Подходы к оценке уровня зрелости кибербезопасности промышленных предприятий

Сычев Артем
Начальник центра мониторинга и реагирования на компьютерные инциденты

ПРЕДПОСЫЛКИ К СОЗДАНИЮ МЕТОДИКИ ОЦЕНКИ УРОВНЯ РЕАЛИЗАЦИИ МЕР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РТ Информационная безопасность

1. Возросшее количество компьютерных атак на IT-инфраструктуру Российской Федерации
2. Наличие собственной методики оценки зрелости SOC-центра на базе SOC-CMM
3. Указ Президента Российской Федерации от 01.05.2022 № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации"
4. Доведение руководству важности информационной безопасности как неотъемлемого элемента для обеспечения устойчивости предприятий
5. Корректность оценки проведенных работ по анализу защищенности со стороны Исполнителя работ и со стороны предприятий

ЦЕЛИ СОЗДАНИЯ МЕТОДИКИ ОЦЕНКИ УРОВНЯ РЕАЛИЗАЦИИ МЕР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РТ Информационная безопасность

Целью методики является стандартизация подходов и способов оценки уровня реализации мер информационной безопасности в компаниях, входящих в Государственную Корпорацию «Ростех» по направлениям оценки:

1. Реализации мер и мероприятий по обеспечению безопасности вычислительной сети
2. Реализации мер и мероприятий в соответствии с нормативными требованиями
3. Реализации мер и мероприятий по мониторингу и реагированию.

Методика разработана с учетом положений и методологий порядка **30 документов**

1. Приказы ФСТЭК России;
2. ГОСТы Р ИСО/МЭК;
3. SOC-CMM: Measuring capability maturity in Security Operations Centers;
4. Cobit;
5. Методический документ «Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств» (утвержден ФСТЭК России 28 октября 2022 г.).
6. Методика оценки угроз безопасности информации ФСТЭК России от 05.02.2021

