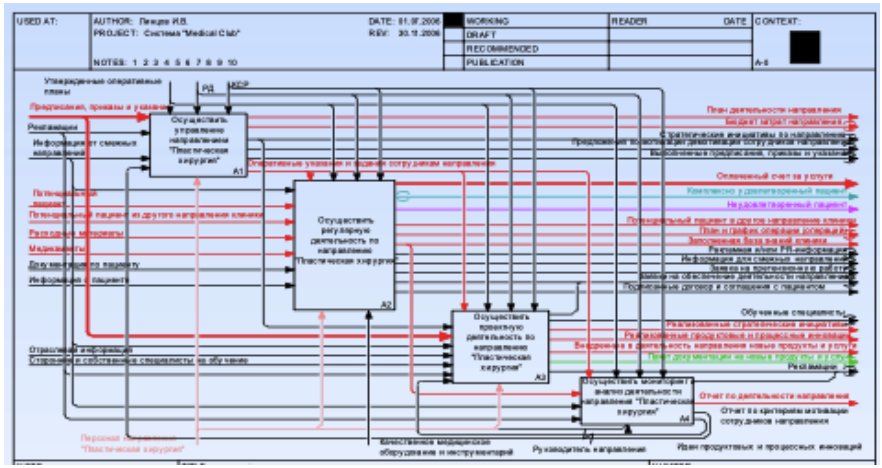
КАРТА ПРОЦЕССОВ УПРАВЛЕНИЯ И ОБЕСПЕЧЕНИЯ ИБ

BEST PRACTICE

СОПЕВУ



КАК ДОБИТЬСЯ ЭФФЕКТИВНОСТИ В РАБОТЕ СЛУЖБ ?



Управление по заданиям: Работает «КТО»

«Мягкий менеджмент»

Лидерство

Корпоративная культура

Мотивация

Человеческие отношения

Рулетка

Управление по функциям

Работает «ЧТО» (Руководящий документ)

«Жесткий менеджмент»

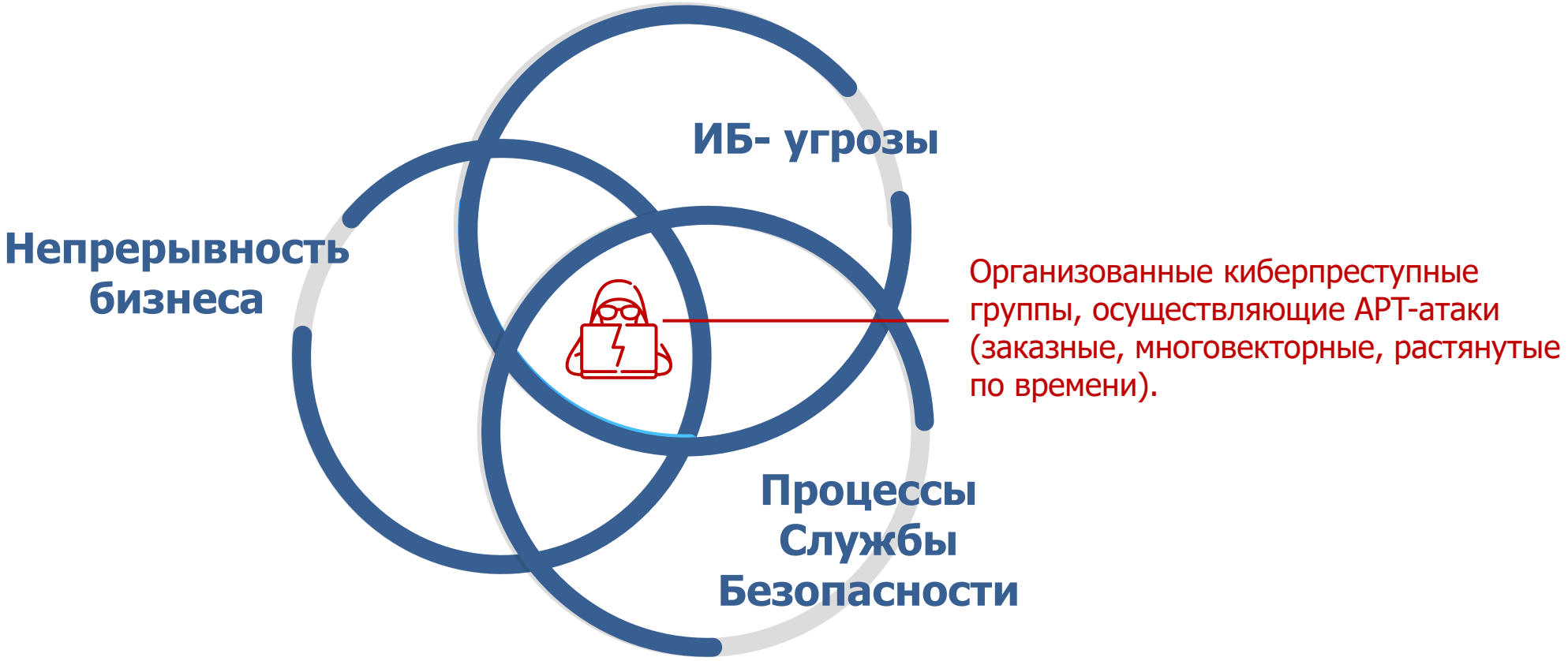
Структуры

Процессы

Руководящие документы

Ожидаемый результат

ВЕКТОР СОВРЕМЕННЫХ КИБЕРАТАК
НЕОБХОДИМОСТЬ В СОГЛАСОВАННОЙ ЭФФЕКТИВНОЙ РАБОТЕ СЛУЖБ



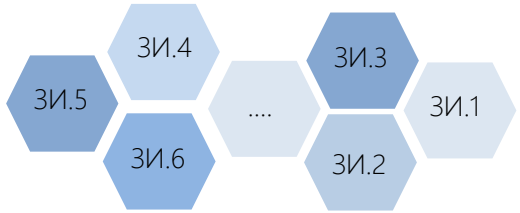
ОРГАНИЗАЦИОННАЯ СТРУКТУРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПОЗИЦИИ КРУПНОГО ПРЕДПРИЯТИЯ

НАПРАВЛЕНИЯ РАБОТЫ – ОБЩИЙ ВИД

Из этого следует –

Основные направления защиты информации и программы проектов ИБ

МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ



- определяет состав и содержание мер защиты информации
- определяет порядок выбора и применимость мер защиты информации в зависимости от типа ИС и АСУ ТП и сегментах их функционирования
- определяет требования к техническим решениям

ТЕХНИЧЕСКИЙ СТАНДАРТ

НАПРАВЛЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ	ПРОГРАММА ПРОЕКТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ИДЕНТИФИКАЦИЯ	П1 Система учета активов и управления рисками ИБ
	П2 Система контроля защищённости ИТ-ресурсов
ЗАЩИТА	П3 Система защиты периметра сети
	П4 Системы управления доступом, антивирусной защиты и защиты хостов
ОБНАРУЖЕНИЕ	П5 Единая система сбора и корреляции событий безопасности
	П6 Система обнаружения аномалий в технологических сегментах
РЕАГИРОВАНИЕ	П7 Система мониторинга, обработки и реагирования на инциденты ИБ
	П8 Система повышения осведомленности персонала в вопросах ИБ
ВОССТАНОВЛЕНИЕ	П9 Система резервного копирования и восстановления данных
	П10 Система контроля неизменности конфигурации

