

**ТОЛЬКО  
ПРОТИВОРЕ  
ЧИВЫЕ  
СОВЕТЫ  
ПОМОГАЮТ  
ПОНЯТЬ,  
ЧТО ТАКОЕ  
ИБ**

**Больше контента:**

[BOOSTY.TE](https://boosty.to)

[SPONSR.RU](https://sponsr.ru)

[TELEGRAM](#)

**Бесплатное издание**

Для новичков в мире ИБ или для тех, кто предпочитает работать с контентом без финансовых обязательств.

**Обычный читатель**

Для постоянных читателей, которые заинтересованы быть в курсе последних тенденций в мире кибербезопасности

**Профессионал**

Для ИТ-специалистов, экспертов, и энтузиастов, которые готовы погрузиться в сложный мир ИБ.

## **ИРОНИЯ БЕЗОПАСНОСТИ ДАЙДЖЕСТ. 2024 / 04**

Добро пожаловать в очередной выпуск ежемесячного сборника материалов, который является вашим универсальным ресурсом для получения информации о самых последних разработках, аналитических материалах и лучших практиках в постоянно развивающейся области безопасности. В этом выпуске мы подготовили разнообразную подборку статей, новостей и результатов исследований, рассчитанных как на профессионалов, так и на обычных любителей. Цель нашего дайджеста - сделать наш контент интересным и доступным. Приятного чтения!

Больше материалов: [Boosty](#) | [Sponsr](#) | [TG](#)

ЧРОНИЯ БЕЗОПАСНОСТИ





# Новости

## ХАКЕРСКАЯ ГРУППА "HANDALA" ВЗЯЛА НА СЕБЯ ОТВЕТСТВЕННОСТЬ ЗА ВЗЛОМ РАДАРНЫХ СИСТЕМ НЕУСТАНОВЛЕННОЙ ЦЕЛИ

Инженеры разработали способ заставить автомобильные радарные системы "галлюцинировать", посылая поддельные сигналы на радар цели. Исследователи продемонстрировали этот способ на реальных радарных системах в реальных автомобилях, движущихся на высокой скорости. Они смогли заставить целевую машину воспринимать другую машину там, где её на самом деле не было, обмануть радар цели, заставив думать, что проезжающей машины нет, хотя на самом деле она существовала, и создать впечатление, что машина внезапно изменила курс. Результаты исследований, проведённых инженерами, публично были поддержаны различными организациями, включая Управление военно-морских исследований, Управление научных исследований BBC и Национальный научный фонд.



## ЖЕЛЕЗНЫЙ КИБЕР КУПОЛ ВЗЛОМАН

Хакерские группы, такие как Anonymous Sudan, заявляли, что они успешно взломали израильские системы предупреждения о ракетном нападении, включая "Железный купол". Однако неясно, соответствуют ли эти заявления действительности или нет. "Железный купол" — это современная система противовоздушной обороны, предназначенная для перехвата ракет малой дальности и артиллерийских снарядов, выпущенных с расстояния от 4 до 70 километров. Железный купол предполагает совместную работу экспертов кибербезопасности из различных ведомств, включая министерства обороны, Силы обороны Израиля и шпионские агентства "Моссад" и "Шин Бет" с применением ИИ и небольшой армии сотрудников спецслужб для защиты жизненно важной инфраструктуры Иерусалима от кибератак со стороны враждебных стран.

## CZECH REPUBLIC CLAIMS RUSSIA LAUNCHES OF ATTACKS ON RAILWAY



Событие дня: Чешская Республика утверждает, что Россия неустанно работает изо всех сил, проводя "тысячи" кибератак на их железнодорожные системы с февраля 2022 года, потому что невозможно завоевать мир, не взломав сначала чешские системы продажи жд билетов. Министр транспорта Мартин Купка, выступающий в качестве "лучшего" аналитика кибервойн, распевал байки о том, как эти кибератаки потенциально вызывают беспорядок и неразбираиху среди проводников поездов

В ответ на эти выдуманные действия Прага заняла решительную позицию и приняла закон, позволяющий принимать меры против иностранных организаций, подозреваемых в киберпреступлениях. Потому что ничто так не говорит "попались, хакеры!" как законодательный акт. Они также устанавливают ограничения для участия иностранных операторов в тендерах на критически важные проекты, потому что ничто так не кричит о безопасности, как бюрократия



## СОТРУДНИК ИЗРАИЛЬСКОГО ПОДРАЗДЕЛЕНИЯ 8200 РАСКРЫЛ СЕБЯ ЧЕРЕЗ ПУБЛИКАЦИЮ КНИГИ НА AMAZON

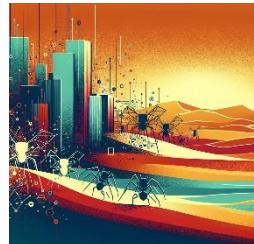
❖ **Раскрытие личности:** Йоси Сариэль, командир израильского подразделения 8200, непреднамеренно раскрыл свою настоящую личность в Интернете. Подразделение 8200 — это очень засекреченная часть израильских вооружённых сил, которую часто сравнивают с АНБ США по возможностям ведения наблюдения

❖ **Цифровой след:** Разоблачение произошло из-за цифрового следа, оставленного книгой Сариэль, опубликованной на Amazon под названием "Человеко-машинная команда". Книга, в которой обсуждается интеграция ИИ в военные операции, была привязана к личному аккаунту автора в Google, что позволило раскрыть его уникальный идентификатор и ссылки на его карты и приложения. профиля календаря

❖ **Критика:** Пребывание Сариэля на посту главы подразделения 8200 было неоднозначным, поскольку подразделение не смогло предсказать и предотвратить крупную атаку ХАМАСА на юг Израиля 7 октября, в результате которой погибло около 1200 израильтян и было захвачено 240 заложников. Подразделение также подверглось критике за его роль в войне в Газе, где в военных операциях использовались системы искусственного интеллекта

❖ **Общественный резонанс:** Раскрытие личности Сариэля произошло в то время, когда он уже находился под пристальным вниманием общественности в Израиле. Армия обороны Израиля (ЦАХАЛ) отреагировала на сообщение, заявив, что адрес электронной почты, связанный с книгой, не был личным аккаунтом Сариэля и был посвящён книге. Армия обороны Израиля признала ошибку и заявила, что этот вопрос будет расследован, чтобы предотвратить подобные случаи в будущем

❖ **Репутация подразделения:** Подразделение 8200 известно своим опытом сбора радио-разведывательных данных и оказывает значительное влияние на технологическую индустрию Израиля. Раскрытие личности Сариэля рассматривается как удар по репутации подразделения и привело к обвинениям в высокомерии и потенциальному компромиссу в сборе разведданных



## ИИ, Большие языковые модели (LLMs) и проблемы ИБ

Появление больших языковых моделей (LLM), таких как ChatGPT, открыло новую эру в области искусственного интеллекта, предлагая беспрецедентные возможности в создании текста, похожего на человеческий, на основе обширных наборов данных. Эти модели нашли применение в различных областях, от автоматизации обслуживания клиентов до создания контента. Однако, как и любая мощная технология, LLMS также создает новые проблемы и возможности для киберпреступников, что приводит к усложнению проблем кибербезопасности.

### ◆ Покупка услуг LLM

Покупка услуг у поставщиков услуг LLM является наиболее простым подходом. Это предполагает использование общедоступных LLM-программ или программ, предлагаемых сторонними поставщиками, для различных вредоносных действий. Простота доступа к этим моделям делает их привлекательными для целого ряда киберпреступлений, от рассылки фишинговых электронных писем до масштабного создания поддельного контента.

### ◆ Создание пользовательских LLM

Некоторые могут предпочесть разработку собственных LLM, адаптированных для выполнения конкретных вредоносных задач. Такой подход требует значительных ресурсов, включая опыт в области машинного обучения и доступ к большим наборам данных для обучения моделей. Специально разработанные LLM могут быть разработаны для обхода мер безопасности и проведения целенаправленных атак, что делает их мощным инструментом в арсенале изощренных киберпреступных групп.

### ◆ Взлом существующих LLM

Ещё одной стратегией является использование уязвимостей в существующих LLM для манипулирования их выводами или получения несанкционированного доступа к их функциональным возможностям. Это может включать в себя такие методы, как быстрое внедрение, когда тщательно продуманные входные данные заставляют LLM генерировать вредоносный контент или раскрывать конфиденциальную информацию. Так называемый джайлбрейк LLM для устранения встроенных ограничений безопасности также является проблемой, поскольку это может привести к созданию некорректного, вводящего в заблуждение или предвзятого контента.

### ◆ Автоматический джайлбрейк LLM

Иновационный подход заключается в использовании одного LLM для нарушения мер безопасности другого. Этот метод предполагает сценарий будущего, напоминающий повествования о киберпанках, где сражения между системами искусственного интеллекта, каждая из которых пытается перехитрить другую, становятся обычным аспектом усилий по обеспечению кибербезопасности. Эта концепция аналогична генеративным состязательным сетям (GAN), где одновременно обучаются две модели: одна для генерации данных (генератор), а другая для оценки их достоверности (дискриминатор). Эта динамика создаёт непрерывный цикл совершенствования обеих моделей, принцип, который может быть применён к LLM как для наступательных, так и для оборонительных целей кибербезопасности.

### ◆ Битва ботов

Задача систем искусственного интеллекта - поддерживать безопасность цифровой инфраструктуры, в то время как их коллеги пытаются проникнуть в неё. Этот сценарий не является полностью вымышленным; он отражает современную практику в области кибербезопасности, когда автоматизированные системы все чаще используются для обнаружения угроз и реагирования на них. Развитие LLM может ускорить эту тенденцию, что приведёт к появлению более сложных и автономных форм киберзащиты и кибератак.

### ◆ Последствия и ответные меры в области кибербезопасности

Использование LLMS киберпреступниками создаёт серьёзные проблемы в области кибербезопасности. Эти модели могут автоматизировать и расширять масштабы традиционных киберпреступлений, делая их более эффективными и труднообнаруживаемыми. Например, LLM могут генерировать весьма убедительные фишинговые электронные письма или атаки с использованием социальной инженерии, что повышает вероятность успешных взломов.

Идея использования состязательных LLM в сфере кибербезопасности имеет несколько последствий. Во-первых, это может повысить эффективность мер безопасности за счёт постоянного совершенствования их с учётом потенциальных уязвимостей. Во-вторых, это поднимает вопросы об этических и практических аспектах использования ИИ в таких двойных ролях, особенно учитывая возможность непредвиденных последствий или эскалации киберконфликтов.

### ◆ Защитные меры

Для противодействия угрозам, связанным с вредоносным использованием LLM, специалисты кибербезопасности разрабатывают ряд защитных мер. К ним относятся улучшение обнаружения контента, созданного искусственным интеллектом, защита LLM от несанкционированного доступа и повышение надёжности моделей от несанкционированного использования.

### ◆ Этические и юридические соображения

Потенциальное неправомерное использование LLM также вызывает этические и юридические вопросы. Растёт спрос на нормативные акты, регулирующие разработку и использование LLM, для предотвращения их использования киберпреступниками. Кроме того, необходимы этические принципы, гарантирующие, что преимущества LLMS будут реализованы без ущерба для безопасности или конфиденциальности.

### ◆ Перспективы на будущее

По мере дальнейшего развития LLM будут усложняться как возможности, которые они предоставляют, так и угрозы, которые они представляют. Постоянные исследования и сотрудничество между разработчиками искусственного интеллекта, экспертами в области кибербезопасности и политиками будут иметь решающее значение для решения стоящих перед ними задач. Понимая стратегии, которые киберпреступники используют для взлома LLM, и разрабатывая эффективные меры противодействия, сообщество специалистов кибербезопасности может помочь защитить цифровой ландшафт от возникающих угроз.



## ЧАТ-БОТ НА БАЗЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ВВС США

Военно-воздушные силы США инвестировали средства в чат-бота на базе ИИ, предназначенного для выполнения задач разведки и наблюдения. Эта инициатива является частью тенденций в военных ведомствах по изучению и интеграции технологий ИИ для различных применений. Чат-бот является продуктом контракта стоимостью 1,2 миллиона долларов с компанией Midstream LLC, также известной как Spectrum, и предназначен для расширения возможностей операций по разведке, наблюдению и рекогносцировке (ISR).

### Ключевые функции и возможности

◆ **Поддержка разведки, наблюдения и рекогносцировки (ISR)** - Чат-бот предназначен для поддержки задач ISR путём обработки таких данных, как изображения и видео, и предоставления аналитической информации в ответ на запросы на простом английском языке. Эта возможность направлена на упрощение анализа данных наблюдения, снижение когнитивной нагрузки на аналитиков и лиц, принимающих решения.

◆ **Инструменты обработки и визуализации данных** - Контракт предусматривает разработку инструментов для обработки и визуализации данных, которые необходимы для обработки огромных объёмов данных, генерируемых в ходе операций ISR. Эти инструменты облегчат организацию и интерпретацию данных, сделав их более доступными и действенными.

◆ **Модель машинного обучения для анализа изображений с борта SAR** - Конкретное приложение, упомянутое в документах, - это модель машинного обучения для анализа изображений судов с помощью радара с синтезированной апертурой (SAR). Эта модель может использоваться для обнаружения и анализа морской активности, предоставляя сводки и оценки достоверности для идентифицированных объектов.

◆ **Взаимодействие пользователя с чат-ботом** - Интерфейс чат-бота позволяет пользователям взаимодействовать с системой, вводя вопросы и получая в ответ визуальные данные, такие как линейные графики и обрезанные изображения. Это взаимодействие разработано таким образом, чтобы быть интуитивно понятным и удобным для пользователей, удовлетворяя потребности операторов, которым требуется быстрая и точная информация.

### Разработка и этические соображения

◆ **Ранняя стадия развития** - Чат-бот на базе искусственного интеллекта в настоящее время находится на ранней стадии разработки. ВВС заявили, что программа не используется для принятия целевых решений и находится на стадии оценки для определения возможных вариантов ее использования в рамках Министерства ВВС.

◆ **Этическое использование ИИ** - ВВС подчёркивают свою приверженность этичному и ответственному использованию технологий искусственного интеллекта.

### Более широкие последствия и перспективы на будущее

◆ **Интерес военных к ИИ** - Инвестиции в чат-бота на базе искусственного интеллекта отражают растущий интерес военных к использованию ИИ для повышения готовности к выполнению миссий и операционной эффективности. Технологии ИИ рассматриваются для широкого спектра военных применений - от прогнозирования логистики и технического обслуживания до анализа боевых действий.

◆ **Конкурентоспособность ИИ** - Главное управление ИИ (CDAO) в области обработки данных разработало план, согласно которому к 2025 году Департамент ВВС будет готов к внедрению искусственного интеллекта, а к 2027 году - конкурентоспособен. Разработка приложений с поддержкой искусственного интеллекта, таких как чат-бот, соответствует этим стратегическим целям.

◆ **Потенциал для гражданских применений** - Технология Spectronn также предполагает гражданские приложения, такие как обнаружение преступлений в сфере розничной торговли и мониторинг кибератак. Универсальность платформы искусственного интеллекта указывает на то, что технология, разработанная для военных целей, может иметь более широкое применение в различных отраслях промышленности.

## XZ ИНЦИДЕНТ



Недавний инцидент с кибербезопасностью связан с программным пакетом XZ Utils, который широко используется в операционных системах Linux для сжатия данных.

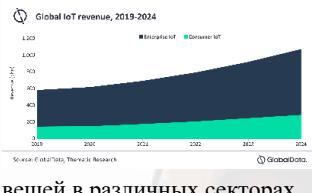
◆ **Расследование:** Об инциденте стало известно, когда инженер Microsoft Andres Freynd заметил необычное замедление при использовании SSH, инструмента для безопасного удалённого входа в систему. Его расследование привело к обнаружению вредоносного кода, встроенного в пакет XZ Utils в его системе.

◆ **Вредоносный код в XZ Utils:** Вредоносный код был представлен в двух последних обновлениях XZ Utils. Он был разработан для нарушения процесса аутентификации по SSH, создания бэкдора, который мог бы обеспечить несанкционированный удаленный доступ к уязвимым системам.

◆ **Влияние и значимость:** Учитывая, что XZ Utils необходим для многих операций в системах Linux, на которых работает подавляющее большинство интернет-серверов, потенциальное воздействие этого бэкдора могло бы быть катастрофическим, затронув бесчисленное множество компьютеров по всему миру.

◆ **Реагирование и предотвращение:** Инцидент подчёркивает важность бдительности и оперативных действий в области кибербезопасности для предотвращения подобных нарушений.

◆ **Последствия:** Эта ситуация подчёркивает серьёзные проблемы, связанные с безопасностью ПО с открытым исходным кодом, и необходимость постоянного мониторинга и обновления такого ПО для защиты от угроз.



## БЕЗОПАСНОСТЬ ИНТЕРНЕТА ВЕЩЕЙ В 2024

В статье рассматривается эволюционирующий ландшафт безопасности Интернета вещей (IoT) по мере того, как технология продолжает интегрироваться в различные аспекты бизнеса и жизни потребителей. В статье освещаются важнейшие проблемы безопасности, с которыми столкнётся Интернет вещей в 2024 году, подчёркивается необходимость тщательного мониторинга, надёжных мер безопасности и соблюдения нормативных требований для снижения рисков, связанных с расширением использования устройств Интернета вещей в различных секторах.

◆ **Рост рынка и зависимость от Интернета вещей:** По прогнозам, в 2024 году объем мирового рынка интернета вещей составит 1,1 трлн долларов, а совокупный годовой темп роста (CAGR) составит 13%. На долю корпоративного интернета вещей приходится более 75% общего дохода, что подчёркивает значительную зависимость предприятий от систем Интернета вещей в своей операционной деятельности.

◆ **Риски для безопасности, связанные с чрезмерной зависимостью:** Растущая зависимость от систем Интернета вещей создаёт ряд рисков для безопасности. Предприятия могут не замечать предупреждающих признаков кибератак из-за автономного характера систем Интернета вещей.

◆ **Распространённые проблемы безопасности Интернета вещей в 2024 году:**

→ Расширение возможностей для атак: Взаимосвязанный характер систем Интернета вещей создаёт множество точек входа для киберпреступников, что затрудняет эффективный мониторинг и защиту этих систем.

→ Риски в сети общего пользования: Сотрудникам рекомендуется не подключать рабочие устройства к небезопасным сетям общего пользования для снижения рисков безопасности.

◆ **Решение проблем безопасности Интернета вещей:**

→ Статистика показывает, что только 4% компаний уверены в своей безопасности, при этом менее 5% считают, что их подключённые устройства защищены от кибератак.

→ Кибератаки происходят каждые 39 секунд, что подчёркивает необходимость принятия надёжных мер безопасности.

→ Ключевые шаги для решения проблем безопасности Интернета вещей включают мониторинг уязвимостей, обеспечение безопасных подключений и внедрение регулярных обновлений и патчей.

◆ **Нормативно-правовая база:** В статье также рассматривается меняющаяся нормативно-правовая база, связанная с кибербезопасностью Интернета вещей, в связи со значительными изменениями в законодательстве ЕС, США и Великобритании, направленными на повышение устойчивости подключённых устройств к киберугрозам и защиту конфиденциальности личной информации.

◆ **Финансовые последствия и управление рисками:** Финансовые последствия угроз Интернета вещей значительны, что настоятельно требует от руководителей служб информационной безопасности (CISO) разработки стратегии предотвращения, включая учёт финансовых последствий этих угроз и соответствующее планирование.

◆ **Природа IoT-атак:** устройства Интернета вещей, зачастую из-за более слабых мер безопасности, являются главной мишенью для киберпреступников. В статье прогнозируется широкий спектр угроз IoT, включая вредоносное ПО, DDoS-атаки и угрозы с использованием ИИ.

◆ **Тенденции и цифры:** Ожидается значительный рост рынка IoT-безопасности - с 3,35 млрд долларов в 2022 году до 13,36 млрд долларов в 2028 году, что свидетельствует о растущем внимании к кибербезопасности в сфере Интернета вещей.



## УТЕЧКА ДАННЫХ AT&T

Компания AT&T подтвердила серьёзную утечку данных, которая затронула около 73 миллионов клиентов, как нынешних, так и бывших. Впервые о такой утечке стало известно, когда в даркнете был обнаружен набор данных, содержащий конфиденциальную информацию о клиентах. Набор данных считается, что с 2019 года или ранее, и включает в себя ряд личную информацию

Скомпрометированные данные включают: ФИО, адреса электронной почты, почтовый адрес, номера телефона, номера социального страхования, даты рождения, номера счетов AT&T, коды доступа (цифровые PIN-коды, состоящие из четырёх цифр).

Важно отметить, что набор данных, вероятно, не содержит личной финансовой информации или истории звонков.

### Масштаб

Утечка затронула около 7,6 миллионов текущих клиентов AT&T и примерно 65,4 миллиона бывших клиентов. Данные были опубликованы в darknet примерно за две недели до подтверждения со стороны AT&T

### Реакция AT&T

- ◆ Сбросила пароли затронутых пользователей.
- ◆ Начало тщательное расследование с привлечением внутренних и внешних экспертов кибербезопасности.
- ◆ Начали уведомлять пострадавших клиентов по электронной почте или в письмах.
- ◆ Предложили оплатить услуги кредитного мониторинга, где это применимо

### AT&T рекомендует клиентам:

- ◆ Заморозить их кредитные отчёты в крупных агентствах (Equifax, Experian и TransUnion).
- ◆ Подписаться на мониторинг кредитоспособности в режиме 24-7.

- ❖ Включить двухфакторную аутентификацию в своих учётных записях AT & T.
- ❖ Изменить пароли и отслеживать активность учётной записи на предмет подозрительных транзакций.
- ❖ Настроить бесплатные оповещения о мошенничестве и замораживании кредитов через Федеральную торговую комиссию для защиты от кражи личных данных и других вредоносных действий.

#### Предыдущие инциденты и отраслевой контекст

За последние годы AT&T столкнулась с несколькими утечками данных, которые имели различные масштабы и последствия. Это нарушение значительно превосходит утечку, произошедшую в январе 2023 года и затронувшую 9 миллионов пользователей. Телекоммуникационная отрасль стала прибыльной мишенью для хакеров, и недавние взломы затронули других крупных провайдеров, таких как T-Mobile и Verizon.

#### Реакция регулирующих органов

В декабре Федеральная комиссия по связи (FCC) обновила свои правила уведомления о нарушениях данных, чтобы привлечь телефонные компании к ответственности за защиту конфиденциальной информации клиентов и дать клиентам возможность защитить себя в случае взлома их данных.

#### Текущее расследование и последствия

Источник утечки все ещё устанавливается, и пока неизвестно, были ли данные получены от AT&T или от одного из ее поставщиков. В настоящее время нет свидетельств несанкционированного доступа к системам AT&T, приведшего к утечке набора данных. Однако, по состоянию на последние обновления, инцидент не оказал существенного влияния на деятельность AT&T.

## THREAT ACTOR UNC1549



Иранский UNC1549 нацелен на израильский и ближневосточный аэрокосмический и оборонный секторы:

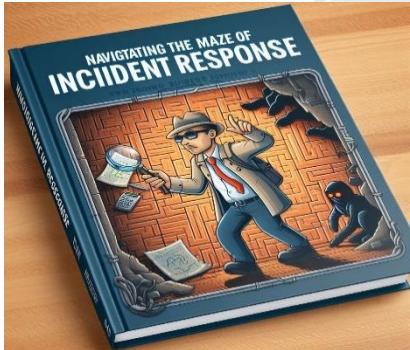
- ❖ **Идентификация участника угрозы:** рассматривается деятельность UNC1549, предполагаемого иранского агента угрозы. Эта группировка также известна под другими названиями, такими как "Черепаховый панцирь" и "Дымчатая песчаная буря", и связана с Корпусом стражей исламской революции Ирана (КСИР).
- ❖ **Целевые секторы и регионы:** UNC1549 нацелен на аэрокосмическую, авиационную и оборонную промышленность Ближнем Востоке, затрагивая такие страны, как Израиль, ОАЭ и, возможно, Турцию, Индию и Албанию.
- ❖ **Продолжительность кампании и методы ее проведения:** Кампания проводится как минимум с июня 2022 года. Группа использует сложные методы кибершпионажа, включая скрытый фишинг, социальную инженерию и использование облачной инфраструктуры Microsoft Azure для C2. Они используют различные "приманки" на тему предложения работ и поддельные веб-сайты для внедрения вредоносного ПО.
- ❖ **Вредоносные программы и инструменты:** Два основных бэкдора, MINIBIKE и MINIBUSUS, используются для проникновения в целевые сети и закрепления. Эти инструменты позволяют собирать информацию и осуществлять дальнейшее проникновение в сеть.
- ❖ **Стратегические последствия:** Разведанные, собранные в результате этой шпионской деятельности, считаются имеющими стратегическое значение для иранских интересов и потенциально влияющими как на шпионаж, и другие операции.
- ❖ **Методы предотвращения обнаружения:** UNC1549 использует различные методы, чтобы избежать обнаружения и анализа. К ним относятся широкое использование облачной инфраструктуры для маскировки своей деятельности и создание поддельных веб-сайтов о вакансиях и профилей в социальных сетях для распространения вредоносного ПО.
- ❖ **Текущее состояние:** Согласно отчётам за февраль 2024 года, кампания остаётся активной, и компании, занимающиеся кибербезопасностью, такие как Mandiant и CrowdStrike, продолжают предпринимать усилия по противодействию этой деятельности.

A stylized, hand-drawn illustration of a robot. The robot has a large, rounded head with a single prominent eye. It wears a white space helmet with a clear visor. A stack of newspapers is tucked under its left arm; the top newspaper's masthead reads "SUBSCRIPTION". The robot's right hand is raised in a fist, with a lightning bolt striking from its fingers. The background is a light grey.

# СОДЕРЖАНИЕ

п.

Больше материалов: [Boosty](#) | [Sponsr](#) | [TG](#)



## NAVIGATING THE MAZE OF INCIDENT RESPONSE

Документ содержит руководство по эффективной стратегии и тактике реагирования на инциденты (IR).

Руководство, разработанное группой реагирования на инциденты Microsoft, призвано помочь избежать распространённых ошибок и предназначено не для замены комплексного планирования реагирования на инциденты, а скорее для того, чтобы служить тактическим руководством, помогающим как группам безопасности, так и старшим заинтересованным сторонам ориентироваться в расследовании реагирования на инциденты.

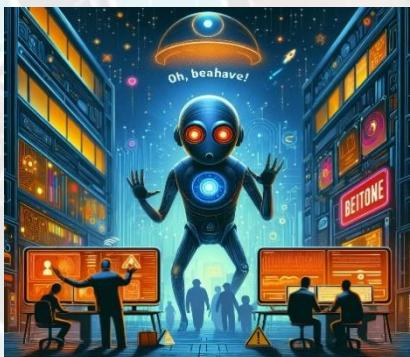
В руководстве также подчёркивается важность управления и роли различных заинтересованных сторон в процессе реагирования на инциденты.



## RISK-BASED APPROACH TO VULNERABILITY PRIORITIZATION

В документе уделяется внимание риск-ориентированному подходу к задаче управления уязвимостями. И всё это в мире, где количество уязвимостей настолько велико, что это может довести любого, кто попытается их все исправить, до нервного срыва. Решение видится «радикальным» и инновационным — расставлять приоритеты на основе реального риска, а не просто бегать, как безголовый всадник, пытаясь справиться с оценкой CVSS. В документе признается абсурдность традиционного подхода "это надо было исправить ещё вчера", учитывая, что только 2–7% опубликованных уязвимостей когда-либо эксплуатировались.

Документ в очередной раз пытается продать идею работать умнее, а не усерднее, в кибербезопасном эквиваленте бесконечной игры в тетрис, где фигуры с уязвимостями просто летят все быстрее и быстрее.



## CYBSAFE-ОН, BEHAVE! 2023

Документ представляет исследование текущего состояния осведомлённости, отношения и поведения пользователей в области кибербезопасности. Отчёт с долей иронии показывает, что, хотя большинство людей осведомлены о рисках кибербезопасности, они не всегда предпринимают необходимые шаги для собственной защиты. Например, только 60% используют надёжные пароли, и лишь 40% используют многофакторную аутентификацию. В отчёте также подчёркиваются некоторые различия поколений в отношении и поведении к кибербезопасности. Z и миллениумы, в большей степени вовлечены в цифровые технологии, но также более рискованно используют пароли и более скептически относятся к ценности мер по обеспечению безопасности. В двух словах, отчёт представляет собой всесторонний анализ текущего состояния осведомлённости, отношения и поведения пользователей Интернета в области кибербезопасности на результаты которого без сарказма не взглянешь.

## ПАТЕНТ US20220232015A1: PREVENTING CLOUD-BASED PHISHING ATTACKS USING SHARED DOCS WITH MALICIOUS LINKS

Ещё один патент, который обещает революционизировать захватывающий мир сетевой безопасности. Приготовьтесь к истории о встроенных прокси, синтетических запросах и невероятно увлекательной логике формирования встроенных метаданных. Это похоже на комикс, но вместо супергероев у нас есть компоненты сетевой безопасности, которые спасают положение. В чём суть этого технологического чуда? По сути, это прославленный вышибала для вашей корпоративной сети, решающий, какие файлы документов будут выставлены напоказ на цифровой красной дорожке, а какие будут загружены.



## ИСТОЧНИКИ ИННОВАЦИОННОСТИ Китая (ПО ВЕРСИИ DGAP)



Пристегнитесь, потому что мы собираемся отправиться в захватывающее путешествие по мистической стране инноваций Китая, где драконы прошлого превратились в единорогов мира технологий. Да, мы говорим о превращении Китая из любой в мире машины Херох в сияющий маяк инноваций. И как им удалось совершить этот удивительный подвиг?

Ведь теперь Запад сидит в стороне, заламывая руки и задаваясь вопросом: "Должны ли мы вскочить в уходящий поезд или придерживаться другого плана действий?" Оказывается, Запад ещё не полностью перехитрили, и у него все ещё есть несколько козырей в рукаве. В статье проповедуется, что сидеть и смотреть не самый разумный выбор. Вместо этого Западу следует напрячь свои демократические мускулы и чутье свободного рынка, чтобы остаться в игре.

## ЧЕМУ ЖЕ УЧИТ СТАНОВЛЕНИЕ КИТАЯ КАК СТАНОВЛЕНИЕ ИННОВАЦИОННОЙ ДЕРЖАВЫ (ПО ВЕРСИИ DGAP)

Помните, когда Запад посмеивался при одной только мысли о том, что Китай является лидером в области инноваций? Очередная статья, чтобы напомнить, что Китай был занят ещё и внедрением инноваций, давая Кремниевой долине возможность заработать свои деньги. Поэтому в статье рассказывается о замедлении экономического роста, которые могут помешать их параду инноваций. И давайте не будем забывать о законе о шпионаже, из-за которого западные компании трясутся от страха, слишком напуганные, чтобы сунуть нос на китайский рынок, ну или потому что не особо уже нужны на этом рынке. И поэтому также утверждается, что несмотря на планы Китая стать самодостаточным, он не может избавиться от своей зависимости от западных технологий.



## ПОЧЕМУ ВЕЛИКИЕ ДЕРЖАВЫ ЗАПУСКАЮТ РАЗРУШИТЕЛЬНЫЕ КИБЕР-ОПЕРАЦИИ И ЧТО С ЭТИМ ДЕЛАТЬ (ПО ВЕРСИИ DGAP)

Здесь мы имеем дело со экспертами по международным отношениям (DGAP), мастерами геополитической проницательности, которые почему-то продают очевидное блюдо в своей очередной публикации. Захватывающая история о том, как большие, плохие страны пытаются посеять хаос среди менее (технологически) удачливых. И что же они предлагают с этим делать? Анализируйте, прогнозируйте и разрабатывайте стратегию. Действительно, новаторское решение.

Вся статья выглядит как рассказ о кризисе среднего возраста: с аспектами кибербезопасности умных городов и экзистенциальным страхом перед технологической зависимостью. Для усиления эффекта они связывают кибервойны и распространение оружия массового уничтожения. Автор указывает на хорошее (блестящие новые технологии), плохое (эти надоедливые, постоянные угрозы) и уродливое (преступные организации с большими амбициями, чем у стартапа из Кремниевой долины).

Итак, вот он, мастер-класс по констатации очевидного с долей пост-иронии. Помните, когда дело доходит до кибервойны, дело не в размере вашего цифрового арсенала, а в том, как вы его используете. По крайней мере, нам так говорят.



## РОССИЯ СТРЕМИТСЯ ПОСТРОИТЬ ПОЛНОСТЬЮ КОНТРОЛИРУЕМУЮ ГОСУДАРСТВОМ ИТ-ЭКОСИСТЕМУ (ПО ВЕРСИИ DGAP)

Очередная скандальная статья DGAP просто переполнена интригой, ревностью и завистью. Как можно было даже пытаться создать свою собственный цифровой мир, свободный от тисков этих назойливых западных технологий и сервисов. Особенно на фоне того, что люди начали беспокоиться о конфиденциальности данных и уже подают в суд направо и налево бедных гигантов Кремниевой долины. Сегодня виновник торжества – компания "Вконтакте", скромный сервис, превратившийся в цифровой конгломерат. "Да как он посмел" возмущается автор, «сделать жизнь своих соотечественников более комфортной, удобной и безопасной». А смелость и наглость развивать цифровую экосистему, включающую в себя множество сервисов, потенциально используемых каждым гражданином, просто поражает.

Вся статья рассказывает о том, как западным странам неприятно видеть, что Россия пожинает плоды этой ИТ-экосистемы. Они добились цифрового суверенитета, расширили свои возможности управления информацией и даже повысили устойчивость к экономическим санкциям. Поэтому автор отмечает, что это просто несправедливо, что России удалось использовать свою ИТ-экосистему в интересах различных отраслей внутри страны, таких как электронная коммерция, финансовые услуги, телекоммуникации, СМИ и развлечения, образование и здравоохранение.



## CYBER DEFENSE DOCTRINE

В постоянно развивающемся мире ИБ, где цифровая сфера устойчива, как карточный домик во время урагана, появился новаторский документ под названием "Доктрина киберзащиты", которая управляет рисками: полное прикладное руководство по организационной киберзащите", предположительно написанный израильским Сунь Цзы из эпохи цифровых технологий.

Доктрина, являющаяся шедевром кибернетической мудрости, делит свои стратегии оценки рисков и управления ими на два направления, вероятно, потому что одно из них является слишком уже не модно. Эти направления изобретательно основаны на потенциальном ущербе для организации – новой концепции, для воплощения которой, должно быть, потребовалось как минимум несколько сеансов мозгового штурма за чашкой кофе.

Как принято сегодня говорить, доктрина является ярким примером приверженности индустрии киберзащиты ... к тому, чтобы как можно подробнее изложить очевидное. Она убеждает нас в том, что перед лицом киберугроз мы всегда можем положиться на объёмные документы, которые защитят нас.



## СТЕМ: CONTINUOUS THREAT EXPOSURE MANAGEMENT

Давайте погрузимся в захватывающий мир непрерывного управления воздействием угроз (СТЕМ). СТЕМ, в своей бесконечной мудрости, — это сложная пятиэтапная программа, которая упростит ваше погружение в бюрократический кошмар.

Сначала у нас есть определение области применения, когда вы притворяйтесь, что знаете, что делаете, определяя первоначальную область воздействия. Затем вы играете в цифрового детектива и охотитесь за уязвимостями. Следующим этапом является определение приоритетов, когда вы решаете, какие цифровые пожары тушить в первую очередь. Валидация — это проверка вашей работы, чтобы убедиться, что вы не сделали только хуже. И, наконец, последним этапом, когда вы сплачиваетесь и надеетесь на лучшее.

Отмечается роль отраслевых практик, в частности регулярности обновления систем, потому что хакеры строго придерживаются графика и будут терпеливо ждать, пока вы все исправите. План реагирования на инциденты также имеет ключевое значение, потому что, когда что-то неизбежно пойдёт не так, вам понадобится план, позволяющий делать вид, что у вас все под контролем. Наконец, решающее значение имеет постоянное совершенствование. В конце концов, единственное, что остаётся неизменным в кибербезопасности, — это факт, что вы всегда на шаг позади от последней угрозы.



## КОМПАНИИ, ВОВЛЁЧЁННЫЕ В РАЗЛИЧНЫЕ КИБЕР-АКТИВНОСТИ. ЧАСТЬ 1

Ах, этот мир частных ИБ компаний, где позиция между белыми и черными шляпами их руководителей и сотрудников так денежно-зависима как swing-state перед выборами.

Эти предпримчивые компании торгуют цифровыми секретными технологиями, предлагая все — от программных имплантов до наборов для взлома, от экспloitов 0day до методов обхода систем безопасности. Большинство из них участвовали в наступательных кибер-операциях национальных государств, что является всего лишь причудливым способом сказать, что они помогают правительствам шпионить друг за другом и превращают паранойю в прибыль, и все, что для этого потребовалось, — это немного творчества и гибкий моральный компас.



## ПЕРСПЕКТИВЫ КИБЕРБЕЗОПАСНОСТИ В ТИХООКЕАНСКОМ РЕГИОНЕ (АРАС)

В этом году АРАС стал звездой бала кибератак, на его долю пришлось 31% всех кибератак в мире, а 60% респондентов АРАС, которые не спали по ночам, беспокоились о взломе сети как об угрозе нацбезопасности. Неожиданным событием стало то, что только 50% организаций Азиатско-Тихоокеанского региона имели официальный план реагирования на программы-вымогатели. И этот показатель ещё вырос на 47% с прошлого года.

Остаётся только надеяться, что усилия по обеспечению кибербезопасности в регионе будут наращиваться быстрее, чем мышцы у бодибилдера, принимающего стероиды. В противном случае кибер-угрозы 2023 года запомнятся тем, что они вызвали массовый «взрыв» в этом регионе.



## РЫНОК КИБЕРСТРАХОВАНИЯ

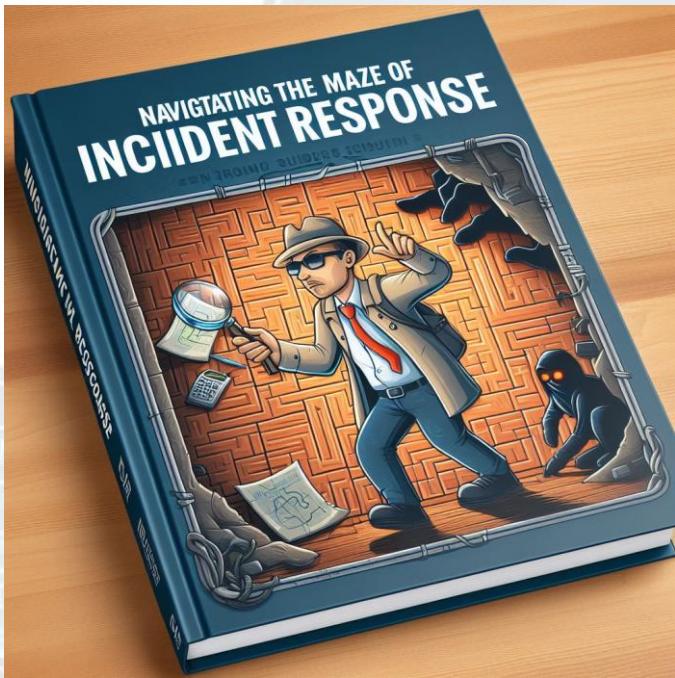
Рынок киберстрахования — это восхитительный парадокс, когда компании выкладывают большие деньги, чтобы защитить себя от тех самых технологий, без которых они не могут жить. Рынок превратился из нишевого продукта в многомиллиардную индустрию, доказав, что ничто так не способствует открытию кошельков, как глобальная цифровая пандемия. Используя данные для стимулирования андеррайтинга, компании по киберстрахованию теперь могут предлагать покрытие без ценников, которые отпугивают клиентов.

В 2024 году, после нескольких лет роста страховых взносов, рынок киберстрахования решил удивить всех, смягчив условия. Но не стоит слишком радоваться, по-прежнему существует проблема системных киберрисков, которые не покрываются страховыми взносами.

NAVIGATING THE MAZE OF  
**INCIDENT RESPONSE**



**III. NAVIGATING  
INCIDENT RESPONSE**



## A. Введение

Документ Microsoft "Navigating Incident Response" представляет собой руководство, призванное помочь организациям разобраться в сложностях реагирования на инциденты (IR). В нем подчёркивается неизбежность инцидентов в области кибербезопасности и важность запуска IR с полным пониманием необходимых действий, сроков и вовлечённых сторон. В руководстве основное внимание уделяется людям и процессам, имеющим решающее значение для эффективного реагирования.

Углубляясь в анализ этого документа, ниже будет представлено качественное изложение его ключевых рекомендаций и стратегий, направленных на то, чтобы снабдить организации знаниями для быстрого сдерживания участников угроз и минимизации воздействия на бизнес, сохраняя при этом фактические данные и понимая соответствие требованиям и нормативных обязательств.

## B. Ключевые тезисы

### 1) Ключевые моменты:

- Инциденты кибербезопасности неизбежны, и наличие проработанного плана реагирования имеет решающее значение для быстрой локализации и восстановления
- Люди и процессы лежат в основе эффективного реагирования на инциденты с чёткими ролями, обязанностями и стратегиями управления
- Методологии реагирования на инциденты разработаны на базе и с использованием NIST
- Управление является ключевым, при этом такие роли, как руководитель управления, менеджер инцидентов и руководитель расследования, имеют решающее значение для структуры реагирования

- Коммуникация необходима, как внутренняя, так и внешняя, для управления сообщениями во время инцидента
- Сохранение и сбор доказательств являются приоритетными для проведения всестороннего расследования и составления полной картины инцидента
- Планирование смен и привлечение поставщиков важны для обеспечения поддержки в разных часовых поясах и со стороны сторонних ИТ-служб
- SITREP-отчёты обеспечивают активную коммуникацию с заинтересованными сторонами, поддерживая единый источник об инциденте
- Криминалистическое расследование должно быть скоординированным, с определением приоритетов задач на основе риска и включать упреждающий сетевой мониторинг
- Использование защищённых каналов взаимодействия для обеспечения конфиденциальности на период разрешения инцидентов
- При планировании восстановления следует учитывать долгосрочное восстановление и ужесточение службы на основе выявленных рисков и пробелов в безопасности
- Нормативные и юридические обязательства должны быть поняты и учтены на ранних стадиях процесса реагирования

### 2) Основные выводы:

- Только четверть организаций имеют постоянный план реагирования на инциденты
- Распространённые ошибки при реагировании на инциденты включают неэффективное устранение неполадок, непреднамеренное уничтожение доказательств, отсутствие документации и отказ от взаимодействия с поставщиками и юристом на раннем этапе
- Привлечение поставщика имеет решающее значение для сбора доказательств и поддержки во время инцидента, а упреждающее участие обеспечивает приоритизацию запросов
- Подходы к противодействию должны быть адаптированы к типу инцидента с учётом воздействия на бизнес и потенциального оповещения субъекта угрозы
- Активные коммуникации играют важную роль в контроле обмена данными и реагировании на запросы о предоставлении информации, обеспечивая последовательность и согласованность с расследованием
- Правовые и нормативные соображения сложны и варьируются в зависимости от юрисдикции, что требует заблаговременного привлечения юриста для представления обязательной отчётности и соблюдения требований

### 3) Ключевые действия и точки приложения

- **Создание структуры управления инцидентами:** в начале инцидента важно разработать модель реагирования для управления инцидентом. Это включает в себя определение ключевых заинтересованных сторон, которые могут помочь сформировать структуру реагирования
- **Определение потенциальных клиентов:** в руководстве предлагается определять потенциальных клиентов в различных рабочих потоках, таких как управление, контроль инцидентов, расследования, инфраструктура, коммуникация и соответствие нормативным требованиям
- **Вовлечение заинтересованных сторон:** руководящему составу следует заблаговременно уведомлять заинтересованные стороны и членов команды исполнительного руководства о реагировании на инциденты
- **Выделение ресурсов:** по возможности следует выделять ресурсы для реагирования или, как минимум, направлять на приоритизацию действий по реагированию по сравнению с другими задачами

#### 4) Лучшие практики

- **Сохранение доказательств:** помимо понимания масштабов компромисса и способов восстановления контроля, важно сохранить доказательства и понимать обязательства по соблюдению нормативных требований.
- **Поддерживание прозрачности и понимания риска:** руководству следует осуществлять надзор за реагированием, чтобы иметь предметное представление о риске, связанном с инцидентом. Это должно поддерживаться на протяжении всего процесса реагирования с помощью отчётов о ситуации, подготовленных менеджером инцидентов
- **Взаимодействие с главными владельцами (ресурсов):** руководитель управления должен оказывать поддержку, если группа реагирования сталкивается с проблемой, которая не может быть решена на оперативном уровне. Типичные проблемы могут включать запросы ресурсов от других подразделений бизнеса, увеличение количества запросов к поставщикам и другим третьим сторонам, а также решения, которые имеют широкомасштабное влияние на бизнес
- **Управление рабочим потоком и распределение задач:** с какого-то момента документирование действий и задач часто утрачивает приоритетность в пользу быстрого реагирования. Но в дальнейшем это может создавать проблемы. Поэтому важно документировать действия и задачи с начала

#### C. План реагирования на инциденты

План реагирования на инциденты (IRP) – это структурированный подход к обработке инцидентов безопасности, брешей и киберугроз. Чётко определённый

IRP может помочь организациям свести к минимуму потерю и кражу данных, смягчить последствия кибератак и сократить время восстановления и затраты. К ключевым компонентам IRP относятся:

- **Подготовка:** включает в себя создание группы реагирования на инциденты, определение их ролей и обязанностей, а также проведение необходимого обучения, подготовку необходимых инструментов и ресурсов для обнаружения инцидентов и реагирования на них.
- **Обнаружение:** этап включает выявление потенциальных инцидентов безопасности, обычно с помощью систем обнаружения вторжений, брандмауэров или систем предотвращения потери данных (DLP).
- **Локализация:** после обнаружения инцидента необходимо предпринять шаги для предотвращения дальнейшего ущерба. Это может включать изоляцию затронутых систем или сетей, чтобы предотвратить распространение инцидента.
- **Устранение:** включает в себя поиск основной причины инцидента и удаление затронутых систем из сети для проведения криминалистического анализа.
- **Восстановление:** восстановление и возвращение системы к нормальной работе возможно в отсутствии следов инцидента. Это может включать исправление программного обеспечения, очистку систем или даже переустановку целых систем.
- **Действия после инцидента:** после рассмотрения инцидента следует провести анализ для повышения эффективности реагирования в будущем. Это может включать обновление IRP, внедрение новых мер безопасности или проведение дополнительного обучения для персонала

При рассмотрении инструментов реагирования на инциденты организации должны учитывать несколько ключевых соображений для обеспечения эффективного реагирования на инциденты кибербезопасности:

##### 1) Интеграция с существующими системами

Инструменты реагирования на инциденты должны быть способны легко интегрироваться с существующей инфраструктурой безопасности организации, такой как брандмауэры, системы обнаружения вторжений и решения SIEM. Такая интеграция позволяет осуществлять автоматический сбор и корреляцию данных, что может ускорить обнаружение и анализ инцидентов безопасности.

