

Руководство пользователя

«Кибер Радар 360»

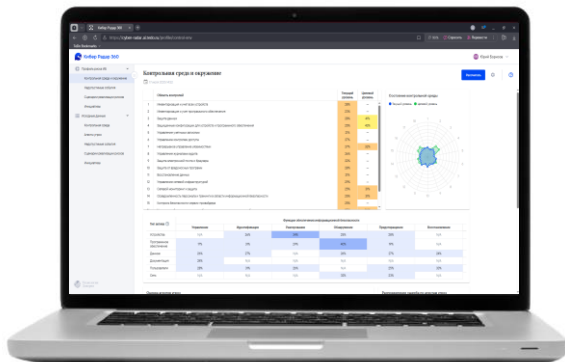
Версия документа: 01.25
2025 г.



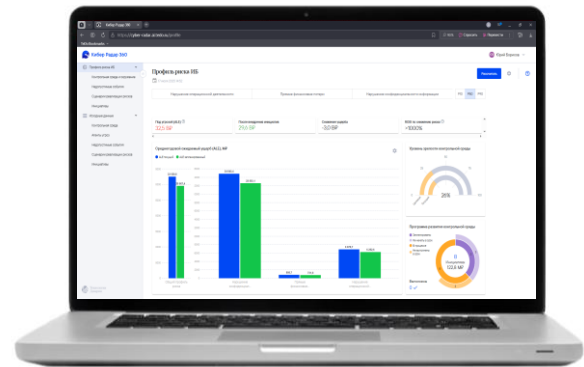
Технологии
Доверия

Платформа количественной оценки рисков ИБ

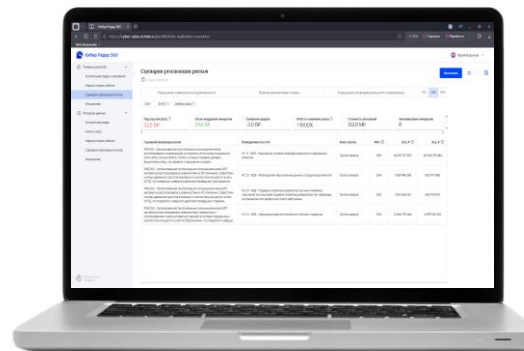
Анализ зрелости
контрольной среды



Профиль киберриска — общий
дашборд для руководства



Определение сценариев
киберрисков



Проблематика

Измерение и описание профиля киберрисков непростая задача для большинства организаций, особенно для тех, менеджмент которых имеет высокий интерес к этой области и зрелые запросы:

- Какие еще усилия мы должны сделать для достижения нужного уровня защищенности?
- Насколько реальны направленные на нас угрозы?
- Защищены ли мы в достаточной для нас степени?
- Инвестиции в какие элементы контрольной среды приведут к наибольшему снижению риска?

Платформа «Кибер Радар 360»

Платформа прагматична, позволяет сфокусироваться на ключевых рисках и компонентах контрольной среды, реализуя при этом количественную оценку профиля киберриска. Платформа позволяет:

- Продемонстрировать финансовую оценку профиля риска Компании
- Рассчитывать финансовую эффективность и отдачу от инвестиций в развитие ИБ
- Предоставить обоснование при формировании бюджета ИБ и вовлечь бизнес в процесс оценки
- Осуществить интеграцию в общекорпоративный риск-менеджмент

Авторизация

Для того чтобы войти в платформу количественной оценки рисков «Кибер Радар 360»:

- Перейдите по ссылке: *<определяется при инсталляции продукта в ИТ-инфраструктуры заказчика>*
- Нажмите кнопку «Выполнить вход»
- Авторизуйтесь по предоставленным учетным данным.



Выполнить вход

Сложности со входом?
Свяжитесь с [администратором](#)

КИБЕР РАДАР 360

Вход в учетную запись русский ▾

Имя пользователя или E-mail

Пароль 👁

Вход








Область навигации

Раздел «Профиль риска ИБ» и входящие в него подразделы демонстрируют текущее и целевое состояние контрольной среды на основе заполненных исходных данных

В раздел «Исходные данные» и входящие в него подразделы заносится исходная информация для количественной оценки рисков ИБ

Кибер Радар 360

-  Профиль риска ИБ 
 - Контрольная среда и окружение 
 - Недопустимые события
 - Сценарии реализации рисков
 - Инициативы
-  Исходные данные 
 - Контрольная среда
 - Агенты угроз
 - Недопустимые события
 - Сценарии реализации рисков
 - Инициативы



Исходные данные

В разделе «Исходные данные» демонстрируется план действий при первом заполнении Платформы

Для каждого шага заполнения представлено краткое описание

После нажатия кнопки «Подробнее» открывается текстовая и видеоинструкция

Исходные данные

Внесите данные согласно шагам

Шаг 1
Контрольная среда
Заполните информацию по контролям для оценки уровня зрелости ИБ
Подробнее Перейти →

Шаг 2
Агенты угроз
Выберите наиболее вероятных для компании агентов угроз и оцените степень их влияния
Подробнее Перейти →

Шаг 3
Недопустимые события
Сформируйте реестр недопустимых событий
Подробнее Перейти →

Шаг 4
Сценарии реализации рисков
Опишите сценарии реализации рисков и параметры расчета их ущерба для наилучшего и наихудшего случаев
Подробнее Перейти →

Шаг 5
Инициативы
Внесите инициативы по снижению рисков ИБ
Подробнее Перейти →

Чтобы попасть на окно заполнения каждого из шагов, необходимо нажать кнопку «Перейти»



Исходные данные (контрольная среда)

Выберите методологию оценки в правом верхнем углу. В зависимости от методологии появится уникальный набор контролей (в разработке), по умолчанию: SANS CIS 18 v8.1

1

Выберите текущие значения критериев по каждому из контролей

2

Для выполнения расчетов должны быть заполнены значения по всем критериям (необходимо заполнить все страницы)

3

При нажатии открывается подробная инструкция

4

Контрольная среда

Методология оценки: SANS CIS 18 v8.1

ID	Область контролей	Название контроля	Документация по контролю	Объем покрытия контролем (охват)	Автоматизация контроля	Отчетность о контроле
1,1	Инвентаризация и учет всех устройств	Создать и поддерживать детальный реестр всех устройств	Частично сфор...	Минимальной	Частично авто...	Частично реал...
1,2	Инвентаризация и учет всех устройств	Реагировать на неавторизованные устройства	Отсутствует	Контроль не вы...	Не применимо	Соответствует ...
1,3	Инвентаризация и учет всех устройств	Использовать инструменты для активного обнаружения	Частично сфор...	Контроль не вы...	Контроль не вы...	Соответствует ...
1,4	Инвентаризация и учет всех устройств	Вести журнал ДНСР (протокола динамической настройки узла) для обновления реестра устройств	Отсутствует	Контроль не вы...	Контроль не вы...	Отсутствует
1,5	Инвентаризация и учет всех устройств	Использовать инструменты для пассивного обнаружения устройств	Частично сфор...	Минимальной	Не применимо	Отсутствует
2,1	Инвентаризация и учет программного обеспечения	Создать и поддерживать реестр используемого программного обеспечения	Частично сфор...	Минимальной	Контроль не вы...	Отсутствует
2,2	Инвентаризация и учет программного обеспечения	Проверить, что авторизованное программное обеспечение из реестра поддерживается вендором	Отсутствует	Контроль не вы...	Автоматизиров...	Отсутствует
2,3	Инвентаризация и учет программного обеспечения	Реагировать на неавторизованное программное обеспечение	Отсутствует	Минимальной	Контроль не вы...	Частично реал...
2,4	Инвентаризация и учет программного обеспечения	Использовать инструменты для автоматического учета программного обеспечения	Частично сфор...	Контроль не вы...	Частично авто...	Частично реал...
2,5	Инвентаризация и учет программного обеспечения	Использовать бейеве списки авторизованного программного обеспечения	Отсутствует	Контроль не вы...	Контроль не вы...	Соответствует ...
2,6	Инвентаризация и учет программного обеспечения	Использовать бейеве списки авторизованных библиотек	Частично сфор...	Контроль не вы...	Контроль не вы...	Соответствует ...
2,7	Инвентаризация и учет программного обеспечения	Использовать бейеве списки авторизованных скриптов	Отсутствует	Контроль не вы...	Контроль не вы...	Отсутствует
3,1	Защита данных	Наладить и поддерживать процесс управления данными	Частично сфор...	Минимальной	Частично авто...	Частично реал...
3,2	Защита данных	Создать и поддерживать реестр для учета данных	Отсутствует	Контроль не вы...	Не применимо	Соответствует ...
3,3	Защита данных	Настроить списки для управления доступом к данным	Частично сфор...	Контроль не вы...	Контроль не вы...	Соответствует ...

