

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ В РЕАЛИЯХ БИЗНЕС-ТРЕБОВАНИЙ РФ

ТЕМА 1

Введение в курс

Спикер: Ануфриев Иван



ЗАНЯТИЕ 1.1

Ландшафт угроз информационной безопасности в индустрии 4.0.

Безопасность как сервис



Условное разделение информации. «Метки» на слайдах *

«Машина-времени-Time-machine» Возвращаемся и освежаем знания с прошлых занятий.	«Назад в будущее» Анонсируем то, что будет сказано на следующих занятиях	Метки по Времени
		

Рабочий «экспертный» инструментарий «Expert tools»	Примеры рабочих документов, лучшие приемы, практики и примеры использования. «Best practice»	Метки по используемым инструментам и практикам
		

Полезные мысли и выводы «Инсайты»	Соответствие требованиям, нормативная база и полезные формы по НПА	В нашем курсе, отдельно выделяется информация, относящаяся к типу «непрерывность бизнеса»	Метки по типу информации
			



ОСНОВНЫЕ РАССМАТРИВАЕМЫЕ ВОПРОСЫ ЗАНЯТИЯ

ВОПРОС 1

Статистика 2022,
последствия от
заказных атак,
кибергруппировки

ВОПРОС 2

Инсайдеры,
саботаж

ВОПРОС 3

Кто подвержен
рisku

ВОПРОС 4

Промышленный
интернет вещей –
увеличение риска
кибератак

ВОПРОС 5

Регулирование,
комплаенс

ВОПРОС 6

Способы работы с
рисками

ВОПРОС 7

Нарушители и
третьи стороны

ВОПРОС 8

Корпоративная
сервис-модель

ВОПРОС 9

Ключевые
вопросы ИБ



Предприятия не справляются со сложными кибератаками

В 4 раза с начала специальной военной операции возросло число кибератак против Российской Федерации

По данным Positive Hack Days

65 млн.данных Россия утекло с начала СВО

В 2022 по данным Сбербанка

\$ 200.000.000

Потери от простоя MAERSK в 2019

\$ 70.000.000

Потери от простоя Norsk Hydro в 2019

56% сетевых энергетических компаний

Потеряли данные или остановили работу в 2019

Обработка большого объема информации для обнаружения

Сложно анализировать события безопасности 24 часа в сутки

Ложные срабатывания при обнаружении составляют 60%

Недостаточная численность и квалификация персонала

Ошибки при обновлении правил обнаружения и блокировки кибератак



Предприятия не справляются со сложными кибератаками

В 4 раза с начала специальной военной операции возросло число кибератак против Российской Федерации

По данным Positive Hack Days

65 млн.данных Россия утекло с начала СВО

В 2022 по данным Сбербанка

\$ 200.000.000

Потери от простоя MAERSK в 2019

\$ 70.000.000

Потери от простоя Norsk Hydro в 2019

56% сетевых энергетических компаний

Потеряли данные или остановили работу в 2019

Обработка большого объема информации для обнаружения

Сложно анализировать события безопасности 24 часа в сутки

Ложные срабатывания при обнаружении составляют 60%

Недостаточная численность и квалификация персонала

Ошибки при обновлении правил обнаружения и блокировки кибератак



Предприятия не справляются со сложными кибератаками

В 4 раза с начала специальной военной операции возросло число кибератак против Российской Федерации

По данным Positive Hack Days

65 млн.данных Россия утекло с начала СВО

В 2022 по данным Сбербанка

\$ 200.000.000

Потери от простоя MAERSK в 2019

\$ 70.000.000

Потери от простоя Norsk Hydro в 2019

56% сетевых энергетических компаний

Потеряли данные или остановили работу в 2019

Обработка большого объема информации для обнаружения

Сложно анализировать события безопасности 24 часа в сутки

Ложные срабатывания при обнаружении составляют 60%

Недостаточная численность и квалификация персонала

Ошибки при обновлении правил обнаружения и блокировки кибератак



Некоторые последствия от таргетированных атак в 2022 году

ТАРГЕТИРОВАННАЯ АТАКА



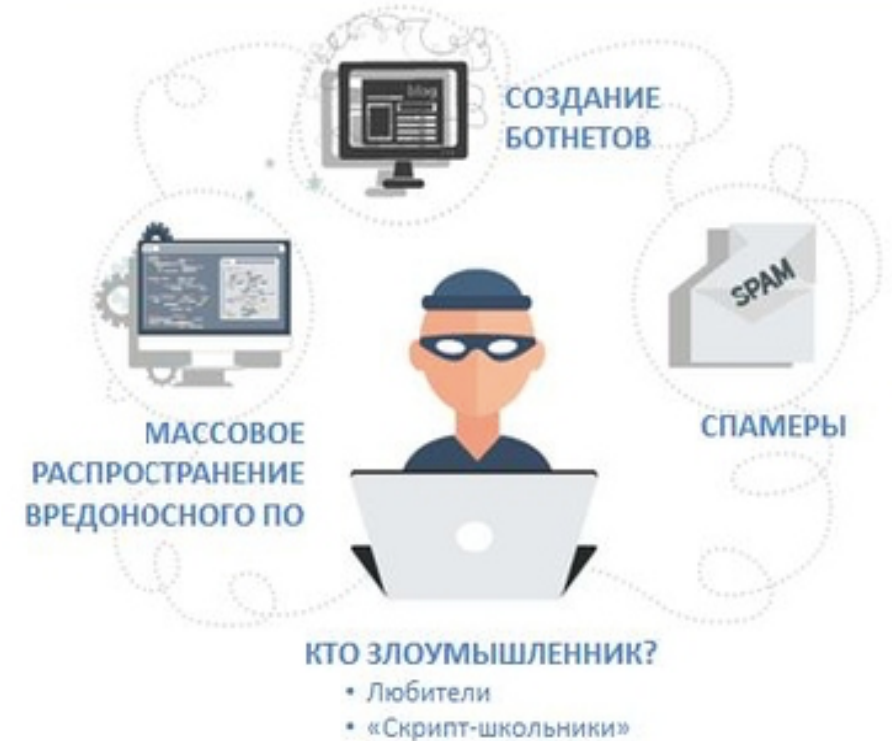
Некоторые последствия от таргетированных атак в 2022 году

ТАРГЕТИРОВАННАЯ АТАКА



VS

НЕТАРГЕТИРОВАННАЯ АТАКА



OldGremlin. MITRE ATT&CK® Mapping.



ТАКТИКА	ТЕХНИКА	ПРОЦЕДУРА
INITIAL ACCESS	Phishing: Spearphishing Link	OldGremlin использовали фишинговые ссылки на архивы, содержащие вредоносные LNK-файлы или исполняемые файлы, представляющие собой самораспаковывающиеся архивы (SFX).
EXECUTION	User Execution: Malicious File Command and Scripting Interpreter: PowerShell Command and Scripting Interpreter: JavaScript/JScript	Пользователю необходимо запустить вредоносный файл, чтобы инициировать исполнение кода. OldGremlin использовали обфусцированные сценарии PowerShell. OldGremlin использовали обфусцированные сценарии JavaScript.
PERSISTENCE	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	OldGremlin использовали раздел реестра Software\Microsoft\Windows\CurrentVersion\Run для закрепления троянов TinyPosh и TinyNode в системе.
DEFENSE EVASION	Signed Binary Proxy Execution: Mshta Signed Binary Proxy Execution: Rundll32 Process Injection: Asynchronous Procedure Call Obfuscated Files or Information	OldGremlin использовали mshta.exe для выполнения обфусцированных сценариев JavaScript. OldGremlin использовали rundll32.exe для открытия документа, предназначенного для отвлечения внимания пользователя. OldGremlin внедряли полезную нагрузку Cobalt Strike в легитимные процессы (например, svchost.exe и rundll32.exe) через очередь асинхронного вызова процедур. OldGremlin обфусцировали использованные в ходе атаки сценарии и команды.
CREDENTIAL ACCESS	Credentials from Password Stores: Credentials from Web Browsers Unsecured Credentials: Credentials In Files	OldGremlin извлекали пароли из веб-браузеров средствами NirSoft WebBrowserPassView. OldGremlin извлекали пароли к учетным записям электронной почты средствами NirSoft Mail PassView.
DISCOVERY	Software Discovery Remote System Discovery	OldGremlin собирали информацию об установленном на скомпрометированном хосте программном обеспечении. OldGremlin собирали информацию о хостах в домене для продвижения по сети и распространения программы-вымогателя TinyCryptor.
LATERAL MOVEMENT	Lateral Tool Transfer Remote Services: Remote Desktop Protocol Remote Services: SMB/Windows Admin Shares	OldGremlin продвигались по сети с использованием полезной нагрузки Cobalt Strike – Beacon. OldGremlin использовали протокол RDP для продвижения по сети. OldGremlin распространяли программу-вымогатель TinyCryptor с помощью модуля PsExec фреймворка Cobalt Strike.
COLLECTION	Screen Capture	OldGremlin делали снимки с экрана скомпрометированного хоста.
COMMAND AND CONTROL	Proxy: Multi-hop Proxy Encrypted Channel: Symmetric Cryptography	OldGremlin использовали Tor для взаимодействия с скомпрометированным хостом. OldGremlin использовали алгоритм RC4 для шифрования передаваемых данных.
IMPACT	Data Encrypted for Impact	OldGremlin осуществляли шифрование данных средствами TinyCryptor с целью последующего получения выкупа.

«Большая охота OldGremlin: операторы шифровальщика атакуют крупные компании и банки России». Сентябрь 2020.



Атака 22 марта

Здравствуйте.

К нам в [REDACTED] поступила достоверная информация введения в ближайшие пару дней новых санкций и полного отключения платежных систем Visa/Mastercard. Все карты выпущенные в нашей стране не будут работать вовсе.

Поэтому всем в срочном порядке необходимо оформить карты системы [REDACTED] и присоединить ее к зарплатным проектам ваших банков.

Воспользуйтесь следующей [инструкцией](#) для банков: [REDACTED]

Заполните [анкету](#) (см вложение), направьте ее обратным письмом, укажите отделение банка, в котором удобно забрать карту.

Не забудьте, что при желании привязать карту к зарплатному проекту, сообщите в свою бухгалтерию реквизиты счета после получения карты.

Прошу Вас в течение 5(пяти) часов с момента получения данного письма подписать и выслать на наш адрес анкету. В целях оперативной работы прошу выслать его по данной электронной почте обратным письмом.

[REDACTED]
старший бухгалтер

[REDACTED]



Атака 22 марта



Office 365

Этот документ создан в онлайн-версии Microsoft Office Word.

Чтобы просмотреть или отредактировать этот документ, нажмите кнопку «**Включить содержимое**» на верхней желтой полосе.



АКТ СВЕРКИ
взаимных расчетов
за период: I квартал 2022 г.
по договору от 21 декабря 2021 г. N 107/20
между ЗАО "Консультант Плюс" (ИНН 7702044361) и ООО "_____" (ИНН 7739125908)

г. Москва 23 марта 2022 г.

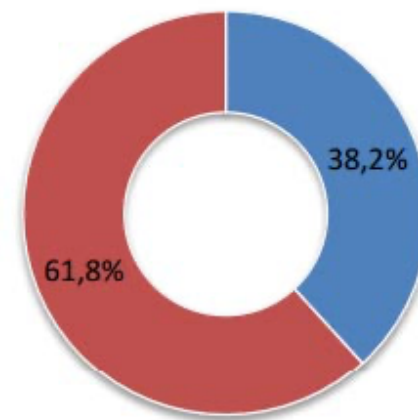
Мы, генеральный директор ЗАО "Консультант Плюс" Дубовицкий Игорь Евгеньевич, с одной стороны и главный бухгалтер ООО "_____" _____а по доверенности от 14.01.2020 N 145 с другой стороны составили настоящий акт сверки расчетов по договору от 21.12.2021 N 107/20 о том, что состояние взаимных расчетов по данным учета следующее:

По данным ООО "_____" (покупателя), руб.				По данным ЗАО "Консультант Плюс" (поставщика), руб.			
Дата	Документ	Дебет	Кредит	Дата	Документ	Дебет	Кредит
Сальдо входящее на 01.01.2022			188 200,0	Сальдо входящее на 01.01.2021		188 200,0	
25.01.2022	Оплата (пл. пор. N 11 от 25.01.2022)	1 188 200,0		25.01.2022	Оплата (пл. пор. N 11 от 25.01.2021)		1 188 200,0
19.02.2022	Предоставление услуг (ТТН N 20080804 от 19.02.2022)		880 000,0	19.02.2022	Предоставление услуг (ТТН N 20080804 от 19.02.2021)	880 000,0	
Обороты за период		1 188 200,0	1 068 200,0	Обороты за период		1 068 200,0	1 188 200,0
Сальдо исходящее		120 000,0		Сальдо исходящее			120 000,0



Инсайдеры, саботаж, промышленный шпионаж ?



