SECURE-T
SOLAR Group

2024

Стратегия киберкультуры

Для коммерческих организаций

Как сформировать полноценную киберкультуру внутри организации, простыми словами о сложном

Версия 1.0

Предисловие

Дорогие друзья!

В наше время человеческий фактор является одним из наиболее важных вызовов для периметра информационной безопасности.

Для того, чтобы своевременно отвечать на актуальные угрозы, организациям необходимо выстроить полноценную программу Киберкультуры. В процессе изучения данной тематики мы обратили внимание на то, что общепринятая методология отсутствует. Она позволила бы организациям выстроить свою собственную программу.

Мы взяли на себя не просто смелую, а поистине дерзкую задачу - составить документ, который позволит систематизировать разрозненные знания о том, как организациям наиболее эффективно управлять процессами формирования Киберкультуры. В нашей работе мы стараемся ответить на насущные вопросы: Как выстраивать процесс повышения осведомленности? Какие группы обучающихся нам следует выделять? Как должен выглядеть процесс обучения для каждой из этих групп? Какие метрики мы должны отслеживать, чтобы оценивать эффективность нашей программы? И, конечно же, самое главное - какие цели перед собой мы ставим?

Данная работа не несет в себе какой-либо коммерческой выгоды и сделана для всего коммьюнити информационной безопасности. Если у вас есть обратная связь или вы знаете, как сделать данную стратегию более состоятельной, приглашаем вас поделиться своими идеями на этот счет - strategy@secure-t.ru

В рамках исследования мы привлекали много разносторонних специалистов, которые были рады поделиться своим мнением, и постарались учесть их опыт в процессе создания документа.

Данный документ носит итерационный характер и будет издаваться в новых версиях, чтобы соответствовать актуальным угрозам.

Мы искренне надеемся, что данный документ принесет пользу для вас и сделает наше пространство еще более безопасным.

С наилучшими пожеланиями,
Генеральный директор ООО "Секьюр-Ти"
Никишкин Харитон

Содержание

Введение

Глобализация и стремительное развитие информационных технологий привели к тому, что формирование киберкультуры стало одной из ключевых задач для всех уровней — от руководства компаний до рядовых сотрудников. Современные вызовы в области киберугроз требуют от организаций внимательного подхода к формированию культуры безопасности и осведомленности среди сотрудников. Киберкультура также служит связующим элементом между поколениями, позволяя учитывать их различия в восприятии цифровой среды и объединяя сотрудников вокруг общих ценностей безопасности.

Совокупное количество персональных данных, скомпрометированных в результате внешних и внутренних утечек, в 2023 году достигло 47,24 млрд записей, тогда как в 2016 году этот показатель составлял всего 4,01 млрд записей, что подчеркивает стремительный рост угроз. В 2023 году стоимость утечки данных достигла нового максимума по всему миру: средняя стоимость утечки данных выросла до 4,45 млн долларов, среднее количество времени на обнаружение инцидента составило 204 дня, а средний ущерб от одной потерянной записи увеличился до 165 долларов.* Причиной 88 % кибератак и утечек данных является человеческий фактор.** Эти данные говорят о необходимости усиления мер защиты данных и повышения уровня киберкультуры среди всех сотрудников организаций.

*Утечки информации в мире, 2022-2023 годы

**Исследование Стэнфордского университета и компании Tessian

Введение

Современные компании всё чаще сталкиваются с вызовами кибербезопасности. Согласно данным Fortinet 2024 Security Awareness и Training Global Research Report, почти 70 % руководителей считают, что их сотрудники не обладают критически важными знаниями в этой области — серьёзный рост по сравнению с 56 % в 2023 году. Свыше 80 % организаций за последний год стали жертвами целенаправленных кибератак, таких как фишинг и вредоносное ПО.

С каждым годом зависимость от цифровых технологий увеличивается, что делает создание киберкультуры необходимым элементом устойчивости организаций. Под киберкультурой подразумевается совокупность норм, убеждений, ценностей, взглядов и предположений, которые являются неотъемлемой частью повседневной деятельности организаций и находят свое отражение в действиях всех подразделений и персонала данных организаций. Стратегия киберкультуры для организации направлена на формирование осознанного и ответственного поведения в цифровом пространстве, повышение уровня киберграмотности и создание безопасной цифровой среды для всех сотрудников. Важным элементом стратегии является вовлечение топ-менеджмента в учет киберрисков и принятие на основе этого решений для защиты организации.

Повышение уровня киберкультуры среди сотрудников организаций является одной из основополагающих задач стратегии. Это включает не только базовое обучение правилам безопасного использования интернет-ресурсов, но и более углубленные знания о защите данных, методах предотвращения фишинговых атак и распознавании киберугроз. Реализация стратегии будет способствовать формированию устойчивых навыков, которые необходимы для защиты информации в повседневной работе сотрудников, а также подготовит их к кризисным ситуациям и действиям в случае киберчрезвычайных ситуаций, обеспечивая оперативное реагирование.

Ключевые принципы

1. **Принцип осведомленности и образования:** повышение уровня знаний и навыков в области киберкультуры среди сотрудников организаций через постоянное обучение и информационные кампании.

2. **Принцип ответственности:** формирование ответственного поведения в цифровом пространстве у сотрудников организаций, способствующего безопасному использованию информационных технологий.

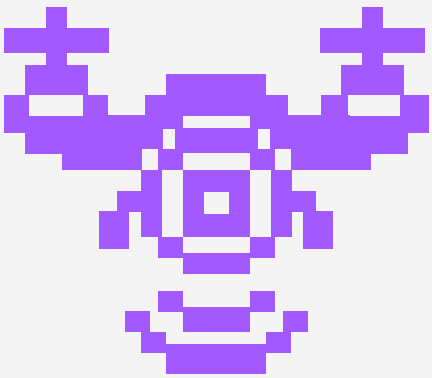
3. **Принцип сотрудничества и обмена опытом:** активное взаимодействие между различными уровнями внутри компании, а также с внешними партнерами и организациями для обмена знаниями и опытом в области киберкультуры.

4. **Принцип инноваций и адаптивности:** постоянное внедрение новых технологий и методик в образовательные программы, а также адаптация стратегии к новым вызовам и угрозам.

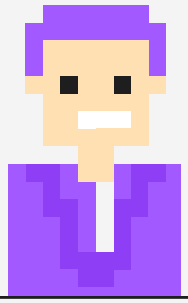
5. **Принцип непрерывного улучшения:** регулярный мониторинг и оценка эффективности реализуемых мер, а также постоянное совершенствование подходов к развитию киберкультуры на основе полученных данных по обучению и обратной связи.

6. **Принцип защиты и конфиденциальности:** обеспечение надежной защиты персональных данных и конфиденциальной информации сотрудников, а также повышение осведомленности о методах защиты личной информации в цифровом пространстве.

7. **Принцип вовлеченности и мотивации:** использование инновационных методов обучения, таких как геймификация и соревновательные элементы, для повышения вовлеченности сотрудников и поддержания их внимания.



Целевая аудитория



Топ-менеджеры и руководители

Включает высокопрофильных руководителей и членов правления организации

Уровень воздействия:

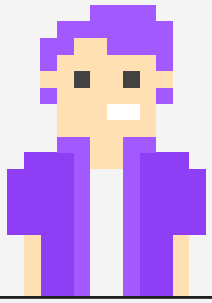
Высокий

Топ-менеджеры обладают доступом к конфиденциальной информации, включая финансовые данные компании, стратегические планы и персональные данные. Данная информация представляет собой высокую ценность для злоумышленников. Руководители имеют более высокий уровень киберкомпетентности в сравнении с обычными сотрудниками, но при этом нуждаются в постоянном обновлении знаний о новых угрозах.

Уровень критичности:

Критический

Неправильные решения в области безопасности могут привести к серьезным финансовым потерям, навредить репутации компании, поставить под угрозу приоритеты ИБ, требующие финансирования и поддержки на всех уровнях.



Технический трек

Включает технических специалистов, таких как системные администраторы, инженеры и разработчики, ответственные за внедрение и поддержку

Уровень воздействия:

Высокий

Технические специалисты также играют очень важную роль в обеспечении безопасности компании, так как они отвечают за внедрение и использование технических средств, гарантирующих защиту. Обязанности и знания технических специалистов напрямую влияют на уровень безопасности всей компании. Технический трек должен постоянно обновлять свои навыки и знания в новых технологиях и уязвимостях, так как угрозы становятся все более серьезными.

Уровень критичности:

Высокий

Технические специалисты обладают высоким уровнем знаний, но если их не поддерживать и не совершенствовать, это может привести к уязвимостям в системе. Тогда злоумышленники могут легко воспользоваться слабыми сторонами компании, что может привести к финансовым и репутационным потерям, а также к утечке данных компании.

Общий трек

Включает сотрудников различных отделов и уровней, которые взаимодействуют с информационными системами и данными

Уровень воздействия:

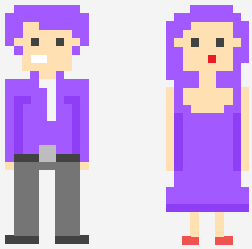
Высокий

Современные угрозы требуют от каждого сотрудника компании понимания основ киберкультуры, а также осознания своей ответственности за защищенность корпоративной информации. Обучение и участие всех работников в процессах обеспечения безопасности помогают создать атмосферу, где кибербезопасность становится частью корпоративной культуры. Повышение знаний всех сотрудников будет способствовать улучшению общего уровня защиты компании.

Уровень критичности:

Средний

Несмотря на то, что сотрудники имеют определенные знания о кибербезопасности, отсутствие постоянного обучения в данной сфере может привести к возникновению инцидентов ИБ. Невозможность интеграции киберкультуры в повседневные рабочие процессы может привести к финансовым потерям, репутационным рискам, утечке данных и другим инцидентам ИБ. Однако регулярное обучение и активная вовлеченность сотрудников значительно повысят защиту организации и помогут предотвращать риски, обеспечив устойчивость бизнеса.