1

4

2

3



Исходные данные (агенты угроз)

Пункты «Название» и «Вид агента угрозы» не требуют изменения

1

Необходимо выбрать актуальные агенты угроз с помощью переключателя

2

Необходимо для всех критериев выставить значения актуальные для оцениваемой организации (для выполнения расчетов по всем актуальным агентам угроз должны быть заполнены все значения критериев)

3

При наведении курсора на условный знак появляется пояснение по критерию оценки

4

При нажатии открывается подробная инструкция

5

Агенты угроз

Преднамеренные

1	2	3	4	5	6	7	8
Название	Вид агента угрозы	Сила агента угрозы	Статистика	История	Ресурсы-Сила	Мотивация	Последовательность
<input checked="" type="checkbox"/> Сотрудники (привилегированные)	Внутренний	Высокий	Средний	Средний	Высокий	Средний	Средний
<input checked="" type="checkbox"/> Сотрудники (рядовые)	Внутренний	Низкий	Средний	Сверхнизкий	Низкий	Средний	Сверхнизкий
<input checked="" type="checkbox"/> Группа хакеров	Внешний	Высокий	Высокий	Средний	Высокий	Высокий	Средний
<input checked="" type="checkbox"/> Одиночный хакер	Внешний	Средний	Высокий	Сверхнизкий	Средний	Средний	Низкий
<input checked="" type="checkbox"/> Журналист-расследователь	Внешний	Низкий	Высокий	Низкий	Низкий	Средний	Низкий
<input checked="" type="checkbox"/> Иностранное государство	Внешний	Высокий	Средний	Высокий	Высокий	Высокий	Высокий
<input checked="" type="checkbox"/> Технологический поставщик / партнер (внутренний)	Внутренний	Средний	Сверхнизкий	Сверхнизкий	Сверхнизкий	Сверхнизкий	Сверхнизкий
<input checked="" type="checkbox"/> Технологический поставщик / партнер (внешний)	Внешний	Средний	Сверхнизкий	Средний	Средний	Сверхнизкий	Сверхнизкий
<input checked="" type="checkbox"/> Террористическая организация	Внешний	Сверхнизкий	Сверхнизкий	Сверхнизкий	Сверхнизкий	Сверхнизкий	Сверхнизкий
<input checked="" type="checkbox"/> Конкурент	Внешний	Средний	Сверхнизкий	Сверхнизкий	Высокий	Средний	Низкий

Случайные

1	2	3	4	5	6	7	8
Название	Вид агента угрозы	Сила агента угрозы	Статистика	История	Привилегии	Культура	Компетентность
<input checked="" type="checkbox"/> Клиент	Внешний	Сверхнизкий	Сверхнизкий	Сверхнизкий	Средний	Низкий	Сверхнизкий
<input checked="" type="checkbox"/> Сотрудники (рядовые)	Внутренний	Низкий	Средний	Сверхнизкий	Низкий	Низкий	Низкий
<input checked="" type="checkbox"/> Сотрудники (привилегированные)	Внутренний	Высокий	Средний	Высокий	Сверхнизкий	Средний	Высокий
<input checked="" type="checkbox"/> Технологический поставщик / партнер (внешний)	Внешний	Средний	Сверхнизкий	Средний	Средний	Средний	Средний
<input checked="" type="checkbox"/> Технологический поставщик / партнер (внутренний)	Внутренний	Высокий	Сверхнизкий	Высокий	Средний	Средний	Высокий



Исходные данные (недопустимые события) 1/3

Недопустимые события

1

3 [Добавить недопустимое событие](#) 2

ID	Категория недопустимого события	Описание недопустимого события	Сегмент / Направление бизнеса / Другое	Приоритет	
11	Нарушение конфиденциальности информации	Нарушение условий конфиденциальности информации клиентов	B2B	Высокий	⋮
12	Нарушение конфиденциальности информации	Разглашение персональных данных сотрудников/клиентов	B2B	Средний	⋮
21	Прямые финансовые потери	Подмена платежных реквизитов крупных платёжных поручений или массовая подмена платежных реквизитов при переводах контрагентам или заработной платы работникам	B2B	Средний	⋮
31	Нарушение операционной деятельности	Нарушение работоспособности систем и сервисов	B2B	Высокий	⋮

4

Для упрощенной навигации в реестре используйте поисковую строку

1

При нажатии открывается подробная инструкция

2

Для создания нового недопустимого события необходимо нажать кнопку «Добавить недопустимое событие» (см. слайд 11)

3

При нажатии открывается список действий позволяющий удалить, редактировать и показать детальное описание (см. слайд 10)

4

4

Приоритет	
Высокий	⋮
Показать детали	
Редактировать	
Удалить	
Высокий	⋮



Исходные данные (недопустимые события) 2/3

Для перехода в режим редактирования нажмите на кнопку «Редактировать»

1

Для того, чтобы удалить недопустимое событие нажмите кнопку «Удалить недопустимое событие»

2

Для того, чтобы сохранить или отменить изменения нажмите соответствующую кнопку

3

Для перехода во вкладку опросы респондентов выберите «Опросы респондентов»

4

Недопустимые события > Просмотр недопустимого события
Нарушение работоспособности систем и сервисов
ID ИС 31

Описание Опросы респондентов

Категория недопустимого события *
Нарушение операционной деятельности

Описание *
Нарушение работоспособности систем и сервисов

Подробное описание
Выход из строя одного или нескольких корневых ИТ-сервисов Компании (AD, DNS, VPN, sets), критичных бизнес систем или рабочих мест работников критично скажется на Компании и может привести к значительным финансовым и репутационным потерям, потере клиентов.

Прямые финансовые потери:
- средний ФОТ работников, которые задействованы в восстановлении ИТ-сервисов за время простоя;
- средний ФОТ работников за время простоя;
- потери выручки за время простоя;
- финансовые потери из-за прямого оттока клиентов (расторжение текущих контрактов).
Косвенные финансовые потери:
- затраты на привлечение специалистов по форензике и расследованию инцидентов ИБ;
- затраты на восстановление репутации.

Сегмент / Направление бизнеса / Другое
B2B

Приоритет
Высокий

1 Редактировать

2

Недопустимые события > Редактирование недопустимого события
Нарушение работоспособности систем и сервисов
ID ИС

Описание Опросы респондентов

Категория недопустимого события *
Нарушение операционной деятельности

Описание *
Нарушение работоспособности систем и сервисов

Подробное описание
Выход из строя одного или нескольких корневых ИТ-сервисов Компании (AD, DNS, VPN, sets), критичных бизнес систем или рабочих мест работников критично скажется на Компании и может привести к значительным финансовым и репутационным потерям, потере клиентов.

