SOLAR

Как контролировать человеческий фактор и не сойти с ума

(И выполнить 56-57 пункты №117 приказа ФСТЭК)

Харитон Никишкин

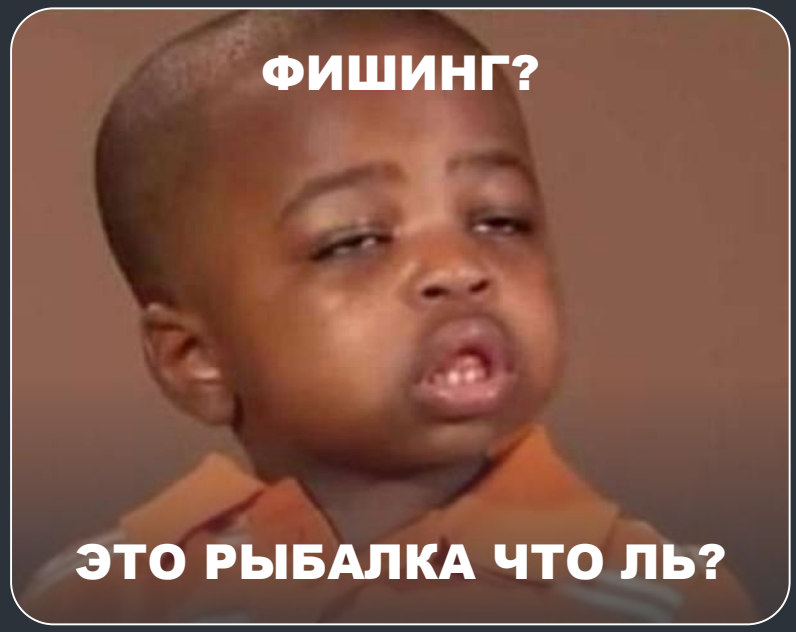
ГЕНЕРАЛЬНЫЙ ДИРЕКТОР SECURE-T

+7 (926) 040-92-00

HG.NIKISHKIN@SECURE-T.RU

МОСКВА, 2025

Проблематика



Краткий список тезисов

SOLAR

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

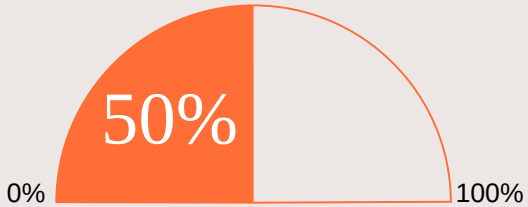
КОНКУРС С ПРИЗОМ!!!

Актуальность

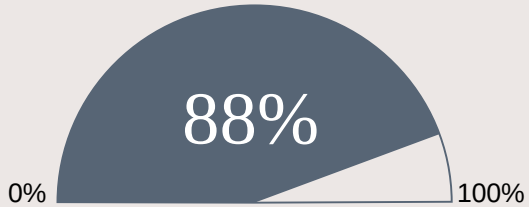
SOLAR

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/#id1

Законодательство

SOLAR

ФЕДЕРАЛЬНЫЙ ЗАКОН № 152-ФЗ О персональных данных: меры по защите персональных данных	ФЕДЕРАЛЬНЫЙ ЗАКОН № 98-ФЗ О коммерческой тайне	ФЕДЕРАЛЬНЫЙ ЗАКОН № 187-ФЗ О безопасности критической информационной инфраструктуры Российской Федерации	ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности
УКАЗ ПРЕЗИДЕНТА РФ ОТ 01.05.2022 № 250 О дополнительных мерах по обеспечению информационной безопасности Российской Федерации	ПРИКАЗ ФСТЭК РОССИИ № 17 Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах	ПРИКАЗ ФСТЭК РОССИИ № 31 Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах	ПРИКАЗ ФСТЭК РОССИИ № 239 Состав мер по обеспечению безопасности и обучению персонала
ПОЛОЖЕНИЕ БАНКА РОССИИ № 382-П О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств	ПОЛОЖЕНИЕ БАНКА РОССИИ № 683-П, 757-П Описание обязательного обучения работников финансовых организаций	ГОСТ Р 56939-2024 Защита информации. Разработка безопасного программного обеспечения. Общие требования	

Законодательство

SOLAR

ПРИКАЗ ФСТЭК РОССИИ ОТ 11.04.2025 № 117

"Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений"
(Зарегистрирован 16.06.2025 № 82619)

4. Настоящий приказ вступает в силу с 1 марта 2026 г.