Специалисты ИБ

Включает сотрудников в области информационной безопасности, ответственных за защиту данных и предотвращение угроз

Уровень воздействия:

Высокий

Специалисты ИБ играют ключевую роль в разработке и реализации стратегии киберкультуры. Поэтому данные специалисты обязаны регулярно обновлять свои знания о новых типах угроз и методах защиты. Несмотря на уже имеющийся высокий уровень осведомленности данной категории сотрудников, постоянно появляются новые виды угроз, в связи с чем специалисты ИБ должны иметь возможность эффективно предотвращать атаки злоумышленников и оперативно решать возникающие проблемы в данной области. Кроме того, им важно развивать эмоциональный интеллект для эффективного взаимодействия с сотрудниками. Также специалисты должны анализировать влияние СЗИ на процессы компании, учитывая их эргономику и соответствие бизнес-потребностям.

Уровень критичности:

Критический

Работа данных специалистов непосредственно влияет на защиту компании от киберугроз и соблюдение нормативных требований, а их культура заключается в непредвзятом отношении к пользователям и создании условий, в которых их не будут бояться. Низкий уровень киберкультуры сотрудников ИБ может привести к утечке конфиденциальной информации, финансовым убыткам и репутационным рискам.

Область применения

Стратегия направлена на развитие киберкультуры внутри организации, охватывая все ключевые подразделения и сотрудников, а также взаимодействие с внешними сторонами, включая клиентов, поставщиков и других участников экосистемы, с целью создания комплексного подхода к защите данных. Стратегия применяется к следующим направлениям:

Руководящие органы и управленческий персонал.

Топ-менеджеры и руководители несут ответственность за принятие стратегических решений в области кибербезопасности. В связи с этим важно обеспечить их понимание ключевых рисков и методов минимизации угроз, включая развитие осведомлённости и формирование культуры безопасного поведения.
Топ-менеджеры должны интегрировать кибербезопасность в общекорпоративную программу обучения, требовать систематического повышения компетенций у сотрудников и своим примером демонстрировать осведомленность и значимость этого направления.

Технические специалисты и ИТ-подразделения.

Сотрудники, которые отвечают за техническое обеспечение безопасности информационных систем, играют ключевую роль в защите критически важной информации. Для данных специалистов важно активно участвовать в обучении, направленном на освоение новых методов предотвращения угроз, а также внедрять передовые практики в повседневную работу.
Стратегия включает меры по усилению киберкультуры среди данных сотрудников для своевременного реагирования на угрозы и предотвращения инцидентов.

Операционные отделы и сотрудники.

Общие сотрудники компании, работающие с персональными данными, корпоративной информацией и внешними ресурсами, являются важным звеном в цепочке информационной безопасности. Стратегия направлена на повышение их киберкультуры, осведомлённости об угрозах и внедрение безопасных практик в повседневную работу.

Стратегия также применяется к следующим процессам:

- Обработка и хранение данных: соблюдение стандартов и требований к защите корпоративной и личной информации;
- Работа с удалёнными сотрудниками: создание и контроль условий для безопасного взаимодействия, включая использование стандартов безопасности;
- Внедрение и использование информационных систем: обеспечение киберкультуры при настройке и эксплуатации всех критически важных систем.

Стратегия распространяется на все уровни организации и способствует формированию единого подхода к вопросам киберкультуры, защите данных и предотвращению угроз. Её внедрение обеспечит более высокий уровень защищённости как внутри компании, так и при взаимодействии с внешними партнерами и организациями, а также соответствует комплаенсу:

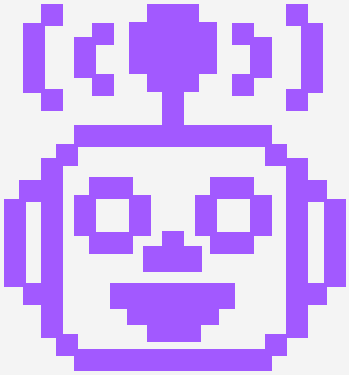
- Приказ ФСТЭК России № 239, № 17, № 31;
- Указ Президента № 250;
- 187-ФЗ;
- 152-ФЗ;
- 98-ФЗ;
- ГОСТ 57580.1, ГОСТ Р ИСО/МЭК 27002-2012;
- ГОСТ Р 56939-2016;
- Положение № 382-П, № 719-П;
- Payment Card Industry Data Security Standard;
- ИСО/МЭК 27001:2022;
- ISO/IEC 27001:2013;
- GDPR;
- NIST Cybersecurity Framework.

Сроки реализации проекта

Реализация стратегии киберкультуры организации рассчитана на период 5 лет. Этот период охватывает все этапы внедрения и совершенствования культуры среди сотрудников и подразделений. В зависимости от доступных ресурсов и приоритетов компании программа может быть сокращена до 1,5-3 лет, с акцентом на ключевые направления и ускоренную реализацию мероприятий.

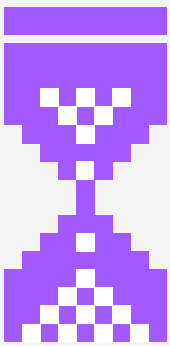
1.Первый год – подготовительный этап

В течение первого года необходимо провести разработку и утверждение обучающих программ, курсов по киберкультуре, фишинговых симуляций и информационных кампаний. Необходимо внедрить платформу для повышения осведомленности сотрудников о киберугрозах и безопасном поведении в цифровой среде, начать обучение ключевых групп сотрудников по созданным программам, а также привлечь амбассадоров кибербезопасности для популяризации культуры, легитимизировать процессы через политику обучения и выделение ресурсов. Необходима оценка результатов проекта за год.



2. Второй и третий годы – активная фаза обучения и проведения мероприятий

Основное внимание необходимо уделить регулярным обучающим мероприятиям, охватывающим всех сотрудников организации. Программы должны быть адаптированы под специфические потребности различных отделов и целевых групп. Фишинговые симуляции должны проводиться регулярно, чтобы отслеживать прогресс сотрудников и корректировать подходы к обучению. При наличии возможностей рекомендуется внедрить программу мотивации для сотрудников с целью дополнительного стимулирования обучения. Необходима оценка результатов проекта за год.



Каждый этап проекта будет сопровождаться регулярным мониторингом и оценкой ключевых показателей, что позволит гибко реагировать на изменчивые угрозы и оперативно корректировать программы обучения.

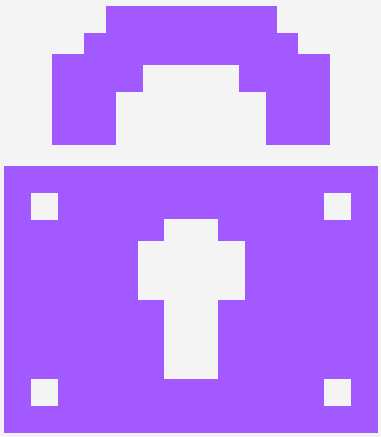
Сроки реализации проекта

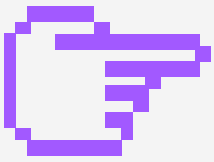
3. Четвертый год – оценка промежуточных результатов и корректировка программ

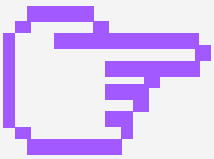
На этом этапе необходимо провести анализ результатов обучения, фишинговых симуляций, а также вовлеченности сотрудников. На основе собранных данных должны быть внесены необходимые изменения в обучающие программы и информационные кампании для достижения целей стратегии.

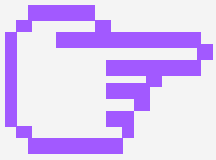
4. Пятый год – завершение проекта и оценка конечных результатов

Итоговый этап включает в себя подведение итогов всех мероприятий и заключение по программе реализации. На основе полученных результатов должен быть разработан план для продолжения и улучшения программы киберкультуры на будущее.









Основные цели

Основные цели стратегии ориентированы на развитие киберкультуры среди сотрудников всех целевых групп. В рамках реализации стратегии планируется добиться следующего:

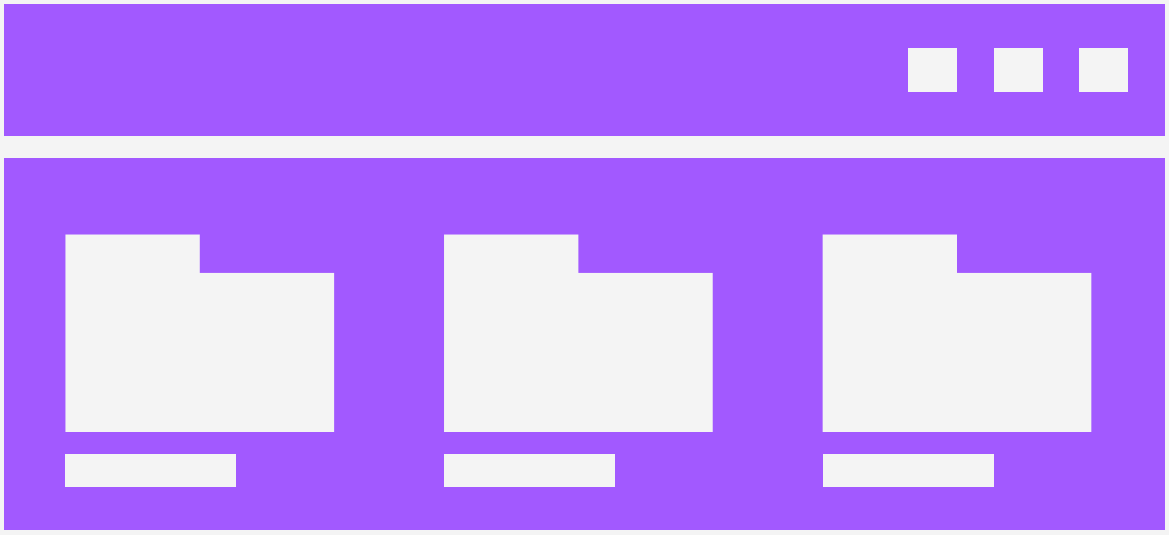
1. **Формирование культуры безопасного поведения в цифровом пространстве:** содействие внедрению и соблюдению практик безопасного поведения в цифровом пространстве, направленных на защиту данных и предотвращение инцидентов ИБ.

2. **Повышение доверия к отделу информационной безопасности:** создание открытой среды для взаимодействия между сотрудниками организации и отделом ИБ с целью повышения уровня доверия и дальнейшего сотрудничества.

3. **Предупреждение цифровых угроз:** активное обучение и информирование сотрудников о существующих типах цифровых угроз и способах их предотвращения с целью повышения уровня безопасности рабочего процесса.