CODEBY
Your Upgrade

№ 3.1

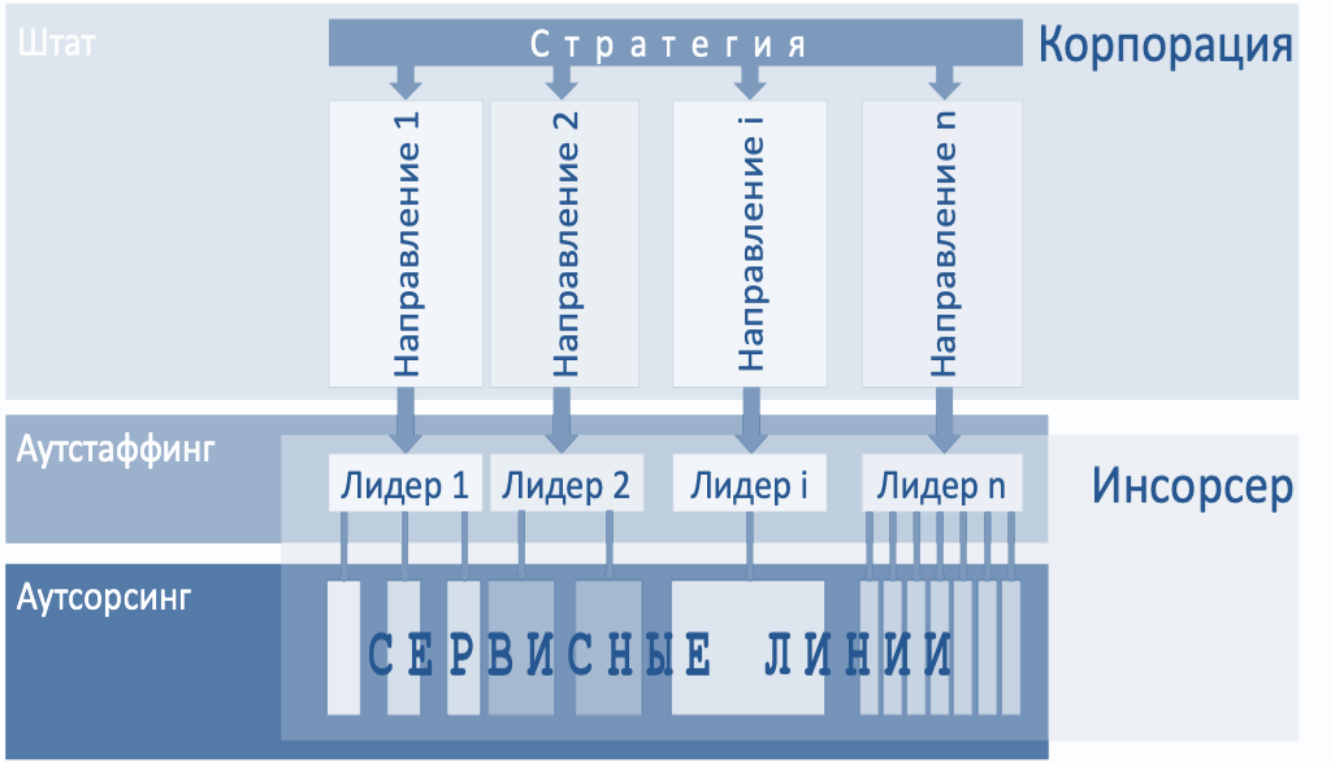
С чего начать?

Пройдемся по шагам

РАССТАВИТЬ АКЦЕНТЫ

- *Сформировать структуру*
- *Определить, чем для нас является непрерывность бизнеса*
- *Разделить процессы*
- *Определить принципиальную модель обеспечения ИБ*
- *Определить ключевую регуляторику*
- *Определить принципиальные цели и задачи*
- *Определить принципиальную модель проведения аудита ИБ и принятия решения*

СПОСОБЫ ОБРАБОТКИ РИСКОВ ИБ И МОДЕЛИ ПРЕДОСТАВЛЕНИЯ УСЛУГ



КЛЮЧЕВЫЕ ВОПРОСЫ ПРИ ВЫБОРЕ МОДЕЛИ ОБЕСПЕЧЕНИЯ ИБ

Чьи ресурсы (железо/софт) ?

1. Сервис -провайдера
2. Заказчика

Что покупаем ?

1. Покупаем сервис безопасности
2. Покупает конкретные услуги

Если оборудование наше, то кто обслуживает ?

1. Сервис-провайдер
2. На нашей стороне есть свои компетенции – обслуживает сам

CODEBY
Your Upgrade

№3.2

Какие инструменты ?

ОТ БИЗНЕС-ПРОЦЕССОВ И РИСКОВ ИБ К ЭКОНОМИЧЕСКОЙ ОЦЕНКЕ

ПРОЦЕССЫ БИЗНЕСА

1 Определение управленческих, ***технологических, производственных***, финансово-экономических и (или) иных процессов

Перечень процессов предприятия по следующим подсистемам:

- Подсистема стратегического управления
- Подсистема контроля и оперативного управления
- Подсистема обеспчения
- ПОДСИСТЕМА ОСНОВНОЙ ДЕЯТЕЛЬНОСТИ

КИБЕРРИСКИ

2 Определение ***возможности возникновения*** негативных последствий вследствие нарушения процессов предприятия, и соответственно вытекающие из них риски информационной безопасности

Из чего складывается:

- Критичные процессы
- Негативные последствия
- Актуальные угрозы
- Возможные сценарии
- Возможные меры защиты

ЭКОНОМИКА

3 Расчет стоимости рисков, расчет возврата инвестиций от внедрения систем ИБ, расчет зрелости системы для инвестора, расчет остаточных рисков и еще 10 параметров.

Перечень доступных инструментов:

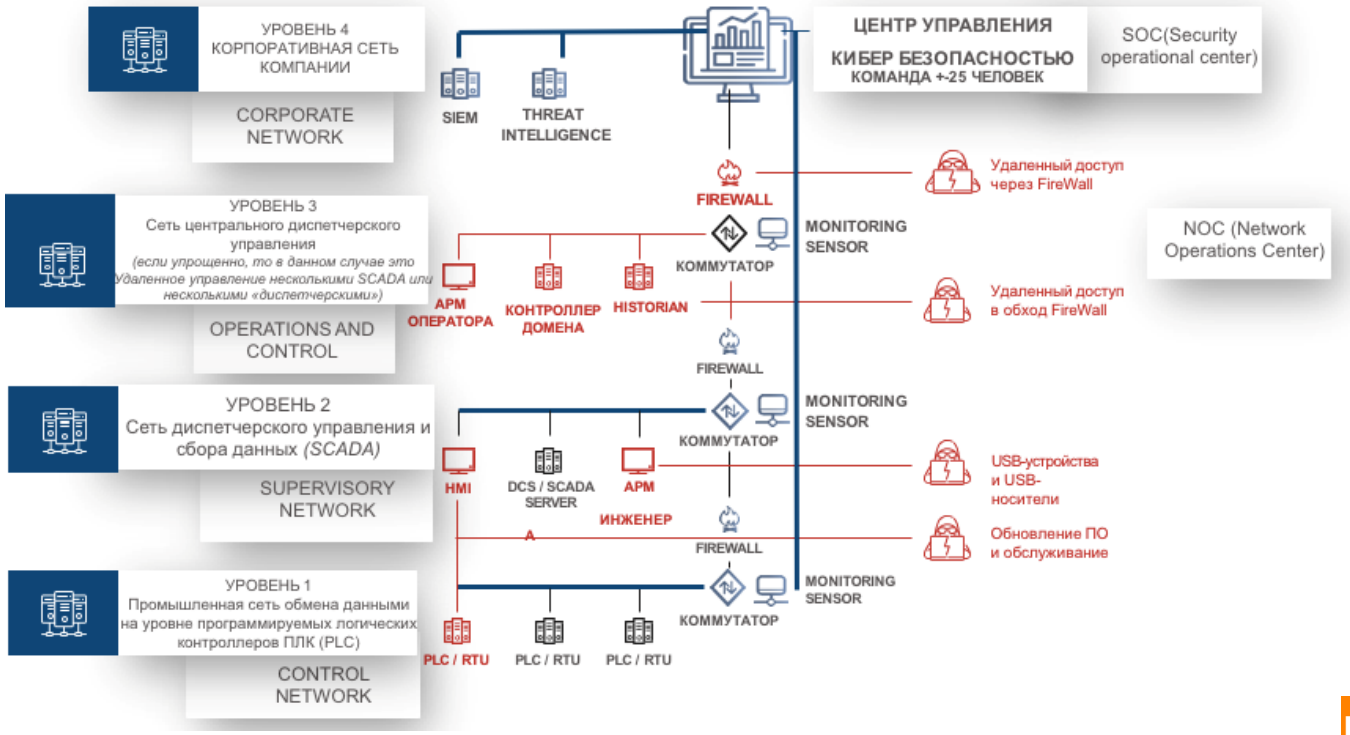
1: Инструменты и методики для форматирования бизнес-процессов

2: Матрица рисков и угроз ИБ

3: Модель приоритезации реализации проектов и расчета финансово-экономических показателей

«ПРИБОРНАЯ ПАНЕЛЬ» БИЗНЕСА И ПОДСИСТЕМЫ БИЗНЕС-МАШИНЫ

КАК НЕГАТИВНЫЕ СЦЕНАРИИ СВЯЗЫВАЮТСЯ С БИЗНЕС-ПРОЦЕССАМИ ?