##### 2) Масштабируемость

Инструменты должны быть масштабируемыми для обработки объёма данных и количества конечных точек внутри организации. По мере роста организации инструменты должны быть способны обрабатывать все больший объём данных и расширять сеть без снижения производительности.

##### 3) Сохранение доказательств

Во время инцидента сохранение улик имеет решающее значение для тщательного расследования и возможного криминалистического разбирательства. Инструменты реагирования на инциденты должны способствовать сбору и сохранению цифровых доказательств с точки зрения криминалистической экспертизы, гарантируя, что они остаются приемлемыми в суде, если это необходимо.

#### 4) Мониторинг и оповещение в режиме реального времени

Возможность отслеживать сеть в режиме реального времени и формировать оповещения о подозрительных действиях имеет важное значение. Это позволяет быстро выявлять потенциальные угрозы и реагировать на них до того, как они смогут нанести значительный ущерб.

#### 5) Автоматизация и управление

Автоматизация повторяющихся задач и координация ответных действий могут значительно повысить эффективность процесса реагирования на инциденты. Инструменты, обеспечивающие автоматизированные рабочие процессы, могут помочь сократить время на реагирование и смягчение последствий угроз, а также свести к минимуму вероятность человеческой ошибки.

#### 6) Удобный интерфейс

Инструменты должны иметь интуитивно понятный и удобный интерфейс, позволяющий специалистам быстро ориентироваться и эффективно использовать функции, особенно в условиях активного инцидента.

#### 7) Подробная отчетность

Инструменты должны обеспечивать комплексные возможности отчётности, позволяющие проводить подробный анализ и документировать инциденты. Это важно для анализа последствий, соблюдения нормативных требований и улучшения системы безопасности организации.

#### 8) Индивидуальность и гибкость

У каждой организации свои уникальные потребности. Инструменты реагирования на инциденты должны настраиваться в соответствии с конкретными процессами организации. Они также должны быть достаточно гибкими, чтобы адаптироваться к меняющемуся ландшафту угроз и организационным изменениям.

#### 9) Поддержка поставщиков и сообщества

Надёжная поддержка поставщиков и активное сообщество пользователей могут стать бесценными ресурсами для устранения неполадок, обмена передовым опытом и получения информации о последних угрозах и стратегиях реагирования.

#### 10) Соблюдение требований законодательства и нормативов

Инструменты должны помочь организациям соблюдать правовые и нормативные требования, связанные с реагированием на инциденты, такие как обязательная отчётность и правила конфиденциальности. Это включает в себя функции, которые поддерживают управление нормативными / правовыми требованиями и облегчают взаимодействие с юрисконсультом, когда это необходимо.

### D. Роли и обязанности

Модифицированная версия модели жизненного цикла реагирования на инциденты, задокументированной Национальным институтом стандартов и технологий (NIST) обычно включает подготовку, обнаружение, локализацию, ликвидацию, восстановление и действия после инцидента или извлечённые уроки. В связи с этим предлагается модель реагирования для управления инцидентом, которая включает следующие роли:

- **Руководитель управления:** эту роль обычно выполняет CISO или СИО. Они поддерживают прозрачность рисков и влияние на бизнес в целом, а также общаются с высокопоставленными заинтересованными сторонами
- **Менеджер инцидентов:** эту роль обычно выполняет руководитель ITSM / операций по обеспечению безопасности. Он координирует все оперативные рабочие процессы для понимания и сдерживания угрозы, а также доводит информацию о риске до руководства
- **Руководитель расследования:** эту роль обычно выполняет старший специалист по информационным технологиям / старший представитель по ИТ-операциям. Он отвечает за понимание общего компромисса и информирование о связанных с ним рисках
- **Руководитель инфраструктуры:** эту роль обычно выполняет старший представитель по ИТ-операциям. Он несёт ответственность за сдерживание угрозы путём снижения риска, связанного с компромиссом
- **Менеджер по коммуникациям:** эту роль обычно выполняет специалист по коммуникациям. Он контролирует обмен данными как внешне, так и внутренне
- **Руководитель отдела регулирования:** эту роль обычно выполняет внутренний юрисконсульт / представитель GRC. Он отвечает за оценку рисков / воздействия и управление нормативными / правовыми требованиями для поддержания соответствия

### Рекомендуемые наборы навыков для работы:

- **Руководитель управления:** оперативный надзор, поддержание прозрачности, понимание рисков и последствий, а также общение с высокопоставленными заинтересованными сторонами
- **Менеджер инцидентов:** оперативное управление и постановка задач, координация всех операционных рабочих потоков и информирование руководства о рисках
- **Руководитель расследования:** криминалистическое расследование для понимания общего компромисса и информирования о связанных с ним рисках

- **Руководитель инфраструктуры:** сдерживание угроз за счёт снижения риска, связанного с компромиссом
- **Менеджер по коммуникациям:** вовлечение заинтересованных сторон и контроль обмена сообщениями как внешними, так и внутренними
- **Руководитель отдела регулирования:** Оценка рисков / последствий и управление нормативными / правовыми требованиями для поддержания соответствия

Обеспечение эффективного плана реагирования на инциденты:

- **Регулярное обновление плана:** обновление плана реагирования на инциденты с учётом меняющегося ландшафта угроз и организационных изменений
- **Тренинги:** проведение регулярных тренингов симуляций для проверки плана и определения областей для улучшения
- **Коммуникация:** установление и поддерживание чётких каналов коммуникации для всех заинтересованных сторон, участвующих в реагировании на инцидент
- **Документирование:** все действия и решения должны быть задокументированы, чтобы избежать путаницы и неэффективности
- **Взаимодействие с поставщиками:** активное взаимодействие с поставщиками для поддержки сбора доказательств и других мероприятий по реагированию
- **Планирование смен:** внедрение планирования смен, чтобы предотвратить выгорание и поддерживать непрерывное реагирование в различных временных зонах

### 1) Руководитель управления

Руководитель управления, которым может быть CISO или СИО, отвечает за оперативный надзор. Его роль заключается в поддержании прозрачности и понимания рисков и их влияния на бизнес в целом, а также в общении с высокопоставленными заинтересованными сторонами. Представитель этой роли должен заблаговременно уведомить заинтересованные стороны и членов команды исполнительного руководства о том, что принимаются серьёзные ответные меры. Это гарантирует, что другие подразделения бизнеса будут осведомлены о потенциальном риске и о том, что во время управления инцидентом могут произойти сбои в обслуживании.

Представитель роли также должен обеспечить выделение специальных ресурсов для принятия ответных мер. Организации, не имеющие выделенных групп безопасности, часто привлекают ресурсы из других подразделений бизнеса для оказания помощи в реагировании. Затем этим сотрудникам необходимо сбалансировать свою существующую рабочую нагрузку с мероприятиями по реагированию. По возможности, для реагирования следует выделять специальные ресурсы или, как минимум, направлять их на приоритизацию

мероприятий по реагированию по сравнению с другой работой

Руководитель управления также является связующим звеном группы реагирования как с внутренними, так и с внешними высокопоставленными заинтересованными сторонами. Если группа реагирования сталкивается с проблемой, которая не может быть решена на оперативном уровне, представитель роли должен оказать поддержку. Типичные проблемы включают запросы ресурсов от других подразделений бизнеса, увеличение количества запросов к поставщикам и другим третьим сторонам, а также утверждение решений, которые имеют широкомасштабные последствия для бизнеса, такие как массовый сброс паролей или отключение подключения к Интернету, и т.д.

### 2) Менеджер инцидентов

Менеджер инцидентов обычно является руководителем ITSM / операций по обеспечению безопасности, основными обязанностями которого являются оперативное управление и постановка задач. Эта роль включает в себя координацию всех операционных потоков работы для понимания, сдерживания и информирования Руководства об угрозе.

Менеджер инцидентов отвечает за управление и отслеживание задач для всех операционных рабочих потоков, чтобы обеспечить приоритетность и документирование действий.

Менеджер инцидентов также играет ключевую роль в поддержании прозрачности и понимания риска. Он готовит отчёты о ситуации для руководителя управления, чтобы иметь предметное представление о риске, связанном с инцидентом

В случае возникновения проблем, которые не могут быть решены на оперативном уровне, менеджер инцидентов инициирует запросы к руководству. Типичные проблемы, которые могут потребовать такого увеличения, включают запросы ресурсов от других подразделений бизнеса, увеличение количества запросов к поставщикам и другим третьим сторонам, а также решения, которые оказывают широкомасштабное влияние на бизнес, такие как массовый сброс пароля или отключение Интернета

Менеджер инцидентов играет ключевую роль в процессе реагирования на инциденты, отвечая за оперативное управление, постановку задач и информирование об угрозах, а также за доведение основных проблем до руководства

### 3) Руководитель расследования

Руководитель расследования, как правило, старший специалист IR / Senior IT Operations, отвечает за проведение криминалистических расследований для понимания общего компромисса и информирования о связанных с ним рисках. Эта роль имеет решающее значение для определения масштаба, воздействия и первопричины инцидента, что определяет стратегию реагирования и помогает предотвратить подобные инциденты в будущем.

Ожидается, что представитель роли будет иметь серьёзное представление об ИТ-среде организации и ландшафте угроз. Представитель роли должен обладать навыками цифровой криминалистики и реагирования на инциденты (DFIR), а также уметь использовать различные инструменты и методы для анализа системных журналов, сетевого трафика и других данных для выявления признаков компрометации (IoC).

Представитель роли тесно сотрудничает с менеджером инцидентов, регулярно предоставляя обновлённую информацию о ходе расследования и его выводах, что имеет значение для поддержания прозрачности инцидента и понимания связанного с ним риска.

В рамках роли может потребоваться сотрудничество с внешними организациями, например правоохранительными органами или сторонними поставщиками, особенно в случаях, связанных с юридическими вопросами или специализированной технической экспертизой.

Представитель играет решающую роль в реагировании на инцидент в рамках своего технического опыта для понимания инцидента, разработки стратегии реагирования и информирования о риске менеджера инцидентов и руководителя управления.

#### 4) Руководитель инфраструктуры

Эту роль обычно выполняет старший представитель по ИТ-операциям, который отвечает за сдерживание угрозы путём снижения риска, связанного с компрометацией.

Основная ответственность представителя роли заключается в сдерживании угроз — это принятие мер по ограничению распространения и воздействия инцидента безопасности в ИТ-инфраструктуре организации. Эта роль имеет решающее значение для управления техническими аспектами реагирования на инцидент и обеспечения эффективного сдерживания угрозы для предотвращения дальнейшего ущерба.

Важность наличия выделенных ресурсов для каждой роли в структуре реагирования на инциденты означает, что лица, назначенные на эти роли, должны отдавать приоритет действиям по реагированию нежели другим задачам.

Что касается необходимых навыков, руководитель инфраструктуры должен обладать опытом, а также некоторыми знаниями в области операций по обеспечению безопасности, управления рисками и цифровой

криминалистики. В документе представлена матрица навыков, в которой описываются требуемые и необязательные наборы навыков для каждой роли.

#### 5) Менеджер по коммуникациям

Эта роль отвечает за контроль как внутренних, так и внешних сообщений кибербезопасности во время инцидента.

Специалист по коммуникациям является частью более крупной структуры реагирования на инциденты, которая включает в себя других руководителей.

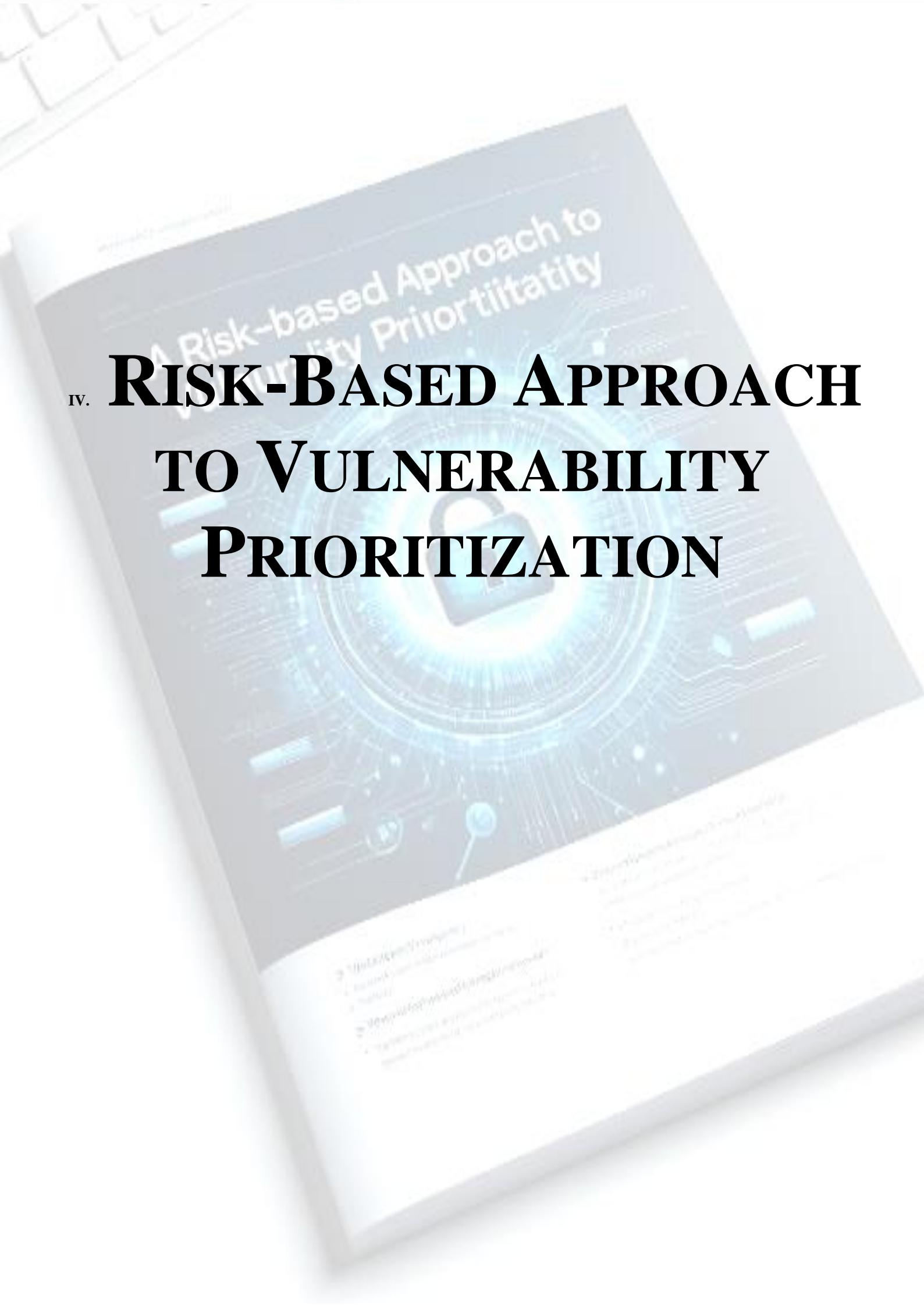
Руководитель отдела коммуникаций, в частности, отвечает за взаимодействие с заинтересованными сторонами. Основная задача — контролировать обмен сообщениями как внешне, так и внутренне. Это включает в себя информирование о статусе и деталях инцидента соответствующих заинтересованных сторон внутри организации и за её пределами, обеспечивая распространение точной и своевременной информации. Это может помочь поддерживать доверие и предотвращать распространение дезинформации.

Руководитель отдела коммуникаций также тесно сотрудничает с руководителем управления, который обеспечивает прозрачность и понимание рисков, связанных с инцидентом. Роль отвечает за оперативный надзор, обеспечение прозрачности ответных мер и понимание риска и воздействия на бизнес в целом.

#### 6) Руководитель отдела регулирования

Эту роль обычно выполняет внутренний юрисконсульт или представитель по вопросам управления, рисков и комплаенса (GRC). Основными обязанностями являются проведение оценки рисков и воздействия, а также управление нормативными и правовыми требованиями для обеспечения соответствия во время инцидента в области кибербезопасности.

Роль имеет значение для обеспечения соответствия реакции организации на инцидент кибербезопасности законодательным и нормативным требованиям. Это может включать обязательства в соответствии с законами о защите данных, отраслевыми нормативными актами или договорными обязательствами. Роль также связана с поддержанием связи с регулирующими органами по мере необходимости и управление любыми юридическими последствиями инцидента.



# **IV. RISK-BASED APPROACH TO VULNERABILITY PRIORITIZATION**



#### A. Введение

В документе "Health-ISAC: Risk-Based Approach to Vulnerability Prioritization", обсуждается важность определения приоритетов уязвимостей в управлении кибербезопасностью и подчёркивается необходимость совершенствования процессов управления уязвимостями и отказа от классических решений и систем. Вместо этого предлагается, чтобы организации внедряли решения, помогающие в расстановке приоритетов и управлении уязвимостями.

Этот документ подлежит тщательному анализу с уделением особого внимания многогранным аспектам управления уязвимостью в секторе здравоохранения. В ходе анализа будут рассмотрены стратегии и структуры, рекомендованные для эффективного определения приоритетов уязвимостей, задача, которая становится все более сложной.

Этот документ содержит практическое руководство по определению приоритетов уязвимостей. Хотя у него есть некоторые недостатки и ограничения, он может стать ценным ресурсом для организаций, стремящихся улучшить свои процессы.

#### B. Преимущества

- Риск-ориентированный подход:** в документе подчёркивается риск-ориентированный подход к управлению уязвимостями, который может помочь организациям сосредоточиться на наиболее критичных из них, представляющих наибольшую угрозу
- Полнота изложения:** документ включает различные методы, такие как базовая оценка CVSS, с упором на известные эксплуатируемые уязвимости, с учётом контекста устройства или размещения, стоимости активов, компенсирующих элементов управления и с использованием таких

инструментов, как EPSS (система оценки прогнозирования экспloitов) и SSVC (классификация уязвимостей для конкретных заинтересованных сторон)

- Практическое руководство:** документ предлагает практическое руководство по внедрению этих методов и инструментов, облегчающее организациям внедрение этих практик

#### C. Недостатки

- Ресурсоёмкость:** внедрение методов и инструментов, предложенных в документе, может быть ресурсоёмким, требующим значительного времени, усилий и опыта
- Сложность:** подход документа сложен, и его внедрение может оказаться сложной задачей для небольших организаций или тех, у кого менее зрелые команды безопасности

#### D. Ограничения

- Зависимость от точных данных:** эффективность методов и инструментов, предложенных в документе, зависит от доступности и точности данных. Например, для определения приоритета стоимости активов требуется точная и согласованная величина воздействия на бизнес для каждой компании
- Динамический ландшафт угроз:** подход документа может не учитывать динамический характер ландшафта угроз. Постоянно появляются новые уязвимости и угрозы, которые могут потребовать внесения корректировок в структуру расстановки приоритетов
- Человеческий фактор:** хотя в документе предлагаются методы устранения человеческого фактора при определении приоритетов, человеческое суждение по-прежнему имеет решающее значение во многих аспектах управления уязвимостями, например, определение эффективности компенсирующих средств контроля или интерпретация результатов таких инструментов, как EPSS и SSVC
- Зависимость от оценки CVSS:** в документе обсуждается использование Общей системы оценки уязвимостей (CVSS) в качестве основы. Хотя CVSS является широко признанным стандартом, его критиковали за то, что он неточно отражает реальный риск уязвимостей. Документ признает это и предлагает использовать дополнительные инструменты, такие как система оценки прогнозирования экспloitов (EPSS) и классификация уязвимостей для конкретных заинтересованных сторон (SSVC), но зависимость от CVSS все ещё можно рассматривать как ограничение
- Отсутствие практических примеров:** хотя документ предоставляет всеобъемлющую теоретическую основу для определения приоритетов уязвимостей, ему могли бы помочь более практические примеры или тематические исследования, иллюстрирующие, как эти концепции могут применяться в реальных сценариях

## E. Концепции документа

Основные идеи:

- **Использование базовой оценки CVSS:** общая система оценки уязвимостей (CVSS) — это стандарт, используемый для оценки критичности и возможности использования уязвимостей. Однако только 2–7% всех опубликованных уязвимостей когда-либо использовались в реальном времени, часто из-за отсутствия расстановки приоритетов
- **Сосредоточение внимания на известных эксплуатируемых уязвимостях:** предлагается более риск-ориентированный подход с упором на известные эксплуатируемые уязвимости. Агентство по кибербезопасности и инфраструктурной безопасности (CISA) опубликовало список известных уязвимостей с использованием эксплойтов (KEV), чтобы помочь организациям расставить приоритеты в их усилиях по исправлению
- **Контекст или размещение устройства:** сетевое местоположение устройства является критическим фактором при определении приоритета уязвимости. Уязвимости и неправильные настройки, связанные с Интернетом, всегда должны быть приоритетом, в то время как внутренние активы должны подпадать под сроки исправления по внутреннему соглашению об уровне обслуживания (SLA)
- **Стойкость активов:** стоимость активов является ещё одним важным фактором при определении приоритетов уязвимости, о чём должны быть поставлены в известности аналитики
- **Компенсирующие средства контроля:** в большинстве организаций используются многоуровневые средства контроля безопасности или стратегии углублённой защиты для предотвращения атак. Эти средства контроля безопасности должны затруднить использование уязвимостей
- **EPSS – Система оценки прогнозирования эксплойтов:** EPSS – это модель машинного обучения, которая предсказывает вероятность того, что уязвимость будет использована в реальности. Это помогает более эффективно расставлять приоритеты в усилиях по устранению уязвимостей
- **SSVC – с конкретными заинтересованными сторонами уязвимости классификации:** SSVC фокусируется на ценностях, включая недостаток безопасности эксплуатации состояния, его влияние на безопасность, и распространённость продуктов. Это улучшает процессы управления уязвимостями и учитывает интересы различных заинтересованных сторон

## F. Использование базовой оценки CVSS

Рассматривается использование Общей системы оценки уязвимостей (CVSS) в качестве основы, особенно для организаций с небольшими группами безопасности или тех, кто находится на ранних стадиях разработки программы управления уязвимостями

- **Базовая оценка CVSS в качестве отправной точки:** для организаций с ограниченными ресурсами или тех, кто только начинает свою программу управления уязвимостями, хорошей отправной точкой может стать использование базовой оценки CVSS для определения приоритетов и устранения всех критических уязвимостей высокой степени критичности. Такой подход устраняет необходимость в человеческом суждении при определении приоритетов уязвимостей, что может быть полезно для небольших команд или тех, у кого несколько обязанностей
- **Ограничения базовой оценки CVSS:** хотя использование базовой оценки CVSS может быть хорошей отправной точкой, у неё есть свои ограничения. Например, группы по устранению неполадок могут быть столкнуты с огромным количеством проблем, на которых их просят сосредоточиться. Кроме того, субъекты угроз не всегда могут использовать уязвимости наивысшей степени критичности и вместо этого объединяют в цепочку несколько эксплойтов менее критичных уязвимостей для получения доступа к системам
- **Необходимость более риск-ориентированного подхода:** учитывая ограничения, связанные с использованием только базового скоринга CVSS предлагается более риск-ориентированный подход, который фокусируется на известных эксплуатируемых уязвимостях. Это значительно сокращает количество проблем, требующих немедленного внимания, и позволяет специалистам-практикам сосредоточиться на уязвимостях, представляющих наибольшую угрозу для организаций

Общая система оценки уязвимостей CVSS — это платформа, используемая для оценки критичности уязвимостей в системе безопасности. Для расчёта баллов используются три группы показателей: базовые, временные и показатели окружения:

- **Базовые показатели (Base Metrics):** дают оценку в диапазоне от 0 до 10, которая отражает неотъемлемые характеристики уязвимости, которые постоянны с течением времени и в разных пользовательских средах. Они разделены на две группы: показатели возможности использования (такие как вектор атаки, сложность атаки, требуемые привилегии и взаимодействие с пользователем) и показатели воздействия (которые измеряют влияние на конфиденциальность, целостность и доступность)
- **Временные показатели (Temporal Metrics):** отражают характеристики уязвимости, которые могут меняться со временем, но вне зависимости от среды пользователя. Они включают зрелость кода эксплойта, уровень исправления и достоверность отчётов. Показатели являются необязательными и используются для получения временной оценки, которая является модификацией базовой оценки
- **Показатели окружения (Environmental Metrics):** позволяют пользователю настраивать оценку CVSS в зависимости от важности затронутого

программного обеспечения, оборудования или данных в его среде. Они включают потенциальный сопутствующий ущерб, целевое распространение, Требования к конфиденциальности, целостности и доступности. Показатели являются необязательными и используются для получения оценки, которая является дальнейшей модификацией временной оценки

Базовая оценка CVSS отличается от других оценок тем, что она учитывает только неотъемлемые, неизменные характеристики уязвимости. Напротив, временная оценка учитывает факторы, которые меняются с течением времени, например, был ли разработан экспloit или доступен патч. Оценка окружения позволяет настраивать её в зависимости от важности затронутых активов в среде конкретного пользователя. Следовательно, хотя базовая оценка одинакова для всех, а другие оценки могут варьироваться в зависимости от времени и конкретной среды пользователя.

Все три показателя влияют друг на друга в том смысле, что каждая следующая является модификацией предыдущей: временная оценка является модификацией базовой оценки, а оценка окружения является модификацией временной оценки. Однако изменения в показателях окружения не влияют на другие оценки, поскольку это зависит от среды пользователя.

Базовая оценка общей системы оценки уязвимостей (CVSS) обычно не меняется с течением времени. Это статическая оценка, которая отражает критичность уязвимости на основе характеристик самой уязвимости, таких как её воздействие и возможность использования. Однако интерпретация и применение оценки CVSS может меняться с течением времени в зависимости от различных факторов.

Например, оценка CVSS может использоваться по-разному в контексте процесса управления уязвимостями организаций. Организация может определять приоритетность уязвимостей не только на основе оценок уязвимостей CVSS, но и на основе таких факторов, как то, активно ли используется уязвимость, стоимость активов, которые могут быть затронуты, наличие компенсирующих элементов управления и контекст устройства.

Более того, в дополнение к оценке CVSS могут использоваться такие инструменты, как система оценки прогнозирования эксплоитов (EPSS) и классификация уязвимостей для конкретных заинтересованных сторон (SSVC). EPSS использует модель машинного обучения для прогнозирования вероятности того, что уязвимость будет использована в реальности, обеспечивая динамический взгляд на риск, связанный с уязвимостью. SSVC, с другой стороны, фокусируется на ценностях, включая статус использования уязвимости, её влияние на безопасность и распространённость затронутых продуктов, что позволяет применять более индивидуальный подход к управлению.

#### G. Сосредоточение внимания на известных эксплуатируемых уязвимостях

Подчёркивается важность определения приоритетности известных эксплуатируемых уязвимостей при управлении рисками кибербезопасности.

- **Известные эксплуатируемые уязвимости:** в отчёте предлагается подход, основанный на оценке рисков, который фокусируется на известных эксплуатируемых уязвимостях. Подчёркивается, что менее 4% всех известных уязвимостей использовались злоумышленниками, поэтому сосредоточение внимания на них может значительно сократить количество уязвимостей, требующих немедленного внимания
- **Определение приоритетов:** в отчёте предполагается, что известные эксплуатируемые уязвимости должны быть главным приоритетом для исправления. Такой подход гарантирует, что специалисты сосредоточат своё внимание на уязвимостях, которые представляют наибольшую угрозу. Процесс, обеспечивающий безопасность организации, будет включать в себя сосредоточение внимания на списке известных эксплуатируемых уязвимостей (KEV) CISA и поворот к устранению с критическими уровнями критичности
- **Уменьшение количества уязвимостей:** эта методология значительно сокращает количество уязвимостей, требующих немедленного внимания. По состоянию на 13 июля 2023 года в списке насчитывалось менее 1000 уязвимостей. Это также позволяет специалистам сосредоточиться на уязвимостях, представляющих наибольшую угрозу для организаций
- **Обязательства по соблюдению требований:** в отчёте также отмечается, что, хотя директива помогает агентствам расставлять приоритеты в своей работе по исправлению, она не освобождает их от каких-либо обязательств по соблюдению требований, включая устранение других уязвимостей
- **Оценка CVSS:** в отчёте признается, что оценка CVSS всё ещё может быть частью усилий организации по управлению уязвимостями, особенно при межмашинной коммуникации и крупномасштабной автоматизации

Сосредоточение внимания на известных эксплуатируемых уязвимостях является важнейшим аспектом. Это позволяет организациям эффективно распределять ресурсы, снижать риски, разрабатывать эффективные стратегии, соблюдать нормативные акты, определять приоритеты с учётом угроз и защищать ценные активы:

- **Эффективное распределение ресурсов:** ежегодно выявляются тысячи уязвимостей, и организациям часто бывает трудно управлять всеми и устранять их из-за ограниченности ресурсов. Сосредоточение внимания на известных эксплуатируемых

- **Снижение риска:** известные эксплуатируемые уязвимости — это те, которые использовались злоумышленниками в реальности. Определяя приоритетность этих уязвимостей, организации могут значительно снизить свою подверженность риску.
- **Эффективные стратегии смягчения последствий и исправления ситуации:** определение приоритетности известных эксплуатируемых уязвимостей способствует разработке эффективных стратегий смягчения последствий и исправления ситуации. Это помогает командам безопасности эффективно взаимодействовать с заинтересованными сторонами, определять стоимость активов и разрабатывать политики исправления, способствующие непрерывности работы критически важных для бизнеса систем
- **Соответствие нормативным требованиям:** регулирующие органы, такие как Агентство по кибербезопасности и инфраструктурной безопасности (CISA), имеют директивы, направленные на снижение риска известных эксплуатируемых уязвимостей.
- **Определение приоритетов на основе угроз:** сосредоточение внимания на известных эксплуатируемых уязвимостях позволяет применять основанный на угрозах подход к управлению уязвимостями.
- **Защита активов:** определение приоритетности известных эксплуатируемых уязвимостей помогает защитить ценные активы. Если устройство, имеющее первостепенное значение для функционирования бизнеса или содержащее критически важную информацию, будет скомпрометировано, это может иметь катастрофические последствия для организации

#### I. Контекст, или размещение, устройства

- **Важность сетевого местоположения:** это знания имеют решающее значение для определения приоритетности уязвимостей, особенно когда речь идёт про уязвимости нулевого дня в отношении «активов», подключённых к Интернету
- **Определение приоритетности уязвимостей, связанных с Интернетом:** уязвимости и неправильные конфигурации на устройствах, подключённых к Интернету, должны быть приоритетными, поскольку они более доступны для субъектов угроз и могут служить лёгкой отправной точкой для атак. Эти уязвимости представляют собой более высокий риск компрометации и должны быть устранены незамедлительно
- **Сроки исправления внутреннего соглашения об уровне обслуживания:** для систем, которые недоступны из Интернета, таких как внутренние активы, рекомендуется, чтобы они подпадали под сроки исправления внутреннего соглашения об

уровне обслуживания (SLA). Это означает, что в зависимости от сетевого расположения активов должны устанавливаться различные SLA, при этом активы, подключённые к Интернету, имеют более короткие SLA, чем внутренние

- **Использование рейтингов приоритета уязвимостей:** большинство инструментов управления уязвимостями сегодня включают дополнительные функции оценки, такие как система оценки прогнозирования эксплойтов (EPSS), для оказания помощи аналитикам в определении приоритетов уязвимостей. Эти инструменты предоставляют рейтинги приоритета уязвимости, которые помогают определить, какие недостатки безопасности следует устраниить в первую очередь, исходя из вероятности использования в сети
- **Риск-ориентированный подход:** учитывая контекст определения местоположения устройства, организации могут действовать в соответствии с риск-ориентированным подходом к управлению уязвимостями. Такой подход гарантирует, что группы по исправлению ошибок сосредоточатся на устранении уязвимостей в зависимости от их вектора атаки, возможности использования и критичности

В контексте управления уязвимостями "контекст устройства или размещение" относится к сетевому местоположению и роли устройства, что является критическим фактором при определении приоритетов уязвимостей. Размещение устройства может существенно повлиять на уровень риска уязвимости и, следовательно, на расстановку приоритетов при усилиях по устранению неполадок.

#### 1) Примеры размещения в системе управления уязвимостями

- **Реагирование на возникающие угрозы:** организациям необходимо быстро реагировать на возникающие угрозы или критические уязвимости на общедоступных устройствах. Например, если обнаруживается новая уязвимость, затрагивающая веб-серверы, эти серверы, подключённые к Интернету, будут иметь приоритет для исправления
- **Внутренние веб-приложения:** хотя это также важно, уязвимости, влияющие на внутренние веб-приложения, могут быть устранены позже уязвимостей на серверах, подключённых к Интернету
- **Рабочие станции или сервера:** локальная уязвимость с повышением привилегий может иметь приоритет на рабочих станциях над серверами, если рабочие станции с большей вероятностью станут мишенью для фишинговых писем, учитывая контекст использования устройств

#### I. Ценность активов

Обсуждается важность понимания ценности актива в контексте определения приоритетов в отношении уязвимости.

- **Важность стоимости актива:** стоимость актива играет решающую роль в определении приоритетов уязвимости. Аналитикам необходимо понимать ценность актива в сочетании с его контекстом и размещением в сети. Это помогает определить приоритеты уязвимостей, связанных с критическими активами
- **Система ранжирования:** команды могут использовать систему ранжирования в своём репозитории приложений для определения критически важных ресурсов. Уязвимости, связанные с этими критически важными активами, должны быть приоритетными для устранения. Такой подход помогает аналитикам влиять на решения по устранению уязвимостей
- **Влияние на бизнес:** если устройство, имеющее решающее значение для функционирования бизнеса или содержащее критически важную информацию, будет скомпрометировано, это может иметь катастрофические последствия для организации. Поэтому рекомендуется уделять приоритетное внимание исправлению этих устройств по сравнению с другими. Учёт влияния на бизнес при оценке степени критичности обеспечивает более точное представление о риске для компании
- **База данных управления конфигурациями (CMDB):** для эффективной реализации этой стратегии необходима точная и согласованная величина воздействия на бизнес для каждого актива компании. В идеале эта информация должна располагаться централизованно, например, в базе данных управления конфигурацией (CMDB). Хотя большинство отраслевых продуктов CMDB предоставляют решение для обнаружения активов, помогающее поддерживать точность инвентаризации, оно лишь частично избавляет от проблем

В управлении уязвимостями стоимость активов относится к важности конкретного актива (такого как устройство, система или данные) для операций организации или непрерывности бизнеса. Это важный фактор при определении приоритетов уязвимостей, помогающий командам безопасности решать, какие уязвимости следует устраниć в первую очередь, исходя из потенциального воздействия на наиболее ценные активы организации.

Расчёт стоимости активов при управлении уязвимостями не является простым процессом и может варьироваться в зависимости от конкретного контекста и потребностей организации. Это часто включает оценку роли актива в организации, чувствительности хранящихся в нем данных, их важности для бизнес-операций и потенциального воздействия на организацию, если актив будет скомпрометирован.

На стоимость активов при управлении уязвимостями могут повлиять несколько факторов:

- **Роль актива:** функция актива в организации может в значительной степени влиять на его стоимость.

Например, сервер, на котором размещены критически важные приложения или конфиденциальные данные, обычно имеет более высокую стоимость активов, чем периферийное устройство, не имеющее доступа к конфиденциальной информации

- **Конфиденциальность данных:** активы, которые хранят или обрабатывают конфиденциальные данные, такие как персональные данные информации (РПИ), финансовые данные или служебная деловая информация, обычно имеют более высокую ценность из-за потенциального воздействия утечки данных
- **Влияние на бизнес:** потенциальное воздействие на бизнес-операции в случае компрометации актива является важным фактором. Это может включать финансовые потери, сбои в работе, ущерб репутации или юридические и нормативные последствия
- **Размещение актива:** расположение актива в сети и подверженность потенциальным угрозам также могут влиять на его стоимость. Например, активы, которые являются общедоступными или расположены в демилитаризованной зоне (DMZ), могут считаться более ценными из-за повышенного риска стать мишенью для злоумышленников
- **Компенсирующие средства контроля:** наличие средств контроля безопасности, которые могли бы смягчить воздействие уязвимости, также может повлиять на предполагаемую стоимость актива. Например, актив с надёжными средствами контроля безопасности может считаться менее ценным с точки зрения управления уязвимостями, поскольку риск успешной эксплуатации снижается

Чтобы эффективно определять приоритеты уязвимостей на основе стоимости активов, организациям необходимо вести точную инвентаризацию и регулярно оценивать их стоимость в контексте деятельности организации и терпимости к рискам

#### J. Компенсирующие элементы управления

Обсуждается роль многоуровневых средств контроля безопасности или стратегий углублённой защиты в смягчении последствий атак, выполняемых с помощью продвинутых угроз безопасности.

- **Компенсирующие элементы управления:** это меры безопасности, которые затрудняют использование уязвимостей. Они являются частью многоуровневой стратегии безопасности организации, также известной как стратегия углублённой защиты
- **Разногласия по поводу корректировки критичности:** практика корректировки критичности уязвимостей на основе компенсирующих средств управления является противоречивой. Некоторые заинтересованные стороны выступают за их снижение, исходя из предположения, что контроль эффективен. Однако изменение критичности уязвимости или рейтинга

риска без достаточных данных может привести к неправильному определению приоритетов и ослабить систему обеспечения безопасности организаций.

- **Тестирование компенсирующих элементов управления:** в отчёте рекомендуется протестировать использование уязвимостей в стеке безопасности компании в изолированной среде. Это может быть сделано персоналом, имеющим опыт работы в redteam, или с помощью инструмента моделирования взломов и атак, имитирующего TTP, наблюдаемые при вредоносных операциях. Эти данные могут помочь определить, можно ли увеличить критичность или рейтинг риска определённых уязвимостей

Компенсирующие средства контроля при управлении уязвимостями — это дополнительные меры безопасности, применяемые для снижения риска, связанного с выявленными уязвимостями. Они используются, когда уязвимости не могут быть немедленно устранены из-за технических ограничений, бизнес-требований или других факторов. Компенсирующие средства контроля могут помочь определить приоритеты уязвимостей за счёт снижения риска, позволяя организациям в первую очередь сосредоточиться на устранении уязвимостей с более высоким уровнем риска.

Компенсирующие элементы управления могут принимать различные формы, включая:

- **Сегментация сети:** это включает разделение сети на несколько сегментов, чтобы ограничить способность злоумышленника перемещаться в поперечном направлении внутри сети. Если уязвимость существует в одном сегменте сети, сегментация сети может помешать злоумышленнику использовать эту уязвимость
- **Брандмауэры и системы предотвращения вторжений (IPS):** эти инструменты могут обнаруживать и блокировать вредоносный трафик, потенциально предотвращая использование определённых уязвимостей
- **Многофакторная аутентификация (MFA):** MFA может помешать злоумышленнику получить доступ к системе, даже если он получил действительные учётные данные, тем самым снижая риск, связанный с уязвимостями, которые могут привести к краже учётных данных
- **Шифрование:** шифрование хранимых и передаваемых данных может снизить воздействие уязвимостей, которые могут привести к раскрытию данных
- **Регулярное исправление и обновления систем:** регулярное обновление и исправление систем может помочь снизить риск, связанный с известными уязвимостями
- **Обучение по повышению осведомлённости о безопасности:** обучение пользователей с целью распознавать потенциальные угрозы безопасности и избегать их может снизить риск использования уязвимостей с помощью атак социальной инженерии

Что касается определения приоритетов уязвимостей, компенсирующие средства контроля могут использоваться для снижения рейтинга риска определённых уязвимостей, позволяя организациям в первую очередь сосредоточиться на устранении других уязвимостей. Однако важно отметить, что эффективность компенсирующих средств контроля должна регулярно проверяться, чтобы убедиться, что они функционируют должным образом, например redteam.

Помимо компенсирующих средств контроля, другие факторы, которые можно использовать для определения приоритетности уязвимостей, включают критичность уязвимости, возможность использования уязвимости, стоимость актива, на который влияет уязвимость, и известно ли, что уязвимость используется в реальности. Такие инструменты, как система оценки прогнозирования эксплайтов (EPSS) и классификация уязвимостей для конкретных заинтересованных сторон (SSVC), также могут быть использованы для определения приоритетности уязвимостей

#### **Разница между компенсирующими элементами управления и исправлениями в управлении уязвимостями.**

В контексте управления уязвимостями компенсирующий контроль и исправление — это две разные стратегии, используемые для снижения риска, связанного с выявленными уязвимостями.

Исправление относится к процессу применения обновлений к программному обеспечению или системам для устранения известных уязвимостей. Это прямой метод устранения, поскольку он включает в себя модификацию системы или программного обеспечения. Исправление часто является наиболее эффективным способом предотвращения использования уязвимости, но оно также может быть ресурсоёмким и разрушительным, поскольку может потребовать перевода систем в автономный режим или перезапуска. Также важно отметить, что не для всех уязвимостей доступны исправления, и даже если они есть, их применение может быть отложено из-за требований к тестируанию или операционных ограничений.

С другой стороны, компенсирующие средства контроля — это альтернативные меры, применяемые для снижения риска, связанного с уязвимостью, когда применение исправления невозможно или желательно. Эти средства контроля не устраниют саму уязвимость, но снижают риск использования. Примеры компенсирующих средств контроля включают сегментацию сети, правила брандмауэра, системы обнаружения вторжений и дополнительный мониторинг. Использование компенсирующих средств контроля может быть спорным, поскольку они не устраниют уязвимость и их эффективность может быть трудно измерить. Однако они могут быть ценным инструментом управления рисками, особенно в случаях, когда немедленное исправление невозможно.

В то время как исправление непосредственно направлено на устранение уязвимостей, компенсирующие

элементы управления предоставляют альтернативные способы снижения риска, связанного с уязвимостями, когда исправление неосуществимо или желательно. Обе стратегии являются важными компонентами комплексной программы управления уязвимостями.

#### K. EPSS

EPSS — это инструмент, который помогает определять приоритеты уязвимостей в сфере кибербезопасности, представляющий оценку вероятности использования на основе данных, которая может дополнять традиционные рейтинги критичности и другие стратегии управления уязвимостями.

- **Проблемы с традиционной системой оценки:** традиционные системы оценки уязвимостей, такие как CVSS, подвергались критике за недостаточность для оценки рисков, связанных с уязвимостями, и определения их приоритетности с учётом фактора, что не все опубликованные эксплоиты находили подтверждение эксплуатации или были пригодны
- **Внедрение EPSS:** EPSS — это решение на основе данных и модели машинного обучения для прогнозирования вероятности того, что уязвимость будет использована в реальности. Это помогает более эффективно расставлять приоритеты в усилиях по устранению уязвимости. EPSS использует различные данные, например список CVE MITRE, данные о CVE, такие как количество дней с момента публикации, и наблюдения за эксплуатацией в реальных условиях
- **Оценка EPSS:** модель EPSS выдаёт оценку вероятности от нуля до единицы (от 0 до 100%). Чем выше оценка, тем больше вероятность того, что уязвимость будет использована
- **Сравнение с CVSS:** EPSS предназначен не для замены CVSS, а для дополнения его. В то время как CVSS предоставляет оценку критичности уязвимостей, EPSS обеспечивает прогнозирование вероятности использования. Эта дополнительная информация может помочь организациям более эффективно расставить приоритеты в своих усилиях по исправлению положения
- **Использование EPSS в управлении уязвимостями:** EPSS можно использовать в сочетании с другими инструментами и стратегиями управления уязвимостями, такими как поиск известных эксплуатируемых уязвимостей, учёт размещения устройств, оценка стоимости активов и применение компенсационных средств контроля
- **Категоризация уязвимостей для конкретных заинтересованных сторон (SSVC):** SSVC — это ещё один инструмент, который можно использовать совместно с EPSS. SSVC фокусируется на таких аспектах, включая статус использования уязвимости в системе безопасности, её влияние на безопасность и распространённость затронутых продуктов. SSVC улучшает процессы управления уязвимостями и учитывает интересы различных заинтересованных сторон

#### 1) Разница в EPSS с другими инструментами

EPSS предлагает более тонкий подход к управлению уязвимостями, прогнозируя вероятность использования, что дополняет оценку критичности, предоставляемую традиционными системами оценки, такими как CVSS. Эта возможность прогнозирования может принести значительную пользу организациям при определении приоритетности их усилий по устранению уязвимостей.