4. **Снижение уязвимости организаций:** внедрение технологий и процессов для защиты данных, что будет способствовать снижению рисков и инцидентов ИБ.

5. **Развитие навыков реагирования на угрозы:** подготовка сотрудников к действиям в случае возникновения инцидентов, что позволит быстро и эффективно реагировать на угрозы.



Стратегия направлена на формирование киберкультуры, которая позволит всем сотрудникам осознавать существующие киберугрозы, действовать проактивно и защищаться от потенциальных рисков. Особое внимание уделяется различным категориям сотрудников, включая топ-менеджмент, технических специалистов и сотрудников без глубоких технических знаний. Каждая группа сталкивается с разными вызовами, и подход к обучению должен быть адаптирован для достижения максимальной эффективности.

Образовательные материалы:

Разработка и распространение материалов в различных форматах, включая статьи, инфографику, видеоролики и курсы. Эти материалы будут охватывать такие темы, как основы информационной безопасности, защита корпоративных данных, безопасное использование корпоративных систем, работа с личной информацией и другое.

Интерактивные мероприятия:

Проведение тренингов, вебинаров и киберсимуляций для сотрудников всех уровней. Использование элементов геймификации повысит уровень вовлеченности и улучшит усвоение информации. Фишинговые симуляции будут проводиться для выявления уязвимых участков и повышения осведомленности о реальных угрозах.

Обучение топ-менеджмента:

Специальные программы для руководителей, направленные на повышение их осведомлённости о стратегической важности киберкультуры и развитие навыков принятия решений в условиях киберугроз. Обучение будет включать практические занятия-тренинги со спикером и рассмотрение кейсов, основанных на реальных инцидентах, чтобы топ-менеджеры могли лучше понимать, как реагировать на кибератаки и защищать данные организации.

Обучение технических специалистов и специалистов ИБ:

Для технических специалистов будут проводиться углубленные курсы (обще-инфраструктурные аспекты безопасности, сетевая безопасность, безопасная архитектура, безопасная разработка др.) Специалисты ИБ проходят внешнее обучение, и важно обеспечить их непрерывное профессиональное развитие. Для технических специалистов будет проводиться внутренняя баг-баунти.

Обучение сотрудников без технической подготовки:

Для общей массы сотрудников будут разработаны адаптированные курсы, направленные на формирование базовых знаний по киберкультуре и безопасному использованию цифровых инструментов в повседневной работе. Особое внимание будет уделено предотвращению ошибок, связанных с человеческим фактором, таким как несанкционированное раскрытие информации или несоблюдение правил безопасности. Для сотрудников организаций, работающих с персональными данными, также будет включено обучение по 152-ФЗ "О персональных данных".

Кампании осведомленности:

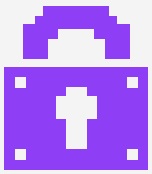
Регулярные кампании по повышению осведомленности сотрудников о киберугрозах через корпоративные информационные каналы и социальные сети. Включение симуляций кибератак (фишинговых писем) поможет сотрудникам научиться распознавать мошеннические действия и защищаться от них в реальных условиях.

Задачи

Создание информационных материалов по киберкультуре

Важной задачей является разработка и активное распространение информационных материалов внутри компании. Эти материалы будут включать рекомендации по обеспечению безопасности в сети и актуальную информацию о новых угрозах.

Обучение и просвещение сотрудников в области киберкультуры



Основной задачей является всестороннее обучение сотрудников, что включает в себя проведение информационных кампаний по современным киберугрозам и методам защиты. Важно, чтобы каждый сотрудник получил практические навыки и знания, необходимые для безопасного взаимодействия с цифровыми ресурсами и защиты личной информации.

Внедрение специализированной платформы для повышения осведомлённости

Для повышения уровня киберкультуры в организации будет внедрена специализированная платформа для повышения осведомленности сотрудников о киберугрозах и безопасном поведении в цифровой среде. Она будет использоваться для симуляции фишинговых атак, что поможет сотрудникам научиться распознавать и эффективно реагировать на киберугрозы, а также для внутреннего обучения. Платформа также будет собирать статистику по результатам обучения, позволяя оценивать эффективность программ и выявлять области, требующие внимания. Платформа позволит эффективно выполнять требования российских стандартов и законодательства, включая ФЗ-152, ФЗ-187, приказ ФСТЭК № 17, № 31, ГОСТ Р 57580.1-2017.

Разработка обучающих модулей и курсов для различных групп сотрудников

Внутри организации будут созданы обучающие модули и курсы, адаптированные под конкретные потребности различных категорий сотрудников — от новых работников до IT-специалистов. Курсы будут охватывать темы от основ информационной безопасности до продвинутых методов защиты данных и управления инцидентами. Также будут разработаны примеры фишинговых атак для повышения осведомленности о возможных угрозах.

Мониторинг и оценка эффективности программ по повышению киберкультуры

Для обеспечения эффективного выполнения программ будет осуществляться регулярный мониторинг их результатов. Это включает анализ данных о прохождении обучающих мероприятий, результаты тестирования на киберугрозы и проведение опросов среди сотрудников. Такой подход позволит своевременно вносить изменения в программы и обеспечивать их актуальность и эффективность.

Комплекс мероприятий (Топ-менеджеры)

Создание материалов по киберкультуре для повышения осведомленности среди топ-менеджеров

1. Создание информационных материалов для топ-менеджеров:
- Разработка специализированных инструкций, буклетов, материалов для соц.сетей, нацеленных на актуальные угрозы и защиту организации на стратегическом уровне. Материалы должны быть ориентированы на управленческую специфику и включать стратегические рекомендации по защите компании от киберугроз. Вместо стандартных инструкций можно предложить краткие, актуальные справки перед важными встречами или поездками, которые фокусируются на возможных киберугрозах и рекомендациях по защите компании в этих ситуациях. Необходимо включить инструкции по принятию управленческих решений в условиях кибератак, которые оказывают влияние на бизнес-процессы и репутацию:
- Регулярно обновлять информационные материалы для топ-менеджеров, отражающие актуальные угрозы и изменения в правовом регулировании.

Обучение и просвещение топ-менеджеров в области киберкультуры

1. Проведение интерактивных обучающих мероприятий:
- Проведение тренингов со спикером для топ-менеджеров с участием экспертов по киберкультуре, направленных на повышение осведомленности об актуальных угрозах, проведение киберритритов.
2. Разработка специализированной программы обучения по вопросам цифровой безопасности:
- Создание рекомендованной программы обучения для топ-менеджеров в формате тренинга, освещающего вопросы стратегического управления рисками и актуальные угрозы киберпространства. Также необходимо включить в программу обучения тематические кейсы, направленные на развитие навыков принятия решений в критических ситуациях.
3. Разработка регламентов обучения для топ-менеджеров (опционально):
- Разработка и утверждение регламента тренингов, включающего график обучения, сроки, цели и задачи, требования к участникам, контроль успеваемости, методы обучения, а также порядок документирования результатов. Регламент должен учитывать специфику деятельности организации. Регламент обучения может быть заменен на программу мотивации для топ-менеджеров.

Обучение и просвещение топ-менеджеров в области киберкультуры

4. Разработка приказов для топ-менеджеров (опционально):
- Издание приказа о проведении обучения топ-менеджеров в области киберкультуры. Приказ должен предусматривать обязательное участие топ-менеджеров в обучении по киберкультуре, а также назначать ответственных за проведение и контроль обучения. Это создаст правовую основу для обязательного прохождения курсов.
5. Распространение учебных материалов:
- Распространение учебных материалов (плакаты, инструкции, буклеты) на тему актуальных угроз и методов безопасного поведения в цифровом пространстве, доступных в электронном виде, включая телеграм-канал (или другой мессенджер), для топ-менеджеров организации.
6. Оценка уровня знаний топ-менеджеров с помощью тестов:
- Проведение тестирования после прохождения тренингов. Проведение оценочных тестов после каждого этапа тренинга для проверки усвоения материала позволит выявить пробелы в знаниях и адаптировать дальнейшее обучение под реальные потребности.

Разработка обучающих материалов для топ-менеджеров

1. Создание обучающих материалов для тренинга, соответствующих уровню подготовки и специфике работы топ-менеджмента:
- Разработка содержания тренинга, исходя из задач топ-менеджеров в организации. Учебные материалы должны быть адаптированы для аудитории высокого уровня с учётом её загруженности и ограниченного времени. Для лучшего восприятия информации материалы должны включать визуальные элементы, такие как инфографика, видеоматериалы с анализом успешных и провальных кейсов, а также таблицы и схемы, демонстрирующие роль топ-менеджмента в укреплении киберкультуры. Каждый модуль обучения должен заканчиваться тестированием, соответствующим специфике управленческих решений, а также опросом для получения обратной связи о качестве и применимости полученных знаний.
- Регулярное обновление материалов с учётом новых угроз и технологий, для сохранения актуальности.

Мониторинг и оценка эффективности программ повышения киберкультуры

1. Регулярный анализ данных о результатах обучающих мероприятий:
- Сбор и анализ отчетов по обучению топ-менеджеров;
- Проведение исследований для оценки уровня киберкультуры и выявления потребностей в дополнительном обучении.

Общий трек (сотрудники организации)

Создание информационных материалов по киберкультуре для сотрудников

1. Создание информационных материалов:
- Создание информационных материалов (плакаты, буклеты, инструкции), которые будут адаптированы для различных категорий сотрудников, на темы актуальных угроз и безопасного поведения в цифровом пространстве;
- Обеспечение регулярного обновления материалов для соответствия современным угрозам.

