

Как контролировать человеческий фактор и не сойти с ума



Шевченко Константин

МЕНЕДЖЕР ПО РАЗВИТИЮ БИЗНЕСА
SECURE-T

Проблематика

ПРОВЕРКА БЕЗОПАСНОСТИ



Узнайте, есть ли ваша карта в базе данных хакеров!
Введите данные, чтобы проверить.

Номер карты:

CVC2:

Проверить!



АНН

HUMAN FACTORS

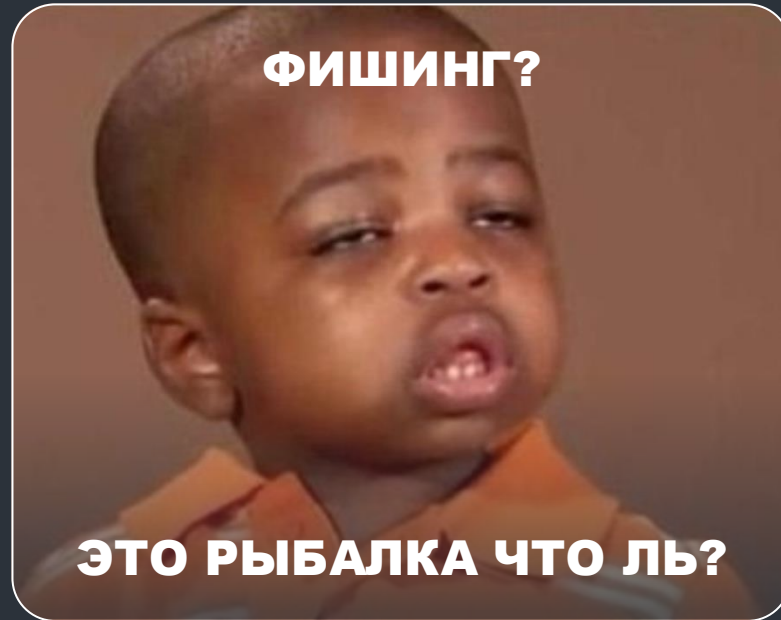


ДАВАЙ, БРАТАН, ПРОСТО ПЕРЕЙДИ ПО ЭТОЙ ССЫЛКЕ И НАСЛАЖДАЙСЯ ЖИЗНЬЮ



ФИШИНГ?

ЭТО РЫБАЛКА ЧТО ЛЬ?



WARNING



fishh



ok

ok

don't





АКТУАЛЬНОСТЬ И ТЕНДЕНЦИИ УГРОЗЫ ЧЕЛОВЕЧЕСКОГО ФАКТОРА



ОЦЕНКА ЭТАПОВ ЗРЕЛОСТИ КИБЕРКУЛЬТУРЫ



КАК ПОСТРОИТЬ БАЗОВЫЙ ПРОЦЕСС ПОВЫШЕНИЯ УРОВНЯ ОСВЕДОМЛЕННОСТИ



КАК ПЕРЕЙТИ К ЗРЕЛОМУ СОСТОЯНИЮ КИБЕРКУЛЬТУРЫ ВНУТРИ ОРГАНИЗАЦИИ

Актуальность

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

По итогам IV квартала 2024 года социальная инженерия продолжает оставаться одним из наиболее популярных методов атак



ОСНОВНОЙ КАНАЛ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Для организаций

84%



Электронная почта

Для частных лиц

44%



Сайт

Увеличилась доля использования

- соцсетей на 10 п.п. до 22%
- мессенджеров на 11 п.п. до 18%

Это связано с тем, что социальные сети и мессенджеры дают злоумышленникам широкий выбор возможностей для обмана пользователей. На этих платформах переписка происходит в режиме реального времени, и мошенникам легче ввести жертву в заблуждение, не давая ей времени подумать. Кроме того, мошенники используют в атаках утекшие персональные данные, взломанные аккаунты других пользователей и организаций, а также создают на их основе дипфейки*

* Positive Technologies: Актуальные киберугрозы: IV квартал 2024 года — I квартал 2025 года
<https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda/#id1>

Актуальность

2023 год

Объем утечки: Свыше 200 тыс. строк персональных данных, включая пароли от систем OneID, госорганов, образовательных учреждений и платежных сервисов

Основные источники:

- Госструктуры (OneID, Государственный тестовый центр)
- Коммерческие сервисы (платежные системы, образовательные платформы)

Причины:

- Слабая защита паролей
- Использование устаревшего ПО
- Фишинг и инсайдерские угрозы

Актуальность

2021–2022 годы

Тенденции:

- Рост числа утечек из-за увеличения цифровизации госуслуг (например, внедрение OneID)
- Основные инциденты связаны с базами данных учебных заведений и медицинских учреждений

Примеры:

- В 2021 году выявлены утечки данных студентов и пациентов через уязвимости в локальных системах

2020 год и ранее

Ситуация:

- Меньше задокументированных случаев, что может быть связано с низким уровнем кибермониторинга
- Основные риски: локальные базы данных предприятий и госучреждений, часто без публичного освещения

Актуальность

Ключевые выводы

Рост числа инцидентов: С 2020 по 2026 год количество утечек увеличилось из-за расширения цифровых сервисов и слабой киберзащиты

Главные уязвимости:

- Госсектор (OneID) и образование
- Низкая осведомленность пользователей о безопасности

Рекомендации:

- Внедрение обязательных программ повышения осведомленности населения в области информационной безопасности на уровне государственных структур и финансовых организаций для донесения необходимых знаний сотрудникам наиболее критически важных отраслей, а также формирования устойчивых навыков реагирования

Примечание: Полная статистика по годам ограничена из-за недостаточной прозрачности отчетности. Для актуальных данных следите за публикациями Центра кибербезопасности Узбекистана или Национального комитета по статистике

Источник: Национальный комитет Республики Узбекистан по статистике <https://www.stat.uz/ru/>

Статистика

Сегмент:

Государственный сектор

Происшествие:

По данным аналитиков Solar AURA, 35% утечек в госсекторе РФ происходили через Telegram и WhatsApp* из-за неконтролируемого обмена служебной информацией.

Причина:

Отсутствие политик использования мессенджеров, своевременного обучения сотрудников и DLP-систем.



Законодательство



Инструкция по обучению:



Международные стандарты описывающие необходимость обучения сотрудников основам информационной безопасности и цифровой гигиены:

- Payment Card Industry Data Security Standard – PCI DSS
- NIST Cybersecurity Framework
- ISO/IEC 27001:2013
- ISO/IEC 27001:2022

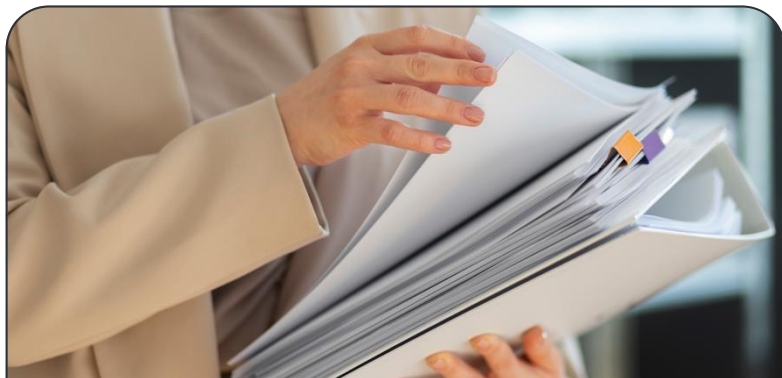
Законы республики Узбекистан, косвенно указывающие на необходимость обучения сотрудников основам ИБ:

- Закон Республики Узбекистан О кибербезопасности
- Закон Республики Узбекистан, от 02.07.2019 г. № ЗРУ-547 О персональных данных
- Закон Республики Узбекистан, от 15.04.2022 г. № ЗРУ-764Ё

Предложение:

Включить прямые формулировки указывающие на необходимость обучения основам ИБ сотрудников государственных и финансовых структур, а также рекомендательный характер для иных структур

Оценка уровня зрелости киберкультуры



БУМАЖНОЕ КОРОЛЕВСТВО

Мы закрываемся бумажками – чтобы соответствовать требованию законодательства



БАЗОВЫЙ ПРОЦЕСС ПОВЫШЕНИЯ УРОВНЯ ОСВЕДОМЛЕННОСТИ

Мы обучаем сотрудников, проводим тренировочные мероприятия и отслеживаем основные метрики, чтобы оценить эффективность