Прямые финансовые потери:
- средний ФОТ работников, которые задействованы в восстановлении ИТ-сервисов за время простоя;
- средний ФОТ работников за время простоя.

Сегмент / Направление бизнеса / Другое
B2B

Приоритет
Высокий

3 Отменить Сохранить



Исходные данные (недопустимые события) 3/3

Для внесения опросов респондентов перейти на вкладку «Опросы респондентов»

1

Для создания нового недопустимого события необходимо заполнить данные поля

2

Необходимо нажать «Добавить опрос» и заполнить информацию по опросу

3

2

5

4

При нажатие открывается подробная инструкция

4

После заполнения всех необходимых полей для сохранения или отмены изменений нажмите соответствующие кнопки

5

Чтобы удалить опрос респондента нажмите данную кнопку

6

3

6



Исходные данные (сценарии реализации рисков) 1/3

Для упрощенной навигации в реестре используйте поисковую строку

1

Для добавления нового сценария нажмите кнопку «Добавить сценарий»

2

Для редактирования списка параметров расчета ущерба от реализации рисков ИБ нажмите кнопку «Параметры»

3

Сценарии реализации рисков

1

3 2 8

Параметры Добавить сценарий

Q. Найти сценарий

Категория недопустимого события	Описание недопустимого события	Краткое описание сценария реализации риска	Тип угрозы	Агент угрозы	Векторы атак	Ущерб – наилучший случай, Р	Ущерб – наихудший случай, Р
Нарушение конфиденциальности информации	НС 11 - БЗВ - Нарушение условий конфиденциальности информации клиентов	РИБ.001 - Организованная группа внешних злоумышленников воспользовалась информацией из открытых источников (социальные сети...	Преднамеренный	Группа хакеров	Фишинг; Слабый/словарный пароль	12 010 000 000	78 010 000 000
Нарушение конфиденциальности информации	НС 12 - БЗВ - Разглашение персональных данных сотрудников/клиентов	РИБ.002 - Организованная группа внешних злоумышленников (АРТ, хактивисты) воспользовалась уязвимостями в ИС Компании, слабостям...	Преднамеренный	Группа хакеров	Эксплуатация уязвимостей в ПО или ОС	10 000 000	3 005 000 000
Прочие финансовые потери	НС 21 - БЗВ - Подмена платежных реквизитов крупных платежных поручений или массовая подмена платежных реквизитов при переводах контрагентам или заработной платы работникам	РИБ.003 - Организованная группа внешних злоумышленников (АРТ, хактивисты) воспользовалась уязвимостями в ИС Компании, слабостям...	Преднамеренный	Группа хакеров	Эксплуатация уязвимостей в ПО или ОС	505 000 000	2 505 000 000
Нарушение операционной деятельности	НС 31 - БЗВ - Нарушение работоспособности систем и сервисов	РИБ.004 - Организованная группа внешних злоумышленников (АРТ, хактивисты) воспользовалась уязвимостями, связанными с...	Преднамеренный	Группа хакеров	Слабый/словарный пароль Атака через посредника	5 210 000 000	20 610 000 000

7

Параметры для расчёта ущерба

4

+ Создать новый параметр

Q. Найти в списке

ID	Название параметра и/или наименование ключевого инцидента	Значение
П18	НС 3 Привлечение специалистов по форензике и расследованию инцидентов	5 000 000
П19	НС 4 Время простоя при наихудшем случае (часы)	40
П20	НС 4 Время простоя при наилучшем случае (часы)	120
П21	НС 4 Количество сотрудников Компании	10 000
П22	НС 4 Средний ФОТ работника (в час)	500
П23	НС 4 Годовая выручка Компании за год	100 000 000 000
П24	НС 4 Привлечение специалистов по форензике и расследованию инцидентов ИБ	5 000 000
П25	НС 4 Маркетинговый бюджет Компании в случае необходимости создания позитивной повести в СМИ	
П26	НС 4 Штрафные санкции со стороны клиентов и иное влияние на выручку Компании (прямой отток клиентов) выраженной в % от годовой выручки Компании в наилучшем случае	0.05
П27	НС 4 Штрафные санкции со стороны клиентов и иное влияние на выручку Компании (прямой отток клиентов) выраженной в % от годовой выручки Компании в наихудшем случае	0.2
П28		

5

5

4

6

Закрыть

Для создания нового параметра нажмите кнопку «Создать новый параметр» и заполните пустую строку

4

При необходимости удаления или редактирования существующего параметра нажмите данную кнопку

5

После заполнения данных по новому параметру сохраните или отмените изменения соответствующими кнопками

6

Ущерб – наилучший случай, Р

78 010 000 000	⋮
3 005 000 000	⋮
20 610 000 000	⋮

7

Показать детали
Редактировать
Удалить

При нажатие открывается список действий позволяющий удалить, редактировать и показать детальное описание

7

При нажатие открывается подробная инструкция

8



Исходные данные (сценарии реализации рисков) 2/3

Для расчет ущерба перейдите на вкладку «Расчет ущерба»

1

Необходимо выбрать Категорию недопустимого события и недопустимое событие

2

Внесите краткое и подробное описание сценария реализации риска

3

Выберите из списка тип угрозы (преднамеренный или случайный) и агента угрозы

4

Добавьте применимые и актуальные векторы атаки и события угроз

5

Для отмены изменений или их сохранения нажмите соответствующие кнопки

6

Сценарии реализации рисков > Создание сценария реализации риска

Создание сценария реализации риска

Описание 1 Расчет ущерба

Категория недопустимого события *

Нарушение операционной деятельности

Описание недопустимого события *

Нарушение работоспособности систем и сервисов

[Изменить выбор недопустимого события](#)

Выбор недопустимого события

Категория недопустимого события

Нарушение операционной деятельности

ID ИС	Сигмент/направление	Описание недопустимого события
31	С2В	Нарушение работоспособности систем и сервисов

[Отменить](#) [Выбрать](#)

Краткое описание сценария *

Пример описания:

В результате атаки с использованием уязвимостей в ПО или ОС, связанных с использованием слабых/словесных паролей в Компании, произошло нарушение условий конфиденциальности информации клиентов

Подробное описание сценария

Пример описания:

Организованная группа внешних злоумышленников (АPT, хактивисты) воспользовалась уязвимостями в ИС Компании, слабостями систем удаленного доступа Компании или уязвимостями, связанными с использованием слабых/словесных паролей в Компании, и смогла получить доступ в сеть КОПД, что позволило совершить действия, приведшие к нарушению условий конфиденциальности информации клиентов

Прямые потери:

- Штрафные санкции со стороны пострадавших клиентов;

Тип угрозы *

Преднамеренный

Агент угрозы *

Группа хакеров

Векторы атак и события угроз *

[+ Добавить вектор атаки](#)