На каком уровне действуют атакующие ?

- ПОДСИСТЕМА СТРАТЕГИЧЕСКОГО УПРАВЛЕНИЯ
- ПОДСИСТЕМА ОПЕРАТИВНОГО УПРАВЛЕНИЯ И КОНТРОЛЯ
- ПОДСИСТЕМА ОСНОВНОЙ (РЕГУЛЯРНОЙ) ДЕЯТЕЛЬНОСТИ
- ПОДСИСТЕМА ОБЕСПЕЧЕНИЯ

ГДЕ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ?

ИНСТРУМЕНТЫ

Инструменты диагностики деятельности организации

Проект
«Маленькие победы»
(«Тушение пожаров»)

1. «Три слайда»;
2. Документ «КСР» ;
3. Документ «Стратегия Развития..»

Инструменты стратегического менеджмента

Инструменты проектирования «жесткого» каркаса организации

1. Система Бизнес-Процессов (ЦДС)
2. Опережающие технологии для критичных БП
3. Структура 4. РД 5. IT-решение

1. Утвержденная система мотивации
2. Модель корпоративной культуры

Инструменты проектирования «мягкой» организационной модели организации

ГДЕ ИБ В КОНТЕКСТЕ СТРАТЕГИИ КОМПАНИИ ?

Как правильно сформулировать главную проблему организации?

Конструкция формулировки главной стратегической проблемы: проблема внутри, проблема внешняя.
ОТ ЭТОГО – АКЦЕНТЫ НА ВНЕШНЕЙ ИЛИ ВНУТРЕННЕЙ БЕЗОПАСНОСТИ

- Информационная безопасность «находится» в бизнес-процессах (подсистеме) обеспечения
- Что пальпировать… в каком срезе: финансовая деятельность, операционная деятельность или инвестиционная? Откуда бюджет – как обосновать?
- Что есть эталон для сравнения ?
- Как консолидировать результаты ?
- Как добиться единообразного понимания результатов исследования организации всеми руководителями?
- Как проанализировать управленческую успешность конкретного владельца бизнес-процесса?

CODEBY
Your Upgrade

№3.3

Как проверить свою безопасность?

ЭТАПЫ ПРОВЕДЕНИЯ АУДИТА ИБ

Обследование	Категорирование информационных ресурсов	Анализ защищенности	Разработка рекомендаций
1. Сбор данных о процессах обработки защищаемой информации 2. Сбор данных об ИТ-инфраструктуре 3. Сбор данных о применяемых организационных и технических мерах защиты информации	1. Определение ресурсов, подлежащих защите 2. Определение владельцев ресурсов 3. Оценка степени критичности ресурсов 4. Формирование перечня ресурсов с указанием их критичности	1. Анализ применяемых технических мер защиты 2. Анализ процессов управления ИБ 3. Анализ организационно-распорядительных документов по ИБ 4. Анализ угроз ИБ 5. Анализ бизнес-процессов на наличие возможных каналов утечки информации 6. Инструментальный анализ защищенности	1. Методические указания и рекомендации по локализации, устранению и контролю выявленных недостатков 2. Рекомендации по внедрению дополнительных СЗИ 3. Рекомендации по разработке или доработке организационно-распорядительной документации 4. Рекомендации по устранению выявленных уязвимостей 5. Рекомендации по изменению конфигураций и настроек сетевых средств защиты информации.

ВЫБИРАЕМ АКТУАЛЬНЫЕ ТРЕБОВАНИЯ

Основные требования, на соответствие которым проводится аудит ИБ

Основные Российские и международные НПА, стандарты

Общий аудит на соответствие законодательству РФ по ИБ

152-ФЗ, 149-ФЗ, 98-ФЗ,

документы ФСТЭК и ФСБ России и другие

Российские и международные стандарты

ISO/IEC 27001, ISO/IEC 27002, NIST 800, СТО БР, стандарты по процессам ИБ, ГОСТ Р ИСО 19011-XXXX, ГОСТ Р ИСО/МЭК 27007-XXXX и другие.

Лучшие практики по обеспечению ИБ

Network Security Policy: Best Practices White Paper, Network Management System

Внутренние требования Заказчика

Выполнение особых задач, соответствие корпоративному комплаенсу

Заточенный аудит на соответствие нормативным требованиям, например по 187-ФЗ

Приказ ФСТЭК №235, №239. При проведении аудита опираемся на последовательность действий, которая выработана на основе ГОСТ Р ИСО 19011-2012 и методики ниже на следующем слайде

Отраслевые требования..

Аудит на соответствие требованиям отраслевых регуляторов

CODEBY
Your Upgrade

№3.4

Добрались до составления карты рисков =)

ОЦЕНКА ПОТЕНЦИАЛЬНЫХ РАСХОДОВ НА ЛИКВИДАЦИЮ ПОСЛЕДСТВИЙ

BEST PRACTICE

Категории возможного ущерба

ОБОРУДОВАНИЕ И РАБОТЫ
(Стоимость восстановления и ремонта средств / закупка нового оборудования)

Средства обеспечения ИБ

+

Средства обеспечения основной деятельности предприятия (системы управления технологическим процессом)

Средства обеспечения поддерживающей деятельности организации (ИТ-системы корпоративный сегмент)

ПРИБЫЛЬ
(Упущенная прибыль)

Прямые материальные убытки

+

Потенциальные убытки, в том числе, связанные с потерей производительности

КОМПЛАЕНС
(Издержки, возникающие вследствие наступления инцидента и повлекшие за собой нарушение законодательства)

Судебные издержки (работа юридической службы)

Штрафные санкции

Мероприятия по минимизации рисков, связанных с ответственностью лица (в случае уголовной ответственности)*

ПОДХОДЫ К ОЦЕНКЕ РИСКОВ ИБ

BEST PRACTICE

Оценка рисков ИБ – это процесс присвоения значений вероятности и последствий риска ИБ

ОБЩИЙ ПОДХОД К ОЦЕНКЕ РИСКОВ ИБ

1. ИДЕНТИФИКАЦИЯ

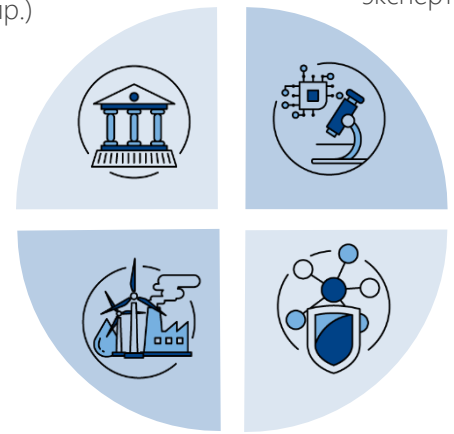
- критичных бизнес-процессов
- критичных активов – ИС, АСУ П, АСУ ТП, сервисов, агрегатов
- основных характеристик ИТ-инфраструктуры

2. ОПРЕДЕЛЕНИЕ КОНТЕКСТА

- применимых требований законодательства (152-ФЗ, ФЗ-98, 187-ФЗ, 149-ФЗ, GDPR и пр.)
- положений международных и национальных стандартов и рекомендаций (NIST, ENISA, ISO, ENISA и пр.)