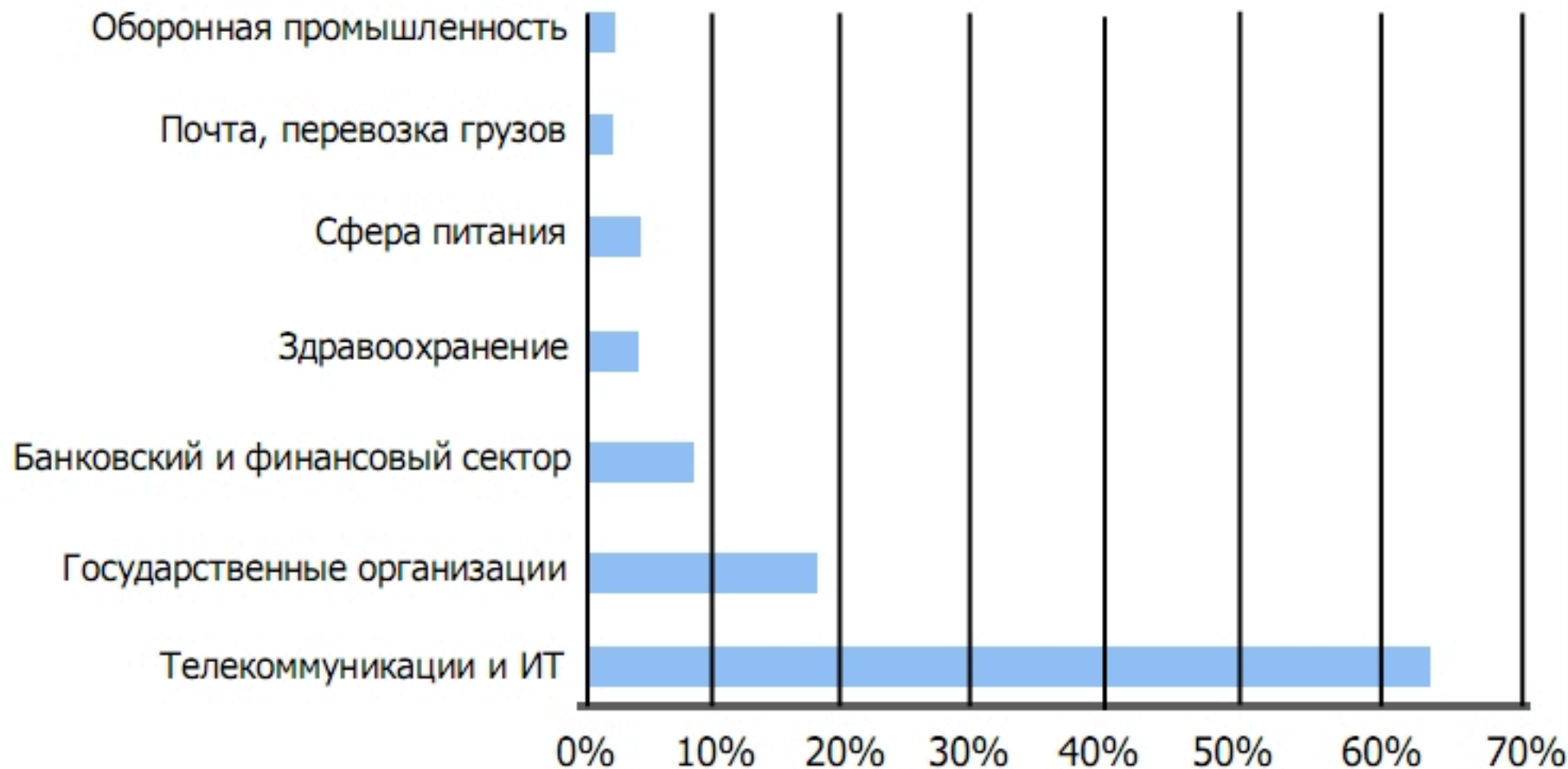


- Внешние атаки
- Внутренний нарушитель

"Стоимость поиска паспортных данных человека по номеру телефона в базе может варьироваться от 2 тыс. до 7 тыс. руб., а отслеживание мобильного — от 80 тыс. руб.", — говорит гендиректор Phishman Алексей Горелкин.



Распределение случаев саботажа по различным секторам бизнеса



Некоторые последствия от таргетированных атак в 2022 году



75% баз и инфраструктуры и 90% резервных копий было поражено

9 мая 2022 взлом RuTube



49 млн.строк с заказами утекло

27 февраля 2022 архив Яндекс.Еда был слит в DarkNet



29 дней длительность DDoS-атаки на финансовый сектор.
В 20 раз выросло количество атак на финансовый сектор

По данным Kaspersky Lab



Адреса, контактные данные, ФИО сотрудников

6 июня 2022 была слита в сеть база данных Ростелекома



208 Гб. Попытка слива внутренних данных в интересах клиентов Банка

21 апреля 2022 действия инсайдера Тинькофф Банка удалось предотвратить благодаря усилиям службы ИБ.

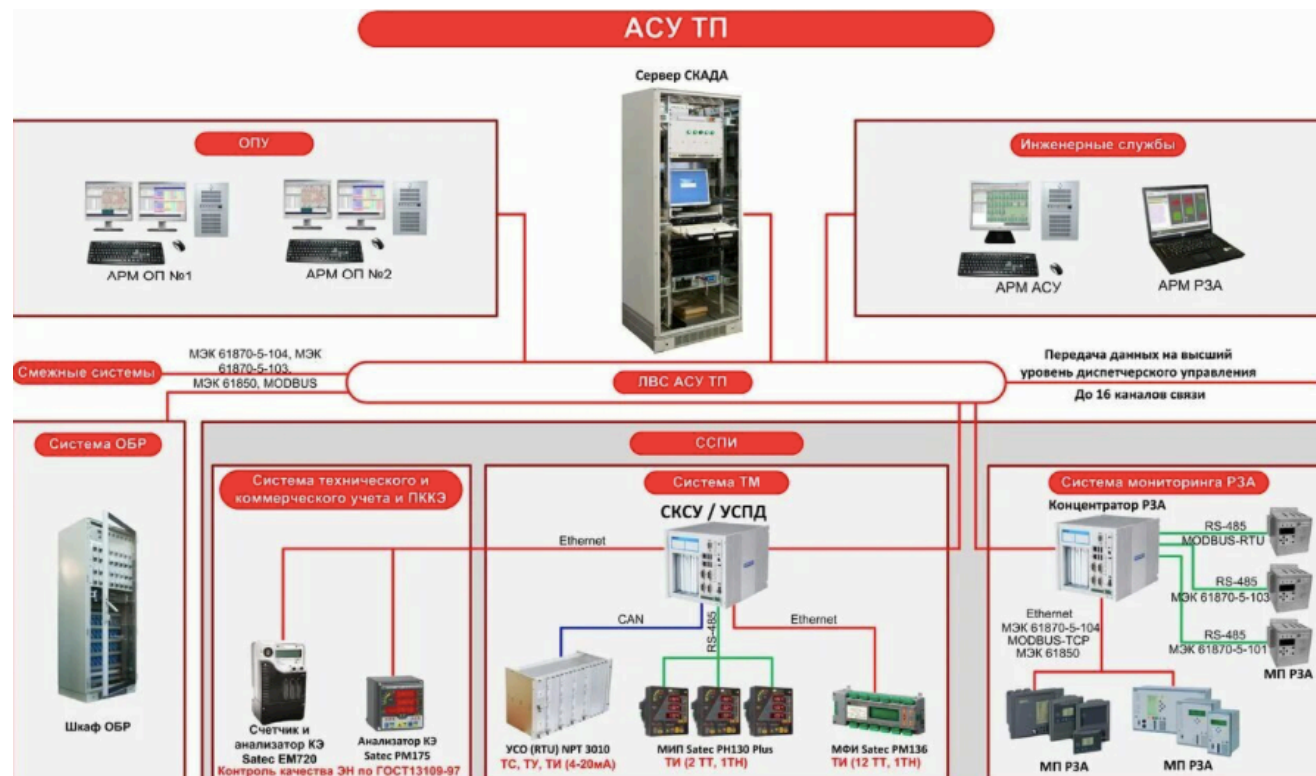
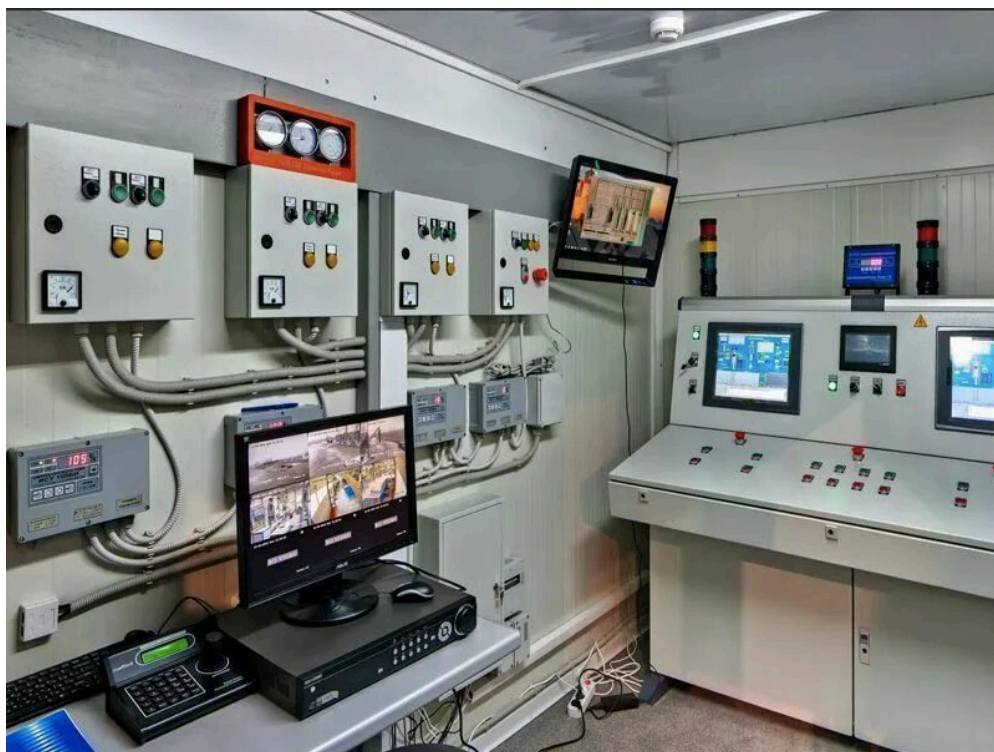
ТАРГЕТИРОВАННАЯ АТАКА



SABOTAGE



Кто подвержен риску кибератак больше всего ?



Реальная готовность к инцидентам оставляет желать лучшего



77%

считают, что компьютеры АСУ ТП могут подвергнуться киберинцидентам в будущем

НО

48%

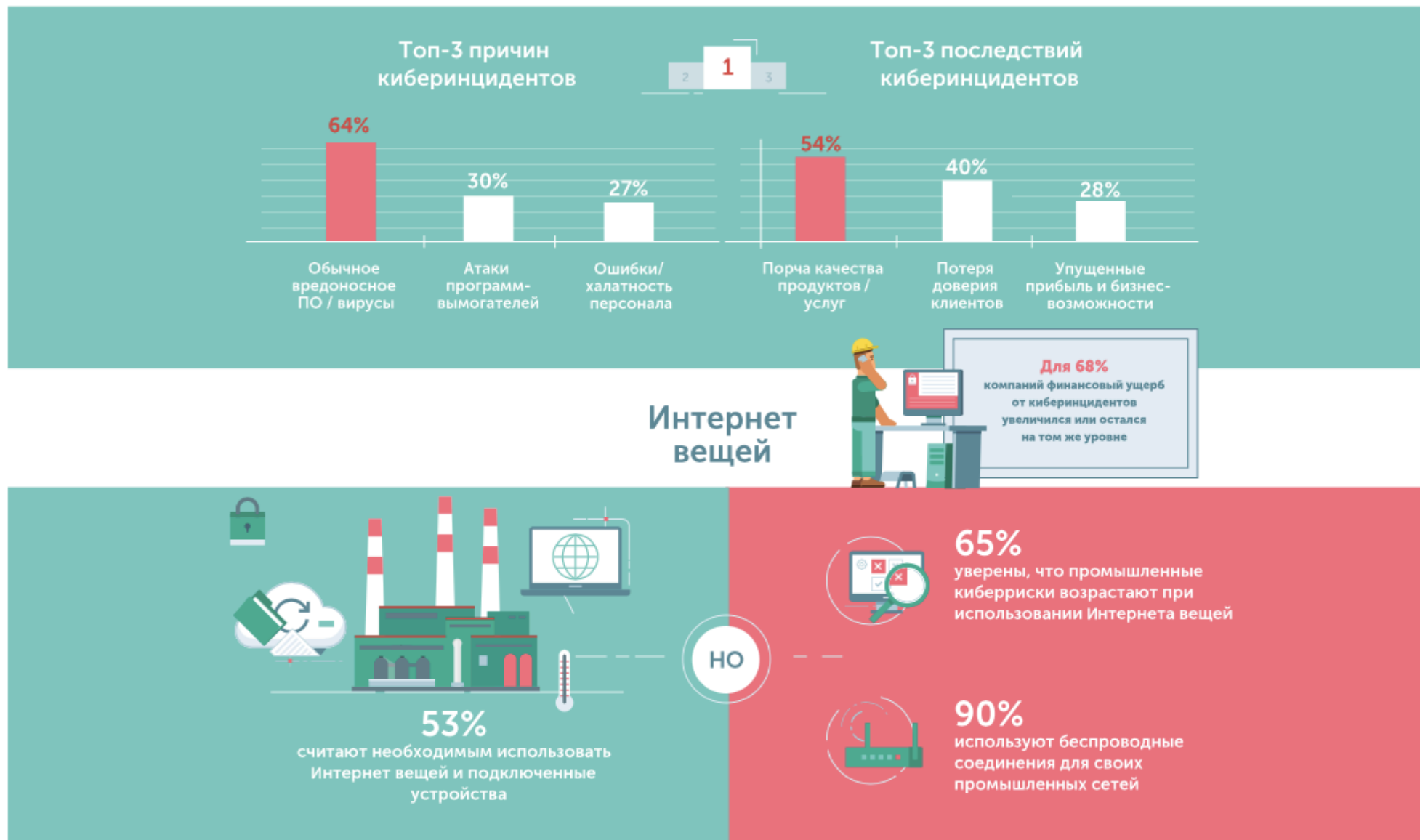
не имеют
программы реагирования
на инциденты,
затрагивающие АСУ ТП

31%

столкнулись
хотя бы с одним
киберинцидентом
в прошлом году



Промышленный интернет вещей (IoT) = увеличение риска кибератак



Области применения интернет вещей (IoT)



Области применения интернет вещей по сферам КИИ (ФЗ-187)



Кибербезопасность IoT – основные тенденции



Современные тенденции развития промышленных и энергетических предприятий, предприятий ТЭК -
IoT Индустрия 4.0 Цифровизация

Большие данные

Машинное обучение

Интернет вещей

Искусственный интеллект

Виртуальная реальность

Роботизация



Кибербезопасность IoT – основные тенденции и связанные с ними риски ИБ



Современные тенденции развития промышленных и энергетических предприятий, предприятий ТЭК -
IoT Индустрия 4.0 Цифровизация