Нет данных

Добавление вектора атаки и событий угроз

Вектор атаки

Фиджит

События угроз

ID события угрозы	Наименование событий угрозы	Описание событий угрозы
ADV002	Несанкционированный доступ к легитимным учетным данным	Злоумышленник получает несанкционированный доступ к легитимным учетным данным аутентификации и использует их для получения доступа к информационным системам организации. Рекомендации по оценке: Информация для аутентификации может быть получена различными способами, включая: - утечку информации для аутентификации; - небезопасное хранение информации для аутентификации; - проведение атак методами перебора/управления паролей; Это событие угрозы может комбинироваться с использованием уязвимостей, таких как: - эксплуатация незашифрованной или слабо зашифрованной информации; - выявление «слабых» паролей, используемых. Злоумышленники внедряют вредоносное программное обеспечение в информационные системы организации. Рекомендации по оценке: На более низком уровне злоумышленник, вероятно, будет использовать относительно простые методы для разработки вредоносного ПО (например, используя общедоступные наборы для разработки вредоносного ПО или существующие вредоносные ПО, наряду с распространяемыми уязвимостями) и доставки вредоносного ПО (например, через использование электронной почты и социальных сетей). На более высоком уровне злоумышленник с большой вероятностью будет использовать ряд сложных методов, чтобы: - разработать вредоносное ПО (например, создавая специально написанное вредоносное ПО с использованием небинарных данных или «zero-day» уязвимостей); - доставить вредоносное ПО (например, нацеливаясь на конкретных ключевых лиц через их личные мобильные устройства, побуждая их посетить зараженные веб-сайты или заражая портативные устройства хранения данных, которые они могут использовать); - создать вредоносное ПО (например, используя руткиты или методы противодействия компьютерной криминалистике). Злоумышленник использует неправильно сконфигурированные информационные системы (т.е. системы, сконфигурированные не в соответствии со стандартами безопасности или организационными требованиями к сбору) для получения несанкционированного доступа. Рекомендации по оценке: Это событие угрозы может затронуть все типы информационных систем организации, включая:
ADV007	Проникновение вредоносной программы в информационные системы	

[Отменить](#) [Сохранить](#)



Исходные данные (сценарии реализации рисков) 3/3

Добавьте описание наилучшего и наихудшего случая реализации риска

1

После внесения всех данных отмените или сохраните изменения нажатием соответствующих кнопок

2

При нажатии открывается подробная инструкция

3

Сценарии реализации рисков > Создание сценария реализации риска

Создание сценария реализации риска

Описание Расчет ущерба

Наилучший случай

Описание

Добавьте описание

Формула расчета

Укажите число или введите формулу расчета ущерба

Ущерб

— P

Наихудший случай

Описание

Добавьте описание

Формула расчета

Укажите число или введите формулу расчета ущерба

Ущерб

— P

Отменить Сохранить ?

2

3

Параметры для расчета ущерба

Параметры

Добавить Или Создать новый

ID Название параметра Значение

Нет строк

Параметры для расчета ущерба

П2 - ИС 1 Годовая валовая выручка Компании

Добавить Или Создать новый

ID Название параметра Значение

П1 ИС 1 Средний размер годовой выручки с одним клиентом 200 000 000

П4 ИС 1 Маркетинговый бюджет Технологии Доверия в случае необходимости создания положительной новости в СМИ

Редактировать имя и значение

Скрыть параметр

6

Внесите параметры из списка ранее заготовленных и/или добавьте новые

5

Добавьте формулы расчета ущерба используя настоящую подсказку и ID добавленных параметров (П1, П2, П3 и т. д.)

4

Укажите число или введите формулу расчета ущерба с использованием цифр, параметров и математических символов:
+ сложение, - вычитание, * умножение, / деление, ^ возведение в степень,
log₂(x) логарифм икс по основанию 2, ln(x) логарифм икс по натуральному основанию e, lg(x) логарифм икс по основанию 10, () скобки для приоритетизации операций, Px ID параметра, где x - номер параметра

4

Скройте или отредактируйте добавленные параметры

6



Исходные данные (инициативы) 1/2

Для упрощенной навигации используйте поисковую строку

1

В реестре инициатив можно отслеживать статус инициатив, а также менять его на актуальный

2

Для добавления новой инициативы нажмите кнопку «Добавить инициативу» (см. слайд 16)

3

Добавленные инициативы можно редактировать, удалять и просматривать детальное описание

4

При нажатии открывается подробная инструкция

5

Инициативы

1

3 [Добавить инициативу](#)

Текущий статус	Название инициативы	Описание инициативы	Владелец	Уровень приоритета	Контроли	Стоимость, Р	Дата начала	Дата окончания	
В процессе	ИНЦ001 Выявление следов компрометации в IT-инфраструктуре	Выявление следов компрометации в IT-инфраструктуре	Миронов А.Г.	Средний	17,8 Проводить разбор и анализ решенных инцидентов	4 800 000	02.06.2025	22.09.2025	⋮
В процессе	ИНЦ002 Внедрение средства защиты контейнеризации	Внедрение средства защиты контейнеризации	Миронов А.Г.	Средний	7,4 Применить автоматическое управление патчами прикладного программного обеспечения 4,1 Настроить и поддерживать процесс настройки безопасности для программного обеспечения и	7 708 680	23.06.2025	13.10.2025	⋮
В процессе	ИНЦ003 Внедрение средств безопасной разработки	Внедрение средств безопасной разработки	Миронов А.Г.	Высокий	16,2 Настроить и поддерживать процесс обнаружения и устранения уязвимостей в программном обеспечении 16,6 Создать и поддерживать классификацию уязвимостей	6 760 000	16.06.2025	22.09.2025	⋮
В процессе	ИНЦ004 Тренинги по безопасной разработке для разработчиков и ИБ команды	Тренинги по безопасной разработке для наших разработчиков и ИБ команды	Миронов А.Г.	Средний	16,9 Обучить разработчиков практикам безопасной разработки программного обеспечения	5 000 000	21.04.2025	28.04.2025	⋮
Запланир...	ИНЦ005 Киберучения для команды ИБ	Киберучения для команды ИБ	Миронов А.Г.	Средний	17,7 Проводить регулярные учения по решению инцидентов безопасности 14,9 Провести направленные тренинги по информационной безопасности в соответствии с	10 000 000	04.04.2025	16.04.2025	⋮
Запланир...	ИНЦ 006 Внедрение MDM	Внедрение MDM	Миронов А.Г.	Средний	4,12 Создать выделенные рабочие пространства на мобильных устройствах пользователей 4,11 Внедрить возможность удаленной очистки корпоративных данных на	50 000 000	02.04.2025	04.04.2025	⋮
В процессе	ИНЦ007 Внедрение модуля для DLP	Внедрение модуля для DLP	Миронов А.Г.	Высокий	3,2 Создать и поддерживать реестр для учета данных 3,14 Вести журнал доступа к конфиденциальным данным 3,7 Создать и поддерживать систему классификации данных	18 500 000	05.04.2025	10.04.2025	⋮
Выполнена	ИНЦ 008 Внедрение NAD	Внедрение NAD	Миронов А.Г.	Средний	13,6 Собрать журналы потоков сетевого трафика	20 000 000	12.04.2025	24.04.2025	⋮

4 [Показать детали](#)
[Редактировать](#)
[Удалить](#)



Исходные данные (инициативы) 2/2

Заполните текстовые поля «Названия инициативы» и «Описание инициативы»

1

Установите даты начала внедрения инициативы, запланированную дату окончания и уровень приоритета

2

Установите стоимость внедрения инициативы и сотрудника ответственного за внедрение инициативы

3

Выберите контроли из списка, на которые будет влиять настоящая инициатива

4

Инициативы > Создание инициативы

Создание инициативы

Название инициативы *

Пример названия: Внедрение EDR/XDR решения и применение политик для различных систем и групп пользователей

Описание инициативы

Пример описания:
Внедрить EDR/XDR решение для мониторинга Mission-critical и Business-critical и административных систем.
Разработать и применить политики EDR/XDR для различных систем и групп пользователей

