

НЕДОПУСТИМОЕ СОБЫТИЕ 2025

ЦИФРОВОЙ **КРАШ-ТЕСТ**
РОССИЙСКОГО БИЗНЕСА

Исследование на базе данных
«Кибериспытание Экспресс» на 15 июля 2025 г.

«УЯЗВИМОСТЬ СЕЙЧАС — НЕ ИСКЛЮЧЕНИЕ, А НОРМА»

Сегодня цифровой мир устроен так, что уязвимость — это не исключение, а норма. Нет системы, которую невозможно взломать. Нет бизнеса, полностью защищённого от инцидента. В условиях, где 100% гарантии не может дать никто, самое разумное — не отрицать риски, а уметь с ними работать.

«Кибериспытание Экспресс» стал первым в России масштабным краш-тестом киберустойчивости бизнеса. Проект создан, чтобы в открытом формате проверить, можно ли реализовать критические сценарии, которые сами компании называют недопустимыми. Мы проверили десятки организаций в разных отраслях и с разным уровнем зрелости. И почти в каждом случае исследователи находили путь к реализации тех самых недопустимых событий, которых мы все боимся.

Мы не ставили цель поймать кого-то на ошибке. Мы хотели дать объективный взгляд на ситуацию — без формальностей, без самоуспокоения. Важно понимать: это не провал. Это диагноз. Честный и своевременный. И пока одни боятся признать проблему, другие получают шанс её исправить.

Благодарю всех участников проекта за смелость и доверие! Это показатель зрелости — готовность увидеть слабое место и начать действовать.

Надеюсь, этот отчет станет не просто срезом текущего состояния, а поводом для роста и переосмысления. Наша цель — не искать виноватых, а сделать недопустимое невозможным.

**НАТАЛЬЯ
ВОЕВОДИНА**

Генеральный директор
АО «Кибериспытание»,
партнёр Сайберус



СОДЕРЖАНИЕ

4	Кибериспытание Экспресс
5	Основа исследования и гипотезы
6	Ключевые цифры
7	Ключевые выводы
8	Участники, недопустимые события и сводка по отраслям
16	Векторы атак и уязвимости
20	Ценность, исходя из потенциального ущерба при реальных атаках
26	Методология КИ, исследователи и вознаграждение
34	Примеры реализованных недопустимых событий
38	История киберустойчивой компании
42	Наши рекомендации
44	Организаторы исследования

КИБЕРИСПЫТАНИЕ ЭКСПРЕСС

УСКОРЕННЫЙ И УПРОЩЕННЫЙ ФОРМАТ БЫСТРОЙ ПРОВЕРКИ ТЕКУЩЕГО СОСТОЯНИЯ

17 ноября 2024 года мы запустили грантовый фонд в 100 млн рублей, чтобы дать возможность разным компаниям бесплатно узнать свой реальный уровень кибезащиты, а нам проверить множество гипотез на большой выборке компаний.

Кибериспытание каждой компании длится 3 месяца. В течение этого времени независимые исследователи демонстрируют возможность реализовать недопустимое событие* (НС). Тип недопустимого события определяет сама компания из установленного перечня:

доступ к чувствительным данным

кража денежных средств

остановка производства

взлом аккаунта первого лица

шифрование ключевой базы данных

остановка продаж

Участники КИ Экспресс выбирают одно недопустимое событие, исследователи пытаются его реализовать.

КИБЕРИСПЫТАНИЕ ЭКСПРЕСС ДАЕТ ОТВЕТ НА ВОПРОС:

МОЖНО ЛИ ВЗЛОМАТЬ ВАШ БИЗНЕС ЗА 1 МЛН ₽?

найти сценарий, способный нанести бизнесу критический ущерб

силами белых хакеров

по методике кибериспытаний

* Недопустимое событие (НС) — одно или несколько событий, которые могут оказать критическое влияние на деятельность компании, ее руководство, клиентов и партнеров.

ОСНОВА ИССЛЕДОВАНИЯ — РЕЗУЛЬТАТЫ КИБЕРИСПЫТАНИЯ ЭКСПРЕСС ЗА ПОЛГОДА

Большинство испытаний уже завершены. И хотя часть компаний продолжают участие в КИ Экспресс, текущие данные уже можно использовать для общей оценки уровня защищенности российского бизнеса и принятия необходимых мер.

МЫ ПРОВЕРИЛИ 6 ГИПОТЕЗ

В рамках проекта мы стремились проверить готовность рынка к новому формату оценки киберустойчивости

Является ли кибериспытание эффективным методом проверки защищенности?

01

Действительно ли неограниченное количество исследователей может имитировать атаки, максимально приближенные к реальным условиям?

Какой будет конверсия во взлом?

02

Сколько кибериспытаний завершится демонстрацией возможности реализации НС при фиксированных сроках и бюджете?

Готов ли бизнес вовлекаться в кибербезопасность всерьёз?

03

Будут ли участвовать CEO и владельцы бизнеса как прямые заказчики проверки?

Готовы ли к этому CISO и ИТ-директора?

04

Классические инструменты оценки, такие как пентест, предполагают больший уровень контроля со стороны службы ИБ. Станут ли они запускать такие проверки без ограничений и страхов?

Способны ли белые хакеры показать возможность реализации НС?

05

Достаточно ли их компетенций, чтобы найти сценарий, приводящий к критически значимому результату?

Сколько исследователей готовы работать по нашей методике?

06

Каков их потенциал при данной методике?

КЛЮЧЕВЫЕ ЦИФРЫ

> 1 500 БЕЛЫХ ХАКЕРОВ В ТЕЧЕНИЕ 7 МЕСЯЦЕВ

проверяли защищенность 74 компаний
разного масштаба из разных отраслей*

3 ИЗ 5 КОМПАНИЙ УДАЛОСЬ ВЗЛОМАТЬ**

67%

были взломаны
простыми атаками

34 МИНУТЫ

самый
быстрый взлом

* Для участия в исследовании было отобрано 105 компаний, 74 из которых уже завершили КИ.

** В исследовании под взломом подразумевается реализация критического риска, т.е. выбранного компанией недопустимого события.

КЛЮЧЕВЫЕ ВЫВОДЫ

РЕАЛЬНАЯ ЗАЩИЩЕННОСТЬ — В 3 РАЗА НИЖЕ ОЖИДАНИЙ

Даже компании, уверенные в уровне своей защиты и регулярно проверяющие периметр, были взломаны с минимальным вознаграждением. Атаки шли по неожиданным векторам - через инфраструктуру, которая не находилась под контролем отдела ИБ (shadow infrastructure), с применением социальной инженерии или за счет неожиданной эксплуатации мелких ошибок.

ДЛЯ ОБЕСПЕЧЕНИЯ ПОЛНОТЫ ИССЛЕДОВАНИЯ ВАЖНО МНОЖЕСТВО УЧАСТНИКОВ

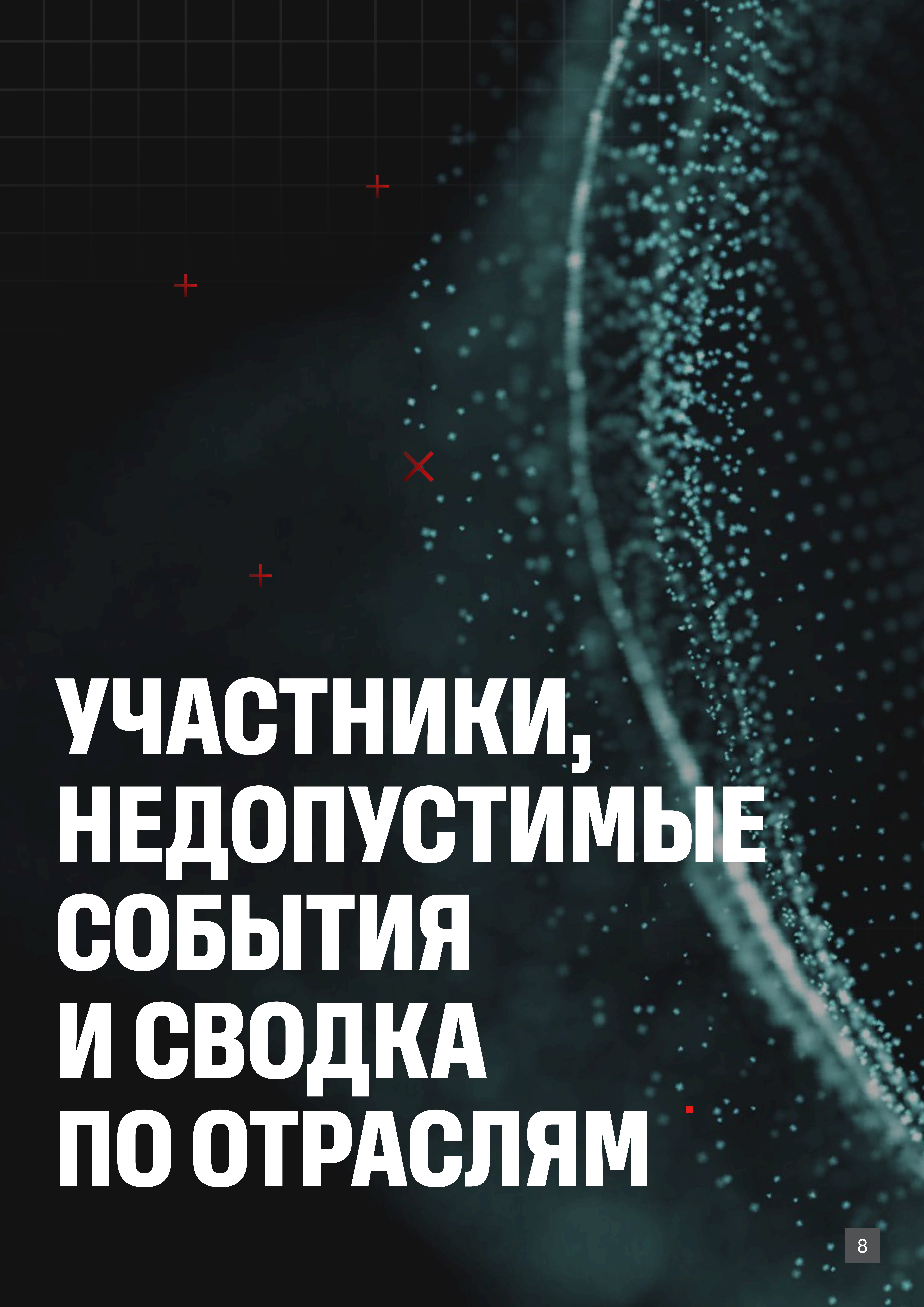
Одному и тому же исследователю не всегда стабильно удастся найти уязвимости во всех компаниях — это творческий процесс. В результате вознаграждение за 45 кейсов распределились между 26 исследователями с разным рейтингом, опытом и используемыми подходами/инструментами.