Большие данные

Машинное обучение

Интернет вещей

Искусственный интеллект

Виртуальная реальность

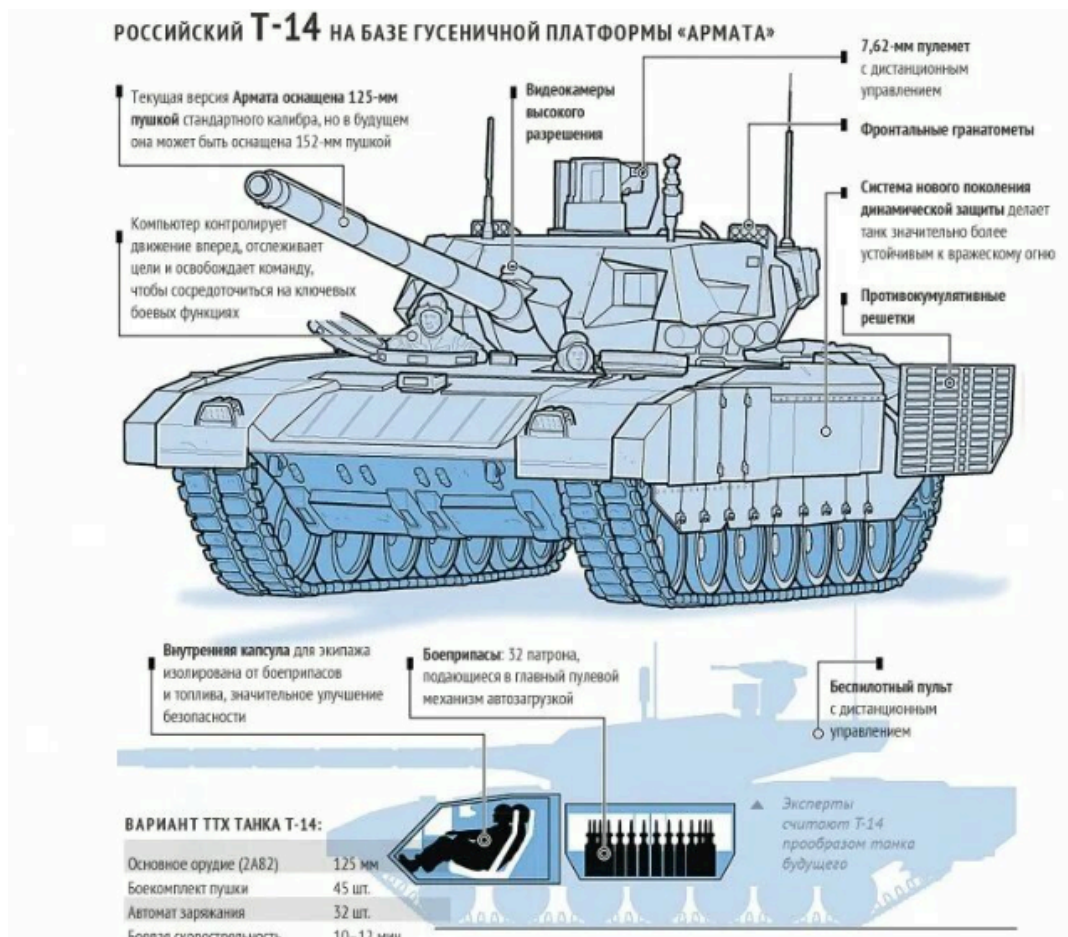
Роботизация

КИБЕРБЕЗОПАСНОСТЬ



Вопрос 1:

построение систем в защищенном исполнении или использование наложенных средств защиты ?



VS



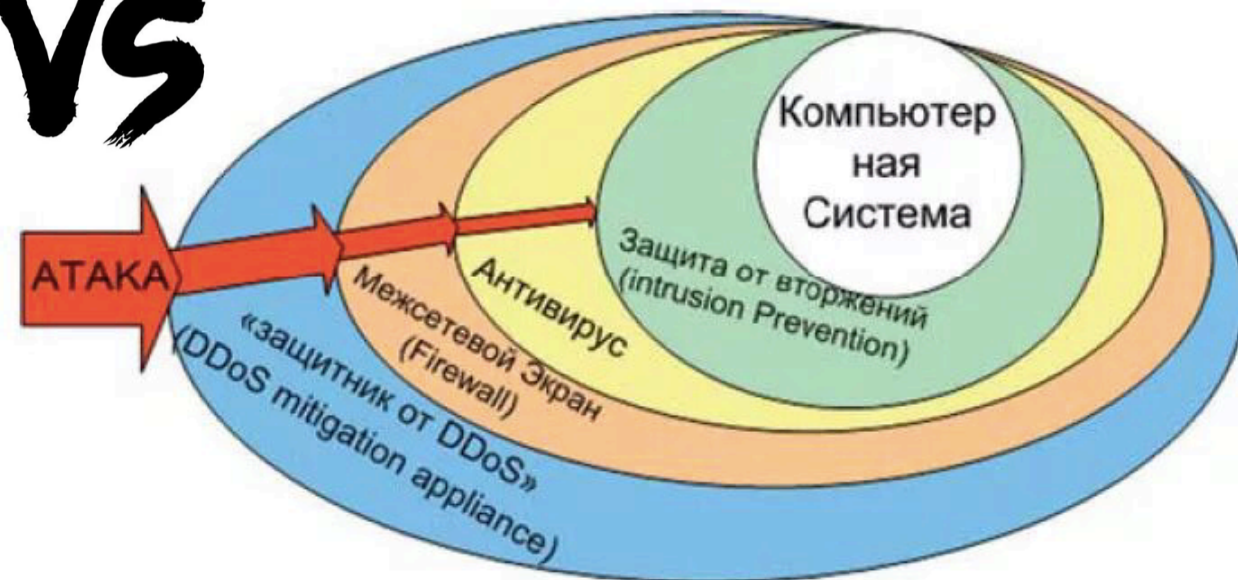
Вопрос 2: Как регулировать ?



Как регулировать:
отталкиваемся от требований или от бизнес задач ?

COMPLIANCE

VS



Комплаенс - это



Часть системы управления, организующая контроль управления рисками, возникающими из несоблюдения требований НПА и внутренних регламентов

КОМПЛАЕНС ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ - это



Необходимость действий компании по приведению в соответствие с нормативными требованиями по обеспечению конфиденциальности целостности и доступности.



Комплаенс - это



Часть системы управления, организующая контроль управления рисками, возникающими из несоблюдения требований НПА и внутренних регламентов

КОМПЛАЕНС ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ - это



Необходимость действий компании по приведению в соответствие с нормативными требованиями по обеспечению конфиденциальности целостности и доступности.

Заявление о риск-аппетите



Определение риск-аппетита



Цели управления рисками в организации



Границы риск-аппетита



Оценка аппетита по категориям

Риск-аппетит

максимальный уровень риска, который организация готова принять в своем стремлении к достижению целевых показателей, до того момента как понадобится принимать меры по снижению риска

Комплаенс



1

Нормативный

2

Корпоративный



Заявление о риск-аппетите

-  Определение риск-аппетита
-  Цели управления рисками в организации
-  Границы риск-аппетита
-  Оценка аппетита по категориям

Ущерб	Франшиза	Сумма выплаты
БЕЗУСЛОВНАЯ ФРАНШИЗА		
100 000 Р	10 000 Р	90 000 Р
10 000 Р	10 000 Р	0 Р
5 000 Р	10 000 Р	0 Р
100 000 Р	15% от ущерба	85 000 Р
УСЛОВНАЯ ФРАНШИЗА		
100 000 Р	10 000 Р	100 000 Р
5 000 Р	5 000 Р	5 000 Р
4 999 Р	5 000 Р	0 Р



Комплаенс - это



Часть системы управления, организующая контроль управления рисками, возникающими из несоблюдения требований НПА и внутренних регламентов

КОМПЛАЕНС ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ - это



Необходимость действий компании по приведению в соответствие с нормативными требованиями по обеспечению конфиденциальности целостности и доступности.

Заявление о риск-аппетите



Определение риск-аппетита



Цели управления рисками в организации



Границы риск-аппетита



Оценка аппетита по категориям

Риск-аппетит

максимальный уровень риска, который организация готова принять в своем стремлении к достижению целевых показателей, до того момента как понадобится принимать меры по снижению риска

Комплаенс



1

Нормативный

2

Корпоративный



Кибербезопасность IoT – основные тенденции и связанные с ними риски ИБ



Современные тенденции развития промышленных и энергетических предприятий, предприятий ТЭК -
IoT Индустрия 4.0 Цифровизация



Большие данные

Машинное обучение

Интернет вещей

Искусственный интеллект

Виртуальная реальность

Роботизация

КИБЕРБЕЗОПАСНОСТЬ

Проекты цифровой трансформации увеличивают степень проникновения ИТ в технологические процессы и влекут к за собой **серьёзные риски ИБ**:



Кибербезопасность IoT – основные тенденции и связанные с ними риски ИБ



Современные тенденции развития промышленных и энергетических предприятий, предприятий ТЭК -
IoT Индустрия 4.0 Цифровизация



Проекты цифровой трансформации увеличивают степень проникновения ИТ в технологические процессы и влекут к за собой **серьёзные риски ИБ**:

- риски нарушения непрерывности и/или приостановки производства, переработки, транспортировки, добычи и хранения продукции
- риски нарушения непрерывности бизнес-процессов



Кибербезопасность IoT – основные тенденции и связанные с ними риски ИБ



Современные тенденции развития промышленных и энергетических предприятий, предприятий ТЭК -
IoT Индустрия 4.0 Цифровизация



Проекты цифровой трансформации увеличивают степень проникновения ИТ в технологические процессы и влекут к за собой **серьёзные риски ИБ**:

- риски нарушения непрерывности и/или приостановки производства, переработки, транспортировки, добычи и хранения продукции
- риски нарушения непрерывности бизнес-процессов
- риски нарушения требований законодательства (в том числе привлечение к уголовной и иным видам ответственности)



Кибербезопасность IoT – основные тенденции и связанные с ними риски ИБ



Современные тенденции развития промышленных и энергетических предприятий, предприятий ТЭК -
IoT Индустрия 4.0 Цифровизация



Проекты цифровой трансформации увеличивают степень проникновения ИТ в технологические процессы и влекут к за собой **серьёзные риски ИБ**:

- риски нарушения непрерывности и/или приостановки производства, переработки, транспортировки, добычи и хранения продукции
- риски нарушения непрерывности бизнес-процессов
- риски нарушения требований законодательства (в том числе привлечение к уголовной и иным видам ответственности)
- риски утечки конфиденциальной информации, репутационные риски



основные тенденции и связанные с ними риски ИБ



Современные тенденции развития промышленных и энергетических предприятий, предприятий ТЭК -
IoT Индустрия 4.0 Цифровизация



Большие данные

Машинное обучение

Интернет вещей

Искусственный интеллект

Виртуальная реальность

Роботизация

КИБЕРБЕЗОПАСНОСТЬ

Проекты цифровой трансформации увеличивают степень проникновения ИТ в технологические процессы и влекут к за собой **серьёзные риски ИБ**:

- риски нарушения непрерывности и/или приостановки производства, переработки, транспортировки, добычи и хранения продукции
- риски нарушения непрерывности бизнес-процессов
- риски нарушения требований законодательства (в том числе привлечение к уголовной и иным видам ответственности)
- риски утечки конфиденциальной информации, репутационные риски

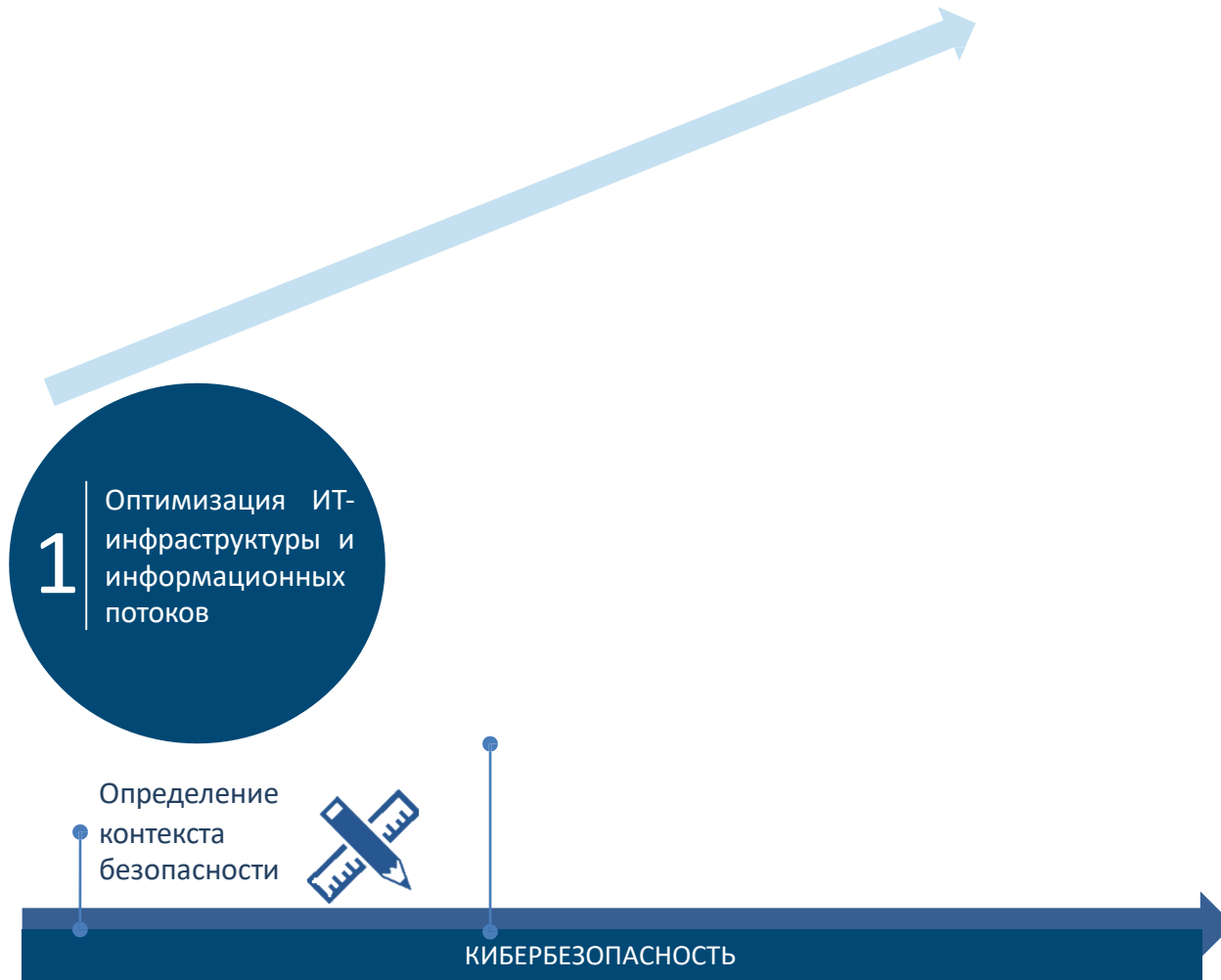


67% российских компаний инвестируют в безопасность в рамках проектов цифровизации*.