1

2

3

4

Дата начала * Планируемая дата окончания * Уровень приоритета

Стоимость # * Владелец

Влияние на контрольную среду *

Выбор контролей

Найти контроль

ID	Область контролей	NIST CSF v2.0	Применимая группа	Описание контроля
<input checked="" type="checkbox"/>	1,1	Идентификация	Базовый	Создать и поддерживать точную, детально и обновляемую инвентаризацию всех активов предприятия, которые потенциально могут хранить или обрабатывать данные, включая устройства конечных пользователей (включая портативные и мобильные), сетевые устройства, некомпьютерные устройства/устройства Интернета вещей и серверы. Убедитесь, что в инвентаризации записаны сетевой адрес (если он статический), IP-адрес, аппаратный адрес, имя компьютера, владелец ресурса данных, отдал для каждого ресурса и то, был ли ресурс одобрен для подключения к сети. Для мобильных устройств конечных пользователей инструменты типа MDM могут поддерживать этот процесс, где это уместно. Этот перечень включает активы, подключенные к инфраструктуре предприятия, физически, виртуально, удаленно, а также те, которые находятся в обычных средах. Кроме того, сюда входят активы, которые регулярно подключаются к сетевой инфраструктуре предприятия, даже если они не находятся под контролем предприятия. Пересматривайте и обновляйте инвентаризацию всех активов предприятия раз в два года или чаще.
<input checked="" type="checkbox"/>	1,2	Реагирование	Базовый	Убедитесь, что существует процесс еженедельной обработки несанкционированных ресурсов. Предприятие может выбрать удаление ресурса из сети, запретить удаленное подключение к сети или поместить ресурс в карантин.
<input type="checkbox"/>	1,3	Обнаружение	Дополнительный	Использовать инструмент активного обнаружения для идентификации активов, подключенных к корпоративной сети. Настройте средство активного обнаружения так, чтобы оно выполнялось еженедельно или чаще.
<input type="checkbox"/>	1,4	Идентификация	Дополнительный	Использовать протоколирование DNSP на всех серверах DNSP или средства управления адресами интернет-протокола (IP) для обновления инвентаризации активов предприятия. Просматривайте и используйте журналы для обновления инвентаризации активов предприятия еженедельно или чаще.
<input type="checkbox"/>	1,5	Обнаружение	Продвинутый	Использовать инструмент пассивного обнаружения для идентификации активов, подключенных к корпоративной сети. Просматривайте и используйте сканы для обновления инвентаризации активов предприятия, по крайней мере, еженедельно или чаще.
<input type="checkbox"/>	2,1	Идентификация	Базовый	Создать и поддерживать подробную инвентаризацию всего программного обеспечения, установленного на корпоративных активах. В инвентаризации программного обеспечения должны быть указаны название, издатель, дата первоначальной установки/использования и бизнес-цель каждой записи; при необходимости указывается унифицированный указатель ресурсов (URL, магазин) приложений, версий, механизм развертывания и дата снятия с эксплуатации. Пересматривайте и обновляйте реестр программного обеспечения раз в два года или чаще. Переведено с помощью DeepL.com (бесплатная версия)
<input type="checkbox"/>	2,2	Идентификация	Базовый	Убедитесь, что только поддерживаемое в данный момент программное обеспечение указано как авторизованное в реестре программного обеспечения для корпоративных активов. Если программное обеспечение не поддерживается, но необходимо для выполнения миссии предприятия, задокументируйте исключение с подробным описанием мер по смягчению последствий и принятию остаточного риска. Для любого неподдерживаемого программного обеспечения без документации об исключениях укажите как неавторизованное. Просматривайте список программного обеспечения, чтобы убедиться в поддержке программного обеспечения, по крайней мере, еженедельно или чаще.
<input type="checkbox"/>	2,3	Реагирование	Базовый	Убедитесь, что несанкционированное программное обеспечение либо удалено из использования на корпоративных ресурсах, либо получило документированное исключение. Просматривайте еженедельно или чаще.



Профиль риска ИБ 1/2

Фильтр по перцентилям (P10, P50, P90): позволяет анализировать потенциальные финансовые потери в разных сценариях вероятности.

1

Фильтр по категориям рисков ИБ: позволяет фильтровать информацию по ключевым категориям риска.

2

При изменении исходных данных необходимо заново провести расчеты

3



При нажатие открывается подробная инструкция

4

При нажатии позволяет настроить доверительный интервал и степень неопределенности для расчета Монте-Карло

5

Расчитать | ⚙️ | 🔄

3 | 5 | 4

Параметры расчёта

Доверительный интервал

Агенты угроз и контрольная среда

90% | 95.4% | 99.7%

Ущерб

90% | 95.4% | 99.7%

Степень неопределенности

5% | 10% | 15% | 20%

Отменить | Расчитать



Профиль риска ИБ 2/2

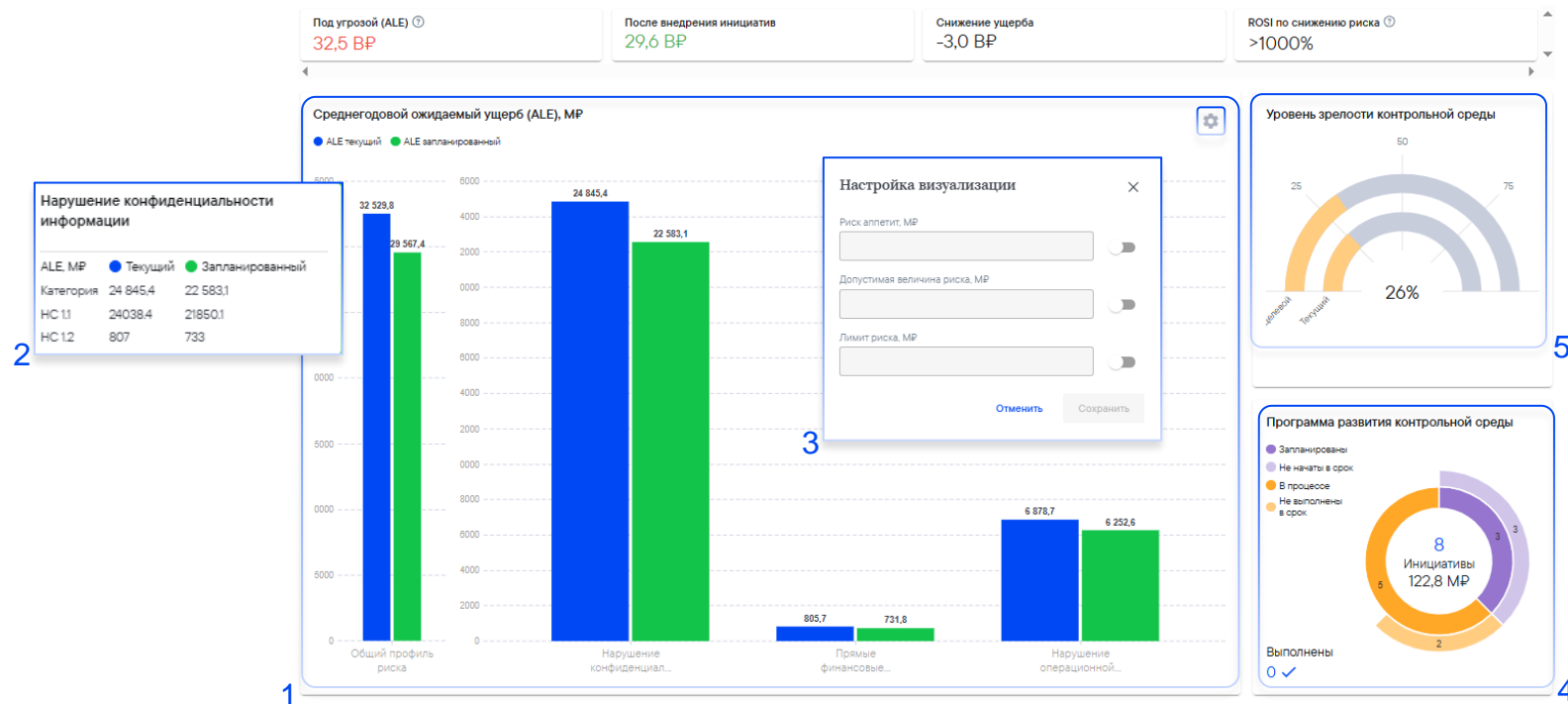
1 Визуализирует общий Среднегодовой ожидаемый ущерб (ALE) и по категориям рисков ИБ, а также отражает остаточный риск ИБ через прогнозируемое снижение средних ожидаемых годовых потерь благодаря реализации инициатив

