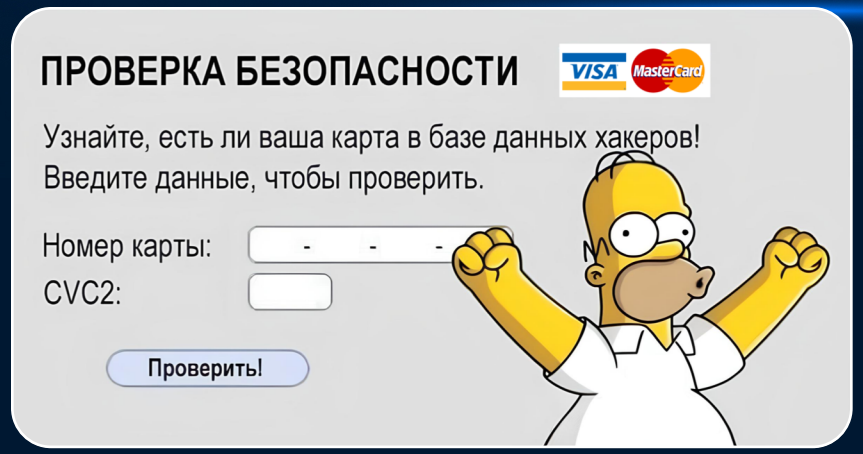
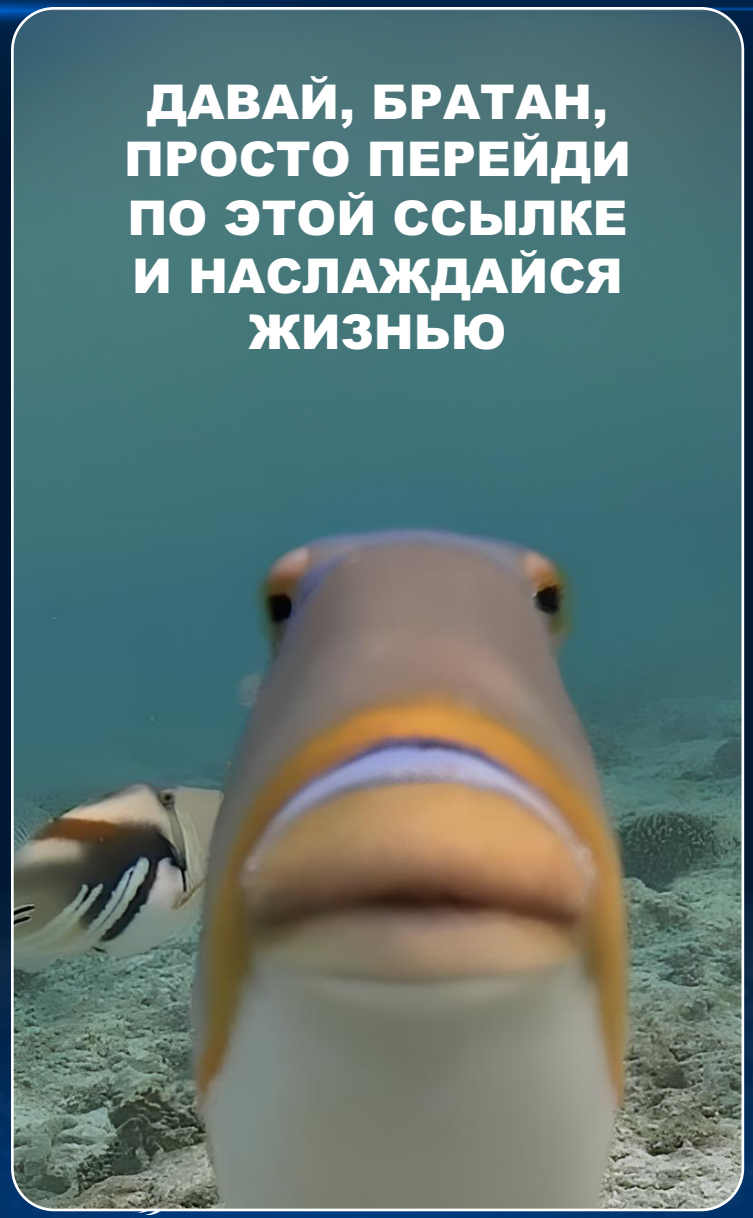
Как контролировать человеческий фактор и не сойти с ума