EPSS отличается от традиционных оценок критичности по ряду признаков:

- **Прогностический характер:** EPSS является прогнозистическим, предоставляя оценку вероятности, основанную на вероятности использования, в то время как CVSS предоставляет оценку критичности, связанную с внутренними характеристиками уязвимости
- **Подход, основанный на данных:** EPSS использует технологию, которая включает текущую информацию об угрозах из CVE и данные о реальных эксплойтах, чего нельзя сказать о рейтингах критичности CVSS
- **Модель машинного обучения:** EPSS использует модель машинного обучения для прогнозирования вероятности использования, используя данные из таких источников, как список MITRE CVE, и наблюдения за эксплуатацией в реальном времени от поставщиков безопасности

Преимущества использования EPSS для управления уязвимостями включают:

- **Эффективная расстановка приоритетов:** EPSS помогает организациям определять приоритеты уязвимостей, которые представляют наибольший риск и с наибольшей вероятностью будут использованы, позволяя им более эффективно распределять ресурсы
- **Дополнение к CVSS:** EPSS можно использовать наряду с CVSS для получения более полного представления об уязвимостях с учётом как критичности, так и вероятности эксплуатации
- **Сокращение усилий по устранению неполадок:** сосредоточив внимание на уязвимостях с более высокой вероятностью использования, организации могут сократить количество уязвимостей, которые им необходимо устраниить, экономя время и усилия.

#### L. SSVC

SSVC — это гибкий, настраиваемый и основанный на фактических данных подход к определению приоритетов уязвимостей. Это помогает организациям принимать обоснованные решения о том, какие уязвимости следует устраниить в первую очередь, исходя из их конкретного контекста и толерантности к риску.

- **Обзор SSVC:** SSVC — это методология анализа уязвимостей, разработанная Институтом программной инженерии Университета Карнеги-Меллон в координации с Агентством США по кибербезопасности и инфраструктурной безопасности (CISA). Он работает как дерево решений, что обеспечивает гибкость в его применении и учитывает интересы различных сторон.

- **Точки принятия решений SSVC:** SSVC использует дерево решений для определения реакций на уязвимость. Возможными результатами являются Track, Track\*, Attend, и Act. У каждого результата есть рекомендуемый график исправления, начиная от стандартных сроков обновления (Track, Track\*) и заканчивая немедленными действиями (Act).
- **Настраиваемость:** SSVC настраивается, помогая аналитикам принимать решения о действиях по устранению уязвимостей в соответствии с сохранением конфиденциальности, целостности и доступности корпоративных систем по согласованию с руководством.
- **Решения, основанные на фактических данных:** Решения SSVC основаны на логической комбинации триггеров, установленных руководством в ответ на такие факторы, как степень использования уязвимости, уровень сложности её использования противником и её влияние на общественную безопасность. Аналитики собирают данные о соответствующих триггерах и используют логику дерева решений для определения приоритетных решений по сортировке.
- **Расширение базовых оценок:** SSVC выходит за рамки просто базовых оценок как отдельный метод расстановки приоритетов. Это помогает организациям эффективно определять приоритеты и сортировать уязвимости, ориентируясь при этом в условиях неопределенности относительно того, какие проблемы следует решать в первую очередь.

## 1) Ключевые компоненты методологии SSVC

- Ключевые компоненты методологии SSVC включают:
- **Точки принятия решения:** SSVC использует дерево решений с точками принятия решений, которые приводят к различным результатам на основе анализа уязвимости. Эти точки принятия решений включают состояние эксплуатации, техническое действие, автоматизируемость, распространённость миссии и влияние на общественное благосостояние.
  - **Возможные результаты:** Дерево решений приводит к одному из четырёх возможных результатов: Track, Track\*, Attend, и Act. Для каждого результата указаны рекомендуемые сроки исправления, при этом "Act" требует немедленных действий.
  - **Настраиваемость:** SSVC разработан таким образом, чтобы его можно было настраивать, позволяя организациям адаптировать процесс принятия решений к их конкретным потребностям.
  - **Решения, основанные на фактических данных:** Решения в рамках SSVC принимаются на основе доказательств, касающихся статуса эксплуатации уязвимости, сложности и воздействия на общественную безопасность.
  - **Динамическое приложение:** SSVC задуман как концепция динамического применения, при этом выпускаются новые версии, включающие улучшения и отзывы.

## 2) Использование SSVC для определения приоритетов уязвимостей

SSVC может быть использован для эффективной расстановки приоритетов уязвимостей с помощью

- **Оценка воздействия:** анализ влияния уязвимости на деятельность организации и общественное благосостояние для определения срочности устранения.
- **Оценка состояния эксплуатации:** рассмотрение вопроса о том, имеется ли активная эксплуатация или подтверждение концепции уязвимости.
- **Определение автоматизируемости:** оценка того, является ли уязвимость самораспространяющейся или требует дополнительных действий для использования злоумышленником.
- **Принятие обоснованных решений:** использование дерева решений для принятия обоснованных решений о том, какие уязвимости следует устраниить в первую очередь, на основе конкретного уровня уязвимости организации и рекомендуемых действий.

## 3) Разница между SSVC и традиционными оценками критичности в управлении уязвимостями

Традиционные системы оценки в управлении уязвимостями, такие как CVSS, предоставляют числовую оценку для обозначения критичности уязвимости. Эти оценки основаны на наборе показателей, которые, среди прочего, включают вектор атаки, сложность атаки, требуемые привилегии и взаимодействие с пользователем. Однако эти традиционные решения подвергаются критике за то, что их недостаточно для оценки рисков, связанных с уязвимостями, и определения их приоритетности, поскольку в них не учитывается, использовалась ли уязвимость в реальности.

С другой стороны, классификация уязвимостей для конкретных заинтересованных сторон (SSVC) представляет собой более динамичный и гибкий подход к управлению уязвимостями. SSVC фокусируется на ценностях, включая статус использования уязвимости в системе безопасности, её влияние на безопасность и распространённость затронутых продуктов. SSVC даёт более полное представление о риске, связанном с уязвимостью, принимая во внимание такие факторы, как состояние эксплуатации, техническое действие, распространённость миссии и общественное благосостояние.

Хотя традиционные рейтинги обеспечивают стандартизированную оценку уязвимости, они не учитывают, её влияние на организацию. SSVC, с другой стороны, обеспечивает более комплексный и настраиваемый подход к управлению уязвимостями за счёт учёта более широкого спектра факторов.

## 4) Скоринг в методологии SSVC

Методология категоризации уязвимостей для конкретных заинтересованных сторон (SSVC) представляет собой процесс принятия решений о действиях по устранению уязвимостей. Методология SSVC предусматривает четыре оценочных решения, которые являются:

- **Track:** уязвимость в настоящее время не требует принятия мер, но организация должна продолжать отслеживать её и повторно оценивать, если станет доступна новая информация. CISA рекомендует устранять уязвимости отслеживания в стандартные сроки обновления.
- **Track\*:** уязвимость имеет специфические характеристики, которые могут потребовать более тщательного мониторинга изменений. CISA рекомендует устранять уязвимости отслеживания \* в стандартные сроки обновления.
- **Attend:** уязвимость требует внимания со стороны внутренних сотрудников организации на уровне надзора. Необходимые действия включают запрос помощи или информации об уязвимости и могут включать публикацию уведомления внутри компании и / или извне. CISA рекомендует устранять уязвимости Attend раньше стандартных сроков обновления.
- **Act:** уязвимость требует внимания со стороны внутренних сотрудников организации, на уровне надзора и руководства. Необходимые действия включают запрос помощи или информации об уязвимости, а также публикацию уведомления внутри компании и / или извне. Как правило, внутренние группы собираются для определения общего ответа, а затем выполняют согласованные действия. CISA рекомендует устраниить уязвимости Act как можно скорее.

## 5) Примеры SSVC

Примеры применения SSVC:

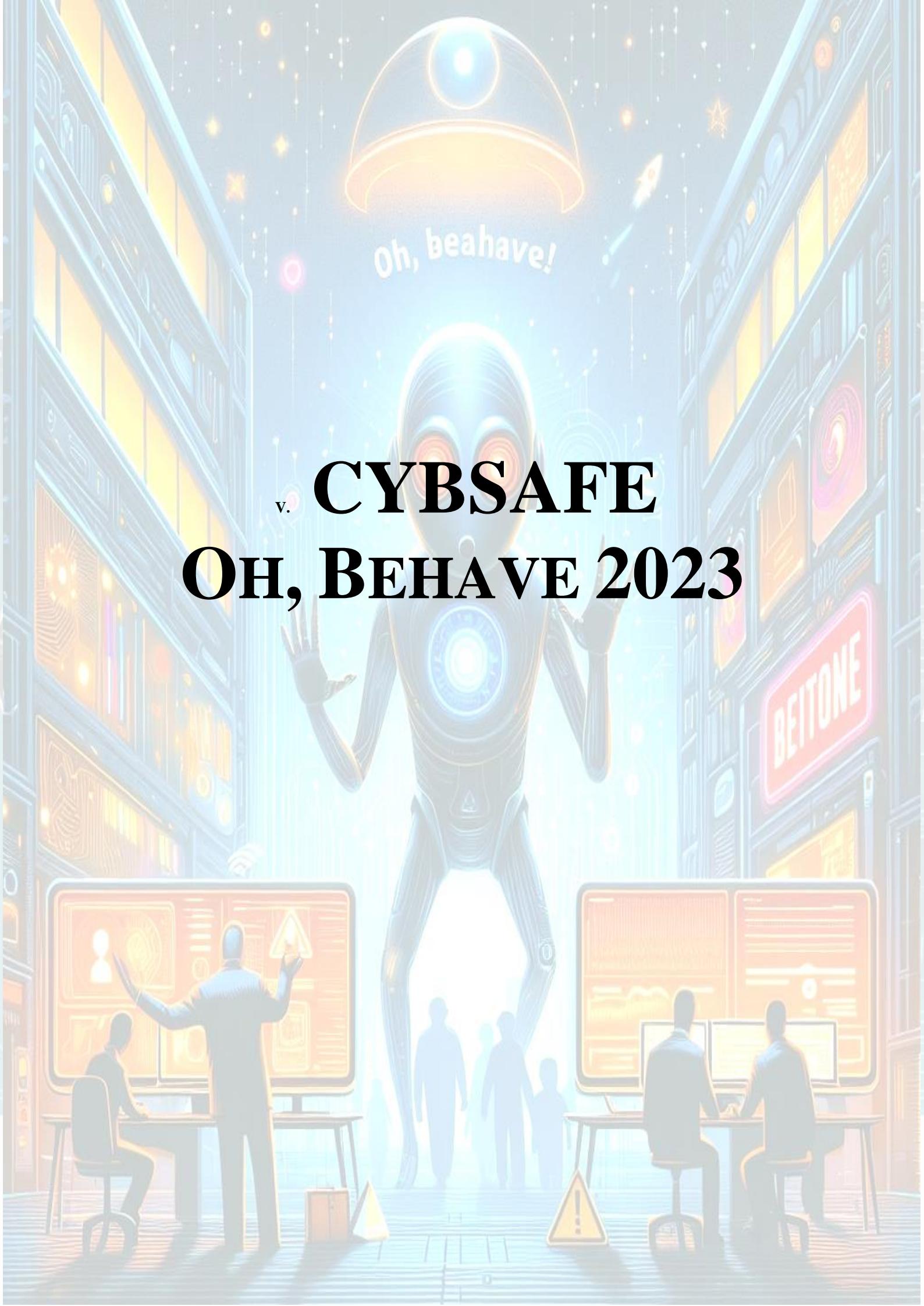
- **Индивидуальное дерево решений:** настройка дерева решений, чтобы сосредоточиться на факторах состояния эксплуатации уязвимости, её влияние на безопасность и распространённости затронутых продуктов
- **Возможные результаты:** дерево решений SSVC приводит к одному из четырёх возможных результатов: Track, Track\*, Attend, и Act. Для каждого результата указаны рекомендуемые сроки устранения, при этом "Act" требует немедленных действий. Это помогает организациям определять приоритеты уязвимостей в зависимости от уровня внимания, которого они требуют
- **Решения, основанные на фактических данных:** решения в рамках SSVC принимаются на основе доказательств, касающихся статуса эксплуатации уязвимости, сложности эксплуатации и воздействия на общественную безопасность. Например, если уязвимость активно используется с высоким техническим воздействием необходимо немедленное решение проблемы (Act)
- **Пример практического использования:** практический пример представляет собой ответ с определением приоритетов на уязвимость Citrix ShareFile, идентифицированную как CVE-2023-24489. Используя SSVC, организация, скорее всего,

выбрала бы значение "Act" после сопоставления информации, собранной аналитиками, с точками принятия решений и связанными с ними значениями. На это решение влияет наличие кода, подтверждающего правильность концепции, свидетельства целенаправленных атак и использования в реальных условиях

## M. Показатели

Обсуждается роль показателей в оценке и совершенствовании программы управления уязвимостями. Подчёркивается важность использования подробных и информативных показателей для оценки эффективности программы управления уязвимостями. Сосредоточившись на ключевых показателях риска и разделив показатели на отдельные группы, организации могут получить полезную информацию и более эффективно расставить приоритеты в усилиях по устранению последствий.

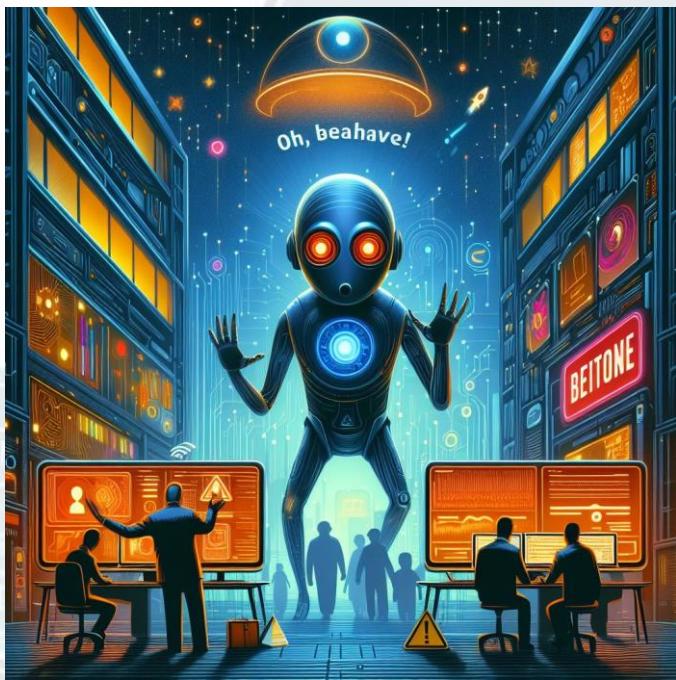
- **Показатели как индикаторы:** показатели необходимы для определения эффективности программы управления уязвимостями и выявления областей, требующих улучшения. Они обеспечивают способ измерения эффективности программы и принятия стратегических решений
- **Детализация:** простого подсчёта количества критических, уязвимостей высокой, средней и низкой критичности недостаточно, чтобы определить, достигают ли усилия по устранению поставленных целей. Показатели должны быть более детализированными и информативными
- **Разделение показателей:** показатели должны быть разделены по технологиям, размещению в сети и Соглашению об уровне обслуживания (SLA), изложенному в политике компании.
- **Фокус на известных эксплуатируемых уязвимостях:** различие между известными эксплуатируемыми уязвимостями и теми, которые в настоящее время не эксплуатируются, помогает направить усилия команды точно на решение проблемы
- **Ключевые показатели риска и показатели эффективности:** организациям следует сосредоточиться на ключевых показателях риска, а не только на ключевых показателях эффективности. Такой подход позволяет получить конкретную информацию, полученную на основе данных об уязвимостях, которая может быть более применимой
- **Пример показателей, основанных на оценке рисков:** сравнение сроков устранения уязвимостей на разных платформах, таких как Chrome и Edge. Это сравнение может выявить, какая платформа представляет более высокий уровень риска, исходя из времени, необходимого для устранения уязвимостей



# CYBSAFE OH, BEHAVE 2023

Oh, beahave!

BEITONE



## A. Введение

Документ "BSAFE-Oh, Behave!" – ежегодный отчёт, в котором содержится всесторонний анализ текущего состояния осведомлённости, отношения и поведения в области кибербезопасности среди пользователей Интернета. Структура отчёта охватывает различные аспекты кибербезопасности, включая «присутствие людей в Интернете», их отношение к онлайн-безопасности, роль науки о поведении и эффективность обучения в кибербезопасности.

Сложная взаимосвязь между поведением человека и рисками кибербезопасности будет рассмотрена ниже, предлагая уникальный взгляд на ландшафт цифровой безопасности. Анализ выявит ключевые выводы о повышении эффективности методов обеспечения безопасности организации, а также послужит важным ресурсом для понимания кибер-рисков человека и управления ими в условиях постоянно меняющегося ландшафта угроз.

## B. Краткое изложение

Основные выводы текущего состояния подходов и поведения в области кибербезопасности человек в Соединённых Штатах, Канаде, Соединённом Королевстве, Германии, Франции и Новой Зеландии:

- **«Присутствие в Сети»:** почти половина (47%) участников имеют десять или более конфиденциальных онлайн-аккаунтов, таких как учётные записи, связанные с платежами, и основные учётные записи электронной почты. 15% признались, что сбились со счета.
- **«Разочарование и сомнения в онлайн-безопасности»:** в то время как 84% считают сохранение безопасности приоритетом, а 69%

считают это достижимым, значительные 39% участников чувствовали разочарование, а 37% были напуганы сохранением безопасности в Интернете. Каждый третий (32%) часто чувствует себя подавленным информацией о кибербезопасности.

- **Обязательное обучение кибербезопасности:** чуть более четверти участников (26%) сообщили, что имели доступ к обучению кибербезопасности и пользовались им. Между тем, две трети (64%) отметили, что у них вообще не было доступа к обучению.
- **«Модели поведения»:** пять ключевых способов обеспечения безопасности: соблюдение пароля, использование MFA, установка обновлений устройства, проверка электронной почты на наличие признаков фишинга и сообщение о них, а также резервное копирование данных.

### 1) «Присутствие в сети»

Излагаются следующие ключевые моменты:

- **Ежедневное использование Интернета:** 93% участников опроса сообщили, что были онлайн по крайней мере один раз в день, и только 7% подключались реже
- **Конфиденциальные онлайн-аккаунты:** почти половина (47%) респондентов имеют десять или более конфиденциальных онлайн-аккаунтов, включая те, которые связаны с платежами, и основные учётные записи электронной почты
- **«Сбились со счета»:** 15% участников сбились со счета, сколькими конфиденциальными онлайн-аккаунтами они владеют
- **Различия поколений:** Z-поколения, сообщили о наличии более 20 конфиденциальных онлайн-аккаунтов, что указывает на больший цифровой след по сравнению со старшими поколениями, молчаливым поколением (1928–1945) и следующим за ними бэби-бумерами

### 2) «Разочарование и сомнения в онлайн-безопасности

Подчёркивается необходимость более персонализированных и практических подходов к обеспечению кибербезопасности, а также важность обеспечения безопасности решений и действий прошле и более понятным для физических лиц:

- **Усталость от безопасности:** многие люди чувствуют себя подавленными сложностями онлайн-безопасности, что приводит к чувству смирения и потере контроля. Более половины опрошенных считали бессмысленным защищать себя, что указывало на высокий уровень усталости от безопасности.
- **Необходимость принятия упрощённых решений в области безопасности:** предлагается ограничить количество решений по обеспечению безопасности, которые люди должны принимать, упростить

защитные действия в области кибербезопасности и обеспечить последовательность рекомендаций и отсутствие ненужных сложностей в работе людей.

- **Склонность к когнитивной склонности:** люди склонны полагаться на простые правила при принятии решений из-за ограниченных когнитивных ресурсов, таких как время, знания, внимание и память
- **Безопасность против производительности:** подчёркивается хрупкий баланс между предполагаемыми выгодами и затратами, связанными с обеспечением безопасности для частных лиц и предприятий.
- **Разочарование и сомнения:** значительная часть участников чувствовали разочарование (39%) и запугивание (37%), а каждый третий (32%) часто чувствует себя подавленным объёмом информации о кибербезопасности, в результате чего сокращает свои действия в Интернете.
- **Стоимость защитных действий:** почти половина участников (49%) считают, что принятие защитных мер в Интернете сопряжено с высокими затратами. В то время как 69% опрошенных считали, что сохранение безопасности в Интернете стоит затраченных усилий, молодое поколение более скептически относилось к окупаемости инвестиций.
- **Влияние СМИ:** более половины участников (56%) заявили, что новости мотивируют их принимать защитные меры безопасности, а 51% считают, что освещение событий в СМИ помогает им оставаться в курсе вопросов онлайн-безопасности. Однако 44% участников заявили, что СМИ вызывают страх, а 42% считают, что они чрезмерно усложняют безопасность в Интернете

### 3) «Обязательное обучение кибербезопасности»

Представлены несколько ключевых моментов и выводов, которые указывают на необходимость более доступного обучения по вопросам кибербезопасности, особенно для неработающих лиц. Переход к оповещениям системы безопасности указывает на предпочтение упреждающих мер безопасности в режиме реального времени. Подразумевается, что существует возможность повысить осведомлённость и практику в области кибербезопасности за счёт более эффективного распространения имеющихся ресурсов и внедрения более привлекательных и удобных для пользователя стратегий обеспечения безопасности

- **Доступ к обучению кибербезопасности:** около четверти (26%) участников имеют доступ к обучению кибербезопасности и пользуются его преимуществами. Значительное большинство (64%) сообщили, что вообще не имели доступа к такому обучению.
- **Предпочтение онлайн-обучению кибербезопасности:** предпочтение отдаётся

онлайн-обучению кибербезопасности. Участники, окончившие курсы, сочли содержание полезным и увлекательным, независимо от того, занимались ли они дома или на работе.

- **Переход к оповещениям системы безопасности:** наблюдается заметный сдвиг в сторону различных стратегий взаимодействия с системой безопасности. Все больше людей предпочитают получать своевременные уведомления при принятии решений, которые могут подвергнуть их риску.
- **Уязвимость неработающих лиц:** лица, вышедшие на пенсию или не занимающиеся активной трудовой деятельностью, остаются уязвимыми, поскольку они сообщают о незначительном доступе к учебным ресурсам или об их полном отсутствии.

#### a) Главный аргумент

Основной аргумент подраздела заключается в том, что, хотя традиционное обучение кибербезопасности приносит пользу, значительная часть населения не имеет доступа к такому обучению.

В рамках изменения подхода людей к обеспечению безопасности: все больше отдается предпочтение своевременным уведомлениям при принятии решений, которые могут подвергнуть их риску. Это указывает на переход к более активным и учитывающим контекст методам обучения кибербезопасности, которые могут предоставлять пользователям своевременные рекомендации и напоминания.

Подчёркивается уязвимость определённых групп, таких как пенсионеры и те, кто не работает активно или не учится, которые сообщают о незначительном доступе к учебным ресурсам или вообще об их отсутствии. Это говорит о необходимости улучшения высококачественного бесплатного контента по вопросам кибербезопасности, доступного в Интернете для этой аудитории.

По сути, приводится аргумент в пользу более широкого и инклюзивного подхода к повышению осведомлённости в области кибербезопасности, который выходит за рамки традиционного обучения и включает поведенческие стратегии для эффективного вовлечения пользователей в практику обеспечения безопасности.

#### b) Проблемы в области кибербезопасности

Обучение кибербезопасности отличаются от традиционных нескольких способов. Традиционное обучение кибербезопасности часто включает официальные занятия, на которых пользователям рассказывают о различных угрозах и способах защиты от них. Это обучение может занять много времени и часто требует от пользователей запоминания большого количества информации. С другой стороны, постоянные напоминания и подсказки предназначены для предсказуемого влияния на поведение, без ограничения каких-либо вариантов или существенного изменения экономических стимулов. Они часто интегрируются в системы, с которыми пользователи взаимодействуют ежедневно, что делает их менее

навязчивыми и более релевантными с точки зрения контекста.

Вынужденное обучение может использоваться для поощрения более эффективных методов обеспечения кибербезопасности различными способами. Например, подсказки могут использоваться для того, чтобы побудить пользователей создавать более длинные и безопасные пароли, снижая вероятность взлома учётной записи. Они также могут быть использованы для поощрения использования многофакторной аутентификации (MFA), что ещё больше повышает безопасность учётной записи. Вынужденное обучение также можно использовать для поощрения пользователей к регулярному обновлению своего программного обеспечения, защищая их от уязвимостей, которыми могут воспользоваться киберпреступники.

c) «Не можешь – научим, не хочешь – заставим»

Для устранения проблем с безопасностью при использовании обязательного обучения важно:

- **Ограничение решений по обеспечению безопасности:** уменьшение количества решений по обеспечению безопасности, которые должны принимать пользователи, например, путём внедрения единого входа (SSO), чтобы избежать многократных запросов пароля
- **Упрощение защитных действий:** упрощение пользователям выполнения защитных действий в области кибербезопасности, гарантируя, что процесс будет простым и удобным для пользователя
- **Последовательные рекомендации:** предоставление последовательных и чётких рекомендаций, которые не вносят путаницы или ненужных трений, которые могут привести к усталости от безопасности

d) Персонализированные и практические мероприятия по повышению осведомленности в области кибербезопасности

Примеры персонализированных и практических подходов к мероприятиям по повышению осведомлённости в области кибербезопасности включают:

- **Интерактивное обучение:** привлечение пользователей к интерактивным обучающим занятиям, имитирующими реальные сценарии, такие как моделирование фишинга или комнаты для побега кибербезопасности
- **Геймификация:** использование игр и заданий, чтобы сделать изучение кибербезопасности увлекательным, например, кроссворды на тему кибербезопасности или соревнования CTF
- **Лекции и практика:** лекции и практики в урезанной занимательной и доступной форме (формата историй или разыгрывания сценок), иллюстрирующей концепции кибербезопасности

- **Занятия в малых группах:** проведение занятий в малых группах, поощряющие обсуждение и практическую практику принципов кибербезопасности

e) Выгоды обязательного обучения

Существует несколько потенциальных преимуществ использования обязательного обучения.

Во-первых, небольшое вынужденное обучение может помочь снизить утомление от безопасности, состояние усталости или нежелания заниматься проблемами кибербезопасности, упрощая и интегрируя решения по безопасности в повседневную рутину пользователей. Это может сделать методы обеспечения безопасности более управляемыми и менее обременительными для пользователей.

Во-вторых, вынужденное ситуативное обучение может помочь сбалансировать безопасность и производительность. Традиционные меры кибербезопасности часто могут затруднять выполнение пользователями основных задач, снижая вероятность того, что они будут следовать методам обеспечения безопасности. Интегрируя решения по обеспечению безопасности в рабочие процессы пользователей, обязательность выполнения безопасных действий могут гарантировать, что методы обеспечения безопасности не будут влиять на производительность.

В-третьих, обучение может помочь преодолеть проблемы поколений в области кибербезопасности. Разные поколения могут по-разному относиться к кибербезопасности и вести себя по-разному, обучение может быть адаптировано к конкретным потребностям и предпочтениям различных групп пользователей.

Доступное обучение может помочь укрепить культуру безопасности в организациях. Поощряя пользователей предпринимать небольшие, управляемые шаги в направлении улучшения практики обеспечения безопасности, возможно создать среду, в которой безопасность рассматривается как общая ответственность и нормальная часть повседневной деятельности.

f) Недостатки обязательного обучения

У такого подхода есть несколько потенциальных недостатков:

- **Усталость от безопасности:** постоянные решения о безопасности в Интернете могут привести к "усталости от безопасности", когда люди становятся нечувствительными к опасностям Интернета. Это затрудняет мотивацию людей к принятию защитных мер
- **Когнитивная нагрузка:** люди склонны полагаться на простые правила при принятии решений из-за ограниченных когнитивных ресурсов, таких как время, знания, внимание и память. Если количество решений по обеспечению безопасности слишком велико, это может ошеломить отдельных людей и привести к неправильному принятию решений

- **Безопасность против производительности:** часто существует хрупкий баланс между предполагаемыми преимуществами мер безопасности и их затратами для частных лиц и предприятий. Если меры безопасности препятствуют достижению основных целей людей, у них меньше шансов принять защитные меры кибербезопасности. Это можно увидеть в таких действиях, как резервное копирование данных, использование многофакторной аутентификации (MFA) и управление паролями
- **Проблемы с доверием:** некоторым инструментам безопасности, таким как менеджеры паролей, может не хватать доверия. Несмотря на то, что они считаются самым безопасным вариантом, многие люди по-прежнему не решаются их использовать из-за опасений по поводу их безопасности и возможности одновременного взлома всех их паролей
- **Отсутствие отчёtnости:** многие люди не сообщают о попытках фишинга либо потому, что не знают как, не могут найти кнопки для сообщения, либо считают, что отчёtnость не остановит киберпреступников. Такое отсутствие отчёtnости может привести к тому, что попытки фишинга не ослабеют
- **Вызовы поколений:** разные поколения обладают разным уровнем уверенности и способности распознавать угрозы кибербезопасности и бороться с ними. Например, старшее поколение, как правило, менее уверено в своей способности распознавать фишинговые сообщения
- **Неэффективность информирования и просвещения:** простое осознание рисков и умение устанавливать обновления или распознавать попытки фишинга не всегда приводит к правильному поведению. Многие люди по-прежнему откладывают или игнорируют обновления, а некоторые не проверяют сообщения на наличие признаков фишинга, прежде чем предпринимать действия

g) *Балансирование воспринимаемых выгод и затрат с помощью обучения*

Документ предлагает возможные варианты баланса достоинство и недостатков обязательного обучения:

- **Выделение непосредственных выгод:** подчёркивание непосредственных преимуществ безопасного поведения, таких как спокойствие, которое приходит от осознания того, что ваши данные защищены
- **Минимизация предполагаемых затрат:** разработка мер, которые минимизируют предполагаемые затраты на безопасность, такие как использование автоматических обновлений для уменьшения усилий, требуемых от пользователей
- **Культурная значимость:** обучение должно иметь культурное значение и находят отклик у целевой

аудитории, что может повысить их воспринимаемую ценность

- **Обратная связь и признание:** обеспечение обратной связи и признание безопасного поведения, усиливая преимущества и поощряя постоянное соблюдение требований

4) *Жертвы киберпреступлений чаще и больше сообщают об инцидентах*

Излагаются следующие ключевые моменты, подчёркивающие важность механизмов отчёtnости в борьбе с киберпреступностью и необходимость продолжения усилий по повышению доступности и эффективности процессов отчёtnости. Они также подчёркивают растущую озабоченность пользователей Интернета по поводу риска стать жертвами киберпреступности.

- **Рост числа сообщений:** значительное число жертв киберпреступлений сообщают об инцидентах - 88% участников, столкнувшихся с киберпреступлениями, сообщили об этом кому-либо

- **Отчёtnость по видам преступлений:** количество сообщений варьировалось в зависимости от типа киберпреступности. О фишинге 59% сообщили в свой банк или компанию, выпускающую кредитные карты, в то время как 54% жертв кражи личных данных и 42% жертв мошенничества с онлайн-знакомствами сделали то же самое

- **Мотивация к профилактике:** основными причинами сообщений о киберпреступлениях, таких как фишинг, мошенничество при онлайн-знакомствах и кража личных данных, были стремление предотвратить повторение преступления с ними самими или с другими, а также возместить потерянные деньги

- **Проблемы с отчёtnостью:** хотя многие знали, как сообщать о фишинговых мошенничествах (49%), некоторые сочли процесс отчёtnости сложным. Четверть жертв кражи личных данных столкнулись с трудностями

- **Причины не сообщать:** некоторые жертвы предпочли не сообщать о киберпреступлениях, поскольку считали ущерб незначительным или полагали, что сообщение не приведёт к каким-либо действиям

- **Восприятие риска:** на 7% увеличилось число людей, которые считают, что могут стать жертвами киберпреступности, при этом 50% участников считают себя потенциальными целями

a) *Почему жертвы киберпреступности сообщают об инцидентах?*

Основные причины, по которым жертвы киберпреступлений сообщают об инцидентах, заключаются в том, чтобы предотвратить повторение преступления с ними или другими и вернуть потерянные деньги. В частности, жертвы таких преступлений, как фишинг,

мошенничество с онлайн-знакомствами и кражи личных данных, сообщали о предотвращении повторения и попытках возместить финансовые потери.

Среди наиболее часто приводимых причин не сообщать об инцидентах, связанных с киберпреступностью, убеждение в том, что отчётность не останавливает киберпреступников, и 72% участников придерживаются этого мнения. Другие причины включают желание предотвратить попадание нежелательных сообщений в их почтовый ящик, желание, чтобы что-то произошло при сообщении о них (например, получение подтверждения), и потребность в большем доверии к процессу сообщения.

Отчётность об инцидентах, связанных с киберпреступностью, менялась с течением времени, при этом общее количество сообщений увеличилось. Среди участников из Северной Америки и Великобритании количество сообщений о фишинге выросло в среднем на 19% по сравнению с предыдущим годом. Количество сообщений о мошенничестве на сайтах знакомств увеличилось на 45% среди канадских и британских участников и на 19% среди американцев. Количество сообщений о краже личных данных увеличилось на 29% среди британских участников, на 19% среди американцев и на 11% среди канадцев.

*b) Распространенные заблуждения относительно сообщений об инцидентах, связанных с киберпреступностью*

Некоторые распространённые заблуждения относительно сообщений об инцидентах, связанных с киберпреступности включают:

- **Сообщение ведёт к огласке:** существует мнение, что сообщение о кибератаках сделает инцидент достоянием общественности, что может удержать организации от подачи сообщений из-за боязни нанесения ущерба репутации
- **Выплата выкупа решает проблему:** ещё одно заблуждение заключается в том, что выплата выкупа автоматически разрешит инцидент, что не всегда так и может увековечить цикл преступлений
- **Отчётность бесполезна:** многие считают, что отчётность не останавливает киберпреступников, что может привести к занижению отчётности. Такого мнения придерживаются 72% участников
- **Отчётность слишком сложна:** процесс подачи отчёта может рассматриваться как слишком сложный или отнимающий много времени, что может отбить у жертв желание сообщать об этом
- **Страх последствий:** существует опасение, что отчётность может привести к юридическим проблемам или нежелательной проверке, что может помешать организациям сообщать об инцидентах

*c) Поощрение сотрудников сообщать об инцидентах, связанных с киберпреступностью*

Организации могут поощрять сотрудников сообщать об инцидентах, связанных с киберпреступностью, путём:

- **Создание культуры поддержки:** формирование культуры отсутствия вины, при которой сотрудники чувствуют себя комфортно, сообщая об инцидентах, не опасаясь последствий
- **Обеспечение обучения и осведомлённости:** регулярное обучение сотрудников важности отчётности и тому, как делать это эффективно
- **Внедрение механизмов отчётности:** упрощение и доступность процесса отчётности, возможно, с использованием анонимных вариантов в качестве последнего средства
- **Демонстрация действий:** демонстрация того, что отчёты ведут к действиям, а улучшения могут мотивировать сотрудников сообщать
- **Разъяснение важности:** объяснение сотрудникам того, как отчётность помогает организации и защищает интересы каждого

*d) Потенциальные последствия непредставления сообщений об инцидентах, связанных с киберпреступностью*

Потенциальные последствия непредставления сообщений об инцидентах, связанных с киберпреступностью, включают:

- **Финансовые потери:** организации могут понести финансовые потери из-за мошенничества, кражи или выплаты выкупа
- **Ущерб репутации:** даже если об инцидентах не сообщается, они могут стать достоянием общественности и нанести ущерб репутации организации
- **Операционный простой:** непредставление отчётов может привести к длительному операционному простою, поскольку организация пытается оправиться от инцидента
- **Правовые и нормативные последствия:** непредставление сообщения может привести к судебным искам, штрафам регулирующих органов и несоблюдению законов о защите данных
- **Подрыв доверия:** клиенты и партнёры могут потерять доверие к организации, которая не в состоянии эффективно управлять киберпреступлениями и сообщать о них

### C. Основные выводы

Эти выводы подчёркивают важность понимания и устранения человеческих факторов, которые способствуют нарушениям безопасности и инцидентам. Они также подчёркивают необходимость эффективного обучения кибербезопасности и роль средств массовой информации в формировании представлений и поведения, связанных с безопасностью в Интернете.

1) Поведение и практика в области кибербезопасности

- **Обновления программного обеспечения:** несмотря на важность обновлений программного обеспечения для защиты от кибер-угроз, многие частные лица и организации откладывают их на потом или игнорируют. Такое поведение может привести к значительным уязвимостям, как это видно в атаках программ-вымогателей WannaCry
- **Осведомлённость о фишинге:** в то время как 65% участников заявили, что знают, как установить последние обновления программного обеспечения и приложений, 18% признали обратное, а ещё 17% знали, как, но, как правило, не устанавливали обновления. Это показывает, что осведомлённость и образование не всегда приводят к правильному поведению
- **Отчёты о фишинге:** только 44% участников сообщили, что использовали кнопки "спам" или "сообщить о фишинге" "очень часто" или "всегда". Значительные 33% участников не принимают мер против киберпреступников
- **Гигиена паролей:** многие люди предпочитают собственные методы управления паролями, такие как их запись в блокноты. Они не доверяют тому, что все их пароли хранятся в одном инструменте, особенно учитывая недавнее внимание СМИ к менеджерам паролей, неспособным защитить пользователей

2) Ответственность за кибербезопасность

- **Различия поколений:** Поколение Z и миллениалы, как правило, придерживаются принципа "невмешательства" в онлайн-безопасность. Киберпреступность среди этих поколений была заметно выше, чем среди других
- **Роль средств массовой информации:** освещение событий в средствах массовой информации может повысить мотивацию к принятию мер по самозащите. Однако это также может привести к тому, что люди неправильно оценят риски просто потому, что это недавно было в новостях (т. е. предвзятое отношение к доступности)
- **Обучение кибербезопасности:** доступ к обучению кибербезопасности не является всеобщим. Пенсионеры или те, кто не работает активно, сообщают о незначительном доступе к учебным ресурсам, а то и вовсе об их отсутствии. Онлайн-тренинги кибербезопасности в целом были предпочтительнее, и те, кто прошёл курсы, сочли содержание тренинга полезным и увлекательным

3) Различия поколений в отношении к онлайн-безопасности

- **Поколение Z и миллениалы:** Эти поколения, как правило, более спокойно относятся к онлайн-безопасности. Они не придают этому такого значения, как старшее поколение, и половина из них

не считает, что обеспечение безопасности в Сети стоит их усилий. Уровень киберпреступности среди этих поколений был заметно выше, чем среди других

- **Старшие поколения:** Старшие поколения в целом были менее уверены в своей способности распознавать фишинговые электронные письма. Например, 20% представителей Молчаливого поколения и 17% бэби-бумеров выразили сомнение в своей способности распознавать фишинговые сообщения

4) Виктимизация киберпреступности

Эти результаты подчёркивают разный уровень виктимизации киберпреступности в разных странах и наиболее распространённые виды киберпреступлений.

- **Глобальный взгляд на виктимизацию киберпреступности:** отношение к вероятности стать жертвой киберпреступности во всем мире было безразличным. Однако немцы (45%) меньше всего беспокоились о том, что могут стать жертвами киберпреступности по сравнению с другими странами, которые варьировались от 57% до 63%
- **Виктимизация киберпреступности в разбивке по странам:** у американцев (61%) были причины беспокоиться о том, что они могут стать жертвами киберпреступности, поскольку более трети (36%) из них сообщили, что стали жертвами одного или нескольких видов киберпреступлений. У канадцев (23%) и немцев (23%) было самое низкое число жертв киберпреступности
- **Тип киберпреступности:** американцы неизменно с большей вероятностью становились жертвами любого вида киберпреступности. При изучении каждого вида преступлений американцы (27%) сообщили о большинстве краж личных данных по сравнению с другими странами, особенно участники из Франции (9%). По сравнению с другими киберпреступлениями, британские участники (19%) чаще становились жертвами мошенничества на сайтах знакомств, чем других видов преступлений (16% фишинга и 18% краж личных данных)

D. Отношение к онлайн-безопасности

Эти результаты подчёркивают положительное отношение большинства участников к онлайн-безопасности, но также выявляют серьёзные проблемы, такие как разочарование, запугивание и ощущение перегруженности информацией о кибербезопасности. Данные также показывают разницу между поколениями в отношении ценности усилий по обеспечению безопасности в Интернете и влияния средств массовой информации на общественное восприятие.

- **Приоритет и достижимость:** подавляющее большинство участников, 84%, считают приоритетом обеспечение безопасности в Сети, а 69% считают, что это достижимо

- **Разочарование и запугивание:** несмотря на важность, придаваемую безопасности, 39% участников почувствовали разочарование, а 37% почувствовали себя напуганными процессом обеспечения безопасности в Интернете
- **Перегрузка информацией:** каждый третий участник (32%) часто чувствует себя перегруженным информацией о кибербезопасности, что заставляет его сокращать свои действия в Интернете
- **Затраты на безопасность:** почти половина участников (49%) считают, что принятие защитных мер в Интернете сопряжено с высокими затратами. Однако 69% по-прежнему считают, что оставаться в безопасности в Интернете стоит затраченных усилий
- **Скептицизм поколений:** молодые поколения, особенно 21% представителей поколения Z и 23% миллениалов, более чем в два раза чаще, чем бэби-бумеры (6%) и молчаливое поколение (9%), сомневаются в том, стоит ли прилагать усилия для обеспечения безопасности в Интернете
- **Влияние СМИ:** более половины участников (56%) заявили, что новости мотивируют их принимать защитные меры безопасности, а 51% считают, что освещение событий в СМИ помогает им оставаться в курсе вопросов онлайн-безопасности. Однако 44% заявили, что СМИ вызывают страх, а 42% считают, что они чрезмерно усложняют безопасность в Интернете

#### E. Обучение кибербезопасности

Эти результаты подчёркивают важность обучения кибербезопасности на рабочем месте и подчёркивают различия в подходах к образованию в области кибербезопасности в разных странах. Данные также свидетельствуют о том, что введение обязательного обучения кибербезопасности потенциально может увеличить его охват, как это видно на примере Великобритании.

- **Доступ к обучению кибербезопасности:** более половины участников из Канады (59%), Новой Зеландии (57%), Великобритании (56%) и Германии (51%) прошли обучение кибербезопасности на своих рабочих местах. Треть участников из США (33%) и Германии (33%) сообщили, что посещали тренинги дома, в то время как французские участники (23%) с большей вероятностью посещали тренинги в общественных местах, таких как библиотека
- **Обязательное обучение:** прохождение обязательного обучения кибербезопасности на работе или учебном заведении было самым высоким среди британских участников (88%) и самым низким среди французских участников, при этом почти четверть (24%) сообщили, что обучение кибербезопасности не является обязательным занятием

- **Общее количество участников:** исследование проводилось среди 6064 участников из США, Канады, Великобритании, Германии, Франции и Новой Зеландии. Из них 2065 участников имели доступ к обучению кибербезопасности

#### F. Заключение

В заключении стоит обобщить ключевые выводы:

- **Усталость от безопасности реальна:** люди чувствуют себя подавленными объёмом информации о кибербезопасности, что может привести к снижению онлайн-активности. Почти половина участников (49%) считают, что принятие защитных мер в Интернете обходится дорого.
- **Безопасность против производительности:** говорится о конфликте между поддержанием безопасности и производительностью. В то время как 69% участников считают, что оставаться в безопасности в Интернете стоит затраченных усилий, молодое поколение (21% представителей поколения Z и 23% миллениалов) более скептически относится к окупаемости инвестиций.
- **Вызовы поколений:** различия поколений в отношении к онлайн-безопасности.
- **Роль СМИ:** более половины участников (56%) заявили, что новости мотивируют их принимать защитные меры безопасности, а 51% считают, что освещение событий в СМИ помогает им оставаться в курсе вопросов онлайн-безопасности. Однако 44% участников заявили, что СМИ вызывают страх, а 42% считают, что они чрезмерно усложняют безопасность в Интернете.
- **Обучение кибербезопасности:** важность обучения кибербезопасности, но в разделе заключения не приводятся конкретные выводы или цифры.

#### 1) Расширенное заключение:

- **Усталость от безопасности:** Многие люди чувствуют себя перегруженными информацией о кибербезопасности, что приводит к снижению онлайн-активности и восприятию того, что принятие защитных мер обходится дорого.
- **Безопасность в сравнении с производительностью:** молодое поколение более скептически относится к окупаемости инвестиций в меры кибербезопасности, обеспечивая баланс между безопасностью и производительностью.
- **Различия поколений:** отношение к онлайн-безопасности у разных поколений разное, причём молодое поколение выражает больше скептицизма и сомнений в ценности усилий по обеспечению кибербезопасности.
- **Влияние средств массовой информации:** средства массовой информации играют важную роль в формировании представлений об онлайн-безопасности. Хотя это может побудить людей предпринять защитные действия, это также может вызвать страх и чрезмерно усложнить проблему.