3. ИССЛЕДОВАНИЕ

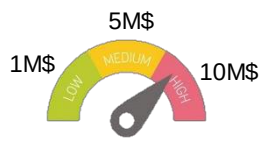
- анализ данных об инцидентах ИБ внутри Компании и их последствий
- анализ внешних источников данных об инцидентах ИБ
- экспертная оценка



4. ОЦЕНКА

- формирование реестра угроз и рисков ИБ
- определение основных сценариев реализации угроз
- определение величины рисков ИБ

Методология оценки рисков ИБ



	Качественная	Количественная	Комбинированная
Определение уровней рисков ИБ	+	+	+
Понимание размера возможных потерь в деньгах и соотнесение с затратами на ИБ	−	+	±
Наличие методологической основы для оценки рисков ИБ	+	−	±
Затраты и сложность выполнения оценки рисков			
Наличие опыта у ЦКИБ	+	±	+

ПРОЙТИСЬ ПО ШАГАМ ОЦЕНКИ РИСКОВ ИБ

ПРИМЕР РАСЧЕТА КОЛИЧЕСТВЕННЫХ РИСКОВ ИБ

ВЛАДЕЛЬЦЫ БИЗНЕС-ПРОЦЕССОВ

- ✓ предоставляют информацию о потерях вследствие негативного влияния на процесс
- ✓ предоставляют информацию о критичности ИТ-активов для бизнес-процессов

35 000 $/ч

Технологический процесс «Производство стали»

ПОДПРОЦЕССЫ

- *Первая холодная прокатка* — 71%
- *Вторая холодная прокатка* — 22%
- *Высокотемпературный отжиг в колпаковых печах* — 2%
- *Обработка металла на агрегатах выпрямляющего отжига* — 5%

Активы

АСУ ТП

- АСУ стана «1300»
- АСУ станов «1200-1,2»
- АСУ ВТО
- АСУ АВО

Оборудование

Информация

ПО

Сервисы

УЯЗВИМОСТИ

- отсутствие средств контроля внесения изменений в протоколы передачи данных
- отсутствие системы разграничения доступа
- отсутствие средств антивирусной защиты

УГРОЗЫ ИБ

- угроза внедрения вредоносного кода
- угроза внесения изменений в сетевые протоколы передачи данных
- угроза несанкционированного создания учётной записи

РАСЧЕТ КРИТИЧНОСТИ (ЦЕННОСТИ) АКТИВА

Критичность АСУ станов «1200-1,2» = *35 000 $/ч* × *22%* = ***7 700 $/ч***

РАСЧЕТ ВЕРОЯТНОСТИ УГРОЗЫ

Вероятность реализации угрозы = *100%* (*Вероятность эксплуатации уязвимости*) × *75%* (*Вероятность угрозы*) = ***75%***

ВРЕМЯ ВОЗДЕЙСТВИЯ

24ч

Время воздействия угрозы и восстановления актива

РИСК ИБ

138 600 $

CODEBY
Your Upgrade

№3.5

Регуляторные риски

Принципиальные изменения 2022

Взаимодействие по линии Роскомнадзора

Исходя из изменений в ФЗ-152 и итогам года

1. Закрепили статус «инцидентов»

✓ Теперь это «компьютерные инциденты, повлекшие неправомерную или случайную передачу (предоставление, доступ) Пдн»

2. Бизнес обязан оперативно уведомлять государство об инцидентах

✓ С 1 сентября в случае утечки компания обязана незамедлительно уведомить РКН (а также НКЦКИ), а именно:

- 24 часа с момента выявления о факте утечки ПД, затронутых данных и субъектах, принятых мерах
- 72 часа с момента выявления о результатах внутреннего расследования инцидента и виновных лицах (включая праздники и выходные)

3. РКН активно проводит проверки и штрафует компании за утечки

✓ **Если компания уведомила об утечке:**

- ✓ **РКН на своей стороне проверяет информацию в уведомлении;**
- ✓ **72 часа с момента выявления о результатах внутреннего расследования инцидента и виновных лицах**

✓ **Если РКН узнал об утечке из СМИ:**

- ✓ **РКН назначает внеплановую проверку (документарную или выездную)**
- ✓ **По итогам проверки компания получает протокол по ч.1 либо по ч.5 статьи 13.11 КоАП РФ**
- ✓ **И предписание по устранению нарушений (которые найдут)**

- **Компании сами уведомляют об утечках (- это работает)**
- **Тактика умалчивания – не лучшее решение**

- **Мораторий распространяется только на плановые проверки. На внеплановые проверки к РКН разрешение Правительства есть**

Куда мы движемся в 2023 г

Взаимодействие по линии Роскомнадзора

Исходя из последних НПА и новостей

1. Прямые оборотные штрафы

✓ *Исходя из прорабатываемых инициатив размер штрафа от 5 до 500 млн руб.*

2. Дополнительные штрафы за неуведомление РКН

✓ Несмотря на отсутствие конкретного законопроекта, это вполне вероятное последствие ужесточения порядка уведомлений

3. Проактивный контроль РКН за информацией об утечках

✓ РКН хочет автоматизировать мониторинг информации о сливах, возможна закупка подобной ситсемы

4. Вывод из моратория проверок по утечкам (плановых)

✓ В том числе для ИТ-компаний – такая инициатива поступила со стороны Госдумы

CODEBY
Your Upgrade

4.1

Построение системы защиты

ЧТО ДЕЛАТЬ ?

3	Создать эшелонированную защиту ПДн
2	Внедрить комплекс организационных и технических мер
1	Контролировать I Осведомлять I Наказывать

ЭШЕЛОНИРОВАННАЯ СИСТЕМА ЗАЩИТЫ – ВЫБИРАЕМ ТЕХНОЛОГИИ

ВНЕШНЕГО ПЕРИМЕТРА УЖЕ НЕТ

Определяющие факторы

- ✓ Специфика бизнес-процессов
- ✓ Производственные и операционные риски

- ✓ Ландшафт безопасности (тенденции)
- ✓ Актуальные угрозы и мотивация нарушителя
- ✓ Актуальные сценарии ИБ

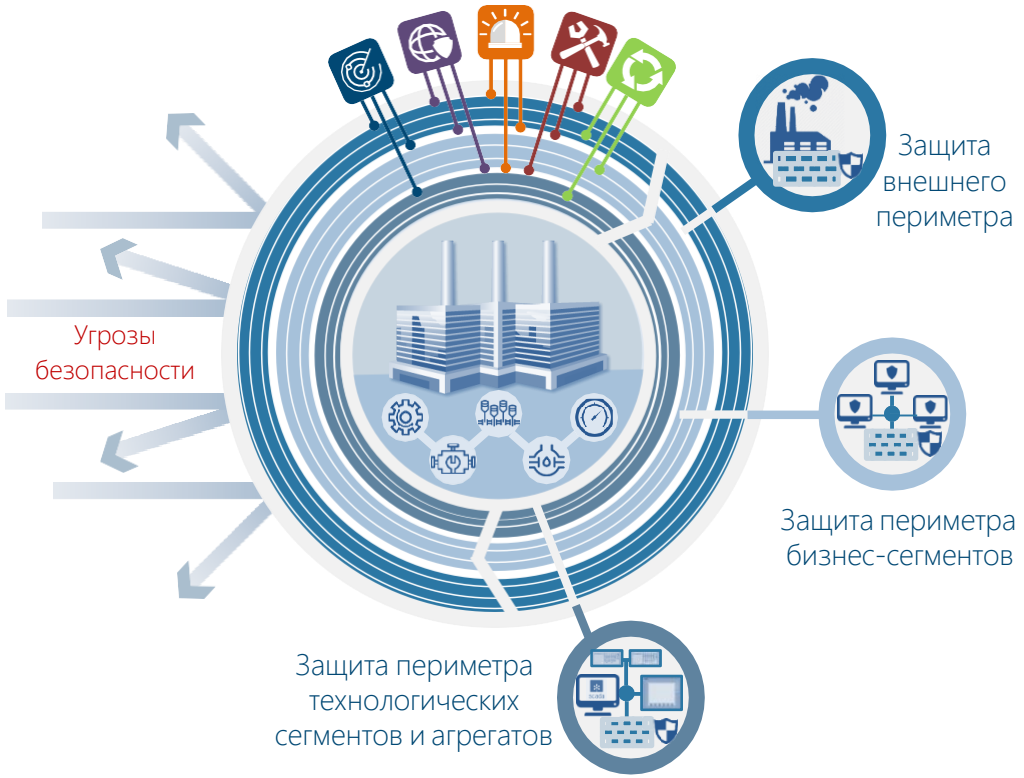
- ✓ География объектов защиты

- ✓ Организационно-штатная структура
- ✓ Квалификация персонала
- ✓ Модель эксплуатации АСУ и ИТ-систем
- ✓ Требования к непрерывности, SLA