ТИПОВОЕ ТЕХНИЧЕСКОЕ ЗАДАНИЕ МИНЦИФРЫ

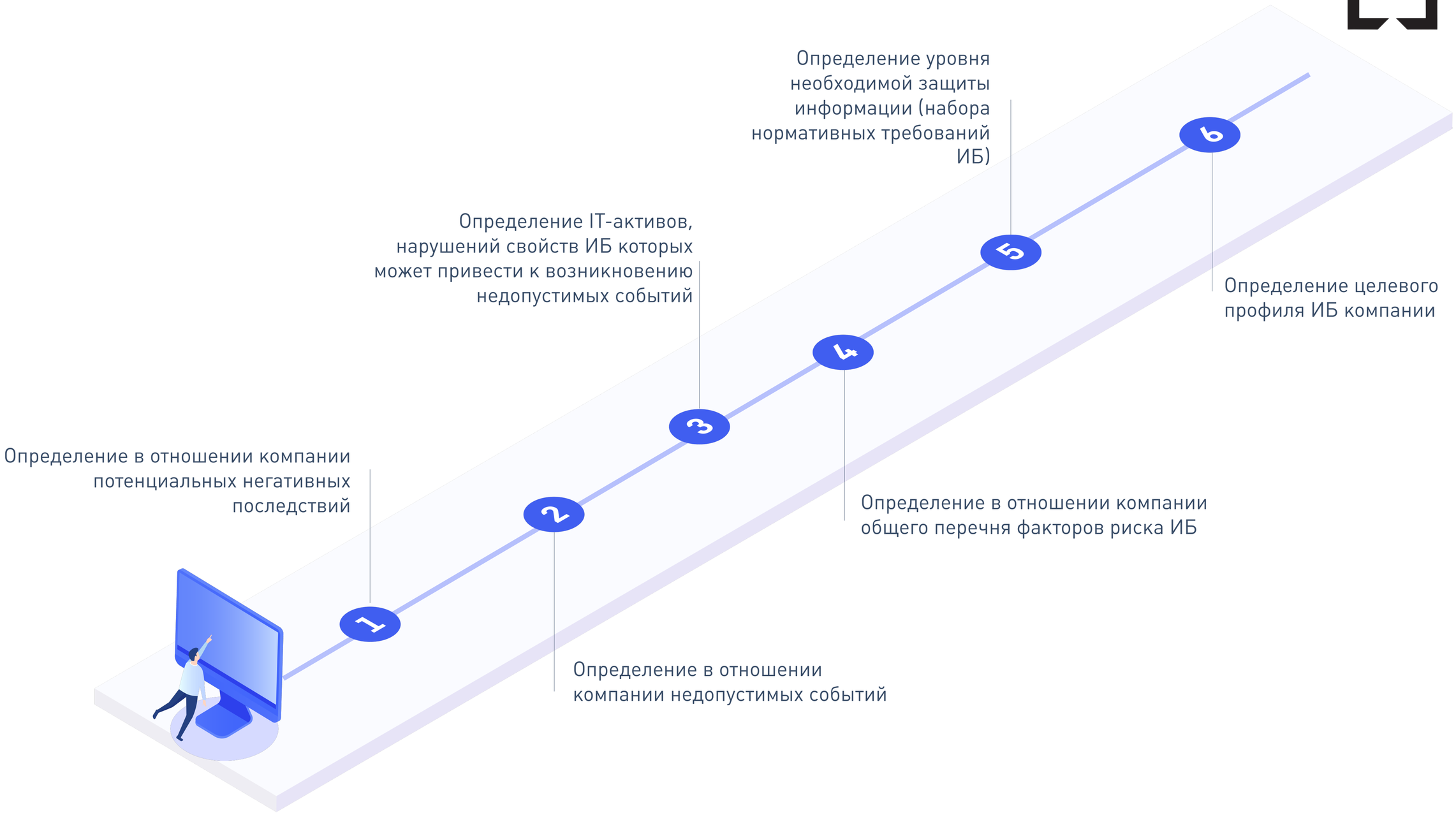
РТ Информационная безопасность

1. Стратегические риски (недопустимые события) ИБ
2. Критерии реализации НС
3. Целевые системы
4. Оценка защищенности внешнего периметра
5. Анализ возможностей внешних и внутренних нарушителей
6. Верификация реализуемости НС

№	Вопрос	Ответ
1.	Наименование организации	*АО «Химия»;*
2.	Отрасль организации (сфера деятельности)	*Химическая промышленность*
3.	Основные виды деятельности	*Производство селитры* *Производство аммиака*
4.	Каким направлениями и нормативно правовым актам по ИБ должны соответствовать организация	• *НПА в области защиты государственных информационных систем (Приказ ФСТЭК № 17)* • *НПА в области защиты Персональных данных (152-ФЗ, Приказ ФСТЭК № 21)* • *НПА в области защиты КИИ (187-ФЗ, Приказ ФСТЭК № 239 и т.д.)* • *ГОСТ ЦБ (ГОСТ Р 57580.1-2017)*
5.	Оцените какие возможные недопустимые события[1] могут иметь место применимо к рассматриваемой организации Перечень возможных недопустимых событий приведён в Приложении 1.	• *Угроза жизни или здоровью* • *Вредные воздействия на окружающую среду*
6.	Оцените возможны масштаб ущерба при наступлении недопустимых событий	*Угроза жизни или здоровью (2000 человек),* *Экологический ущерб (вредные выбросы на территории, где проживают 125 000 человек)*
7.	Приведите перечень типов целевых систем, воздействие на которых может непосредственно привести к наступлению недопустимого события в рамках деятельности организации	*АСУ ТП по производству химии;* *Ситуационный центр*