- **Обучение кибербезопасности:** доступ к обучению кибербезопасности остаётся ограниченным, и только четверть участников сообщили о доступе к обучению. Однако те, кто прошёл обучение, сообщили о положительных изменениях в своём поведении в области кибербезопасности.
  - **Сообщения о киберпреступлениях:** количество сообщений о киберпреступлениях увеличилось, и большинство жертв сообщают об инцидентах в соответствующие органы. Однако о значительном количестве инцидентов по-прежнему не сообщается из-за кажущейся незначительности или отсутствия веры во власть.
  - **Поведение в области кибербезопасности:** соблюдение правил пароля, использование MFA, обновления устройств, предупреждение о фишинге и резервное копирование данных — вот ключевые аспекты кибербезопасности, которые нуждаются в улучшении.
  - **Присутствие в Сети:** у многих людей из них десять или более конфиденциальных онлайн-аккаунтов. Это подчёркивает необходимость надёжных методов обеспечения кибербезопасности.
  - **Отношение к онлайн-безопасности:** хотя большинство людей считают приоритетом обеспечение безопасности в Интернете, многие чувствуют разочарование и напуганность этим процессом.
  - **Ответственность за кибербезопасность:** необходимо воспитывать чувство общей ответственности за кибербезопасность у отдельных лиц, организаций и правительства.
  - **Вынужденное и доступное обучение:** поучение могут быть эффективным инструментом поощрения позитивного поведения в области кибербезопасности, но они должны быть персонализированными, практическими и учитывать предполагаемые выгоды и затраты от мер кибербезопасности.
  - **Усталость от безопасности:** усталость от безопасности можно устраниТЬ путём проведения персонализированных практических мероприятий по повышению осведомлённости в области кибербезопасности, в которых основное внимание уделяется преимуществам кибербезопасности и учитывается предполагаемая стоимость.
  - **Обучение кибербезопасности:** обучение кибербезопасности должно быть доступным, увлекательным и адаптированным к различным аудиториям. В нем также должны быть рассмотрены предполагаемые выгоды и затраты, связанные с мерами кибербезопасности.
  - **Отчётность о киберпреступлениях:** поощрение отчётности о киберпреступлениях требует устранения причин непредставления отчётности, таких как кажущаяся незначительность инцидентов и отсутствие доверия к властям.
  - **Поведение в области кибербезопасности:** улучшение поведения в области кибербезопасности требует учёта предполагаемых выгод и затрат от мер кибербезопасности, проведения персонализированных и практических мероприятий по повышению осведомлённости и обеспечения баланса между безопасностью и производительностью.
  - **Присутствие в Сети:** управление обширным присутствием в Сети требует строгих мер кибербезопасности, включая соблюдение правил безопасности паролей, использование MFA, обновления устройств, предупреждение о фишинге и резервное копирование данных.
  - **Отношение к онлайн-безопасности:** устранение негативного отношения к онлайн-безопасности требует учёта предполагаемых затрат и выгод от мер кибербезопасности, проведения персонализированных и практических мероприятий по повышению осведомлённости и воспитания чувства общей ответственности.
  - **Ответственность за кибербезопасность:** воспитание чувства общей ответственности за кибербезопасность требует учёта предполагаемых затрат и выгод от мер кибербезопасности, проведения персонализированных и практических мероприятий по повышению осведомлённости, а также учёта предполагаемых затрат и выгод от мер кибербезопасности.
- 2) **Усталость от безопасности реальна**
- Эти выводы подчёркивают реальность усталости пользователей от безопасности, подчёркивая необходимость более удобных для пользователя и экономически эффективных мер кибербезопасности, а также чёткой и действенной информации об онлайн-безопасности.
- **Разочарование и запугивание:** значительное число участников выразили разочарование и запугивание по поводу обеспечения безопасности в Интернете. В частности, 39% участников почувствовали разочарование, а 37% были напуганы безопасностью в Интернете
  - **Перегруженность информацией:** каждый третий участник (32%) часто чувствовал себя подавленным информацией о кибербезопасности, что заставляло их сокращать свои действия в Интернете
  - **Стоимость безопасности:** почти половина участников (49%) сочли, что принятие защитных мер в Интернете обходится дорого
  - **Сомнения в целесообразности усилий:** В то время как 69% участников считали, что обеспечение безопасности в Сети стоит затраченных усилий, молодое поколение (21% представителей поколения Z и 23% миллениалов) более скептически относилось к окупаемости инвестиций. Они более

чем в два раза чаще, чем бэби-бумеры (6%) и представители Молчаливого поколения (9%), сомневались в том, что онлайн-безопасность стоит затраченных усилий

- **Влияние СМИ:** более половины участников (56%) заявили, что новости мотивируют их принимать защитные меры безопасности, а 51% считают, что освещение событий в СМИ помогает им оставаться в курсе вопросов онлайн-безопасности. Однако 44% участников заявили, что СМИ вызывают страх, а 42% считают, что они чрезмерно усложняют безопасность в Интернете

### 3) Безопасность против производительности

Основные выводы заключаются в следующем:

- **Закон о балансе:** обсуждается проблема обеспечения баланса между мерами безопасности и производительностью, при этом признается, что чрезмерно сложные или отнимающие много времени методы обеспечения безопасности могут снизить эффективность работы и соответствие требованиям пользователей.
- **Пользовательский опыт:** это может подчеркнуть важность разработки мер безопасности, которые удобны для пользователя и не мешают выполнению основных задач пользователей, для обеспечения принятия и поддержания методов обеспечения безопасности.
- **Поведенческие привычки:** в этом подразделе также может быть сделан акцент на использовании анализа поведения для создания решений безопасности, которые не только эффективны, но и соответствуют рабочим привычкам и предпочтениям пользователей.
- **Проблемы с производительностью:** можно обсудить, как проблемы с производительностью иногда могут приводить к неэффективным методам обеспечения безопасности, таким как использование слабых паролей ради удобства, и как решить эти проблемы.
- **Интеграция безопасности:** предложены способы плавной интеграции безопасности в повседневные рабочие процессы, чтобы это повышало, а не снижало производительность.

### 4) Вызовы поколений

Эти результаты указывают на значительные различия между поколениями в отношении онлайн-безопасности: молодое поколение чувствует себя менее контролируемым и более перегруженным информацией о кибербезопасности. Это говорит о необходимости специальных образовательных и коммуникационных стратегий в области кибербезопасности, которые находят отклик у разных возрастных групп

- **Расстановка приоритетов между поколениями:** старшее поколение уделяет большее внимание онлайн-безопасности, чем молодое поколение. Например, 91% бэби-бумеров считают приоритетом

безопасность в Интернете по сравнению с 69% представителей поколения Z.

- **Страх сложности онлайн-безопасности:** Молчаливое поколение (43%) и миллениалы (40%) подвергаются наибольшему уровню страха со стороны онлайн-безопасности, в отличие от поколения X.
- **Скептицизм в отношении усилий:** молодое поколение, в частности 21% представителей поколения Z и 23% миллениалов, более чем в два раза чаще, чем бэби-бумеры (6%) и молчаливое поколение (9%), сомневаются в том, что онлайн-безопасность стоит их усилий.
- **Достижимость онлайн-безопасности:** в то время как 59% представителей поколения Z считают, что безопасность в Интернете достижима, другие поколения согласны с более высокими показателями - от 68% до 79%.
- **Чувство контроля:** менее половины представителей поколения Z (44%) чувствуют контроль над своей безопасностью в Интернете, что ниже, чем уверенность, выраженная другими поколениями.
- **Перегруженность информацией:** молодое поколение, особенно поколение Z (35%) и миллениалы (38%), а также молчаливое поколение (45%) чувствуют себя перегруженными информацией о безопасности в Интернете и склонны минимизировать свои действия в Интернете больше, чем поколение X (29%) и бэби-бумеры (28%)

### 5) Роль средств массовой информации

Эти выводы подчёркивают важность средств массовой информации в повышении осведомлённости о безопасности в Интернете и необходимость более доступного обучения по вопросам кибербезопасности.

- СМИ играют важную роль в формировании взглядов людей на онлайн-безопасность. 59% немцев согласились с тем, что СМИ / новости помогают им оставаться в курсе безопасности в Интернете, по сравнению с 44% новозеландцев и 47% французских участников
- СМИ также мотивируют людей предпринимать защитные действия для обеспечения своей онлайн-безопасности. 61% немцев и американцев почувствовали вдохновение на принятие защитных мер в результате освещения событий в СМИ / новостях. Однако новозеландцы чувствовали себя наименее мотивированными освещением новостей / СМИ: 48% согласились и 14% не согласились с этим заявлением
- Несмотря на положительное влияние, 44% участников заявили, что СМИ вызывают страх, а 42% считают, что они чрезмерно усложняют безопасность в Интернете
- В целом, доступ к обучению кибербезопасности был низким во всех странах. 70% французских

участников сообщили, что у них не было доступа к обучению, за ними следуют канадцы (67%). Американцы (44%) сообщили, что у них больше всего возможностей получить доступ к обучению кибербезопасности

#### 6) Обучение кибербезопасности

Эти результаты подчёркивают важность обучения кибербезопасности и его влияние на улучшение поведения в области безопасности. Они также предполагают, что, хотя доступ к обучению доступен некоторым, значительная часть населения по-прежнему не имеет доступа, что указывает на необходимость более широкой доступности и вовлеченности в образовательные инициативы кибербезопасности

- **Доступ к обучению кибербезопасности:** более половины канадцев (59%), новозеландцев (57%), британских участников (56%) и немцев (51%) прошли обучение кибербезопасности на работе. Треть американцев (33%) и немцев (33%) сообщили, что посещали тренировки дома, в то время как французские участники (23%) с большей вероятностью посещали тренировки в общественном месте

- **Обязательное обучение:** прохождение обязательного обучения кибербезопасности на работе или учебном заведении было самым высоким среди британских участников (88%) и самым низким среди французских участников, при этом почти четверть (24%) сообщили, что обучение кибербезопасности не является обязательным занятием
- **Полезность и вовлеченность:** большинство людей оценили обучение кибербезопасности как полезное (84%) и увлекательное (78%), независимо от того, проходили ли они его дома или на работе
- **Изменение поведения:** семьдесят девять процентов участников сообщили, что применили рекомендации кибербезопасности на практике. Обучение повлияло на поведение, такое как лучшее распознавание фишинговых сообщений и сообщение о них (50%), использование надёжных и уникальных паролей (37%) и начало использования MFA (34%)

vi. ПАТЕНТ  
**US20220232015A1**

PREVENTING CLOUD PYMING ATTACKS

Providing resilient cloud computing services against pycning attacks by identifying and mitigating malicious code execution within cloud provider environments through job monitoring, real-time analysis, and corrective action.

The present invention relates generally to cloud computing, and more particularly to preventing malicious code execution within cloud provider environments.



## A. Введение

US20220232015A1 – патент (за авторством Ravi Prasanna и Netskope, Inc.) подан 30 июля 2021 года и опубликован 21 июля 2022 года. Патент описывает решение, которое включает в себя систему сетевой безопасности, расположенную между клиентами и облачными приложениями. Эта система настроена на генерацию синтетического запроса с последующим его внедрением в сеанс приложения для передачи в облачное приложение. Система также включает встроенную логику формирования метаданных, настроенную для выдачи синтетических запросов.

Ниже рассмотрим публикацию US20220232015A1 с целью проанализировать различные аспекты этого документа, углубившись в его технические описания, новизну изобретения, которое в нем раскрывается, и его значение в более широком контексте его области. Также оценим качественную сущность патента, и идеи, которые не только проясняют его содержание, но и подчёркивают его значимость и потенциальное воздействие. Эта работа будет включать критическую оценку структуры документа, формулы изобретения и предлагаемых в нем технологических решений, тем самым обеспечивая детальное понимание его вклада в соответствующую область.

## B. Ключевая идея

Основная идея патента заключается в создании системы сетевой безопасности, которая может эффективно отслеживать и контролировать поток файлов (документов) внутри корпоративной сети, уделяя особое внимание выявлению потенциальных угроз безопасности и управлению ими. Система использует встроенный прокси-сервер в качестве посредника между облаком и корпоративной сетью, контролируя файлы, поступающие извне. Он идентифицирует файлы документов, используя

различные методы и метаданные, в том числе источник файла документа. Система также классифицирует документы как санкционированные (разрешённые без проверки на наличие угроз), внесённые в черный список (автоматически и навсегда блокируемые) или неизвестные (оценённые и потенциально помечённые в карантин для дальнейшего анализа). В патенте подчёркивается использование правил, основанных на политике, сканирование угроз и "песочница" для неизвестных или потенциально вредоносных документов.

В патенте представлено несколько ключевых моментов:

- **Система сетевой безопасности:** Патент описывает систему сетевой безопасности, которая устанавливается между клиентами и облачными приложениями. Эта система предназначена для повышения безопасности в облачных средах
- **Формирование синтетического запроса:** Система настроена на генерацию синтетического запроса и внедрение его в сеанс приложения, который затем передаётся в облачное приложение
- **Логика формирования встроенных метаданных:** Система включает описание логики формирования встроенных метаданных. Эта логика настроена на выдачу синтетических запросов, что может обеспечить дополнительные меры безопасности
- **Разделение синтетических запросов:** Раскрываемая технология относится к встраиваемому прокси-серверу, сконфигурированному с внедрением синтетического запроса. Он может формировать во время сеанса приложения синтетические запросы, которые отделены от входящих запросов
- **Принудительное применение облачной политики:** Внедрение синтетического запроса используется для извлечения метаданных для принудительного применения облачной политики.

### 1) Преимущества

Преимуществами предлагаемого решения являются:

- **Повышенная безопасность:** Система обеспечивает механизм мониторинга и управления потоком файлов документов в корпоративной сети, особенно тех, которые передаются через облачное хранилище
- **Проактивное обнаружение угроз:** Используя синтетические запросы для формирования метаданных, система может проактивно обнаруживать потенциальные угрозы безопасности и реагировать на них до того, как они повлияют на сеть
- **Динамическое применение политик:** Логика формирования встроенных метаданных обеспечивает динамическое применение политик облачной безопасности на основе метаданных в реальном времени, которые могут адаптироваться к изменяющимся ландшафтам угроз

- **Эффективность:** Система может повысить эффективность передачи данных за счёт автоматического блокирования известных вредоносных файлов без необходимости глубокого сканирования угроз, уменьшая задержку
- **Эффективное формирование метаданных:** Встроенная логика формирования метаданных выдаёт синтетические запросы для предоставления метаданных второй точке присутствия
- **Стабильность и согласованность:** Использование системой уникальных идентификаторов файлов гарантирует, что файлы можно будет отслеживать и управлять ими последовательно на протяжении всего их жизненного цикла, даже если их имена изменятся
- **Формирование синтетического запроса:** Система настроена с внедрением синтетического запроса, который может формироваться отдельно от входящих запросов во время сеанса приложения. Это может помочь в улучшении мониторинга и управления сетевым трафиком
- **Защита от вредоносных атак:** Система может идентифицировать и блокировать документы с известных вредоносных веб-сайтов, тем самым защищая сеть от потенциальных угроз
- **Гибкость и динамичность:** Система может адаптироваться к различным экземплярам (личным или корпоративным) и может обрабатывать документы из различных источников, таких как Google Drive, Docs, Sheets, и др.
- **Повышенная эффективность передачи данных:** благодаря автоматическому удалению внесённых в черный список URL-адресов, которые, содержат вредоносные объекты или ссылки, система сокращает время ожидания и повышает эффективность передачи данных

## 2) Недостатки

Недостатками предлагаемого решения являются:

- **Сложность:** Внедрение системы и управление ею могут усложнить сеть инфраструктуру, требуя специальных знаний и потенциально увеличивая административные издержки
- **Ложные срабатывания:** Система может неправильно классифицировать подлинные документы как угрозы (ложные срабатывания) или не обнаруживать реальные угрозы (ложные негативы), что может нарушить нормальные бизнес-операции или сделать сеть уязвимой
- **Обслуживание и обновления:** Хранилище метаданных и правила политики могут нуждаться в регулярных обновлениях, чтобы соответствовать развивающимся угрозам, которые могут быть ресурсоёмкими и требовать постоянного внимания со стороны группы безопасности

- **Влияние на взаимодействие с пользователем:** Процесс блокировки и карантина документов может повлиять на взаимодействие с пользователем, особенно если подлинные документы задерживаются или если пользователям необходимо выполнить дополнительные шаги по обеспечению безопасности
- **Чрезмерная зависимость от известных угроз:** Эффективность системы против известных вредоносных сайтов и файлов может не распространяться на угрозы нулевого дня или сложные атаки, которые ещё не были идентифицированы и классифицированы
- **Влияние на производительность:** Дополнительная обработка, необходимая для формирования синтетических запросов и анализа метаданных, потенциально может повлиять на производительность сети, особенно в средах с высоким трафиком
- **Адаптивность:** Способность системы адаптироваться к новым типам облачных сервисов и приложений может быть ограничена её текущей конструкцией, что, в свою очередь, может потребовать дальнейшей доработки в связи с новыми технологиями
- **Проблемы с конфиденциальностью:** Сбор и анализ метаданных могут вызывать проблемы с конфиденциальностью, в зависимости от типа собираемых данных и способа их использования в системе
- **Стоимость:** Внедрение и эксплуатация такой системы безопасности могут повлечь за собой значительные затраты, включая аппаратное обеспечение и расходы на персонал

## C. Система сетевой безопасности

"Система сетевой безопасности" — это система, предназначенная для повышения безопасности связи между клиентами и облачными приложениями:

- **Взаимодействие:** Система устанавливается между клиентами и облачными приложениями, действуя как посредник или прокси-сервер для мониторинга и потенциального изменения трафика
- **Внедрение синтетических запросов:** Система генерирует синтетические запросы, которые вводятся в сеансы приложения. Эти синтетические запросы используются для взаимодействия с облачными приложениями отдельно от реальных запросов клиентов
- **Встроенное формирование метаданных:** Система включает логику, которая генерирует встраиваемые метаданные в поток трафика. Эти метаданные используются для отправки синтетических запросов, которые могут быть использованы для

различных целей безопасности, таких как применение политики или оценка безопасности

- **Применение облачной политики:** Синтетические запросы используются для извлечения метаданных, которые имеют решающее значение для применения облачной политики безопасности. Это говорит о том, что система может динамически адаптировать и применять меры безопасности
- **Точки присутствия:** Система может включать в себя несколько точек присутствия, которые обеспечивают промежуточный трафик. Эти точки присутствия оснащены встраиваемой логикой формирования метаданных и способны выдавать синтетические запросы
- **Избыточность при синхронизации метаданных:** Система устраняет потенциальные избыточности при синхронизации метаданных между точками присутствия, что важно для поддержания согласованности и эффективности операций по обеспечению безопасности

#### 1) Важность "Системы сетевой безопасности"

Система предназначена для контроля и мониторинга файлов, поступающих извне, особенно тех, которые передаются через облачное хранилище. Система использует встроенный прокси-сервер в качестве посредника между облаком и корпоративной сетью.

Система идентифицирует файлы документов, поступающие в корпоративную сеть, используя различные методы и метаданные, которые идентифицируют источник файла документа. Метаданные размещаются в хранилище метаданных, доступном прокси-серверу. Система позволяет документам, исходящим из санкционированных источников, таких как известные организации с предыдущим опытом работы в корпоративной сети, попадать в сеть без сканирования угроз.

Система также идентифицирует и блокирует файлы документов, полученные с известных вредоносных веб-сайтов. Это веб-сайты и URL-адреса, которые в прошлом были связаны с фишинговыми атаками или каким-либо другим образом ставили под угрозу сетевую безопасность. Хранилище метаданных отслеживает, хранит и поддерживает базу данных всех известных сайтов, внесенных в черный список.

Для неизвестных документов система оценивает их принадлежность и другие свойства метаданных, чтобы идентифицировать источник. Если источник документа не может быть идентифицирован, его доступ в корпоративную сеть временно блокируется. Это включает в себя правила, основанные на политике, и методы сопоставления. Документ помещен в карантин и первоначально проверяется на наличие угрозы. Если будет точно установлено, что может быть задействован вредоносный код, документ попадет в изолированную среду для дальнейшего анализа.

#### D. Формирование синтетического запроса

"Формирование синтетических запросов" является ключевым компонентом системы сетевой безопасности, описанной в патенте. Формирование синтетических запросов — это метод, используемый в синтетическом мониторинге или тестировании, где создаются искусственные запросы для имитации реального пользовательского трафика. Эти запросы используются для взаимодействия с системами, такими как облачные приложения, отдельно от реальных запросов клиентов. Целью формирования таких запросов является тестирование и мониторинг производительности и функциональности систем, помогая выявлять потенциальные проблемы до того, как они затронут реальных пользователей.

- **Определение:** Формирование синтетических запросов включает в себя создание искусственных запросов, имитирующих реальный пользовательский трафик.
- **Назначение:** Синтетические запросы используются для тестирования и мониторинга производительности и функциональности систем. Они могут помочь выявить потенциальные проблемы и гарантировать корректную работу систем.
- **Использование в сетевой безопасности:** В контексте патента синтетические запросы вводятся в сеансы приложения и передаются в облачные приложения. Это позволяет системе взаимодействовать с облачными приложениями и извлекать метаданные в рамках принудительного применения облачной политики.
- **Процесс формирования:** Синтетические запросы могут формироваться программно, часто с использованием скриптов или инструментов, предназначенных для синтетического мониторинга или тестирования. Эти инструменты могут имитировать различные сценарии, типы объектов и переменные среды.
- **Преимущества:** Формирование синтетических запросов позволяет осуществлять упреждающий мониторинг производительности и функциональности системы. Это может помочь выявить проблемы на ранней стадии, прежде чем они затронут реальных пользователей, и может предоставить ценную информацию о времени безотказной работы системы, времени отклика и показателях успешности транзакций.
- **Проблемы:** хотя формирование запросов может дать ценную информацию, это также сопряжено с трудностями. Например, может возникнуть ситуация, когда не полностью воспроизводится непредсказуемость реального поведения пользователей. Кроме того, требуется тщательное проектирование и реализация, чтобы гарантировать, что синтетические запросы точно представляют

взаимодействия, которые они призваны имитировать

Формирование синтетического запроса может использоваться в различных целях:

- **Нагрузочное тестирование:** Синтетические запросы могут использоваться для оценки поведения системы при большой нагрузке, помогая определить, есть ли вероятность сбоя веб-сайта или приложения из-за резкого увеличения трафика пользователей.
- **Мониторинг транзакций:** Разработчики или инженеры по контролю качества могут использовать синтетические запросы, чтобы определить, как система обрабатывает определённый тип запроса
- **Мониторинг компонентов:** В распределённых системах, таких как приложения микросервисов, синтетические запросы могут направляться к конкретным компонентам для измерения их отклика
- **Мониторинг API:** Синтетические тесты API позволяют инженерам оценить, управляют ли API запросами так, как требуется
- **Конфиденциальность данных:** Формирование синтетических данных может позволить создавать более крупные наборы данных, повысить производительность модели и защитить конфиденциальность отдельных пользователей.

Потенциальные области применения:

- **Разработка программного обеспечения и обеспечение качества:** Синтетические запросы могут использоваться для тестирования практически любого типа транзакции или запроса пользователя с любой целью. Если реальный пользователь может инициировать запрос, его также можно отслеживать синтетически
- **Сетевая безопасность:** Синтетические запросы могут использоваться для извлечения метаданных для принудительного применения облачной политики
- **Мониторинг производительности:** Компании могут использовать синтетическое тестирование для активного мониторинга доступности своих сервисов, времени отклика своих приложений и функциональности транзакций клиентов
- **Оптимизация взаимодействия с пользователем:** Синтетический мониторинг может использоваться для понимания того, как реальный пользователь может взаимодействовать с приложением или веб-

сайтом, помогая выявить возможности для оптимизации

### 1) Значение

Значение формирования синтетических запросов заключается в её применении в системе сетевой безопасности для улучшения мониторинга и контроля взаимодействий с облачными приложениями:

- **Упреждающие меры безопасности:** Формирование синтетических запросов используется для упреждающего тестирования и мониторинга производительности и функциональности облачных приложений, что крайне важно для выявления и устранения потенциальных проблем безопасности до того, как они повлияют на реальных пользователей
- **Извлечение метаданных:** Встроенная логика формирования метаданных в системе сетевой безопасности выдаёт синтетические запросы на предоставление метаданных. Затем они используются для принудительного применения облачной политики, позволяя системе динамически адаптировать и применять меры безопасности
- **Применение облачной политики:** Синтетические запросы используются для извлечения метаданных, которые имеют решающее значение для применения облачной политики безопасности. Это говорит о том, что система может динамически адаптировать и применять меры безопасности на основе метаданных, полученных в результате синтетических запросов
- **Улучшенный мониторинг:** Синтетический мониторинг, который включает в себя генерацию синтетических запросов, является важнейшим компонентом мониторинга производительности сети и цифрового взаимодействия. Это позволяет командам ИТ-разработчиков, NetOps и DevOps улучшать взаимодействие с пользователями и оптимизировать критически важные для бизнеса функции
- **Универсальность тестирования:** Формирование синтетических запросов может использоваться для тестирования практически любого типа пользовательских транзакций или запросов для любых целей, обеспечивая комплексный подход к системному тестированию и мониторингу.

### E. Встроенная логика формирования метаданных

Эта логика формирования встроенных метаданных является частью более широкой тенденции в области инноваций в области кибербезопасности, когда компании инвестируют в R&D для создания передовых решений безопасности, способных защитить от возникающих угроз в облачной и сетевой средах.

"Встроенная логика формирования метаданных" является ключевым компонентом системы сетевой безопасности:

- **Определение:** Логика формирования встроенных метаданных относится к способности системы формировать метаданные "встраиваемо" или в режиме реального времени по мере прохождения трафика через систему с целью предоставления дополнительного контекста или информацию о обрабатываемых файлах
- **Функция:** Встроенная логика формирования метаданных настроена на выдачу синтетических запросов. Эти синтетические запросы используются для взаимодействия с облачными приложениями и извлечения метаданных для принудительного применения облачной политики.
- **Роль в сетевой безопасности:** система может динамически применять политики безопасности на основе метаданных, полученных в результате синтетических запросов
- **Точки присутствия:** Система включает в себя несколько точек присутствия, которые обеспечивают промежуточный трафик. Каждая из этих точек присутствия оснащена встраиваемой логикой формирования метаданных и способна выдавать синтетические запросы
- **Избыточности при синхронизации метаданных:** Система устраниет потенциальные избыточности при синхронизации метаданных между точками присутствия. Это важно для поддержания согласованности и эффективности операций по обеспечению безопасности

Цель встраиваемой логики формирования метаданных – выдавать синтетические запросы для взаимодействия с облачными приложениями и извлечения метаданных для принудительного применения облачной политики.

Логика формирования встроенных метаданных работает путём мониторинга потока трафика между клиентами и облачными приложениями. По мере прохождения трафика через систему логика генерирует метаданные в режиме реального времени. Затем эти метаданные используются для выдачи синтетических запросов, которые вводятся в сеансы приложения и передаются в облачные приложения.

Ключевыми моментами являются:

- **Создание метаданных в режиме реального времени:** логика предназначена для формирования метаданных в режиме реального времени по мере прохождения сетевого трафика через систему
- **Выдача синтетических запросов:** настройка на выдачу синтетических запросов, которые отделены от реальных запросов клиентов, для

взаимодействия с облачными приложениями и извлечения необходимых метаданных

- **Применение облачной политики:** метаданные, формируемые встраиваемой логикой, используются для обеспечения соблюдения облачных политик безопасности, позволяя системе динамически адаптировать и применять меры безопасности
- **Операционная эффективность:** встроенное формирование метаданных помогает поддерживать операционную эффективность, гарантируя, что метаданные формируются и применяются к трафику без значительной задержки
- **Управление резервированием:** система может включать в себя несколько точек присутствия со встраиваемой логикой формирования метаданных, и это устраняет потенциальную избыточность при синхронизации метаданных между этими точками
- **Повышенная безопасность:** благодаря встраиваемому формированию метаданных система может проактивно реагировать на угрозы безопасности и более эффективно применять политики

Потенциальные области применения встраиваемой логики формирования метаданных:

- **Сетевая безопасность:** Встроенная логика формирования метаданных может использоваться для повышения сетевой безопасности путём динамического применения политик безопасности на основе метаданных, полученных из синтетических запросов
- **Разработка программного обеспечения и обеспечение качества:** Встроенная логика формирования метаданных может использоваться при разработке и тестировании программного обеспечения для мониторинга и анализа поведения приложений в режиме реального времени
- **Мониторинг производительности:** Встроенная логика формирования метаданных может использоваться для мониторинга производительности систем и приложений в режиме реального времени, помогая выявлять потенциальные проблемы до того, как они затронут реальных пользователей
- **Управление данными:** Встроенная логика формирования метаданных может использоваться в системах управления данными для отслеживания изменений и поддержания согласованности и эффективности операций
- **Разработка API:** логика формирования встроенных метаданных может использоваться

при разработке API для предоставления дополнительного контекста или информации об обрабатываемых данных, повышая функциональность и удобство использования API

- **R&D:** Поддержка воспроизводимых вычислительных исследований путём предоставления метаданных, документирующих вычислительные процессы и происхождение данных
- **Соответствие требованиям и управление:** обеспечение соответствия обработки данных соответствующим нормативным актам и политике управления

#### 1) Значение встраиваемой логики формирования метаданных

Важность "встраиваемой логики формирования метаданных" заключается в том, что она расширяет возможности системы по обеспечению соблюдения политик облачной безопасности и повышению общей безопасности корпоративных сетей:

- **Формирование метаданных:** Встроенная логика формирования метаданных предназначена для выдачи синтетических запросов на предоставление метаданных. Эти метаданные необходимы для работы системы сетевой безопасности, особенно для обеспечения применения политик облачной безопасности
- **Применение облачной политики:** Метаданные, формируемые встраиваемой логикой формирования метаданных, используются для обеспечения соблюдения политик облачной безопасности.
- **Повышение сетевой безопасности:** Встроенная логика формирования метаданных является важнейшим компонентом системы сетевой безопасности. Генерируя и используя метаданные, система может лучше отслеживать и контролировать взаимодействие с облачными приложениями, тем самым повышая общую безопасность корпоративной сети
- **Эффективность и точность:** Централизация бизнес-логики на уровне метаданных, выполняемая встраиваемой логикой формирования метаданных, может помочь устраниć ошибки и повысить эффективность. Это особенно полезно в сложных сетевых средах, где решающее значение имеет точная и эффективная работа

#### F. Отдельные синтетические запросы

Термин "Отдельные синтетические запросы" относится к синтетическим запросам, которые генерируются и выдаются отдельно от входящих запросов во время сеанса приложения. Они не являются ответами на запросы клиентов, а независимо генерируются системой.

Система, описанная в патенте, включает встроенный прокси-сервер, настроенный с возможностью ввода синтетических запросов. Этот прокси-сервер может формировать синтетические запросы, которые отделены от входящих запросов во время сеанса подачи заявки. Эти отдельные синтетические запросы используются для взаимодействия с облачными приложениями и извлечения метаданных для применения облачной политики.

Формирование отдельных синтетических запросов позволяет системе взаимодействовать с облачными приложениями независимо от действий клиента. Это может обеспечить дополнительные меры безопасности, поскольку система может извлекать метаданные и применять политики безопасности динамически

Ключевые особенности:

- **Независимость от клиентских запросов:** Эти синтетические запросы не являются ответами на клиентские запросы, а независимо генерируются системой
- **Взаимодействие с облачными приложениями:** Отдельные синтетические запросы используются для взаимодействия с облачными приложениями и извлечения метаданных для применения облачной политики
- **Поиск метаданных в реальном времени:** формирование отдельных синтетических запросов позволяет системе взаимодействовать с облачными приложениями независимо от действий клиента.
- **Повышенная безопасность:** Использование отдельных синтетических запросов может повысить безопасность облачных приложений, позволяя системе активно извлекать метаданные и применять политики безопасности
- **Потенциальные области применения:** Отдельные синтетические запросы могут использоваться в различных областях, включая сетевую безопасность, мониторинг производительности, разработку программного обеспечения и обеспечение качества, управление данными и разработку API

Потенциальные области применения:

- **Сетевая безопасность:** Отдельные синтетические запросы могут использоваться для повышения сетевой безопасности путём динамического применения политик безопасности на основе метаданных, полученных из синтетических запросов
- **Мониторинг производительности:** Отдельные синтетические запросы могут использоваться для мониторинга производительности систем и приложений в режиме реального времени, помогая

выявлять потенциальные проблемы до того, как они затронут реальных пользователей

- **Разработка программного обеспечения и обеспечение качества:** Отдельные синтетические запросы могут использоваться при разработке и тестировании ПО для мониторинга и анализа поведения приложений в режиме реального времени
- **Управление данными:** Отдельные синтетические запросы могут использоваться в системах управления данными для отслеживания изменений в данных и поддержания согласованности и эффективности операций
- **Разработка API:** Отдельные синтетические запросы могут использоваться при разработке API для предоставления дополнительного контекста или информации об обрабатываемых данных, повышая функциональность и удобство использования API

#### 1) Значимость отдельных синтетических запросов

Использование отдельных синтетических запросов в системе сетевой безопасности повышает способность системы применять политики облачной безопасности, заблаговременно выявлять потенциальные проблемы безопасности и повышать общую безопасность корпоративных сетей:

- **Формирование метаданных:** Встроенная логика формирования метаданных использует отдельные синтетические запросы для формирования метаданных. Эти метаданные имеют решающее значение для обеспечения соблюдения политик облачной безопасности и для функционирования системы сетевой безопасности
- **Упреждающие меры безопасности:** Отдельные синтетические запросы позволяют проводить упреждающее тестирование и мониторинг взаимодействия системы с облачными приложениями. Это может помочь выявить и устранить потенциальные проблемы безопасности до того, как они повлияют на реальных пользователей
- **Применение облачной политики:** Метаданные, полученные в результате отдельных синтетических запросов, используются для применения политик облачной безопасности. Это позволяет системе динамически адаптировать и применять меры безопасности
- **Эффективность и точность:** Использование отдельных синтетических запросов может повысить эффективность и точность системы сетевой безопасности. Генерируя и используя метаданные из этих запросов, система может лучше отслеживать и контролировать взаимодействие с облачными приложениями

#### G. Принудительное применение облачной политики

"Принудительное применение облачной политики" относится к применению политик безопасности в облачных средах на основе метаданных, извлекаемых из синтетических запросов

Система сетевой безопасности, описанная в патенте, настроена на формирование синтетических запросов и внедрение их в сеанс приложения. Эти синтетические запросы передаются в облачное приложение, а ответы предоставляют метаданные. Затем система применяет политику к входящему запросу на основе этих метаданных.

Принудительное применение облачной политики имеет решающее значение для поддержания безопасности в облачных средах. Политики могут включать правила, касающиеся контроля доступа, защиты данных, сетевой безопасности и многое другое. Применяя эти политики, система может предотвращать несанкционированный доступ, защищать конфиденциальные данные и поддерживать целостность сети.

Система, описанная в патенте, улучшает применение облачной политики за счёт использования синтетических запросов для извлечения метаданных. Это позволяет системе динамически применять политики безопасности на основе метаданных, полученных из синтетических запросов, обеспечивая более упреждающий и адаптивный подход к облачной безопасности.

Ключевые моменты:

- **Динамическое применение политики:** Система динамически применяет политики безопасности на основе метаданных, полученных в результате синтетических запросов. Это говорит о том, что система может адаптировать и применять меры безопасности в режиме реального времени
- **На основе метаданных:** применение облачных политик основано на метаданных, извлекаемых из синтетических запросов. Эти метаданные предоставляют системе необходимый контекст для принятия решения о том, какие политики применять
- **Повышение безопасности:** Применение облачной политики является важнейшим аспектом поддержания безопасности в облачных средах. Политики могут включать правила контроля доступа, защиты данных, сетевой безопасности и многое другое
- **Проактивная безопасность:** Система, описанная в патенте, улучшает применение облачной политики за счёт использования синтетических запросов для извлечения метаданных. Это позволяет системе активно применять политики безопасности, обеспечивая более адаптивный подход к облачной безопасности
- **Потенциальные области применения:** принудительное применение облачной политики может использоваться в различных областях,

включая облачную безопасность, контроль доступа, защиту данных, соответствие требованиям и управление рисками

Говоря подробнее про потенциальные области применения стоит выделить:

- **Облачная безопасность:** Применение облачной политики является фундаментальным аспектом облачной безопасности, помогающим защитить данные, приложения и инфраструктуру в облаке
- **Контроль доступа:** Политики могут использоваться для контроля того, кто имеет доступ к определённым ресурсам в облаке, предотвращая несанкционированный доступ
- **Защита данных:** Политики могут использоваться для защиты конфиденциальных данных в облаке, например для шифрования данных в состоянии покоя и при передаче
- **Соответствие требованиям:** применение облачной политики может помочь организациям соблюдать правила и стандарты, связанные с защитой данных и конфиденциальностью
- **Управление рисками:** применяя политики в облаке, организации могут управлять рисками, связанными с безопасностью, конфиденциальностью и соблюдением требований

#### 1) Значимость отдельных синтетических запросов

"Принудительное применение облачной политики" имеет важное значение, поскольку оно относится к принудительному применению политик безопасности в облачной среде. Это предполагает использование синтетических запросов и встраиваемой логики формирования метаданных для обеспечения соответствия трафика данных между клиентами и облачными приложениями установленным политикам безопасности. Это может помочь предотвратить несанкционированный доступ и защитить конфиденциальные данные, тем самым повысив общую безопасность облачной среды.

#### H. Поддержка профиля Google Chrome'

"Поддержка профиля Google Chrome" для обозначения способности системы обрабатывать и интерпретировать информацию о сеансе пользователя, такую как идентификаторы аутентификации и идентификаторы сеанса (cookies), связанные с профилем пользователя Google Chrome:

- **Информация о сеансе пользователя:** когда пользователь открывает файл (например, файл Google Drive, документы, таблицы и т.д.) Из своей корпоративной учётной записи для входа в систему, открытый файл будет содержать информацию об уже вошедшем в систему пользователе, такую как auth\_id и SID (файлы cookie)
- **Идентификация файла:** при текущем подходе этот файл будет идентифицирован как уже вошедший в систему пользователь. Это означает, что система

может распознать действие и связать его с правильным профилем пользователя

- **Пример сценария:** например, если пользователь входит в Gmail с идентификатором "abc@kkrlog.com" и получает документ от внешнего пользователя "xyz@gmail.com". Когда пользователь откроет файл, он покажет, что "abc@kkrlog.com" — это пользователь, выполняющий действие, а экземпляр файла - "kkrlog.com", но "gmail.com" — это фактический экземпляр файла
- **Управление профилем Google Chrome:** Google Chrome позволяет пользователям создавать несколько профилей и управлять ими. У каждого профиля есть свой набор закладок, расширений и настроек для разделения личных действий в Интернете и действий, связанных с работой, обеспечивая конфиденциальность и предотвращая утечку данных.
- **Потенциальные области применения:** Возможность обработки и интерпретации информации о сессиях пользователя, связанной с профилями Google Chrome, может использоваться в различных областях, включая сетевую безопасность, управление данными и оптимизацию взаимодействия с пользователем

#### I. Политика обработки файлов вложений»

Политики обработки файлов-вложений описывают подход к обработке файлов в корпоративной сети, особенно в отношении облачных приложений и служб. Эти политики и механизмы предназначены для повышения безопасности и соответствия требованиям в корпоративной среде, особенно при использовании облачных средств обмена файлами и совместной работы:

- **Две основные политики:** Система различает две основные политики для пользователей в отношении вложений файлов: "разрешённый корпоративный экземпляр" и "блокирующий личный экземпляр"
- **Определение корпоративного экземпляра:** корпоративный экземпляр определяется как санкционированный компанией экземпляр облачного приложения. Даже если владельцем общего файла является внешний пользователь, и экземпляр файла считается корпоративным, активируется политика "разрешённого корпоративного экземпляра", позволяющая пользователю выполнять действия с файлами, предоставляемыми извне
- **Идентификация владельца файла:** Системе необходимо идентифицировать владельца созданного файла. Для предотвращения фишинговых атак и несанкционированного доступа внешним файлам запрещён доступ к корпоративной сети или выполнение каких-либо действий
- **Анализ трафика:** когда пользователь получает документ с Google Диска, Docs, Таблиц, по

электронной почте или общей ссылке, данные транзакции ответа включают владельца файла. Система использует шаблоны, чтобы определить, создан ли документ личной учётной записью или корпоративной

- **Извлечение экземпляра:** Система извлекает экземпляр для операции просмотра файла и заполняет его в качестве владельца файла. Для других действий (загрузка / редактирование) владелец может быть неизвестен в трафике, но file\_id уникален, по крайней мере, для экземпляра
- **Блокировка личных документов:** Система помогает корпоративным пользователям блокировать просмотр документов, созданных лично, и разрешает просмотр только корпоративных документов. Однако это может заблокировать доступ клиентов к персонально созданным документам из их личного экземпляра
- **Определение экземпляра:** когда пользователи просматривают документы с Google Диска, Docs, таблиц и т.д., данные ответа содержат сведения об экземпляре. Если пользователь входит в личную учётную запись, инстансом будет gmail.com, а если пользователь входит в систему с корпоративной учётной записью – корпоративный инстанс

#### J. Технологический процесс

Технологический процесс описывается как процедура оценки файлов документов, совместно используемых в корпоративной сети, в частности, в отношении потенциальных угроз безопасности.

- Вредоносный документ
- Встроенный прокси
- Идентификация документа
- Санкционированные документы
- Сайты, внесенные в Черный список
- Неизвестные документы

Вредоносный документ, созданный на вредоносном веб-сайте, передаётся в облачное хранилище, доступное в корпоративной сети. Цель злоумышленника – сделать документ привлекательным, чтобы к нему могли получить доступ несколько пользователей в корпоративной сети или с помощью удалённых корпоративных устройств.

Встроенный прокси-сервер, являющийся частью системы сетевой безопасности, действует как посредник между облаком и корпоративной сетью, контролируя файлы, поступающие извне корпоративной сети.

Файлы документов, пытающиеся поступающие в корпоративную сеть, идентифицируются методами, описанными в патенте, и другими метаданными, которые идентифицируют источник файла документа. Метаданные размещаются в хранилище метаданных, доступном встраиваемому прокси-серверу.

На внутренние корпоративные документы всегда распространяются санкции. Документы, созданные за пределами корпоративной сети, если на них наложены санкции, всегда допускаются в корпоративную сеть без проверки на угрозы. Это документы из известных источников, включая крупные организации и организации, которые ранее имели дело с корпоративной сетью.

Файлы документов, полученные с известных вредоносных веб-сайтов, идентифицируются встроенным прокси-сервером как сайты, внесённые в черный список. Это веб-сайты и URL-адреса, которые в прошлом были связаны с фишинговыми атаками или каким-либо другим образом ставили под угрозу сетевую безопасность. Хранилище метаданных отслеживает, сохраняет и поддерживает в базе данных все известные сайты, внесённые в черный список. Документы, полученные в этой категории, автоматически и навсегда блокируются.

Неизвестные документы оцениваются на предмет их принадлежности и других свойств метаданных, которые позволяют идентифицировать источник неизвестного документа. Если источник документа не может быть идентифицирован, его доступ в корпоративную сеть временно блокируется. Для этого используются правила, основанные на политике, включая методы сопоставления. Документ помещается в карантин и первоначально проверяется на наличие угрозы. Большая часть этой работы требует участия администратора сетевой безопасности. Если есть уверенность, что может быть задействован вредоносный код, документ попадёт в изолированную среду для дальнейшего анализа.



vii. **Источники  
инновационности  
Китая  
(по версии DGAP)**



#### A. Введение

В статье "The Sources of China's Innovativeness" обсуждается, как Китай превратился из предполагаемого «подражателя» в инновационный центр. Автор выделяет пять причин (достоинств), которые способствовали успеху Китая в области инноваций, однако отмечается, что будущий успех Китая не является неизбежным и зависит от сочетания выбора внутренней политики и событий в международной среде.

Ниже рассматриваются определённые причины становления Китая с целью анализа различных аспектов, способствующих растущей роли Китая как глобального инновационного центра, что позволяет расширить понимание факторов сильных и слабых сторон Китая.

Основное внимание уделяется анализу факторов, которые способствовали превращению Китая в инновационный центр, и обсуждению последствий этой трансформации для западных стран.

#### Пять причин инновационной активности Китая

- Умелое управление протекционизмом на большом рынке:** Китай использовал масштаб своего рынка и степень протекционизма, чтобы впитывать новые тенденции с Запада, защищая при этом зарождающиеся китайские технологические фирмы.
- Привлечение знаний в страну:** Китай привлекает знания и передачу технологий различными способами, включая возвращение китайских учёных из-за рубежа, принудительную передачу технологий и становление (страны) неотъемлемой частью глобальных цепочек поставок.
- Связь с западными субъектами:** несмотря на свою цель обеспечения самостоятельности, Китай имеет

глубокие связи с субъектами частного сектора и исследовательскими институтами на Западе, что включает импорт передовых технологий западного производства, целенаправленное приобретение ноу-хау и долгосрочное сотрудничество с западными университетами.

- Партийно-государственное руководство вместо контроля:** роль партии-государства в Китае сместилась с контроля на руководство экономической деятельностью, сигнализируя широкому кругу участников о главных партийно-государственных приоритетах и поощряя эксперименты в таких областях, как технологии.
- Внутренняя конкуренция с китайскими особенностями:** Китай создал конкурентную среду, поощряющую инновации, при этом значительную роль играют государственные предприятия.

#### B. Причина 1: Протекционизм Огромного рынка

Обнаружив «проницаемость Великого брандмауэра, который служит для фильтрации нежелательного контента из китайского Интернета», внешние наблюдатели часто бывают озадачены его эффективностью. Такая проницаемость объясняется не отсутствием у Китая потенциала, а скорее преднамеренной калибровкой протекционистских мер. В течение последних двадцати лет Китай стратегически извлекал выгоду как из размеров своего рынка, так и из масштабов своей протекционистской политики. Рынок Китая с его населением в 1,4 миллиарда человек и предполагаемой численностью среднего класса около 400 миллионов в 2017 году был невероятно привлекательным для иностранных предприятий, включая крупные технологические фирмы. Потенциальные возможности, предоставляемые огромным китайским рынком, риски капиталистической жадности.