ВАЖНА ДЛИТЕЛЬНОСТЬ ИССЛЕДОВАНИЯ — НЕ МЕНЕЕ ТРЕХ МЕСЯЦЕВ, А ЛУЧШЕ НЕПРЕРЫВНО

Реализация недопустимого события в ряде компаний заняли два месяца и более. С учетом сезонной загрузки исследователей и необходимости в увеличении количества участников, важно обеспечить достаточный срок на развитие атак.

КОМАНДЫ КОМПАНИЙ ОКАЗАЛИСЬ НЕ ГОТОВЫ К РЕАЛЬНЫМ АТАКАМ

В большинстве случаев противодействие атакам со стороны ИБ и ИТ было минимальным или отсутствовало вовсе. Причем успешное противодействие не зависело от масштаба бизнеса, а определялось компетенциями и вовлеченностью команды. Сотрудники компаний оказались совершенно не готовы к социальной инженерии.



УЧАСТНИКИ, НЕДОПУСТИМЫЕ СОБЫТИЯ И СВОДКА ПО ОТРАСЛЯМ

УЧАСТНИКИ — 105 КОМПАНИЙ ИЗ 9 ОТРАСЛЕЙ ЭКОНОМИКИ

Из 1 000+ заявок мы отобрали первых 105 участников, среди которых компании из 9 отраслей российской экономики с разным масштабом бизнеса. Многие из них входят в цепочки поставок крупных предприятий по всей экономике.



> 50% УЧАСТНИКОВ ПРОЕКТА — КОМПАНИИ ИЗ ОТРАСЛИ ИНФОРМАЦИЯ И СВЯЗЬ, КОТОРАЯ ОКАЗАЛАСЬ НАИБОЛЕЕ ГИБКОЙ И БЫСТРОЙ В ПРИНЯТИИ РЕШЕНИЙ

* В рамках исследования мы не рассматривали отдельно отрасли, доля участия которых составила < 5%. Подробнее в «Методологии».

ИНИЦИАТОРЫ КИ — СЕО И РУКОВОДИТЕЛИ ИБ/ИТ ОТДЕЛОВ

Кибериспытания стали понятным методом оценки защищенности для высшего руководства компаний. У 51% компаний инициатором выхода на испытания были генеральный директор и/или акционеры.

В 49% случаев участие в проекте отстаивали руководители блока ИТ / ИБ / Цифровизации, которые оценили технические особенности проекта — сочетание преимуществ редтиминга, пентестов и багбаунти.



**КИБЕРИСПЫТАНИЯ ЗАИНТЕРЕСОВАЛИ И ПРОФИЛЬНЫХ
РУКОВОДИТЕЛЕЙ, И ВЫСШЕЕ РУКОВОДСТВО КОМПАНИЙ**

80% ВЫБРАННЫХ НС СВЯЗАНЫ С ЗАЩИТОЙ ДАННЫХ

Результаты исследования подтверждают высокий интерес бизнеса к двум типам недопустимых событий – шифрованию данных, а также их краже. Их выбрали 80% компаний.

Наименее актуальным НС является доступ к аккаунту руководителя.



54% КОМПАНИЙ СЧИТАЮТ НЕДОПУСТИМЫМИ СОБЫТИЯ, СВЯЗАННЫЕ С ОСТАНОВКОЙ БИЗНЕС-ПРОЦЕССОВ

ВЫБОР ИС ПО ОТРАСЛИ*

Шифрование баз данных сочли наиболее критичным большинство компаний из отраслей «Информация и связь» и «Обрабатывающие производства». А компании из финансовой сферы чаще выбирали в качестве ИС кражу данных.

Практически для всех индустрий доступ к аккаунту руководителя стал наименее популярным вариантом выбора. Естественным образом, остановка продаж/производства наиболее актуальна для компаний, занимающихся торговлей (44% компаний).



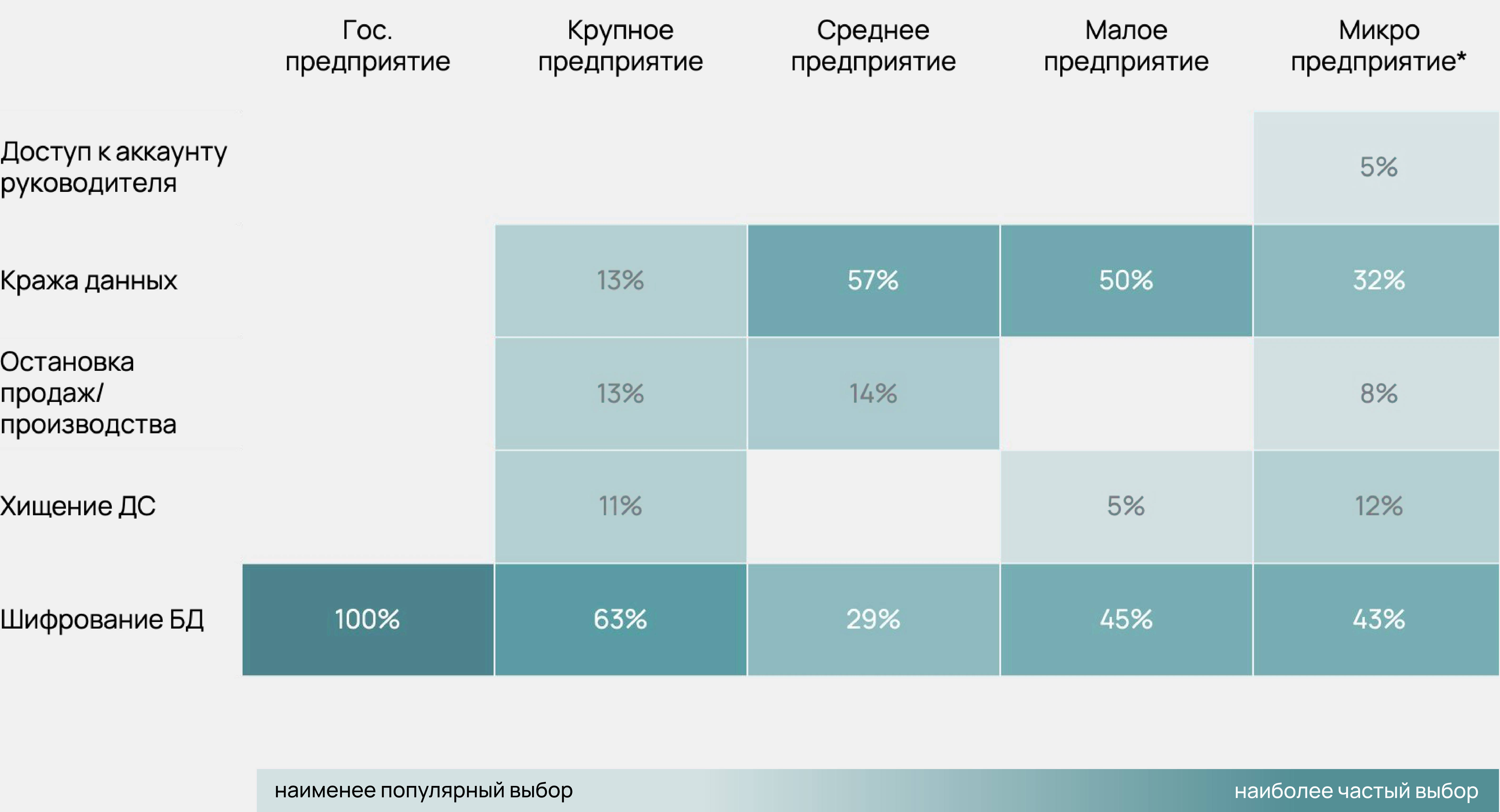
* Анализ по 5 отраслям, без учета отраслей с долей участия < 5%.
Подробнее в разделе «Методология»

12

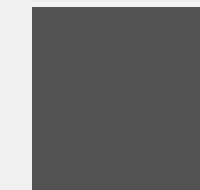
ВЫБОР ИС ОТНОСИТЕЛЬНО МАСШТАБА БИЗНЕСА

Бизнес видит возросшую роль данных (даже по сравнению с денежными средствами), поэтому ИС, связанные с данными, чаще всего выбирались для испытаний.

При этом крупные организации видят больший риск в шифровании данных, а средние — скорее в их краже.

