I. Введение

Документ "BSAFE-Oh, Behave! 2023-FINAL REPORT" – 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

II. 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 по 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.

A. «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

B. «Разочарование и сомнения в онлайн-безопасности

Подчёркивается необходимость более персонализированных и практических подходов к обеспечению кибербезопасности, а также важность обеспечения безопасности решений и действий проще 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 скупости**: 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

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

1) Главный аргумент

Основной аргумент подраздела заключается в том, что, хотя традиционное обучение по 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.

2) Проблемы в области кибербезопасности

Обучение по кибербезопасности отличаются от традиционного несколькими способами. 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.

3) «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 рекомендации, которые не вносят путаницы или ненужных трений, которые могут привести к усталости от безопасности

4) 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, имитирующим реальные сценарии, такие как моделирование фишинга или комнаты для побега по 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

5) 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.

6) 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 отчётности**: многие люди не сообщают о попытках фишинга либо потому, что не знают как, не могут найти кнопки для сообщения, либо считают, что отчётность не остановит киберпреступников. Такое отсутствие отчётности 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

7) Балансирование воспринимаемых выгод и затрат с помощью обучения

Документ предлагает возможные варианты баланса достоинство и недостатков обязательного обучении:

- **Выделение непосредственных выгод**: подчёркивание непосредственных преимуществ безопасного поведения, таких как спокойствие, которое приходит от осознания того, что ваши данные защищены

- **Минимизирование 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

D. Жертвы киберпреступлений чаще и больше сообщают об инциднентах

Излагаются следующие ключевые моменты, подчёркивающие важность механизмов отчётности в борьбе с киберпреступностью и необходимость продолжения усилий по повышению доступности и эффективности процессов отчётности. 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

- **Отчётность 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 отчётностью**: хотя многие знали, как сообщать о фишинговых мошенничествах (49%), некоторые сочли процесс отчётности 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

1) 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 кража 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

2) Распространенные заблуждения относительно сообщений об инцидентах, связанных с киберпреступностью

Некоторые распространённые заблуждения относительно сообщений об инцидентах 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

3) 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

4) 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

III. 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.

A. 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

B. 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 по кибербезопасности**: доступ к обучению по 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 по кибербезопасности в целом были предпочтительнее, и те, кто прошёл курсы, сочли содержание тренинга полезным и увлекательным

C. 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

D. 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% кражи личных данных)

IV. 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

V. Обучение по 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 по кибербезопасности**: более половины участников из Канады (59%), Новой Зеландии (57%), Великобритании (56%) и Германии (51%) прошли обучение по 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 по 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 по 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 по кибербезопасности

VI. 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 по кибербезопасности**: важность обучения по кибербезопасности, но в разделе заключения не приводятся конкретные выводы или цифры.

A. 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 по кибербезопасности**: доступ к обучению по 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 власти.
- **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 правительств.
- **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 по кибербезопасности**: обучение по 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.

B. 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

C. 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.

D. Вызовы поколений

Эти результаты указывают на значительные различия между поколениями в отношении к 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%)

E. 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 по 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 по кибербезопасности

F. Обучение по 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 по кибербезопасности

- **Доступ к обучению по кибербезопасности**: более половины канадцев (59%), новозеландцев (57%), британских участников (56%) и немцев (51%) прошли обучение по 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 по 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 по 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 по 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%)