- Применение принципа Security By Design
- Затраты на ИБ в среднем составляют до 10% от стоимости проекта в зависимости от его сложности

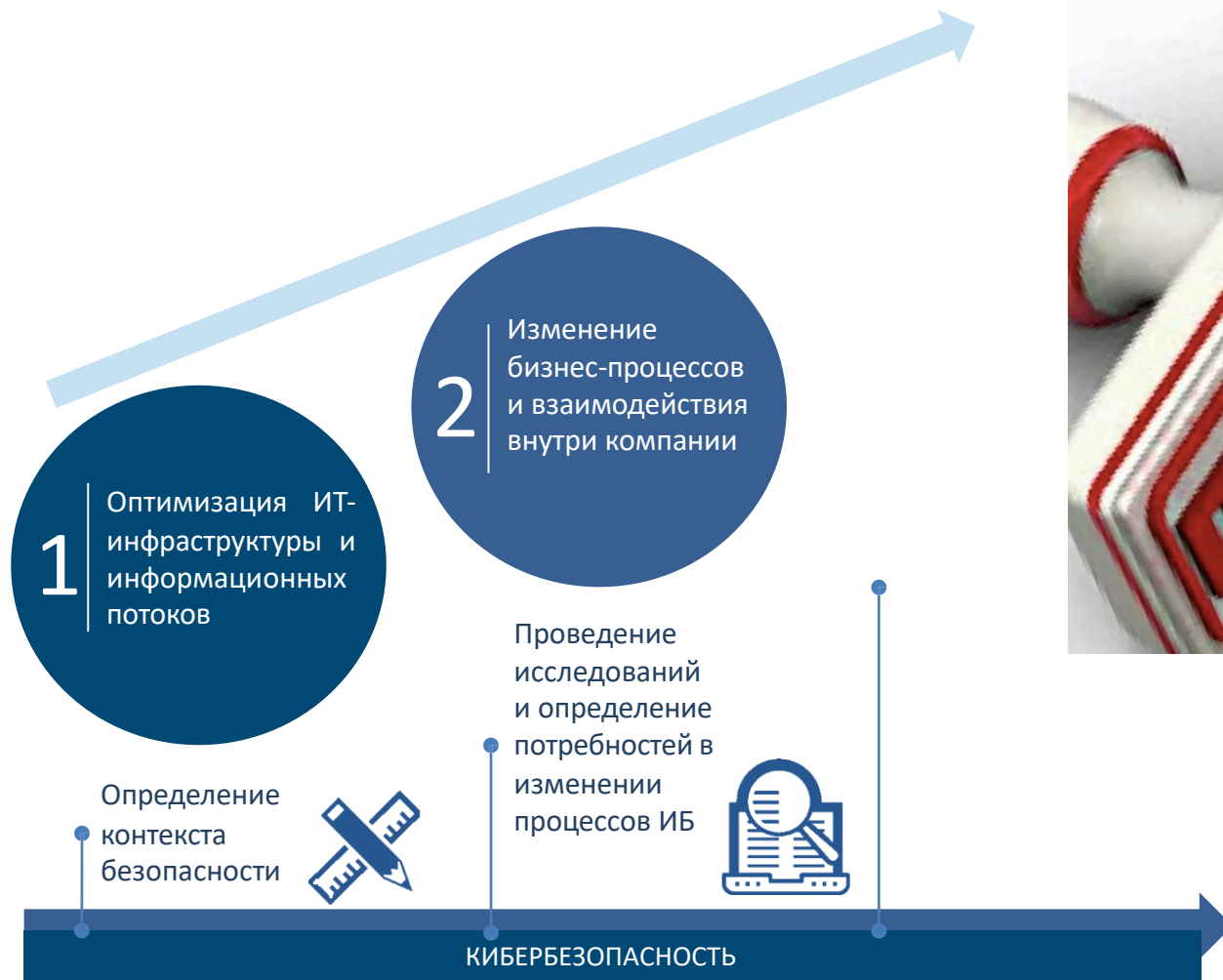


Цифровая трансформация и кибербезопасность



Цифровая трансформация и кибербезопасность

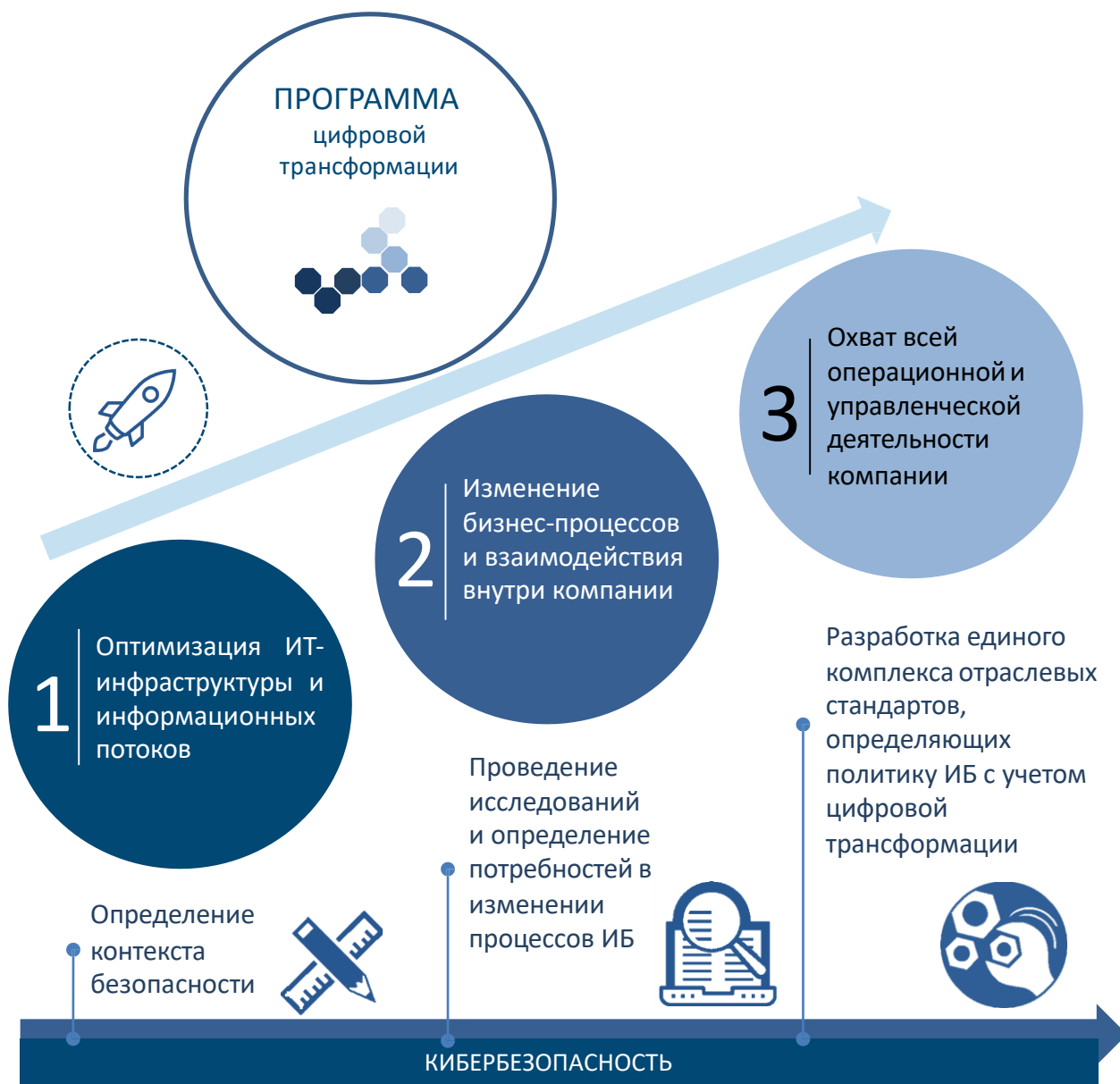
Организационные меры = №1



Цифровая трансформация и кибербезопасность



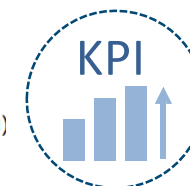
Цифровая трансформация и кибербезопасность



Куда смотреть?

Метрики трафика юзеров

- ✓ всплески и плато RPS
- ✓ кол-во одновременных сессий
- ✓ IP distribution (матчинг с прокси-листами)
- ✓ странные UserAgent
- ✓ паттерн и скорость переходов по URL



Метрики бизнеса

- ✓ посещаемость
- ✓ наполнение корзины
- ✓ конверсия и time to buy
- ✓ время сессии
- ✓ паттерн переходов по URL



Цифровая трансформация и кибербезопасность

(BEST PRACTICE)



Оценка рисков нарушения ИБ информационного пространства компании



Определение общих и частных требований по ИБ ИУС, АСУ ТП



Классификация отраслевых ИУС, АСУ ТП и ЦОД по требованиям ИБ



Унификация и стандартизация подходов к обеспечению ИБ



Кибербезопасность в индустрии 4.0 – защита экосистемы компании



ВЧЕРА



Служба АСУТП

СЕГОДНЯ



Служба АСУТП

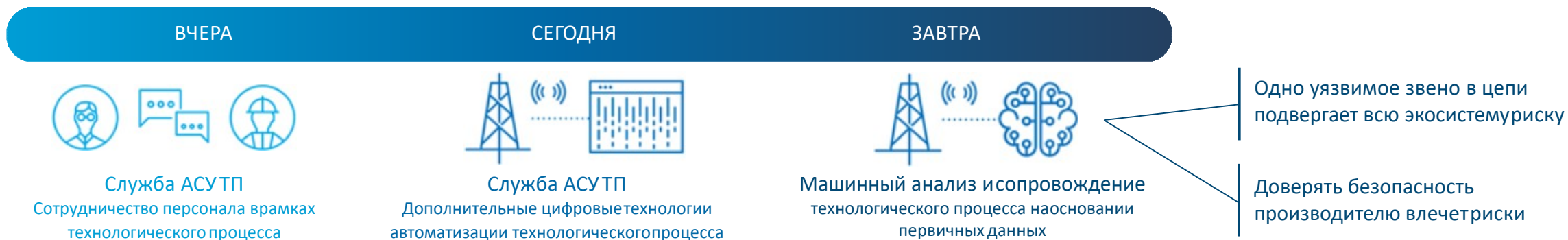
ЗАВТРА



Машинный анализ и сопровождение



Кибербезопасность в индустрии 4.0 – защита экосистемы компании



Централизация → Новые типы устройств и технологии → Новые риски ИБ



Необходимость в методологическом обеспечении и стандартизации ИБ в компании



Кибербезопасность в индустрии 4.0 – защита экосистемы компании



Разработка требований не к отдельным устройствам, а к экосистеме компании в целом и/или отдельным её составляющим исходя из взаимосвязей устройств, потоков данных, процессов и людей



Разработка методологического обеспечения и стандартов ИБ к отраслевым продуктам и услугам



Кибербезопасность в индустрии 4.0 – защита экосистемы компании



ВЧЕРА



Служба АСУ ТП

Сотрудничество персонала в рамках технологического процесса

СЕГОДНЯ



Служба АСУ ТП

Дополнительные цифровые технологии автоматизации технологического процесса

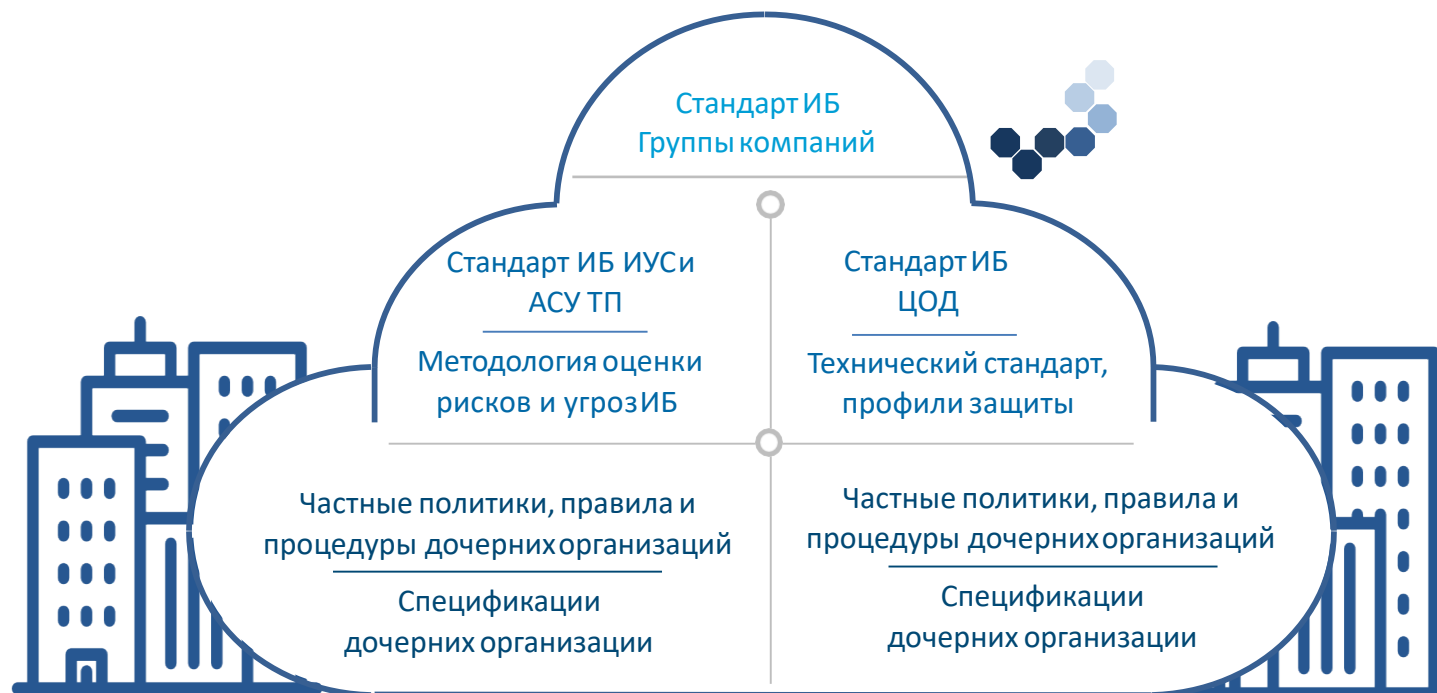
ЗАВТРА



Машинный анализ и сопровождение технологического процесса на основании первичных данных

Одно уязвимое звено в цепи подвергает всю экосистему риску

Доверять безопасность производителю влечет риски



Кибербезопасность в индустрии 4.0. – стандартизация процессов и защита экосистемы

(BEST PRACTICE)



ВЧЕРА

СЕГОДНЯ

ЗАВТРА



Служба АСУ ТП

Сотрудничество персонала в рамках технологического процесса



Служба АСУ ТП

Дополнительные цифровые технологии автоматизации технологического процесса



Машинный анализ и сопровождение технологического процесса на основании первичных данных