- ✓ Наличие и зрелость процессов
- ✓ Степень централизации процессов

- ✓ Требования законодательства
- ✓ Отраслевые требования
- ✓ Внутренние нормативные акты
- ✓ Стандарты и мировые практики

- ✓ Топология и инфраструктура
- ✓ Архитектура АСУ и ИТ-систем
- ✓ Программные и технические средства
- ✓ Существующие средства защиты



SOC / SOAR

Кросс-интеграции со средствами системой мониторинга и анализа состояния и системой автоматизации процессов ИБ

Структура и состав

Сетевая безопасность

- ✓ Многофункциональные МЭ (NGFW)
- ✓ Микросегментация (Microsegmentation)
- ✓ Межсетевой экран веб-приложений (WAF)
- ✓ Защищенный удаленный доступ (VPN)
- ✓ Контроль доступа в Интернет (Web-Gateway)
- ✓ Защита электронной почты (Email Gateway)
- ✓ Предотвращение вторжений (IPS)
- ✓ Защита от DDoS-атак

Прикладная безопасность

- ✓ Антивирусная защита (Antivirus)
- ✓ Защита от утечек данных (DLP)
- ✓ Шифрование данных (Data/Disc Encryption)
- ✓ Защита от APT и 0-Day угроз (Sandbox)
- ✓ Защита баз данных (Database Protection)

Управление доступом

- ✓ Аутентификация и авторизация (AAA)
- ✓ Многофакторная аутентификация
- ✓ Управление мобильными устройствами (MDM)
- ✓ Управление привилегированным доступом (PIM)
- ✓ Управление идентификационными данными (IDM)

Аудит и мониторинг

- ✓ Управление уязвимостями (Vulnerability Manager)
- ✓ Выявление сетевых аномалий (Anomaly Detection)
- ✓ Профилирование сетевой активности (NBA)
- ✓ Профилирование активности пользователей (UBA)
- ✓ Анализаторы исходного кода

КАК СВЯЗАТЬ РИСКИ И ПРОЕКТЫ ИБ? КАК ПОНЯТЬ ЧТО НАМ НУЖНО ?

ИСХОДНЫЕ ДАННЫЕ

Основа для определения набора угроз, сценариев, актуальных угроз и рисков ИБ

ТАКСОНОМИЯ УГРОЗ

БАНК ДАННЫХ УГРОЗ ФСТЭК РОССИИ

РЕЗУЛЬТАТЫ ОЦЕНКИ РИСКОВ ИБ

Результаты оценки критичности активов

КАТЕГОРИИ/ УРОВНИ ЗНАЧИМОСТИ

Внешние требования нормативных документов и стандартов ИБ

ЗАКОНОДАТЕЛЬСТВО РФ

152-ФЗ 187-ФЗ

149-ФЗ 98-ФЗ

МЕЖДУНАРОДНЫЕ ТРЕБОВАНИЯ ПО ИБ И СТАНДАРТЫ ИБ

АКТУАЛЬНЫЕ УГРОЗЫ И РИСКИ ИБ

УГРОЗЫ	СЦЕНАРИИ	РИСКИ	МЕРЫ ЗАЩИТЫ*
Угрозы внедрения и эксплуатации вредоносного ПО	Вирусное заражение, в том числе внедрение вирусов-шифровальщиков	Нарушение непрерывности бизнес-процессов и/или приостановка производства	ЗИ.1 Выявление несанкционированных действий персонала (использование несанкционированных сетевых подключений, устройств, программного обеспечения)
		Несанкционированное изменение информации	ЗИ.2 Обнаружение вредоносного кода
		Разглашение и утечка информации, составляющей коммерческую тайну	ЗИ.3 Контроль портов ввода (вывода) конфиденциальной информации
Угрозы компрометации учетных записей пользователей и администраторов	Скрытое получение злоумышленником контроля над ИТ-инфраструктурой путем реализации целенаправленной атаки	Нарушение непрерывности бизнес-процессов и/или приостановка производства	ЗИ.4 Определение ролей и обязанностей по обнаружению потенциально негативных и/или аномальных событий ИБ
		Несанкционированное изменение информации	ЗИ.5 Изучение уведомлений от систем, позволяющих обнаружить инциденты ИБ
		Разглашение и утечка информации, составляющей коммерческую тайну	ЗИ.6 Мониторинг сети с целью обнаружения инцидентов ИБ
Угрозы, реализуемые с использованием уязвимостей сетевых протоколов и сетевых уязвимостей	Подмена параметров технологического процесса вследствие действий киберпресутпников	Нарушение непрерывности бизнес-процессов и/или приостановка производства	ЗИ.7 Определение и периодическое уточнение типовых сетевых операций и потоков данных для пользователей и систем
		Несанкционированное изменение информации	ЗИ.8 Контроль конфигураций компонентов ИС и АСУ ТП ...

НА ОСНОВАНИИ ДАННЫХ ВЫБИРАЕМ МЕРЫ ЗАЩИТЫ

Унификация мер по одному стандарту для предприятия.

Унифицируем меры в таблица с перечнем конкретных мер и указанием, для каких типов систем эти меры должны применяться.

Направление Защиты	Группа мер	Мера защиты	Применимость согласно техническому стандарту ИБ	Группы угроз
Идентификация			ИСПДн, ЗООКИИ, КТ, АСУ ТП, иные	Угрозы УБИ-1 … УБИ-10
Защита				
Обнаружение				
Реагирование				
Восстановление				

БДУ ФСТЭК

Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

NISTIR 8183 «Cybersecurity Framework Manufacturing Profile»

БАЗОВЫЕ СОСТАВЛЯЮЩИЕ БЮДЖЕТА СЛУЖБЫ ИБ

Какие основные типы затрат на ИБ?	*«Сверстанный» бюджет* службы информационной безопасности можно рассмотреть на уровне простой модели как комплекс трех составляющих компонент.

«В конечном счете, нужно понимать, что рано или поздно мы будем взломаны. Вопрос в том какие будут последствия и как мы быстро их минимизируем»

«Тогда возникает другой вопрос : а может быть мы специально оставим организационную/техническую брешь (BackDoor) или сымитируем его (Honeypot) на том участке, где нам это выгоднее? Таким образом мы поймем ряд признаков, в том числе цели и характер действий злоумышленника»

КАТЕГОРИИ ЗАТРАТ НА БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ АКТИВОВ

(разделение до и после инцидент а ИБ)

CODEBY
Your Upgrade

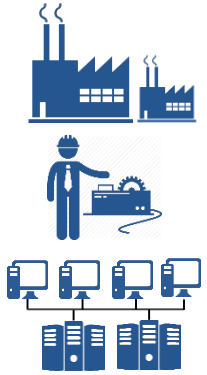
5

Экономика

РАСЧЕТ ПОКАЗАТЕЛЯ ВОЗВРАТА ИНВЕСТИЦИЙ В ИБ.
ДЕКОМПОЗИРУЕМ ПОКАЗАТЕЛИ

РЕЗУЛЬТАТЫ ОЦЕНКИ РИСКОВ ДЛЯ ХОЛДИНГА

ИСХОДНЫЕ ДАННЫЕ



Сведения об активах Компании:

- сведения о предприятиях
- сведения о технологических процессах предприятий
- сведения об агрегатах
- сведения об объектах ИТ-инфраструктуры
- сведения о реализованных мерах защиты информации

Сведения для расчета потенциального ущерба:

Внутренние документы Компании:

- стоимость простоев агрегатов
- стоимость отдельных документов и данных
- сведения об инцидентах ИБ в Компании

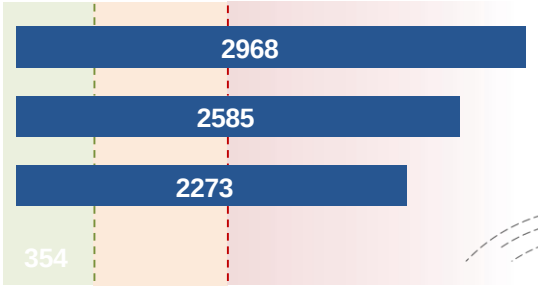
Внешние источники (аналитические агентства, сообщения в СМИ):

- сведения об инцидентах в отрасли (частоте возникновения, времени воздействия, потерях от инцидентов)
- стоимость отдельных документов и данных

	ЗАТРАТЫ НА ПРОЕКТ	ВЕЛИЧИНА СНИЖАЕМЫХ РИСКОВ
П1 Система учета активов и управления рисками ИБ	50 млн р.	100 млн р.
П2 Система контроля защищённости ИТ-ресурсов	10 млн р.	200 млн р.
П3 Система защиты периметра сети	30 млн р.	300 млн р.
Проект N	N млн р.	N млн р.
• • •		
Итоговые затраты на Программу проектов ИБ	300 млн р.	1000 млн р.