Приказ ФСТЭК №117

Законодательство

SOLAR

ПРИКАЗ ФСТЭК РОССИИ ОТ 11.04.2025 № 117

56. Мероприятия по повышению уровня знаний и информированности пользователей информационных систем по вопросам защиты информации должны включать:

а) доведение до пользователей информационных материалов, в том числе в форме памяток, баннеров, буклетов, по актуальным вопросам защиты информации;

б) проведение лекций, семинаров, обучающих игр по вопросам защиты информации;

в) проведение имитационных рассылок электронных писем на служебные адреса электронной почты, иные служебные средства коммуникаций с целью оценки устойчивости пользователей к методам социальной инженерии;

г) проведение тренировок с пользователями по практической отработке мероприятий по защите информации, предусмотренных внутренними регламентами по защите информации, и формированию навыков по защите информации.

Приказ ФСТЭК №117

Законодательство

SOLAR

ПРИКАЗ ФСТЭК РОССИИ ОТ 11.04.2025 № 117

57. Применяемые оператором (обладателем информации) способы повышения уровня знаний пользователей по вопросам защиты информации, периодичность и формы оценки уровня знаний должны определяться во внутренних регламентах по защите информации. Оценка уровня знаний должна проводиться не реже одного раза в три года или после компьютерного инцидента, произошедшего у оператора (обладателя информации). Для пользователей, у которых отсутствуют знания по вопросам защиты информации, должно быть организовано повторное прохождение обучающих курсов по вопросам защиты информации.

Приказ ФСТЭК №117

Оценка уровня зрелости киберкультуры

SOLAR

БУМАЖНОЕ КОРОЛЕВСТВО

Мы закрываемся бумажками – чтобы соответствовать требованию законодательства

БАЗОВЫЙ ПРОЦЕСС ПОВЫШЕНИЯ УРОВНЯ ОСВЕДОМЛЕННОСТИ

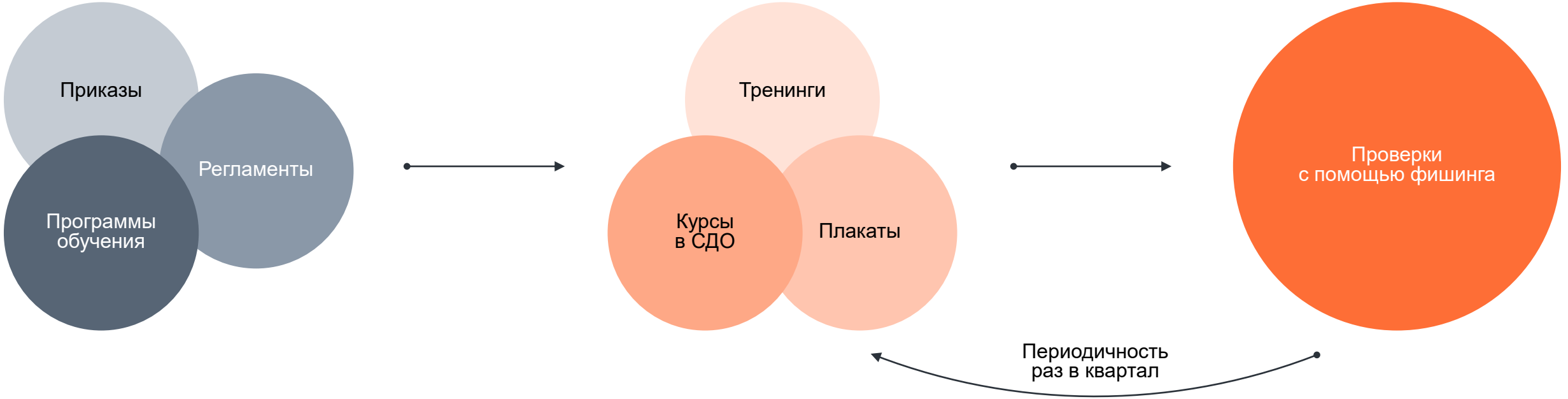
Мы обучаем сотрудников, проводим тренировочные мероприятия и отслеживаем основные метрики, чтобы оценить эффективность