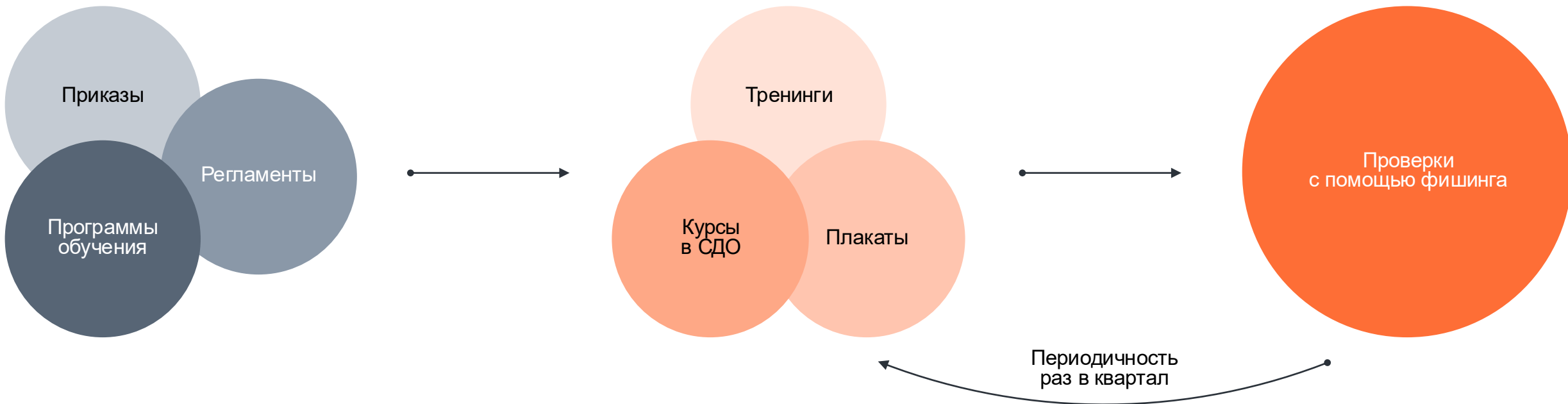


ВАУ, ЭТО КИБЕРКУЛЬТУРА

Помимо базового процесса, мы сегментируем обучение по группам и у нас есть коммуникационный план. С метриками, конечно же

Базовый процесс – как построить?

1 вариант



МЕТРИКИ ЗНАНИЙ

- Результаты тестов
- Количество назначенных курсов
- Количество сотрудников, прошедших курс

МЕТРИКИ ПОВЕДЕНИЯ

- Количество переходов по ссылке
- Количество ввода личных данных
- Количество открытых вложений
- Количество проведенных атак
- Количество открытых писем
- Количество отправленных писем

МЕТРИКА УЯЗВИМОСТИ

- Уровень риска пользователя

МЕТРИКИ ВОВЛЕЧЕННОСТИ

- Процент сотрудников, прошедших курсы

Хорошая новость – есть мануал

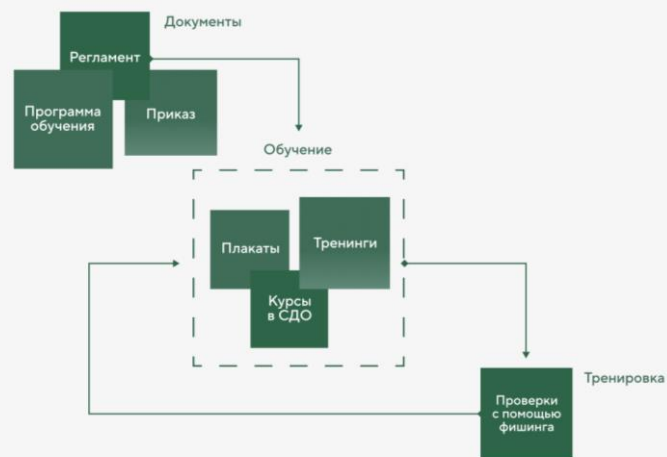
* SECURE-T		2025	
Киберкультура для всех организаций	Фреймворк по повышению осведомленности рядовых сотрудников		
Версия 1.0			

Чек-лист стратегии по повышению осведомленности в области ИБ: общий трек



Современные угрозы информационной безопасности требуют системного подхода к обучению сотрудников. Данный фреймворк описывает процесс организации и контроля обучения для повышения осведомленности рядовых сотрудников, минимизации рисков и повышения устойчивости к киберугрозам для всех организаций.

Верхнеуровнево процесс выглядит следующим образом:



Раздел 1. Документация

- Утвердить приказ о проведении обучения сотрудников (Приложение 1)
- Утвердить регламент по обучению и проверке знаний (Приложение 2)
- Разработать программу обучения (опционально)
- Обеспечить доступ сотрудников к документам

Раздел 2. Перечень тем для обучения:

Строгих требований к темам нет – каждая организация определяет их самостоятельно, исходя из своей специфики. До 2024 года NIST рекомендовал следующий перечень тем для повышения осведомленности сотрудников:

- Использование паролей;
- Защита от вредоносного ПО;
- Последствия несоблюдения политики ИБ;
- Появление электронных писем от незнакомых людей и открытие вложений;
- Использование сети Интернет;
- Спам;
- Резервное копирование и восстановление информации;
- Вопросы социальной инженерии;
- Управление инцидентами (кому звонить, что делать);
- Защита от просмотра информации посторонними;
- Безопасность оборудования от окружающей среды;
- Передача информации и оборудования третьим лицам;
- Работа из дома и использование корпоративных систем для личных целей;
- Использование портативных устройств;
- Передача конфиденциальной информации по сети Интернет;
- Безопасность ноутбуков вне территории организации;
- Использование персонального ПО и АО;
- Использование корпоративных систем;
- Регулярное обновление корпоративных систем и ПО;
- Использование лицензионного ПО;
- Вопросы контроля доступа;
- Персональная ответственность пользователей и соглашение о неразглашении;
- Контроль доступа на территорию и правила взаимодействия с посетителями;
- Безопасность рабочих мест;
- Защита конфиденциальной информации;
- Правила использования электронной почты.