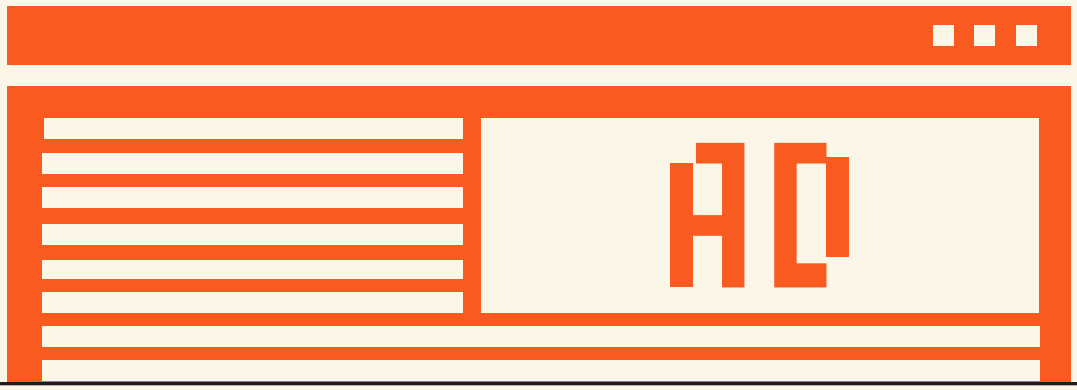
Обучение сотрудников организации в области киберкультуры

1. Проведение вебинаров для сотрудников:
- Проведение вебинаров-знакомств с отделом ИБ, а также вебинаров-тренингов по киберкультуре, направленных на повышение осведомленности об актуальных угрозах.
2. Разработка обучающих программ для сотрудников организаций:
- Создание специализированных рекомендованных программ обучения для сотрудников организаций с последующим прохождением по повышению осведомленности сотрудников в области информационной безопасности. Данный документ должен определять рекомендуемый порядок назначения учебных материалов для сотрудников организаций. Программа обучения должна разрабатываться на основе годового плана с разделением на кварталы.
3. Разработка регламентов обучения для сотрудников организаций:
- Разработка и утверждение регламента обучения сотрудников организаций, включающего график обучения, сроки, цели и задачи обучения, требования к участникам, контроль успеваемости, методы обучения, а также порядок документирования результатов. Регламент должен учитывать специфику деятельности организации.
4. Разработка приказов для сотрудников организаций:
- Издание приказа о проведении обязательного обучения сотрудников организаций в области киберкультуры. Приказ должен содержать перечень сотрудников, которым назначено обучение, сроки прохождения, а также ответственное лицо за организацию и контроль выполнения. Приказ является основанием для обязательного прохождения обучения и обеспечения его должного уровня.
5. Распространение учебных материалов:
- Распространение учебных материалов (плакаты, инструкции, буклеты) на тему актуальных угроз и методов безопасного поведения в цифровом пространстве, доступных в электронном виде для сотрудников организаций.

Общий трек (сотрудники организации)

Обучение сотрудников организации в области киберкультуры

6. Оценка уровня знаний сотрудников организаций с помощью тестов :
- Проведение тестирований на платформе по повышению осведомленности сотрудников в области информационной безопасности после прохождения теории в курсах для всех сотрудников организаций.



Внедрение платформы по повышению осведомлённости сотрудников в области информационной безопасности для имитации фишинговых атак, обучения, сбора статистики

1. Подготовка технической инфраструктуры для внедрения платформы в случае выбора on-premise версии;
2. Обеспечение доступа к платформе для сотрудников организации и предоставление поддержки в её использовании:
- Выдача доступов к платформе по повышению осведомленности сотрудников в области информационной безопасности организации;
- Организация технической поддержки и консультаций для администраторов платформы.
3. Обучение сотрудников работе с платформой:
- Передача инструкций по использованию платформы и проведение демонстраций её функционала для пользователей платформы.
4. Настройка и адаптация платформы под конкретные нужды организации:
- Брендирование платформы с учетом корпоративной символики;
- Интеграция с каталогами пользователей и настройка сквозной аутентификации;
5. Постоянное обновление и улучшение платформы на основе обратной связи от пользователей и изменений в киберугрозах.

Общий трек (сотрудники организации)

Разработка обучающих модулей, курсов и фишинговых шаблонов для различных групп сотрудников организаций

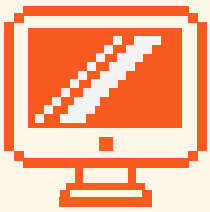
1. Создание обучающих материалов на платформе по повышению осведомленности сотрудников в области информационной безопасности, соответствующих уровню подготовки и специфике отделов:
- Разработка модульных и интерактивных курсов, адаптированных к разным уровням подготовки сотрудников, от начального до продвинутого, с учетом специфики организации, включая использование практик SANS и KnowBe4;
- Регулярное обновление учебных материалов с учётом новых угроз и технологий, чтобы они всегда оставались актуальными.
2. Внедрение системы геймификации для повышения вовлеченности участников:
- Создание учебных курсов, которые представляют собой игровые сценарии.
3. Разработка и реализация сценариев имитации фишинговых атак:
- Создание разнообразных сценариев фишинговых атак, адаптированных к различным отраслям и уровням сложности. С целью уведомления сотрудников ИБ о нахождении потенциально опасного письма необходимо внедрение плагина для пересылки фишинговых сообщений в отдел ИБ через почтовый клиент сотрудника;
- Включение реалистичных и современных примеров фишинговых атак, которые могут возникнуть в реальной жизни;
- Постоянное обновление сценариев атак в зависимости от новых видов угроз и изменений в методах фишинга.

Мониторинг и оценка эффективности программ повышения киберкультуры

1. Регулярный анализ данных о результатах обучающих мероприятий и фишинговых кампаний на платформе по повышению осведомлённости сотрудников в области информационной безопасности:
- Сбор и анализ отчетов по обучению сотрудников (определение процентного соотношения завершения курсов по теории и тестированию, выявление тем, которые вызывают затруднения у участников, оценка количества попыток на прохождение тестирования, времени на прохождение тестирования), фишинга (анализ результатов фишинговых кампаний для определения уровня уязвимости сотрудников к фишинговым атакам);
- Проведение исследований для оценки уровня киберкультуры и выявления потребностей в дополнительном обучении;
- Регулярное создание материалов, содержащих информацию об актуальных угрозах и методах, которые используют злоумышленники, для своевременного информирования об актуальных угрозах через платформу для повышения осведомленности.

Комплекс мероприятий (Сотрудники ИБ)

Разработка специализированных информационных материалов для специалистов ИБ



- Обеспечение регулярного обновления содержания материалов с учетом новых киберугроз (OWASP, NIST, SANS и др.), стандартов и законодательства (ISO/IEC 27001, GDPR, ФЗ 152, ФЗ 187 (банковский сектор) и др.).

Обучение и просвещение специалистов ИБ

1. Обеспечение участия сотрудников ИБ в отраслевых мероприятиях:
- Вовлечение сотрудников ИБ в мероприятия по киберкультуре. Специалисты ИБ должны выступать проводниками киберкультуры, активно участвуя в обучении и поддержке коллег. Их задача — демонстрировать важность безопасного поведения и вдохновлять других сотрудников на соблюдение лучших практик в области кибербезопасности.
- Сотрудники ИБ попадают под внешнее обучение, что требует предварительного планирования и включения соответствующих расходов в бюджет. В качестве обучающих программ могут выступать курсы от EC-Council, OffSec, SANS и других ведущих организаций. Дополнительно в процессе обучения могут применяться подходы и методики, рекомендованные NIST NICE и ENISA. Для специалистов этой области особенно важно поддерживать непрерывное развитие профессиональных навыков, включая участие в сертификационных курсах и тренингах, направленных на изучение актуальных тем в кибербезопасности. Это позволяет не только повысить квалификацию, но и быть готовыми к новым вызовам в условиях стремительно меняющихся угроз.
2. Разработка регламентов обучения для специалистов ИБ:
- Разработка и утверждение регламента обучения, специфичного для специалистов в области информационной безопасности. Регламент должен включать график обучения, сроки, цели и задачи, требования к участникам, методы оценки успеваемости и порядок документирования результатов. Учет специфики деятельности организации является обязательным для обеспечения соответствия требованиям ИБ.
3. Разработка приказов для специалистов ИБ:
- Издание приказа о проведении обучения в области киберкультуры и информационной безопасности. Приказ должен содержать список специалистов, подлежащих обучению, сроки прохождения и назначение ответственного лица за организацию и контроль выполнения. Данный приказ служит основанием для обязательного прохождения обучения и соблюдения стандартов безопасности.

Комплекс мероприятий (Сотрудники ИБ)

Обучение и просвещение специалистов ИБ

4. Сотрудники службы безопасности должны регулярно отрабатывать действия по реагированию на фишинговые атаки, направленные на компанию.
5. Распространение учебных материалов:

- Распространение специализированных учебных материалов (плакаты, инструкции, буклеты) на темы актуальных киберугроз и методов безопасного поведения в цифровом пространстве. Эти материалы должны быть доступны в электронном виде для сотрудников ИБ, а также могут быть размещены на официальных порталах компании и в мессенджерах.

6. Проведение опросов среди специалистов ИБ для получения обратной связи и выявления текущих знаний и привычек в области киберкультуры, что позволит корректировать подходы к обучению.

Внедрение платформы по повышению осведомленности сотрудников в области информационной безопасности для имитации фишинговых атак, сбора статистики

1. Подготовка технической инфраструктуры для внедрения платформы в случае выбора on-premise версии.
2. Обеспечение доступа к платформе для специалистов ИБ организации, и предоставление поддержки в её использовании:

- Выдача доступов к платформе по повышению осведомленности сотрудникам в области информационной безопасности;
- Организация технической поддержки и консультаций для администраторов платформы.

3. Обучение специалистов работе с платформой:

- Передача инструкций по использованию платформы и демонстрация её функционала.

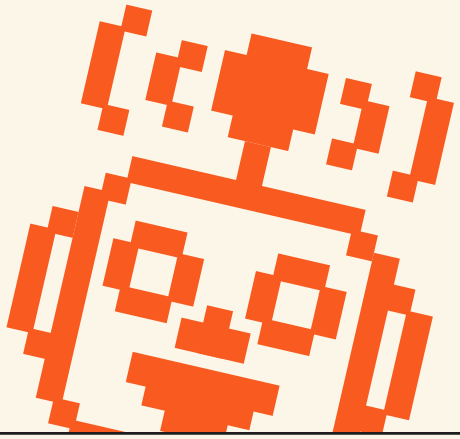
4. Настройка и адаптация платформы под конкретные нужды организации;

- Брендирование платформы с учетом корпоративной символики;
- Интеграция с каталогами пользователей и настройка сквозной аутентификации;
- Постоянное обновление и улучшение платформы на основе обратной связи от пользователей и изменений в киберугрозах.