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

SOLAR

SECURE-T

2025

Киберкультура для всех организаций

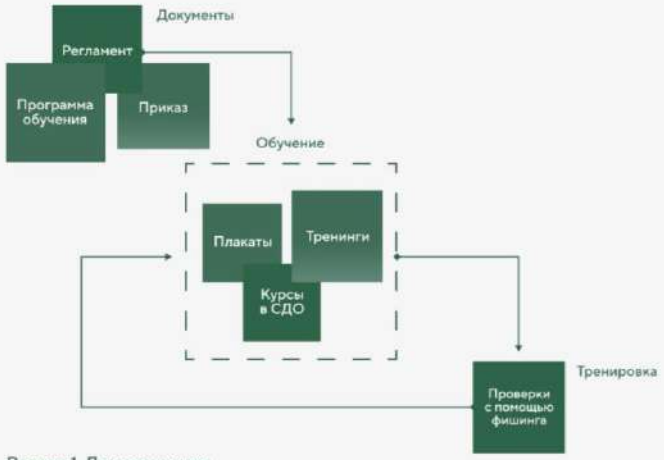
Фреймворк по повышению осведомленности рядовых сотрудников

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

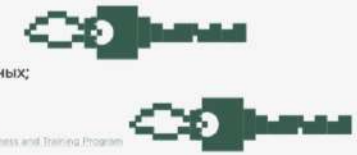
Раздел 2. Перечень тем для обучения:

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

SOLAR

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

Приложение 2. Регламент по обучению и проверке знаний

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

1. Общие положения
1.1. 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 угроз нарушения информационной безопасности, связанных с человеческим фактором.
1.2. Настоящий Регламент разработан в соответствии с законодательными актами и нормативными документами Российской Федерации по обеспечению информационной безопасности.
1.3. Требования настоящего Регламента распространяются на все структурные подразделения «Компания».

2. Термины и определения
2.1. Информационная безопасность – состояние защищенности информационной среды, обеспечивающее ее формирование, использование и развитие в интересах «Компания».
2.2. 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.
2.3. Индидент информационной безопасности – событие ИБ или их комбинация, указывающие на свершившуюся, предпринимаемую или вероятную реализацию угрозы информационной безопасности.
2.4. 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
3.1. 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.
3.2. 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 «».
3.3. 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	×					
Обучение		Курс 1			Курс 2	
Фишинг	1	2	3	4	5	6
Состав курса	Курс 1 Персональная ответственность пользователей и соглашение о неразглашении. Охрана коммерческой тайны. Контроль доступа на территорию и правила взаимодействия с посетителями. Использование терминалов. Вопросы контроля доступа. Безопасность рабочих мест. Использование сети Интернет. Спам. Правила использования электронной почты.			Курс 2 Вопросы социальной инженерии. Появление электронных писем от незнакомых людей и открытие вложений. Защита от вишинга. Использование портативных устройств. Безопасность ноутбуков вне территории организации. Работа на дому 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 (кому звонить, что делать). Последствия несоблюдения политики ИБ. Использование корпоративных систем. Использование персонального ПО и АО. Безопасность оборудования от окружающей среды.			Курс 4 Распознавание дипфейков. Актуальные угрозы и инструменты. 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	×	×	×	×
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	× × × × × × × × × × × × × × × ×			
Количество отправленных писем	× × × × × × × × × × × × × × × ×			
Метрики уязвимости				
Средний уровень риска пользователя*	%	%	%	%
Метрики вовлеченности				
Процент сотрудников, прошедших курсы	%	%	%	%
Курсы	Курс1	Курс2	Курс3	Курс4