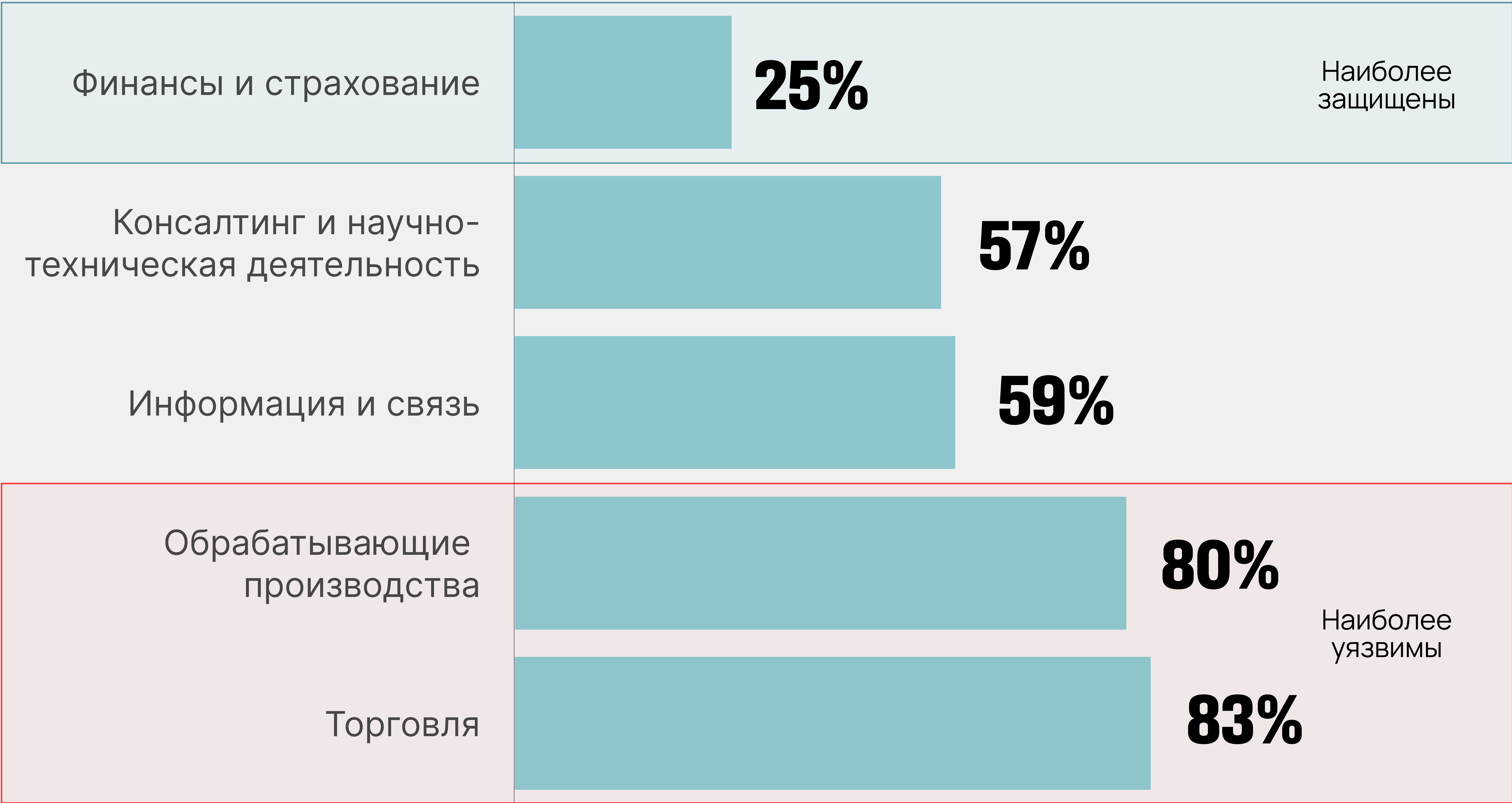


63% КРУПНЫХ КОМПАНИЙ ВЫБРАЛИ В КАЧЕСТВЕ НЕДОПУСТИМОГО СОБЫТИЯ ШИФРОВАНИЕ БАЗ ДАННЫХ



ОБРАБАТЫВАЮЩИЕ ПРОИЗВОДСТВА И ТОРГОВЛЯ **НАИБОЛЕЕ УЯЗВИМЫ**

Все представленные отрасли российской экономики достаточно уязвимы. По мере цифровизации и проникновения технологий риски будут возрастать.

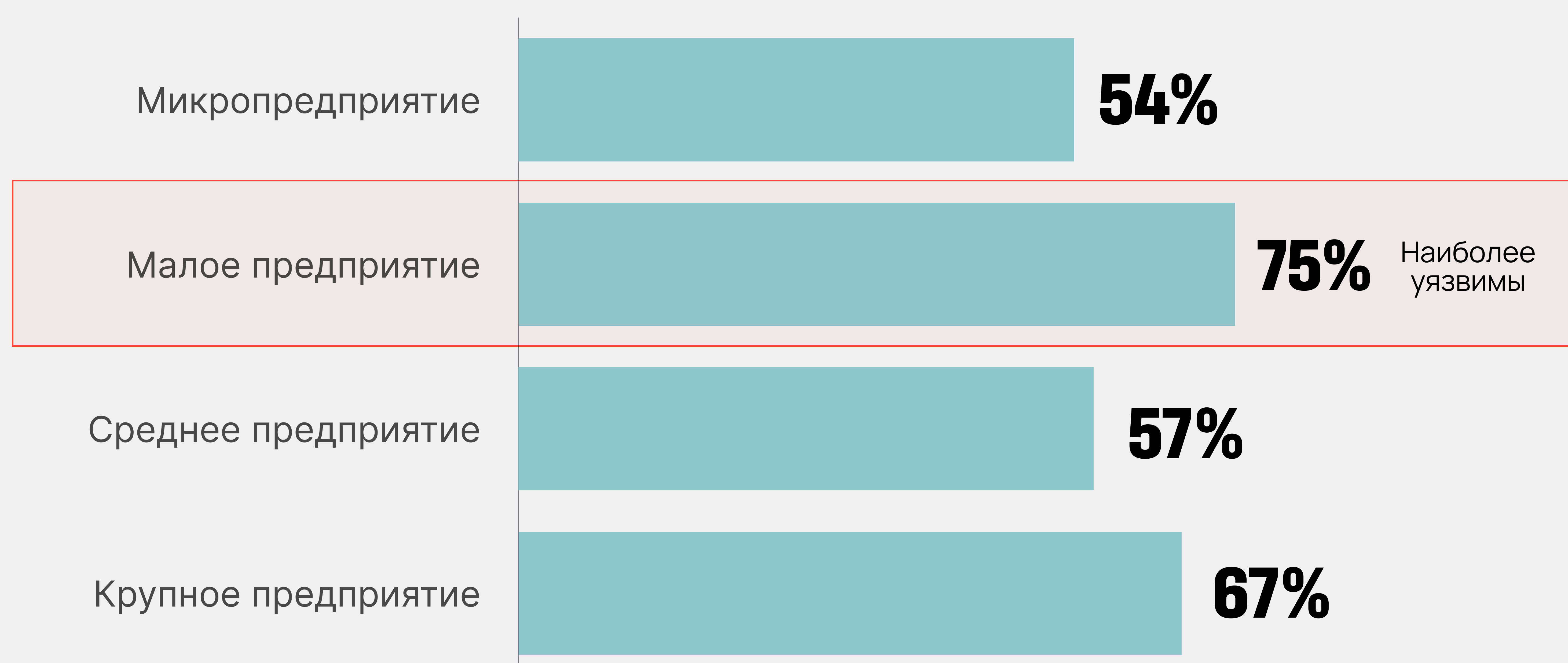


ПО 4 ИЗ 5 ОТРАСЛЕЙ ДОЛЯ ВЗЛОМОВ ОКАЗАЛАСЬ > 50%

НАИБОЛЬШИЙ ПРОЦЕНТ ВЗЛОМА — У МАЛЫХ ПРЕДПРИЯТИЙ

По всем типам предприятий доля взломов оказалось >50%.
Наибольший процент взлома (75%) — у малых предприятий,
которые активно используют цифровые технологии, но могут
уделять недостаточно внимания кибербезопасности.

У микропредприятий уровень реализации НС оказался ниже, что
может объясняться меньшим уровнем цифровизации или работой
на сервисах B2B, предоставляемых третьими сторонами, такими
как Яндекс, 1С и другие.

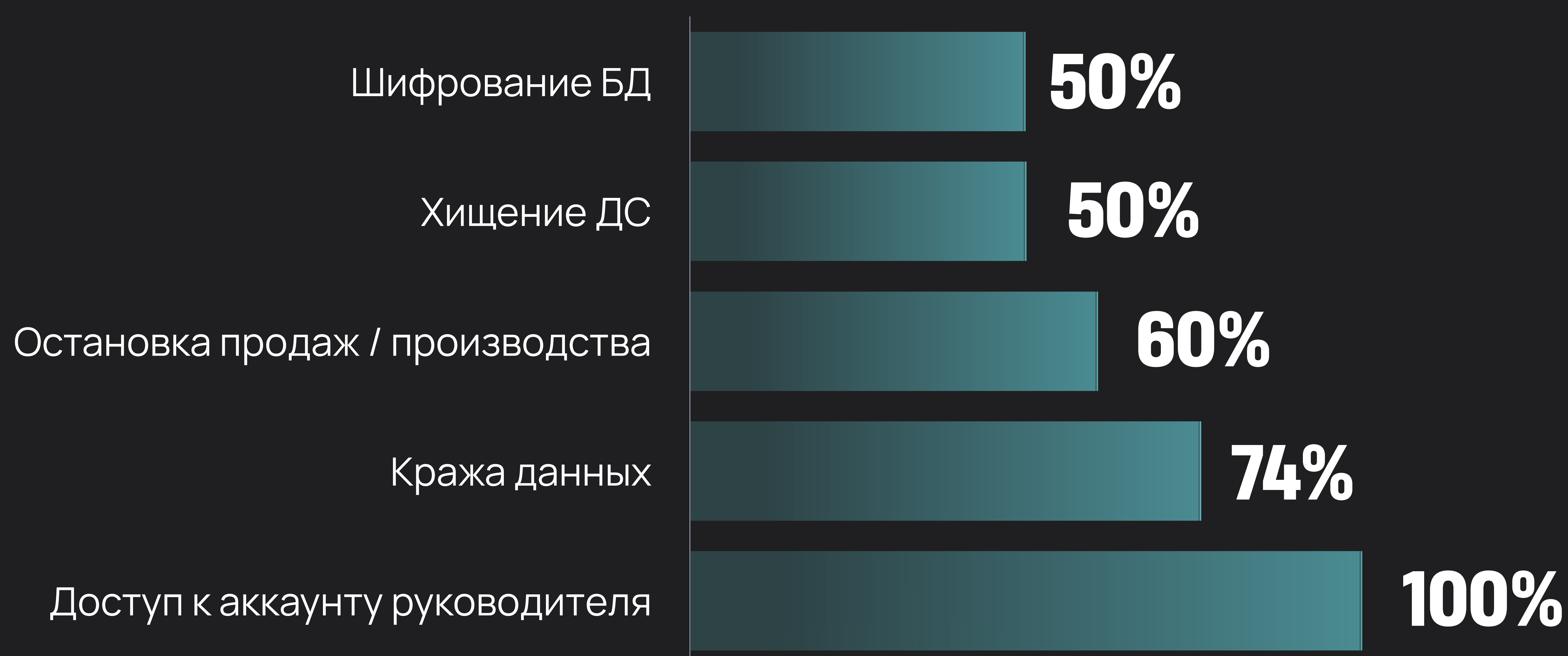


The background is a dark, textured surface. A faint grid is visible in the upper left. A glowing blue line, composed of many small dots, curves from the top right towards the bottom right. Several red markers are scattered: two plus signs (+) and one cross (X).