Комплекс мероприятий (Сотрудники ИБ)

Разработка обучающих фишинговых шаблонов для специалистов ИБ

1. Разработка и реализация сценариев имитации фишинговых атак:
- Создание разнообразных сценариев фишинговых атак, ориентированных на различные отрасли и уровни сложности, с целью оценки готовности специалистов ИБ к реагированию на реальные угрозы.
- Включение реалистичных и актуальных примеров фишинговых атак, соответствующих современным трендам и методам, применяемым злоумышленниками в реальной жизни, для повышения уровня осведомленности и подготовки сотрудников. Для специалистов по информационной безопасности используется плагин, позволяющий пересылать фишинговые сообщения для проведения учебных мероприятий внутри отдела.
- Постоянное обновление сценариев атак с учетом новых видов угроз, изменений в методах фишинга и аналитических данных о текущих атаках, что позволяет поддерживать актуальность и эффективность тренировок.



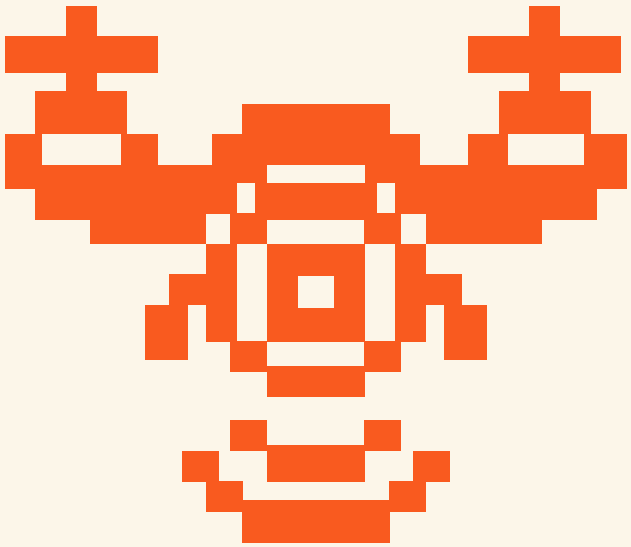
Мониторинг и оценка эффективности программ повышения киберкультуры

1. Регулярный анализ данных о результатах обучающих мероприятий и фишинговых кампаний:
- Сбор и анализ отчетов по обучению специалистов ИБ, анализ результатов фишинговых кампаний для определения уровня уязвимости сотрудников к фишинговым атакам, что позволяет выявить слабые места и скорректировать процессы обучения;
- Проведение исследований для оценки уровня киберкультуры и выявления потребностей в дополнительном обучении.

Комплекс мероприятий (Технические специалисты)

Создание информационных материалов и организация мероприятий для повышения киберкультуры среди технических специалистов

1. Создание информационных материалов для технических специалистов:
- Подготовка образовательных материалов с акцентом на актуальные угрозы для бизнеса и новые методы защиты. Форматы включают плакаты, чек-листы, инструкции и буклеты;
- Регулярное обновление материалов, чтобы они отражали современные угрозы и методы защиты в области кибербезопасности.



Обучение и просвещение технических специалистов в области киберкультуры

1. Проведение мероприятий для технических специалистов:
- Проведение внутренних форумов по вопросам IT и ИБ, организация площадок для внутренних докладов по ИБ. Создание форумов и докладов позволит техническим специалистам компании обмениваться опытом, обсуждать новые угрозы и лучшие практики в области информационной безопасности;
- Проведение внутренних баг-баунти. Внутренние баг-баунти программы будут стимулировать сотрудников к поиску уязвимостей в инфраструктуре компании, что будет способствовать выявлению и устранению слабых мест до того, как ими воспользуются злоумышленники. Для организации внутренней программы баг-баунти требуется разработать документацию, регламентирующую порядок сдачи найденных уязвимостей и вознаграждения сотрудников за их сдачу;
- Проведение тренингов и открытых заданий CTF. Тренинги и соревнования в формате CTF (Capture the Flag) развивают практические навыки сотрудников в области кибербезопасности, позволяя им лучше подготовиться к реальным атакам.

Обучение и просвещение технических специалистов в области киберкультуры

2. Разработка обучающих программ для технических специалистов:
- Формирование программ обучения с учетом уровня подготовки и задач компании, с обучением на платформе по повышению осведомленности сотрудников в области информационной безопасности, разработка поэтапного плана для освоения теоретических и практических аспектов кибербезопасности. Программа должна включать обучение по безопасной разработке и основам уязвимостей.
3. Разработка регламентов обучения технических специалистов:
- Утверждение регламентов с графиком обучения, контрольными точками, методами тестирования и документирования результатов, учитывая специфику работы технических специалистов.
4. Оформление приказов об обязательном обучении:
- Издание приказов для обязательного обучения технических специалистов, указание сроков, перечня тем и ответственных лиц. Данный приказ служит основанием для обязательного прохождения обучения и соблюдения стандартов безопасности.
5. Распространение учебных материалов:
- Распространение специализированных учебных материалов (плакаты, инструкции, буклеты) на темы актуальных киберугроз и методов безопасного поведения в цифровом пространстве. Эти материалы должны быть доступны в электронном виде для тех.специалистов, а также могут быть размещены на официальных порталах компании и в мессенджерах.
6. Оценка уровня знаний технических сотрудников организаций с помощью тестов:
- Проведение тестирования на платформе по повышению осведомленности сотрудников в области информационной безопасности для оценки знаний специалистов после завершения теоретических курсов по киберкультуре;
- Проведение опросов среди технических специалистов для получения обратной связи и выявления текущих знаний и привычек в области киберкультуры, что позволит корректировать подходы к обучению.

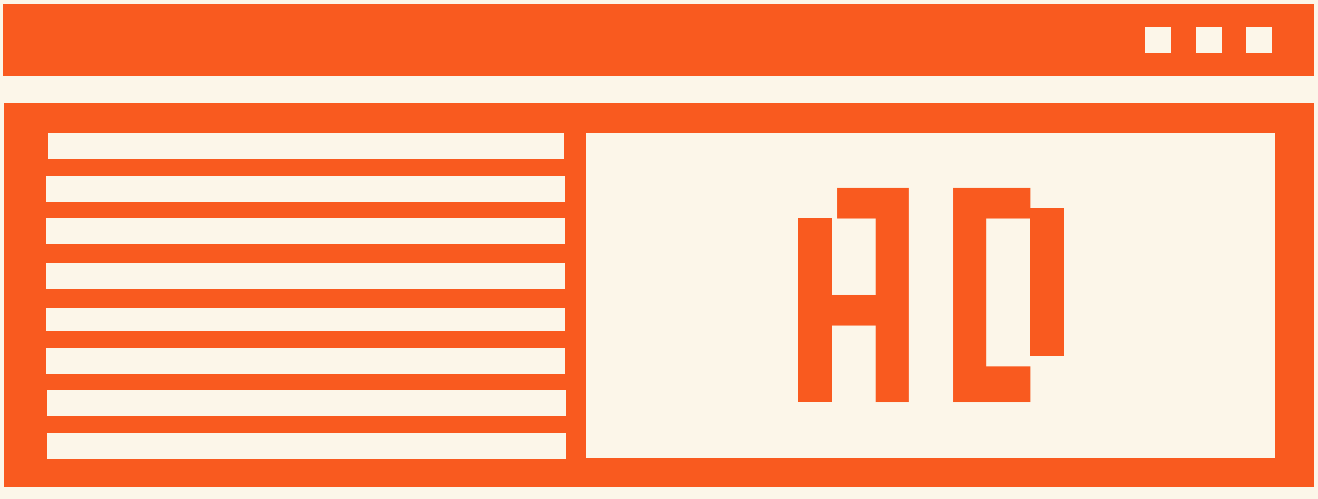
Внедрение платформы по повышению осведомленности сотрудников в области информационной безопасности для имитации фишинговых атак, обучения и сбора статистики

Обеспечение доступа к платформе и технической поддержки:
1. Предоставление доступа к курсам по безопасной разработке.
2. Обучение сотрудников работе с платформой:
- Проведение инструктажей и обучающих сессий по работе с функциями платформы.
3. Настройка и адаптация платформы под задачи компании:
- Брендирование платформы;
- Интеграция с каталогами пользователей и настройка сквозной аутентификации.

Комплекс мероприятий (Технические специалисты)

Разработка обучающих модулей и фишинговых сценариев для технических специалистов

1. Создание специализированных учебных курсов:
- Разработка интерактивных курсов и тестов, ориентированных на текущие и специфические угрозы для технических специалистов, с учётом разных уровней их подготовки и потребностей в навыках противодействия кибератакам. Для специалистов ИТ необходимы курсы по общим инфраструктурным аспектам безопасности, сетевой безопасности, разделении ролей, хранения данных и др. Для разработчиков - по безопасной архитектуре, безопасной разработке, хранению данных и др.
- Обучение должно также включать курсы по безопасной разработке и использование практик SANS и KnowBe4.
2. Внедрение системы геймификации:
- Создание учебных курсов в формате игровых сценариев, которые повышают интерес и мотивацию технических специалистов к обучению, помогая эффективнее усваивать материал.
3. Разработка и обновление сценариев имитации фишинговых атак:
- Включение реалистичных и актуальных примеров фишинговых атак, соответствующих современным трендам и методам, применяемым злоумышленниками в реальной жизни, для повышения уровня осведомлённости и подготовки сотрудников, учитывая специфику работы технических специалистов. Для уведомления сотрудников ИБ о потенциально опасном письме, необходимо внедрить плагин. Этот плагин будет пересылать фишинговые сообщения в отдел ИБ через почтовый клиент сотрудника.
- Постоянное обновление сценариев атак с учётом новых видов угроз, изменений в методах фишинга и аналитических данных о текущих атаках, что позволяет поддерживать актуальность и эффективность тренировок.