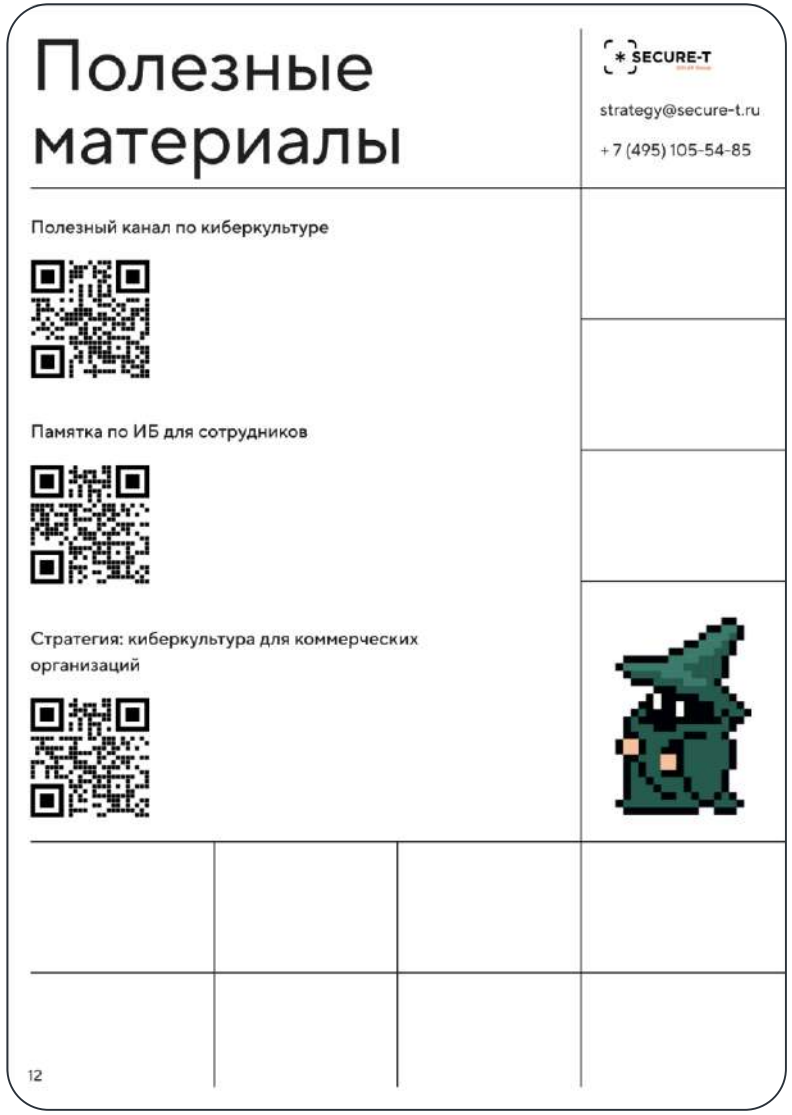
*Пример формулы для расчета уровня риска.
По умолчанию уровень риска пользователя равен = 5, так как его поведение — это X (неизвестно). При сборе статистики в будущем он может измениться в сторону большего или меньшего значений, где 10 отражает наиболее подверженного риску пользователя и 1 - наиболее защищенного.
Risk level по пользователю считается по следующей формуле:
R = 10 * (1 - (α * Φ + (1 - α) * Ξ)) где
α = 0.7 - коэффициент

Расчет показателя сотрудника по Фишингу
Φ = max (0,(W_1 / V - b * (F_2 / F) - c * (F_3 / F) - d * (W_1 / W))) где α= 0.ре 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 выявил фишинг (т.е. не перешел по ссылке, не ввел данные и не открыл вложение)
V - общее количество векторов, которые использовались (например, если участвал 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
Ξ = S.SIN (T_1) / T_max ,где α= 0.дс 1 где
T_max = SUM (q_i)
T_i = d * max (1 / (1 + k * n); 0.5) * y_i где
d - признак удачного теста (если сдал, то d = 1, если нет, то d = 0)
k - количество неудачных попыток прохождения i-ого теста
m - коэффициент веса неудачной попытки (сейчас m = 0,1)
y_i - максимальная оценка за тест (пока все y_i = 1)