##### 1) Ключевые моменты:

В этом разделе обсуждается, как Китай использовал масштаб своего рынка и степень протекционизма, чтобы впитывать новые тенденции с Запада, одновременно защищая зарождающиеся китайские технологические фирмы

В разделе также отмечается, что подход Китая к становлению инновационным существенно отличается от западного подхода

Также выясняется, что Китаю удалось совершить этот подвиг несмотря на то, что его правительство ужесточило контроль над рынками, высказываниями и политикой

Большой, частично защищённый рынок Китая стал ключевым фактором его роста как технологической державы и для сохранения конкурентоспособности США Вашингтону следует изучить определённые элементы стратегии Китая, включая готовность экспериментировать с про-инновационной политикой

Это также предполагает, что для поддержания конкурентоспособности США Вашингтону следует изучить определённые элементы стратегии Китая, включая

готовность экспериментировать с про-инновационной политикой

#### C. Причина 2: Привлечение технологий и знаний в Китай

По мере улучшения экономических условий и качества жизни в Китае китайские учёные и исследователи, которые обучались и работали на Западе, все чаще предпочитали возвращаться на родину. Эта тенденция была обусловлена не только растущей привлекательностью Китая, но и целевыми программами найма талантов, такими как программа выдающейся тысячи талантов и её аналог для молодых специалистов – программа Young Thousand Talents. Эти инициативы, курируемые ассоциацией вернувшихся с Запада учёных Отдела работы Объединённого фронта КПК, предлагали такие стимулы, как престижные звания, конкурентоспособные зарплаты, визовые льготы и щедрое финансирование исследований. Сообщается, что в период с 2008 по 2018 год эти программы привлекли около 7000 стипендиатов вернуться в Китай. Хотя оценка программы "Тысяча молодых талантов" подтвердила её эффективность, также был отмечен дефицит в привлечении академических талантов высшего уровня. Несмотря на различные мнения о степени успеха Китая в этой области, западные спецслужбы выразили обеспокоенность по поводу передачи знаний, которые потенциально могут усилить военный потенциал Китая.

##### 1) Ключевые моменты:

В этом разделе обсуждается, как Китай привлекал передачу знаний и технологий из-за рубежа, включая возвращение китайских учёных, принудительную передачу технологий и интеграцию в глобальные цепочки поставок, что стало ключевым фактором его роста как технологической державы

Также отмечается, что многие китайские технологические гиганты продолжают импортировать передовые технологии западного производства, слишком хорошо зная об их превосходном качестве

Также выясняется, что Китаю удалось совершить этот подвиг несмотря на то, что его правительство ужесточило контроль над рынками, высказываниями и политикой

Это также предполагает, что для поддержания конкурентоспособности США Вашингтону следует изучить определённые элементы стратегии Китая, включая готовность экспериментировать с про-инновационной политикой

#### D. Причина 3: Связь с частными технологиями и исследованиями на Западе

Стремление Китая к местным инновациям не отменяет его зависимости от Запада в плане технологий и знаний. Эта в контексте инновационной стратегии Китая, включает в себя многогранный подход. Во-первых, Китай стремится к самостоятельности, стремясь заменить иностранные технологии отечественными альтернативами. Несмотря на эту цель, китайские технологические гиганты продолжают импортировать западные технологии из-за их превосходного качества. Эта зависимость стала особенно очевидной, когда западные санкции были направлены

против китайских технологических компаний, подчеркнув иронию стремления Китая к самостоятельности. В результате этих санкций китайские компании по производству бытовой электроники, такие как Oppo, Vivo и Xiaomi, все чаще обращаются к отечественным поставщикам либо из-за ограниченного доступа к западным технологиям, либо в ожидании более широких санкций. Этот сдвиг принёс значительную пользу отечественному производителю полупроводников UNISOC, доля которого на мировом рынке чипсетов выросла с менее чем 3% до более чем 10% в период с 2019 по 2022 год.

##### 1) Ключевые моменты:

Китай, несмотря на свою политическую цель достижения самостоятельности, полагается на глубокие связи с субъектами частного сектора и исследовательскими институтами на Западе

Эти связи являются частью стратегии Китая по достижению максимальной самостоятельности путём замены высокотехнологичной продукции иностранного производства местными инновациями

Это также подразумевает, что подход Запада к ограничению передачи технологий Китаю, возможно, не полностью подавляет инновационные возможности Китая, поскольку страна уже усвоила большую часть знаний и продолжает участвовать в международном сотрудничестве

Важным выводом является то, что инновационная стратегия Китая многогранна, включая как развитие внутреннего потенциала, так и стратегическое использование западных технологий и знаний

В этом разделе также предполагается, что политика Запада, направленная на ограничение технологического прогресса Китая, должна учитывать нюансы и взаимосвязанную природу глобальных инновационных экосистем

#### E. Причина 4: Руководящая роль государства

Хотя централизованное планирование часто рассматривается как препятствие творчеству и инновациям, подход Китая к планированию значительно изменился по сравнению с эпохой строго контролируемой экономики Мао Цзэдуна. Текущие пятилетние планы (FYPS), реализуемые Китаем, являются не исчерпывающими экономическими директивами, а скорее стратегическими рамками, которые определяют приоритеты центрального правительства для широкого круга участников, включая частный сектор, субнациональные партийно-государственные структуры и государственные предприятия. Эти FYPS инициируют циклы планирования и исполнения, которые охватывают пять лет, в течение которых они направляют экономическую деятельность, не регулируя её на микроуровне. Субнациональные и секторальные планы дополнительно детализируют эти приоритеты по регионам и секторам экономики, однако они остаются достаточно широкими, чтобы обеспечить интерпретацию и гибкость при их реализации. Такая гибкость побуждает местных чиновников экспериментировать, особенно в технологических секторах, выделенных FYPS. Целенаправленное

дерегулирование в этих секторах также используется для стимулирования инноваций. Таким образом, партийно-государственное планирование в современном Китае сводится не столько к строгому контролю, сколько к политической сигнализации, задающей направление и способствующей инновациям на субнациональном уровне.

#### 1) Ключевые моменты:

Роль партии-государства в Китае сместилась с контроля на руководство экономической деятельностью

Руководство государства-участника сыграло важную роль в создании конкурентной среды, поощряющей инновации

Это также свидетельствует о том, что руководящие указания государства-участника сыграли важную роль в создании конкурентной среды, поощряющей инновации

#### F. Причина 5: Конкуренция на внутреннем рынке с китайскими особенностями

В пределах страны и рынка существует острая конкуренция, которая, хотя и отличается от западной конкуренции, является ключевой движущей силой технологического прогресса. Основной силой, продвигающей вперёд сектор цифровых технологий Китая, стало появление частных компаний, созданных предпринимателями. Среди пяти крупнейших китайских компаний—разработчиков программного обеспечения — Huawei, JD.com, China Mobile, Alibaba и Tencent — только China Mobile принадлежит государству. Остальные были запущены частными лицами, при этом Tencent даже получала поддержку от венчурного капитала США. Хотя эти компании, несомненно, извлекли выгоду из поддержки партии-государства, предпринимательский дух и решения их основателей сыграли решающую роль в их успехе. Эти "красные предприниматели" должны поддерживать тесные связи с правительством, но они остаются конкурентоспособными бизнесменами, стремящимися к доминированию на рынке.

#### 1) Ключевые моменты:

В конкурентной среде, создаваемой Китаем, значительную роль играют государственные предприятия. Эта конкуренция, характеризующаяся сочетанием государственных и частных предприятий, уникальна для Китая и сыграла важную роль в стимулировании инноваций и роста.

#### G. Препятствия

Пять препятствий, по одному на каждое из Пяти достоинств, которые сделали Китай инновационным, ставят под угрозу устойчивость превращения Китая в инновационный центр. Анализ этих препятствий помогает оценить перспективы КНР оставаться инновационной страной.

#### 1) Препятствие 1: Растущий протекционизм

Огромный рынок Китая по-прежнему характеризуется частичным протекционизмом. Однако в последние годы ряд мер внутренней политики ограничили трансграничный поток информации и знаний. В 2018 году Министерство промышленности и информационных технологий Китая объявило, что VPN-сервисы, обходящие Great Firewall, в будущем потребуют одобрения правительства. Это сделало

большинство широко используемых VPN-сервисов незаконными. С тех пор несколько VPN-сервисов были закрыты, приостановлены или были вынуждены заплатить высокие штрафы за нарушение закона Китая о кибербезопасности.

#### a) Ключевые моменты:

Общие аргументы в поддержку протекционизма включают национальную безопасность, защиту потребителей, сохранение рабочих мест и отраслей промышленности, а также развитие зарождающихся отраслей.

Растущий протекционизм вызывает обеспокоенность по поводу будущего глобализации и потенциальных негативных последствий для мировой экономики.

Протекционистские меры могут сделать мир менее устойчивым, более неравным и более склонным к конфликтам.

Несмотря на намерения защитить отечественную промышленность, протекционизм может иметь непреднамеренные последствия, такие как ограничение потребительского выбора и снижение общей экономической эффективности.

Экономисты и политики часто отвергают протекционизм как решение экономических проблем, выступая вместо этого за перераспределение доходов от победителей к проигравшим в мировой торговле.

Протекционистская политика, хотя и направлена на поддержку национальной экономики, может иметь более широкие негативные последствия для международной торговли и экономического роста.

Дебаты о ценности протекционизма продолжаются, аргументы как за, так и против него основаны на его влиянии на рабочие места, ВВП и внутреннюю конкурентоспособность.

Любой политический ответ на риски в нынешней глобальной торговой системе должен учитывать сложное взаимодействие между моделями торговли, факторами, специфичными для конкретной страны, и необходимостью реформ и институтов, поддерживающих производительность и гибкость.

#### 2) Препятствие 2: Барьеры для входа на рынок

Подобно тому, как Китай ужесточил контроль над своим частично защищённым рынком, КНР также усложнила доступ иностранных компаний на рынки Китая. В более общем плане секьюритизация экономики в Китае является Вторым препятствием для китайской инновационности. Например, пересмотренная версия Закона о контрразведке от 2023 года резко расширяет определение шпионажа в законе. Неоднозначное определение секретов национальной безопасности может в итоге привести к наказанию за традиционную деловую деятельность. Данные, необходимые для традиционных исследований акционерного капитала для оценки риска, легко могут быть признаны представляющими национальный интерес, а обращение с ними может быть кriminalизировано. Это может иметь огромные сдерживающие последствия, которые сведут к минимуму любое трансграничное

сотрудничество, требующее значительных объёмов данных, включая экономический и технологический обмен.

a) Ключевые моменты:

Барьеры для входа на рынок относятся к препятствиям, которые затрудняют выход новых фирм на рынок, хотя могут привести к экономии за счёт масштаба, лояльности к бренду, госрегулированию, и патентуемым технологиям.

Высокие начальные затраты или другие препятствия могут помешать новым конкурентам легко войти в отрасль или сферу бизнеса

Эти барьеры могут быть вызваны естественным путём, вмешательством правительства или давлением со стороны существующих фирм и могут защитить действующие фирмы, но они также могут подавлять конкуренцию и инновации, потенциально приводя к доминированию на рынке и монополистическому поведению

Директивным органам необходимо учитывать эти факторы при разработке нормативных актов и политики, способствующих созданию конкурентной и инновационной рыночной среды

3) Препятствие 3: Враждебная среда

Экономическая и технологическая зависимость все чаще воспринимается как потенциальная угроза. “Вооружённая взаимозависимость” вытеснила традиционную интерпретацию того, что взаимная зависимость является стабилизирующей силой в международных делах. Несколько стратегий Китая отражают эту тенденцию секьюритизации. Особое значение для растущей изоляции Китая может иметь введение в действие Закона КНР о разведке от 2017 года, статья 7 которого требует, чтобы все китайские организации сотрудничали со службами безопасности КНР по запросу. Это вызвало подозрения и озабоченность на Западе. Например, доверительные отношения исследовательского сотрудничества были поставлены под сомнение, поскольку китайские партнёры по сотрудничеству по закону были обязаны раскрывать информацию китайским органам безопасности по запросу.

a) Ключевые моменты:

Враждебная среда относится к условиям, неблагоприятным или бросающим вызов бизнесу или инновациям

Эти условия могут включать регуляторные барьеры, острую конкуренцию, нехватку ресурсов или политическую нестабильность

Компаниям, работающим во враждебной среде, необходимо разрабатывать стратегии выживания и процветания, такие как инновационные стратегии или стратегии укрепления доверия

Враждебная среда может стимулировать инновации, поскольку компании вынуждены находить новые способы преодоления трудностей и добиваться успеха

4) Препятствие 4: Централизация контроля во время кризиса

Наиболее примечательно, что в марте 2023 года было объявлено о создании новой Центральной комиссии по науке и технологиям при Центральном комитете КПК что рассматривается как ужесточение контроля над научно-технической политикой. Такое ужесточение контроля происходит во время экономического кризиса. Следовательно, руководящая функция партии-государства – высвобождение огромных ресурсов для инноваций – оказывается под давлением централизованного контроля и меньшего количества ресурсов в системе.

a) Ключевые моменты:

Централизация контроля во время кризиса может привести к более скординированному и единому реагированию на насущные вызовы.

Такая централизация может включать постановку целей, предписание ролей и полномочий, а также определение правил для поддержания структуры и порядка.

Централизация во время кризисов может быть как средством, так и препятствием для изменений, в зависимости от того, как ими управляют и в каком контексте они происходят.

Политики и лидеры должны осознавать, что централизация может привести к сбоям, и стремиться управлять ею таким образом, чтобы поддерживать, а не препятствовать инновациям и адаптации.

5) Препятствие 5: Нагнетание неуверенности

Пятым и последним препятствием является растущая незащищённость в Китае, как в технологическом секторе, так и в обществе в целом. Все началось с того, что было названо “ректификацией” компаний частного сектора в технологическом секторе, в первую очередь Alibaba и основателя компании Джека Ма, но также Tencent и Didi. Эти и другие компании были объектом различных расследований, которые широко интерпретировались как репрессии в отношении компаний частного сектора, которые стали слишком влиятельными с точки зрения руководства КПК. Независимо от того, верна ли эта интерпретация, исправление экономики платформ внесло неопределённость в сектор и может отбить у предпринимателей охоту рисковать. Лидеры КПК сейчас пытаются успокоить частных технологических предпринимателей и дали понять, что исправление ситуации подошло к концу.

Усиление незащищённости может привести к более осторожному подходу к инновациям, поскольку предприятия могут неохотно инвестировать в новые технологии или процессы в неопределенной среде

Однако отсутствие безопасности также может стимулировать инновации, поскольку предприятия вынуждены адаптироваться и находить новые решения для преодоления проблем



<sup>viii.</sup> ЧЕМУ ЖЕ УЧИТ  
**СТАНОВЛЕНИЕ КИТАЯ**  
КАК СТАНОВЛЕНИЕ  
ИННОВАЦИОННОЙ  
ДЕРЖАВЫ  
(ПО ВЕРСИИ DGAP)



## A. Введение

Несмотря на то, что ещё совсем недавно существовало мнение о том, что Китай не способен на инновации и лишь копирует западные технологии, сегодняшняя реальность демонстрирует совершенно иное. На базе публикации "Was uns Chinas Aufstieg zur Innovationsmacht lehrt" от DGAP подробно анализируются различные аспекты, которые способствовали трансформации Китая в инновационную силу.

В частности, будет рассмотрена роль международного сотрудничества, влияние государственной политики и стратегических планов, а также способность Китая к адаптации и преодолению технологических и инновационных барьеров. Этот анализ предоставит качественную выжимку ключевых моментов, которые позволили Китаю достичь таких высот в сфере инноваций, и рассмотрит, какие уроки могут извлечь другие страны из этого опыта

## B. Основные выводы

Ключевыми выводами из доклада о становлении инновационной мощи Китая являются:

- **Глобальная экономическая мощь:** Китай превратился в экономическую сверхдержаву, конкурирующую с США во многих аспектах и влияющую на глобальную экономическую политику.
- **Инновации и передовые отрасли промышленности:** инвестиции Китая в НИОКР и интеллектуальную собственность повысили его глобальную конкурентоспособность в области инноваций.
- **Стратегия в области обороны и безопасности:** национальная стратегия Китая включает акцент на инновациях для поддержки его целей в области обороны и безопасности, включая такие инициативы, как "Сделано в Китае 2025".

- **Вызовы и возможности:** подъем Китая сопряжен с трудностями, но также открывает возможности для других стран с точки зрения торговли, инвестиций и сотрудничества в области инноваций.

## C. Второстепенные выводы

Второстепенные выводы доклада о становлении инновационной мощи Китая включают:

- **Экономические инициативы и глобальное влияние:** экономические инициативы Китая могут значительно расширить его экспортные и инвестиционные рынки, увеличив его глобальную "мягкую силу".
- **Вызовы экономическому росту:** Китай сталкивается с трудностями в поддержании экономического роста, такими как необходимость экономических реформ и последствия незавершённого перехода к рыночной экономике.
- **Интеграция в мировую торговлю:** ожидается, что интеграция Китая в глобальную торговую систему принесёт пользу мировой экономике, но это также может привести к краткосрочным негативным эффектам из-за перераспределения между странами.
- **Технологическое развитие и производительность:** поскольку технологическое развитие Китая приближается к уровню развитых стран, рост производительности и ВВП в Китае может замедлиться, если он не станет крупным центром новых инноваций.
- **Инновационный потенциал:** Китай превзошёл США по общему объёму инновационной продукции и быстро догоняет их в корпоративных исследованиях и разработках, что бросает вызов лидерству США в области инноваций.
- **Последствия для инвесторов и цепочек поставок:** способность Китая мобилизовать капитал позволила ему догнать западные экономические державы, оказывая влияние на глобальные цепочки поставок и инвестиции.

## D. Экономические проблемы Китая

Китай сталкивается с рядом проблем в поддержании своего экономического роста. К ним относятся замедление роста, растущий долг, демографические сдвиги, экологические проблемы, напряжённость в мировой торговле и технологическая конкуренция. Замедление некогда взрывных темпов роста ВВП является серьёзной проблемой. Факторы, способствующие этому замедлению, включают снижение отдачи от инвестиций и сокращение численности населения. Китай также сталкивается с проблемами, связанными с доступом к передовым технологиям и высококвалифицированным кадрам, особенно в областях, имеющих решающее значение для технологического лидерства, таких как производство полупроводников.

В области инноваций Китай добился значительного прогресса и сейчас конкурирует с такими странами с развитой экономикой, как США и Швеция. Десятилетия быстрого экономического роста позволили Китаю инвестировать в ключевые области, стимулирующие инновации, такие как R&D и создание новой интеллектуальной собственности. Однако Китай по-

прежнему отстает от некоторых аспектов инноваций, включая проблемы с высшим образованием, бизнес-средой и культурой труда. Несмотря на эти проблемы, инновационный потенциал Китая значительно вырос, и в настоящее время он считается мировым лидером в определенных областях инноваций.

Экономический рост Китая имеет значительные последствия для глобальной цепочки поставок. Как крупнейший участник глобальных производственно-сбытовых цепочек (20% мировой торговли продукцией обрабатывающей промышленности), изменения в экономической политике и темпах роста Китая могут иметь далеко идущие последствия. Пандемия COVID-19 и другие геополитические события выясвили зависимость многих экономик от Китая и привели к сбоям в глобальной цепочке поставок. Эти события побудили некоторые компании диверсифицировать свое производство за пределами Китая.

В долгосрочной перспективе восстановление экономического баланса Китая может создать новые возможности для экспортёров обрабатывающей промышленности, хотя это может снизить спрос на сырьевые товары. Влияние Китая на другие развивающиеся экономики посредством торговли, инвестиций и идей растёт, и многие из сложных проблем развития, с которыми сталкивается Китай, актуальны и для других стран.

#### E. Экологические проблемы

Быстрый экономический рост Китая привёл к серьёзным экологическим проблемам, в том числе:

- **Энергия и загрязнение:** рост ВВП сопровождался значительным увеличением чистого импорта энергии, загрязнением и разрушением окружающей среды и увеличением выбросов CO<sub>2</sub>. Эти проблемы достигли критической точки, поскольку доля Китая в глобальных выбросах значительно возросла
- **Изменение климата:** являясь крупнейшим в мире источником выбросов парниковых газов, углеродоёмкие отрасли промышленности Китая вносят свой вклад в загрязнение воздуха, нехватку воды и почвы. Уголь, на долю которого приходится значительная часть энергопотребления Китая, является основным фактором в решении этих экологических проблем
- **Деградация окружающей среды:** лесные ресурсы истощились, что привело к опустыниванию, наводнениям и исчезновению биологических видов. Ухудшение состояния окружающей среды также имеет существенные последствия для социального и экономического благосостояния китайского народа
- **Стоимость загрязнения:** в период с 2004 по 2012 год загрязнение окружающей среды обошлось экономике Китая в 3,05% ВВП. Страна должна изменить траекторию своего экономического роста, чтобы достичь устойчивого развития и справиться с "накопительным эффектом" массового загрязнения

#### F. Меры, принятые Китаем для борьбы с загрязнением окружающей среды

Китай принял ряд мер по борьбе с загрязнением окружающей среды. Правительство реализовало план по снижению концентрации опасных частиц в городах, что привело к значительному снижению уровня загрязнения

воздуха во многих регионах, хотя некоторые районы по-прежнему сильно подвержены нему.

Китай предпринимает усилия по сокращению загрязнения воздуха за счёт финансирования экологически чистой энергетики. Это включает в себя предоставление предприятиям финансирования для сокращения загрязняющих веществ в воздухе и выбросов углерода. Также принимаются меры по замене угля природным газом для отопления жилых и коммерческих помещений, замене половины производства электроэнергии на угле в Китае возобновляемыми источниками энергии или атомной энергетикой и утилизации транспортных средств, загрязняющих окружающую среду.

Ключевые тезисы:

- **Сокращение сталелитейных мощностей:** в период с 2016 по 2017 год Китай закрыл сталелитейные мощности на 115 миллионов тонн, при этом планируются дальнейшие сокращения.
- **Контроль выбросов транспортных средств:** в крупных городах, Пекин, Шанхай и Гуанчжоу, транспортные выбросы контролируются путём ограничения количества автомобилей на дороге.
- **Обеспечение соблюдения стандартов выбросов:** производство моделей автомобилей, которые не соответствовали стандартам экономии топлива, было приостановлено в конце 2017 года.
- **Прозрачность и мониторинг:** создана общенациональная сеть, состоящая из более чем 5000 мониторов загрязнения воздуха.
- **Финансирование экологически чистой энергетики:** инвестиции оборудование для удаления твёрдых частиц и дымовых газов, и сокращению загрязняющих веществ в воздухе и выбросов углерода путём инвестирования в экологически чистую энергию.
- **Комплексные меры:** Китай принял срочные меры по борьбе с загрязнением окружающей среды из различных источников, включая сжигание угля, строительство и бытовое топливо. Транспортный сектор был нацелен на развитие электромобилей.

#### G. Последствия старения населения

Ожидается, что старение населения Китая окажет несколько последствий на его экономический рост:

- **Сокращение предложения рабочей силы:** сокращение численности населения трудоспособного возраста, приведёт к снижению темпов экономического роста Китая примерно на 1 процентный пункт ежегодно с 2035 по 2050 год.
- **Расходы на социальное обеспечение:** быстрое старение населения создаёт проблемы с точки зрения расходов на социальное обеспечение, которые могут повлиять на экономический рост
- **Замедление потребления:** меньшее количество людей означает меньшее внутреннее потребление, что приводит к замедлению экономического роста.

## *H. Влияние старения населения Китая на расходы на социальное обеспечение*

Быстрое старение населения Китая создаёт серьёзные проблемы для расходов на социальное обеспечение и экономического роста. По мере увеличения средней продолжительности жизни населения Китая отдельные лица все чаще получают пенсии, что приводит к росту расходов на благотворительное страхование. По оценкам, к 2040 году 28 процентов населения Китая будут старше 60 лет, что является нынешним законным пенсионным возрастом для большинства мужчин в стране. Ожидается, что эта тенденция приведёт к увеличению расходов на социальное обеспечение и медицинское обслуживание, что может вытеснить другие расходы.

## *I. Расходы Китая на социальное обеспечение по сравнению с другими странами*

Расходы Китая на социальное обеспечение составили 11,8% его ВВП в 2019 году, что ниже, чем в США и значительно ниже, чем в странах ОЭСР. Для сравнения, государственные социальные расходы в Японии составляли около 22% ВВП и около 20% в Новой Зеландии, в то время как в Китае они составляли около 10% ВВП.

## *J. Влияние на глобальную торговлю*

Экономический рост Китая имеет последствия для напряжённости в глобальной торговле:

- **Торговые споры:** торговая напряжённость между США и Китаем негативно сказалась на потребителях и производителях в обеих странах, сократив товарооборот между ними. Хотя дефицит двустороннего торгового баланса в целом остаётся неизменным, напряжённость может нарушить глобальные цепочки поставок
- **Геополитические риски:** экономическая политика и темпы роста Китая, наряду с внешними факторами, такими как геоэкономическая фрагментация, существенно влияют на динамику мировой торговли
- **Влияние на мировой рынок:** экономическое влияние Китая в создании стоимости и торговле обрабатывающей промышленностью означает, что изменения в экономической политике и темпах роста Китая могут иметь далеко идущие последствия для структуры мировой торговли.

## *K. Последствия экономического роста Китая для напряжённости в мировой торговле*

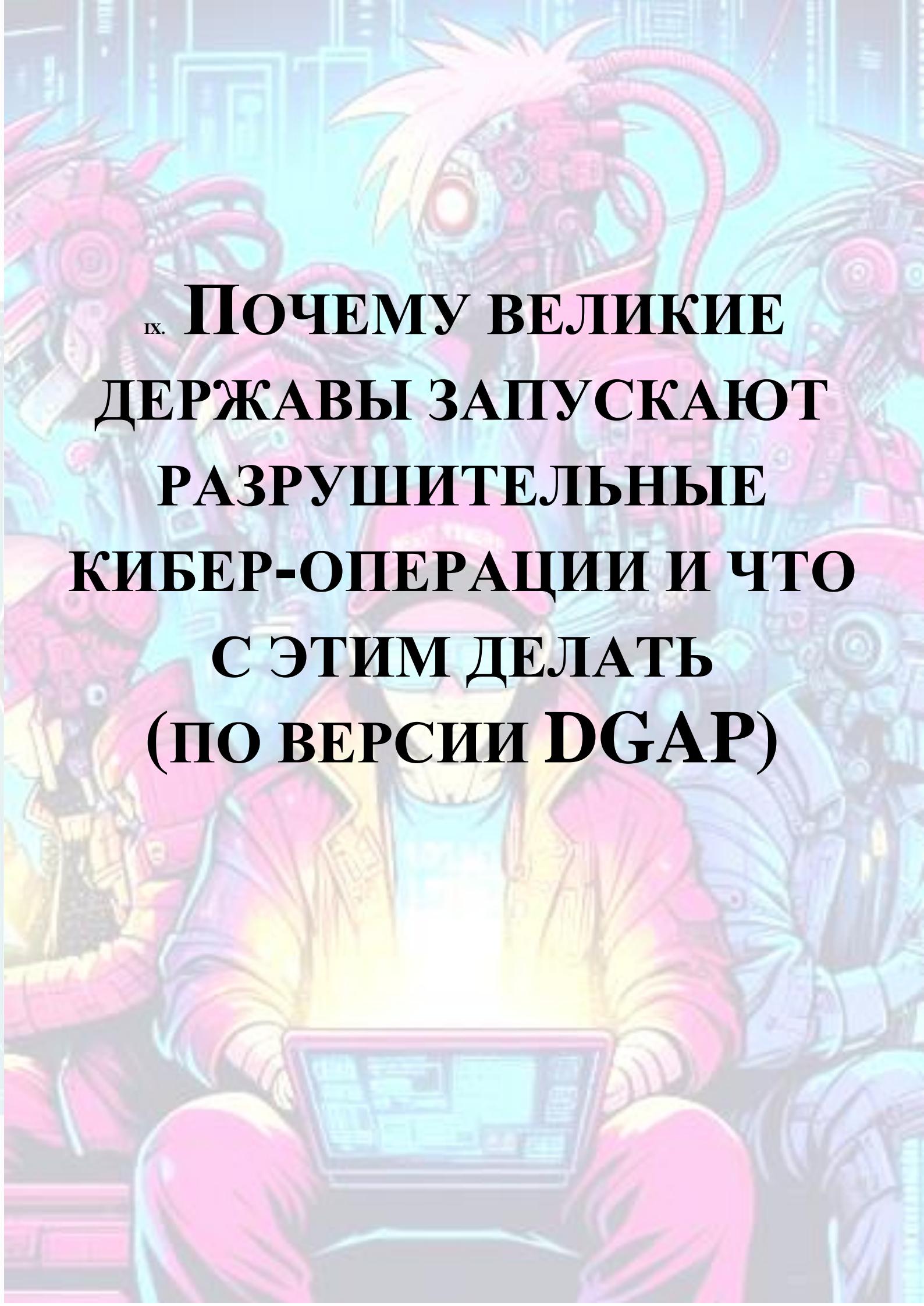
Экономический рост Китая имеет значительные последствия для напряжённости в глобальной торговле. Торговая напряжённость между США и Китаем негативно сказалась на потребителях и производителях в обеих странах, сократила торговлю между двумя странами и потенциально может нарушить глобальные цепочки поставок. Тарифы, введённые обеими странами, существенно не изменили дефицит двустороннего торгового баланса, но создали торговые возможности для других стран.

Кроме того, напряжённость между Китаем и Западом, включая вопросы, связанные с торговыми тарифами, технологическим соперничеством и обвинениями в шпионаже, подрывает давно налаженные цепочки поставок и потенциально может привести к росту инфляции и процентных ставок. Однако эта напряжённость также может создать возможности для развивающихся стран и технологических гигантов, которые соответствуют динамике власти

## *L. Потенциальные последствия экономического роста Китая для глобальной цепочки поставок*

Экономический рост и перестройка глобальной цепочки поставок могут привести к нескольким последствиям:

- **Избыточное предложение и недостаточный спрос:** перестройка глобальной цепочки поставок может привести к переизбытку предложения, недостаточному спросу и проблемам с занятостью.
- **Зависимость от Китая:** сбои в цепочке поставок в результате пандемии подчеркнули зависимость многих экономик от Китая, побудив некоторые компании диверсифицировать своё производство за пределами Китая.
- **Торговля и производство:** центральная роль Китая в глобальных цепочках создания стоимости и торговле обрабатывающей промышленностью означает, что изменения в экономической политике Китая и темпах роста могут иметь далеко идущие последствия для структуры мировой торговли.
- **Перестановки в цепочках поставок:** компании и правительства уделяют больше внимания устойчивости, чем эффективности, что приводит к некоторым перестановкам в цепочках поставок, при этом часть производства переносится из Китая.



**ix. ПОЧЕМУ ВЕЛИКИЕ  
ДЕРЖАВЫ ЗАПУСКАЮТ  
РАЗРУШИТЕЛЬНЫЕ  
КИБЕР-ОПЕРАЦИИ И ЧТО  
С ЭТИМ ДЕЛАТЬ  
(ПО ВЕРСИИ DGAP)**



## A. Введение

Статья DGAP "Why major Powers launch destructive cyber operations and what to do about it" является частью более широкого исследования DGAP в области технологий и их влияния на международные отношения, включая аспекты кибербезопасности «умных городов» и риски, связанные с технологической зависимостью.

В этом анализе будут рассмотрены предполагаемые мотивы, стоящие за инициированием кибер-активностей крупными державами, последствия таких действий и стратегические ответные меры, которые могут быть сформулированы для решения этой растущей проблемы.

Основное внимание публикации уделяется анализу прошлых кибер-операций и их последствий для лучшего понимания и прогнозирования будущих кампаний, а также предложению стратегий борьбы с такими угрозами.

Цель этого анализа – предоставить ценную информацию специалистам кибербезопасности и стратегическому планированию (но не ограничиваясь ими).

## B. Критическая составляющая статьи

Как выше было отмечено, публикация является частью более широкого исследования DGAP в области технологий и их влияния на международные отношения, включая аспекты кибербезопасности «умных городов» и риски, связанные с технологической зависимостью. Это также вписывается в контекст глобальных вызовов безопасности, таких как кибер-война и распространение оружия массового уничтожения, и необходимости стратегического реагирования на эти угрозы.

В статье даётся исчерпывающий обзор положительных и отрицательных аспектов кибербезопасности. В качестве положительных аспектов выделяются достижения в области технологий безопасности, такие как передовые методы шифрования, биометрическая аутентификация и обнаружение угроз на базе искусственного интеллекта. Повышение осведомлённости общественности о проблемах кибербезопасности также рассматривается как позитивное событие. В качестве отрицательных аспектов отмечается сохранение угроз, недостаточная

осведомлённость о киберпространстве и причастность преступных организаций.

Из недостатков статьи стоит отметить недостаточную глубину обсуждения негативных аспектов кибербезопасности. Хотя упоминается о сохраняющихся угрозах и причастности преступных организаций, коллективный автор не вникает в специфику этих вопросов и не приводит конкретных примеров и особенно нет глубокой проработки потенциальных решений этих проблем.

Говоря про опыт при подготовке материала, который, как правило, имеет решающее значение, подразумевается, что опыт работы в области кибербезопасности позволяет обладать глубоким пониманием сложностей данной области, что позволит ему провести глубокий анализ и высказать обоснованные мнения. Недостаток этого опыта, очевидно, наблюдается и наличие опыта придало бы статье достоверности, сделав её надёжным источником информации для читателей.

В целом, что касается положительных и отрицательных сторон статьи, то она даёт некий сбалансированный взгляд на кибербезопасность, подчёркивая как её достижения, так и текущие проблемы. Этот взгляд полезен для читателей, стремящихся понять текущее состояние кибербезопасности. Тем не менее отмеченные недостатки определённо снижают качество статьи.

## C. Ключевые моменты

Основными мотивами для начала деструктивных кибер-операций являются территориальные завоевания, предотвращение угроз и ответные действия.

Первой известной кибер-операцией, уничтожившей физические объекты, была Stuxnet, американо-израильская операция в 2010 году, в ходе которой был осуществлён саботаж иранских центрифуг по обогащению урана.

Размер выборки деструктивных кибер-операций, нацеленных на государства за пределами крупного конфликта, довольно ограничен. Исторически было выбрано пять операций.

Все рассмотренные кибератаки проводились с учётом фактора, что атакующие страны, США и другие чувствовали себя в безопасности и не боялись какой-либо серьёзной реакции на совершаемые действия.

Иран, Северная Корея, Южная Корея, и Тайвань были основными целями деструктивных кибер-операций.

Для США будущие цели, вероятно, будут ограничены странами, которые стремятся приобрести ядерное оружие, такими как Иран и Северная Корея, а также расширения своего экономического влияния в Южно-Азиатском регионе.

Учитывая продолжающиеся пограничные споры, развязанные США рядом стран, в частности, Китай вероятно, будут нацелены на соседние страны с помощью деструктивных кибератак.

В публикации подчёркивается необходимость сравнительного анализа того, почему некоторые страны проводят деструктивные кибер-атаки, и даются рекомендации относительно того, что Германия и другие государства-члены ЕС могут сделать для их смягчения.

Публикация определяет деструктивные кибер-операции как те, которые приводят к значительному физическому ущербу или значительным экономическим потерям.

В публикации также отмечается, что некоторые операции были исключены из анализа из-за неопределённых утверждений и фактов.

#### D. Краткая история деструктивных кибератак

В разделе представлен обзор значительных кибератак, имевших место в прошлом, с акцентом на их мотивации, воздействии и общих чертах.

Первой обсуждаемой крупной кибератакой является американо-иранский конфликт 2010–2019 годов. Ярким примером является операция Stuxnet в 2010 году, целью которой вероятно были объекты по обогащению урана в Иране. В 2019 году США отключили иранские базы данных, использовавшиеся для атак на нефтяные танкеры в Персидском заливе.

Американо-северокорейский конфликт 2014–2017 годов – ещё одна важная кампания. Однако анализ исключает некоторые операции из-за неопределённых утверждений о причастности, таких как Китай, вызвавший перебои в подаче электроэнергии в Индии в 2021 году и закрытие порта в Японии в 2023 году, и США, вызвавшие взрывы газопровода.

Общим для этих кампаний является стремление снизить атакующие возможности противника. Например, США развернули разрушительные кампании против Северной Кореи и Ирана, чтобы задержать их приобретение и развертывание наступательных вооружений.

#### E. Общие черты прошлых и будущих кибератак

Деструктивные кибератаки часто преследуют общие цели, такие как снижение возможностей противника, нанесение значительного физического ущерба и даже травматизм человека.

Изоцрённость и опыт злоумышленников, неизбирательный размах атак и целенаправленное враждебное намерение максимизировать ущерб являются общими характеристиками этих кампаний.

Использование искусственного интеллекта и расширенной системы анализа угроз улучшило обнаружение этих атак.

Растущая кибер-угроза может в итоге заставить пересмотреть значение оружия массового уничтожения.

Глобальные пути распространения интернета означают, что кибер-активность стирает большую часть давней

Следующая крупная деструктивная кибератака может быть вызвана различными мотивами, включая geopolитическую напряжённость, финансовую выгоду или желание нанести значительный физический ущерб или травмы людям.

Идентификация кибератак может быть сложной из-за способности участников скрывать свою личность, выдавать себя за другие компьютеры, использовать виртуальные

частные сети для усложнения наблюдения или захватывать другие устройства для проведения операций.

Кибератаки затронули 120 стран, чему способствовал шпионаж, спонсируемый правительством.

Международное сообщество ещё официально не разработало конвенцию, классифицирующую кибервойны, но оно предприняло шаги для определения этого.

#### F. Что делать

В разделе "Что делать" обсуждаются стратегии и рекомендации по смягчению последствий деструктивных кибер-операций.

В публикации предлагается, чтобы страны сосредоточились на наращивании своего потенциала в области кибербезопасности и сборе разведанных, особенно в отношении угроз финансовой системе.

В нем также подчёркивается важность международного сотрудничества в борьбе с кибер-угрозами, учитывая глобальный взаимозависимый характер системы.

В документе подчёркивается необходимость уменьшения фрагментации среди заинтересованных сторон и инициатив, которая в настоящее время препятствует международному сотрудничеству и ослабляет возможности восстановления системы и реагирования.

В публикации упоминается, что странам необходимо разработать более эффективные пути и средства противодействия информационным операциям с использованием киберпространства.

В нем также обсуждается идея создания новых инструментов для достижения целей, которые ставят перед собой разные страны в отношении того, как они действуют в киберпространстве.

В документе предлагается, чтобы крупные державы рассмотрели вопрос о том, как использовать кибер-операции для усиления сдерживания вооружённого нападения.

##### 1) Основные рекомендации:

Международное сотрудничество имеет решающее значение в борьбе с кибер-угрозами, учитывая глобально взаимозависимый характер системы.

Необходимо уменьшить фрагментацию среди заинтересованных сторон и инициатив, которая в настоящее время препятствует международному сотрудничеству и ослабляет возможности восстановления системы и реагирования.

Существует необходимость в создании новых инструментов для достижения целей, которые различные страны ставят перед собой в отношении того, как они действуют в киберпространстве.

<sup>х.</sup> **Россия стремится  
построить  
полностью  
контролируемую  
государством ИТ-  
экосистему  
(по версии DGAP)**



#### A. Введение

В статье с кликбейтным названием "Россия стремится создать полностью контролируемую государством ИТ-экосистему" обсуждается стратегия России по созданию цифровой независимой платформы.

В этом анализе мы рассмотрим усилия России по созданию мощной экосистемы, уделяя особое внимание различным аспектам и предоставив всесторонний обзор. Этот анализ будет особенно полезен специалистам в области кибербезопасности, включая технических и стратегических экспертов, поскольку он проливает свет на цифровые стратегии страны и их потенциальные последствия.

Российское государство развивает цифровую экосистему, которая включает в себя множество услуг, потенциально используемых каждым гражданином. Эта экосистема призвана упростить информационное управление и повысить качество жизни страны. Центральным игроком является компания VK, конгломерат цифровых сервисов, который начался с сервиса электронной почты, Mail.ru. Стратегия российского государства заключается в повышении удобства предоставления услуг, тем самым побуждая людей ими активнее пользоваться.

Компания "ВКонтакте", конгломерат цифровых сервисов, разрабатывает супер-приложение, аналогичное китайскому WeChat. Это приложение, наряду с другими цифровыми сервисами, предназначено для широкого использования с возможностью получения доступа к сервисам из любой точки мира с помощью мобильного устройства. Важно помнить, что цифровой ландшафт — это это также инновации, экономический рост и предоставление услуг, которые люди находят полезными. Стратегическая цель VK — создавать сервисы, которые делают жизнь людей более комфортной и безопасной, а также помогать обществу, бизнесу и государству в цифровой трансформации.

С другой стороны, также важно учитывать глобальный контекст конфиденциальности в Интернете. Громкие судебные процессы против гигантов Кремниевой долины, растущая озабоченность общественности по поводу конфиденциальности данных и знаковые законодательные действия во всем мире подчеркнули критический и неотложный характер этой проблемы. Появляются инновационные подходы, такие как дифференцированная конфиденциальность и федеративное обучение, которые предлагают новые способы обучения на основе данных без ущерба для конфиденциальности.

И хотя важно осознавать потенциальные риски и вызовы, связанные с развитием цифровых технологий в разных странах, не менее важно не упускать из виду положительные аспекты и потенциальные выгоды. Это сложный ландшафт, который требует сбалансированной и детализированной перспективы.

Преимущества российской ИТ-экосистемы для правительства и положительные аспекты для экономики можно резюмировать следующим образом:

#### B. Возможности для российского правительства:

- **Цифровой суверенитет:** Стремление России к цифровому суверенитету направлено на достижение технологической независимости и информационного контроля. Это согласуется со стремлением правительства к большей независимости от западных технологий и услуг.
- **Наблюдение и контроль:** ИТ-экосистема, контролируемая государством, обеспечивает расширенные возможности наблюдения, которые могут использоваться для мониторинга внешних информационных угроз и оказания помощи населению.
- **Управление информацией:** Правительство может использовать ИТ-экосистему для распространения критически важной информации в считанные секунды.
- **Устойчивость к экономическим санкциям:** Укрепляя внутреннюю ИТ-экосистему, Россия может смягчить воздействие международных санкций, особенно тех, которые направлены на экспорт технологий.

#### C. Положительные аспекты для российской экономики:

- **Инновации и рост:** Развитие цифровой экосистемы может стимулировать инновации и экономический рост, о чем свидетельствует расширение компании "ВК" и рост её выручки на 19% в 2022 году.
- **Глобальная конкурентоспособность:** Повышение международной конкурентоспособности российского ИТ-сектора может открыть новые рынки и предложить лидерство в качестве альтернативной технологической мощи.
- **Цифровая трансформация:** Такие инициативы, как Национальная программа цифровой экономики и Национальная стратегия развития искусственного интеллекта, направлены на преобразование общества, правительства и частного бизнеса, что потенциально ведёт к более развитой цифровой экономике.

- **Электронное правительство и платёжные системы:** Россия, опережая некоторые западные страны, добилась успехов в области электронного правительства и платёжных систем, что уже привело к повышению эффективности государственных услуг и финансовых транзакций.
- **Использование ресурсов:** ИТ-экосистема может использовать богатые природные ресурсы России и квалифицированную ИТ-рабочую силу для создания более диверсифицированной и устойчивой экономики.

#### D. Отраслевая польза

ИТ-экосистема России оказала значительное влияние на различные отрасли промышленности внутри страны. Вот несколько ключевых отраслей, которые выиграли:

- **Электронная коммерция:** Рост ИТ-экосистемы привёл к буму электронной коммерции за счет того, что такие компании, как VK Company, предлагают интегрированные возможности онлайн-покупок. Это позволило предприятиям охватить более широкую клиентскую базу и способствовало росту онлайн-торговли.
- **Финансовые услуги:** Цифровая трансформация оказала значительное влияние на финансовый сектор. Развитие цифровых платёжных систем и финтех-решений сделало финансовые транзакции более эффективными и доступными для общественности.
- **Телекоммуникации:** ИТ-экосистема способствовала развитию телекоммуникационной отрасли, повысив спрос на интернет и услуги мобильной связи. Компании этого сектора извлекли выгоду из роста цифровых сервисов и платформ.
- **Средства массовой информации и развлечения:** Рост цифровых платформ преобразил индустрию средств массовой информации и развлечений. Онлайн-сервисы потокового вещания, цифровые новостные платформы и социальные сети становятся все более популярными, предоставляя новые возможности для создания и распространения контента.
- **Образование:** ИТ-экосистема также оказала влияние на сектор образования. Появление платформ онлайн-обучения и цифровых образовательных ресурсов изменило способ предоставления образования, сделав его более доступным и гибким.
- **Здравоохранение:** Цифровые решения в области здравоохранения, такие как телемедицина и электронные медицинские карты, улучшили качество сервиса, повысили эффективность и клиентаориентированность при предоставлении медицинских услуг.

#### E. Вклад в экономику

ИТ-экосистема в России способствовала росту российской экономики несколькими способами:

- **Инновации и технологическое развитие:** Сосредоточение внимания на создании надёжной ИТ-экосистемы стимулировало инновации и

технологический прогресс внутри страны. Это привело к разработке новых продуктов и услуг, способствующих экономическому росту.

- **Создание рабочих мест:** Расширение ИТ-сектора создало множество рабочих мест, как непосредственно в отрасли, так и косвенно в смежных секторах. Это помогло снизить безработицу и увеличить доходы домохозяйств.
- **Повышение производительности:** Внедрение ИТ-решений в различных отраслях привело к повышению производительности. Автоматизация и цифровые инструменты упростили процессы, снизили затраты и повысили эффективность.
- **Расширение электронной коммерции:** ИТ-экосистема способствовала росту электронной коммерции, позволяя предприятиям выходить на более широкий рынок и предоставляя потребителям доступ к более широкому спектру продуктов и услуг онлайн.
- **Привлечение инвестиций:** Развитие мощной ИТ-инфраструктуры может привлечь в страну как внутренние, так и иностранные инвестиции, поскольку инвесторы стремятся извлечь выгоду из растущего цифрового рынка.
- **Диверсификация экономики:** Развивая ИТ-сектор, Россия диверсифицирует свою экономику, выходя за рамки традиционной зависимости от природных ресурсов, таких как нефть и газ, что делает экономику более устойчивой к внешним потрясениям.
- **Повышение глобальной конкурентоспособности:** Развитая ИТ-экосистема может позволить российским компаниям более эффективно конкурировать на международном рынке.
- **Цифровая трансформация:** ИТ-экосистема поддерживает цифровую трансформацию традиционных отраслей промышленности, помогая им модернизироваться и конкурировать во все более цифровом мире.