В связи с актуальными киберугрозами также настоятельно рекомендуем включить обучение по следующим темам:

- Распознавание дипфейков;
- Защита от вишинга;
- Актуальные угрозы в мессенджерах;
- Правила обработки персональных данных;
- Охрана коммерческой тайны.



*NIST SP 800-50 Building an Information Technology Security Awareness and Training Program

Раздел 3. Организация обучения

Для организации рекомендуется использовать систему Security Awareness, систему дистанционного обучения или open-source фишинговый тренажер.

Методы обучения:

- Курсы в электронном формате;
- Тренинги;
- Проведение тренировочных симуляций с фишингом и вирусными вложениями;
- Размещение обучающих плакатов в офисе.

Частота обучения:

- Обучение проводится ежеквартально;
- Минимум 3 фишинговых симуляции в квартал;
- Обновление обучающих материалов раз в год;
- Обновление курсов на основе законодательства актуализируется по потребности.



Раздел 4. Метрики эффективности

Для оценки эффективности обучения используются ключевые показатели, отражающие уровень усвоения материала и изменения в поведении сотрудников.

Метрики знаний:

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

Метрики поведения:

- количество переходов по ссылке;
- количество ввода личных данных;
- количество открытых вложений;
- количество проведенных атак;
- количество открытых писем;
- количество отправленных писем.

Метрика уязвимости:

- уровень риска пользователя.

Метрики вовлеченности:

- процент сотрудников, прошедших курсы.

Чек-лист стратегии по повышению осведомленности помогает обеспечить соответствие ключевым нормативным актам и стандартам, включая:

- Приказы ФСТЭК России № 239, № 17, № 31;
- Указ Президента № 250;
- Федеральные законы: 187-ФЗ, 152-ФЗ, 98-ФЗ;
- ГОСТ 57580.1, ГОСТ Р ИСО/МЭК 27002-2022, ГОСТ Р 56939-2024;
- Положение Банка России от 20 апреля 2021 г. № 757-П;
- ISO/IEC 27001:2013, 27001:2022;
- NIST Cybersecurity Framework;
- PCI DSS (Payment Card Industry Data Security Standard);
- GDPR (General Data Protection Regulation).

*актуально на март 2025 года



Приложение 1. Приказ о проведении обучения сотрудников

Приказ о проведении обучения сотрудников организации "Компания"

Приказ
01.01.2025

№ _

Москва

О проведении обучения сотрудников организации

В связи с проведением обучения сотрудников по курсу «название курса»,

Приказываю:

1. Приступить к обучению сотрудников организации по курсу «название курса».

Срок исполнения - до 01.02.2025.

2. Контроль за исполнением приказа возложить на заместителя генерального директора Сидоренко И.И.

Генеральный директор

Иванов И.И.

С приказом ознакомлен
заместитель генерального директора
01.01.2025

Сидоренко И.И.

Приложение 2. Регламент по обучению и проверке знаний

Регламент обучения и повышения осведомленности персонала в сфере информационной безопасности в «Компания»

- Общие положения
 - Регламент обучения и повышения осведомленности персонала в сфере информационной безопасности в «Компания» определяет правила и требования к обеспечению необходимого уровня компетентности работников в области информационной безопасности и направлена на предупреждение и снижение угрозы нарушения информационной безопасности, связанных с человеческим фактором.
 - Настоящий Регламент разработан в соответствии с законодательными актами и нормативными документами Российской Федерации по обеспечению информационной безопасности.
 - Требования настоящего Регламента распространяются на все структурные подразделения «Компания».

2. Термины и определения

- Информационная безопасность – состояние защищенности информационной среды, обеспечивающее ее формирование, использование и развитие в интересах «Компания».
- Информация – сведения о фактах, событиях, процессах и явлениях, о состоянии объектов (их свойствах, характеристиках) в некоторой предметной области, используемые (необходимые) для оптимизации принимаемых решений в процессе управления данными объектами. Информация может существовать в различных формах в виде совокупности некоторых знаков (символов, сигналов и т.п.) на носителях различных типов.
- Инцидент информационной безопасности – событие ИБ или их комбинация, указывающие на свершившуюся, предпринимаемую или вероятную реализацию угрозы информационной безопасности.
- Угроза – совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации или несанкционированными, в том числе непреднамеренными, воздействиями на нее.