КЛЮЧЕВЫЕ РЕЗУЛЬТАТЫ

Ожидаемые средние потери в разрезе отдельных рисков ИБ (ALE), млн р./год



«РИСК-АППЕТИТ»

Ожидаемые средние потери в разрезе всех рисков ИБ, млн р./год

Величина последствий реализации рисков ИБ

Ожидаемые потери от реализации рисков ИБ за 5 лет, млн р.

Финансовые и экономические последствия	10 898

ВКЛАД ПРОЕКТОВ В НЕЙТРАЛИЗАЦИЮ СЦЕНАРИЕВ

Рассмотрим на примере количественную оценку по проектам (вклад в нейтрализацию актуальных угроз)

Обозначение сценария	Наименование сценария	Приоритет нейтрализации сценария с учетом качественной оценки уровня рисков ИБ	Единая система сбора и корреляции событий информационной безопасности	Система обнаружения вторжений и аномалий в локальной сети предприятий	Система обнаружения вторжений и аномалий в технологических сегментах предприятий	Система защиты периметра корпоративной сети	Система защиты АРМ и серверов	Обеспечение соответствия требованиям регуляторов и международным стандартам информационной безопасности
			П01	П02	П03	П04	П05	П06
S1	Вирусное заражение, в том числе внедрение вирусов-шифровальщиков	9,1						
S2	Скрытое получение злоумышленником контроля над ИТ-инфраструктурой и большим объемом критичных данных путем реализации целенаправленной атаки	16,3						
S3	Подмена параметров технологического процесса вследствие действий киберпреступников	11,3						
S4	Изменение параметров конфигурации технологического оборудования вследствие действий киберпреступников	11,3						
S5	Нецелевое использование вычислительных и электрических мощностей Компании, в том числе майнинг криптовалют	3,2						
S6	Нарушение доступности внешних ресурсов Компании вследствие сетевой DoS-атаки	5,7						
S7	Наложение санкций регуляторами в области ИБ за нарушения в области защиты персональных данных или требований по защите КИИ	1,0						
S8	Нарушение работоспособности систем из-за ошибок в действиях пользователей, наступившее вследствие недостаточности мер ИБ	7,1						
S9	Хищение данных путем несанкционированного копирования информации (на съемные носители, внешние почтовые сервисы, в мессенджеры и т.п.) или хищения носителей информации	6,2						
S10	Нарушение работы компании политически мотивированными хакерами или террористическими группировками	25,0						

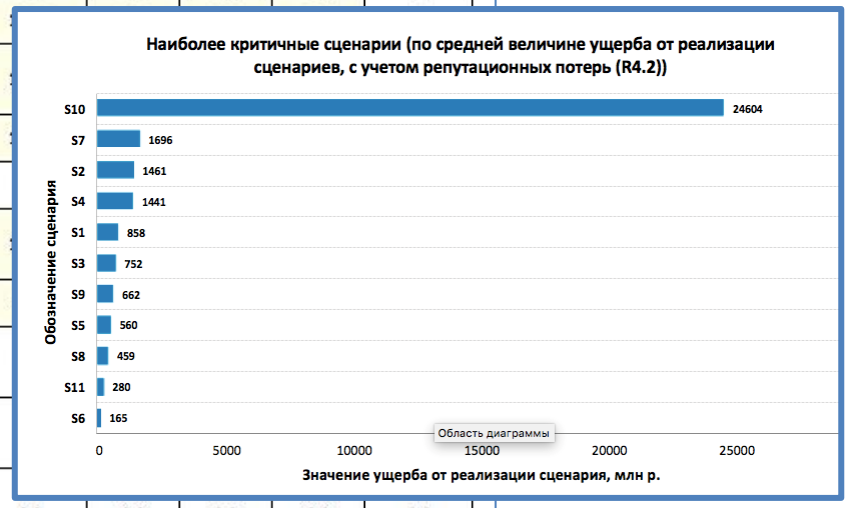
ИБ						
ем несанкционированного копирования мные носители, внешние почтовые еры и т.п.) или хищения носителей	6,2					
омпании политически мотивированными истическими группировками	25,0					
еннего мошенничества с использованием ролей путем взлома компьютерных систем	3,9					
Доля вклада проекта в нейтрализацию сценария:		**9,62**	**6,44**	**7,57**	**8,25**	**5,0**
		1,1	1,1	1,1	1,0	1,

РЕПУТАЦИОННЫЕ РИСКИ (ВАЖНО ДЛЯ СТРАХОВОЙ КОМПАНИИ)

Рассмотрим на примере расчет репутационных рисков

S1	Вирусное заражение, в том числе внедрение вирусов-шифровальщиков	1359
S2	Скрытое получение злоумышленником контроля над ИТ-инфраструктурой и большим объемом критичных данных путем реализации целенаправленной атаки	2399
S3	Подмена параметров технологического процесса вследствие действий киберпреступников	1120
S4	Изменение параметров конфигурации технологического оборудования вследствие действий киберпреступников	560
S5	Нецелевое использование вычислительных и электрических мощностей Компании, в том числе майнинг криптовалют	1120
S6	Нарушение доступности внешних ресурсов Компании вследствие сетевой DoS-атаки	240
S7	Наложение санкций регуляторами в области ИБ за нарушения в области защиты персональных данных или требований по защите КИИ	1120
S8	Нарушение работоспособности систем из-за ошибок в действиях пользователей, наступившее вследствие недостаточности мер ИБ	800
S9	Хищение данных путем несанкционированного копирования информации (на съемные носители, внешние почтовые сервисы, в мессенджеры и т.п.) или хищения носителей информации	560
S10	Нарушение работы компании политически мотивированными хакерами или террористическими группировками	3279
S11	Осуществление внутреннего мошенничества с использованием методов обхода контролей путем взлома компьютерных систем	560
	Величина покрываемого ущерба (млн р.):	
	Величина покрываемых рисков ИБ (млн р.):	

	Репутационный ущерб от реализации сценария (млн р.)	Единая система сбора и корре информационной безоп	Система обнаружения вторжени локальной сети предпр	Система обнаружения вторжени технологических сегментах п	Система защиты периметра кор	Система защиты АРМ и с	Обеспечение соответствия тр регуляторов и международны информационной безоп
		П01	П02	П03	П04	П05	П06
		1,1	1,1	1,1	1,0	1,0	1,1
русов-	1359	166,6					
я над ИТ-их данных	2399	158,4					
а	1120	109,7					
ического упников	560	54,7					
е майнинг	1120	183,4					
пании	240	27,2					
за ных или	1120	0,0					
ибок в зие	800	112,8					
и, п.) или	560	87,9	0,0	0,0	0,0	0,0	0,0
кими	3279	242,1	243,1	244,9	233,7	227,5	250,3
ем взлома	560	0,0	0,0	0,0	134,1	0,0	0,0
окрываемого ущерба (млн р.):		1143	891	953	1143	828	716
рываемых рисков ИБ (млн р.):		104	81	87	104	75	65



РЕЙТИНГ ПРОЕКТОВ ДЛЯ ПРИОРИТИЗАЦИИ

Рассмотрим на примере расчет рейтинга

Ранжирование проектов по величине снижаемого ими прямого ущерба (ранжирование по коэффициенту)