Комплекс мероприятий (Технические специалисты)

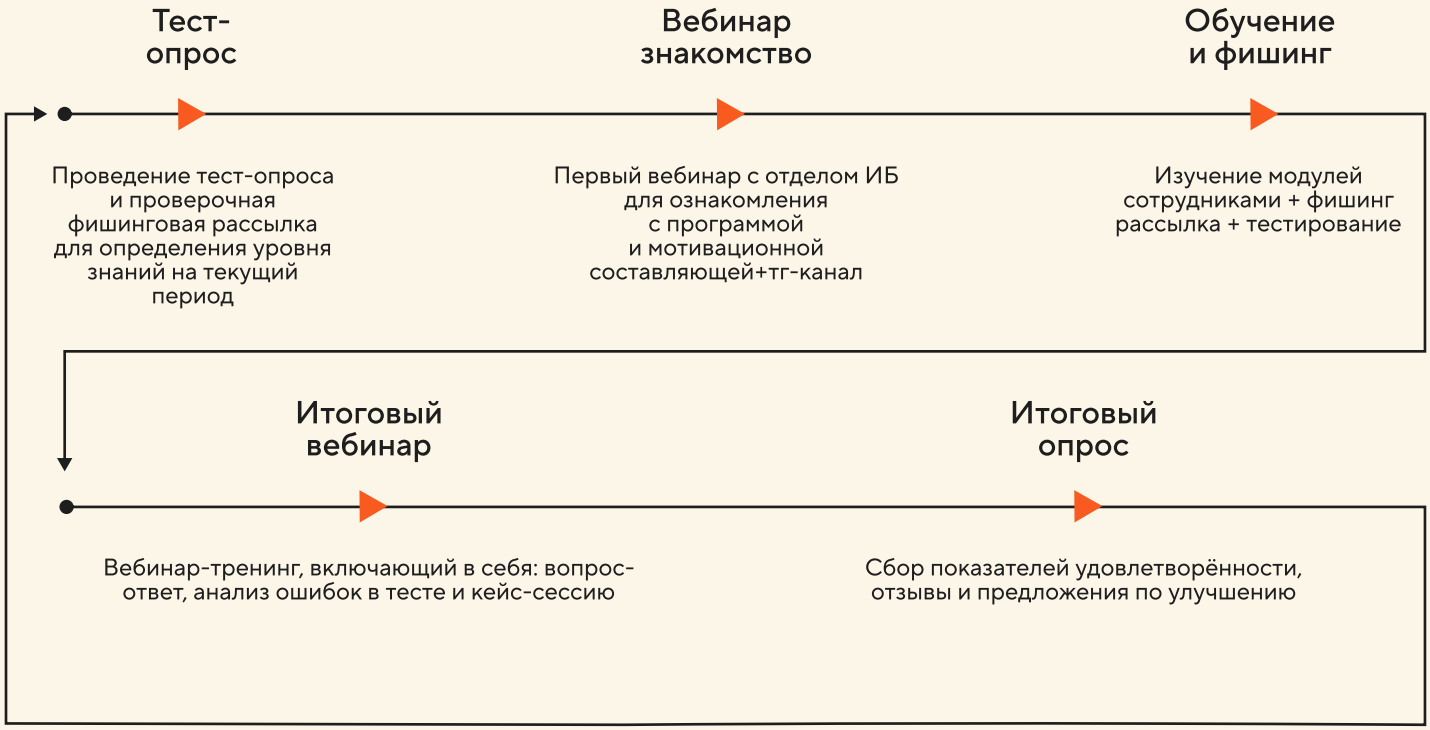
Мониторинг и оценка эффективности киберпрограмм

1. Анализ данных обучающих мероприятий и фишинговых кампаний:
- Проведение детального анализа результатов курсов и фишинговых симуляций, выявление тем и навыков, требующих дополнительных тренировок, анализ времени прохождения тестов для понимания уровня подготовки специалистов.
2. Исследования для оценки уровня киберкультуры:
- Проведение опросов и исследований для определения уровня осведомлённости специалистов, выявление пробелов в навыках и планирование дополнительных обучающих мероприятий для улучшения киберграмотности.

Трек обучения сотрудников

Топ-менеджеры

Общий трек



Трек обучения сотрудников

Специалисты ИБ

Обучение
Непрерывное обучение специалистов ИБ, включая использование методик NIST NICE, ENISA

Фишинг
Углублённые тренинги по предотвращению атак и анализ ошибок

Отраслевые мероприятия
Вовлечение сотрудников ИБ в мероприятия по киберкультуре

Коммуникация
Телеграм-канал или другой мессенджер

Технический трек

Обучение и фишинг
Обучение по безопасной разработке и основам уязвимости, фишинг рассылка

Внутренние мероприятия
Площадки для внутренних докладов по ИБ, форумы по вопросам IT и ИБ

Тренинг
Участие в тренингах и открытых заданиях CTF

Внутренняя баг-баунти
Участие в программе поиска и устранения уязвимостей в системах

Коммуникация
Телеграм-канал или другой мессенджер

Метрики

Для эффективного управления киберкультурой среди целевых групп важно иметь четкое представление о том, как данные группы воспринимают и применяют полученные знания и навыки. Были выделены ключевые метрики, которые помогут оценить уровень подготовки и вовлеченности целевых групп в области киберкультуры:

1. Метрики для топ-менеджеров

1.1 Метрики знаний:

- результаты тестов.

1.2 Метрики удовлетворенности:

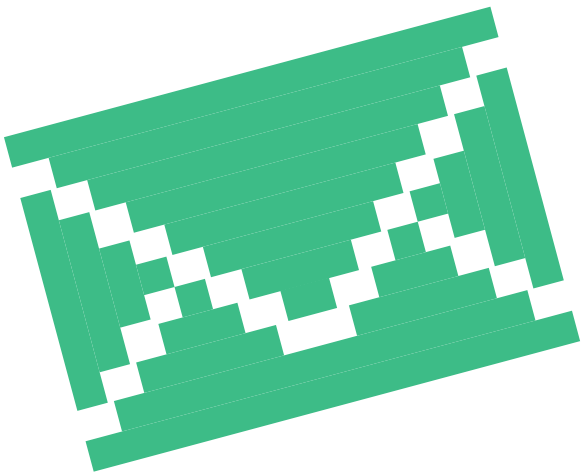
- оценка уровня удовлетворённости топ-менеджеров тренингами по киберкультуре.

1.3 Метрика вовлеченности:

- процент менеджеров, прошедших тренинги.

1.4 Метрика успешности информационных материалов:

- количество скачиваний или просмотров размещённых материалов. Периодичность отслеживания метрик — раз в квартал. Периодичность обучения — раз в квартал.



2. Метрики для сотрудников компании (общий трек)

2.1. Метрики знаний:

- количество назначенных курсов;
- прогресс обучения;
- результаты тестов;
- количество сотрудников, прошедших курс.

2.2 Метрики поведения:

- количество проведённых атак;
- количество отправленных писем;
- количество открытий писем;
- количество переходов по ссылке;
- количество ввода личных данных;
- количество открытий вложений;
- процент сотрудников, попавшихся на фишинг;
- индекс изменения поведения (снижение инцидентов безопасности, вызванных человеческим фактором).

2.3 Метрика уязвимости сотрудника компании:

- уровень риска сотрудника компании;
- процент обновленных и актуальных рабочих устройств;
- процент инцидентов с зараженными компьютерами (уточняется через службу поддержки);
- случаи потери данных сотрудниками (уточняется через стандартные процессы отслеживания отчетов об инцидентах);
- нарушения политики безопасности сотрудниками компании.

2.4 Метрики удовлетворенности:

- оценка уровня удовлетворённости сотрудников компании курсами по киберкультуре с помощью опросов. Опросы добавляются в состав курсов, и размещаются в конце тестирования.

2.5 Метрика осведомленности:

- оценка уровня осведомлённости сотрудников о новых типах киберугроз и атаках, возникающих в цифровом пространстве через опросы;
- количество сотрудников, использующих надежные пароли (уточняется через специализированные решения)

2.6 Метрика вовлеченности:

- процент сотрудников, прошедших курсы;
- процент сотрудников, посетивших вебинары;
- процент сотрудников, посетивших очные встречи;
- количество обращений в службу ИБ за советами по кибербезопасности.

2.7 Метрика успешности информационных материалов:

- количество скачиваний или просмотров размещённых материалов;
- количество подписанных на канал.

2.8 Метрики плагина для почты:

- количество пересланных тренировочных писем;
- количество обнаруженных пользователями фишинговых атак;
- количество обнаруженных пользователями реальных фишинговых атак.

Для оценки эффективности обучения и вовлечённости сотрудников будут проводиться регулярные опросы, позволяющие измерить удовлетворённость курсами по киберкультуре и выявить области, требующие улучшений. Все данные будут анализироваться для разработки дальнейших шагов по снижению киберрисков и повышения киберграмотности сотрудников. Периодичность отслеживания метрик — раз в квартал.

Периодичность обучения сотрудников — раз в квартал. Организация должна проводить минимум одну имитацию в месяц, охватывающую минимум 80 % сотрудников. Перед организацией будут поставлены задачи по киберучениям, что является цикличным процессом с указанием и профилированием групп организаций.

Метрики

3. Метрики для специалистов ИБ:

3.1. Метрики знаний:

- количество назначенных курсов;
- прогресс обучения;
- результаты тестов;
- количество специалистов ИБ, прошедших курс.

3.2 Метрики поведения:

- количество проведённых атак;
- количество отправленных писем;
- количество открытий писем;
- количество переходов по ссылке;
- количество ввода личных данных;
- количество открытий вложений;
- процент специалистов ИБ, попавшихся на фишинг;
- время обнаружения инцидента;
- время обнаружения учебного инцидента.

3.3 Метрика уязвимости специалиста ИБ:

- уровень риска специалиста ИБ.

3.4 Метрики удовлетворенности:

- оценка уровня удовлетворённости специалистов ИБ курсами по киберкультуре с помощью опросов.

3.5 Метрика осведомленности:

- оценка уровня осведомлённости специалистов ИБ о новых типах киберугроз и атаках, возникающих в цифровом пространстве, через опросы.