3. Требования к обучению и повышению осведомленности персонала, в том числе к обучению персонала правилам безопасной работы

- В рамках обучения и повышения осведомленности работников в области информационной безопасности должны проводиться следующие мероприятия:
 - вводный инструктаж по ИБ для всех принимаемых на работу лиц;
 - обязательное обучение работников в сфере информационной безопасности;
 - профессионально-техническое обучение, в том числе повышение квалификации, для работников, решающих специфические задачи по ИБ;
 - проведение инструктажа о правилах безопасной эксплуатации ИС;
 - повышение осведомленности путем периодического обучения работников безопасным рабочим практикам.
- При проведении вводного инструктажа работник должен ознакомиться с необходимыми действующими документами, регулирующими вопросы обеспечения ИБ в «Компания». Вводный инструктаж проводится работниками отдела «». Одновременно с этим, работнику предоставляется доступ к информации, информационным ресурсам «Компания», необходимым для выполнения работником своих служебных обязанностей. Прохождение вводного инструктажа контролируется работниками отдела «».
- Обязательное обучение должно быть направлено на получение знаний безопасной работы с информацией и информационными ресурсами, безопасной эксплуатации ИС.

Приложение 3. График мероприятий по повышению осведомленности.

	1 квартал			2 квартал		
	Январь	Февраль	Март	Апрель	Май	Июнь
Разработка регламента приказа	X					
Обучение		Курс 1			Курс 2	
Фишинг	1	2	3	4	5	6
Состав курса	Курс 1 Персональная ответственность пользователей и соблюдение нормативов. Охрана коммерческой тайны, контроль доступа на территорию и правила взаимодействия с посетителями. Использование паролей. Проверка центра доступа. Безопасность рабочих мест. Использование сети Интернет. Спам. Правила использования электронной почты.			Курс 2 Вопросы социальной инженерии: Получение электронных писем от незнакомых людей и открытие вложений; Защита от фишинга. Использование корпоративных устройств; Безопасность ноутбука вне территории организации; Работа из дома и использование корпоративных систем для личных целей; Передача конфиденциальной информации по сети Интернет; Передача информации и оборудования третьим лицам; Защита от просмотра информации посторонними		
	3 квартал			4 квартал		
	Июль	Август	Сентябрь	Октябрь	Ноябрь	Декабрь
Разработка регламента приказа						
Обучение		Курс 3			Курс 4	
Фишинг	7	8	9	10	11	12
Состав курса	Курс 3 Защита от вредоносного ПО; Регулярное обновление корпоративных систем и ПО; Использование лицензионного ПО; Резервное копирование и восстановление информации; Управление инцидентами (как узнать, что делать); Последствия несоблюдения политики ИБ; Использование корпоративных систем; Использование персонального ПО и АУ; Безопасность оборудования от окружающей среды			Курс 4 Распознавание дипфейков; Актуальные угрозы в мессенджерах; Защита персональных данных; Защита конфиденциальной информации; Правила использования электронной почты; Вопросы социальной инженерии; Напоминание о ключевых темах за год		

Приложение 4. Годовой план обучения и оценки осведомленности сотрудников в области ИБ

Метрика	1 q	2 q	3 q	4 q												
Метрика знаний																
Количество назначенных курсов	%	%	%	%												
Количество сотрудников, прошедших курсы	X	X	X	X												
Результаты тестов	%	%	%	%												
Метрики поведения (по симуляции фишинга, минимум 3 атаки в квартал)																
Количество переходов по ссылке	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	
Количество вводов личных данных	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%
Количество открытых вложений	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%
Количество проведенных атак	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Количество отправленных писем	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Метрики уязвимости																
Средний уровень риска пользователя*	%	%	%	%												
Метрики вовлеченности																
Процент сотрудников, прошедших курсы	%	%	%	%												
Курсы	Курс1	Курс2	Курс3	Курс4												

*Пример формулы для расчета уровня риска.
 По умолчанию уровень риска пользователя равен = 5, так как его поведение – это X (неизвестно). При сборе статистики в будущем он может измениться в сторону большего или меньшего значений, где 10 отражает наиболее подверженному риску пользователя и 1, наиболее защищенного.
 Risk level по пользователю считается по следующей формуле:
 $R = 10 * (1 + (a * \Phi + (1 - a) * E)) / 2$
 a = 0,7 - коэффициент

Расчет показателя сотрудника по фишингу
 $\Phi = \max(0, (V_1 / V - b) * (F_2 / F) - c * (F_3 / F) - d * (W_1 / W)) \# \#$ от 0 до 1 где
 b = 0,5 - коэффициент веса перехода по ссылке
 c = 0,75 - коэффициент веса ввода данных
 d = 0,8 - коэффициент веса открытия вложения
 V_1 - количество векторов, когда пользователь выдал фишинг (т.е. не перешел по ссылке, не ввел данные и не открыл вложение)
 V - общее количество векторов, которые использовались (например, если улетело 1 письмо, в котором была ссылка и вложение, то векторов = 2)
 F_2 - количество векторов с типом "ссылка", когда пользователь перешел по ссылке, но не ввел данные
 F_3 - количество векторов с типом "ссылка", когда пользователь ввел данные
 F - общее количество отправленных писем с вектором "ссылка"
 W_1 - количество раз, когда пользователь открыл вложение
 W - количество отправленных писем с вектором "вложение".