#### F. Сравнение экосистем

ИТ-экосистема России предлагает правительству страны уникальный набор преимуществ, которые можно сравнить с ИТ-экосистемами других стран в нескольких ключевых аспектах:

- 1) **Государственный надзор и контроль**
  - **Россия:** Российское правительство извлекает выгоду из своей ИТ-экосистемы за счёт расширения возможностей наблюдения и контроля над цифровым пространством. Это включает в себя мониторинг злонамеренных действий и блокировку опасной и заведомо ложной информации, распространяемой другими странами.
  - **Китай:** По сравнению с Россией ИТ-экосистема Китая технически предлагает уникальные функции, расширяющие наблюдение и цензуру с помощью таких платформ, как WeChat и Great Firewall, с целью заглушить «демократическую» пропаганду западных стран.

- **Западные демократии (например, Соединённые Штаты и Европейский союз):** хотя в этих странах существуют нормативные рамки для защиты конфиденциальности цифровых данных (например, GDPR в ЕС), правительственные учреждения активно используют технологии в целях национальной безопасности. Однако здесь больше внимания уделяется правам на неприкосновенность частной жизни в отношении денег, а уровень государственного контроля и слежки значительно выше по сравнению с Россией и Китаем для обычных граждан.
- 2) *Цифровой Суверенитет и независимость*
  - **Россия:** Ключевым преимуществом для российского правительства является стремление к цифровому суверенитету, направленное на снижение зависимости от иностранных технологий и смягчение последствий международных санкций.
  - **Китай:** Китай также уделяет приоритетное внимание цифровому суверенитету, реализуя такие инициативы, как план "Сделано в Китае к 2025 году", призванный стать самостоятельным в области технологий. Китайское правительство вкладывает значительные средства в отечественные технологические компании, чтобы конкурировать на мировом рынке.
  - **Западные демократии:** Хотя цифровой суверенитет вызывает озабоченность, особенно с точки зрения защиты данных и отказа от зависимости от нескольких технологических гигантов, эти страны, как правило, выигрывают от более открытой и конкурентоспособной ИТ-экосистемы за счёт шпионажа с помощью этих же открытых технологических решений при распространении их по всему миру. Этот подход реализуется как якобы обеспечивающий безопасность и конфиденциальность при одновременном стимулировании слежки.
- 3) *Экономический рост и инновации*
  - **Россия:** Российская ИТ-экосистема призвана стимулировать экономический рост и диверсификацию, в частности, снизить зависимость от нефти и газа. Правительство поддерживает развитие отечественных ИТ-компаний и сервисов.
  - **Китай:** ИТ-экосистема Китая стала важной движущей силой его экономического роста, а технологические гиганты, такие как Alibaba и Tencent, трансформировали различные секторы. Государственная поддержка этих компаний сделала Китай мировым лидером в области электронной коммерции и мобильных платежей.
  - **Западные демократии:** ИТ-экосистемы в этих странах вносят значительный вклад в экономический рост и инновации, при этом особое внимание уделяется развитию стартапов и технологических инноваций. Правительство извлекает выгоду из развивающегося технологического сектора, который лидирует в таких областях, как разработка программного обеспечения, биотехнологии и чистая энергетика.

#### 4) Управление информацией

- **Россия:** информационный ландшафт очень разнообразен, и существуют правовые и общественные механизмы противодействия ложной информации. Способность правительства контролировать информацию ограничена законами, защищающими свободу слова и прессы и защищающими граждан от фейков.
- **Китай:** Китай использует свою ИТ-экосистему для управления информацией и распространения сообщений, проверенных фактами, и поддержания имиджа партии в т.ч. от различных посягательств на неё.
- **Западные демократии:** Западная экосистема используется как инструмент распространения государственной пропаганды и управления общественным восприятием как внутри страны, так и на международном уровне. Существует много дезинформации и пропаганды, а медиаландшафт более разнообразен, чтобы продавать её любым категориям граждан, без действительно правовых и общественных механизмов противодействия ложной информации.

Все экосистемы обладают своими уникальными сильными сторонами и служат различным национальным интересам и стратегиям:

В случае России механизмы экосистемы предлагают широкие возможности управленческого контроля и наблюдения, которые могут быть полезны для национальной безопасности и контроля за информацией, уравновешивая потребности в наблюдении с индивидуальными свободами; при этом подобного не наблюдаются в демократических странах

Россия активно стремится к цифровому суверенитету, уменьшая зависимость от иностранных технологий, что имеет стратегическое значение для национальной безопасности и экономической независимости, в то время как другие угрожают глобальному ИТ-ландшафту, получая экономическую выгоду от проблем, связанных с конфиденциальностью данных и международными отношениями.

Россия, обладает высокоразвитой индустрией кибербезопасности и совместными усилиями правительства и частного сектора обеспечивается сложный, но эффективный контроль требуемого уровня безопасности в различных секторах и социальных сетях.

Россия фокусируется на развитии своего ИТ-сектора для стимулирования инноваций и снижения экономической зависимости от природных ресурсов, в то время как другие страны пытаются заменить подобные независимые решения своими открытыми с целью поддержания своего доминирования.

Россия использует свою ИТ-экосистему для демонстрации мягкой силы и предоставления незападных технологических решений, привлекательных для определённых стран, в то время как другие получают огромное глобальное влияние через свои технологические компании, формируя глобальные технологические тенденции и стандарты.

**xl. CYBER DEFENSE  
DOCTRINE THAT  
MANAGES RISKS: A  
COMPLETE APPLIED  
GUIDE TO  
ORGANIZATIONAL  
CYBER DEFENSE**

CYBER DEFENSE DOCTRINE  
MANAGING THE RISK FULL  
APPLIED GUIDE TO ORGANIZATIONAL CYBER DEFENSE



**Аннотация – Анализ «Cyber Defense Doctrine Managing the Risk: Full Applied Guide to Organizational Cyber Defense» посвящён различным аспектам организационной киберзащиты, включая системы управления рисками, элементы кибербезопасности в военных операциях, планирование реагирования на инциденты и применение инструментов и методов киберзащиты. Подчёркивая полезность для специалистов кибербезопасности и специалистов в различных отраслях, изложенный материал можно рассматривать в качестве руководства, которое даёт представление о реализации стратегий киберзащиты, повышении уровня безопасности организации и развитии кибер-культуры.**

**Он также служит полезным ресурсом для специалистов в области информационных технологий, криминалистики, правоохранительных органов и других секторов, которым требуется глубокое понимание принципов и практик киберзащиты и необходимость непрерывного обучения и адаптации с учётом постоянно развивающихся кибер-угроз.**

#### A. Введение

Ключевые моменты дающие представление о доктрине представлены следующим списком:

- **Цель (основная):** продвижение киберзащиты в израильской экономике как часть национальных усилий (Израиля) по защите гражданского киберпространства
- **Цель (вторичная):** предоставление системного профессионального метода управления кибер-リスクами в организациях, распознавания соответствующих рисков, формулирования защитных мер и реализации плана снижения рисков.
- **Категории организаций:** различие двух типов организаций в зависимости от размера потенциального ущерба от кибер-инцидента.

- **Процесс оценки и управления рисками:** различные методы оценки и управления рисками, в зависимости от размера организации, соответствия законодательным и нормативным требованиям и других параметров (например, с небольшим потенциалом ущерба до 1,5 млн долларов и более).
- **Результат:** понимание карты организационных рисков и то, какие меры контроля необходимы для снижения этих рисков; которые (меры) станут основой для построения плана работы, распределения ресурсов и подготовки организации.
- **Принципы доктрины:** ответственность управления, защита с точки зрения противника, защита, основанная на израильских знаниях и опыте, защита в соответствии с потенциалом ущерба.

#### B. Принципы доктрины

Целью является формирование принципов, которых организациям следует придерживаться, чтобы эффективно управлять кибер-рискаами и повышать свою киберустойчивость.

**Целевая аудитория** включает руководителей организаций, специалистов по информационной безопасности и экспертов по киберзащите, которые отвечают за управление кибер-рискаами и реализацию стратегий защиты в своих организациях.

##### 1) Процесс автоматизации и интеграции

Подчёркивается важность процессов автоматизации и интеграции:

- Процессы автоматизации снижают необходимость участия человека в защитных и операционных процессах, тем самым сводя к минимуму вероятность человеческой ошибки.
- Внедрение MITRE ATT&CK с целью использования передовых автоматизированных решений для непрерывного контроля и реализации процессов реагирования минимизирует объём ручного участия человека.
- Применение превентивных мер сохранения информации, включая поддержание эффективных возможностей реагирования на случаи утечки информации, например получение возможности удалять информацию, которая попала в Интернет и даркнет.
- Директор по информационной безопасности (CISO) играет важную роль в защите информации и конфиденциальности и должен использовать различные инструменты для максимизации уровня защиты.
- Средства контроля доктрины включены в систему, включающую аспекты идентификации, защиты, обнаружения, реагирования и восстановления.

- Концепция защиты, необходимая для борьбы с современными угрозами поможет организации достичь новых возможностей с целью выиграть время, измотать злоумышленника и даже создать факторы сдерживания против злоумышленников.

## 2) Роль директора по информационной безопасности

Директор по информационной безопасности играет решающую роль в защите информации и конфиденциальности внутри организации. Это включает в себя понимание и соблюдение мер конфиденциальности, баланса различных интересов, управление рисками, разработку стратегий защиты и эффективное внедрение средств контроля:

- **Закон о защите конфиденциальности:** любое посягательство на неприкосновенность частной жизни должно осуществляться в соответствии с законом и общими принципами разумности и добросовестности
- **Баланс интересов:** Директор по информационной безопасности должен найти правильный баланс между различными интересами, чтобы обеспечить обоснованные решения внутри организации. Это включает в себя рассмотрение аспектов конфиденциальности и соблюдение таких принципов, как «Security by Design», «Privacy by Design» и защита с учётом угроз.
- **Оценка и управление рисками:** процесс оценки и управления рисками включает определение основных целей защиты, выявление пробелов в защите и построение плана работы по минимизации этих пробелов.
- **Ответственность руководства:** Ответственность за защиту информации в первую очередь лежит на руководстве организации и директор по ИБ является ключевой фигурой в обеспечении выполнения этой обязанности.
- **Защита с точки зрения противника:** Директор по информационной безопасности должен понимать распространённые сценарии атак и эффективность рекомендаций по защите от них. Это понимание определяет вес и приоритет рекомендаций защиты.
- **Защита, основанная на потенциальном ущербе:** инвестиции в защиту каждой цели защиты должны соответствовать уровню её критичности для функционирования организации. Директор по информационной безопасности должен управлять этими инвестициями
- **Организационная классификация:** классификации основана на потенциальном ущербе от кибер-инцидента. Директор по информационной безопасности должен понимать место организации для формирования стратегий защиты.

## C. Процесс планирования с точки зрения организации

Процесс планирования с точки зрения организации — это метод управления рисками внутри организации. Цель этого процесса — помочь организациям выявить соответствующие риски, сформулировать защитные меры и соответствующим образом реализовать план снижения рисков.

**Целевая аудитория** включает менеджеров и экспертов в области информационной безопасности и киберзащиты.

Применяются различные методы оценки и управления рисками, в зависимости от размера организации, соответствия законодательным и нормативным требованиям и другими параметрами. Например, к организациям категории А относятся организации, у которых объем ущерба, причинённого кибер-инцидентом, не превышает 1,5 млн долларов США, а к организациям категории Б — организации, у которых размер ущерба, причинённого кибер-инцидентом, может стоить более 1,5 млн долларов США.

Для организаций категории А применяется простой и быстрый процесс определения целей защиты, специально предназначенных для организаций этой категории.

Для организаций категории В применяется не только процесс оценки рисков, но понимание необходимых мер защиты по матрице рисков и склонности к риску, изучение текущей ситуации с точки зрения принятых в отрасли рекомендаций по защите и формулирование плана работы для снижения рисков.

Конечный результат работы заключается в том, что организация определяет карту организационных рисков и то, какие средства контроля необходимы для снижения этих рисков, включая правильные приоритеты для реализации плана работы. Эти средства контроля станут основой для построения плана работы, распределения ресурсов и соответствующей подготовки организации.

### 1) Ключевые компоненты процесса планирования

Ключевые компоненты процесса планирования в организации включают:

- **Разграничение деятельности:** понимание цифровых активов организации и места их хранения для определения подлежащего защите набора объектов.
- **Оценка рисков:** выявление соответствующих рисков для организации, анализ этих рисков и их оценка для понимания их потенциального воздействия и вероятности.
- **Управление риском:** принятие решения о стратегии борьбы с выявленными рисками
- **Построение плана работы:** после того как риски идентифицированы и определена стратегия борьбы с ними, организация должна разработать план работы по устранению рисков. Этот план может включать внедрение процессов, приобретение решений и обучение сотрудников.

- **Непрерывный аудит и контроль:** реализация плана работы должна регулярно пересматриваться, чтобы гарантировать его эффективность и актуальность. Это включает в себя проверку новых информационных активов, реализованных средств контроля и необходимых управленических данных.
- **Привлечение юрисконсульта:** юрисконсульт организации должен быть привлечён на ранних стадиях процесса планирования, чтобы обеспечить соблюдение законодательных и нормативных требований и быть интегрированным в ключевые процессы принятия решений.
- **Принятие решений, подкреплённое доказательствами:** организация должна использовать независимых аудиторов и экспертов, чтобы справиться с различными угрозами и гарантировать, что принятие решений подкреплено доказательствами, которые обеспечивают реалистичную картину ситуации с безопасностью.
- **Минимизация вторжения в частную жизнь:** Структура управления предлагает директору по ИБ широкую свободу действий для снижения уровня риска до приемлемого значения, одновременно сводя к минимуму вторжение в частную жизнь.

#### D. Реализация Доктрины

##### 1) Основные моменты:

- Подчёркивается важность процессов автоматизации и координации для уменьшения человеческих ошибок и воздействия личной информации.
- Поощряется использование передовых автоматизированных решений для непрерывного контроля и выполнения процессов реагирования, при этом участие человека требуется лишь в исключительных случаях.
- Необходимость применения превентивных мер защиты для сохранения информации, а также для поддержания эффективных возможностей реагирования на случай утечки информации.
- Средства контроля доктрины включены в структуру, включающую аспекты идентификации, защиты, обнаружения, реагирования и восстановления.
- Необходимость внедрения средств контроля на разных уровнях зрелости по таким вопросам, как SOC, DLP или исследования рисков.
- Сосредоточение внимание на рисках, актуальных для каждой организации, при этом периодические проверки и разведывательные оценки проводятся по всей израильской экономике.
- Инвестиции в защиту каждого объекта защиты в организации будут соответствовать уровню его критичности для функционирования организации.

##### 2) Разница контроля уровня

Контроль базового уровня обычно указывает на процесс, который существует, но не управляемся и выполняется вручную. Это отправная точка для организаций, позволяющая им внедрить базовые элементы управления, прежде чем переходить к более продвинутым и сложным элементам управления.

С другой стороны, контроль инновационного уровня означает реализацию контроля управляемым, документированным, автоматическим, эффективным и действенным образом. Этот уровень контроля является более комплексным и учитывает ограничения организации, классификацию информации и адаптацию к бизнес-процессам.

##### 3) Реализация Доктрины для организаций категории А

В случае организаций категории А рассматривается пятиэтапный процесс реализации доктрины.

- **Этап 1: Разграничение деятельности.** этап включает определение объёма деятельности организации, которую необходимо защитить.
- **Этапы 2 и 3: Оценка рисков и определение стратегии борьбы с ними.** этапы включают выявление потенциальных рисков для организации и разработку стратегии управления этими рисками.
- **Этап 4: Составление плана работы.** этап включает в себя создание подробного плана реализации стратегии защиты.
- **Этап 5: Непрерывный аудит и контроль.** этап включает постоянный мониторинг и контроль для обеспечения эффективности стратегии защиты и внесения необходимых корректировок.

##### 4) Реализация Доктрины для организаций категории Б

В случае организаций категории Б рассматривается пятиэтапный процесс реализации доктрины.

- **Этап 0 – Корпоративное управление и стратегия управления корпоративными рисками.** этап включает в себя создание структуры управления и стратегии управления корпоративными рисками. Он закладывает основу подхода организации к киберзащите.
- **Этап 1 – Разграничение деятельности и обследование по оценке рисков.** этап включает в себя определение сферы деятельности организации и проведение обследования по оценке рисков. Это помогает организации понять свои потенциальные уязвимости и риски, связанные с её деятельностью.
- **Этап 2 – Оценка рисков.** этап включает детальную оценку рисков, выявленных на предыдущем этапе. Организация оценивает потенциальное воздействие и вероятность каждого риска, что помогает расставить приоритеты для их смягчения.
- **Этап 3 – Управление риском.** этап включает разработку стратегий по управлению ими: снижение риска, принятие или предотвращение, в

зависимости от характера риска и толерантности к риску организации.

- **Этап 4 – Построение плана работы:** на основе стратегий управления рисками, разработанных на предыдущем этапе, этот этап включает в себя создание подробного плана работы, где описываются шаги, которые организация предпримет для реализации своих стратегий управления рисками.
- **Этап 5 – Непрерывный аудит и мониторинг.** этап включает постоянный аудит и мониторинг, чтобы гарантировать эффективную реализацию стратегий управления рисками и выявлять любые новые или изменяющиеся риски.

#### E. Структура защиты

Структура представлена следующим образом:

- **Идентификация:** функция включает в себя развитие организационного понимания управления рисками кибербезопасности для систем, активов, данных и возможностей.
- **Защита:** функция определяет соответствующие меры безопасности для обеспечения предоставления критически важных инфраструктурных услуг.
- **Обнаружение:** функция определяет соответствующие действия для выявления возникновения события кибербезопасности.
- **Ответ:** функция включает в себя соответствующие действия для принятия мер в отношении обнаруженного инцидента кибербезопасности.
- **Восстановление:** функция определяет соответствующие действия для поддержания планов устойчивости и восстановления любых возможностей или услуг, которые были нарушены из-за инцидента кибербезопасности.

Эти функции построены в соответствии со структурой кибербезопасности NIST (CSF), которая обеспечивает высокоуровневую классификацию результатов кибербезопасности и методологию оценки этих результатов и управления ими.

#### F. Прочее

Ключевые принципы включают принцип согласия, который даёт клиентам контроль над их личной информацией, и принцип близости цели, который предусматривает, что информация может использоваться

только для той цели, для которой она была первоначально собрана. В нем также изложены обязательства относительно регистрации баз данных и их безопасности, включая необходимость периодической проверки необходимости сохранения информации исходя из её первоначальной цели сбора.

##### 1) Средства защиты организации

Ключевые аспекты в контексте мер по контролю за защитой организации категории А:

**Требование к доказательствам:** подчёркивается необходимость надлежащей документации для обеспечения правильной интеграции средств контроля в организацию. Эти данные также могут служить основой для регулирования и/или аккредитации/сертификации.

**Ранжирование и установление приоритетов:** элементы управления классифицированы по шкале от 1 до 4. Средства управления уровня 1 являются самыми базовыми и необходимы для любой организации для каждого актива, тогда как элементы управления уровня 4 необходимы только для объекта защиты, потенциальный ущерб которого 4

**Непрерывный контроль.** Непрерывный контроль позволяет понять, каковы пробелы в защите и какие шаги необходимы для улучшения ситуации. Непрерывный контроль может осуществляться на уровне соответствия, решая определённые проблемы и средства контроля, или путём измерения рисков, угроз, готовности к сценариям атак и т. д.

**Ключевые показатели эффективности (KPI):** KPI позволяют организации измерять и количественно определять уровень защиты в определённый момент времени, сравнивая его с историей измерений, таким образом исследуя тенденцию.

**Процесс оценки и управления рисками.** Деятельность по киберзащите осуществляется в связи с желанием организации управлять кибер-рискаами, которым она подвергается. Сначала определяются основные цели защиты, требуемый уровень защиты и пробелы в защите по сравнению с желаемой ситуацией, а затем формируется план работы по минимизации пробелов.

- **Конечный продукт:** карта организационных рисков и то, какие средства контроля необходимы для снижения этих рисков в качестве средств контроля являются основой для построения плана работы, распределения ресурсов и соответствующей подготовки организации

xii. **CONTINUOUS THREAT  
EXPOSURE  
MANAGEMENT (CTEM)**



**Аннотация – В этом документе представлен анализ Continuous Threat Exposure Management (СTEM) – стратегического подхода к кибербезопасности, в котором особое внимание уделяется непрерывному мониторингу, выявлению, оценке киберугроз и уязвимостей и управлению ими.**

**В ходе анализа будут рассмотрены различные аспекты СTEM, включая его определение, этапы внедрения и преимущества для специалистов кибербезопасности и организаций в различных отраслях.**

**Выводы, представленные в этом анализе, представляют ценность для специалистов по безопасности в различных отраслях для совершенствования мер кибербезопасности и снижения вероятности рисков.**

#### A. Введение

Непрерывное управление выявлением угроз (СTEM) – это стратегия кибербезопасности, которая фокусируется на выявлении, оценке и снижении рисков в цифровой среде организации посредством непрерывного мониторинга и повышения уровня безопасности. СTEM – это не отдельный инструмент или технология, а набор процессов и возможностей, выраженных в программе/структуре, которая включает в себя определение сферы охвата, обнаружение, расстановку приоритетов, валидацию и практическую реализацию.

СTEM – это упреждающий и непрерывный подход, который отличается от традиционного управления уязвимостями (реактивного похода), фокусируется на широком спектре угроз, включает существующие меры безопасности и использует передовые инструменты моделирования для проверки.

#### 1) Инструменты и технологии

СTEM использует множество инструментов и технологий для поддержки своего внедрения и совершенствования. Эти инструменты помогают на этапах

обнаружения, оценки, расстановки приоритетов, валидации и практической реализации цикла управления угрозами. Ключевые инструменты и технологии включают СAASM (Cyber Asset Attack Surface Management), EASM (External Attack Surface Management), EM (Exposure Management), RSAS (Red Team Automation Systems).

Эти инструменты обеспечивают наглядное представление о сегментах сети, средствах контроля безопасности, типах угроз и тактиках / приемах и имеют решающее значение для выявления и анализа векторов атаки организации, которая включает внешнюю, внутреннюю и облачную среду

#### 2) Методология

Программа СTEM состоит из пяти этапов:

- **Определение области действия:** Определение начальной области воздействия, учёт критически важной для бизнеса активов, вместо сосредоточения на известных уязвимостях.
- **Обнаружение:** Активный поиск и идентификация потенциальных уязвимостей с использованием таких инструментов, как автоматические сканеры, ручное тестирование и тестирование на проникновение.
- **Определение приоритетов:** сосредоточение внимания на наиболее значительных угрозах, которые могут повлиять на бизнес, и соответствующее определение приоритетности усилий по устранению последствий.
- **Валидация:** Оценка эффективности операций по исправлению и обеспечение надлежащего устранения уязвимостей.
- **Практическая реализация:** введение в действие результатов СTEM и определение стандартов коммуникации и документированных рабочих процессов между командами

#### 3) «Лучшие практики»

Лучшие практики определения приоритетности угроз при внедрении СTEM включают:

- **Взаимодействие с заинтересованными сторонами:** такими как ИТ, юридические подразделения, комплаенс и бизнес-подразделения, для понимания их конкретных требований и проблем.
- **Регулярные обновления:** установка регулярного графика обновлений и исправлений для защиты сети от текущих известных угроз и превентивного устранения потенциальных угроз в будущем.
- **План реагирования на инциденты:** разработка эффективного (и регулярно обновляемого в соответствии с возникающими угрозами) плана реагирования на инциденты для оперативного реагирования на угрозы.

- **Оптимизированные процессы снижения рисков:** все существующие процессы снижения рисков должны быть оптимизированы и масштабируемые. Это поможет управлять возросшим спросом на передачу данных между системами после внедрения программы СТЕМ
- **Использование искусственного интеллекта:** использование подхода, основанного на искусственном интеллекте, для определения приоритетов угроз. Это может помочь справиться с динамичным характером угроз и обеспечить направление ресурсов туда, где они имеют наибольшее значение.
- **Непрерывное совершенствование:** СТЕМ — это непрерывный процесс, и организациям следует регулярно пересматривать и корректировать свои стратегии приоритизации угроз по мере появления новых угроз и эволюции бизнес-целей

## B. Возможности и ограничения внедрения СТЕМ

### 1) Возможности

- **Упреждающее управление рисками:** СТЕМ позволяет организациям последовательно отслеживать, оценивать и снижать риски безопасности с помощью планов стратегических улучшений
- **Определение приоритетов угроз:** СТЕМ обеспечивает системный подход для эффективной расстановки приоритетов потенциальных угроз
- **Повышенная устойчивость к киберугрозам:** СТЕМ повышает способность организации противостоять кибер-угрозам и восстанавливаться после них
- **Аналитические данные для принятия мер:** СТЕМ генерирует информацию о кибер-угрозах на основе данных
- **Соответствие бизнес-целям:** СТЕМ гарантирует, что усилия по обеспечению безопасности и планы управления рисками соответствуют целям компании
- **Адаптивность:** Гибкий и масштабируемый характер СТЕМ гарантирует, что его можно адаптировать к конкретным потребностям любой организации
- **Экономия средств:** СТЕМ может значительно снизить затраты, связанные с нарушениями безопасности, за счёт упреждающего выявления и смягчения угроз

### 2) Ограничения

Несмотря на его преимущества, существует ряд ограничений и проблем, связанных с внедрением СТЕМ:

- **Проблемы в интеграции:** СТЕМ требует комплексного подхода в рамках программы обеспечения безопасности, что означает, что она

должна быть построена с использованием комбинации существующих технических решений. При неправильном управлении это может привести к возникновению пробелов в интеграции, поскольку различные решения могут не работать слаженно вместе

- **Зависимость от несопоставимых решений:** Неспособность внедрить СТЕМ приводит зависимости от несопоставимых решений. Это может привести к неэффективности и несогласованности в управлении угрозами
- **Ограниченная поддержка в условиях ограничений реального времени:** СТЕМ работает в пределах определённого временного горизонта, следя «мандатам» по управлению, рискам и соблюдению требований, и информирует об изменениях в долгосрочных стратегиях. Это может не полностью учитывать ограничения в режиме реального времени, налагаемые действиями по обнаружению угроз и реагированию на них.
- **Ресурсоёмкость:** Реализация СТЕМ может быть ресурсоёмкой, требующей значительного времени и усилий для постоянного мониторинга и оценки состояния безопасности организации
- **Необходимость непрерывной проверки:** СТЕМ уделяет значительное внимание проверке, используя такие инструменты, как моделирование взломов и атак (BAS) и проверка средств контроля безопасности, для проверки защиты организации от имитируемых угроз. Это требует постоянных усилий и ресурсов для обеспечения эффективности внедрённых средств контроля
- **Проблемы при определении приоритетов угроз:** хотя СТЕМ стремится определять приоритеты угроз на основе их потенциального воздействия, это может быть непросто из-за динамичного характера угроз и необходимости согласовывать эти усилия с целями бизнеса

## C. Сложности внедрения СТЕМ

Согласование действий специалистов, не связанных с безопасностью: ИТ-инфраструктура, DevOps и службы безопасности часто имеют пробелы в коммуникации, что может представлять проблему при внедрении СТЕМ

- **Взгляд на картину в целом (преодоление диагностической перегрузки):** Комплексная программа СТЕМ охватывает множество областей, каждая из которых имеет свой набор инструментов; при этом следует иметь в виду, что объединение всей информации для понимания приоритетов и обязанностей может быть сложной задачей
- **Принятие подхода, ориентированного на учёт рисков:** Традиционные меры кибербезопасности часто направлены на достижение соответствия требованиям. СТЕМ уделяет особое внимание пониманию рисков, специфичных для уникального

контекста организации, и управлению ими, что требует тонкого понимания ландшафта бизнеса

- **Интеграция инструментов и технологий непрерывного мониторинга:** поскольку организации внедряют инновации, такие как Интернет вещей (IoT) и облачные вычисления, они должны адаптировать свои платформы СТЕМ для решения уникальных задач, связанных с этими технологиями

#### D. Ключевые шаги по внедрению СТЕМ

Внедрение СТЕМ включает систематический пятиэтапный процесс, который помогает организациям активно управлять рисками кибербезопасности и снижать их. Внедрение СТЕМ — это непрерывный цикл, поскольку ландшафт угроз постоянно меняется следуя регулярно пересматривать каждый шаг, чтобы адаптироваться к новым угрозам и изменениям в цифровой среде:

- Определение области применения (Scoping)
- Обнаружение (Discovery)
- Определение приоритетов (Prioritization)
- Проверка (Validation)
- Практическая реализация (Mobilization)

##### 1) Определение области применения (Scoping)

На этом этапе группам безопасности необходимо понять, какие системы, активы и сегменты инфраструктуры имеют решающее значение для бизнеса и могут стать потенциальными целями для киберугроз и будут включены в область применения и определение заинтересованных сторон, которые будут вовлечены. Это включает в себя определение ключевых векторов атаки, на которых можно управлять уязвимостями.

Процесс определения области обеспечивает точную идентификацию критических и уязвимых систем, что делает его основополагающим шагом в разработке мер безопасности. Этап определения объёма работ составляет основу программы СТЕМ и имеет важное значение для её общего успеха, поскольку он устанавливает рамки для последующих этапов. Важно включить все соответствующие области в сферу действия СТЕМ, такие как внешние атаки и облачные среды, чтобы не оставлять незащищёнными любые потенциальные точки взлома.

##### 2) Обнаружение (Discovery)

Организация активно ищет и выявляет уязвимости и слабые места в оцениваемых активах с применением инструментов и технологий для поиска и анализа потенциальных проблем безопасности на внешнем контуре атак, которая охватывает внешнюю, внутреннюю и облачную среды. Этот этап включает в себя идентификацию и каталогизацию всех уязвимых ресурсов организации, таких как оборудование, программное обеспечение, базы данных и сетевая инфраструктура. На этапе обнаружения предприятия используют широкий спектр инструментов и методов обнаружения ИТ для

аудита всех своих ИТ-ресурсов. Часто это включает проведение оценок уязвимостей, тестирования на проникновение и других аудитов безопасности. Цель состоит в активном поиске и выявлении потенциальных уязвимостей в системах и активах организации.

На этапе обнаружения важно привлечь разнообразную команду экспертов, включая ИТ-персонал, сотрудников службы безопасности и других сотрудников, которые могут иметь уникальный взгляд на потенциальные уязвимости. Это гарантирует выявление и оценку всех потенциальных угроз. Этап обнаружения служит связующим звеном между этапами определения объёма и определения приоритетов в процессе СТЕМ. После этапа анализа, на котором определяются ключевые вектора атаки и заинтересованные стороны, этап обнаружения фокусируется на детальной идентификации всех активов и уязвимостей.

##### 3) Определение приоритетов (Prioritization)

Этот этап имеет решающее значение, поскольку помогает организациям определить, каким ценным активам необходимо уделить приоритетное внимание на основе их потенциального воздействия на бизнес, так как не все можно защитить сразу.

На этапе определения приоритетов организации оценивают уровень риска. Это включает в себя компенсирующие средства контроля безопасности и потенциальные уязвимости, выявленные на этапе обнаружения, исходя из того, насколько вероятно, что они будут использованы.

Основная цель расстановки приоритетов — составить список задач для эффективного снижения рисков. Это позволяет организациям оптимально распределять свои ресурсы, обеспечивая эффективное использование. А также определить, какие активы являются наиболее важными и нуждаются в наивысшем уровне защиты.

Текущий этап — это непрерывный процесс, который включает в себя постоянную переоценку, ранжирование и выбор активов, требующих немедленного внимания. Этот этап динамичен и должен адаптироваться для эффективного противодействия возникающим угрозам.

##### 4) Проверка (Validation)

Этот этап обеспечивает точную оценку уязвимости организации к угрозам и эффективности операций по исправлению. На этапе проверки организаций оценивают, как они справились бы с реальной атакой, и оценивают свою способность защититься от неё. Это включает в себя использование таких практик, как моделирование взломов и атак (BAS) и тренинги Red Team для имитации атак и проверки защиты на месте.

Этап проверки гарантирует, что планы по устранению уязвимостей и угроз, выявленных на этапе определения приоритетов, эффективны. Это может включать добавление дополнительных мер предосторожности, обновление программного обеспечения или изменение настроек безопасности.

Также важно привлечь к этапу проверки широкий круг заинтересованных сторон, включая ИТ-персонал,

сотрудников службы безопасности и другие соответствующие команды. Это гарантирует, что процесс валидации будет всеобъемлющим и что меры по исправлению будут эффективными во всей организации

#### 5) Практическая реализация (*Mobilization*)

Этот этап заключается в практической реализации результатов процесса СТЕМ и осуществлении необходимых действий для устранения выявленных рисков.

На этапе практической реализации организации приводят в действие планы по устранению уязвимостей и угроз, выявленных на этапе определения приоритетов и подтверждённых на этапе валидации. Это может включать добавление дополнительных мер предосторожности, обновление программного обеспечения или изменение параметров безопасности.

Этот этап также включает в себя обеспечение того, чтобы все команды в организации были проинформированы и согласованы с усилиями по обеспечению безопасности. Это может включать автоматизацию мер по смягчению последствий за счёт интеграции с платформами управления информацией о безопасности и событиями (SIEM) и управления безопасностью, автоматизации и реагирования (SOAR), а также установление стандартов связи и документированных межкомандных рабочих процессов.

На данном этапе становится понятно, что восстановление не может быть полностью автоматизировано и требует вмешательства человека и подчёркивается необходимость того, чтобы руководители служб безопасности мобилизовали ответные меры и устранили риски из окружающей среды.

### E. Другие аспекты реализации

#### 1) Определение приоритетов угроз

Этап определения приоритетов — это третий этап в СТЕМ. На этом этапе организации оценивают потенциальные уязвимости, выявленные на этапе обнаружения, исходя из того, насколько вероятно, что они будут использованы, и потенциального воздействия, которое это окажет на организацию. Ключевые шаги, связанные с определением приоритетов угроз:

- **Оценка критичности и вероятности:** Компании часто используют методологию оценки рисков для анализа критичности и вероятности каждой уязвимости. Это включает в себя оценку потенциального ущерба, который мог бы быть причинён в случае использования уязвимости.
- **Учёт влияния на бизнес:** программы СТЕМ помогают организациям определять приоритеты угроз на основе их потенциального воздействия на бизнес. Это включает в себя рассмотрение таких факторов, как критичность затронутой системы или данных, потенциальные финансовые последствия и потенциальный ущерб репутации.
- **Наличие компенсирующих средств контроля:** Наличие компенсирующих средств контроля,

которые являются альтернативными мерами, способными снизить риск использования уязвимости, также является фактором при определении приоритетов.

- **Толерантность к остаточному риску:** Толерантность организации к остаточному риску, который остаётся после применения всех средств контроля, является одним фактором, который может влиять на расстановку приоритетов.
- **Распределение ресурсов:** на основе расстановки приоритетов организации могут эффективно распределять ресурсы для устранения наиболее значительных рисков. Такой стратегический подход к управлению угрозами приводит к более эффективному использованию ресурсов и более быстрому реагированию на наиболее потенциально опасные угрозы

#### 2) Методы приоритизации

Распространённые методы и рекомендации по приоритизации угроз при внедрении СТЕМ включают:

- **Определение приоритетов с учётом потребностей бизнеса:** СТЕМ устанавливает приоритеты в соответствии с бизнес-целями, уделяя особое внимание наиболее критичным угрозам и уязвимостям, которые могут повлиять на наиболее ценные активы организации. Такой подход гарантирует, что ресурсы распределяются там, где они имеют наибольшее значение, согласовывая усилия организации с постоянно меняющимся ландшафтом угроз
- **Анализ воздействия:** Определение приоритетов должно включать анализ потенциального воздействия каждой угрозы. Оценивая критичность и потенциальный ущерб от каждой угрозы, организации могут эффективно распределять ресурсы для устранения наиболее значительных рисков
- **Динамическая расстановка приоритетов:** Ландшафт угроз динамичен, и новые уязвимости появляются регулярно. Следовательно, стратегии расстановки приоритетов должны быть адаптируемыми для эффективного противодействия возникающим угрозам.
- **Распределение ресурсов:** Человеческие ресурсы ограничены, и группы безопасности должны расставлять приоритеты в своих усилиях. Ключевым моментом является выделение ресурсов для устранения критичных уязвимостей, которые могут оказать существенное влияние на организацию

Чтобы обеспечить соответствие приоритизации угроз бизнес-целям, организациям следует включить стратегические бизнес-цели в свою программу СТЕМ. Такой подход позволяет организациям оценивать критичность и потенциальный ущерб от каждой угрозы,

а затем соответствующим образом распределять ресурсы, гарантируя, что меры безопасности будут сосредоточены на защите наиболее важных бизнес-активов

#### F. Эффективность СТЕМ

Для измерения эффективности программы непрерывного управления выявлением угроз (СТЕМ) организации могут использовать несколько ключевых показателей эффективности. Используя эти показатели и постоянно отслеживая их, организации могут получить представление об эффективности своей программы СТЕМ и принимать обоснованные решения по повышению своей кибербезопасности. Важно отметить, что эффективность программы СТЕМ не является статичной и должна регулярно оцениваться для адаптации к меняющемуся ландшафту угроз и потребностям бизнеса.

- **Снижение рисков:** оценка снижения рисков безопасности, отслеживая количество выявленных и устраниённых уязвимостей с течением времени. Успешная программа СТЕМ должна демонстрировать тенденцию к снижению количества и серьёзности рисков для безопасности
- **Улучшенное обнаружение угроз:** оценка эффективности возможностей обнаружения угроз, отслеживая время, необходимое для обнаружения новых уязвимостей или угроз. Более низкое среднее время обнаружения (MTTD) указывает на более эффективную программу СТЕМ
- **Время для исправления:** оценка скорости устранения выявленных угроз и уязвимостей. Успешная программа СТЕМ должна помочь сократить время между обнаружением и устранением неполадок, известное как среднее время реагирования (MTTR)
- **Эффективность контроля безопасности:** Использование таких инструментов, как проверка контроля безопасности и моделирование взломов и атак, чтобы протестировать защиту организации от имитируемых угроз. Полученные результаты могут подтвердить эффективность внедрённых средств контроля и действующих на месте мер безопасности
- **Показатели соответствия:** для отраслей с нормативными требованиями достижение и поддержание соответствия является ключевым показателем успеха. Отслеживание нарушения или проблем, связанных с соблюдением требований, чтобы оценить эффективность программы СТЕМ в поддержании нормативных стандартов
- **Соответствие требованиям и приоритетам:** это можно измерить качественно, оценив, направлены ли усилия по восстановлению на защиту наиболее важных бизнес-активов и соответствуют ли они ключевым целям бизнеса
- **Обратная связь с заинтересованными сторонами:** Сбор и анализ обратной связи от

заинтересованных сторон, вовлечённых в процесс СТЕМ. Положительные отзывы могут указывать на то, что программа достигает своих целей и хорошо воспринимается теми, кого она затрагивает

#### G. Плотность уязвимостей и время на устранение

**Плотность уязвимостей и время на устранение** — это два ключевых показателя, которые можно использовать для измерения эффективности программы непрерывного управления выявлением угроз (СТЕМ).

**Плотность уязвимостей** — это показатель количества уязвимостей на единицу кода или систему. Он даёт представление об общем состоянии безопасности систем организаций. Более низкая плотность уязвимостей указывает на более безопасную систему, в то время как более высокая плотность уязвимостей предполагает больший потенциал для использования. Для эффективного использования этого показателя организациям следует отслеживать изменения плотности уязвимостей с течением времени. Тенденция к снижению указывает на то, что программа СТЕМ эффективно выявляет и устраняет уязвимости, тем самым улучшая уровень безопасности организации. Показатель рассчитывается путём деления общего количества уязвимостей на общее количество систем или приложений. Этот показатель может быть использован для оценки количества остаточных уязвимостей во вновь выпущенной программной системе с учётом её размера. Высокая плотность уязвимостей указывает на то, что существует больше уязвимостей, требующих устранения, что может привести к более высокому риску эксплуатации. Организации должны стремиться поддерживать низкую плотность уязвимости, чтобы снизить риск эксплуатации

**Время до устранения (также известное как Среднее время реагирования или MTTR)** — это показатель среднего времени, необходимого для реагирования и устранения выявленных уязвимостей или угроз. Более низкий MTTR указывает на эффективную реакцию и разрешение, что предполагает более эффективную программу СТЕМ. Этот показатель имеет решающее значение, поскольку чем дольше уязвимость остаётся без внимания, тем выше вероятность того, что ею могут воспользоваться злоумышленники. Следовательно, успешная программа СТЕМ должна помочь сократить время между обнаружением и исправлением. Оно рассчитывается путём вычитания даты обнаружения из даты исправления. Проще говоря, MTTR — это количество дней, необходимое для устранения уязвимости в системе безопасности после её обнаружения. MTTR также может рассчитываться в каждом конкретном случае или на макроуровне. **Уравнение для MTTR выглядит следующим образом:**  $MTTR = (\text{Общая сумма обнаружений и времени исправления}) / (\text{Общее количество инцидентов})$ . Меньшее время на исправление указывает на то, что уязвимости устраняются быстро, и снижает риск эксплуатации. Организациям следует стремиться к сокращению времени на исправление, чтобы снизить риск

Оба показателя дают ценную информацию об эффективности программы СТЕМ. Постоянно отслеживая эти показатели, организации могут определить области, требующие улучшения, и принять меры по повышению уровня своей безопасности.

#### *Н. Альтернативы*

Существуют альтернативы СТЕМ, которые могут лучше подходить для определённых организаций или сценариев:

- **Open-source Cloud Security Posture Management (CSPM):** Инструменты с открытым исходным кодом являются экономически эффективными и гибкими решениями для обеспечения облачной безопасности. Они предлагают преимущества поддержки сообщества и возможности настройки. Однако их внедрение может быть ресурсоёмким и может поставить организацию в зависимость от сообщества в плане обновлений и улучшений
- **Vanta:** платформа для развития молодёжного киберспорта, которая предоставляет экспертный коучинг и наставничество. Он получил аккредитацию от STEM.org, что свидетельствует о его приверженности развитию необходимых навыков, таких как инновации, командная работа.
- **Defense Surface Management (DSM):** DSM предоставляет более эффективный способ подключения данных анализа угроз (TID) и СТЕМ. Это помогает организациям расставить приоритеты и оптимизировать свою защиту путём выявления сильных и слабых сторон и сравнения возможностей с тактиками, методами и процедурами противодействия (ТРР)
- **CloudBees Jenkins Enterprise and Operations Center:** Эти инструменты предоставляют больше

возможностей для визуализации конвейеров доставки программного обеспечения и восстановления после сбоев. Они обеспечивают большую наглядность операций Jenkins и позволяют централизованно управлять кластерами Jenkins masters, разработками и аналитикой производительности.

- **Unifying Remediation:** Этот подход использует автоматизацию для оптимизации реагирования на проблемы безопасности, сокращая ручное вмешательство и время реагирования. Это также включает рассмотрение контекста проблем безопасности, что помогает выявить наиболее важные проблемы, понять их первопричины и определить эффективные стратегии устранения
- **Pen Testing:** В то время как СТЕМ ориентирована на выявление и предотвращение как можно большего количества уязвимостей, тестирование с помощью пера — это управляемый человеком наступательный тест, который пытается достичь определённой цели. Использование обеих методологий значительно повышает прозрачность и обеспечивает более комплексный подход к обеспечению безопасности
- **Automation in Tax Preparation:** Автоматизация может помочь устраниТЬ риск человеческой ошибки, которая может возникнуть при ручном вводе данных, что приведёт к более точной финансовой отчётности. Это также может упростить процессы аудита, позволяя налоговым специалистам выявлять и расставлять приоритеты в областях с высоким уровнем риска.

**хiii. КОМПАНИИ,  
ВОВЛЕЧЁННЫЕ В  
РАЗЛИЧНЫЕ КИБЕР-  
АКТИВНОСТИ. ЧАСТЬ 1**



**Аннотация – В этом документе представлен анализ компаний, занимающихся наступательной безопасностью". Анализ охватывает различные аспекты инвентаризации, включая характер компаний, включённых в список, типы возможностей, которые они предлагают, и geopolитические последствия их услуг.**

**Предоставленная выдержка обобщает общедоступную информацию без раскрытия чувствительных или конфиденциальных данных. Она служит ценным ресурсом для специалистов по безопасности, предлагая представление об условиях участия частного сектора в наступательных кибер-операциях.**

#### A. Введение

Ряд компаний участвовали в наступательных кибер-операциях на уровне национальных государств, и предоставили такие возможности, как программные имплантаты, наборы средств взлома (включая эксплойты нулевого дня, структуры эксплуатации, методы обхода безопасности) и продукты для перехвата коммуникаций. Список не касается утечки секретной или конфиденциальной информации, а скорее объединяет то, что уже общедоступно. В список включены действующие, ликвидированные или приобретённые компании из разных стран мира. Перечень представляет собой совокупность общедоступной информации и включает ссылки на разведывательные данные из открытых источников (OSINT), в которых упоминается участие этих организаций в такой деятельности.

#### B. Разница между частными и публичными компаниями

Разница между частными и публичными компаниями заключается, прежде всего, в их структуре собственности и доступе к капиталу.

Частные компании принадлежат избранной группе лиц, часто принадлежащих членам семьи, основателям или

частным инвесторам. Их акции не торгуются на публичных биржах и не выпускаются посредством первичного публичного размещения акций (IPO). В результате частным фирмам не нужно соблюдать строгие требования Комиссии по ценным бумагам и биржам (SEC) к подаче деклараций. Акции этих предприятий менее ликвидны, и их оценку сложнее определить.

С другой стороны, акции публичных компаний котируются и торгуются на фондовых биржах, что делает их доступными для более широкого круга инвесторов. Это приводит к более децентрализованной структуре собственности. Публичные компании зачастую могут с большей лёгкостью продать акции или привлечь деньги посредством размещения облигаций. Они также подчиняются большему количеству правил и должны регулярно раскрывать информацию, публиковать свои финансы и действовать прозрачно.