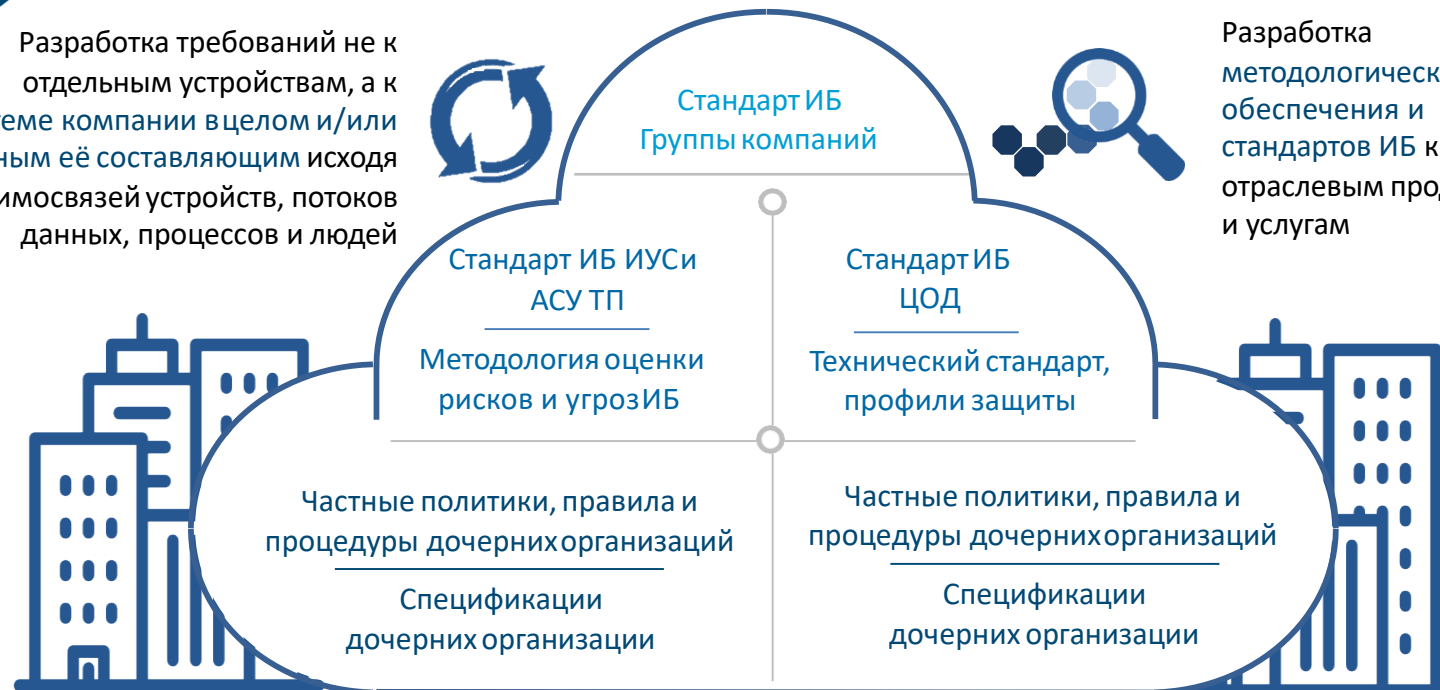
Одно уязвимое звено в цепи подвергает всю экосистему риску

Доверять безопасность производителю влечет риски

— Централизация — Новые типы устройств и технологии — Новые риски ИБ —>

Разработки в области методологического обеспечения и стандартизации ИБ в компании

Разработка требований не к отдельным устройствам, а к экосистеме компании в целом и/или отдельным её составляющим исходя из взаимосвязей устройств, потоков данных, процессов и людей



Разработка методологического обеспечения и стандартов ИБ к отраслевым продуктам и услугам

Базирование на:



- принятых в компании стандартах ИТ и ИБ
- внешних требованиях законодательства
- зарубежных Industrial IoT Security Standards & Frameworks



Что такое риски информационной безопасности ?

РИСК - это

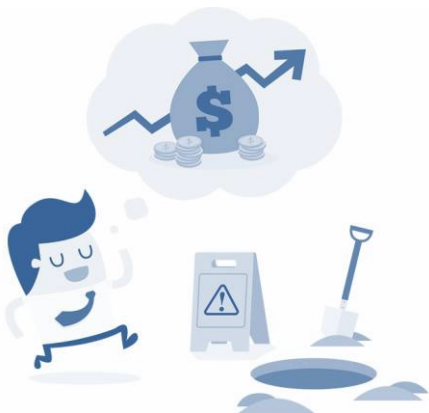


вероятность возникновения убытков или недополучения доходов Компанией по сравнению с прогнозируемым вариантом

РИСК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ - это



возможность того, что угроза ИБ сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб Компании



Риск-ориентированная методика принятия решений по ИБ позволяет предприятию снижать потери от инцидентов.



Это позволит обосновать уже запланированные проекты ИБ и эффективно использовать имеющийся бюджет



Что такое риски информационной безопасности ?

РИСК - это

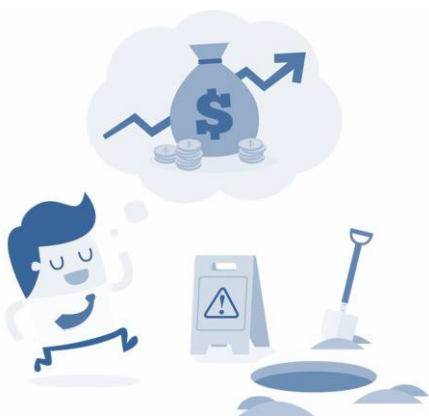


вероятность возникновения убытков или недополучения доходов Компанией по сравнению с прогнозируемым вариантом

РИСК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ - это



возможность того, что угроза ИБ сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб Компании



Риск-ориентированная методика принятия решений по ИБ позволяет предприятию снижать потери от инцидентов.



Это позволит обосновать уже запланированные проекты ИБ и эффективно использовать имеющийся бюджет



Что такое риски информационной безопасности ?

РИСК - это



вероятность возникновения убытков или недополучения доходов Компанией по сравнению с прогнозируемым вариантом

РИСК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ - это



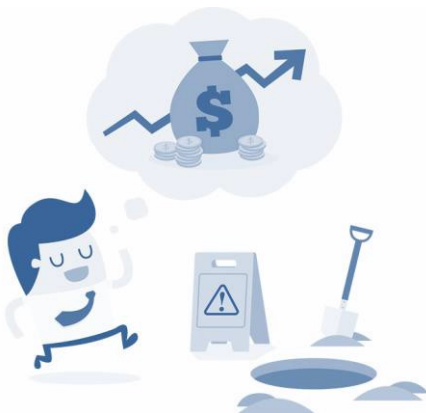
возможность того, что угроза ИБ сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб Компании

Зачем управлять рисками ИБ?

АНАЛИЗ И ОЦЕНКА
РИСКОВ ПОМОГАЕТ
ОТВЕТИТЬ НА
ВОПРОСЫ

1

ФОРМАЛЬНЫЙ
ПОДХОД



Риск-ориентированная методика принятия решений по ИБ позволяет предприятию снижать потери от инцидентов.



Это позволит обосновать уже запланированные проекты ИБ и эффективно использовать имеющийся бюджет



Что такое риски информационной безопасности ?

РИСК - это



вероятность возникновения убытков или недополучения доходов Компанией по сравнению с прогнозируемым вариантом

РИСК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ - это



возможность того, что угроза ИБ сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб Компании

Зачем управлять рисками ИБ?

АНАЛИЗ И ОЦЕНКА
РИСКОВ ПОМОГАЕТ
ОТВЕТИТЬ НА
ВОПРОСЫ



1

ФОРМАЛЬНЫЙ
ПОДХОД

2

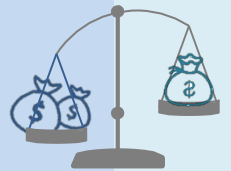
ВЫПОЛНЕНИЕ
ОЦЕНКИ
РИСКОВ ИБ в
соответствии с
реалиями



Риски ИБ

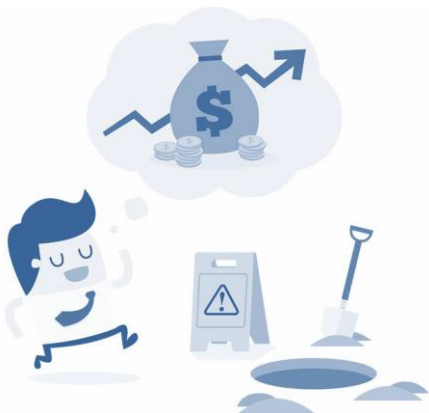


Затраты на
систему ИБ



Это позволит обосновать уже
запланированные проекты ИБ и
эффективно использовать
имеющийся бюджет

Риск-ориентированная
методика принятия
решений по ИБ
позволяет предприятию
снижать потери от
инцидентов.



Что такое риски информационной безопасности ?

РИСК - это



вероятность возникновения убытков или недополучения доходов Компанией по сравнению с прогнозируемым вариантом

РИСК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ - это



возможность того, что угроза ИБ сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб Компании

Ключевые вопросы ИБ



Что защищать?

**АНАЛИЗ И ОЦЕНКА
РИСКОВ ПОМОГАЕТ
ОТВЕТИТЬ НА
ВОПРОСЫ**

Зачем управлять рисками ИБ?



1

ФОРМАЛЬНЫЙ
ПОДХОД

2

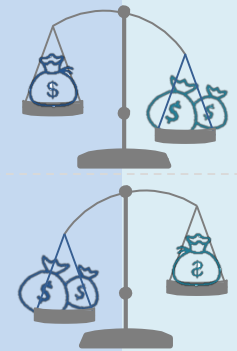
ВЫПОЛНЕНИЕ
ОЦЕНКИ
РИСКОВ ИБ в
соответствии с
реалиями



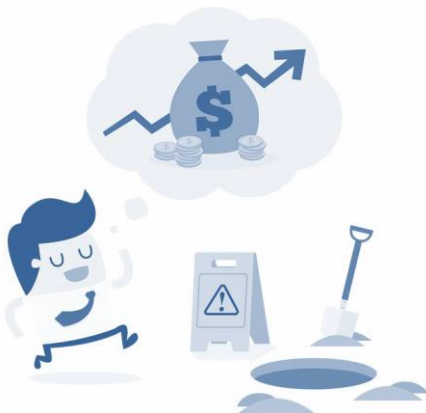
Риски ИБ



Затраты на
систему ИБ



**Это позволит обосновать уже
запланированные проекты ИБ и
эффективно использовать
имеющийся бюджет**



Риск-ориентированная методика принятия решений по ИБ позволяет предприятию снижать потери от инцидентов.



Что такое риски информационной безопасности ?

РИСК - это



вероятность возникновения убытков или недополучения доходов Компанией по сравнению с прогнозируемым вариантом

РИСК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ - это



возможность того, что угроза ИБ сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб Компании

Ключевые вопросы ИБ



Что защищать?



Почему защищать?

Зачем управлять рисками ИБ?



1

ФОРМАЛЬНЫЙ ПОДХОД

2

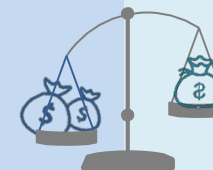
ВЫПОЛНЕНИЕ ОЦЕНКИ РИСКОВ ИБ в соответствии с реалиями



Риски ИБ



Затраты на систему ИБ

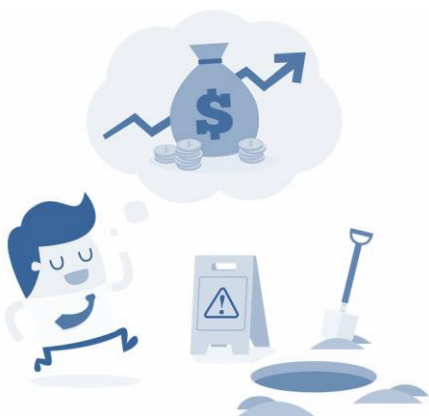


**АНАЛИЗ И ОЦЕНКА
РИСКОВ ПОМОГАЕТ
ОТВЕТИТЬ НА
ВОПРОСЫ**

Риск-ориентированная методика принятия решений по ИБ позволяет предприятию снижать потери от инцидентов.



Это позволит обосновать уже запланированные проекты ИБ и эффективно использовать имеющийся бюджет



Что такое риски информационной безопасности ?

РИСК - это



вероятность возникновения убытков или недополучения доходов Компанией по сравнению с прогнозируемым вариантом

РИСК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ - это



возможность того, что угроза ИБ сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб Компании

Ключевые вопросы ИБ



Что защищать?



Почему защищать?



От чего защищать?

Зачем управлять рисками ИБ?

**АНАЛИЗ И ОЦЕНКА
РИСКОВ ПОМОГАЕТ
ОТВЕТИТЬ НА
ВОПРОСЫ**



1

ФОРМАЛЬНЫЙ
ПОДХОД

2

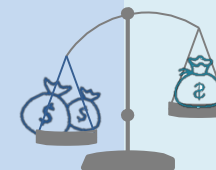
ВЫПОЛНЕНИЕ
ОЦЕНКИ
РИСКОВ ИБ в
соответствии с
реалиями



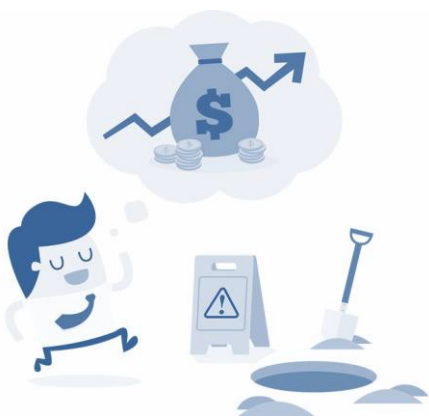
Риски ИБ



Затраты на
систему ИБ



**Это позволит обосновать уже
запланированные проекты ИБ и
эффективно использовать
имеющийся бюджет**



Риск-ориентированная методика принятия решений по ИБ позволяет предприятию снижать потери от инцидентов.



Что такое риски информационной безопасности ? (INSIGHTS) (BEST PRACTICE)



РИСК - это



вероятность возникновения убытков или недополучения доходов Компанией по сравнению с прогнозируемым вариантом

РИСК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ - это



возможность того, что угроза ИБ сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб Компании

Ключевые вопросы ИБ



Что защищать?



Почему защищать?



От чего защищать?



Как защищать?

Зачем управлять рисками ИБ?