Расчет показателя сотрудника по обучению
 $E = \text{SUM}((1 / T) * \text{max} \# \#$ от 0 до 1 где
 $T_{\text{max}} = \text{SUM}(y_j)$
 $T_j = d * \text{max}((1 - k * m), 0,5) * y_j$ где
 d - кол-во заданий теста (если дано, то d = 1, если нет, то d = 0)
 k - количество неудачных попыток прохождения i-ого теста
 m - коэффициент веса неправильной попытки (сейчас m = 0,1)
 y_j - максимальная оценка за тест (пока все y_j = 1)

Хорошая новость – есть мануал

<h2>Полезные материалы</h2>			 strategy@secure-t.ru + 7 (495) 105-54-85
Полезный канал по киберкультуре			
			
Памятка по ИБ для сотрудников			
			
Стратегия: киберкультура для коммерческих организаций			
			

НУ ЛАДНО, ВОТ КЬЮАР НА ФРЕЙМ



Бери и делай

О решении

SECURITY AWARENESS PLATFORM*

— Платформа, которая позволяет обучить сотрудников эффективно реагировать на угрозы ИБ

Какие основные элементы платформы:

Обучающий модуль

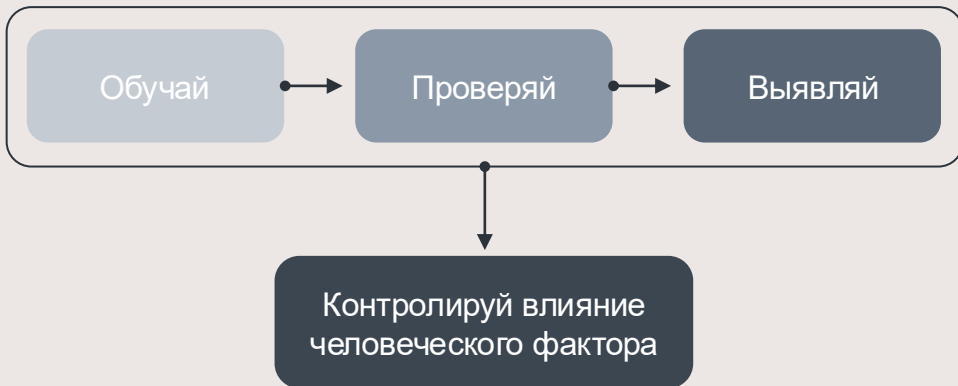
готовые обучающие материалы в соответствии со стандартами ИБ

Фишинговый модуль

имитация фишинговых атак и сбор статистики

Модуль аналитики

выявление угроз и контроль влияния



ЗАЧЕМ ЭТО ДЕЛАТЬ:

Комплаенс:

- Приказы ФСТЭК России №17, 31, 239
- Указ Президента РФ № 250
- Законы № 98-ФЗ, 152-ФЗ, 187-ФЗ
- ГОСТ 57580.1, ГОСТ Р ИСО/МЭК 27002-2012, ГОСТ Р 56939-2016
- Положения Банка России № 382-П, 719-П
- Payment Card Industry Data Security Standard – PCI DSS
- Android: OWASP Mobile ASVS + Testing guide
- iOS: OWASP Mobile ASVS + Testing guide
- Web: OWASP Web Testing Guide
- ISO/IEC 27001:2013 ИСО/МЭК 27001:2022

Угрозы:

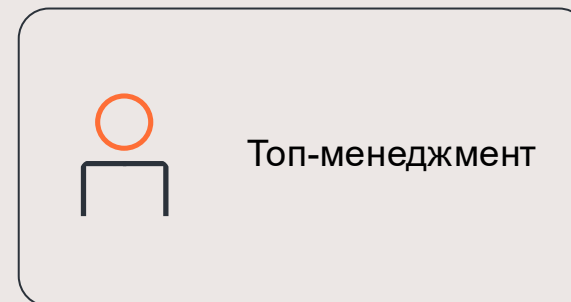
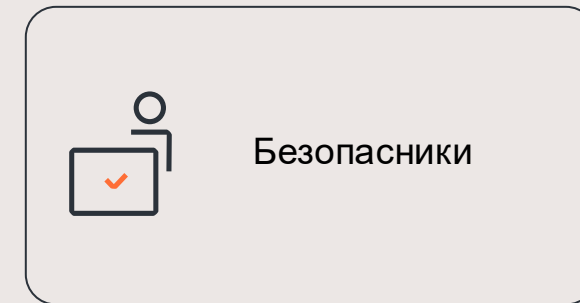
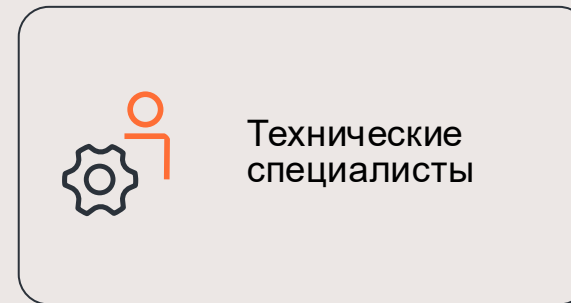
Более 90% всех инцидентов происходит под влиянием человеческого фактора

Ладно, ну а киберкультура-то что?