ВЕКТОРЫ АТАК И УЯЗВИМОСТИ

ПО ВСЕМ ГРУППАМ НС, КАК МИНИМУМ В ПОЛОВИНЕ СЛУЧАЕВ, ИССЛЕДОВАТЕЛИ ПРОДЕМОНСТРИРОВАЛИ ВОЗМОЖНОСТЬ РЕАЛИЗАЦИИ НЕДОПУСТИМОГО СОБЫТИЯ

Процент взлома
по типу недопустимых событий



Хотя хищение денежных средств в качестве НС выбрали только 6% участников, атаки по этому направлению были не менее успешны, чем, например, по шифрованию данных. А доступ к аккаунту руководителя был получен во всех компаниях, которые выбрали данный тип НС.

ИССЛЕДОВАТЕЛИ «АТАКОВАЛИ» ЧАЩЕ ВСЕГО ПО **4 ВЕКТОРАМ**

Самым популярным вектором реализованных атак стала эксплуатация уязвимостей на периметре компаний. Многие исследователи также выбрали векторы, связанные с уязвимостью веб-приложений и использовали данные из ранее допущенных бизнесом утечек.

Реже всего в сценариях реализации НС используются инструменты социальной инженерии: хакерам чаще всего было достаточно использовать простые сценарии атак.

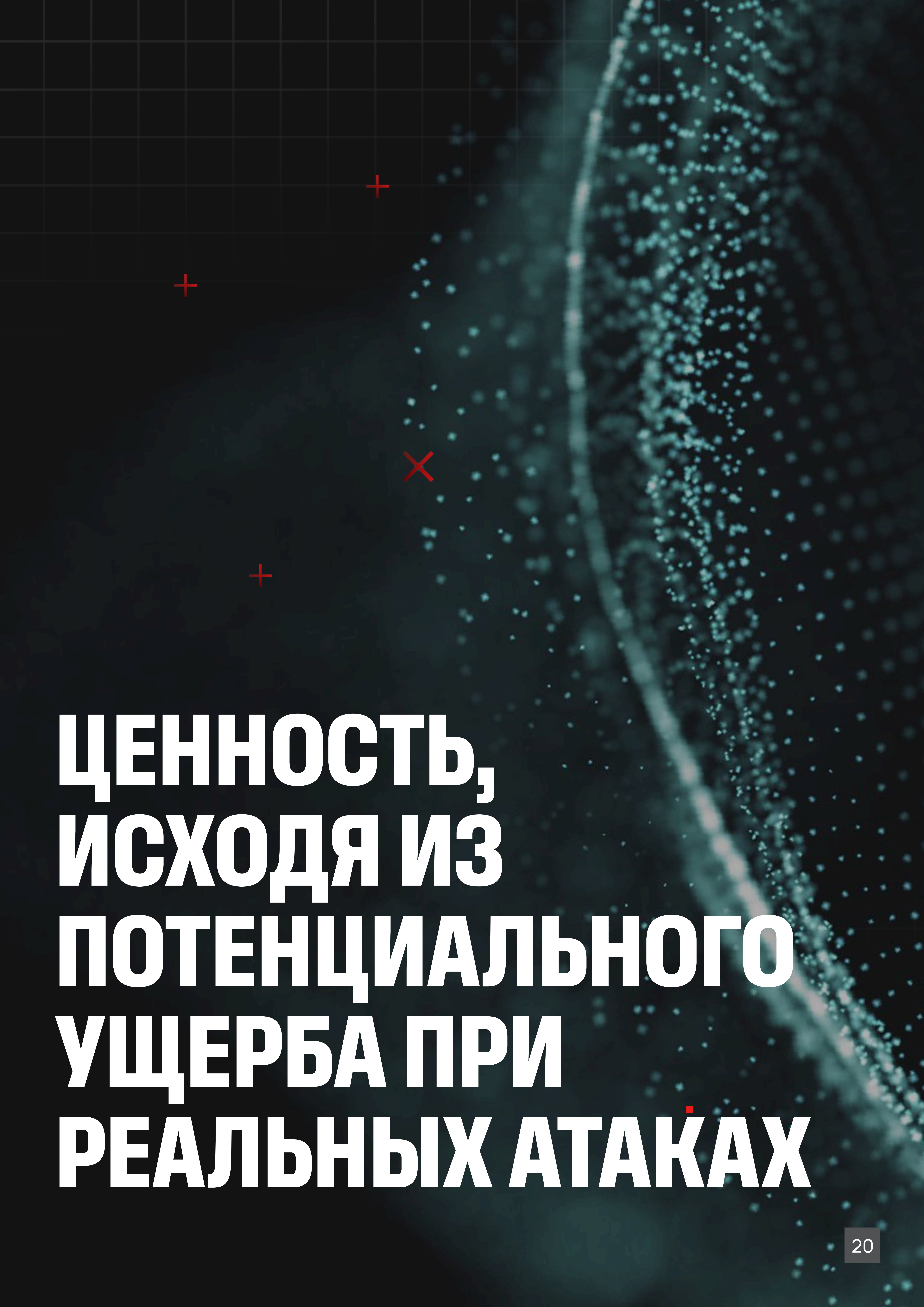


**В 60% СЛУЧАЕВ СЦЕНАРИЙ УСПЕШНОЙ РЕАЛИЗАЦИИ
НС ВКЛЮЧАЛ ИСПОЛЬЗОВАНИЕ УЯЗВИМОСТЕЙ
И НЕБЕЗОПАСНЫХ КОНФИГУРАЦИЙ ПЕРИМЕТРА**

* Для реализации одного недопустимого события может быть использовано сочетание нескольких векторов атак.

В 2 ИЗ 3 СЛУЧАЕВ АТАКА БЫЛА РЕАЛИЗОВАНА ЗА СУТКИ ИЛИ НЕ ТРЕБОВАЛА ВЫСОКОЙ КВАЛИФИКАЦИИ



The background is a dark, textured surface. A faint grid is visible in the upper left. Several red symbols are scattered: a plus sign (+) in the upper left, another plus sign (+) below it, a plus sign (+) further right, and a red 'X' mark below that. A bright, glowing blue line with a trail of small dots curves from the top right towards the bottom right. The text is in large, bold, white capital letters.

**ЦЕННОСТЬ,
ИСХОДЯ ИЗ
ПОТЕНЦИАЛЬНОГО
УЩЕРБА ПРИ
РЕАЛЬНЫХ АТАКАХ**

77% КОМПАНИЙ ОТНЕСЛИ ИБ В ТОП-5 ПРИОРИТЕТОВ БИЗНЕСА

Большинство компаний в нашей выборке – это те, кто уже высоко оценивает влияние кибербезопасности на свой бизнес и заинтересован узнать реальный уровень защищенности, а не довольствоваться формальным аудитом.

1 МЛН ₽

вложенный
в кибериспытания

Позволяет
выявить
и предотвратить
ущерб на сумму

В 40 МЛН ₽

5,3 ТРЛН ₽

НАХОДЯТСЯ ПОД РИСКОМ ПРИ ТЕКУЩЕМ УРОВНЕ ЗАЩИЩЕННОСТИ КОМПАНИЙ В 5 ОТРАСЛЯХ РОССИЙСКОЙ ЭКОНОМИКИ

2,7%

ВВП России
за 2024 г.

Сравнимо
**С БЮДЖЕТОМ
МОСКВЫ**

за 2024 г.

В 18 РАЗ БОЛЬШЕ

всего
российского
рынка ИБ

Источники: официальный портал Департамента финансов
«Открытый бюджет города Москвы 2024 год», данные Росстат по оценке
ВВП от 11 апреля 2025 года, группа компаний Б1

ШИФРОВАНИЕ ДАННЫХ ПРИВЕЛО БЫ К ПОТЕРЕ 1,57 МЛРД ₽ СРЕДИ УЧАСТНИКОВ

С учетом полученных данных о доле взломов* мы оценили ущерб, который мог быть нанесен в случае реальной атаки и шифрования баз данных участников КИ Экспресс. Результаты показывают, что шифрование привело бы к простоя и, как следствие, недополученной выручке на сумму 1,57 млрд руб. Такие потери могут стать шоком для бизнеса, привести к снижению его стоимости и другим долгосрочным негативным последствиям.

Если предположить, что часть компаний согласилась бы заплатить выкуп**, оценка ущерба возрастает до 1,76 млрд руб. Эти средства ушли бы в «черную» теневую экономику.

Потенциальный ущерб компаний-участников из отрасли, млн ₽

Обрабатывающие производства	941	59,9%
Информация и связь	312	19,9%
Торговля	287	18,3%
Финансы и страхование	16	1,0%
Консалтинг и научно-техническая деятельность	14	0,9%
ИТОГО	1 570 МЛН ₽	

ОБЩАЯ СУММА УЩЕРБА,

Общая сумма ущерба, если часть компаний заплатит выкуп**

~ 1 760 МЛН ₽

ОТ 1,6 ДО 1,8 МЛРД РУБЛЕЙ МОГЛИ БЫ ПОТЕРЯТЬ СУММАРНО УЧАСТНИКИ КИ ЭКСПРЕСС ОТ ШИФРОВАНИЯ

* Расчет по 5 отраслям, без учета отраслей с долей участия < 5%. Подробнее в разделе «Методология».

** Средняя сумма выкупа в размере 10 млн руб. по оценке Bi.Zone согласно Интерфакс.

ДЛЯ 5 ОТРАСЛЕЙ УЩЕРБ ОТ ШИФРОВАНИЯ МОГ БЫ СОСТАВИТЬ 5,33 ТРЛН ₽

Если спроецировать результаты испытаний на 5 отраслей российской экономики, потенциальный объем ущерба от шифрования при текущем уровне защищенности достигнет 5,33 трлн руб.* даже без учета выплаты выкупа.

При этом важно помнить, что по мере развития технологий и экономики в целом взаимосвязанность и взаимозависимость отраслей растет, в том числе расширяются цепочки поставок. Поэтому последствия реализации недопустимых событий более комплексные, и уязвимость даже микро- и малых предприятий может приводить к серьезным последствиям для всей экономики.