**АНАЛИЗ И ОЦЕНКА
РИСКОВ ПОМОГАЕТ
ОТВЕТИТЬ НА
ВОПРОСЫ**



1

ФОРМАЛЬНЫЙ
ПОДХОД

2

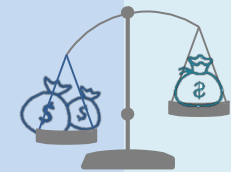
ВЫПОЛНЕНИЕ
ОЦЕНКИ
РИСКОВ ИБ в
соответствии с
реалиями



Риски ИБ

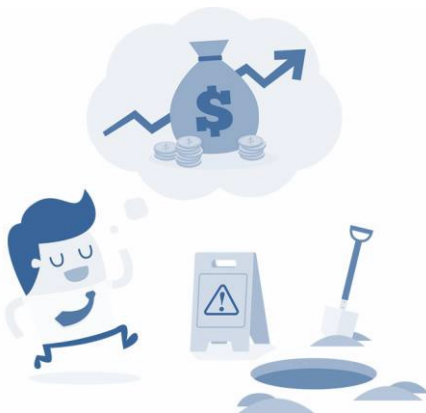


Затраты на
систему ИБ

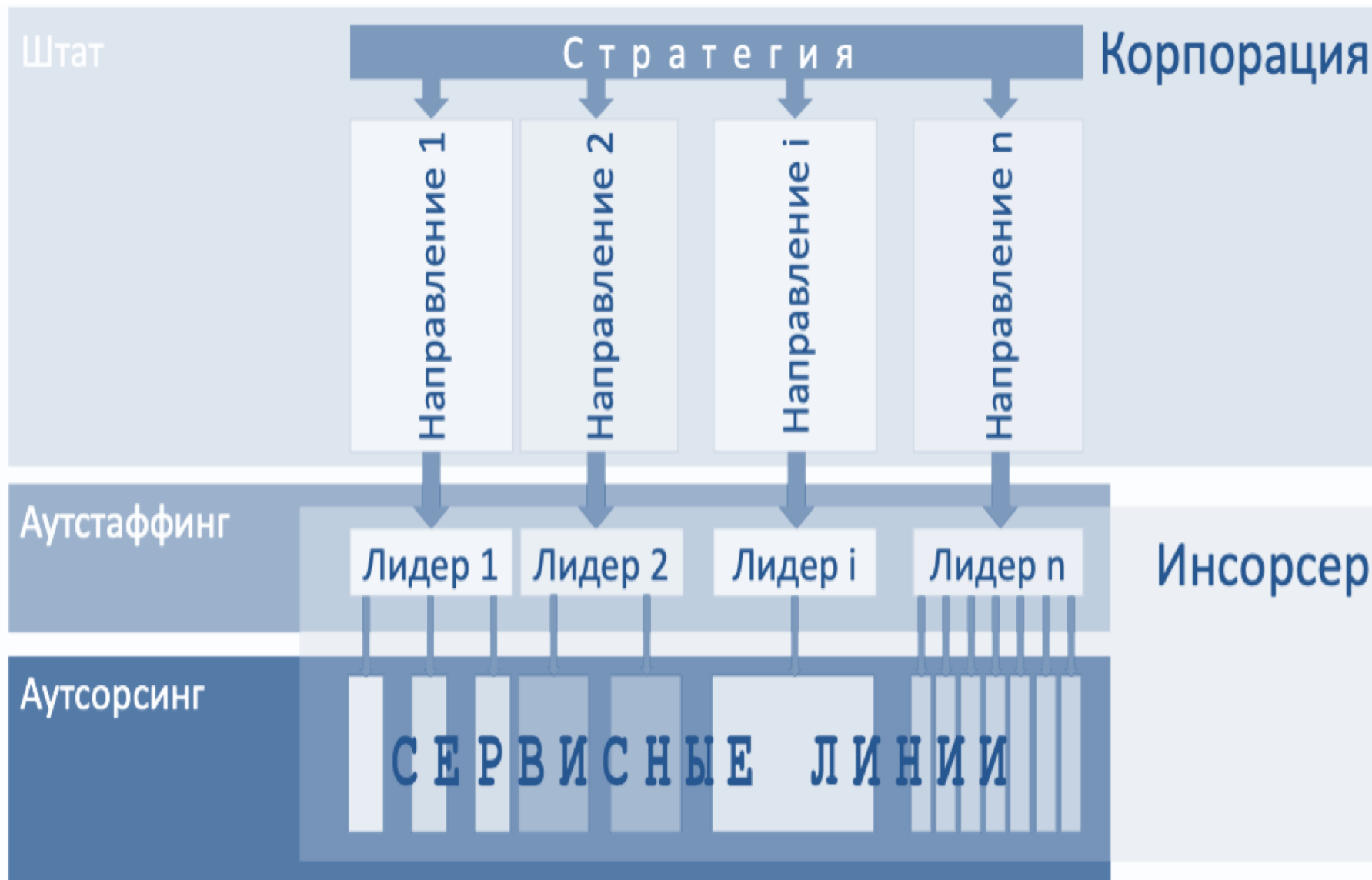


**Это позволит обосновать уже
запланированные проекты ИБ и
эффективно использовать
имеющийся бюджет**

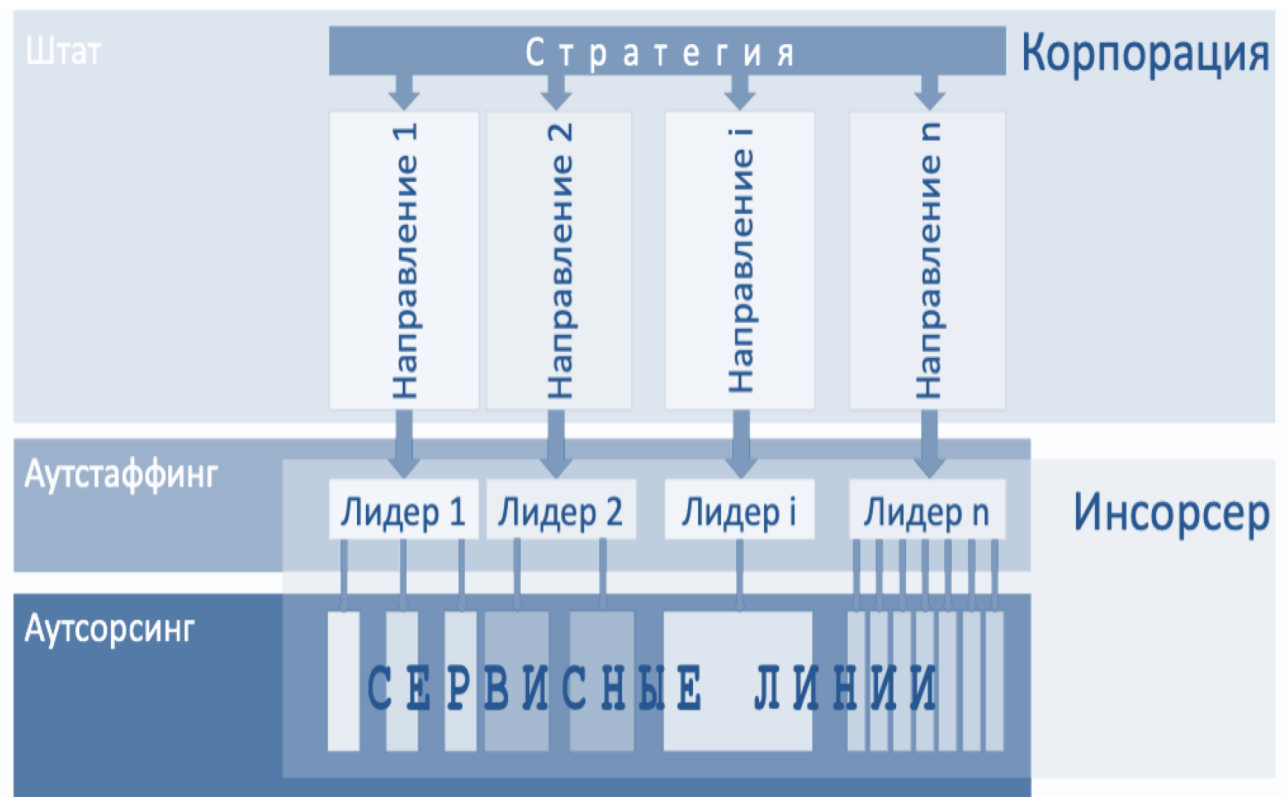
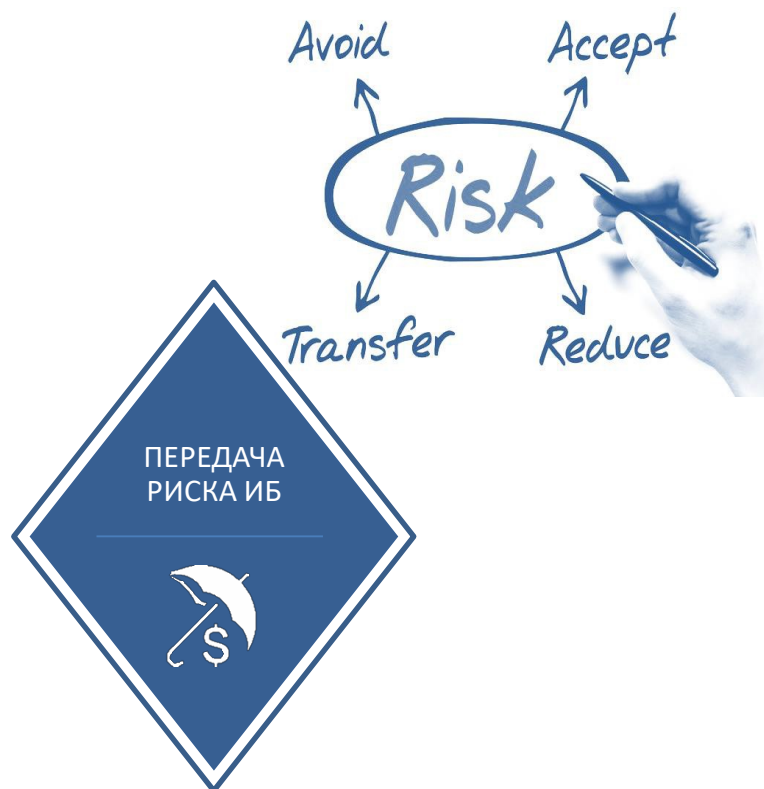
Риск-ориентированная методика принятия решений по ИБ позволяет предприятию снижать потери от инцидентов.



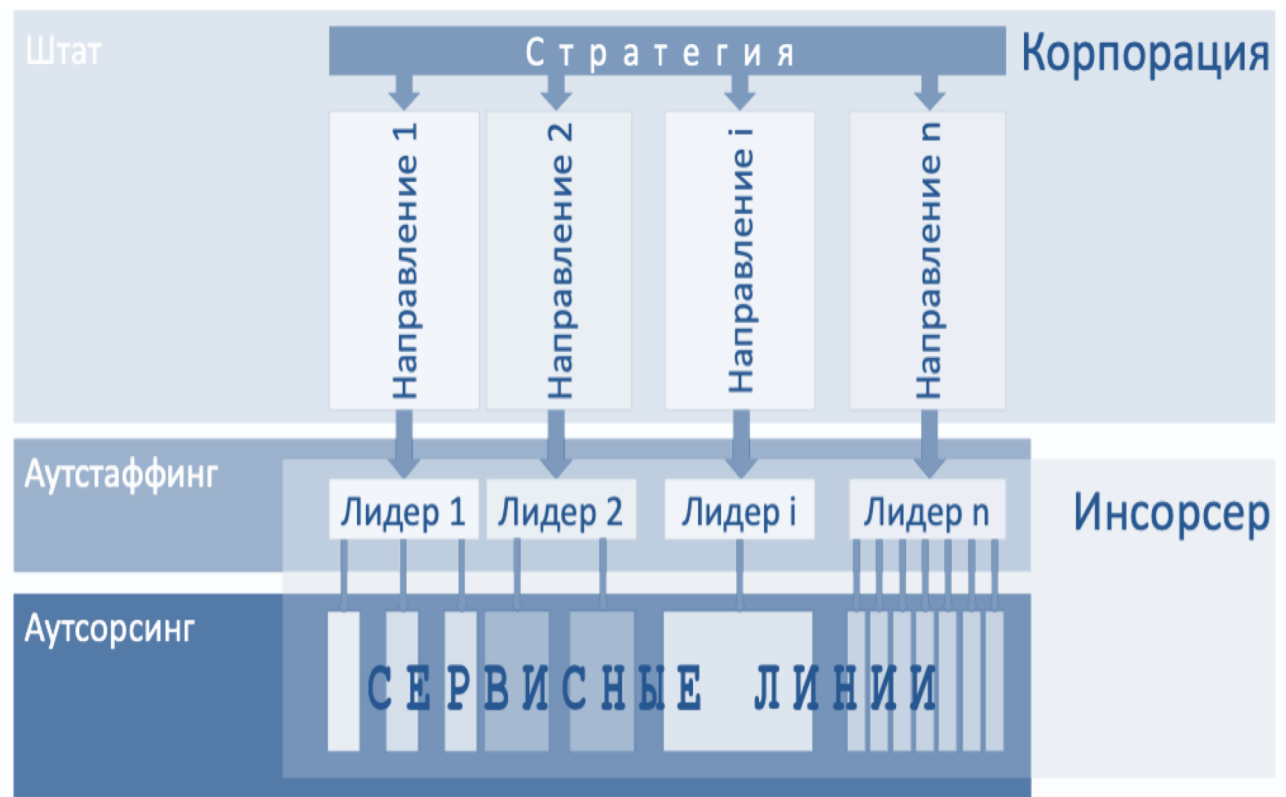
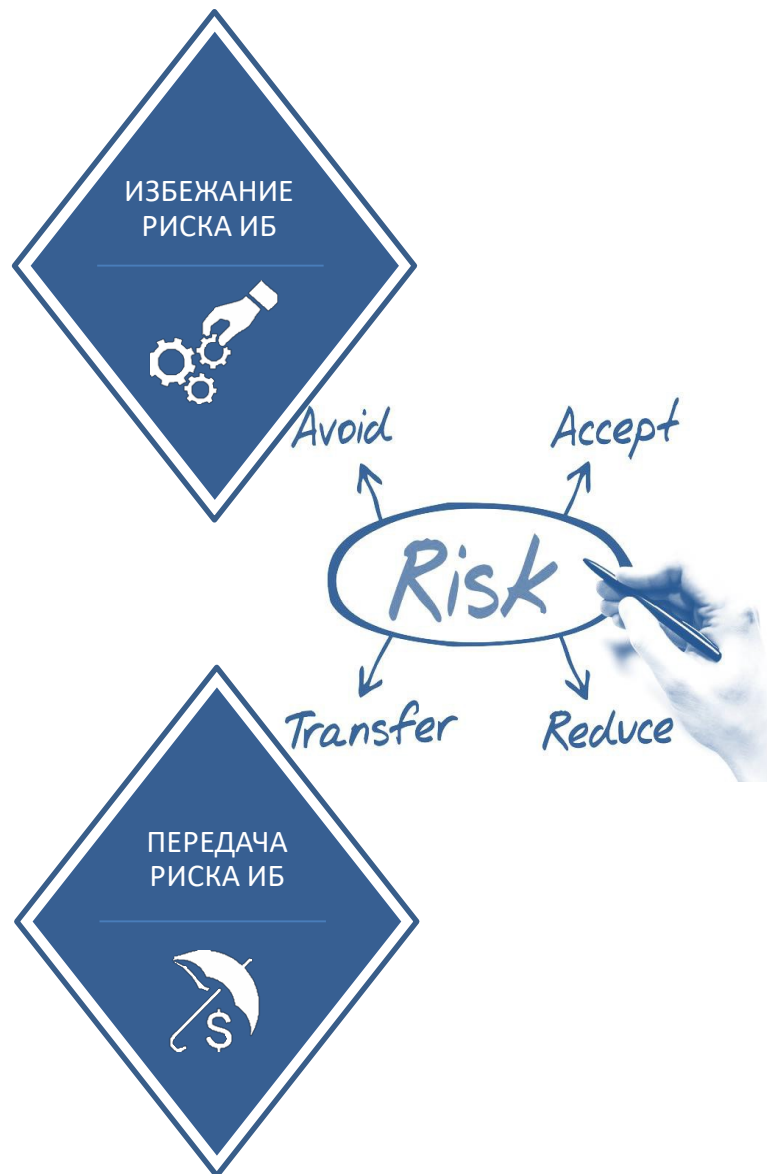
Способы обработки рисков ИБ и модели предоставления услуг