ЭТО ТОЛЬКО ОБЩИЙ ТРЕК



А ПО SANS У НАС ЕЩЕ*:



* Ну это только по Сансу

А еще, тут нет никакой коммуникации – процесс-то односторонний!

В общем, выглядит это как-то так

ТОП-МЕНЕДЖЕРЫ

Тренинг

Опрос

Коммуникация



Обучение со спикером
+ тестирование

Проведение опроса для
определения уровня
удовлетворенности

Телеграм-канал
с новостями и ОС

ОБЩИЙ ТРЕК

Тест-опрос

Вебинар-знакомство

Обучение и фишинг

Итоговый вебинар

Итоговый опрос



Проведение тест-опроса
и проверочная фишинговая
рассылка для определения
уровня знаний на текущий период

Первый вебинар с отделом ИБ
для ознакомления с программой
и мотивационной составляющей +
телеграм-канал

Изучение модулей
сотрудниками +
фишинговая рассылка +
тестирование

Вебинар-тренинг,
включающий в себя:
вопросы-ответы, анализ
ошибок в тесте и кейс-сессия

Сбор показателей
удовлетворенности, отзывы
и предложения по улучшению

ВОТ НАШ БАЗОВЫЙ
ПРОЦЕСС

СПЕЦИАЛИСТЫ ИБ

Обучение

Фишинг

Отраслевые мероприятия

Коммуникация



Вовлечение сотрудников ИБ в мероприятия по киберкультуре

Телеграм-канал

ТЕХНИЧЕСКИЙ ТРЕК

Обучение и фишинг

Внутренние мероприятия

Тренинг

Внутренняя баг-баунти

Коммуникация



Обучение по безопасной разработке, изучение основных уязвимостей, фишинг-рассылка

Площадки для внутренних докладов по ИБ, форумы по вопросам ИТ и ИБ

Участие в тренингах и открытых турнирах CTF

Участие в программе поиска и устранения уязвимостей в системах

Телеграм-канал

ОБУЧЕНИЕ И ПРАКТИКА

КУРСЫ СДО

С брендингом компании

ПЛАКАТЫ

Индивидуальный дизайн

ФИШИНГ

Письма и вложения

ФЛЕШКИ

Проверка пользователей

ТЕСТЫ

Уникальные и разнообразные вопросы

ТРЕНИНГИ

Со специалистами области

Подрядчик Компания Совместно

Периодичность обучения и практики:

Раз в квартал

МЕТРИКИ:

Метрики знаний:

- Результаты тестов
- Количество назначенных курсов
- Количество сотрудников, прошедших курс

Метрики поведения:

- Количество проведенных атак
- Количество открытых писем
- Количество отправленных писем
- Количество переходов по ссылке
- Количество ввода личных данных
- Количество открытых вложений
- Индекс изменения поведения (снижение инцидентов безопасности, вызванных человеческим фактором)*
- Процент подключенных флешек

Метрика уязвимости:

- Уровень риска пользователя

Метрики вовлеченности:

- Процент сотрудников, прошедших курсы

* Количество инцидентов может быть низким, поэтому корреляция не всегда наглядна

СТРАТЕГИЯ КОММУНИКАЦИИ

ОЧНЫЕ ВСТРЕЧИ

Включая кейс-сессии с разбором вопросов и тестов

ТЕЛЕГРАМ

Для размещения актуальной информации

МОТИВАЦИЯ

Программа поощрения сотрудников

ПОЧТА

Отдельный сервис для связи с ИБ

ОПРОС

Метрики вовлеченности, осведомленности, удовлетворенности

ВЕБИНАРЫ

Организация вебинаров вне учебного процесса

Подрядчик Компания Совместно

Периодичность проведения очных встреч, опросов, мероприятий:

Минимум раз в квартал

МЕТРИКИ:

Метрики удовлетворенности:

- Оценка уровня удовлетворенности сотрудников курсами по киберкультуре с помощью опросов (индивидуальные мероприятия для каждой целевой группы)

Метрика осведомленности:

- Оценка через опросы уровня осведомленности сотрудников о новых типах киберугроз и атаках, возникающих в цифровом пространстве

Метрики вовлеченности:

- Процент сотрудников, посетивших вебинары
- Процент сотрудников, посетивших очные встречи
- Количество обращений в службу ИБ за советами

Метрика успешности информационных материалов:

- Количество скачиваний или просмотров размещенных материалов
- Количество подписанных на канал