В данном контексте частных компаний в сфере наступательной безопасности термин «частные» относится к компаниям, находящимся в частной собственности. В инвентаризации не проводится различие между частными и государственными компаниями; скорее, он фокусируется на компаниях, участвующих в наступательных кибер-операциях национальных государств. Термин «публичный» в этом контексте относится не к публичным компаниям, а к тому факту, что информация об этих компаниях является общедоступной.

#### C. Примеры частных компаний

Примеры частных компаний, которые участвовали в наступательных кибер-операциях на уровне национальных государств, перечисленные в Перечне частных компаний, занимающихся наступательной безопасностью, включают:

- **CyberPoint (США):** действует с 2015 года, есть ссылки в Википедии.
- **CyberRoot Risk Advisory (Индия):** действует с 2013 года, есть ссылки на IntelligenceOnline.
- **Cucura (Канада):** действует с 2013 года, есть ссылки на IntelligenceOnline.
- **DarkMatter Group (ОАЭ):** действует с 2014 года, есть ссылки в Википедии.
- **Cytrox Holdings Zrt (Венгрия):** действует с 2017 года, есть ссылки на CitizenLab.
- **STEALIEN Inc. (Южная Корея):** действует с 2015 года, отзывы на официальном сайте.
- **Synacktiv (Франция):** действует с 2012 года, есть ссылки на EX Files.
- **Syndis (Исландия):** действует с 2013 года, есть ссылки на DarkReading.

Эти компании были вовлечены, предоставляя такие возможности, как программные имплантаты, наборы средств вторжения (например, эксплойты 0day, платформы эксплуатации, методы обхода безопасности, продукты для перехвата коммуникаций и т. д.).

### 1) Предлагаемые услуги

Частные компании кибербезопасности, акции которых не торгуются на бирже, предлагают широкий набор услуг, направленных на защиту организаций от киберугроз. Эти услуги необходимы для защиты цифровых активов, обеспечения конфиденциальности данных и поддержания целостности информационных систем.

#### CyberPoint (США)

CyberPoint предлагает широкий набор услуг кибербезопасности, включая:

- **Тестирование на проникновение:** моделируются кибератаки для выявления уязвимостей.
- **Управление уязвимостями:** непрерывный мониторинг/тестирование и политики управления уязвимостями.
- **Реагирование на инциденты:** инфильтрация, «захват и контроль» активной системы, судебная экспертиза и анализ после взлома.
- **Облачное проектирование и инфраструктура:** безопасные и быстрые процессы разработки.
- **Искусственный интеллект (ИИ) и машинное обучение (МО) в кибербезопасности:** использование ИИ и МО для обнаружения вредоносного ПО, обратного проектирования, и предотвращения атак.
- **Технологический консалтинг и стратегии ИТ/ОТ:** индивидуальный консалтинг по технологиям, политике и операциям на глобальном рынке.

#### CyberRoot (Индия)

CyberRoot Risk Advisory включала:

- **Сети фишинга и шпионского ПО:** создание поддельных учётных записей для фишинга и слежки за пользователями по всему миру. Они использовали поддельные домены крупных провайдеров электронной почты и других сервисов для кражи учётных данных.

#### Cusura (Канада)

Cusura предлагает такие услуги, как:

- Аудит кибербезопасности
- Криминалистика и реагирование на инциденты
- Анализ вредоносного ПО
- Обучение безопасности

#### Группа DarkMatter (ОАЭ)

DarkMatter принимал участие в:

- **Наблюдение и кибершпионаж:** заключён контракт на проект «Project Raven», чтобы помочь ОАЭ наблюдать за правительствами и активистами. Для

этих операций они привлекли бывших сотрудников американской разведки.

#### Cytrix Holdings Zrt (Венгрия)

Cytrix включает в себя:

- **Разработка шпионского ПО:** известен разработкой шпионского ПО Predator, используемого в операциях по слежке за журналистами, политиками и другими людьми. Они были внесены в черный список Министерства торговли США за торговлю кибер-экспloitами.

#### STEALIEN Inc. (Южная Корея), Synaktiv (Франция), Syndis (Исландия)

STEALIEN Inc., Synaktiv или Syndis. предоставлять широкий набор услуг в области кибербезопасности:

- Пентест
- Оценка безопасности
- Реагирование на инциденты
- Консультации по безопасности

#### 2) Список предлагаемых услуг

Частные компании, занимающиеся кибербезопасностью, акции которых не торгуются на бирже, предлагают различные услуги по защите организаций от киберугроз

- **Оценка рисков:** выявление уязвимостей в сетях, данных и коммуникациях, а также рекомендации по их устранению и улучшению безопасности.
- **Услуги защиты:** реализация таких мер безопасности, как брандмауэры, системы обнаружения вторжений и антивирусное программное обеспечение.
- **Обнаружение угроз и реагирование:** мониторинг киберугроз, их обнаружение и реагирование для предотвращения ущерба, что может включать услуги управляемого обнаружения и реагирования (MDR).
- **Центр управления безопасностью (SOC) как услуга:** обеспечение круглосуточного мониторинга и управления угрозами для предприятий, которые не могут создать внутренний SOC.
- **Аналитика угроз:** предоставление информации о новейших тактиках взлома и возникающих угрозах.
- **Соблюдение требований и управление:** Помощь организациям в соблюдении нормативных требований и отраслевых стандартов.
- **Реагирование на инциденты:** Помощь организациям в реагировании на инциденты безопасности и восстановлении после них, включая судебно-медицинский анализ и планы исправления.

- **Обучение кибербезопасности:** обучение сотрудников передовым методам кибербезопасности для усиления человеческого элемента безопасности.
- **Управление уязвимостями:** сканирование и анализ систем на наличие уязвимостей и предоставление решений для их устранения.
- **Защита конечных точек:** защита конечных точек, таких как ноутбуки, мобильные телефоны и планшеты.
- **Сетевая безопасность:** защита целостности и удобства использования сети и данных.
- **Облачная безопасность:** защита облачной инфраструктуры и приложений.
- **Безопасность электронной почты:** защита электронной почты от таких угроз, как фишинг, спам и вредоносное ПО.
- **Услуги управляемой безопасности:** аутсорсинг управления устройствами и системами безопасности сторонним экспертам.

#### D. Публичные компании Примеры

Примеры публичных компаний, которые занимаются кибербезопасностью:

- **Palo Alto Networks (NYSE: PANW):** многонациональная компания в области кибербезопасности, известная своими передовыми межсетевыми экранами и облачными предложениями.
- **CrowdStrike Holdings, Inc. (NASDAQ: CRWD):** предоставляет облачные решения для защиты конечных точек, анализа угроз и услуг реагирования на кибератаки.
- **Check Point Software Technologies (NASDAQ: CHKP):** израильская компания, специализирующаяся на ИТ-безопасности, включая сетевую безопасность, безопасность конечных точек, облачную безопасность и мобильную безопасность.
- **CyberArk Software Ltd. (NASDAQ: CYBR):** израильско-американская компания кибербезопасности, специализирующаяся на безопасности привилегированного доступа.
- **Cloudflare Inc. (NYSE: NET):** американская компания, предоставляющая веб-инфраструктуру и безопасность веб-сайтов, включая предотвращение DDoS-атак и сетевые услуги безопасной доставки контента.
- **Rapid7 (NASDAQ: RPD):** компания, предоставляющая решения для данных и аналитики безопасности, включая услуги по управлению уязвимостями.

- **Cisco Systems (NASDAQ: CSCO):** многонациональный технологический конгломерат, который предоставляет решения в области кибербезопасности как часть своего разнообразного портфеля продуктов.
- **Broadcom (NASDAQ: AVGO):** глобальная технологическая компания, предоставляющая широкий набор полупроводниковых и инфраструктурных программных решений, включая программное обеспечение для кибербезопасности.
- **IBM (NYSE: IBM):** многонациональная технологическая компания, предлагающая ряд решений в области кибербезопасности в рамках своих более широких предложений продуктов и услуг.
- **VMware, Inc. (NYSE: VMW):** компания, специализирующаяся на программном обеспечении и услугах облачных вычислений и виртуализации, включая услуги безопасности.

Эти компании предлагают широкий набор решений в области кибербезопасности: от безопасности сети и конечных точек до облачной безопасности и анализа угроз. Они публично торгуются, то есть их акции доступны для покупки на публичных фондовых биржах.

#### 1) Предлагаемые услуги по компаниям

Публичные компании, занимающиеся кибербезопасностью, предлагают широкий набор услуг, предназначенных для защиты цифровых активов, данных и сетей от киберугроз и атак. Эти услуги обслуживают различные аспекты кибербезопасности, включая сетевую безопасность, облачную безопасность, безопасность конечных точек, анализ угроз и многое другое.

#### Palo Alto Networks (NYSE: PANW)

Palo Alto Networks предлагает комплексный набор услуг кибербезопасности, в том числе:

- **Службы поддержки клиентов:** рекомендации по обеспечению безопасности бизнеса и техническим результатам, онлайн-поддержка сообщества самообслуживания и экспертная помощь при переходе на новые технологии безопасности.
- **Глобальная поддержка:** Быстрая экспертная поддержка для максимального увеличения времени безотказной работы, снижения рисков и оптимизации операций.
- **Обучение и сертификация:** множество вариантов обучения, сертификации и цифрового обучения для расширения знаний и навыков в области кибербезопасности.
- **Целенаправленные услуги:** расширенная поддержка с участием менеджеров по работе с клиентами и технических экспертов, знакомых со средой клиента, индивидуальное рассмотрение обращений, анализ первопричин критических

проблем, а также упреждающие оповещения и планирование обновлений.

### CrowdStrike Holdings, Inc. (NASDAQ: CRWD)

CrowdStrike обеспечивает:

- Платформа CrowdStrike Falcon: унифицированная платформа для современной безопасности, предлагающая защиту от взломов в облаке с помощью унифицированной агентной и безагентной защиты, видимости в реальном времени, обнаружения и защиты от атак на основе личных данных.
- Управляемые услуги кибербезопасности и услуги по требованию: реагирование на инциденты, технические оценки, обучение и консультативные услуги для подготовки и защиты от сложных угроз.
- Полностью управляемые услуги: для обнаружения и реагирования (MDR), поиска угроз и защиты от цифровых рисков.

### Check Point Software Technologies (NASDAQ: CHKP)

Check Point предлагает:

- Платформа Check Point Infinity: прогнозирует и предотвращает атаки в сетях, облаках, конечных точках и устройствах с помощью облачной безопасности на базе искусственного интеллекта.
- ThreatCloud AI: выявляет и блокирует возникающие угрозы нулевого дня, обеспечивая точное предотвращение менее чем за две секунды для сотен миллионов точек применения.
- Унифицированное решение безопасности. Защищает везде, где выполняется работа, включая электронную почту, конечные точки и мобильные устройства, с помощью мощных инструментов искусственного интеллекта для команд Центра управления безопасностью.

### CyberArk Software Ltd. (NASDAQ: CYBR)

CyberArk фокусируется на безопасности личных данных, предлагая:

- Платформа безопасности личных данных: защищает каждую личность с помощью необходимого уровня контроля привилегий в любой инфраструктуре.
- Беспрятственный и безопасный доступ: сочетает в себе безопасный единый вход, адаптивный MFA, управление жизненным циклом, службы каталогов и аналитику поведения пользователей.
- Интеллектуальное управление привилегиями: применяет средства контроля мирового класса ко всему ИТ-ресурсу, обеспечивая безопасность пользователей, сторонних поставщиков, конечных точек и идентификации компьютеров.

### Дополнительные услуги

Другие компании, такие как Cloudflare Inc. (NYSE: NET), Rapid7 (NASDAQ: RPD), Cisco Systems (NASDAQ: CSCO), Broadcom (NASDAQ: AVGO), IBM (NYSE: IBM) и VMware, Inc. (NYSE: VMW). ) также предлагают ряд решений кибербезопасности. К ним относятся смягчение последствий DDoS, сетевые услуги безопасной доставки контента, решения для данных и аналитики безопасности, решения кибербезопасности как часть разнообразного портфеля продуктов, программные решения для полупроводников и инфраструктуры, а также программное обеспечение и услуги для облачных вычислений и виртуализации соответственно.

- **Cloudflare (NET):** предлагает услуги кибербезопасности через свою платформу облачной безопасности, выступая в качестве посредника между серверами и посетителями клиентских сайтов. Услуги Cloudflare предназначены для различных отраслей, включая образование, электронную коммерцию, финансы, государственный сектор и игры. Его глобальная сеть охватывает более 300 городов в более чем 100 странах.
- **Secureworks (SCWX):** Имея более чем 20-летний опыт сбора информации об угрозах и изучения кибератак, Secureworks предлагает облачную платформу безопасности SaaS. Ее платформа Taegis может обрабатывать более 470 миллиардов событий каждый день, предоставляя комплексный обзор сети компании.
- **Cyren (CYRN):** создает службы интернет-безопасности для облака, помогающие защититься от атак, связанных с электронной почтой, таких как фишинг. Технология Cyren выявляет необычные закономерности для предотвращения кибератак без ущерба для конфиденциальности данных клиентов.
- **Splunk:** специализируется на программном обеспечении кибербезопасности, которое выявляет цифровые уязвимости и предотвращает атаки вредоносных программ. Платформа Splunk использует искусственный интеллект и машинное обучение для автоматического и точного обнаружения угроз, позволяя предприятиям сосредоточиться на реальных киберугрозах.
- **Сети A10 (ATEN):** обеспечивает безопасность присутствия в облаке и беспроводной сети 5G за счет использования машинного обучения и автоматизации для распознавания и предотвращения киберугроз. A10 также предлагает встроенный анализ данных для выявления попыток взлома.
- **Fortinet (FTNT):** предоставляет программное обеспечение безопасности, используемое в различных отраслях, предлагая такие инструменты, как защита брандмауэра, VPN, защита конечных точек и облачная безопасность. Fortinet придерживается политики нулевого доверия, чтобы

обеспечить доступ к приложениям и конфиденциальной информации только одобренному персоналу.

## 2) Список предлагаемых услуг

Компании, занимающиеся кибербезопасностью, как публичные, так и частные, предлагают широкий набор услуг для защиты организаций от киберугроз. Эти услуги обычно включают в себя:

- **Оценка рисков:** выявление потенциальных уязвимостей сети, данных и коммуникаций, а также рекомендации по их устранению и улучшению безопасности.
- **Услуги защиты:** внедрение таких средств защиты, как межсетевые экраны, системы обнаружения вторжений (IDS) и антивирусное программное обеспечение для защиты от несанкционированного доступа и кибератак.
- **Обнаружение угроз и реагирование на них:** мониторинг киберугроз, их обнаружение и быстрое реагирование, чтобы остановить их и предотвратить ущерб. Сюда могут входить услуги управляемого обнаружения и реагирования (MDR).
- **Центр управления безопасностью (SOC) как услуга:** обеспечение круглосуточного мониторинга и устранения угроз через SOC, что ценно для предприятий, которые не могут создать внутренний SOC из-за ограничений бюджета или кадров.
- **Разведка угроз:** идти в ногу с новейшими тактиками взлома и предоставлять информацию о возникающих угрозах для защиты от них.
- **Соответствие и управление:** обеспечение соответствия организаций нормативным требованиям и отраслевым стандартам, таким как HIPAA для здравоохранения или GDPR для защиты данных.
- **Реагирование на инциденты:** предложение услуг, помогающих организациям реагировать на инциденты безопасности и восстанавливаться после них, включая судебно-медицинский анализ и планы исправления.
- **Обучение кибербезопасности:** обучение сотрудников передовым методам кибербезопасности и потенциальным последствиям их действий по усилению человеческого элемента безопасности.
- **Управление уязвимостями:** сканирование и анализ систем на наличие уязвимостей и предоставление решений для их устранения.
- **Защита конечных точек:** защита конечных точек, таких как ноутбуки, мобильные телефоны и планшеты, от использования киберпреступниками.
- **Сетевая безопасность:** защита целостности и удобства использования сети и данных с помощью различных мер, включая сегментацию сети и контроль доступа.
- **Облачная безопасность:** предложение решений для защиты облачной инфраструктуры и приложений.
- **Безопасность электронной почты:** защита электронной почты от таких угроз, как фишинг, спам и вредоносное ПО.
- **Услуги управляемой безопасности:** аутсорсинг управления устройствами и системами безопасности сторонним экспертом.



**xiv. ПЕРСПЕКТИВЫ  
КИБЕРБЕЗОПАСНОСТИ В  
ТИХООКЕАНСКОМ  
РЕГИОНЕ (АРАС)**



**Аннотация** – В рамках анализа ситуации с кибербезопасностью в Азиатско-Тихоокеанском регионе (APAC) на 2023 год в этом документе рассматриваются различные аспекты киберугроз, которые оказали значительное влияние на регион. На регион приходится 31% глобальных кибератак, и он превратился в центр киберпреступной деятельности, причём более половины его организаций становятся жертвами этих угроз. Этот анализ направлен на то, чтобы обеспечить качественный синтез преобладающих угроз кибербезопасности, опираясь на информацию из различных исследований и отчётов, чтобы предложить целостное представление о вызовах и уязвимостях, с которыми сталкивается регион.

Выводы, полученные в результате этого анализа, имеют важное значение для специалистов в области кибербезопасности, ИТ-специалистов-практиков и заинтересованных сторон в различных секторах, предоставляя им более глубокое понимание проблем и вооружая их знаниями для совершенствования их стратегий защиты от меняющегося ландшафта киберугроз.

#### A. Введение

В 2023 году Азиатско-Тихоокеанский регион (APAC) столкнулся с множеством угроз кибербезопасности. На этот регион пришлось 31% глобальных кибератак, при этом более половины всех организаций региона сообщили, что они подвергались кибератакам.

Конкретные угрозы, нацеленные на регион в 2023 году, включали кампанию социальной инженерии группы Kimsuky по краже учётных данных, использование группой UNC4841 уязвимости нулевого дня и использование вредоносного ПО RDStealer, нацеленного на протокол удаленного рабочего стола.

В отчете Thales Data Threat Report также подчёркивается, что 60% респондентов из региона назвали расшифровку сети угрозой безопасности квантовых

вычислений, вызывающей наибольшую озабоченность. Кроме того, 50% организаций региона имели официальный план реагирования на программы-вымогатели по сравнению с 47% в 2022 году.

Рост числа кибератак угрожает жизненно важным секторам экономики Азии, которые становятся более уязвимыми по мере продолжения цифровой трансформации. Несмотря на увеличение количества специалистов кибербезопасности в регионе, по-прежнему существует нехватка подготовленных сотрудников, которая оценивается в 2,16 миллиона человек.

#### B. Топ угроз:

- Фишинг
- Инфостилеры
- Методы обхода MFA
- Программы-вымогатели
- Supply-chain атаки
- Атаки, мотивированные хактивизмом
- Риски генеративного ИИ.

Фишинг остаётся одной из наиболее распространённых киберугроз в регионе, при этом число инцидентов значительно возросло. Киберпреступники использовали различные методы, такие как SMS (смишинг), вишинг и выдачу себя за другое лицо в социальных сетях, чтобы обманом заставить людей разгласить конфиденциальную информацию. Использование генеративных технологий искусственного интеллекта, таких как ChatGPT, ещё больше усилило эти фишинговые кампании, позволяя злоумышленникам создавать более убедительный и целевой фишинговый контент.

InfoStealers, вредоносное ПО, предназначеннное для сбора и кражи конфиденциальных данных из систем жертв, продемонстрировали повышенную активность. Эти угрозы были нацелены на широкий спектр данных, включая личную идентификационную информацию, финансовые данные и учётные данные для входа в систему, создавая значительные риски как для отдельных лиц, так и для организаций.

Несмотря на широкое распространение многофакторной аутентификации (MFA) в качестве меры безопасности, киберпреступники разработали и использовали различные методы обхода защиты MFA. Эти методы использовали уязвимости в реализации систем MFA, с целью получения конфиденциальной информации.

Атаки программ-вымогателей резко возросли, при этом увеличилось количество инцидентов, направленных против предприятий и критической инфраструктуры. В рамках атак происходило не только шифрование данных, но и их кража, что удваивало давление вымогательства на жертв.

В регионе наблюдался рост числа chain-атак, когда киберпреступники проникали в системы программного обеспечения на этапе создания или обновления. Эти атаки

позволили злоумышленникам распространять вредоносное ПО среди пользователей скомпрометированного программного обеспечения, подчёркивая уязвимости в процессах разработки и распространения программного обеспечения.

Хактивизм набрал силу в регионе и были нацелен на правительственные учреждения, корпорации и другие организации, движимые различными политическими, социальными и экологическими мотивами. Последствия этих атак варьировались от утечек данных до разрушительных атак типа «отказ в обслуживании».

Потенциальное злоупотребление генеративными технологиями искусственного интеллекта стало новой угрозой кибербезопасности. Эти технологии могут быть использованы для автоматизации и усиления кибератак, включая фишинг, создание контента для вредоносных целей и создание дипфейков. Быстрое развитие технологий искусственного интеллекта потребовало переоценки стратегий кибербезопасности для борьбы с этими возникающими угрозами.

Угрозы кибербезопасности, с которыми столкнулся регион в 2023 году, имели серьёзные экономические и стратегические последствия. Прямые финансовые потери от кибератак, сбоев в работе, репутационного ущерба и увеличения затрат на кибербезопасность создали проблемы для экономической стабильности и роста региона. Более того, стратегические последствия спонсируемой государством кибердеятельности и атак на критически важную инфраструктуру подчёркивают важность национальной и региональной устойчивости кибербезопасности.

#### C. Последствия кибератак в Азиатско-Тихоокеанском регионе

Кибератаки в регионе имеют серьёзные последствия, затрагивающие как организации, так и отдельных лиц. Эти последствия подчёркивают необходимость более активных усилий по обеспечению кибербезопасности в регионе, включая увеличение инвестиций, улучшение возможностей обнаружения и реагирования, а также большую прозрачность в отношении кибератак.

- Компрометация конфиденциальной информации.** Примерно 49% успешных атак на организации привели к компрометации конфиденциальной информации. Сюда могут входить персональные данные клиентов или сотрудников, финансовые данные или конфиденциальная деловая информация.
- Нарушение основных операций.** В 27% случаев жертвы пострадали от сбоев в основных операциях, включая приостановку бизнес-процессов и услуг. Это может привести к значительным финансовым потерям и ущербу репутации организаций.
- Экономический потери:** если не будут приняты меры по повышению стандартов кибербезопасности, азиатские страны будут

продолжать сталкиваться с экономическими потерями от кибератак каждый год.

- Задержка обнаружения и реагирования.** Организациям в регионе требуется в 1,7 раза больше времени, чем в среднем по миру, чтобы обнаружить нарушение. Эта задержка может позволить злоумышленникам нанести больший ущерб или украсть больше информации.
- Недостаточная осведомлённость о кибербезопасности и инвестиции:** 70% организаций в регионе не имеют чёткого понимания своей кибер-позиции, а инвестиции в кибербезопасность в регионе на 47% ниже, чем в Северной Америке. Отсутствие осведомлённости и инвестиций может сделать организации более уязвимыми для атак.
- Отсутствие прозрачности.** Многие кибератаки не разглашаются из-за репутационных рисков. Отсутствие прозрачности может помешать региону осознать весь масштаб угрозы и эффективно отреагировать.
- Ответственность правительства:** правительство региона также несут ответственность за слабую кибербезопасность в регионе, при этом в некоторых странах действуют более комплексные законы о защите данных и кибербезопасности, чем в других.

#### D. Экономические последствия

- Финансовые потери:** около 63% организаций в регионе сообщили о финансовых последствиях из-за киберинцидентов. Точные денежные потери могут широко варьироваться в зависимости от характера и масштаба атаки, но они могут включать в себя прямые затраты, такие как выкуп, ремонт и восстановление системы, а также косвенные затраты, такие как потеря дохода из-за простоя.
- Нарушение основных операций.** В 27% случаев жертвы пострадали от сбоев в основных операциях, включая приостановку бизнес-процессов и услуг. Это может привести к значительным эксплуатационным расходам и снижению производительности.
- Репутационный ущерб:** публичное признание нарушения обычно влечёт за собой значительный репутационный ущерб в дополнение к повреждению систем. Это может привести к потере доверия клиентов и потенциальному снижению бизнеса, что может иметь долгосрочные экономические последствия.
- Экономический саботаж.** атаки направлены на экономический саботаж, который может иметь широкомасштабные последствия для экономики страны или региона.
- Нарушения в цепочках поставок.** могут вызвать сбои в цепочках поставок, что может привести к росту цен и экономической нестабильности.

- **Потеря рабочих мест.** крупная кибератака может привести к значительной потере рабочих мест. Например, уровень безработицы может вырасти до 5,7% в первом квартале после крупной атаки, что эквивалентно потере 3,1 миллиона рабочих мест.
- **Инвестиционные потери:** возможность потерять в общей сложности 2,884 миллиарда долларов США (в реальном выражении) инвестиций за 5 лет.
- **Увеличение затрат на кибербезопасность:** по мере роста киберугроз организациям и правительствам необходимо больше инвестировать в меры кибербезопасности, что может стать значительным экономическим бременем.
- **Репутационный ущерб:** репутационный ущерб от кибератаки может иметь долгосрочные последствия для ценности бренда компании и доверия клиентов, что потенциально может привести к снижению бизнеса и доходов.
- **Снижение кредитного рейтинга:** атака может привести к снижению кредитного рейтинга компании, что может увеличить стоимость заимствований и повлиять на её способность привлекать капитал.

В 2023 году наиболее пострадавшими от кибератак отраслями в регионе были:

- **Производство.** в отрасли зарегистрировано 48% случаев кибератак.
- **ИТ-компании:** входят в тройку наиболее целевых отраслей благодаря ценным данным, с которыми они работают, и быстрой цифровой трансформации в регионе.
- **Финансы и страхование.** сектор также подвергся серьёзным кибератакам.
- **Розничная торговля:** за последние 24 месяца произошло наибольшее количество успешных кибератак, в основном из-за нехватки бюджета на кибербезопасность.
- **Правительственные учреждения:** подвергались атакам, поскольку содержат ценную информацию, такую как личные данные граждан и информацию национального значения.
- **Промышленные компании:** подверглись нападению из-за потенциального экономического кризиса и кражи интеллектуальной собственности.
- **Фармацевтика и сельское хозяйство:** эти отрасли жизненно важны для экономики и национальной безопасности, что делает их привлекательными целями для киберпреступников.
- **Здравоохранение:** организации здравоохранения хранят конфиденциальную информацию и часто имеют ограниченные ИТ-ресурсы, что делает их уязвимыми для кибератак.

- **Образование/исследования:** этот сектор подвергся наибольшему количеству атак: в среднем 2160 атак на организацию в неделю.

### 1) Производство

#### Непосредственные финансовые и операционные последствия

- **Прямые финансовые потери:** крупные производственные компании в регионе могут потерять в среднем 10,7 миллионов долларов США из-за кибератаки. Эти потери включают в себя как прямые затраты, такие как потеря производительности, штрафы и затраты на исправление ситуации, так и косвенные затраты, (отток клиентов из-за репутационного ущерба).
- **Операционные сбои.** атаки могут нарушить производственные операции, что приведет к простоям и снижению производительности. Сложность управления большим портфелем ИБ-решений может привести к увеличению времени восстановления после кибератак, что ещё больше усугубляет сбои в работе.
- **Нарушения в цепочке поставок.** организации не только теряют время и ресурсы на борьбу с последствиями атаки, но также может быть нарушена вся цепочка поставок, что затронет как организацию, так и ее партнеров.

#### Долгосрочные экономические и стратегические последствия

- **Задержка цифровой трансформации.** три из пяти производственных организаций в регионе задержали ход цифровой трансформации из-за проблем с кибербезопасностью. Эта задержка ограничивает возможности производственных организаций защищаться от кибератак и использовать новые технологии, такие как искусственный интеллект, облака и Интернет вещей, для повышения производительности и предоставления новых линий обслуживания.
- **Компрометация конфиденциальной информации.** производственные организации подвергаются нападениям из-за своих ценных данных, включая интеллектуальную собственность и конфиденциальную оперативную информацию. Компрометация таких данных может иметь серьёзные последствия для конкурентных преимуществ и позиционирования на рынке.
- **Повышенная кибербезопасность затраты.** Чтобы защититься от растущих угроз, производственным организациям необходимо больше инвестировать в меры кибербезопасности, что может стать значительным экономическим бременем. Это включает в себя инвестиции в возможности искусственного интеллекта и машинного обучения для автономного выявления киберугроз и улучшения их обнаружения и реагирования.

#### Отраслевые уязвимости

- **Цель по экономическому разрушению и краже интеллектуальной собственности.** Производственный сектор особенно уязвим из-за его решающей роли в экономике и потенциального экономического кризиса и кражи интеллектуальной собственности.

#### Стратегии реагирования и смягчения последствий

- **Укрепление кибербезопасности с помощью ИИ.** ИИ играет решающую роль, позволяя организациям защищаться от все более сложных киберугроз. Решения кибербезопасности, дополненные возможностями ИИ и машинного обучения, могут помочь быстро выявлять угрозы за счёт обнаружения поведенческих аномалий и введения правил для блокировки или карантина устройств, ведущих себя неожиданно.

#### 2) ИТ-компании

##### Непосредственные финансовые и операционные последствия

- **Прямые финансовые потери.** В ИТ-секторе региона наблюдается рост количества атак на веб-приложения и API на 36%, при этом произошло более 3,7 миллиардов атак. Эти атаки могут привести к существенным финансовым потерям из-за ремонта системы, затрат на восстановление и потенциальных штрафов за несоблюдение нормативных требований.
- **Сбои в работе.** атаки могут привести к значительным сбоям в работе ИТ, что приведет к простоям и снижению производительности. Сложность управления большим портфелем ИБ-решений может привести к увеличению времени восстановления после кибератак.

##### Долгосрочные экономические и стратегические последствия

- **Репутационный ущерб.** Публичное раскрытие информации о кибератаке может нанести ущерб репутации ИТ-компании, что приведёт к потере доверия среди потребителей, партнёров и инвесторов. Это может иметь долгосрочные последствия для доли рынка и прибыльности.
- **Проблемы с нормативным регулированием и соблюдением требований.** Кибератаки могут привести к несоблюдению нормативных требований, что приведёт к штрафам и судебным разбирательствам. Это особенно важно для ИТ-компаний, где соблюдение законов о защите данных и конфиденциальности клиентов имеет первостепенное значение.

#### Отраслевые уязвимости

- **Цель по краже данных и финансовой выгоде.** ИТ-сектор особенно уязвим из-за его роли в эпоху цифровой трансформации и ценных данных, с которыми он работает. Киберпреступники могут

атаковать ИТ-компании, чтобы нарушить работу, украсть конфиденциальные данные или совершить финансовое мошенничество.

#### Стратегии реагирования и смягчения последствий

- **Увеличение затрат на кибербезопасность.** ИТ-компаниям необходимо инвестировать значительные средства в защитные меры. Это включает в себя усиление киберзащиты, проведение регулярных проверок безопасности и обучение персонала, что может стать существенным экономическим бременем.

#### 3) Финансы и страхование

##### Непосредственные финансовые и операционные последствия

- **Прямые финансовые потери.** количество атак на веб-приложения и API увеличилось на 36%, что в общей сложности составило более 3,7 миллиардов атак. Эти атаки могут привести к прямым финансовым потерям из-за «ремонта» системы, затрат на восстановление и штрафов за несоблюдение нормативных требований.

- **Сбои в работе.** атаки могут привести к значительным сбоям в работе, простоям и снижению производительности. Сложность управления большим портфелем решений кибербезопасности может привести к увеличению времени восстановления после кибератак.

##### Долгосрочные экономические и стратегические последствия

- **Репутационный ущерб.** Публичное раскрытие информации о кибератаке может нанести ущерб репутации финансового учреждения, что приведёт к потере доверия среди потребителей, партнёров и инвесторов. Это может иметь долгосрочные последствия для доли рынка и прибыльности.
- **Проблемы с нормативным регулированием и соблюдением требований.** атаки могут привести к несоблюдению нормативных требований, штрафам и судебным разбирательствам. Это особенно важно для финансовых учреждений, где соблюдение законов о защите данных и конфиденциальности клиентов имеет первостепенное значение.

#### Отраслевые уязвимости

- **Цель по экономическим потрясениям и краже данных.** Финансовый и страховой сектор особенно уязвим из-за роли в экономике и потенциального экономического сбоя и кражи конфиденциальных данных. Атаки этот сектор, могут сорвать операции, украсть конфиденциальные данные или совершить финансовое мошенничество.

#### Стратегии реагирования и смягчения последствий

- **Увеличение затрат на кибербезопасность.** учреждениям необходимо инвестировать

значительные средства в меры кибербезопасности. Это включает в себя усиление киберзащиты, проведение регулярных проверок безопасности и обучение персонала, что может стать существенным экономическим бременем.

- **Регуляторные и репутационные риски:** контроль со стороны регулирующих органов и репутационные риски усилились по всему региону, при этом громкие утечки данных влияют на финансовые показатели, вызывают негативную проверку со стороны регулирующих органов, подрывают акционерную стоимость и подвергают риску корпоративных должностных лиц.

#### 4) Розничная торговля

##### Непосредственные финансовые и операционные последствия

- **Прямые финансовые потери.** За последние 24 месяца в сфере розничной торговли в регионе произошло наибольшее количество успешных кибератак, в первую очередь из-за недостаточности бюджетов на кибербезопасность. Это привело к прямым финансовым потерям, включая затраты на «ремонт» и восстановление системы, а также потенциальным штрафам за несоблюдение нормативных требований.
- **Операционные сбои.** Кибератаки могут привести к серьёзным сбоям в работе розничной торговли, простоям и снижению производительности. Сложность управления большим портфелем ИБ-решений может привести к увеличению времени восстановления после кибератак.

##### Долгосрочные экономические и стратегические последствия

- **Репутационный ущерб.** Публичное раскрытие информации о кибератаке может нанести ущерб репутации розничной организации, что приведёт к потере доверия среди потребителей, партнёров и инвесторов. Это может иметь долгосрочные последствия для доли рынка и прибыльности.
- **Проблемы с нормативным регулированием и соблюдением требований.** атаки могут привести к несоблюдению нормативных требований, что приведёт к штрафам и судебным разбирательствам. Это особенно важно для организаций розничной торговли, где соблюдение законов о защите данных и конфиденциальности клиентов имеет первостепенное значение.

##### Отраслевые уязвимости

- **Цель по экономическим потрясениям и краже данных.** Сектор розничной торговли особенно уязвим из-за его критической роли в экономике и возможности экономического разрушения и кражи конфиденциальных данных. Атаки на розничные компании, могут нарушить их работу, украсть

конфиденциальные данные или совершить финансовое мошенничество.

##### Стратегии реагирования и смягчения последствий

- **Увеличение затрат на кибербезопасность.** организациям необходимо инвестировать значительные средства в меры кибербезопасности. Это включает в себя усиление киберзащиты, проведение регулярных проверок безопасности и обучение персонала.

##### Дополнительные соображения

- **Атаки программ-вымогателей.** Сектор розничной торговли уязвим для атак программ-вымогателей, поскольку он обрабатывает большой объем транзакций по кредитным картам. Использование программ-вымогатели для шифрования важных данных приводит к требованию выкупа, что ещё больше усугубляет финансовые потери.
- **Вредоносные боты.** В коммерческом секторе также наблюдалось значительное количество вредоносных ботов, чему способствовало количество и частота праздничных торговых мероприятий, а также рост количества онлайн-бронирований путешествий. Однако в первом квартале 2023 года активность вредоносных ботов существенно снизилась.

#### 5) Государственные органы

##### Непосредственные последствия для эксплуатации и безопасности

- **Компрометация конфиденциальной информации.** Госсистемы хранят огромное количество ценной информации, включая личные данные граждан, статистику и информацию национального значения. Злоумышленникам удалось похитить данные в 44% успешных атак на правительственные организации, что создало значительный риск для национальной безопасности и конфиденциальности личности.
- **Нарушение работы государственных служб.** атаки серьёзно нарушают работу правительства, что приведёт к приостановке работы важнейших государственных служб, что имеет последствия для жизни граждан и экономики.

##### Финансовые затраты

- **Прямые и косвенные финансовые потери.** Финансовые последствия включают в себя прямые затраты, такие как восстановление системы, и косвенные затраты, такие как потеря производительности и репутационный ущерб, что отвлекает ресурсы от основных госуслуг.

##### Репутационный ущерб

- **Потеря общественного доверия.** атаки подрывают доверие общества к государственным учреждениям. Восприятие неадекватных мер кибербезопасности

может привести к снижению уверенности в способности правительства защитить конфиденциальную информацию и обеспечить общественную безопасность.

## Проблемы регулирования и соблюдения требований

- **Несоблюдение правил:** атаки приводят к несоблюдению различных правил, касающихся защиты данных и конфиденциальности, что приведет к штрафам и судебным разбирательствам. Это особенно важно для государственных учреждений, которые придерживаются высоких стандартов защиты данных.

## Угрозы национальной безопасности

- **Шпионаж и саботаж.** Правительственные учреждения являются основными объектами спонсируемого государством кибершпионажа и диверсий. Атаки приводят к краже конфиденциальной информации о национальной безопасности или нарушению работы критически важной инфраструктуры, создавая серьёзную угрозу безопасности на уровне страны.

## Долгосрочные стратегические последствия

- **Международные отношения и геополитическая напряжённость.** Атаки на правительственные учреждения могут иметь долгосрочные последствия для международных отношений, особенно если их приписывают субъектам иностранных государств. Подобные инциденты могут привести к эскалации геополитической напряжённости и привести к ответным действиям.
- **Увеличение затрат на кибербезопасность.** правительственным учреждениям необходимо вкладывать значительные средства в меры кибербезопасности. Это включает в себя усиление киберзащиты, проведение регулярных проверок безопасности и обучение персонала, что может стать существенным экономическим бременем.

## Влияние на цифровую трансформацию

- **Препятствие для инициатив цифрового правительства.** ИБ-инциденты замедляют прогресс цифрового правительства, направленных на улучшение государственных услуг с помощью технологий, что, в свою очередь, может привести к сложности внедрения новых цифровых решений.

## 6) Промышленные компании

### Непосредственные финансовые и операционные последствия

- **Прямые финансовые потери:** крупные компании могут потерять в среднем 10,7 миллионов долларов США из-за кибератаки. Эти потери включают в себя прямые затраты: потеря производительности, штрафы, затраты на исправление ситуации, и

косвенные затраты, такие как отток клиентов из-за репутационного ущерба.

- **Сбои в работе.** Атаки приводят к значительным сбоям в производственных операциях, простоям и снижению производительности. Сложность управления большим портфелем решений кибербезопасности может привести к увеличению времени восстановления после кибератак.
- **Нарушения в цепочке поставок.** Вся цепочка поставок может быть нарушена в результате кибератак на производственные организации, затрагивающих не только целевую компанию, но и ее партнеров.

## Долгосрочные экономические и стратегические последствия

- **Задержка цифровой трансформации:** почти три из пяти производственных организаций в регионе задержали ход цифровой трансформации. Эта задержка может ограничить их возможности по защите от кибератак и использованию новых технологий для повышения производительности и предоставления новых линий обслуживания.
- **Компрометация конфиденциальной информации.** Производственные организации часто подвергаются нападениям из-за своих ценных данных, включая интеллектуальную собственность и конфиденциальную оперативную информацию. Компрометация таких данных может иметь серьёзные последствия для конкурентных преимуществ и позиционирования на рынке.

## Отраслевые уязвимости

- **Цель по экономическому разрушению и краже интеллектуальной собственности.** Производственный сектор особенно уязвим из-за его решающей роли в экономике и потенциального экономического кризиса и кражи интеллектуальной собственности. Киберпреступники и представители национальных государств могут атаковать этот сектор, чтобы сорвать операции, украсть конфиденциальные данные или провести промышленный шпионаж.

## Стратегии реагирования и смягчения последствий

- **Укрепление кибербезопасности с помощью ИИ.** ИИ играет решающую роль, позволяя производственным организациям защищаться от все более сложных киберугроз. Решения кибербезопасности, дополненные возможностями искусственного интеллекта и машинного обучения, могут помочь быстро выявлять угрозы за счёт обнаружения поведенческих аномалий и введения правил для блокировки или карантина устройств, ведущих себя неожиданно.

- 7) **Фармацевтика и сельское хозяйство**  
**Фармацевтический сектор**

- **Кражи интеллектуальной собственности.** Фармацевтический сектор является основной мишенью кибератак, направленных на кражу интеллектуальной собственности особенно в отношении формул лекарств и данных клинических испытаний. Такое воровство может подорвать конкурентные преимущества и привести к значительным финансовым потерям.
- **Операционные сбои.** Кибератаки могут нарушить производственные процессы и цепочки поставок, что приведёт к задержкам в производстве и распространении лекарств. Это может оказывать прямое влияние на общественное здравоохранение, особенно если пострадает производство важнейших лекарств.
- **Финансовые потери.** Финансовые последствия кибератак на фармацевтические компании могут быть ошеломляющими: затраты, связанные с нарушениями, в среднем превышают 5 миллионов долларов США. Эти затраты включают в себя прямые расходы, такие как выплаты выкупа и восстановление системы, а также косвенные затраты, такие как потерянный доход и судебные издержки.
- **Репутационный ущерб.** Публичное раскрытие информации о кибератаке может нанести ущерб репутации фармацевтической компании, что приведет к потере доверия среди потребителей, партнеров и инвесторов. Это может иметь долгосрочные последствия для доли рынка и прибыльности.
- **Проблемы с нормативным регулированием и соблюдением требований.** Атаки приводят к несоблюдению нормативных требований, к штрафам и судебным разбирательствам. Это особенно важно в фармацевтической отрасли, где соблюдение законов о защите данных и конфиденциальности пациентов имеет первостепенное значение.

## Сельскохозяйственный сектор

- **Нарушение операций.** Кибератаки могут нарушить сельскохозяйственную деятельность, затрагивая все: от мониторинга посевов до управления животноводством. Это может привести к снижению производительности и финансовым потерям для фермеров и агробизнеса.
- **Компрометация конфиденциальных данных.** Сельскохозяйственный сектор собирает и хранит огромное количество данных, от финансовых отчётов до информации об урожайности. Кибератаки могут поставить под угрозу эти данные, что приведёт к нарушению конфиденциальности и финансовой краже.
- **Уязвимости цепочки поставок:** Сельскохозяйственный сектор глубоко интегрирован в глобальные цепочки поставок. Кибератаки могут разрушить эти цепочки, что

приведет к нехватке продовольствия, росту цен и экономической нестабильности.

- **Финансовые последствия.** Затраты, связанные с восстановлением после кибератаки, включая выплаты выкупа, восстановление системы и усиление мер кибербезопасности, могут быть значительными для сельскохозяйственного бизнеса.
- **Репутационный ущерб.** Как и в фармацевтическом секторе, сельскохозяйственный бизнес может понести репутационный ущерб в результате кибератаки, что повлияет на доверие потребителей и деловые отношения.

## 8) Здравоохранение

Последствия кибератак на сектор здравоохранения в регионе глубоки и многогранны, они затрагивают не только непосредственные оперативные возможности медицинских учреждений, но также имеют долгосрочные последствия для доверия пациентов, финансовой стабильности и здравоохранения в целом. Вот некоторые из ключевых эффектов:

### Моментальный сбой в работе

Кибератаки могут серьёзно нарушить работу здравоохранения, мешая больницам оказывать своевременную помощь. Эти сбои могут быть особенно критичными во время чрезвычайных ситуаций в области здравоохранения, таких как пандемия COVID-19, когда спрос на медицинские услуги резко возрастает. Восстановление ИТ-систем и получение украденных данных часто требуют уплаты значительного выкупа, что ещё больше истощает ресурсы здравоохранения.

### Компрометация конфиденциальных данных пациентов

Организации здравоохранения хранят огромные объёмы конфиденциальных данных о пациентах, что делает их главной мишенью для киберпреступников. Компрометация таких данных может иметь серьёзные последствия для конфиденциальности пациентов и привести к краже личных данных и мошенничеству. Потеря конфиденциальных медицинских данных может привести к непоправимому репутационному ущербу, потере доверия и оттоку пациентов из медицинских организаций.

### Финансовые потери

Экономические последствия кибератак на организации здравоохранения в регионе могут быть ошеломляющими. Инцидент кибератаки может стоить крупной организации здравоохранения примерно 23,3 миллиона долларов США. Сюда входят как прямые затраты, такие как потеря производительности, штрафы и затраты на исправление ситуации, так и косвенные затраты, такие как отток клиентов из-за репутационного ущерба.

### Выкупные выплаты

Значительная часть медицинских организаций в регионе, ставших жертвами атак программ-вымогателей, в

итоге выплачивают выкуп. Это не только обременяет организации финансово, но и побуждает киберпреступников продолжать свою вредоносную деятельность.

### **Влияние на оказание медицинской помощи**

Кибератаки могут оказать умеренное или серьёзное влияние на оказание медицинской помощи, ставя под угрозу здоровье и безопасность пациентов. В некоторых случаях лечение неотложной помощи, необходимое пациентам, может быть отложено, а не экстренные случаи могут быть принудительно отменены, поскольку врачи и медицинский персонал не имеют доступа к жизненно важной информации о пациентах.

### **Проблемы регулирования и соблюдения требований**

Сектор здравоохранения строго регулируется, и кибератаки могут привести к несоблюдению различных правил конфиденциальности и безопасности медицинской информации. Это может привести к огромным штрафам и судебным разбирательствам, что ещё больше усугубит финансовую нагрузку на организацию здравоохранения.

### **Увеличение затрат на кибербезопасность**

Чтобы защититься от растущих угроз, организациям здравоохранения необходимо инвестировать в меры кибербезопасности, что может стать значительным экономическим бременем. Это включает в себя инвестиции в людей, процессы и технологии, такие как обучение кибербезопасности и разработку планов реагирования на инциденты.