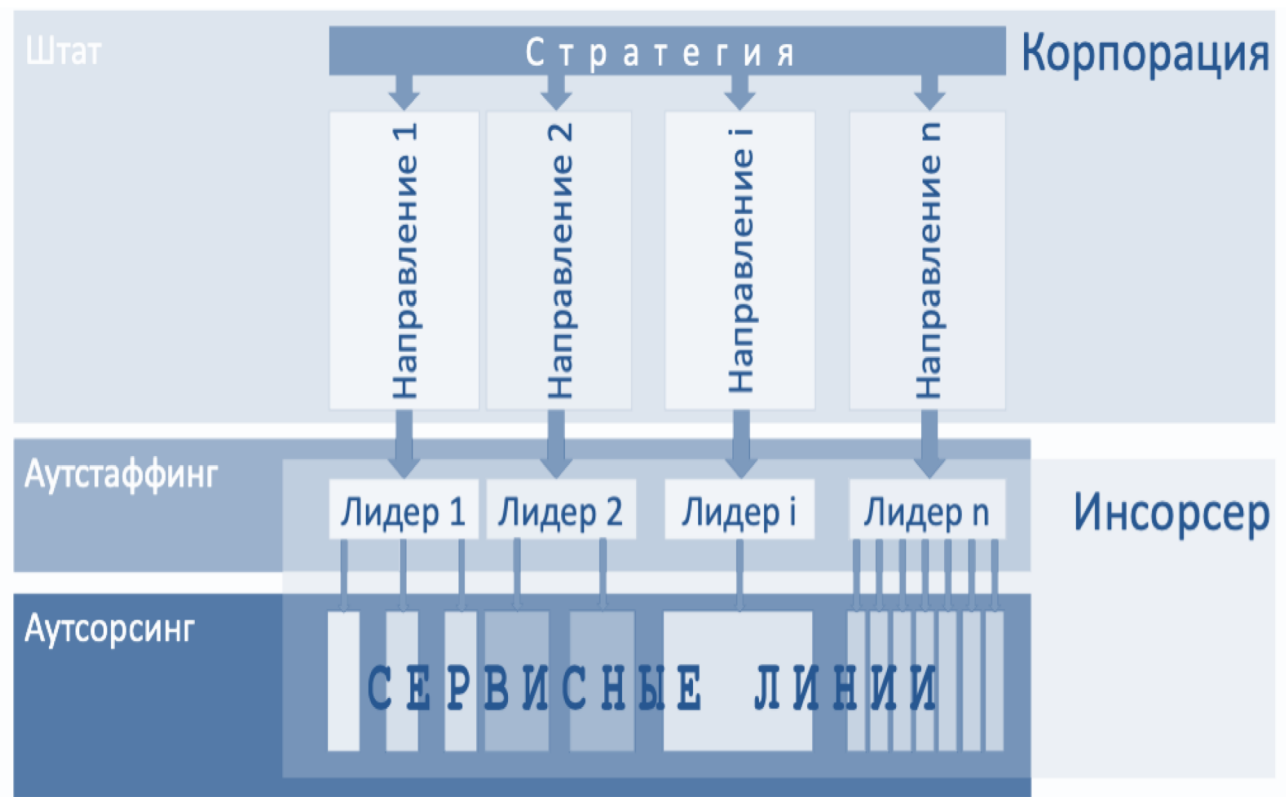
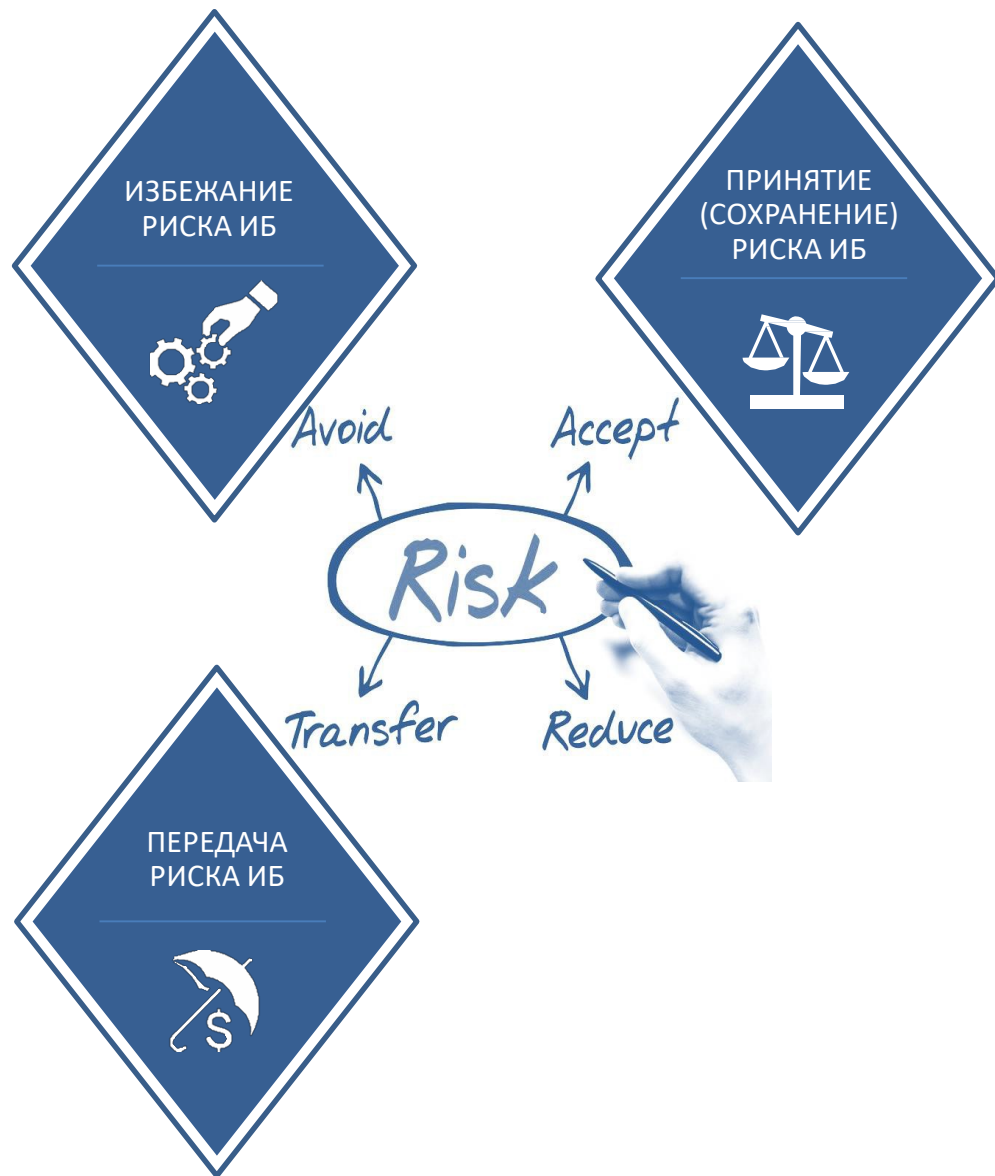
Способы обработки рисков ИБ и модели предоставления услуг