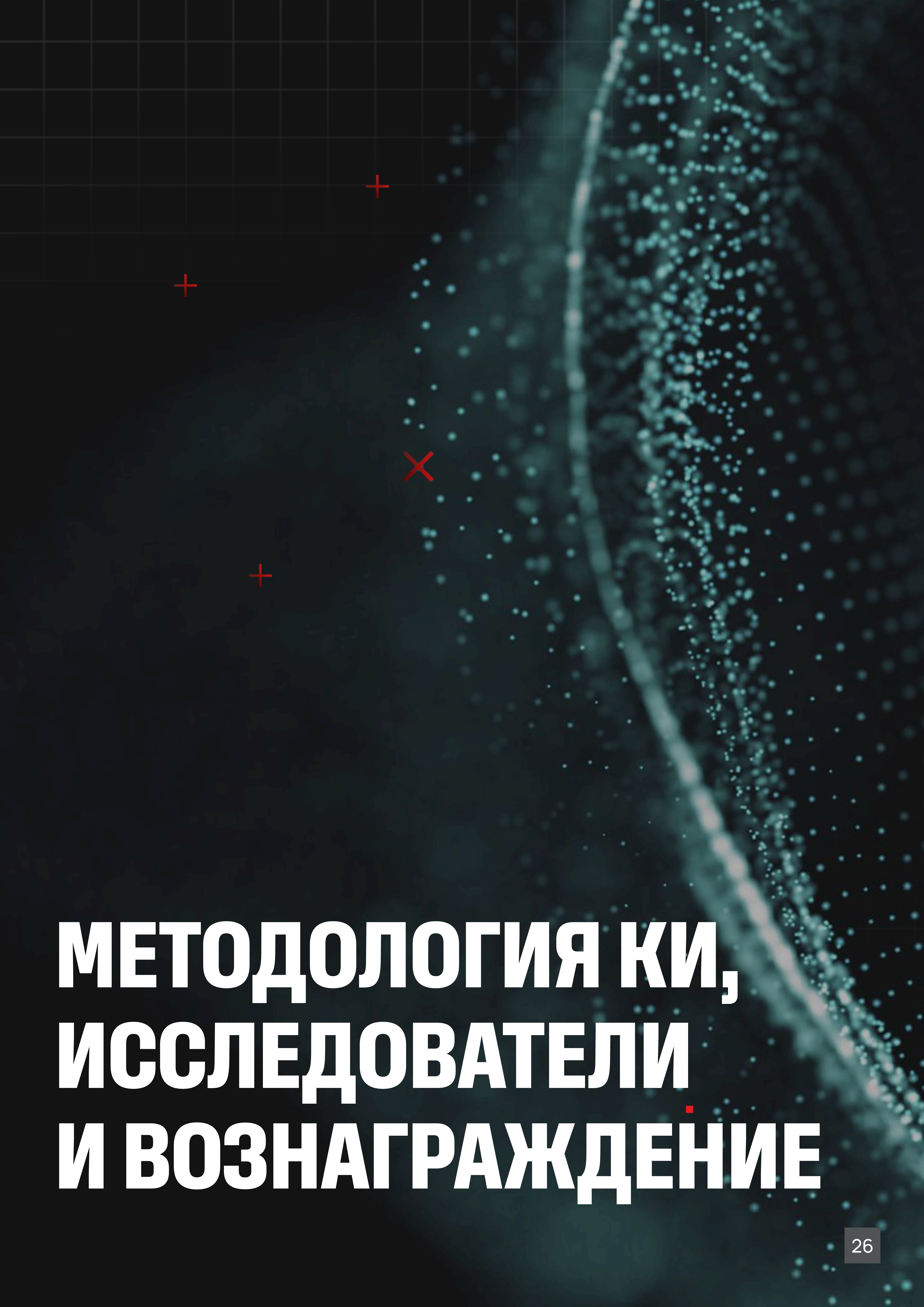
Потенциальный ущерб отрасли
в случае шифрования, млрд ₽

Торговля	3 492
Обрабатывающие производства	1 213
Информация и связь	251
Консалтинг и научно-техническая деятельность	227
Финансы и страхование	150

ИТОГО **~5 333 МЛРД ₽**

**5,3 ТРЛН ₽ — ПОТЕНЦИАЛЬНЫЙ УЩЕРБ
НА УРОВНЕ ЭКОНОМИКИ ОТ ШИФРОВАНИЯ**

* Мы выбрали более консервативный подход к оценке ущерба на основе данных о средней длительности простоя, частоте взломов и объёме выручки по отраслям. В оценке не учтены потенциальные косвенные затраты на восстановление, репутационные и юридические потери. На уровне экономики не оценивались мультипликативные эффекты. Подробнее в разделе «Методология».

The background is a dark, textured surface. A faint grid is visible in the upper left. Several red markers are scattered: two plus signs (+) and one cross (X). A bright, glowing blue line with a grainy texture curves from the top right towards the bottom right. The text is in a bold, white, sans-serif font.

МЕТОДОЛОГИЯ КИ, ИССЛЕДОВАТЕЛИ И ВОЗНАГРАЖДЕНИЕ

ГИПОТЕЗЫ:

КАКИЕ ОТВЕТЫ МЫ ПОЛУЧИЛИ

На старте проекта мы сформулировали 6 ключевых вопросов, определяющих актуальность, значимость и жизнеспособность проекта.

Ниже ключевые ответы, которые мы получили в результате исследования:

01 **Является ли кибериспытание эффективным методом проверки защищенности?**

Да, кибериспытание оправдало себя как новый метод оценки защищенности и проактивной защиты. Компании, которые приняли участие в КИ, на практике проверили реальный уровень защищенности и получили информацию о том, как не допустить реализацию НС. При этом факт взлома 61% компаний даже по упрощенной методологии КИ Экспресс подчеркивает важность предварительной диагностики и нейтрализации критических уязвимостей базового уровня.

02 **Какой будет конверсия во взлом?**

Конверсия во взлом оказалась в 3 раза выше, чем мы прогнозировали на старте проекта. Это не повод для паники, а скорее чёткий сигнал, что бизнес может недооценивать риски и некорректно приоритизировать бюджет, а также пренебрегать базовой цифровой гигиеной.

03 **Готов ли бизнес вовлекаться в кибербезопасность всерьёз?**

Да, мы увидели большой отклик со стороны первых лиц бизнеса (51% заказчиков). Им близок выбранный подход оценки киберустойчивости — в деньгах и приоритизации рисков по НС. Данный подход позволяет перевести сложные вопросы информационной безопасности в плоскость бизнес-рисков и стратегического планирования.

04 **Готовы ли к этому CISO и ИТ-директора?**

Да, практически в половине случаев заказчиком кибериспытаний выступили руководители блока ИТ/ИБ. Они оценили, что в разработанной методологии сочетаются преимущества сразу нескольких инструментов оценки киберзащищенности, которые уже используются на рынке, но по отдельности не дают комплексного и объективного результата.

05 **Способны ли белые хакеры показать возможность реализации НС?**

Да, для 3 из 5 компаний исследователи показали возможность реализации НС. Уже сейчас 26 белых хакеров получили вознаграждение за помощь компаниям в поиске слабых мест в их защите. Кроме того, мы увидели, что формат кибериспытаний позволяет привлечь достаточное количество белых хакеров (> 1 500 исследователей) с разным набором компетенций и навыков, чтобы выстроить полноценную цепочку атаки и провести максимально правдивую оценку киберустойчивости бизнеса.

06 **Сколько исследователей готовы работать по нашей методике?**

По результатам проекта в каждом испытании приняли участие в среднем 162 белых хакера, а максимальное количество исследователей на одно кибериспытание — 332.

ПРИВЛЕКЛИ >1500 БЕЛЫХ ХАКЕРОВ

ЭТО ПОЗВОЛИЛО ОБЪЕКТИВНО ОЦЕНИТЬ УРОВЕНЬ КИБЕРЗАЩИЩЕННОСТИ РОССИЙСКОГО БИЗНЕСА

Исследователи помогли компаниям найти слабые места в их киберзащите. В КИ Экспресс участвовали как опытные специалисты, так и те, кто ранее не занимался поиском уязвимостей в подобном формате.

1 500+

исследователей
суммарно

26

исследователей
уже получили
вознаграждение

162

По методологии
достаточно 50
исследователей
на испытании

среднее
количество
исследователей
на одно КИ

332

максимальное
количество
исследователей
на одно КИ

МИНИМАЛЬНОЕ ВОЗНАГРАЖДЕНИЕ ИССЛЕДОВАТЕЛЯ ВЫШЕ ЗАРПЛАТЫ ОПЫТНОГО ИБ-СПЕЦИАЛИСТА

5 600 тыс. ₽

максимальная сумма заработка
одного исследователя,
получившего выплату

700 тыс. ₽

в среднем заработал каждый
из 26 исследователей

300 тыс. ₽

минимальная сумма заработка
одного исследователя,
получившего выплату

259 тыс. ₽

средний заработок
ИБ-специалиста в найме
с опытом более 6 лет*

ИССЛЕДОВАТЕЛИ РАБОТАЛИ В РАЗНЫХ ФОРМАТАХ, ЧТОБЫ ОЦЕНКА БЫЛА ОБЪЕКТИВНЕЕ

Для того, чтобы всесторонне проверить защищенность компаний, недостаточно было привлечь одного исследователя или одну команду. Формат проведения КИ Экспресс позволил обеспечить достаточное количество участников для комплексной и объективной оценки киберустойчивости каждой компании-участника.

В ОДИНОЧКУ, В КОМАНДЕ И СМЕШАННО

Исследователи могли участвовать самостоятельно и в составе команды. В 39% случаев белые хакеры, получившие вознаграждение, подали отчёт как команда и поделили выплату по своему усмотрению. Ещё 15% исследователей совместили оба формата.

39%
Только
в команде



46%
В одиночку

15%
Совмещали
форматы

**> 50% ИССЛЕДОВАТЕЛЕЙ, КОТОРЫЕ ПОЛУЧИЛИ
ВОЗНАГРАЖДЕНИЕ, РАБОТАЛИ В КОМАНДЕ**

МЕТОДОЛОГИЯ ИССЛЕДОВАНИЯ

ЦЕЛЬ ИССЛЕДОВАНИЯ

Представить текущие результаты проекта «Кибериспытание Экспресс» по состоянию на **15 июля 2025 г.**

Оценить уровень защищенности компаний-участников на основе данных о возможности реализации недопустимых для них событий, в том числе в разрезе размера бизнеса и отрасли.	Оценить потенциальный ущерб от реализации недопустимых событий на уровне отдельно взятых компаний и отраслей в целом.
---	---

УЧАСТНИКИ

Российские предприятия, получившие грант от АО «Кибериспытание». В состав участников вошли компании из 9 отраслей российской экономики.

Информация и связь	Обрабатывающие производства	Финансы и страхование
Консалтинг и научно-техническая деятельность	Торговля	Строительство
Здравоохранение	Транспортировка и хранение	Аренда и деловые услуги

Распределение компаний по отраслям производилось на основании Общероссийского классификатора видов экономической деятельности (ОКВЭД) в соответствии с информацией о компаниях, представленной в системе СПАРК-Интерфакс. В рамках исследования мы не рассматривали отдельно отрасли, доля участия которых составила < 5%. Также в отраслевом разрезе не рассматривались индивидуальные предприниматели.