### **Долгосрочный репутационный ущерб**

Публичное признание нарушения может нанести значительный репутационный ущерб, что потенциально может привести к долгосрочной потере доверия клиентов и снижению бизнеса. Это может иметь далеко идущие последствия для ценности бренда организации здравоохранения и ее способности привлекать и удерживать пациентов.

#### **9) Образование/Исследования**

Последствия кибератак на сектор образования и исследований в регионе серьёзны и могут иметь долгосрочные последствия для вовлечённых учреждений. Вот некоторые из ключевых эффектов:

### **Нарушение образовательных услуг**

Кибератаки могут привести к значительным сбоям в предоставлении образовательных услуг. Поскольку многие учреждения полагаются на цифровые платформы для обучения и исследований, кибератака может остановить занятия, задержать исследовательские проекты и привести к потере данных, что повлияет на студентов, преподавателей и результаты исследований.

### **Компрометация конфиденциальных данных**

Образовательные учреждения хранят множество конфиденциальных данных, включая личную информацию

студентов и сотрудников, финансовые отчеты и данные собственных исследований. Кибератаки могут привести к краже таких данных, что приведет к нарушению конфиденциальности и потенциальной краже личных данных.

### **Финансовые затраты**

Финансовые последствия кибератак на образовательные учреждения могут быть существенными. Затраты могут включать в себя выкуп, восстановление и восстановление системы, усиление мер кибербезопасности, а также потенциальные судебные издержки и штрафы за утечку данных.

### **Ущерб репутации**

Успешная кибератака может нанести ущерб репутации учебного заведения, привести к потере доверия среди учащихся, родителей и академического сообщества. Это может иметь долгосрочные последствия для числа учащихся и партнёрских отношений.

### **Вопросы регулирования и соответствия**

На образовательные учреждения распространяются различные правила, касающиеся защиты данных и конфиденциальности. Кибератаки, приводящие к утечке данных, могут привести к проблемам с несоблюдением требований, что приводит к штрафам и судебным разбирательствам.

### **Влияние на исследования**

Кибератаки могут поставить под угрозу ценные исследования, что приведёт к потере данных, краже интеллектуальной собственности и срыву исследовательской деятельности. Это может оказать существенное влияние на научный прогресс и инновации.

### **Увеличение затрат на кибербезопасность**

В ответ на киберугрозы образовательные учреждения должны инвестировать в меры кибербезопасности, что может стать значительным экономическим бременем. Сюда входят затраты на технологии безопасности, обучение и, возможно, найм дополнительного персонала кибербезопасности.

### **Утечка талантов и ресурсов**

Инциденты кибербезопасности могут отвлекать внимание и ресурсы ИТ-персонала от их основных обязанностей, влияя на общую производительность и операционную эффективность учреждения.

### **Долгосрочное образовательное воздействие**

Долгосрочное воздействие кибератак на образование может включать снижение качества образования из-за разрушения платформ цифрового обучения и потенциальную потерю исследовательских данных, на восстановление которых могут уйти годы.



# **xv. РЫНОК КИБЕР- СТРАХОВАНИЯ**



**Аннотация – В этом документе представлен анализ рынка кибер-страхования, на котором в последние годы наблюдался значительный рост и проблемы. Национальная страховая ассоциация (NAIC) сообщила о росте премий по кибер-страхованию на 75% в период с 2020 года по недавний период, что указывает на реакцию рынка на растущие кибер-угрозы и растущий спрос на страховое покрытие. Несмотря на этот рост, рынок является относительно новым, за последние пять-семь лет он значительно расширился и в настоящее время сталкивается с такими проблемами, как высокий спрос, превышающий готовность предложения, и неподходящая практика андеррайтинга.**

**Документ полезен тем, что специалисты по безопасности и специалисты из различных отраслей смогут понять последствия роста рынка кибер-страхования и полезность анализа для совершенствования мер кибербезопасности и стратегий управления рисками.**

#### A. Текущее состояние рынка

S&P Global Ratings сообщило, что глобальные премии по кибер-страхованию достигли около 12 миллиардов долларов в 2022 году и прогнозируют среднегодовой рост на 25%–30%, потенциально достигая 23 миллиардов долларов к 2025 году. Рост рынка кибер-страхования в значительной степени зависит от перестраховочной защиты, и перестраховщики считаются решающими для его устойчивого расширения. Отрасли рекомендуется способствовать более устойчивому базовому росту, который зависит не только от повышения ставок, но и от устранения системных кибер-рисков и расширения охвата большего числа малых и средних предприятий.

Текущее состояние рынка кибер-страхования демонстрирует признаки стабилизации после периода высокого давления и роста премий. Этот рынок описывается как «сложный», поскольку страховщики сталкиваются с такими проблемами, как рост премий и

снижение гибкости в плане политики. Однако последние тенденции показывают, что темпы роста страховых взносов замедляются, а в некоторых случаях продление полисов происходит по фиксированным ставкам.

Несмотря на эту стабилизацию, не ожидается, что рынок вернётся к более мягким условиям, наблюдавшимся в предыдущие годы. Продукты теперь покрывают меньше, а операторы связи вводят новые ограничительные формулировки политики. Строгие требования к контролю над андеррайтингом, которые действовали в прошлом, сохраняются, а спрос на мощности по-прежнему превышает предложение. Кроме того, на рынках кибер-страхования растёт обеспокоенность по поводу системного кибер-риска, который фокусируется на количественной оценке последствий катастрофического кибер-события.

Рынок кибер-страхования является относительно новым, набравшим значительную популярность за последние пять-семь лет, и он все ещё сталкивается с различными проблемами. Страховщики разрабатывают более строгие требования к полису, что привело к уменьшению количества страховых компаний и увеличению спроса. Тем не менее, есть оптимизм в отношении того, что страховщики и поставщики будут сотрудничать для разработки устойчивых решений с упором на улучшение управления рисками и их количественную оценку.

#### 1) Топ кибер-инцидентов

Полисы кибер-страхования обычно покрывают целый ряд кибер-атак и инцидентов, в том числе:

- **Утечки данных.** инциденты связаны с несанкционированным доступом к конфиденциальным данным или их кражей. Кибер-страхование может помочь покрыть расходы, связанные с реагированием на утечку данных, такие как расходы на уведомление, услуги кредитного мониторинга и судебные издержки.
- **Инциденты сетевой безопасности:** сюда входят атаки, которые ставят под угрозу безопасность сети компании, например заражение вредоносным ПО, распределённые атаки типа «отказ в обслуживании» (DDoS) и другие.
- **Вымогательство.** страхование часто покрывает расходы, связанные с кибер-вымогательством, например атаки программ-вымогателей, когда хакеры требуют оплаты восстановления доступа к цифровым активам компании.
- **Уничтожение данных.** если кибер-атака приводит к потере или уничтожению данных, кибер-страхование может помочь покрыть расходы на восстановление данных.
- **Перебои в работе компании.** если кибер-атака нарушает работу компании, кибер-страхование может покрыть потерю дохода во время простоя и затраты на восстановление операций.

- **Халатность:** данное покрытие распространяется на убытки, возникшие в результате ошибок или халатности при предоставлении услуг с учётом сбоев в услугах кибербезопасности.
- **Ответственность СМИ:** сюда входят претензии, связанные с цифровым контентом, такие как обвинения в нарушении авторских прав, клевете или вторжении в частную жизнь.

## B. Страхование ответственности или киберстрахование

Кибер-страхование и страхование киберответственности — это термины, которые часто используются как синонимы, но в зависимости от контекста они могут относиться к разным типам покрытия.

Кибер-страхование — это широкий термин, который обычно относится к ряду покрытий, предназначенных для защиты бизнеса от различных рисков, связанных с технологиями. Оно может включать как собственные, так и сторонние покрытия. Страхование собственной стороны защищает от финансовых потерь, которые застрахованная организация несёт непосредственно из-за кибер-инцидента, таких как убытки от прерывания бизнеса, затраты на восстановление данных и выплаты выкупа. Страхование третьих лиц относится к страхованию ответственности за претензии, предъявленные к застрахованной организации в связи с кибер-инцидентом, например, судебные иски, связанные с утечкой данных.

С другой стороны, страхование киберответственности часто используется для обозначения части страхования ответственности перед третьими лицами в полисе киберстрахования. Он покрывает ответственность застрахованной организации за ущерб, возникший в результате утечки данных или потери конфиденциальной информации. Сюда могут входить расходы, связанные с юридической защитой, урегулированием споров и вынесением судебных решений, а также штрафы и пени, налагаемые регулирующими органами.

Оба типа полисов направлены на смягчение финансовых последствий кибер-событий, но конкретные покрытия могут сильно различаться в зависимости от страховщиков и отдельных полисов.

### 1) Полисы страхования киберответственности

Киберответственность обычно включает покрытие претензий третьих сторон, возникших в результате киберинцидентов:

- **Покрытие ответственности за конфиденциальность:** защищает от ответственности, возникающей в результате утечки данных, которая раскрывает частные данные, и нарушений закона о конфиденциальности.
- **Инциденты сетевой безопасности:** покрывает убытки из-за нарушений безопасности, таких как несанкционированный доступ, вредоносное ПО и DDoS-атаки.

- **Нарушение работы бизнеса:** обеспечивает покрытие потери дохода и дополнительных расходов, понесённых в результате кибер-события, которое нарушает работу бизнеса.
- **Ответственность СМИ:** охватывает юридические претензии, связанные с электронным контентом, такие как нарушение авторских прав, клевета или вторжение в частную жизнь.
- **Халатность:** защищает от потерь из-за ошибок в предоставляемых услугах, особенно для фирм, предоставляющих технологические и профессиональные услуги.

### 2) Полисы киберстрахования

покрытие как собственных, так и третьих сторон.  
Типичные включения:

- **Уничтожение данных:** покрывает расходы, связанные с потерей или повреждением данных.
- **Вымогательство:** обеспечивает защиту от угроз раскрытия конфиденциальной информации или атак на системы, если не будет уплачен выкуп.
- **Интернет-кражи:** защищает от потерь из-за несанкционированных онлайн-транзакций.
- **Хакерская деятельность:** покрывает ущерб от взлома, включая утечку данных и вторжение в систему.
- **Отказ в обслуживании:** включает покрытие убытков, вызванных преднамеренными или случайными атаками типа «отказ в обслуживании».
- **Фонды вознаграждения за преступления:** некоторые политики могут предлагать средства за информацию, ведущую к аресту и осуждению киберпреступников.

### C. текущие тенденции на рынке киберстрахования

Современные тенденции на рынке киберстрахования:

- **Рост рынка:** прогнозируется, что рынок киберстрахования вырастет с 16,66 млрд долларов США в 2023 году до 84,62 млрд долларов США к 2030 году, при этом среднегодовой темп роста составит 26,1% в течение прогнозируемого периода.
- **Географическое доминирование.** Ожидается, что Северная Америка будет доминировать на рынке киберстрахования в течение прогнозируемого периода.
- **Увеличение спроса.** Существует высокий спрос на киберстрахование из-за растущего внедрения общедоступных облачных сервисов, развития моделей рабочего пространства, увеличения угроз кибербезопасности и потребности в технологических достижениях.
- **Стабилизация рынка.** После периода быстрого роста рынок начинает стабилизоваться.

Это связано с тем, что страховщики совершенствуют свои методы оценки рисков, новыми участниками рынка, обеспечивающими покрытие, а также естественным балансом спроса и предложения.

- **Более строгий андеррайтинг:** страховщики разрабатывают более строгие требования к полисам, что привело к сокращению количества страховых компаний и увеличению спроса.
- **Фокус на управлении рисками.** Управление кибер-рисками становится основным направлением деятельности в цифровом мире, и кибер-страхование рассматривается как неотъемлемая часть этого процесса. Отрасль работает над созданием устойчивого рынка кибер-страхования.
- **Влияние технологических тенденций.** Ожидается, что будущие кибер-атаки будут ускоряться благодаря ключевым технологическим тенденциям, таким как искусственный интеллект, мета-вселенная и конвергенция ИТ, Интернета вещей и операционных технологий (OT), которые создадут новые поверхности для атак и системные риски.
- **Нормализация цен.** Рост цен на кибер-страхование прекратился в четвёртом квартале 2022 года, что указывает на тенденцию к нормализации цен.
- **Увеличение удержаний по самострахованию.** Удержания по самострахованию продолжают увеличиваться, а это означает, что застрахованные стороны сохраняют больше риска до того, как начнёт действовать страховое покрытие.
- **Изменения основных лимитов:** снижение основных лимитов, которое было тенденцией, прекратилось в течение 2022 года.

#### D. Изменения рынка за последний год

Рынок кибер-страхования претерпел значительные изменения за последний год, с 2023 по 2024 год. Вот некоторые ключевые изменения:

- **Нормализация рынка.** После двух лет роста цен рынок кибер-страхования нормализуется. Коэффициенты убытков страховых компаний сейчас лучше, чем в последние несколько лет.
- **Рост цен прекратился:** рост цен на кибер-страхование прекратился в четвёртом квартале 2022 года.
- **Продолжающееся внимание к средствам контроля безопасности.** Андеррайтеры продолжают уделять внимание мерам безопасности, которые представляют собой меры, принимаемые для защиты цифровых активов.
- **Стабилизация.** Рынок кибер-страхования начал стабилизоваться после всплеска атак программ-вымогателей в последние годы.

- **Снижение цен.** Цены на кибер-страхование в США продолжали снижаться, снизившись на 6% в третьем квартале 2023 года.

#### E. Изменения страховых премий за последний год

За последний год на рынке кибер-страхования произошло несколько изменений в размерах премий:

- **Увеличение прямых письменных премий:** Прямые письменные премии по отдельному страхованию кибербезопасности в 2022 году увеличились на 61,5% по сравнению с предыдущим годом.
- **Стабилизация цен.** На рынке началась некоторая коррекция в 2022 и 2023 годах, когда цены на кибер-страхование начали стабилизироваться. Прямые письменные премии на признанном рынке выросли примерно на 50% в 2022 году по сравнению с увеличением более чем на 75% в 2021 году.
- **Снижение темпов роста политики:** количество действующих политик сократилось на 6,8% в 2021 году, но увеличилось на 4,4% в 2022 году.
- **Одобрения и исключения:** страховщики внедряют одобрения в отношении мер безопасности, чтобы ограничить свои риски и ужесточить формулировки политики, ограничивая покрытие путём исключений.
- **Повышенная ответственность за кибер-гигиену:** страхователям приходится более ответственно относиться к своей кибер-гигиене при получении страхового покрытия, а процесс подачи заявления стал более сложным.
- **Умеренный рост ставок:** цены на кибер-страхование в США выросли в среднем на 11% в годовом исчислении в первом квартале 2023 года, что было меньшим увеличением по сравнению с ростом на 28% в четвёртом квартале 2022 года. Темпы роста были умеренными, со средним ростом на 17% в декабре 2022 года по сравнению с высоким средним ростом в 133% в декабре 2021 года.
- **Снижение цен.** Цены на кибер-страхование в США продолжали снижаться, снизившись на 6% в третьем квартале 2023 года.

Эти изменения указывают на то, что рынок переживает переход от быстрого роста премий к более стабильному и умеренному росту премий, при этом страховщики становятся более избирательными и осторожными в своей практике андеррайтинга.

#### F. Повышенный спрос

К наиболее распространённым типам кибер-атак, которые привели к увеличению спроса на кибер-страхование в прошлом году, относятся:

- **Атаки программ-вымогателей.** Число атак программ-вымогателей резко возросло, что привело к значительному увеличению претензий по кибер-страхованию. В этих атаках киберпреступники шифруют данные жертв и требуют выкуп за их раскрытие. Средний спрос на выкуп также увеличился, что ещё больше стимулирует спрос на кибер-страхование.
- **Утечки данных.** Утечки данных остаются серьёзной проблемой, поскольку все больше страховых клиентов выбирают киберзащиту. Эти нарушения связаны с несанкционированным доступом к конфиденциальным данным, что может привести к значительному финансовому и репутационному ущербу.
- **Кибер-атаки на кибер-физическеские системы.** Атаки на кибер-физическеские системы, предполагающие взаимодействие цифровых и физических компонентов, растут. По оценкам, ущерб от этих атак достигнет более 50 миллиардов долларов США, что подчёркивает растущий риск и необходимость кибер-страхования.
- **Крупномасштабные атаки.** Крупномасштабные атаки, такие как атака с использованием программы-вымогателя Colonial Pipeline, выявили потенциал значительных сбоев и финансовых потерь, что увеличивает спрос на кибер-страхование.

#### G. Страхование и отрасли

Премии по кибер-страхованию могут значительно различаться в зависимости от отрасли и размера компаний

- **Факторы отраслевого риска:** некоторые отрасли считаются более рискованными из-за характера их деятельности и данных, которые они обрабатывают. Например, отрасли здравоохранения, финансов и розничной торговли часто обрабатывают конфиденциальные данные клиентов, что делает их привлекательными целями для киберпреступников. В результате компании в этих отраслях могут столкнуться с более высокими премиями.
- **Размер компании.** Более крупные компании обычно имеют более сложные системы и больше данных, что может увеличить их профиль риска. Поэтому им могут грозить более высокие премии. Однако малые и средние предприятия с сильным кибер-контролем и в отраслях с низким уровнем риска могут иметь средние премии в диапазоне от примерно 1400 до примерно 3000 долларов за миллион лимита.

- **Средства контроля кибербезопасности.** Компании с надёжным контролем и практикой кибербезопасности могут рассматриваться как менее рискованные и, следовательно, могут получить выгоду от более низких премий. И наоборот, компании, не имеющие базового контроля кибер-гигиены, могут столкнуться с более высокими страховыми взносами или даже столкнуться с трудностями при получении страхового покрытия.
- **История претензий.** Компании, в истории которых происходили кибер-инциденты, могут рассматриваться как компании с более высоким риском и получать более высокие премии.
- **Потребности в страховом покрытии.** Конкретные потребности компании в страховом покрытии, такие как тип и размер страхового покрытия, также могут влиять на размер премии. Более полное покрытие обычно предполагает более высокие страховые взносы.

#### H. Проблемы страхового рынка

В прошлом году рынок кибер-страхования столкнулся с рядом проблем:

- **Недостаток исторических данных.** Индустрия кибер-страхования сталкивается с нехваткой исторических данных, что затрудняет прогнозирование будущих кибер-рисков и установление цен на кибер-страхование.
- **Высокий спрос, ограниченное предложение.** Спрос на кибер-страхование растёт, но ограниченные возможности со стороны предложения привели к росту ставок и корректировкам покрытия, сроков и условий.
- **Просчёт риска.** Рынок кибер-страхования понёс значительные потери из-за просчёта риска, что привело к переходу рынка от мягкого цикла, характеризующегося более низкими премиями и более высокими лимитами, к жёсткому циклу, что привело к стремительному росту страховых премий.
- **Неподходящая практика андеррайтинга.** Рынок характеризуется неподходящей практикой андеррайтинга, при этом страховщики разрабатывают более строгие требования к полисам, что приводит к сокращению числа страховых компаний и резкому росту спроса.
- **Системный кибер-риск:** возможность крупномасштабной атаки, при которой потери сильно коррелируют между компаниями, затрудняет разработку комплексной политики.
- **Проблемы, специфичные для сектора.** Определённые сектора с исторически плохим состоянием безопасности, такие как

образование, или узкоспециализированные сектора, такие как разработчики программного обеспечения, могут испытывать более трудные времена с получением покрытия.

### I. Разница страховых взносов

Премии по кибер-страхованию могут значительно различаться в зависимости от отраслей с высокими и низкими кибер-рисками.

Для отраслей с высокими кибер- рисками, таких как здравоохранение, финансы и розничная торговля, которые часто обрабатывают конфиденциальные данные клиентов, премии обычно выше. Эти отрасли являются привлекательными целями для киберпреступников, и в результате они сталкиваются с более высокими премиями из-за повышенного риска.

С другой стороны, в отраслях с низкими кибер- рисками, например в отраслях со строгим кибер- контролем, средние премии могут варьироваться от примерно 1400 до примерно 3000 долларов за миллион лимита.

Кроме того, размер компании также играет роль в стоимости премии. Более крупные компании обычно имеют более сложные системы и больше данных, что может увеличить их профиль риска и, следовательно, они могут столкнуться с более высокими премиями. И наоборот, более мелкие предприятия в отраслях с низким уровнем риска и строгим кибер- контролем могут иметь более низкие премии.

Страховщики также стали более избирательно подходить к тому, кто и что покрывается страховкой, и ужесточили условия полиса, чтобы сократить непредвиденные убытки.

Высокие премии на рынке кибер-страхования обусловлены несколькими факторами:

- Рост кибер-угроз.** Число и стоимость кибер- угроз растут, что, в свою очередь, увеличивает стоимость страховых премий. По мере роста стоимости угроз растёт и стоимость премий.
- Рост претензий.** Частота и стоимость претензий растут, что приводит к увеличению коэффициента убытков страховщиков. Это привело к увеличению премий для покрытия возросших выплат.
- Недостаток исторических данных.** На рынке кибер-страхования отсутствуют обширные исторические данные, что затрудняет страховщикам точное прогнозирование будущих рисков и соответствующее установление премий.
- Отраслевые риски:** риск и, следовательно, стоимость кибер-страхования могут значительно различаться в зависимости от отрасли. Отрасли с более высокими кибер-

рисками обычно сталкиваются с более высокими премиями.

- Размер и характер бизнеса.** Размер и характер бизнеса также могут влиять на размер страховых премий. Более крупные предприятия или предприятия с более высоким профилем риска обычно сталкиваются с более высокими премиями.
- Географическое положение и нормативно-правовая среда.** Местоположение предприятия и нормативно-правовая среда, в которой оно работает, также могут влиять на премии. Например, предприятия, работающие в регионах со строгими правилами защиты данных, могут столкнуться с более высокими премиями.
- Тип покрытия.** Тип покрытия, который выбирает компания, также может влиять на размер страховых взносов. Более полное покрытие обычно сопровождается более высокими страховыми взносами.
- Практика управления рисками.** Страховщики часто учитывают практику кибербезопасности компании при установлении премий. Компании, применяющие надёжные меры кибербезопасности, могут быть вознаграждены более низкими премиями, в то время как компании с плохой практикой могут столкнуться с более высокими премиями.

### J. Страховое покрытие

Полисы кибер-страхования обычно покрывают широкий спектр кибер-атак, а конкретное покрытие может варьироваться в зависимости от размера бизнеса и конкретных рисков, с которыми он сталкивается:

- Утечки данных:** это один из наиболее распространённых типов кибер-атак, покрываемых кибер-страхованием. Речь идёт об инцидентах, когда к конфиденциальным, защищённым или конфиденциальными данным был получен доступ или они были раскрыты несанкционированным образом.
- Кибер-вымогательство:** сюда входят атаки программ-вымогателей, когда тип вредоносного программного обеспечения угрожает опубликовать данные жертвы или навсегда заблокировать доступ к ним, если не будет уплачен выкуп.
- Нарушения сетевой безопасности:** сюда относятся инциденты, когда неавторизованное лицо получает доступ к сети компании, что потенциально может привести к краже или повреждению данных.
- Перебои в бизнесе:** сюда входят убытки, которые бизнес может понести из-за кибер-

атаки, нарушающей его нормальную бизнес-операцию.

- **Ответственность за конфиденциальность:** сюда входят обязательства, возникающие в результате нарушений закона о конфиденциальности или кибер-инцидентов, в результате которых раскрываются частные данные.

Для крупных корпораций эти полисы часто включают покрытие обязательств перед третьими лицами, таких как расходы, связанные со спорами или судебными исками, убытки, связанные с клеветой, а также нарушением авторских прав или товарных знаков.

Для малых предприятий страховое покрытие может быть в большей степени сосредоточено на убытках, таких как расходы, связанные с уведомлением клиентов о взломе, оплатой судебных издержек и наймом экспертов по компьютерной криминалистике для восстановления скомпрометированных данных.

Предприятиям часто требуется сочетание как собственных, так и сторонних страховок, чтобы быть полностью защищёнными от целого ряда кибер-рисков, с которыми они сталкиваются.

### 1) Собственное страхование в полисах кибер-страхования

Страхование предназначено для покрытия прямых расходов, которые бизнес несёт в результате кибер-инцидента:

- **Прерывание деятельности:** потеря дохода и дополнительные расходы, понесённые из-за кибер-события, которое нарушает деятельность бизнеса.
- **Кибер-вымогательство:** покрытие выплат выкупа, произведённых в ответ на программы-вымогатели или другие угрозы кибер-вымогательства.
- **Восстановление данных:** Затраты, связанные с восстановлением или заменой утерянных или повреждённых данных.
- **Затраты на уведомление:** расходы на уведомление пострадавших лиц, клиентов или регулирующих органов после утечки данных.
- **Услуги кредитного мониторинга:** затраты на услуги кредитного мониторинга, предлагаемые пострадавшим лицам после утечки данных.
- **Связи с общественностью:** расходы, связанные с управлением репутацией компании после кибер-инцидента.
- **Судебное расследование:** гонорары экспертам за определение причины и масштаба кибер-нарушения.

### 2) Страхование третьих лиц в полисах кибер-страхования

Страхование ответственности третьих лиц — это страхование ответственности, которое защищает бизнес от претензий других лиц (клиентов, партнёров и т. д.) в связи с кибер-инцидентом, за который компания несёт ответственность. Это покрытие обычно включает в себя:

- **Расходы на юридическую защиту:** Плата за защиту от судебных исков, связанных с кибер-инцидентами.
- **Мировые соглашения и судебные решения:** расходы на судебные приговоры или урегулирования, возникающие в результате таких исков.
- **Нормативные штрафы и пени:** покрытие штрафов и санкций, которые могут быть наложены регулирующими органами после утечки данных или кибер-инцидента.
- **Ответственность перед СМИ:** защита от претензий о нарушении прав интеллектуальной собственности, клевете или вторжении в частную жизнь из-за электронного контента.

### 3) Чем отличаются полисы кибер-страхования от третьих сторон по размеру премий?

Размер страховых взносов по полисам кибер-страхования, предоставляемым собственными и третьими сторонами, может варьироваться в зависимости от нескольких факторов, и разница между ними обычно не стандартизируется в отрасли.

При страховании на размер страховых взносов часто влияют тип и объём конфиденциальных данных, которыми владеет компания, её отрасль, надёжность мер кибербезопасности и история кибер-инцидентов. Чем обширнее потенциальные прямые затраты (например, прерывание деятельности, восстановление данных и антикризисное управление), тем выше, вероятно, будет премия.

С другой стороны, премии по страхованию третьих лиц часто зависят от подверженности компании рискам ответственности. Это может зависеть от таких факторов, как характер деятельности компании, степень, в которой она обрабатывает или имеет доступ к данным третьих сторон, а также её договорные обязательства, связанные с безопасностью данных. Компании, которые предоставляют технологические услуги или обрабатывают большие объёмы сторонних данных, могут столкнуться с более высокими премиями за стороннее покрытие.

Важно отметить, что многие полисы кибер-страхования включают покрытие как собственных, так и третьих сторон, и общая премия по такому полису будет отражать совокупный риск. Как и в случае любого другого страхования, премии могут сильно различаться между страховщиками и отдельными полисами, поэтому

предприятиям следует получать котировки от нескольких страховщиков, чтобы гарантировать, что они получают наилучшую стоимость.

**4) Чем отличаются полисы кибер-страхования от третьих лиц с точки зрения франшизы**

Франшизы по полисам кибер-страхования как для собственной, так и для третьей стороны могут варьироваться в зависимости от нескольких факторов, включая тип и размер бизнеса, уровень кибер-риска, с которым он сталкивается, а также конкретные покрытия, включённые в полис.

При страховании на франшизу могут влиять потенциальные прямые затраты бизнеса в результате кибер-инцидента, такие как прерывание деятельности, восстановление данных и затраты на антикризисное управление. Компания с надёжной инфраструктурой кибербезопасности и хорошим опытом управления кибер- рисками может договориться о более низкой франшизе.

При страховании третьих лиц на франшизу может влиять подверженность бизнеса рискам ответственности. Компании, которые обрабатывают большое количество сторонних данных или предоставляют технологические услуги, могут иметь более высокие франшизы из-за повышенного риска претензий третьих сторон.

Как правило, более высокие франшизы приводят к более низким страховым взносам, и наоборот. Таким образом, предприятия должны сбалансировать стремление к более низким страховым взносам с возможностью платить более высокую франшизу в случае претензии.

**5) Факторы, влияющие на премии по собственным полисам кибер-страхования**

На размер страховых взносов по полисам кибер- страхования могут повлиять несколько факторов:

- Тип и объём данных.** Компании, которые обрабатывают большие объёмы конфиденциальных данных, таких как личная информация или данные кредитных карт, могут столкнуться с более высокими премиями из-за повышенного риска утечки данных.
- Отрасль:** некоторые отрасли, такие как здравоохранение и финансы, часто становятся объектами атак киберпреступников и могут столкнуться с более высокими премиями.
- Меры кибербезопасности.** Компании, применяющие надёжные меры кибербезопасности, могут договориться о более низких страховых взносах.
- Прошлые инциденты:** Компании, в прошлом сталкивавшиеся с кибер-инцидентами, могут столкнуться с более высокими премиями.
- Доход:** более крупные компании с более высокими доходами могут столкнуться с более высокими страховыми премиями из-за более серьёзных

потенциальных финансовых последствий кибер- инцидента.

- Пределы покрытия и франшизы:** более высокие лимиты покрытия и более низкие франшизы обычно приводят к более высоким страховым взносам.

**6) Факторы, влияющие на премии по сторонним полисам кибер-страхования**

На размер премий по полисам кибер-страхования третьих лиц также могут влиять несколько факторов:

- Тип предоставляемых услуг:** Компании, предоставляющие услуги, связанные с доступом к сторонним данным или системам, могут столкнуться с более высокими премиями из-за повышенного риска ответственности.
- Контрактные обязательства:** Компании могут столкнуться с более высокими премиями, если у них есть контрактные обязательства, которые увеличивают их ответственность в случае утечки данных.
- Отрасль:** как и в случае с собственным страхованием, некоторые отрасли могут столкнуться с более высокими страховыми премиями из-за повышенного риска кибер- инцидентов.
- Прошлые инциденты:** история кибер-инцидентов или претензий может привести к более высоким выплатам.
- Пределы покрытия и франшизы.** Как и в случае с собственным страхованием, более высокие лимиты покрытия и более низкие франшизы обычно приводят к более высоким страховым взносам.

**K. Исключения из страхования**

Полисы кибер-страхования обычно включают в себя несколько исключений, которые представляют собой конкретные ситуации или обстоятельства, не подпадающие под действие полиса.:

- Война и терроризм.** Полисы кибер-страхования обычно не включают покрытие убытков, возникших в результате военных действий, терроризма или других враждебных действий.
- Физический ущерб:** если кибер-атака разрушает физическую инфраструктуру или оборудование, страховщик не может покрыть расходы на ремонт или замену этих активов.
- Технологические улучшения:** Кибер-страхование помогает предприятиям восстановить свои компьютерные системы до состояния, в котором они находились до кибер-инцидента. Однако стоимость модернизации или усовершенствования технологии обычно не покрывается.
- Незашифрованные данные:** если утечка данных связана с незашифрованными данными, страховщик

может отклонить иск на основании этого исключения. Чтобы свести к минимуму риск отклонения претензии, предприятиям следует следовать лучшим отраслевым практикам шифрования данных и других мер безопасности.

- **Потенциальная будущая упущенная выгода и потеря стоимости из-за кражи интеллектуальной собственности.** Полисы кибер-страхования обычно не покрывают потенциальную будущую упущенную выгоду или потерю стоимости из-за кражи интеллектуальной собственности.

#### L. Отрасли с высоким кибер-риском

Отраслями с высоким уровнем кибер-риска обычно являются те, которые обрабатывают конфиденциальные данные и имеют высокую степень цифровой связи:

- **Здравоохранение:** эта отрасль является основной мишенью из-за конфиденциального характера данных, которые она обрабатывает, включая личную медицинскую информацию и платёжные реквизиты. Кибер-атаки также могут нарушить работу критически важных служб здравоохранения.
- **Финансовые услуги.** Банки и другие финансовые учреждения являются привлекательными целями из-за финансовых данных, которые они обрабатывают. Они часто преследуются с целью получения финансовой выгоды или разрушения финансовых систем.
- **Образование:** Образовательные учреждения часто располагают большими объёмами персональных данных и исследовательской информации, что делает их привлекательными целями. Они также часто имеют менее надёжные меры кибербезопасности по сравнению с другими секторами.
- **Розничная торговля.** Розничные торговцы обрабатывают большой объём личных и финансовых данных клиентов, что делает их привлекательными целями для киберпреступников. Платформы электронной коммерции особенно уязвимы из-за своей онлайновой природы.
- **Государственный сектор:** правительственные учреждения часто подвергаются нападениям из-за хранимой ими конфиденциальной информации, которая может включать личные данные, финансовую информацию и государственную тайну. Эти атаки могут быть мотивированы финансовой выгодой, шпионажем или подрывом деятельности.
- **Производство:** Производственный сектор становится все более объектом нападений из-за его высокого фактора разрушения и

возможности кражи интеллектуальной собственности.

- **Автомобильная промышленность.** Автомобильная промышленность становится мишенью из-за растущего числа транспортных средств и возможности крупномасштабных сбоев.

#### M. Отрасли с низким кибер-риском

Низко-рисковые отрасли включают в себя:

- **Сельское хозяйство.** Традиционное сельское хозяйство может быть не столь привлекательным для киберпреступников из-за меньшей зависимости от цифровых технологий и меньшего количества ценных цифровых активов по сравнению с другими отраслями.
- **Строительство.** Хотя строительные компании все чаще используют технологии, они могут быть не столь ценными объектами, как такие отрасли, как финансы или здравоохранение.
- **Развлечения и средства массовой информации.** Хотя эти отрасли действительно сталкиваются с кибер-riskами, особенно связанными с кражей интеллектуальной собственности, они, возможно, не так сильно подвергаются воздействию конфиденциальных персональных данных, как такие отрасли, как здравоохранение или финансовые услуги.
- **Услуги (нефинансовые):** Сфера услуг, которые не обрабатывают большие объёмы конфиденциальных финансовых данных, могут столкнуться с меньшими кибер-riskами.

Важно отметить, что ни одна отрасль не застрахована от кибер-risков, а уровень риска может варьироваться внутри отрасли в зависимости от конкретной практики компании и её подверженности. Даже в отраслях, в которых обычно считается более низкий кибер-risk, компании, которые больше связаны с цифровыми технологиями или обрабатывают любые конфиденциальные данные, все равно могут сталкиваться со значительными рисками и должны принимать соответствующие меры кибербезопасности.

#### N. Отраслевые кибер-риски

##### Здравоохранение

- **Утечки данных.** Медицинские организации хранят большие объёмы конфиденциальных данных, что делает их главной мишенью для утечек данных.
- **Программы-вымогатели.** Киберпреступники нацелены на здравоохранение, чтобы вызвать сбои в работе и вымогать деньги, шифруя данные пациентов и требуя выкуп.

##### Финансовые услуги

- **Кража данных.** Финансовые учреждения преследуются из-за финансовых данных, которые они обрабатывают, и которые могут быть использованы для мошенничества или проданы в даркнете.
- **Нарушение системы.** Атаки, направленные на нарушение работы финансовых систем, могут иметь широкомасштабные экономические последствия.

### Образование

- **Утечки данных.** Образовательные учреждения хранят ценные исследовательские данные и личную информацию студентов и сотрудников, которые могут быть атакованы.
- **Программы-вымогатели.** Школы и университеты все чаще становятся жертвами атак программ-вымогателей, которые нарушают работу и получают доступ к конфиденциальным данным.

### Розничная торговля

- **Мошенничество с платёжными картами.** Розничные торговцы обрабатывают большие объёмы платёжных транзакций, что делает их мишенью для киберпреступников, стремящихся украсть информацию о кредитных картах.
- **Атаки на электронную коммерцию.** Платформы онлайн-торговли подвержены различным кибер-атакам, включая утечку данных и атаки типа «отказ в обслуживании».

### Государственный сектор

- **Шпионаж.** Правительственные данные часто крадут в шпионских целях.
- **Финансовая выгода:** Государственное управление нацелено на получение финансовой выгода посредством различных кибер-атак.

### Производство

- **Кража интеллектуальной собственности.** Производственные компании становятся жертвами хакеров, которые хотят украсть интеллектуальную собственность, такую как дизайн продукции и чертежи.
- **Нарушение работы.** Кибер-атаки могут привести к физическому повреждению продуктов или машин, что приведёт к сбоям в работе.

### Автомобильная промышленность

- **Атаки на подключённые транспортные средства.** Поскольку транспортные средства становятся все более подключёнными, они подвергаются риску кибер-атак, которые могут

поставить под угрозу функциональность и безопасность транспортных средств.

- **Кража интеллектуальной собственности.** Автомобильные компании могут столкнуться с кибер-рискаами, связанными с кражей проектных и производственных данных.

### Сельское хозяйство

- **Кража данных.** Поскольку сельское хозяйство становится все более цифровым, данные, связанные с урожайностью сельскохозяйственных культур, здоровьем скота и производительностью техники, могут стать целью.
- **Нарушение операционной деятельности:** Кибер-атаки на сельскохозяйственные технологии могут нарушить работу сельского хозяйства.

### Строительство

- **Утечки данных.** Строительные компании часто обрабатывают конфиденциальные данные проектов, которые могут стать целью киберпреступников.
- **Нарушение операционной деятельности:** Кибер-атаки на строительные технологии могут нарушить сроки реализации проекта и привести к финансовым потерям.

### Развлечения и СМИ

- **Кража интеллектуальной собственности:** развлекательные и медиакомпании часто владеют ценной интеллектуальной собственностью, которая может стать целью киберпреступников.
- **Утечки данных.** Эти компании часто обрабатывают персональные данные клиентов, которые могут быть атакованы.

### Услуги (нефинансовые)

- **Утечки данных.** Сервисные компании часто обрабатывают персональные данные клиентов, которые могут быть атакованы.
- **Финансовое мошенничество.** Киберпреступники могут атаковать эти компании с целью получения финансовой выгода, например, посредством мошеннических транзакций.

### O. Прогнозы на будущее рынка кибер-страхования

Ожидается, что в рынок кибер-страхования будет иметь значительный рост, обусловленный увеличением частоты и стоимости кибер-угроз:

- **Рост рынка:** прогнозируется, что мировой рынок кибер-страхования значительно вырастет. По данным Fortune Business Insights, в

2022 году рынок оценивался в 13,33 млрд долларов США, и, по прогнозам, к 2030 году он вырастет до 84,62 млрд долларов США, при этом среднегодовой темп роста составит 26,1% в течение прогнозируемого периода.

- **Растущий спрос.** Спрос на кибер-страхование растёт, но ограниченные возможности предложения привели к корректировкам покрытия, сроков и условий. Этот спрос, вероятно, будет продолжать расти по мере роста кибер-угроз.
- **Динамический андеррайтинг.** Поскольку управление кибер-рискаами и их количественная оценка становятся все более популярными, переход к динамическому андеррайтингу станет более осуществимым. Это предполагает корректировку страховых премий на основе текущего состояния и практики компаний в области кибербезопасности, а не статических факторов.
- **Более строгие требования:** страховщики разрабатывают более строгие требования к полисам, что может привести к уменьшению количества страховых компаний, но увеличению спроса на кибер-страхование.
- **Политики, основанные на данных:** использование данных для реализации политики будет увеличиваться. Это может привести к более точному определению премий, снижению коэффициента убыточности и повышению прибыльности страховой отрасли.
- **Расширение сотрудничества:** ожидается, что страховщики и поставщики будут более тесно сотрудничать для разработки устойчивых решений для рынка кибер-страхования. Это может включать в себя усиление коммуникации и сотрудничества для предотвращения атак.

#### P. Факторы роста

- **Рост кибер-угроз.** Рост числа кибер-атак и утечек данных привёл к повышению осведомлённости о рисках и необходимости защиты, что привело к увеличению спроса на кибер-страхование.
- **Растущая осведомлённость:** все большее предприятий понимают необходимость кибер-страхования, поскольку они все больше осознают потенциальный финансовый и репутационный ущерб, который может возникнуть в результате кибер-угроз.
- **Нормативно-правовая среда:** Нормативно-правовая среда также является движущей силой роста. Поскольку правила защиты данных становятся более строгими, предприятия все чаще обращаются за кибер-страхованием, чтобы

помочь управлять своими регуляторными рисками.

- **Цифровая трансформация.** Сдвиг бизнес-моделей в сторону большего количества возможностей цифровой и электронной коммерции увеличил подверженность кибер-угрозам, что привело к увеличению спроса на кибер-страхование.
- **Политики, основанные на данных.** Использование данных для реализации политики становится все более распространённым. Это позволяет компаниям кибер-страхования предлагать более точно оценённые премии, что может привести к снижению коэффициента убытков и повышению прибыльности отрасли, тем самым стимулируя рост.
- **Ограниченнное предложение:** спрос на кибер-страхование растёт, но ограниченные возможности со стороны предложения привели к корректировкам покрытия, условий и положений, что способствовало бы росту рынка.
- **Осведомлённость о рисках и готовность:** повышение осведомлённости предприятий о кибер-рисках и признание необходимости защищать себя от этих рисков способствуют росту рынка.
- **Достижения в моделях андеррайтинга и оценки рисков:** страховщики работают над лучшим пониманием и количественной оценкой кибер-рисков, что способствует росту рынка.

Ожидается, что новые технологии будут определять будущее кибер-страхования несколькими способами:

- **ИИ и Метавселенная:** Будущие кибер-атаки будут все больше зависеть от ключевых технологических тенденций, таких как искусственный интеллект и так называемая «метавселенная».
- **Интернет вещей (IoT) и операционные технологии (ОТ):** Расширяющиеся миры IoT и ОТ открывают большие возможности, но также создают новые поверхности для атак, уязвимости и системные риски.
- **Услуги криpto-страхования:** ожидается, что растущее распространение услуг криpto-страхования будет способствовать расширению рынка, отражая растущую оцифровку финансовых услуг.

#### Q. Как страховые компании адаптируются к меняющемуся киберпространству

- **Более строгие практики андеррайтинга:** страховщики требуют более подробной информации об ИТ-системах и средствах контроля безопасности от компаний, желающих получить страховое покрытие. Это помогает им

лучше оценить риск и соответствующим образом адаптировать политику.

- **Более высокие франшизы и ограничения покрытия.** Чтобы управлять рисками, страховщики увеличивают франшизы и устанавливают ограничения на покрытие, особенно в отношении системных рисков, а также технологических ошибок и упущений.
- **Акцент на упреждающем управлении рисками.** Страховщики уделяют больше внимания упреждающему управлению рисками, поощряя предприятия к использованию комплексных методов управления рисками, включая партнёрство со сторонними поставщиками услуг безопасности для выявления и устранения уязвимостей.
- **Сотрудничество с ИБ-фирмами:** страховщики сотрудничают с фирмами кибербезопасности для разработки комплексных страховых продуктов, которые отражают лучшее понимание связанных с этим рисков.
- **Инвестиции в меры кибербезопасности:** страховщики инвестируют в надёжные меры кибербезопасности, регулярно обновляя свои системы и проводя комплексное обучение сотрудников по выявлению потенциальных угроз и реагированию на них.
- **Адаптация страховых продуктов:** Страховщики адаптируют свои продукты для удовлетворения индивидуальных потребностей клиентов, осознавая, что разные предприятия имеют разные проблемы и профиля рисков.
- **Построение партнёрских отношений за пределами страховой отрасли.** Страховщики работают с государственными учреждениями, научными учреждениями и отраслевыми ассоциациями, чтобы справляться с возникающими рисками и развивать более полное понимание ландшафта кибер-угроз.
- **Адаптация к волатильности рынка.** Опытные страховщики используют свои исторические знания, чтобы ориентироваться в колебаниях рынка и предоставлять клиентам стабильные и эффективные решения.

#### R. Страховые выплаты

Кибер-страхование имеет ряд преимуществ для бизнеса:

- **Покрытие от утечек данных.** Кибер-страхование может покрыть расходы, связанные с утечкой данных, включая судебные разбирательства, восстановление и

кражу личных данных. Это особенно выгодно, учитывая, что кибер-атака в среднем может стоить компании более 1 миллиона долларов.

- **Возмещение потерь бизнеса.** атаки часто прерывают бизнес и приводят к потере доходов, что возмещается полисом.
- **Защита от кибер-вымогательства.** страхование обеспечивает защиту от вымогательства, когда критически важные бизнес-данные шифруются до тех пор, пока компания не заплатит.
- **Покрытие убытков от перерыва в бизнесе.** Кибер-страхование может покрыть убытки от перерыва в бизнесе, поддерживая бизнес на плаву в финансовом отношении, пока предпринимаются усилия по восстановлению.
- **Соответствие нормативным требованиям.** Кибер-страхование может помочь покрыть потенциальные штрафы и расходы на юридическую защиту, связанные с несоблюдением правил защиты данных.
- **Управление репутацией:** если информация о клиентах взломана или данные взяты в заложники, это может существенно повредить репутации организаций. Кибер-страхование часто обеспечивает кризисное управление и поддержку по связям с общественностью для управления такими ситуациями.
- **Ресурсы для снижения рисков и восстановления:** Кибер-страхование предоставляет ресурсы для снижения рисков и восстановления, помогая предприятиям быстро реагировать на инциденты.
- **Ограничение финансовой ответственности:** страхование ограничивает финансовую ответственность бизнеса в случае кибер-атаки, предоставляя финансовую компенсацию для реагирования.
- **«Душевное спокойствие»:** страхование даёт уверенность, что предприятия приняли меры для обеспечения своей финансовой стабильности в случае кибер-инцидента.
- **Конкурентная дифференциация.** Наличие страхования может обеспечить конкурентное преимущество, демонстрируя приверженность бизнеса управлению кибер-リスクами.

ИРДОНИЯБЕЗОПАСНОСТЬ