2 При наведении курсора можно получить детальную информацию о финансовых потерях в рамках каждой категории риска и соответствующих недопустимых событиях, входящих в категорию

3 Позволяет настроить риск-аппетит, допустимую величину риска и лимит риска на диаграмме

4 Демонстрирует общую стоимость реализации и статус инициатив, направленных на улучшение контрольной среды

5 Демонстрирует текущий уровень зрелости контрольной среды Компании и целевой показатель по результатам внедрения инициатив





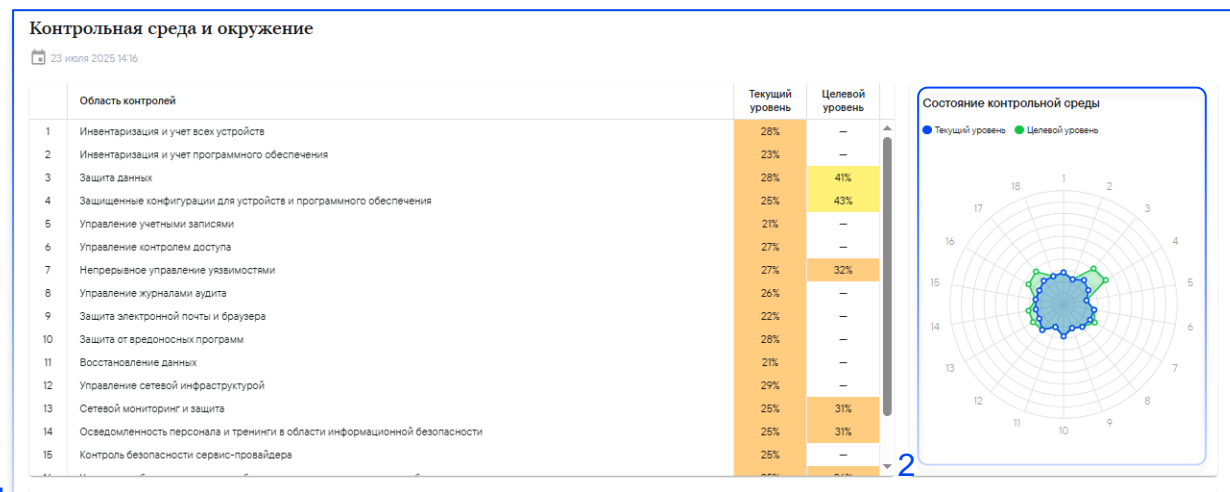
Профиль риска ИБ (контрольная среда и окружение) 1/2

Предоставляет текущий уровень реализации мер защиты для различных областей контрольной среды.

1

Демонстрирует состояние контрольной среды по ключевым областям контролей, что позволяет оценить разницу между текущим и целевым уровнем

2

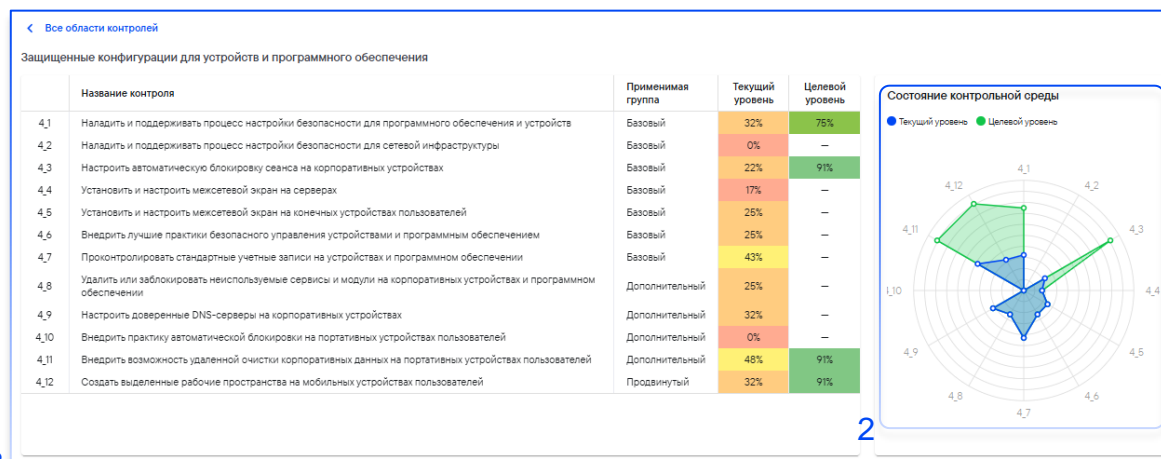


1

2

При выборе конкретной области позволяет увидеть детализацию по отдельным мерам/контролям

3



3

2



Профиль риска ИБ (контрольная среда и окружение) 2/2

Демонстрирует степень защищённости активов в отношении каждой из функций методологии. Эти данные позволяют оценить, насколько текущие меры соответствуют требованиям кибербезопасности на каждом этапе жизненного цикла угроз или противодействия угрозам. Если у актива отсутствует пересечения с функцией NIST CSF, значение указывается как "N/A"

1

Тип актива	Функции обеспечения информационной безопасности					
	Управление	Идентификация	Реагирование	Обнаружение	Предотвращение	Восстановление
Устройства	N/A	26%	34%	25%	28%	N/A
Программное обеспечение	17%	31%	29%	40%	19%	N/A
Данные	26%	27%	N/A	26%	27%	24%
Документация	24%	N/A	N/A	N/A	N/A	N/A
Пользователи	28%	31%	26%	N/A	25%	33%
Сеть	N/A	N/A	N/A	32%	23%	N/A

1

Демонстрирует анализ потенциальных агентов угроз

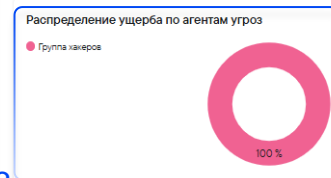
2

Демонстрирует распределение агентов угроз по их влиянию на общий ущерб от реализации рисков ИБ.

3

Оценка агентов угроз			
Агенты угроз	Вид агента угрозы	Возможность инициации атаки	Сила атаки
Преднамеренные			
Сотрудники (привилегированные)	Внутренний	67%	78%
Сотрудники (рядовые)	Внутренний	43%	32%
Группа хакеров	Внешний	88%	88%
Одиночный хакер	Внешний	56%	56%
Журналист-расследователь	Внешний	67%	46%
Иностранные государства	Внешний	88%	91%
Технологический поставщик / партнер (внутренний)	Внутренний	4%	4%
Технологический поставщик / партнер (внешний)	Внешний	22%	22%
Террористическая организация	Внешний	7%	7%
Конкурент	Внешний	22%	67%
Случайные			
Клиент	Внешний	30%	80%
Сотрудники (рядовые)	Внутренний	41%	41%
Сотрудники (привилегированные)	Внутренний	41%	10%
Технологический поставщик / партнер (внешний)	Внешний	20%	39%
Технологический поставщик / партнер (внутренний)	Внутренний	20%	20%