КАЧЕСТВЕННЫЕ И КОЛИЧЕСТВЕННЫЕ ИНСТРУМЕНТЫ АНАЛИЗА

- Анкетирование компаний-участников КИ Экспресс, экспертный анализ и отбор кейсов
- Статистические методы анализа
- Анализ открытых источников для сравнительных выводов.

ПОДХОД К ОЦЕНКЕ

С учетом размера выборки мы использовали достаточно простой и консервативный подход к оценке потенциальных ущербов с рядом допущений. Расчет производился только по недопустимым событиям, связанным с шифрованием данных, без учета индивидуальных предпринимателей, участвовавших в КИ Экспресс. Потери высчитывались как недополученная выручка в связи с простоем, вызванным приостановлением ключевых бизнес-процессов. За основу были взяты усреднённые данные о длительности простоя российских компаний из-за шифрования, взвешенные по уровню цифровизации различных отраслей в соответствии с индексом ВШЭ, а также информация о размере выручки по отраслям согласно СПАРК-Интерфакс.

В дальнейшем по мере обновления результатов и увеличения выборки может быть проведена более комплексная оценка, в том числе включены в размер ущерба косвенные затраты на восстановление, репутационные и юридические потери, а также оценка мультипликативных эффектов на межотраслевом уровне.

КОМАНДА ИССЛЕДОВАНИЯ

Исследование подготовлено командами АО «Кибериспытание» и фонда «Сайберус» при участии привлеченных экспертов.

Управленческая команда

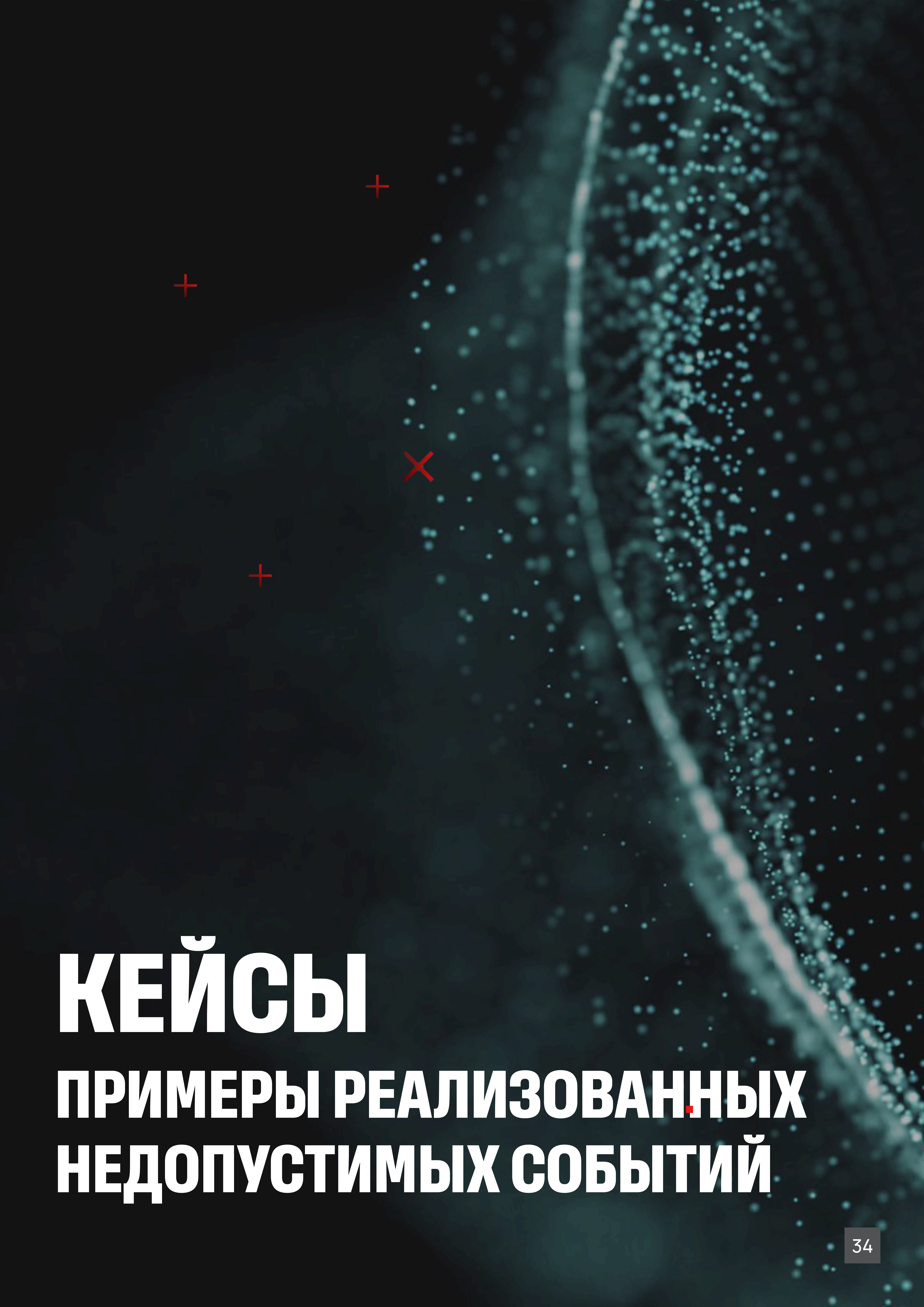
НАТАЛЬЯ ВОЕВОДИНА	генеральный директор АО «Кибериспытание»
ОЛЬГА МАХОВА	заместитель генерального директора АО «Кибериспытание»

Аналитико-операционная команда

СЕРГЕЙ БАЛЫБЕРДИН	методолог АО «Кибериспытание»
ЕЛЕНА СТЕПАНОВА	старший аналитик АО «Сайберэкс»
АЛЕКСАНДР ЛИСИЧКИН	директор по продукту АО «Кибериспытание»
ДИАНА САФИУЛЛИНА	комьюнити-директор АО «Кибериспытание»
СЕРГЕЙ ВОЙНОВ	управляющий директор АО «Сайберэкс»
ВАЛЕРИЙ ИВАНОВ	PR-lead, АО «Кибериспытание»
ПОЛИНА ГЕНЗЕЛЬ	менеджер проектов, АО «Кибериспытание»
АРТЕМ НАЛИВАЙКО	управляющий партнер 3side
АНТОН БОЧКАРЕВ	основатель и генеральный директор 3side
АЗИЗ АЛИМОВ	ведущий эксперт по симуляции атак Angara Security

Команда маркетинга и дизайна

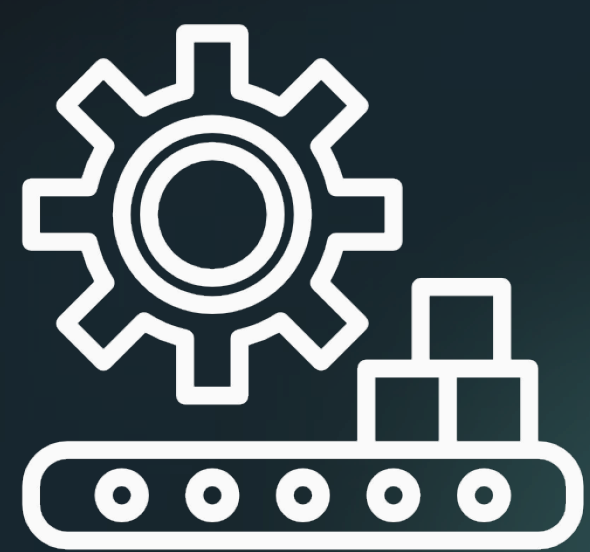
ДМИТРИЙ ЮЩЕНКО	директор по маркетингу АО «Кибериспытание»
ЮЛИЯ СЕМОЧКИНА	креативный продюсер АО «Кибериспытание»
ИЛЬЯ ЖЕРДЕР	продюсер спецпроектов АО «Кибериспытание»
СЕРГЕЙ СЛУЦКИЙ	дизайнер АО «Кибериспытание»



КЕЙСЫ

ПРИМЕРЫ РЕАЛИЗОВАННЫХ НЕДОПУСТИМЫХ СОБЫТИЙ

ОТ ОФИСНОГО WI-FI ДО ОСТАНОВКИ ПРОИЗВОДСТВА



Производственная
компания

ЦЕЛЬ

Демонстрация возможности
получения несанкционированного
доступа к клиентской базе данных

Исследователи предприняли попытки эксплуатации уязвимостей на периметре компании (лендинг-сайт) и социальной инженерии, но они не увенчались успехом – поэтому они решили попробовать подключиться к Wi-Fi компании, находясь в непосредственной близости к ее офису.

В ходе изучения выяснилось, что гостевая сеть не изолирована от корпоративной. Атакующие смогли поймать сигнал с улицы и запустить сканирование внутренних активов компании, в ходе которого был найден пароль от системы удаленного доступа.

Используя его, специалисты проникли в технологический сегмент сети, закрепились в инфраструктуре и не только получили доступ к базе клиентов, но и вышли в технологическую зону, откуда можно было бы вмешаться в производственные процессы — вплоть до их остановки.

Ключевые точки уязвимости:

Гостевая Wi-Fi-сеть не была изолирована от внутренней сети

Использование одинаковых «защитых» паролей на всех устройствах

Наличие дефолтных учётных записей в критически важной системе учёта

**АТАКУЮЩИЕ НЕ ТОЛЬКО ПОЛУЧИЛИ ДОСТУП К БАЗЕ КЛИЕНТОВ, НО
ТАКЖЕ ВОШЛИ В ТЕХНОЛОГИЧЕСКУЮ ЗОНУ, ЧТО ПОЗВОЛЯЕТ ВМЕШАТЬСЯ
В ПРОИЗВОДСТВЕННЫЕ ПРОЦЕССЫ — ВПЛОТЬ ДО ИХ ОСТАНОВКИ**

КРАЖА ДЕНЕЖНЫХ СРЕДСТВ ИЗ-ЗА СТАНДАРТНЫХ НАСТРОЕК



Финтех

ЦЕЛЬ

Продemonстрировать возможность хищения денежных средств со счета компании

В открытом доступе в интернете был обнаружен незащищенный сервис компании X, содержащий базу данных. Причиной утечки стало использование открытого порта доступа, а также стандартного системного пароля по умолчанию.