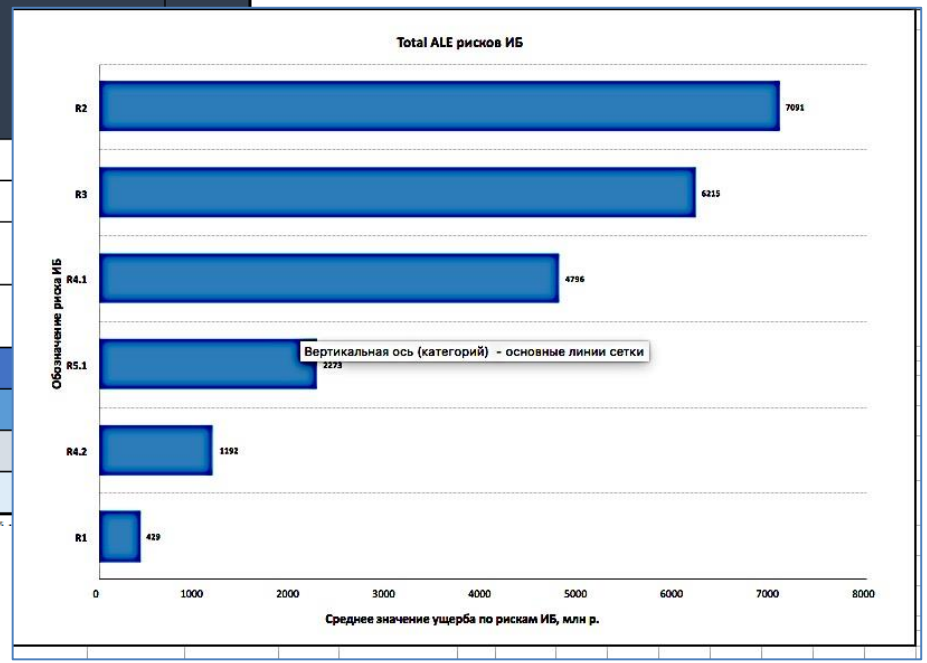
Код	Наименование	Сумма снижения прямого ущерба (млн р.)	Стоимость проекта (млн р.)	Коэфф. отношения прямого ущерба к затратам на КСИ
П06	Обеспечение соответствия требованиям регуляторов и международным стандартам информационной безопасности	4381	0	#ССЫЛКА!
П19	Система защиты от таргетированных атак	3889	48	80
П10	Система контроля и анализа событий информационной безопасности	3807	76	50
П15	Система защиты сред виртуализации	4206	63	67
П08	Система анализа защищенности ИТ ресурсов	3900	61	64
П18	Система защиты внешних ресурсов	36	4	9
П01	Единая система сбора и корреляции событий информационной безопасности	3881	161	24
П05	Система защиты АРМ и серверов	3817	95	40
П09	Система контроля доступа к локальной сети	4478	99	45
П03	Система обнаружения вторжений и аномалий в технологических сегментах предприятий	3787	223	17
П04	Система защиты периметра корпоративной сети	4176	186	22
П11	Система управления доступом и ресурсами	4405	171	26
П17	Система управления инфраструктурой открытых ключей	16	19	1
П12	Система предотвращения утечек информации	150	84	2
П13	Система повышения осведомленности пользователей	16	34	0
П02	Система обнаружения вторжений и аномалий в локальной сети предприятий	3533	179	20
П14	Защищенная корпоративная почтовая система	154	79	2
П07	Система контроля действий привилегированных пользователей	3811	107	36
П16	Система управления конфигурациями сетевого оборудования	321	137	2

Ранжирование проектов по величине снижаемого общего ущерба (прямого и репутационного, ранжирование по коэффициенту)

ОЖИДАЕМЫЕ ЕЖЕГОДНЫЕ ПОТЕРИ (ALE)

Рассмотрим на примере расчет ALE

Обозначение риска	Риск	Ущерб от реализации сценария (ALE), млн. руб.											Total ALE (annual loss expectancy - ожидание ежегодной потери), млн р.	Реализация риска
		Вирусное заражение, в том числе внедрение вирусов-шифровальщиков	Скрытое получение злоумышленником контроля над ИТ-инфраструктурой и большим объемом критичных данных путем реализации целенаправленной атаки	Подмена параметров технологического процесса вследствие действий киберпреступников	Изменение параметров конфигурации технологического оборудования вследствие действий киберпреступников	Нецелевое использование вычислительных и электрических мощностей Компании, в том числе майнинг криптовалют	Нарушение доступности внешних ресурсов Компании вследствие сетевой DoS-атаки	Наложение санкций регуляторами в области ИБ за нарушения в области защиты персональных данных или требований по защите КИИ	Нарушение работоспособности систем из-за ошибок в действиях пользователей, наступившее вследствие недостаточности мер ИБ	Хищение данных путем несанкционированного копирования информации (на съемные носители, внешние почтовые сервисы, в мессенджеры и т.п.) или хищения носителей информации	Нарушение работы компании международными хакерскими группировками (конкурентами и т.д.) с целью нанесения существенного ущерба	Осуществление внутреннего мошенничества с использованием методов обхода контролей путем взлома компьютерных систем		
		S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11		
	Реализация сценария	Да	Да	Да	Да	Да	Да	Да	Да	Да	Да	Да		
R1	Разглашение и утечка информации, составляющей коммерческую тайну		X							X		X		
R2	Несанкционированное изменение информации	X	X	X	X				X		X	X		
R3	Нарушение непрерывности бизнес-процессов и/или приостановка производства	X	X	X	X	X	X		X		X			
R5.1	Привлечение к ответственности из-за нарушения требований законодательства РФ							X						
R4.1	Финансовые и экономические последствия	357	523	384	2323	0	90	2273	119	764	45929	1		
R4.2	Репутационные риски (влияние на капитализацию)	1 359	2 399	1 120	560	1 120	240	1 120	800	560	3 279	560		
R5.2	Уголовная ответственность для Руководства							до 10 лет						
	Максимальный ущерб по сценарию, млн р.	1 717	2 922	1 503	2 883	1 120	329	3 392	919	1 324	49 207	560		
	Средний ущерб по сценарию, млн р.	858	1 461	752	1 441	560	165	1 696	459	662	24 604	280		

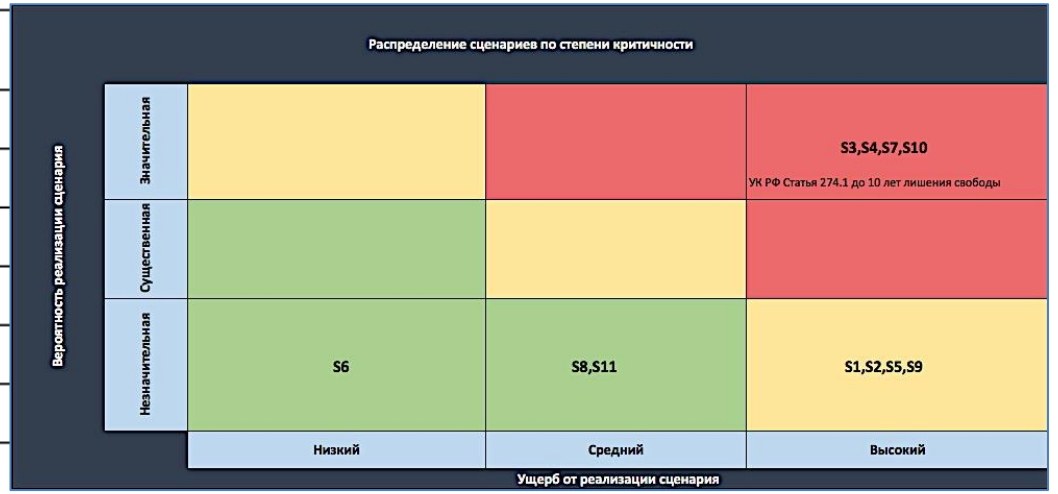


КАЛЬКУЛЯТОР ПРОЕКТОВ. ВЛИЯНИЕ ПРОЕКТОВ НА РИСКИ ИБ

Рассмотрим результаты на выходе

Код	Наименование проекта	Реализация проекта	Максимальная сумма снижения прямого ущерба (млн р.)	Сумма снижения рисков ИБ (млн р.)	Сумма снижения рисков ИБ (млн р.)	Ма
				За 1 год	За 5 лет	
			Учитывать прямые риски?			
			Да			
П01	Единая система сбора и корреляции событий информационной безопасности	Да	3881	353	1764	
П02	Система обнаружения вторжений и аномалий в локальной сети предприятий	Да	3533	321	1606	
П03	Система обнаружения вторжений и аномалий в технологических сегментах предприятий	Да	3787	344	1721	
П04	Система защиты периметра корпоративной сети	Да	4176	380	1898	
П05	Система защиты АРМ и серверов	Да	3817	347	1735	
П06	Обеспечение соответствия требованиям регуляторов и международным стандартам информационной безопасности	Да	4381	398	1991	
П07	Система контроля действий привилегированных пользователей	Да	3811	346	1732	
П08	Система анализа защищенности ИТ ресурсов	Да	3900	355	1773	
П09	Система контроля доступа к локальной сети	Да	4478	407	2035	
П10	Система контроля и анализа событий информационной безопасности	Да	3807	346	1731	
П11	Система управления доступом и ресурсами	Да	4405	400	2002	
П12	Система предотвращения утечек информации	Да	150	14	68	
П13	Система повышения осведомленности пользователей	Да	16	1	7	