2



3



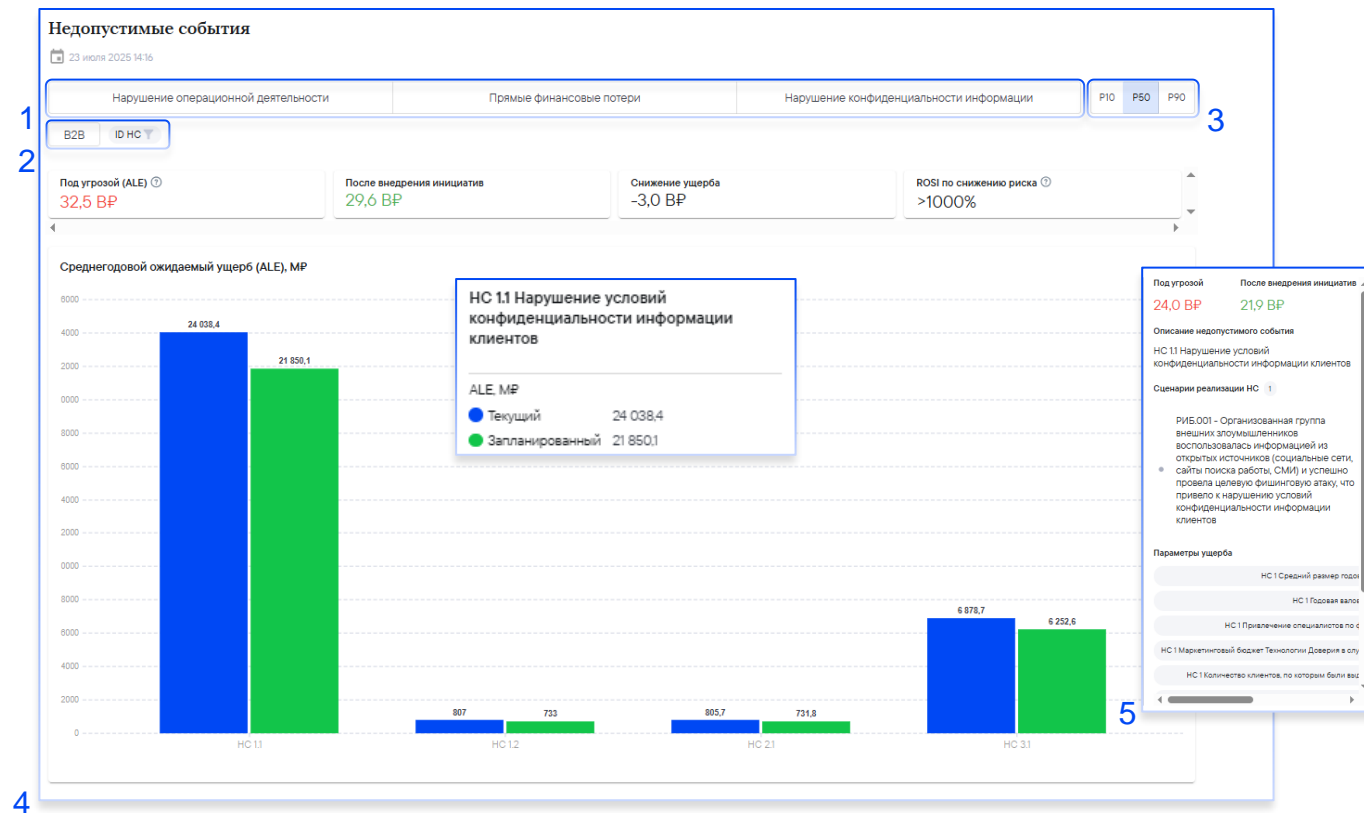
Профиль риска ИБ (недопустимые события)

1
Фильтр по категориям рисков ИБ позволяет фильтровать информацию по ключевым категориям риска.

2
Фильтры по сегментам бизнеса и по конкретным недопустимым событиям позволяют более детально рассмотреть информацию

3
Фильтр по перцентильям (P10, P50, P90) позволяет анализировать потенциальные финансовые потери в разных сценариях вероятности.

4
Распределение текущего и планируемого уровня ущерба (ALE) по недопустимым событиям



5
При нажатии на конкретное событие можно ознакомиться с его подробным описанием и увидеть, по каким параметрам он рассчитан



Профиль риска ИБ (сценарии реализации рисков)

Фильтр по перцентилям (P10, P50, P90) позволяет анализировать потенциальные финансовые потери в разных сценариях вероятности.

1

Фильтр по категориям рисков ИБ позволяет фильтровать информацию по ключевым категориям риска.

2

Фильтры по сегментам бизнеса, недопустимым событиям и агентам угроз позволяют более детально рассмотреть информацию

3

Детализированное описание всех зарегистрированных рисков ИБ компании, включая их значения и взаимосвязь с контрольными мерами

4

Сценарии реализации рисков

23 июля 2025 14:16

Нарушение операционной деятельности | Прямые финансовые потери | Нарушение конфиденциальности информации

P10 P50 P90

B2B ID ИС Агенты угроз

Под угрозой (ALE) 32,5 ВР | После внедрения инициатив 29,6 ВР | Снижение ущерба -3,0 ВР | ROSI по снижению риска >1000% | Стоимость улучшений 122,8 МР | Запланировано инициатив 8

Сценарий реализации риска	Принадлежность к ИС	Агент угрозы	ARO	SLE, P	ALE, P
РИБ.001 - Организованная группа внешних злоумышленников воспользовалась информацией из открытых источников (социальные сети, сайты поиска работы, СМИ) и успешно провела целевую фишинговую атаку, что привело к нарушению условий...	ИС 11 - B2B - Нарушение условий конфиденциальности информации клиентов	Группа хакеров	53%	44 957 157 550	24 038 375 484
РИБ.002 - Организованная группа внешних злоумышленников (APT, хактивисты) воспользовалась уязвимостями в ИС Компании, слабостями систем удаленного доступа Компании и смогла получить доступ в сеть КСПД, что позволило совершить действия приведшие к разглашению...	ИС 12 - B2B - Разглашение персональных данных сотрудников/клиентов	Группа хакеров	53%	1 508 948 358	
РИБ.003 - Организованная группа внешних злоумышленников (APT, хактивисты) воспользовалась уязвимостями в ИС Компании, слабостями систем удаленного доступа Компании и смогла получить доступ в сеть КСПД, что позволило совершить действия приведшие к подмене...	ИС 21 - B2B - Подмена платежных реквизитов крупных платёжных поручений или массовая подмена платежных реквизитов при переводах контрагентам или заработной платы работникам	Группа хакеров	53%	1 506 568 133	
РИБ.004 - Организованная группа внешних злоумышленников (APT, хактивисты) воспользовалась уязвимостями, связанными с использованием слабых/словесных паролей в системе подрядчика и смогла получить доступ в сеть КСПД Компании, что позволило соверши...	ИС 31 - B2B - Нарушение работоспособности систем и сервисов	Группа хакеров	53%	12 864 799 686	

4

При выборе конкретного риска пользователь может ознакомиться с дополнительной информацией по каждому риску

5

5

ARO SLE, P ALE, P

53% 44 957 157 550 24 038 375 484

Сила защиты 31%

Возможность инициации 88%

Сила атаки 88%

Описание недопустимого события

РИБ.001 - Организованная группа внешних злоумышленников воспользовалась информацией из открытых источников (социальные сети, сайты поиска работы, СМИ) и успешно провела целевую фишинговую атаку, что привело к нарушению условий конфиденциальности информации клиентов

Векторы атак / События угроз

Фишинг

- Несанкционированный доступ к легитимным учетным данным
- Проникновение вредоносной программы в информационную систему
- Эксплуатация уязвимостей в корпоративных информационных системах с ошибками в конфигурации
- Сбор общедоступной информации об организации
- Фишинг
- Механические манипуляции



Профиль риска ИБ (инициативы) 1/2

Фильтр по перцентилям (P10, P50, P90) позволяет анализировать потенциальные финансовые потери в разных сценариях вероятности.