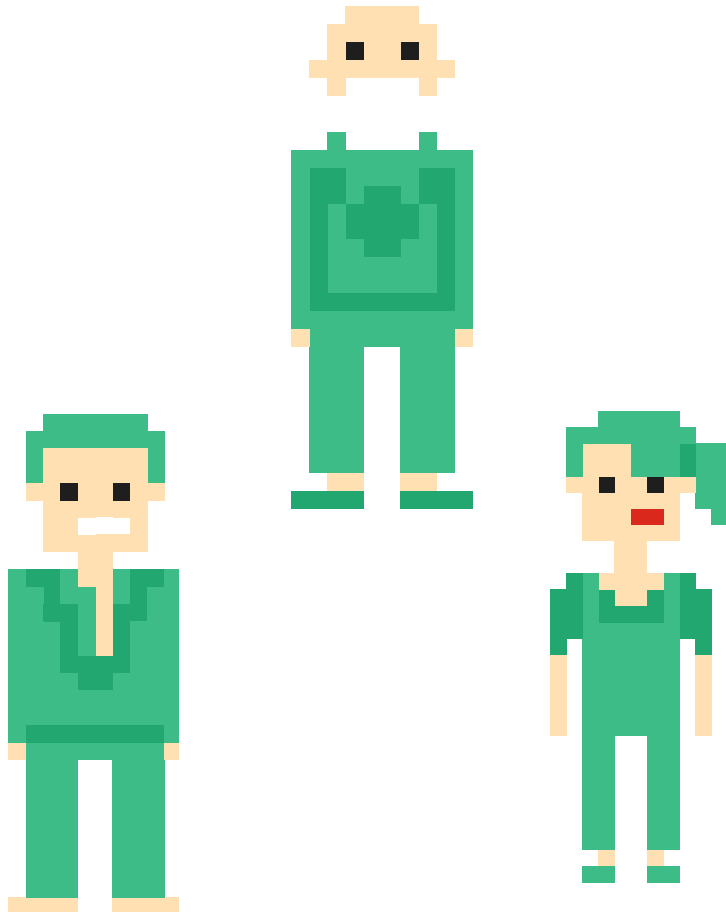
3.6 Метрика вовлеченности:

- процент специалистов ИБ, прошедших курсы;
- процент специалистов ИБ, посетивших вебинары;
- процент специалистов ИБ, посетивших очные встречи.

3.7 Метрика успешности информационных материалов:

- количество скачиваний или просмотров размещённых материалов;
- количество подписанных на канал.

Периодичность отслеживания метрик — раз в квартал. Периодичность обучения — раз в квартал. Организация должна провести раз в месяц минимум одну имитацию, охватывающую минимум 80 % специалистов ИБ. Перед организацией будут поставлены задачи по киберучениям, что является цикличным процессом с указанием и профилированием групп организаций.



Метрики

4. Метрики для технических специалистов:

4.1. Метрики знаний:
- количество назначенных курсов;
- прогресс обучения;
- результаты тестов;
- количество технических специалистов, прошедших курс.

4.2 Метрики поведения:
- количество проведенных атак;
- количество отправленных писем;
- количество открытий писем;
- количество переходов по ссылке;
- количество ввода личных данных;
- количество открытий вложений;
- процент специалистов, попавшихся на фишинг;
- индекс изменения поведения (снижение инцидентов безопасности, вызванных человеческим фактором).

4.3 Метрика уязвимости технического специалиста:
- уровень риска технического специалиста.

4.4 Метрики удовлетворенности:
- оценка уровня удовлетворённости технических специалистов курсами по киберкультуре с помощью опросов, которые добавляются в состав курсов и размещаются в конце тестирования.

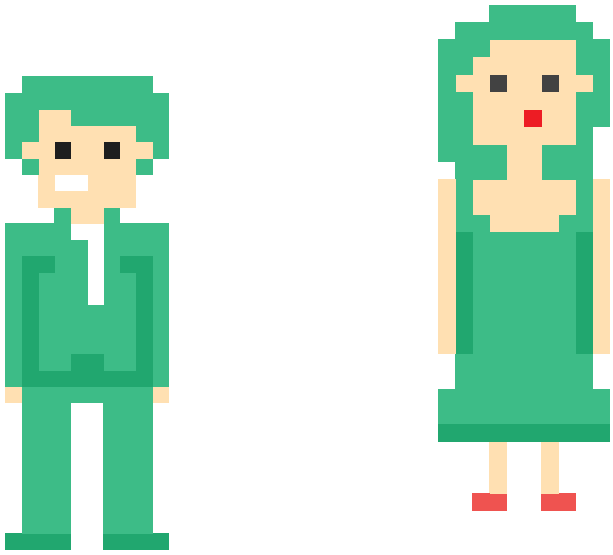
4.5 Метрика осведомленности:
- оценка уровня осведомлённости технических специалистов о новых типах киберугроз и атаках, возникающих в цифровом пространстве, через опросы.

4.6 Метрика вовлеченности:
- процент технических специалистов, прошедших курсы;
- процент технических специалистов, посетивших вебинары;
- процент технических специалистов, посетивших очные встречи;
- процент технических специалистов, принявших участие в баг-баунти;
- количество обращений в службу ИБ за советами.

4.7 Метрика успешности информационных материалов:
- количество скачиваний или просмотров размещённых материалов;
- количество подписанных на канал.

4.8 Метрики плагина для почты:
- количество пересланных тренировочных писем;
- количество обнаруженных пользователями фишинговых атак.

Периодичность отслеживания метрик — раз в квартал. Периодичность обучения — раз в квартал. Организация должна провести раз в месяц минимум одну имитацию, охватывающую минимум 80 % технических специалистов.



Критерии успеха

Критерии успеха являются важными показателями, которые позволяют оценить, достигнуты ли цели программы повышения киберкультуры в организации. На основании заранее установленных метрик критерии успеха служат ориентиром для оценки эффективности обучающих программ, информационных кампаний и внедрения платформы для повышения киберосведомленности. Эти критерии позволяют измерить результативность мероприятий и вовлечённость целевых групп, а также помогают определить, насколько успешно участники применяют полученные знания и навыки в области киберкультуры. Данные критерии служат индикативным значением, и в каждой организации может быть установлен свой собственный порог.

1. Критерии для топ-менеджеров:

1.1 Критерии знаний:

- результаты тестов: средний балл по тестам выше 80 % у 90 % топ-менеджеров.

1.2 Критерий удовлетворенности:

- уровень удовлетворённости топ-менеджеров тренингами по киберкультуре: уровень удовлетворенности выше 85 % по итогам опросов.

1.3 Критерий вовлеченности:

- процент менеджеров, прошедших тренинги: 90 % топ-менеджеров прошли обучение в запланированный период.

1.4 Критерий успешности информационных материалов:

- количество скачиваний или просмотров размещённых материалов: минимум 60 % топ-менеджеров ознакомились с материалами;
- количество подписанных на канал: минимум 60 % топ-менеджеров подписаны на канал.

2. Критерии для сотрудников компании (общий трек):

2.1. Критерии знаний:

- прогресс обучения: не менее 70 % сотрудников успешно завершили образовательные курсы по киберкультуре в установленные сроки;
- результаты тестов: минимум 70 % сотрудников сдают итоговые тесты с результатом выше 85 %;
- количество назначенных курсов: назначено 99 % необходимых курсов всем сотрудникам;
- количество сотрудников, прошедших курс: успешное прохождение курсов минимум 85 % сотрудников.

2.2 Критерии поведения:

- количество проведённых атак: проведено минимум 3 имитированных атаки в течение квартала;
- количество переходов по ссылке: менее 30 % сотрудников переходят по ссылкам в фишинговых письмах, что демонстрирует повышение уровня киберкультуры.

Критерии успеха

2. Критерии для сотрудников компании (общий трек):

- количество ввода личных данных: менее 20 % сотрудников вводят свои личные данные в фишинговые формы;
- количество открытий вложений: не более 30 % сотрудников открывают потенциально опасные вложения в электронных письмах;
- процент сотрудников, попавшихся на фишинг: менее 7 % сотрудников попадаются на фишинг;
- индекс изменения поведения (снижение инцидентов безопасности, вызванных человеческим фактором): снижение числа инцидентов в организациях на 30 %.

2.3 Критерий уязвимости сотрудника компании:

- уровень риска сотрудника компании: количество сотрудников с высоким уровнем риска снизилось на 50 %;
- процент обновленных и актуальных рабочих устройств поддерживается на уровне не менее 95 % от общего числа;
- процент инцидентов с зараженными компьютерами: уровень заражения рабочих устройств не превышает 2 % от общего числа;
- случаи потери данных сотрудниками: количество случаев потери данных сотрудниками сокращено на 10 %;
- нарушения политики безопасности сотрудниками компании: количество нарушений политики безопасности сокращено на 50 %.

2.4 Критерий удовлетворенности:

- оценка уровня удовлетворённости сотрудников компании курсами по киберкультуре с помощью опросов: если более 75 % сотрудников положительно оценивают курсы по результатам опросов, программа считается успешной.

2.5 Критерий осведомленности:

- оценка уровня осведомлённости сотрудников о новых типах киберугроз и атаках, возникающих в цифровом пространстве, через опросы: не менее 75 % сотрудников демонстрируют высокий уровень осведомлённости о новых киберугрозах, согласно результатам опросов;
- не менее 85 % сотрудников используют надежные пароли, которые соответствуют установленным требованиям безопасности внутри организации.

2.6 Критерий вовлеченности:

- процент сотрудников, прошедших курсы: минимум 85 % сотрудников завершили все назначенные курсы;
- процент сотрудников, посетивших вебинары: минимум 30 % сотрудников посетили вебинары;
- процент сотрудников, посетивших очные встречи: минимум 30% приняли участие в очных встречах;
- количество обращений в службу ИБ за советами увеличилось после внедрения программы.

Критерии успеха

2. Критерии для сотрудников компании (общий трек):

2.7 Критерий успешности информационных материалов:

- количество скачиваний или просмотров размещённых материалов: 25 % материалов просмотрено или скачано;
- количество подписанных на канал: 25 % сотрудников подписаны на внутренний канал.

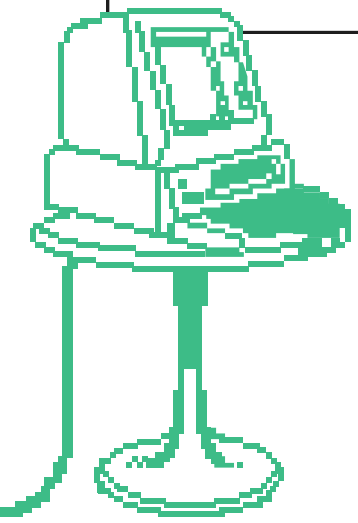
2.8 Критерий плагина для почты:

- количество пересланных тренировочных писем: 50 % сотрудников пересылают тренировочные письма (когда используют плагин);
- количество пересланных фишинговых писем: 80 % сотрудников пересылают реальные письма;
- количество обнаруженных пользователями фишинговых атак: 80 % фишинговых атак обнаружено пользователями.