В ходе анализа базы данных была выявлена административная учетная запись, предоставившая доступ к другим корпоративным базам, включая хранилище персональных данных клиентов. Данная учетная запись позволяла изменять реквизиты банковских карт, что создавало риск перенаправления платежей на сторонние счета. В случае эксплуатации данной уязвимости компания-заказчик могла не сразу обнаружить несанкционированные транзакции.

Дополнительно в ходе проверки были обнаружены административные учетные записи системы для обработки платежей, использование которых позволяло осуществлять несанкционированные платежи.

ИЗ-ЗА ДЕФОЛТНЫХ НАСТРОЕК ИНФРАСТРУКТУРЫ АТАКУЮЩИЕ С МИНИМУМ УСИЛИЙ ПОЛУЧИЛИ ДОСТУП К УЧЕТНОЙ ЗАПИСИ АДМИНИСТРАТОРА И К ПЛАТЕЖНЫМ ДОКУМЕНТАМ. ПОДМЕНА РЕКВИЗИТОВ МОГЛА ДОЛГОЕ ВРЕМЯ ОСТАВАТЬСЯ НЕЗАМЕЧЕННОЙ

НЕ ОСТАНОВИЛИ ХАКЕРОВ — ОСТАНОВИЛОСЬ ПРОИЗВОДСТВО



Производственная
компания

ЦЕЛЬ

Продемонстрировать возможность остановки производства через эксплуатацию слабостей в IT-инфраструктуре

Атакующие нашли тестовый сервер, на котором использовались и небезопасно хранились актуальные учетные данные, с их помощью хакеры получили доступ в инфраструктуру компании.

Исследователи применили социальную инженерию, провели фишинговые рассылки и даже позвонили администратору, но это не дало результата — персонал был предупрежден.

Обнаруженная исследователями уязвимость Basic Auth на тестовом Битриксе сыграла злую шутку — атакующие вытащили логи авторизаций, а позже и письмо с инструкцией по удаленному подключению. Далее атака развивалась по принципу домино — этичные хакеры смогли получить привилегированную учетную запись, отключить системы защиты и захватить сервер ERP — фактически получить контроль над всем производством.

Результат: Система, управляющая производством, оказалась полностью захвачена. В любой момент она могла быть зашифрована, а производство остановлено. Недопустимое событие реализовано.

Для бизнеса это означает:

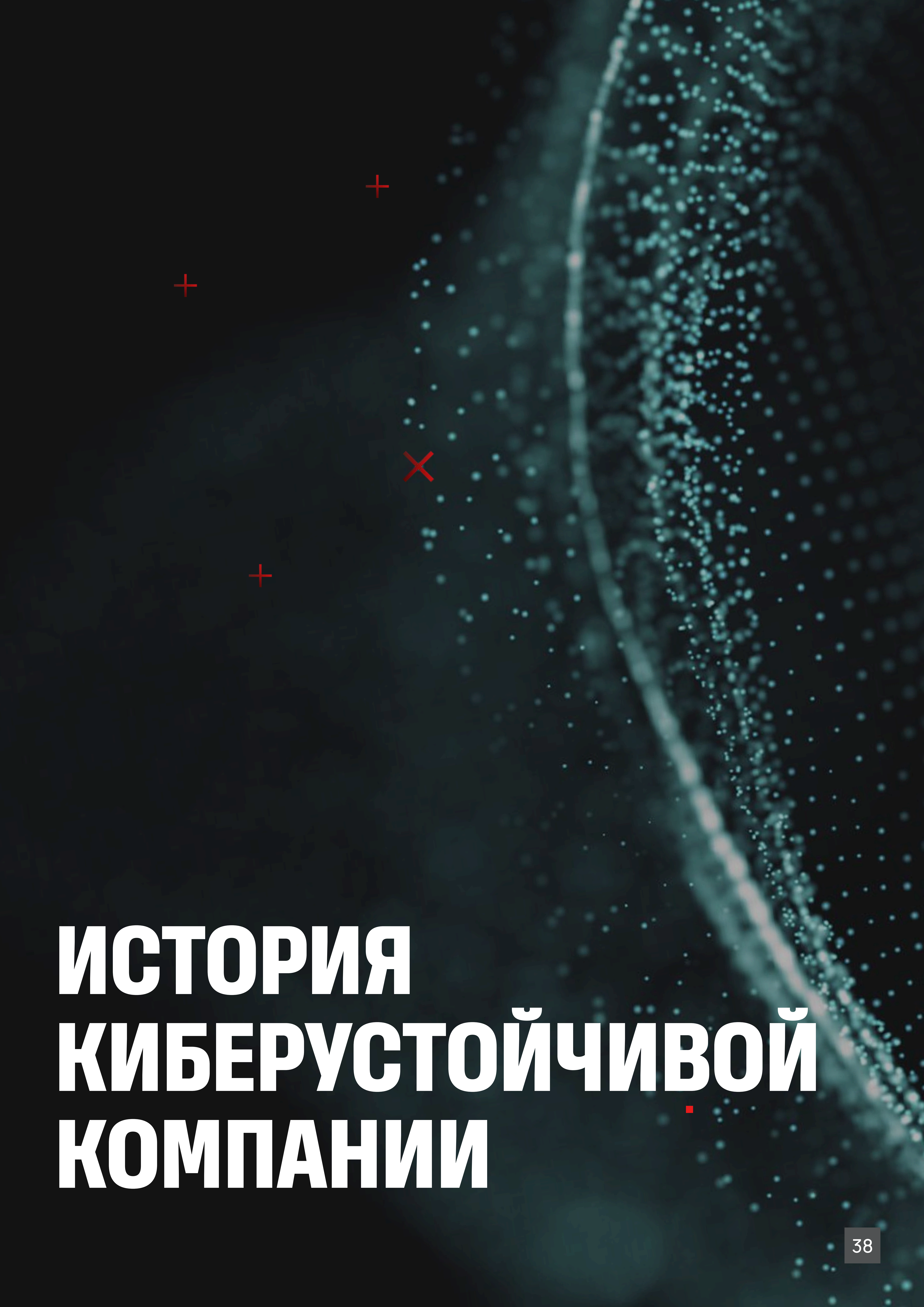
Хакеры могли остановить выпуск продукции

Испорченная деловая репутация

Компания может лишиться клиентов

Восстановление после атаки заняло бы недели и миллионы рублей

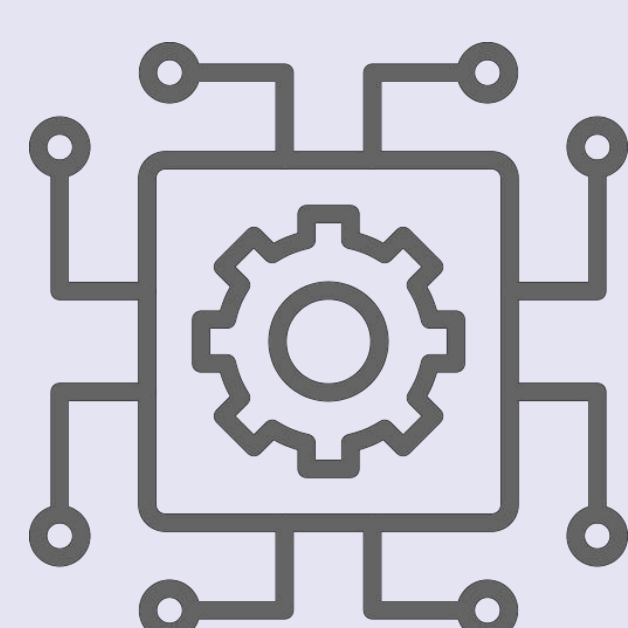
**ИТ-КОМАНДА ОТРЕАГИРОВАЛА ОПЕРАТИВНО, НО ИЗ-ЗА
ОТСУТСТВИЯ КОМПЛЕКСНОГО ПОДХОДА АТАКУЮЩИЕ ДВИГАЛИСЬ
ВНУТРИ ИНФРАСТРУКТУРЫ ПРАКТИЧЕСКИ БЕЗ СОПРОТИВЛЕНИЯ**

The background is a dark, textured surface. A prominent, glowing teal particle trail curves from the top right towards the bottom right. Scattered across the dark field are several red symbols: three plus signs (+) and one minus sign (-).

ИСТОРИЯ КИБЕРУСТОЙЧИВОЙ КОМПАНИИ

УСПЕШНЫЙ КЕЙС

INNOSTAGE ПЕРВАЯ В РОССИИ ПРОШЛА ОТКРЫТЫЕ КИ: ОТ «МЫ НЕ ГОТОВЫ» ДО «НАС НЕВОЗМОЖНО ВЗЛОМАТЬ ДАЖЕ ЗА 20 МЛН ₽»



ИТ-компания

ЦЕЛЬ

Украсть со счета 2 000 руб.

С 2022 года весь российский интернет и его пользователи — лёгкая мишень для хакеров: компании пользуются гибридными решениями для киберзащиты, а ИБ-специалистов не хватает. Хакеры, напротив, стали действовать более нагло: каждый год атак становится в полтора раза больше.

В результате Кибериспытания Экспресс мы выяснили, что реальная защищенность компаний намного ниже ожидаемой.

Но также есть примеры компаний, которые можно назвать киберустойчивыми. Одна из таких компаний — Innostage. Убедиться в киберзащищённости для нее было необходимо: ИБ-компания должна служить примером киберустойчивости. Недопустимо, чтобы ее можно было взломать.

Убедиться в киберзащищённости было необходимо: если можно взломать ИБ-компанию, можно взломать всех.



АЙДАР ГУЗАИРОВ

CEO Innostage

« Если можно взломать компанию, которая защищает других от хакеров, то что говорить об остальных? Innostage должна быть примером киберустойчивости. »

ЗА ПОЛГОДА С НАЧАЛА КИБЕРИСПЫТАНИЯ INNOSTAGE ОТРАЗИЛА 780 000 КИБЕРАТАК ОТ 1 000 «БЕЛЫХ» ХАКЕРОВ

**У ХАКЕРОВ БЫЛА КОНКРЕТНАЯ ЗАДАЧА —
УКРАСТЬ 2 000 ₽ СО СЧЁТА INNOSTAGE.
ЗА ЭТО ХАКЕР ПОЛУЧИЛ БЫ НАГРАДУ В 5 000 000 ₽**

Сумма недостаточно мотивировала хакеров: в первые месяцы была только «разведка» и базовые атаки.

INNOSTAGE УВЕЛИЧИЛА НАГРАДУ В 2 РАЗА — ДО 10 МЛН ₽

Тогда к исследованиям подключились 3 сильнейшие в России Red Team команды: DreamTeam, Wetox и True0xA3.