Хорошая новость – есть мануал

SOLAR



НУ ЛАДНО, ВОТ КЬЮАР НА ФРЕЙМ

Бери и делай

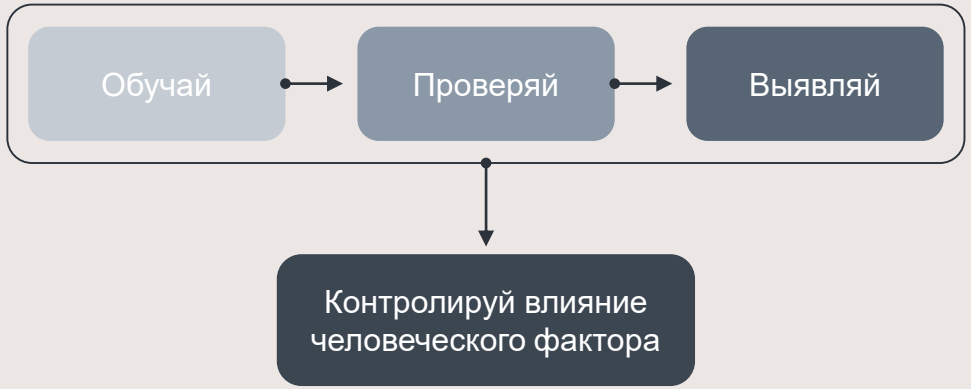
О решении

SOLAR

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:

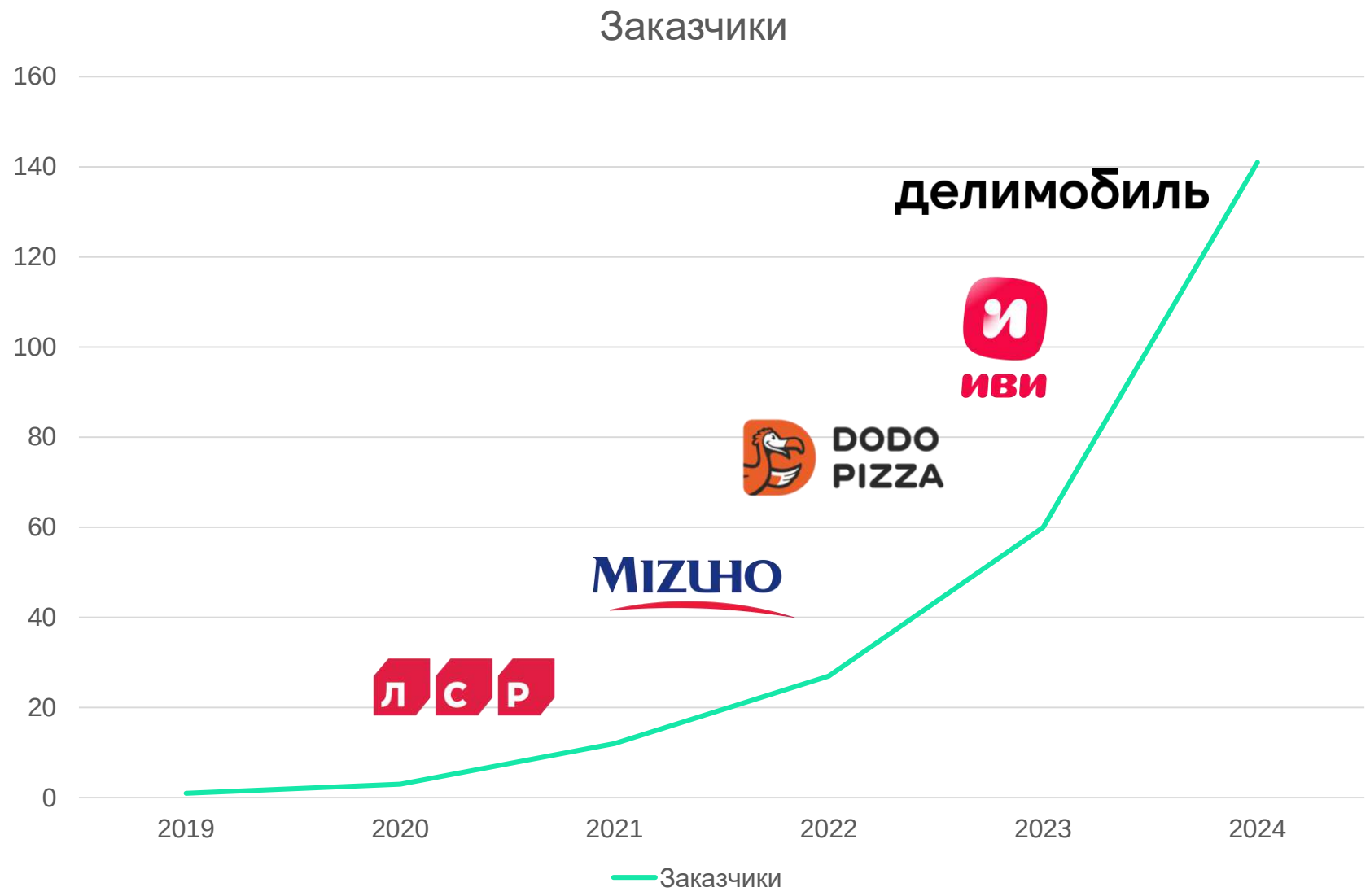
- Приказы ФСТЭК России №17, 31, 239
- Указ Президента РФ № 250
- Законы № 98-ФЗ, 152-ФЗ, 187-ФЗ
- ГОСТ 57580.1, ГОСТ Р ИСО/МЭК 27002-2012, ГОСТ Р 56939-2016
- Положения Банка России № 382-П, 719-П
- Payment Card Industry Data Security Standard – PCI DSS
- Android: OWASP Mobile ASVS + Testing guide
-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