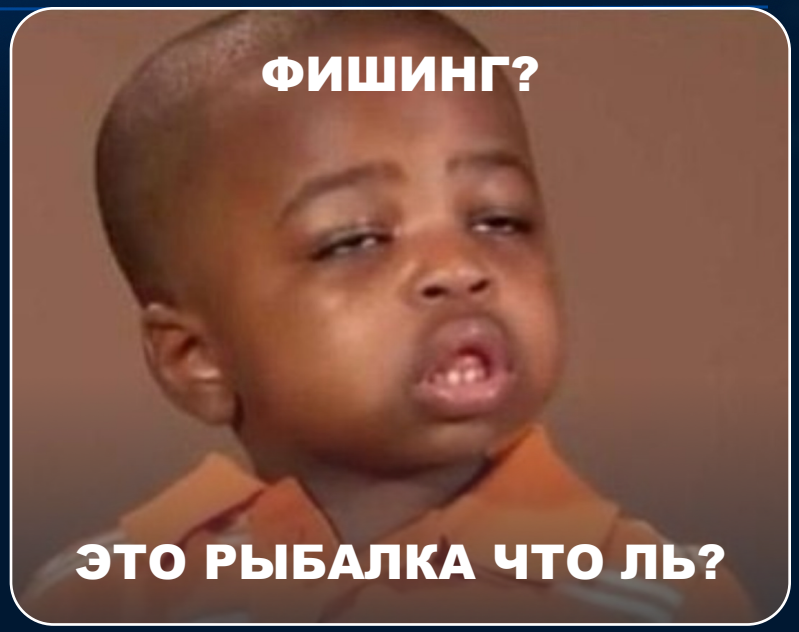
Харитон Никишкин

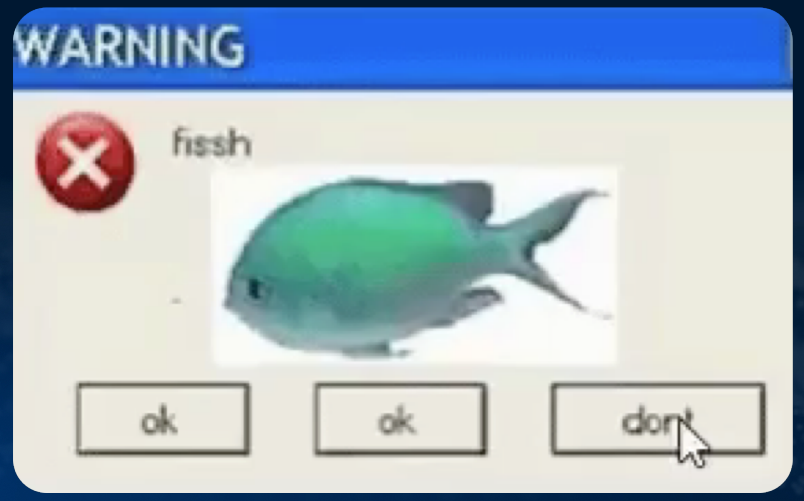
ГЕНЕРАЛЬНЫЙ ДИРЕКТОР SECURE-T

Проблематика







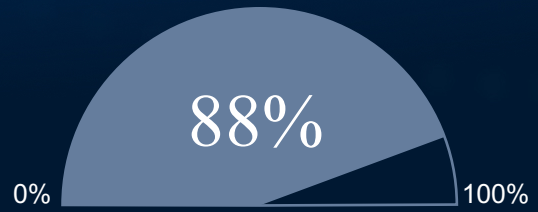


Актуальность

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

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

Атаки на организации



Атаки на частных лиц

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/#id

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

Источник: Межгосударственный статистический комитет содружества независимых государств: https://new.cisstat.org/uzbekistan

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

Источник: Межгосударственный статистический комитет содружества независимых государств: https://new.cisstat.org/uzbekistan

Актуальность

Ключевые выводы

Рост числа инцидентов: С 2020 по 2023 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.

Источник: 35% утечек конфиденциальной информации происходит через мессенджеры: https://www.comnews.ru/content/237885/2025-02-20/2025-w08/1010/35-utechek-konfidencialnoy-informacii-proiskhodit-cherez-messendzhery

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-764È

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?

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

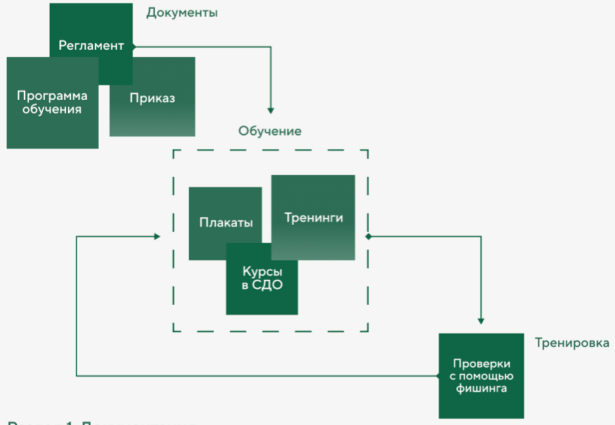
Фреймворк по повышению осведомленности рядовых сотрудников

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

Хорошая новость – есть мануал

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 открытий вложений;
- количество проведенных атак;
- количество открытий 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 Сидоренко И.И.
01.01.2025

Хорошая новость – есть мануал

Полезные материалы

SECURE-T

strategy@secure-t.ru

+ 7 (495) 105-54-85

Полезный канал по киберкультуре

Памятка по ИБ для сотрудников

Стратегия: киберкультура для коммерческих организаций

12

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

* Система повышения уровня осведомленности пользователей

БЛАГОДАРЮ ЗА ВНИМАНИЕ!
ВОПРОСЫ?

UZTELECOM

КОНТАКТНЫЕ ДАННЫЕ:

Дамир Зарипов
Менеджер продаж
+998 95 008 01 75

Тут можно заявку

Secure-T: Insights

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

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

UZTELECOM