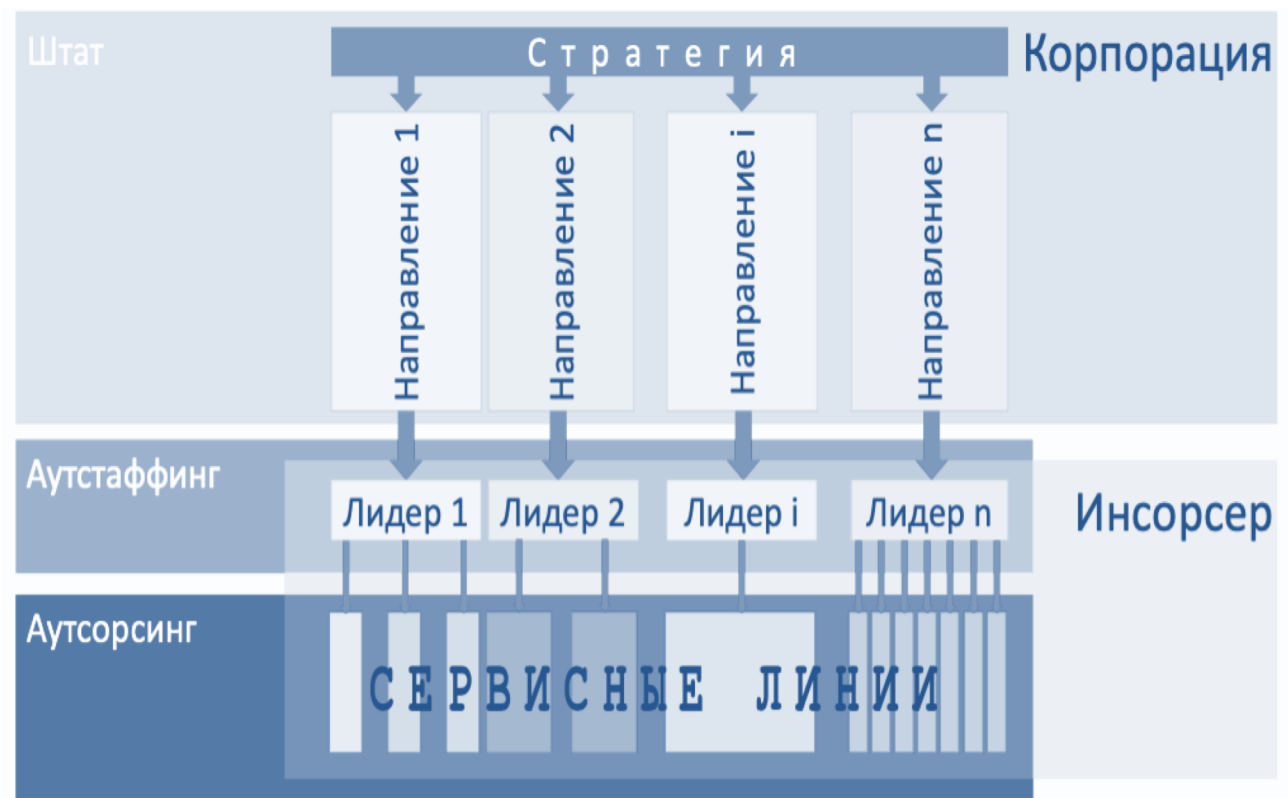


Способы обработки рисков ИБ и модели предоставления услуг

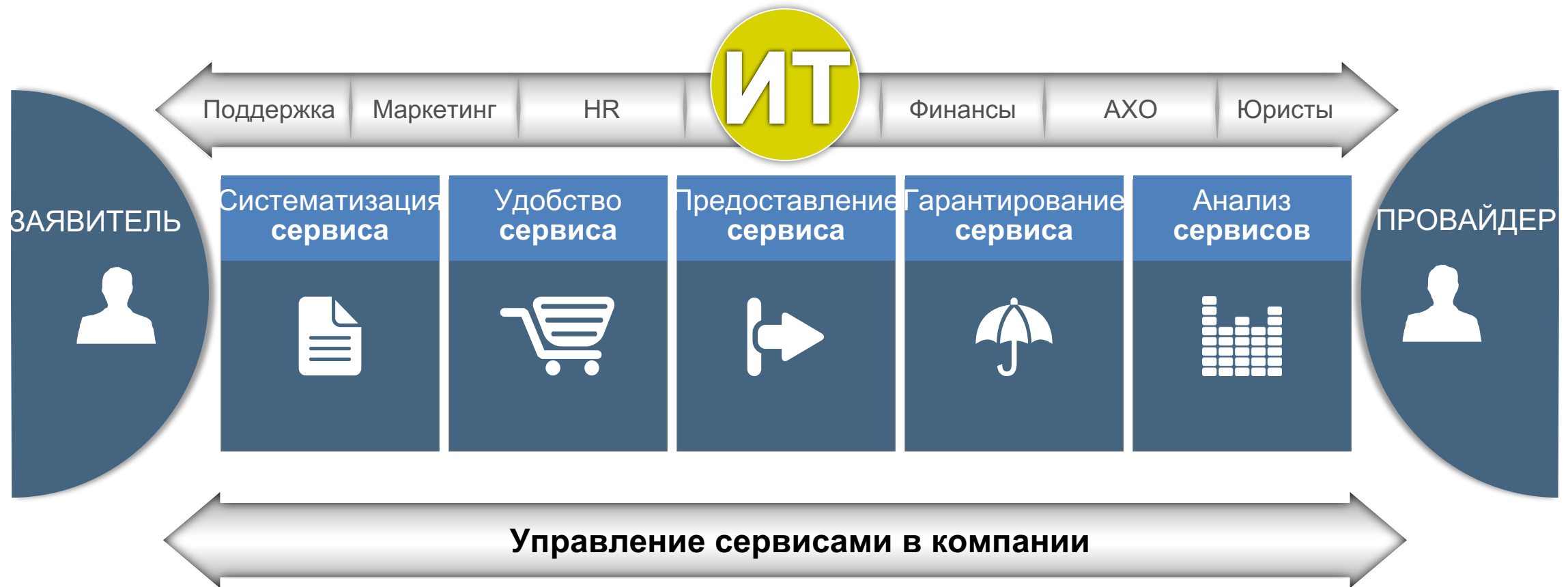


Способы обработки рисков ИБ и модели предоставления услуг





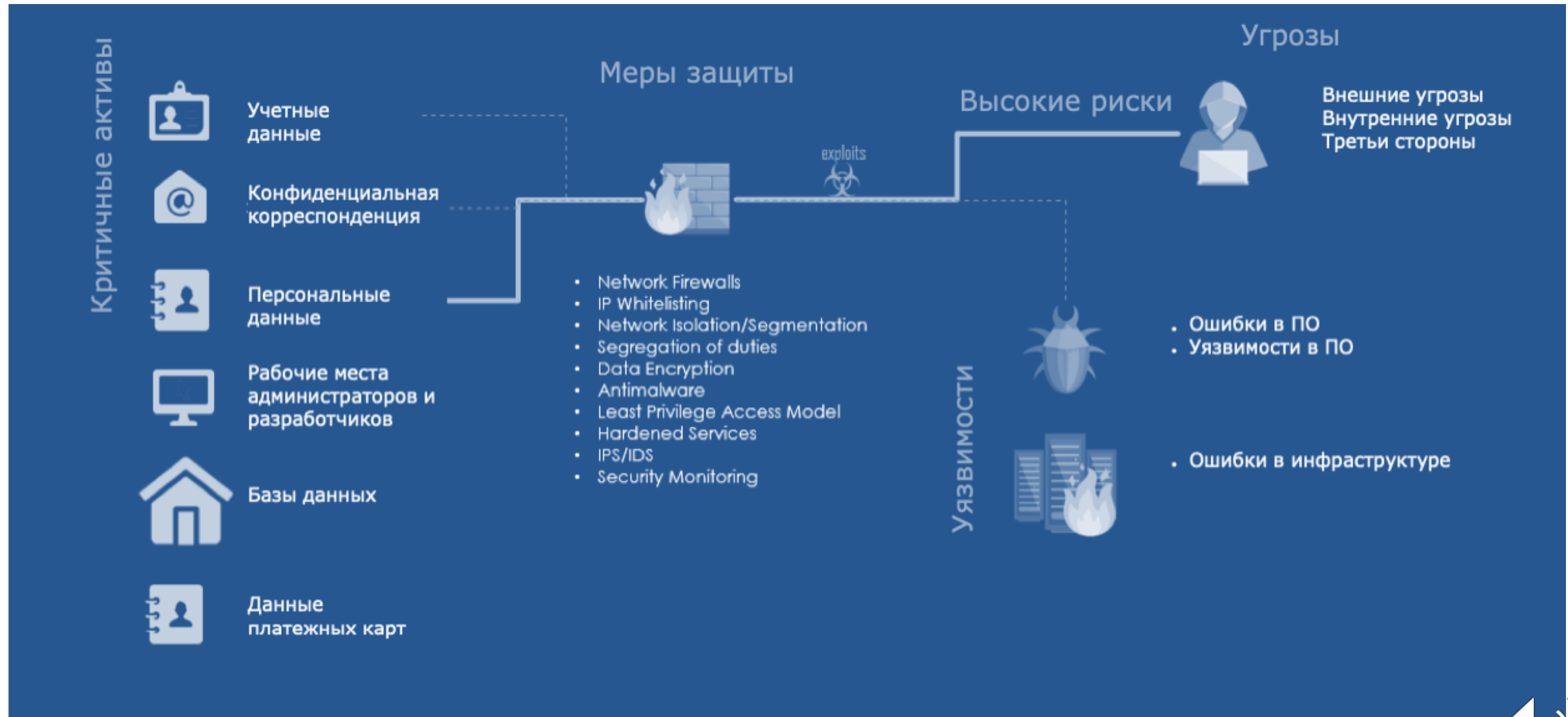
Корпоративная сервис-модель



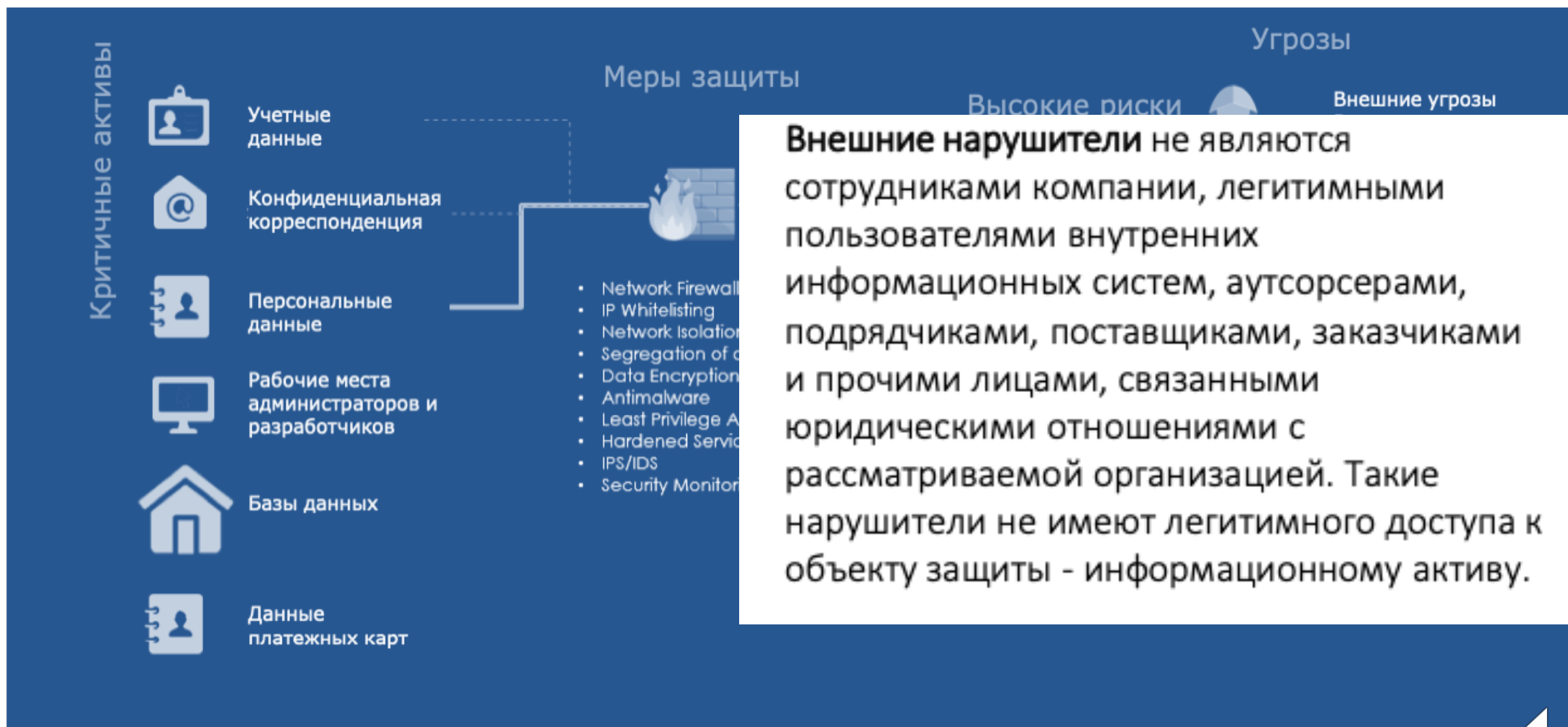
Информационная безопасность стремится в поддержку оптимизации сервисов



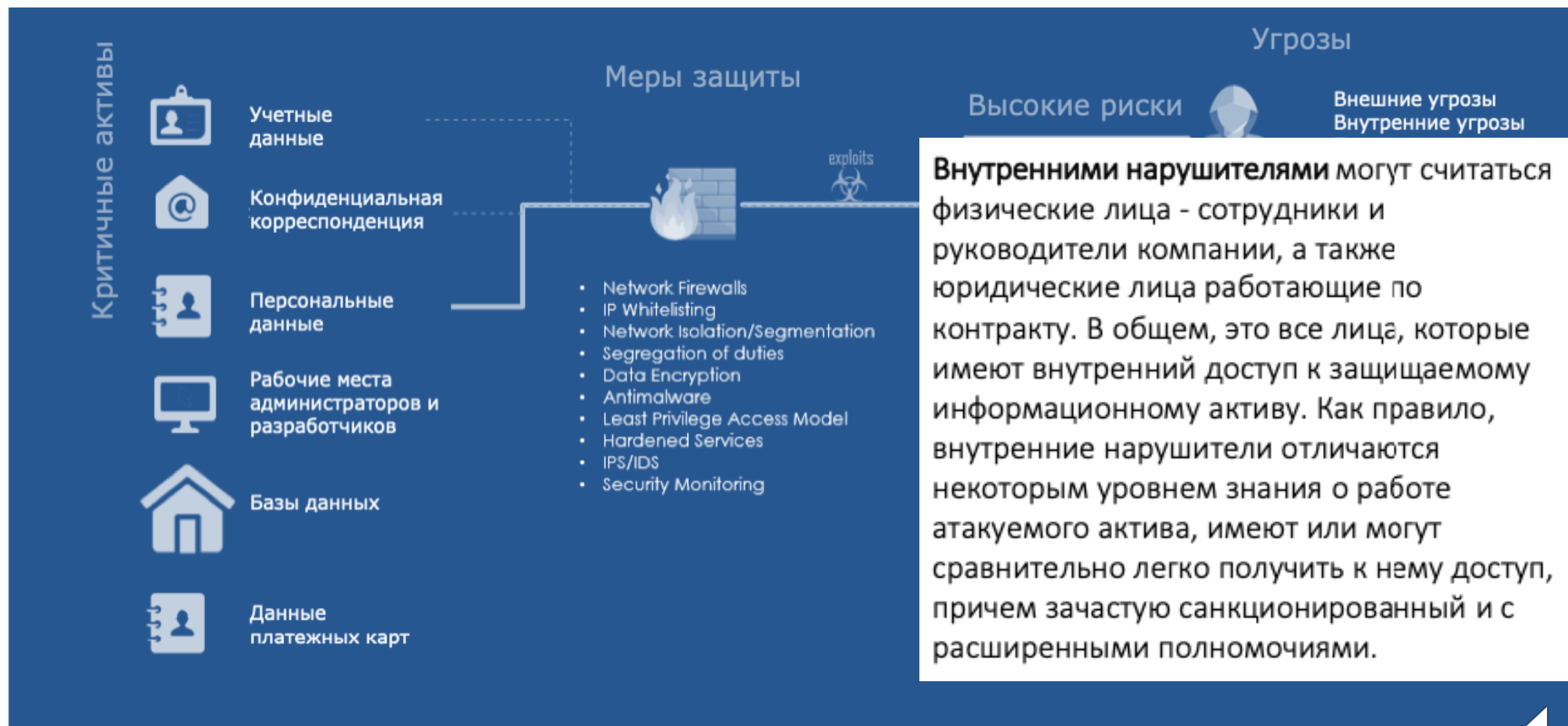
Модель управления угрозами информационной безопасности



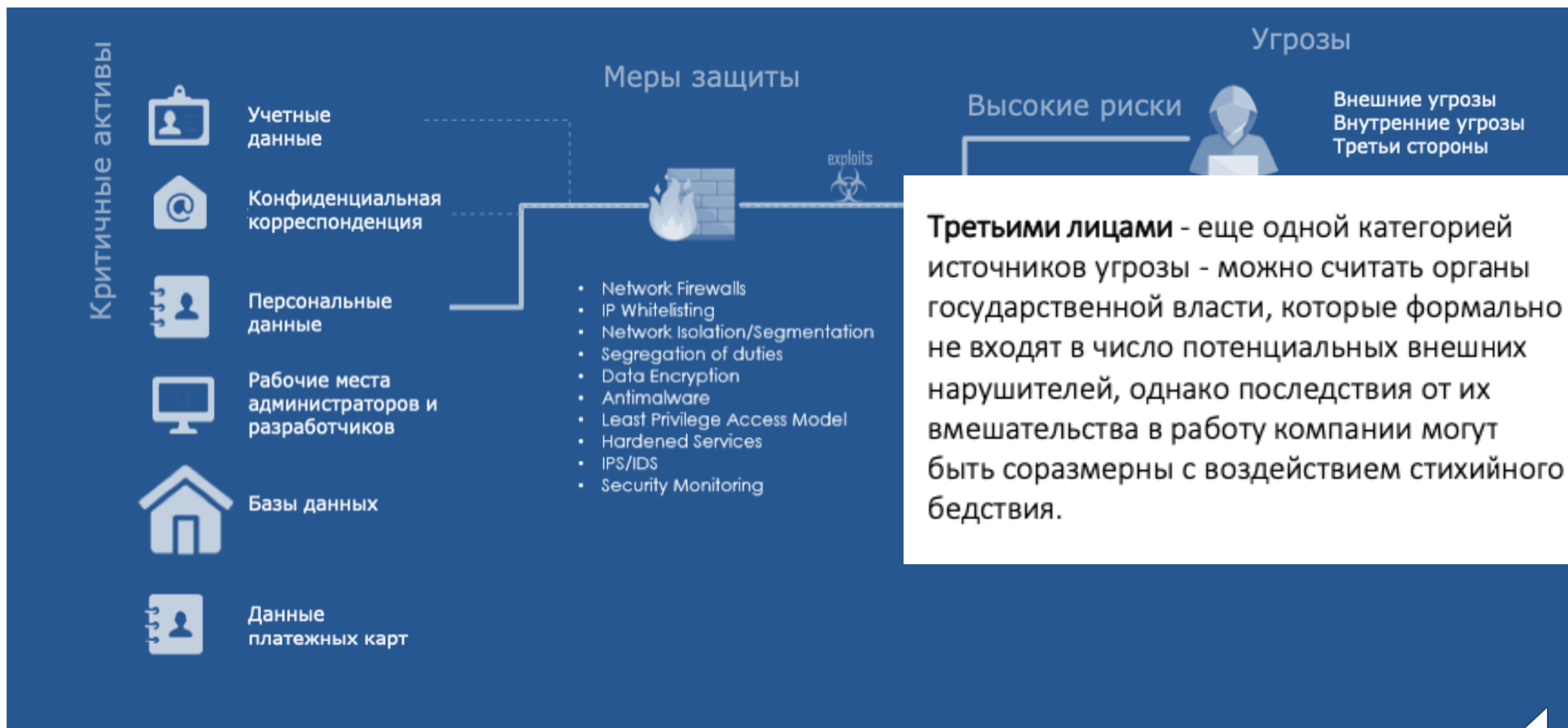
Модель управления угрозами информационной безопасности



Модель управления угрозами информационной безопасности



Модель управления угрозами информационной безопасности



**Благодарю
за внимание!**