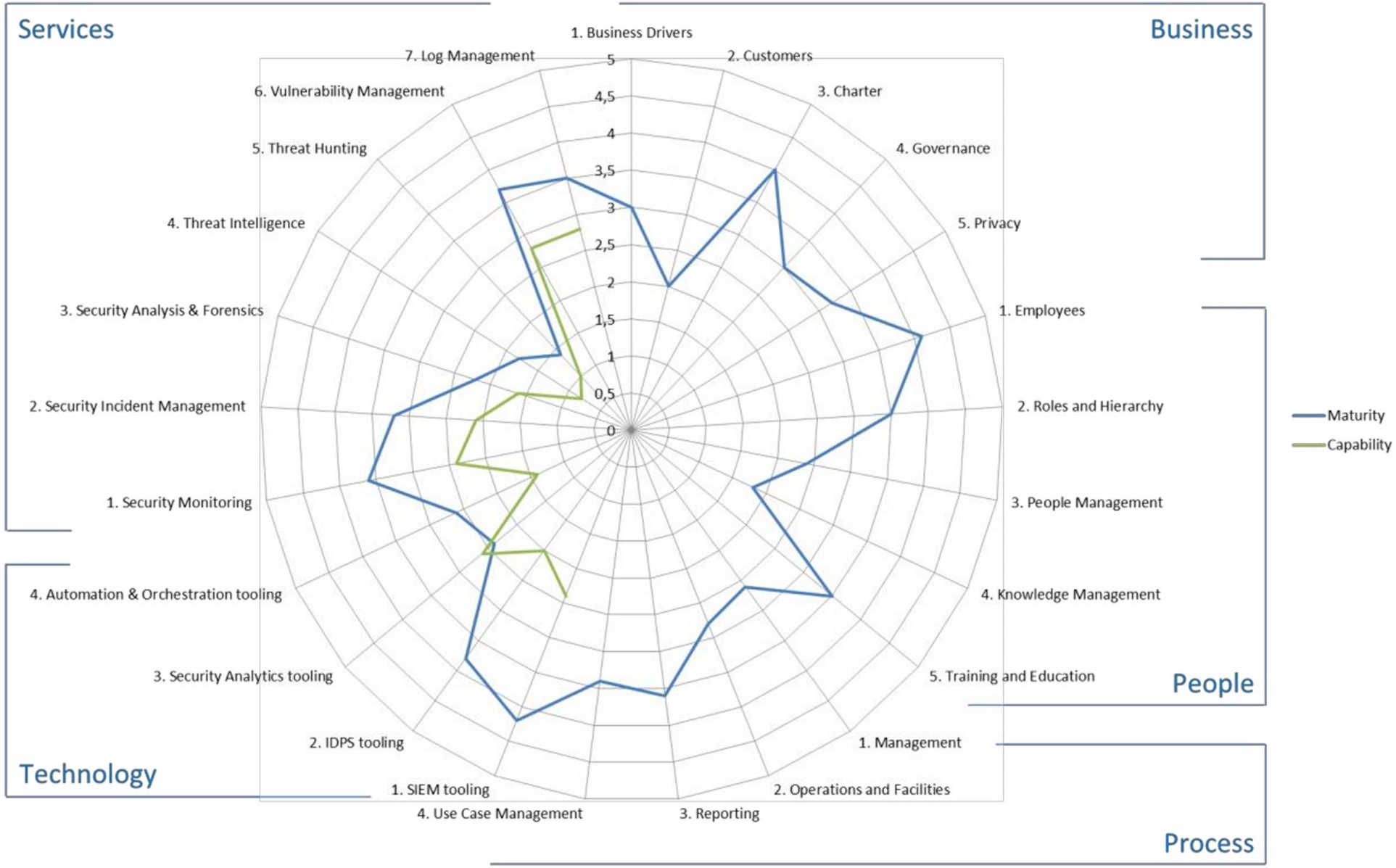
ОПРЕДЕЛЕНИЕ ПРОФИЛЯ ЗАЩИТЫ ДЛЯ ПРЕДПРИЯТИЙ

PT Информационная безопасность

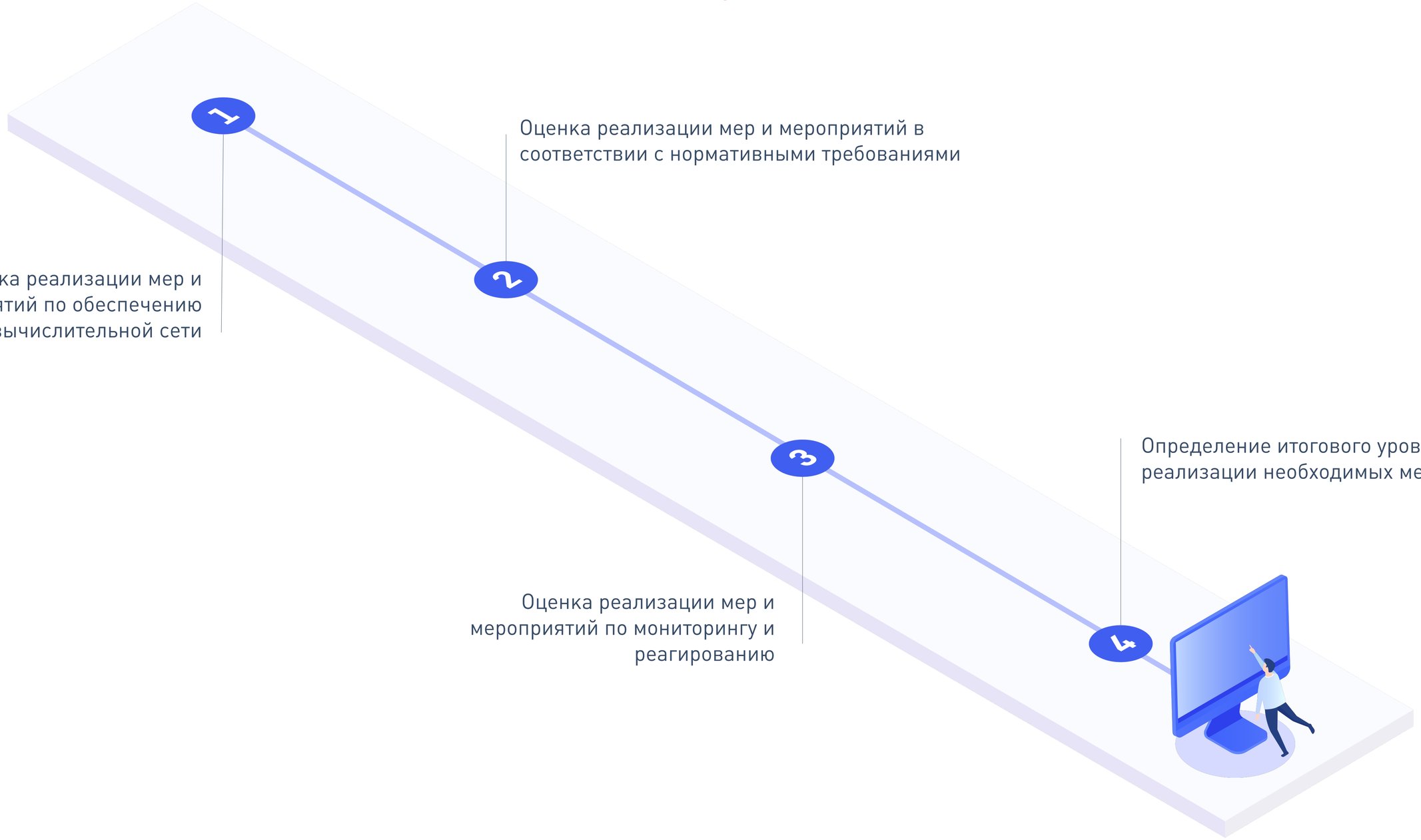


ОПРЕДЕЛЕНИЕ ПРОФИЛЯ ЗАЩИТЫ ДЛЯ КОМПАНИИ И МЕТОДИКА ОЦЕНКИ УРОВНЯ РЕАЛИЗАЦИИ МЕР

PT Информационная безопасность



ОПРЕДЕЛЕНИЕ ПРОФИЛЯ ЗАЩИТЫ ДЛЯ КОМПАНИИ И МЕТОДИКА ОЦЕНКИ УРОВНЯ РЕАЛИЗАЦИИ МЕР



ВЫЗОВЫ

РТ Информационная безопасность

1

- Отсутствие фиксированного числа недопустимых событий от регуляторов

2

- Уход из РФ большего числа сканеров уязвимостей. Доработка методики оценки уровня критичности уязвимостей программных, программно-аппаратных средств с практической точки зрения.