R4.2	Репутационные риски (влияние на капитализацию)	1 359	2 399	1
R5.2	Уголовная ответственность для Руководства			
	Максимальный ущерб по сценарию, млн р.	**1 717**	**2 922**	**1**
	Средний ущерб по сценарию, млн р.	**858**	**1 461**	**7**
	Для сценариев S3, S4, S7 и S10 при определении значений рисков ИБ не уч максимальные ущербы от их реализации.			
Оценка влияния на сегменты	Бизнес-сегмент	0	13	
	Технологический сегмент	357	510	3
R1	Бизнес-сегмент		X	
	Технологический сегмент			
R2	Бизнес-сегмент	X	X	
	Технологический сегмент			
R3	Бизнес-сегмент	X	X	
	Технологический сегмент			
R5.1	Бизнес-сегмент			
	Технологический сегмент			



КАЛЬКУЛЯТОР ПРОЕКТОВ. ВЛИЯНИЕ ПРОЕКТОВ НА РЕАЛИЗАЦИЮ МЕР

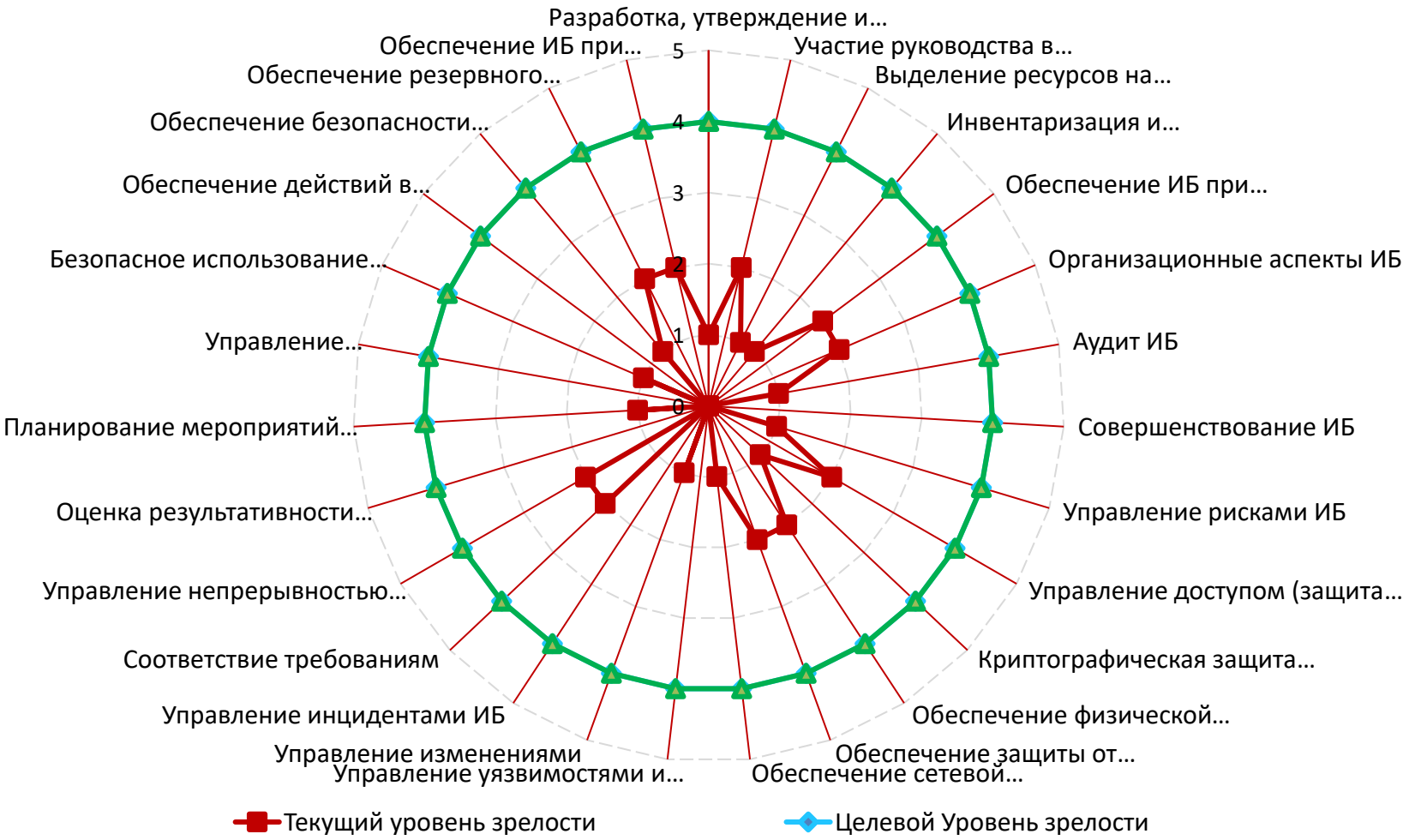
Рассмотрим результаты на выходе

Код	Наименование проекта	Реализация проекта	Оценка вклада систем КСИБ в реал					
			I. Идентификация и аутентификация (ИАФ)	II. Управление доступом (УПД)	III. Ограничение программной среды (ОПС)	IV. Защита машинных носителей информации (ЗНИ)	V. Аудит безопасности (АУД)	VI. А за
П01	Единая система сбора и корреляции событий информационной безопасности	Да					7	
П02	Система обнаружения вторжений и аномалий в локальной сети предприятий	Да		1			4	
П03	Система обнаружения вторжений и аномалий в технологических сегментах предприятий	Да				1	4	
П04	Система защиты периметра корпоративной сети	Да	2	4			4	
П05	Система защиты АРМ и серверов	Да		3		1	4	
П06	Обеспечение соответствия требованиям регуляторов и международным стандартам информационной безопасности	Да	1	4	3	4	10	
П07	Система контроля действий привилегированных пользователей	Да	4				4	
П08	Система анализа защищенности ИТ ресурсов	Да		5			12	
П09	Система контроля доступа к локальной сети	Да	4			1	4	
П10	Система контроля и анализа событий информационной безопасности	Да		3			6	
П11	Система управления доступом и ресурсами	Да	4				4	
П12	Система предотвращения утечек информации	Да				2	4	
П13	Система повышения осведомленности пользователей	Да						
П14	Защищенная корпоративная почтовая система	Да		5			4	
П15	Система защиты сред виртуализации	Да	6				4	
П16	Система управления конфигурациями сетевого оборудования	Да					5	
П17	Система управления инфраструктурой открытых ключей	Да	2				4	
П18	Система защиты внешних ресурсов	Да					4	
П19	Система защиты от таргетированных атак	Да		1			4	

КАЛЬКУЛЯТОР ПРОЕКТОВ. УРОВЕНЬ ЗРЕЛОСТИ

Рассмотрим результаты на выходе

Оценка уровней зрелости процессов ИБ/ областей деятельности в ИБ с учетом проектов КСИБ



Остались вопросы ?

Благодарю за внимание!

Рад продуктивному общению, жду на своих курсах!

ЭКОСИСТЕМА CODEBY