3. Критерии для специалистов ИБ:

3.1. Критерии знаний:

- прогресс обучения: не менее 85 % специалистов ИБ успешно завершили образовательные курсы по киберкультуре в установленные сроки;
- результаты тестов: минимум 85 % специалистов ИБ сдают итоговые тесты с результатом выше 85 %;
- количество назначенных курсов: назначено 99 % необходимых курсов всем специалистам ИБ;
- количество специалистов ИБ, прошедших курс: успешное прохождение курсов минимум 85 % специалистами.



3. Критерии для специалистов ИБ:

3.2 Критерии поведения:

- количество проведённых атак: проведено минимум 3 имитированных атаки в течение квартала;
- количество переходов по ссылке: менее 10 % специалистов переходят по ссылкам в фишинговых письмах;
- количество ввода личных данных: менее 5 % специалистов вводят свои личные данные в фишинговые формы;
- количество открытий вложений: не более 5 % специалистов ИБ открывают потенциально опасные вложения в электронных письмах;
- процент специалистов ИБ, попавшихся на фишинг: менее 3 % специалистов попадаются на фишинг;
- среднее время обнаружения инцидента составляет 15-30 минут;
- среднее время обработки учебного инцидента улучшилось на 10 % или соответствует внутреннему регламенту по обнаружения.

3.3 Критерии уязвимости специалиста ИБ:

- уровень риска специалиста ИБ: меньше или равен 5.

3.4 Критерии удовлетворенности:

- оценка уровня удовлетворённости специалистов ИБ курсами по киберкультуре с помощью опросов: более 85 % специалистов положительно оценивают курсы по результатам опросов, программа считается успешной.

3.5 Критерии осведомленности:

- оценка уровня осведомлённости специалистов ИБ о новых типах киберугроз и атаках, возникающих в цифровом пространстве, через опросы: не менее 85 % специалистов демонстрируют высокий уровень осведомлённости о новых киберугрозах согласно результатам опросов.

3.6 Критерии вовлеченности:

- процент специалистов ИБ, прошедших курсы: минимум 85 % специалистов завершили все назначенные курсы;
- процент специалистов ИБ, посетивших вебинары: минимум 85 % специалистов посетили вебинары;
- процент специалистов ИБ, посетивших очные встречи: минимум 85 % специалистов приняли участие в очных встречах.

3.7 Критерии успешности информационных материалов:

- количество скачиваний или просмотров размещённых материалов: 85 % материалов просмотрено или скачано;
- количество подписанных на канал: 85 % специалистов ИБ подписаны на внутренний канал.

Критерии успеха

4. Критерии для технических специалистов

4.1. Критерии знаний:

- прогресс обучения: не менее 80 % специалистов успешно завершили образовательные курсы по киберкультуре в установленные сроки;
- результаты тестов: минимум 80 % сотрудников сдают итоговые тесты с результатом выше 80 %;
- количество назначенных курсов: назначено 99 % необходимых курсов всем сотрудникам;
- количество технических специалистов, прошедших курс: успешное прохождение курсов минимум 80 % сотрудников.

4.2 Критерии поведения:

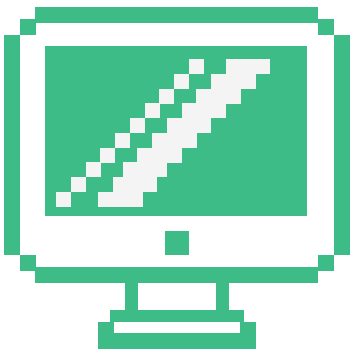
- количество проведённых атак: проведено минимум 3 имитированных атаки в течение квартала;
- количество переходов по ссылке: менее 15 % специалистов переходят по ссылкам в фишинговых письмах;
- количество ввода личных данных: менее 10 % специалистов вводят свои личные данные в фишинговые формы;
- количество открытий вложений: не более 10 % специалистов открывают потенциально опасные вложения в электронных письмах;
- процент специалистов, попавшихся на фишинг: менее 15 % специалистов попадаются на фишинг;
- индекс изменения поведения (снижение инцидентов безопасности, вызванных человеческим фактором): снижение числа инцидентов на 30 %.

4.3 Критерии уязвимости технического специалиста:

- уровень риска технического специалиста: меньше или равен 6.

4.4 Критерии удовлетворенности:

- оценка уровня удовлетворённости технических специалистов курсами по киберкультуре с помощью опросов: более 85 % специалистов положительно оценивают курсы по результатам опросов, программа считается успешной.



Критерии успеха

4. Критерии для технических специалистов

4.5 Критерии осведомленности:

- оценка уровня осведомлённости технических специалистов о новых типах киберугроз и атаках, возникающих в цифровом пространстве, через опросы: не менее 80 % специалистов демонстрируют высокий уровень осведомлённости о новых киберугрозах, согласно результатам опросов.

4.6 Критерии вовлеченности:

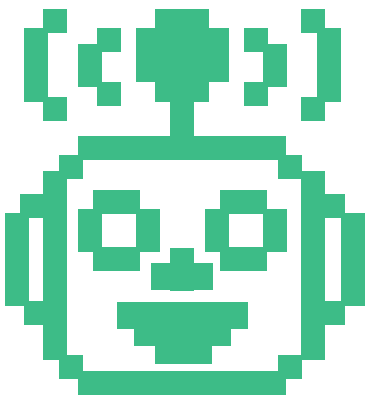
- процент технических специалистов, прошедших курсы: минимум 80 % специалистов завершили все назначенные курсы;
- процент технических специалистов, посетивших вебинары: минимум 80 % специалистов посетили вебинары;
- процент технических специалистов, посетивших очные встречи: минимум 85 % специалистов приняли участие в очных встречах;
- процент технических специалистов, принявших участие в баг-баунти: минимум 50 % специалистов приняли участие в очных встречах;
- количество обращений в службу ИБ за советами: увеличилось после внедрения программы.

4.7 Критерии успешности информационных материалов:

- количество скачиваний или просмотров размещённых материалов: 50 % материалов просмотрено или скачано;
- количество подписанных на канал: 50 % технических специалистов подписаны на внутренний канал.

4.8 Критерии плагина для почты:

- количество пересланных тренировочных писем: 70 % специалистов пересылают тренировочные письма (когда используют плагин);
- количество обнаруженных пользователями фишинговых атак: 80 % фишинговых атак обнаружено пользователями.



Риски и вызовы

Реализация стратегии киберкультуры для организации может столкнуться с рядом рисков и вызовов, которые могут повлиять на её успешное внедрение и достижение целей. В условиях быстрого развития цифровых технологий и увеличения числа кибератак важно учитывать потенциальные препятствия, которые могут замедлить создание безопасной цифровой среды внутри компании.

Риски	Пояснения
Сопротивление изменениям	Внедрение стратегии может вызвать сопротивление со стороны некоторых сотрудников, особенно если обучение воспринимается как дополнительная нагрузка. Также возможен скептицизм по поводу необходимости изменения устоявшихся рабочих процессов, что может затормозить внедрение новых практик и подходов.
Низкая защищённость цифровой инфраструктуры	Устаревшие или недостаточно защищённые IT-системы компании могут стать лёгкой мишенью для кибератак. Это может подорвать доверие сотрудников к используемым системам и инструментам, а также снизить их желание участвовать в программах по киберкультуре.
Негативное восприятие киберкультуры	Некоторые сотрудники могут воспринимать меры по повышению уровня киберкультуры как вмешательство в их привычный образ работы или даже в личную жизнь, что может вызвать недовольство и снизить активность участия в обучающих мероприятиях.
Быстрое изменение киберугроз	Киберугрозы постоянно эволюционируют, и методы атак становятся всё более сложными. Стратегия должна предусматривать возможность быстрого обновления образовательных материалов и подходов к обучению. Если организация не будет оперативно реагировать на новые угрозы, программы могут устареть и стать менее эффективными.

Риски и вызовы

Риски	Пояснения
Недостаточная поддержка со стороны руководства	Если руководство организации не будет демонстрировать приверженность киберкультуре или не поддержит инициативы по её продвижению, это может снизить мотивацию сотрудников участвовать в программах обучения. Успех стратегии во многом зависит от активной поддержки высшего руководства и примера, который оно подаёт.
Ограниченные ресурсы на внедрение программы	Недостаточное финансирование, нехватка специалистов или времени на реализацию стратегии могут замедлить её успешное внедрение. Для эффективного обучения и повышения осведомлённости сотрудников необходимы инвестиции в инструменты, платформы и профессиональные кадры, способные поддерживать актуальность программы.

Литература

1. Утечки информации в мире, 2022-2023 годы: https://www.infowatch.ru/sites/default/files/analytics/files/issledovaniye-utechek-informatsii-v-mire-za-2022-2023-gody.pdf

2. Fortinet Report Finds Nearly 70% of Organizations Say Their Employees Lack Fundamental Security Awareness: https://investor.fortinet.com/news-releases/news-release-details/fortinet-report-finds-nearly-70-organizations-say-their/

3. Современные подходы к защите информации, методы, средства и инструменты защиты: https://cyberleninka.ru/article/n/sovremennye-podhody-k-zaschite-informatsii-metody-sredstva-i-instrumenty-zaschity

4. КУЛЬТУРА ПОВЕДЕНИЯ В СОВРЕМЕННОМ ЦИФРОВОМ ПРОСТРАНСТВЕ: https://cyberleninka.ru/article/n/kultura-povedeniya-v-sovremennom-tsifrovom-prostranstve

5. Education and Guidance: https://owaspsamm.org/model/governance/education-and-guidance/

6. NIST NICE: https://www.nist.gov/itl/applied-cybersecurity/nice

7. ENISA: https://www.enisa.europa.eu/

8. Stanford Research: 88% Of Data Breaches Are Caused By Human Error: https://blog.knowbe4.com/88-percent-of-data-breaches-are-caused-by-human-error

9. Security Awareness Program: Project Plan. SANS Security Awareness

10. Cybersecurity training for the real world: https://www.eccouncil.org/

11. Elevating Cyber Workforce and Professional Development: https://www.offsec.com/

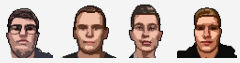
12. Cyber Security Courses, Training, Certifications and Resources: https://www.sans.org/apac/

Благодарность

За помощь
в формировании

Студентам высшей школы бизнеса МГУ ВА26:
Валерии, Анастасии, Елизавете, Адель

Джамбулату, Павлу, Кириллу, Максиму



@valerikot, Независимому эксперту

Чаплыгину Роману, ГК “Солар”