1

Фильтр по категориям рисков ИБ позволяет фильтровать информацию по ключевым категориям риска.

2

Фильтры по сегментам бизнеса и статусу позволяют более детально рассмотреть информацию

3

Демонстрирует общую стоимость реализации и статус инициатив, направленных на улучшение контрольной среды

4

Демонстрирует изменение затрат на инициативы и ожидаемого ущерба по мере их внедрения

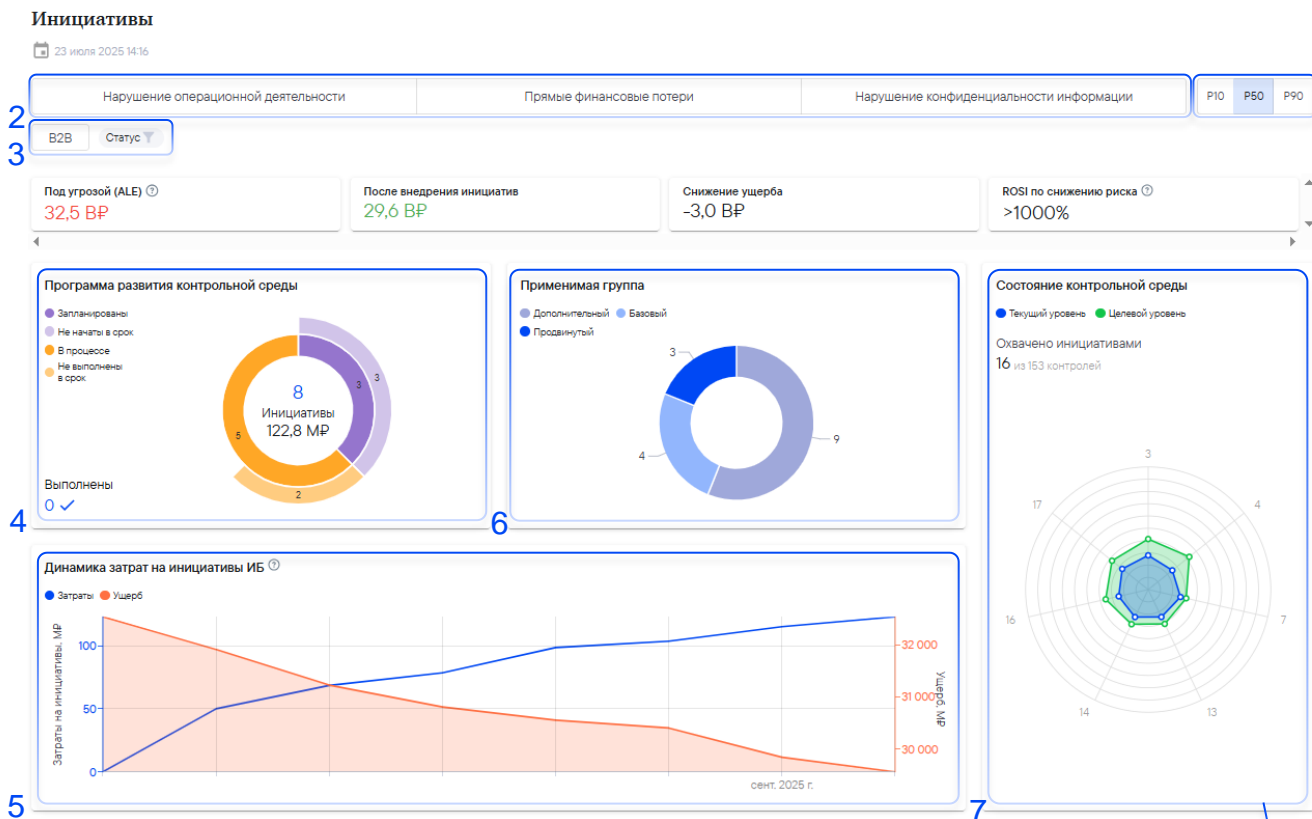
5

Демонстрирует распределение инициатив по контролям по их применимой группе

6

Демонстрирует состояние контрольной среды по ключевым областям контролей, что позволяет оценить разницу между текущим и целевым уровнем

7





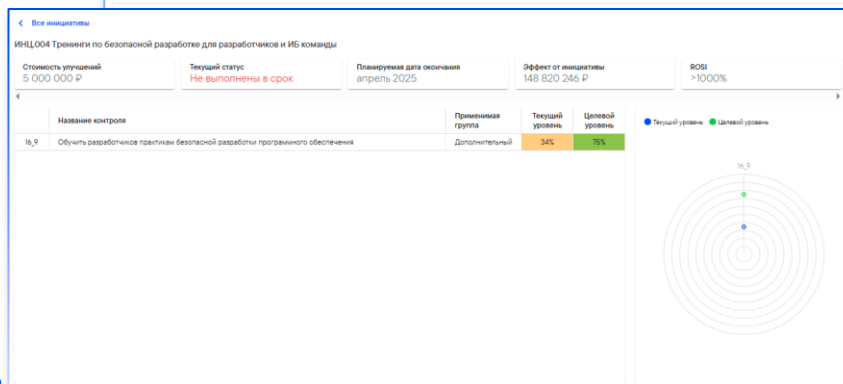
Профиль риска ИБ (инициативы) 2/2

1 Содержит подробную информацию о каждой активной инициативе, включая «Срок окончания», «Эффективность от внедрения» в процентах и «ROSI». Данные инициативы идут в расчет целевого состояния

2 При нажатии на конкретную инициативу открывается подробная информация и зависимые компоненты

3 Содержит подробную информацию о каждой активной инициативе, включая «Срок окончания», «Эффективность от внедрения» в процентах и «ROSI». Данные инициативы идут в расчет целевого состояния

Активные инициативы					
Название инициативы	Стоимость, Р	Текущий статус	Планируемая дата окончания инициативы	Эффект от инициативы, Р ?	ROSI
ИНЦ.001 Выявление следов компрометации в IT-инфраструктуре	4 800 000	В процессе	сентябрь 2025	148 602 284	>1000%
ИНЦ.002 Внедрение средства защиты контейнеризации	7 708 680	В процессе	октябрь 2025	278 485 557	>1000%
ИНЦ.003 Внедрение средств безопасной разработки	6 760 000	В процессе	сентябрь 2025	411 280 936	>1000%
ИНЦ.004 Тренинги по безопасной разработке для разработчиков и ИБ команды	5 000 000	Не выполнена в срок	апрель 2025	148 820 246	>1000%
ИНЦ.005 Киберучения для команды ИБ	10 000 000	Не начата в срок	апрель 2025	417 014 773	>1000%
	50 000 000	Не начата в срок	апрель 2025	621 996 803	>1000%
	18 500 000	Не выполнена в срок	апрель 2025	682 770 943	>1000%
	20 000 000	Не начата в срок	апрель 2025	253 406 295	>1000%



3

Выполненные инициативы	
Инициативы не определены	



Технологии Доверия

Аналитика и комментарии
экспертов в телеграм-канале
https://t.me/tedo_business



tedo.ru

Компания «Технологии Доверия» (www.tedo.ru) предоставляет аудиторские и консультационные услуги компаниям разных отраслей. В офисах «Технологий Доверия» в Москве, Санкт-Петербурге, Екатеринбурге, Казани, Новосибирске, Ростове-на-Дону, Краснодаре, Воронеже и Нижнем Новгороде работают 3 000 специалистов. Мы помогаем нашим клиентам выстраивать и укреплять доверие к бизнесу благодаря нашему опыту и качеству оказываемых услуг.

© 2025 «Технологии Доверия». Все права защищены.