- Учет наличия эксплойтов в сети Интернет, время с момента публикации уязвимости до обнаружения её в ИТ-инфраструктуре и др.

3

- Отсутствие подходов к инвентаризации ИТ-активов, особенно в сегменте АСУ ТП

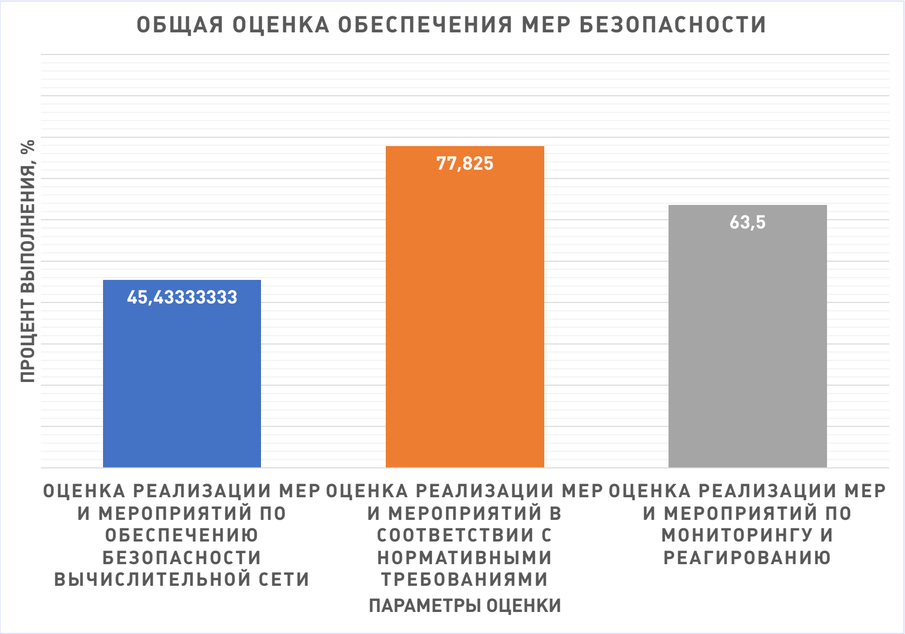
РЕЗУЛЬТАТ

РТ Информационная безопасность

По результатам оценки уровня реализации мер ИБ в организациях, входящих в контур государственной корпорации «Ростех», должно осуществляться:

- Формирование выводов о степени реализуемости в компании недопустимых событий ИБ и наступлении негативных последствий
- Определение первоочередных мер и мероприятий обеспечения защищённости целевых активов и сетевого периметра компании
- Закрепление персональной ответственности за реализацию требований ИБ и/или достижение минимального и целевого уровня реализации необходимых мер ИБ

Параметр оценки	Результаты оценки
Оцнка реализации мер и мероприятий по обеспечению безопасности вычислительной сети	45,43333333
Оценка реализации мер и мероприятий в соответствии с нормативными требованиями	77,825
Оценка реализации мер и мероприятий по мониторингу и реагированию	63,5
Общий процент выполнения (количественная интегрированная оценка), %:	62,3
Качественная интегрированная оценка уровня обеспечения мер безопасности:	Второй



РТ

Информационная
безопасность

rt-ib.ru
info@rt-ib.ru
+7(499) 390-79-05