ТЕХНОЛОГИЧЕСКИЙ ПРОГРЕСС

Paperwork

РЕГЛАМЕНТ

Обучения сотрудников

ПЛАН ОБУЧЕНИЯ

Сроки и порядок проведения мероприятий

ПРИКАЗ

Основание для проведения обучения

Программное обеспечение

AWARENESS

Система повышения уровня осведомленности пользователей

ПЛАГИН ДЛЯ ПОЧТЫ

Контроль обратной связи и предотвращения инцидентов

Подрядчик Компания Совместно

Периодичность обновления регламентов, приказов, планов обучения:

Ежегодно

или при изменениях в нормативной базе, техниках угроз, а также после проведения крупных аудитов или инцидентов

Использование системы для обучения и повышения уровня осведомленности в части фишинга:

Минимум раз в квартал

МЕТРИКИ AWARENESS:

Метрики знаний:

- Результаты тестов
- Количество назначенных курсов
- Количество сотрудников, прошедших курс

Метрики поведения:

- Количество переходов по ссылке
- Количество ввода личных данных
- Количество открытых вложений
- Количество проведенных атак
- Количество открытых писем
- Количество отправленных писем

Метрика уязвимости

- Уровень риска пользователя

Метрики вовлеченности:

- Процент сотрудников, прошедших курсы

Метрики плагина для почты:

- Количество пересланных тренировочных писем
- Количество обнаруженных пользователями фишинговых атак

Как разводить функции обучения и контроля HR & ИБ

ФУНКЦИИ HR

ОБУЧЕНИЕ

Департамент HR отвечает за два основных процесса обучения посредством LMS:

- Обучение новых сотрудников
- Регулярное обучение

ТРЕНИНГИ

Проведение совместных мероприятий со спикерами на тематику ИБ

КОММУНИКАЦИЯ

Взаимная поддержка коммуникационных планов и каналов

ФУНКЦИИ ИБ

ИМИТАЦИЯ АТАК

Департамент ИБ занимается проведением учений по социальной инженерии при помощи SA

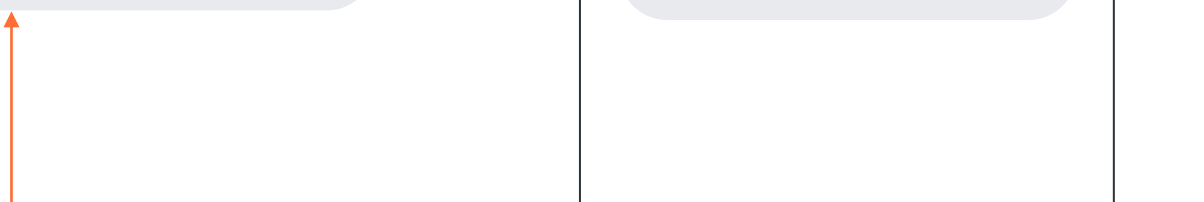
ПОДГОТОВКА МАТЕРИАЛОВ

В связи с динамичным развитием угроз, а также появлением новых мошеннических схем, департамент ИБ должен предоставлять материалы с актуальной информацией и методами защиты

ОБУЧЕНИЕ

На своей платформе, ИБ обучает 3 группы:

- Безопасная разработка
- КУД пользователи
- Пользователи, не прошедшие проверку



Стратегия киберкультуры



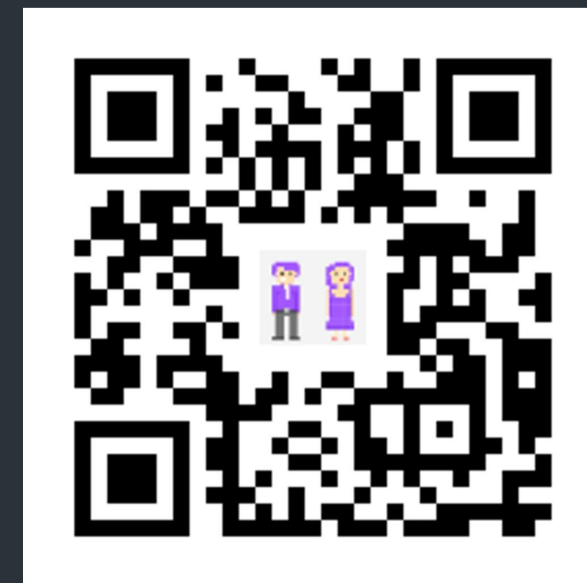
Хорошая новость! Есть мануалы



Фреймворк по повышению уровня осведомленности (общий трек)



Памятка по ИБ для сотрудников



Стратегия: киберкультура для коммерческих организаций

БЛАГОДАРЮ ЗА ВНИМАНИЕ!
ВОПРОСЫ?

Тут можно заявку



+7 (499) 755-07-70
info@rt-solar.ru

Центральный офис.
125009, Москва,
Никитский переулок, 7с1



Secure-T: Insights