О нас



Действующие заказчики:

170+↑

Retention:

90%↑

Ладно, ну а киберкультура-то что?

SOLAR

ЭТО ТОЛЬКО ОБЩИЙ ТРЕК

А ПО SANS У НАС ЕЩЕ*:

- Технические специалисты
- Безопасники
- Топ-менеджмент

* Ну это только по Сансу

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

В общем, выглядит это как-то так

SOLAR

ТОП-МЕНЕДЖЕРЫ

Тренинг
Обучение со спикером + тестирование

Опрос
Проведение опроса для определения уровня удовлетворенности

Коммуникация
Телеграм-канал с новостями и ОС

ОБЩИЙ ТРЕК

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

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

Обучение и фишинг
Изучение модулей сотрудниками + фишинговая рассылка + тестирование

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

Итоговый опрос
Сбор показателей удовлетворенности, отзывы и предложения по улучшению

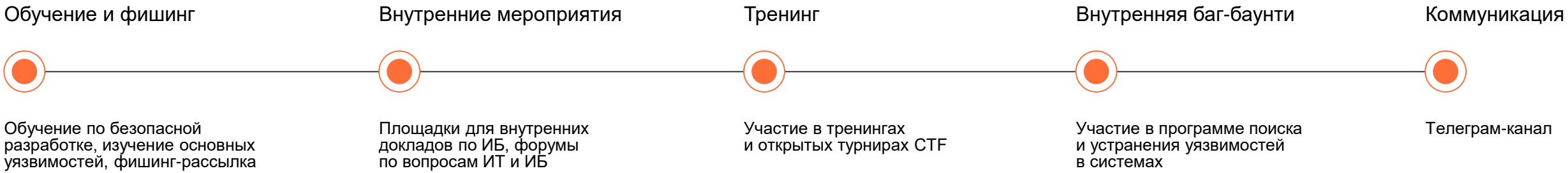
ВОТ НАШ БАЗОВЫЙ ПРОЦЕСС

И так

SOLAR

СПЕЦИАЛИСТЫ ИБ

ТЕХНИЧЕСКИЙ ТРЕК



Элементы киберкультуры

SOLAR

ОБУЧЕНИЕ И ПРАКТИКА

КУРСЫ СДО
С брендированием 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

Элементы киберкультуры

SOLAR

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:

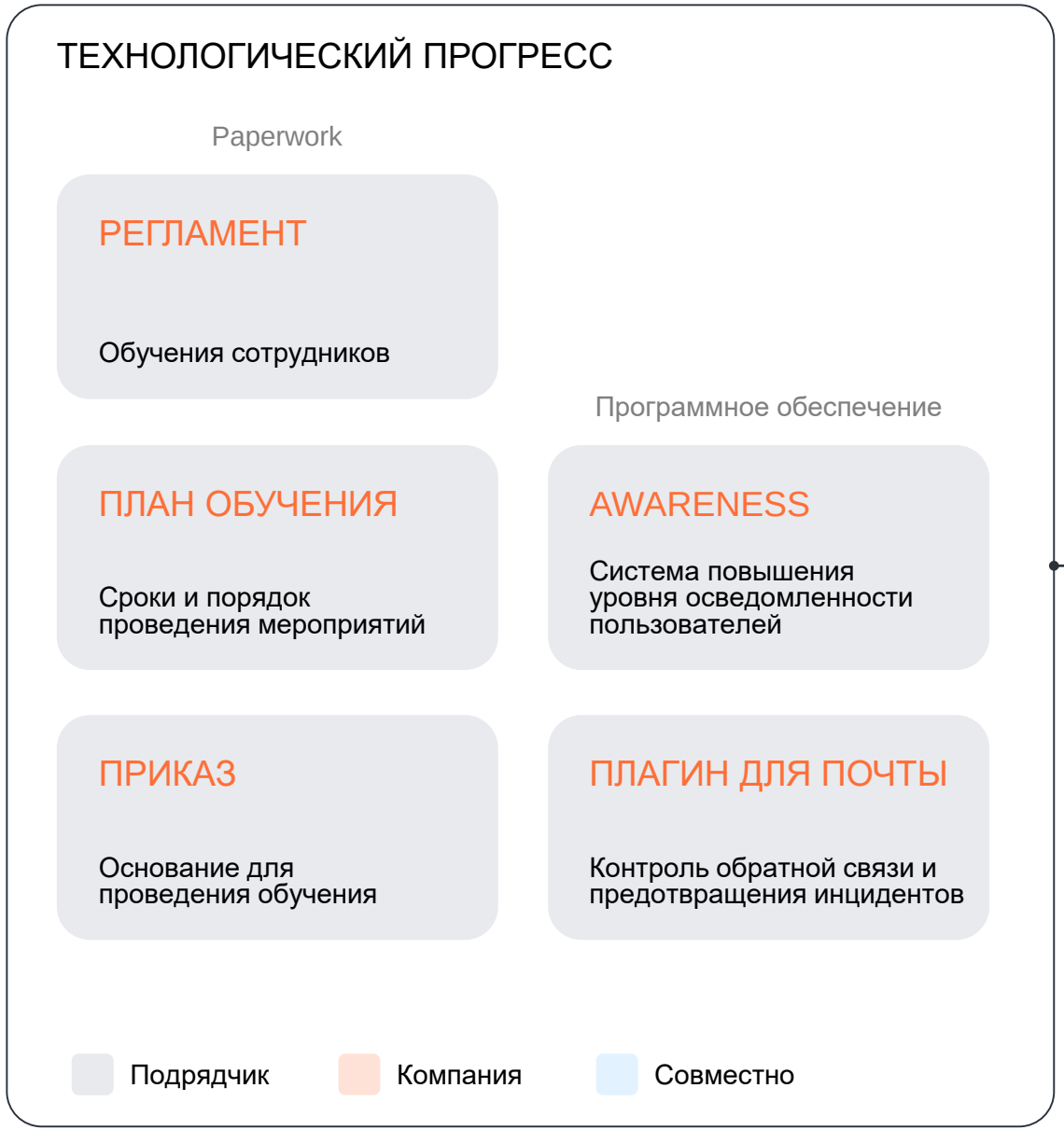
- Процент сотрудников, посетивших вебинары
- Процент сотрудников, посетивших очные встречи
- Количество обращений в службу ИБ за советами

Метрика успешности информационных материалов:

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

Элементы киберкультуры

SOLAR



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

SOLAR

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 методах защиты

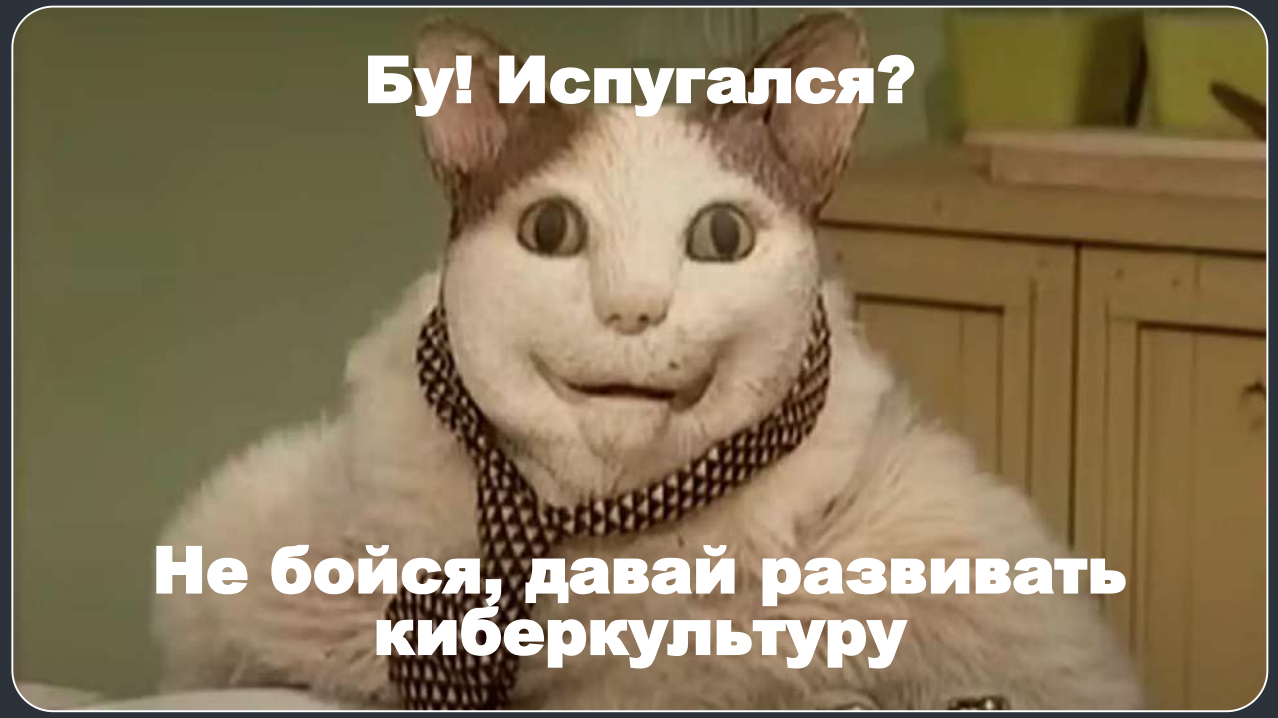
ОБУЧЕНИЕ

На своей платформе, ИБ обучает 3 группы:

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

Стратегия киберкультуры

SOLAR



Квиз по итогам партнерского вебинара

SOLAR

Код Викторины:
00782940

Критерии:

- 5 вопросов
- Правильный ответ
- Скорость ответа

Основной функционал решения

SOLAR

1

Модуль фишинга, обучение, статистика

2

Модуль фишинга, обучение, DLP

3

Модуль фишинга, обучение, защита корпоративной почты

Когда вступает в силу 117 приказ ФСТЭК?

SOLAR

1

1-го Апреля 2026 года

2

1-го Мая 2026 года

3

1-го Марта 2026 года

Обучай - проверяй - выявляй и тем самым:

SOLAR

1

Контролируй влияние человеческого фактора

2

Порти людям жизнь

3

Мерч получай

Выберите доступную опциональную услугу

SOLAR

1

Brand protection + Анализ утечек в даркнет

2

Фишинговая атака конкурентов

3

Лекция для топ-менеджмента + Стратегия

Какие две основные причины, по которым заказчики выстраивают процесс повышения осведомленности внутри организации?

SOLAR

1

Агрессивное поведение проверяющих органов

2

Комплаенс + ИБ

3

Комплаенс и только комплаенс

Хорошая новость! Есть мануалы

SOLAR

Фреймворк по повышению уровня осведомленности (общий трек)

Памятка по ИБ для сотрудников

Стратегия: киберкультура для коммерческих организаций

SOLAR

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