**В ИТОГЕ ВСЕГО ДВА ИССЛЕДОВАТЕЛЯ НАШЛИ
ЛАЗЕЙКИ, НО НЕ СМОГЛИ ПРОДВИНУТЬСЯ ДАЛЬШЕ**

Первый пообщался с сотрудниками и составил правдоподобное фишинговое письмо. На него попались 3 сотрудника, несмотря на постоянные обучения внутри компании. Исследователь получил награду в 100 000 ₽ за то, что показал, что обучение и пентесты — не панацея.

Вторая команда исследователей создала фальшивую бесплатную Wi-Fi точку возле офиса Innostage. Телефоны двух сотрудников подключились автоматически, но хакеру не удалось скачать пароли.

В МАЕ 2025 КОМПАНИЯ ПОДНЯЛА НАГРАДУ ДО 20 МЛН ₽!

РЕАЛИЗОВАТЬ НЕДОПУСТИМОЕ СОБЫТИЕ НИКОМУ ТАК И НЕ УДАЛОСЬ

ИТОГ: КОМПАНИЯ INNOSTAGE «КИБЕРИСПЫТАНА», ЕЕ НЕ ВЗЛОМАТЬ ДАЖЕ ЗА 20 000 000 ₽

Кибериспытания помогли Innostage трансформироваться в единственную компанию в России, которую официально невозможно взломать. Об этом знают клиенты, партнеры и реальные злоумышленники.

Благодаря кибериспытаниям Innostage достигла точки антихрупкости: компания продолжает выдерживать сильные воздействия, но получает от этого только пользу. Антихрупкость — элемент конкурентного превосходства, киберустойчивость — признак лидерства и конкурентоспособности.

> 50 000

атак было
отражено
в каждый месяц

1 000 +

белых хакеров
пытались показать
возможность взлома

3

Red Team команды
было среди хакеров.
Это победители
русских кибербитв



АЙДАР ГУЗАИРОВ

CEO Innostage

« Если безопасность моей компании постоянно проверяется на кибериспытаниях, я могу предоставить большую степень доверия по защите информации клиентам. Если говорить о моей личной трансформации — теперь я могу снова спать спокойно: «белые» хакеры подсветят уязвимости сильно раньше, чем реальные злоумышленники до нас доберутся. »

**КОМПАНИЯ ПРОДОЛЖАЕТ КИ И ПЛАНИРУЕТ УВЕЛИЧИТЬ
ВОЗНАГРАЖДЕНИЕ ДО 50 МЛН РУБЛЕЙ, ЧТОБЫ И ДАЛЬШЕ
ПОВЫШАТЬ СВОЮ КИБЕРЗАЩИЩЕННОСТЬ.**

The background is a dark, textured surface. A prominent, curved, teal-colored trail of small, bright particles or dust extends from the top right towards the bottom right. Scattered across the dark background are several red symbols: three plus signs (+) and one minus sign (-).

НАШИ РЕКОМЕНДАЦИИ

СТОИТ НАЧАТЬ С БАЗОВОЙ ЦИФРОВОЙ ГИГИЕНЫ

Для поддержания минимального уровня защищенности не нужны дорогостоящие средства защиты, необходимо начать с базовой гигиены.

ПОЛИТИКА БЕЗОПАСНОСТИ УЧЕТНЫХ ЗАПИСЕЙ

Настройка строгих требований к паролям и контроль жизненного цикла учетных записей сотрудников.

ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ

Обязательное использование для критически важных систем и сервисов.

ОБУЧЕНИЕ СОТРУДНИКОВ

Регулярные тренинги по кибергигиене и защите от фишинговых атак.

СОБЛЮДЕНИЕ БАЗОВЫХ ПРИНЦИПОВ БЕЗОПАСНОЙ РАЗРАБОТКИ

Соблюдение принципов secure coding на всех этапах создания и развития инфраструктуры, а также программного обеспечения.

ОБНОВЛЕНИЯ И ПАТЧИ

Регулярный мониторинг и своевременная установка критических обновлений ПО и систем.

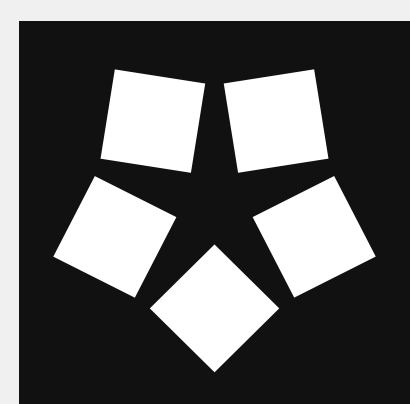
РЕЗЕРВНОЕ КОПИРОВАНИЕ

Регулярное проведение резервного копирования критически важных систем и данных.

The background is a dark, textured surface. A faint grid is visible in the upper left. A glowing, teal-colored trail of particles curves from the top right towards the bottom right. Several red symbols are scattered: three plus signs (+) and one minus sign (-).

ОРГАНИЗАТОРЫ ИССЛЕДОВАНИЯ

КИБЕРИСПЫТАНИЕ — КЛЮЧЕВОЙ ПРОЕКТ В ЭКОСИСТЕМЕ ФОНДА



Сайберус



САЙБЕРУС ОБЪЕДИНЯЕТ ИНДУСТРИЮ, БИЗНЕС И ГОСУДАРСТВО ДЛЯ БЕЗОПАСНОГО ЦИФРОВОГО БУДУЩЕГО РОССИИ И МИРА

ЦЕЛЬ №1

Создать новую
архитектуру
кибербезопасности

ЦЕЛЬ №2

Сделать Россию
самой защищённой
от киберугроз
страной в мире

ЦЕЛЬ №3

Помочь другим
странам построить
суверенную ИБ-
индустрию

УЧАСТНИКИ ФОНДА САЙБЕРУС

F6

Ведущий российский разработчик технологий для борьбы с киберпреступлениям

Стратегическая инвестиция Сайберуса

Positive Technologies

Разработчик продуктов для комплексной защиты от киберугроз, единственная публичная кибербез-компания в РФ

Сотрудничество с Сайберусом в проектах уровня отраслей и государств

Innostage

Крупнейший в РФ системный интегратор в сфере кибербезопасности

Сотрудничество с Сайберусом в проектах уровня отраслей и государств

Кибердом

Первый в мире кибербез-хаб и место силы российской индустрии кибербезопасности

Стратегическая инвестиция Сайберуса

CyberED

Образовательный центр для специалистов по противодействию кибератакам

Стратегическая инвестиция Сайберуса

CyberOK

Разработчик систем контроля кибератак и реагирования на угрозы

Создан по инициативе и поддержке Сайберуса

Эвритег

Вендор решений для защиты информации и предотвращения утечек

Стратегическая инвестиция Сайберуса

АНО НАМИБ

Национальная ассоциация международной информационной безопасности, уполномоченная Советом Безопасности РФ содействовать российским ИБ-компаниям в развитии экспорта

Поддержка Сайберус от государства

КИБЕРИСПЫТАНИЕ — ИННОВАЦИОННАЯ РОССИЙСКАЯ МЕТОДОЛОГИЯ

Создается в рамках АО «Кибериспытание», совместно с ведущими представителями индустрии кибербезопасности*.

В рамках Кибериспытания исследователи (белые хакеры) моделируют ситуацию реального взлома, при которой происходит недопустимое событие, способное нанести критический ущерб бизнесу (остановка производства, кража денег, авария и т.д.).

Кибериспытание проверяет защищенность всего бизнеса как взаимосвязанной системы: люди, процессы, ИТ-инфраструктура.

Кибериспытания проходят в открытом формате, когда множество исследователей может принять участие с оплатой за результат. Соответственно - чем выше награда, тем больше исследователей участвуют, выше их уровень, а так же выше частота атак.

Безопасность процесса и достоверность результатов гарантируется независимым экспертным советом.

**КИБЕРИСПЫТАНИЕ
ДАЕТ ОТВЕТ НА ВОПРОС:**

СКОЛЬКО СТОИТ ВЗЛОМАТЬ ВАШ БИЗНЕС?

* Состав экспертного совета Кибериспытания опубликован на официальном сайте www.cyberQ.ru

ФОРМАЛЬНЫЕ АУДИТЫ ДАЮТ ОЦЕНКУ СООТВЕТСТВИЯ. КИБЕРИСПЫТАНИЕ — ОЦЕНКУ РЕАЛЬНОЙ ЗАЩИЩЕННОСТИ

Классическая модель ИБ строится вокруг документов, процессов и внутреннего контроля. Однако большинство серьезных инцидентов последних лет происходят не из-за недостатка регламентов, а потому что делают вид, что всё под контролем, когда по факту — нет.

В условиях, где 100% гарантии не может дать никто, самое разумное — не отрицать риски, а уметь с ними работать. Смотреть на реальность открыто — это и есть настоящая устойчивость.

Кибериспытание проверяет защищенность всего бизнеса как взаимосвязанной системы: люди, процессы, ИТ-инфраструктура.



КИБЕРИСПЫТАНИЕ ПОЗВОЛЯЕТ ИЗМЕРИТЬ ЗАЩИЩЕННОСТЬ В ДЕНЬГАХ

CyberQuality (CQ) — оценка, которую получает кибериспытанная компания. Размер CQ означает сумму вознаграждения исследователям за реализацию недопустимого события. CQ отвечает на вопрос: «На какую сумму вы оцениваете свою защищенность в данный момент?».



50+ МЛН ₽

Высокий уровень защищенности компании, способность эффективно выявлять внутренних нарушителей, детектировать атаки нарушителей с высоким уровнем потенциала, в т.ч. APT-групп

20 МЛН ₽

Продвинутый уровень защищенности от внешних и внутренних нарушителей, способность выявлять и отражать таргетированные атаки

10 МЛН ₽

средний уровень защищенности от внешних нарушителей с умеренным потенциалом, например, ransomware-группировок

5 МЛН ₽

базовый уровень защищенности от низкоуровневых атакующих — хактивистов, вымогателей с минимальным уровнем знаний

1 МЛН ₽

минимальный уровень защищенности от наиболее простых массовых атак

ПРОВЕРЯЙ, ЧТОБЫ ДОВЕРЯТЬ

В мире, где угрозы невидимы, а последствия кибератак измеряются сотнями миллиардов, важно действовать на опережение.

Мы изучаем катастрофы, которые ещё не случились, чтобы их предотвратить.



cyberq.ru