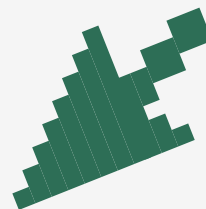


Киберкультура  
для всех  
организаций

Фреймворк по повышению  
осведомленности рядовых  
сотрудников

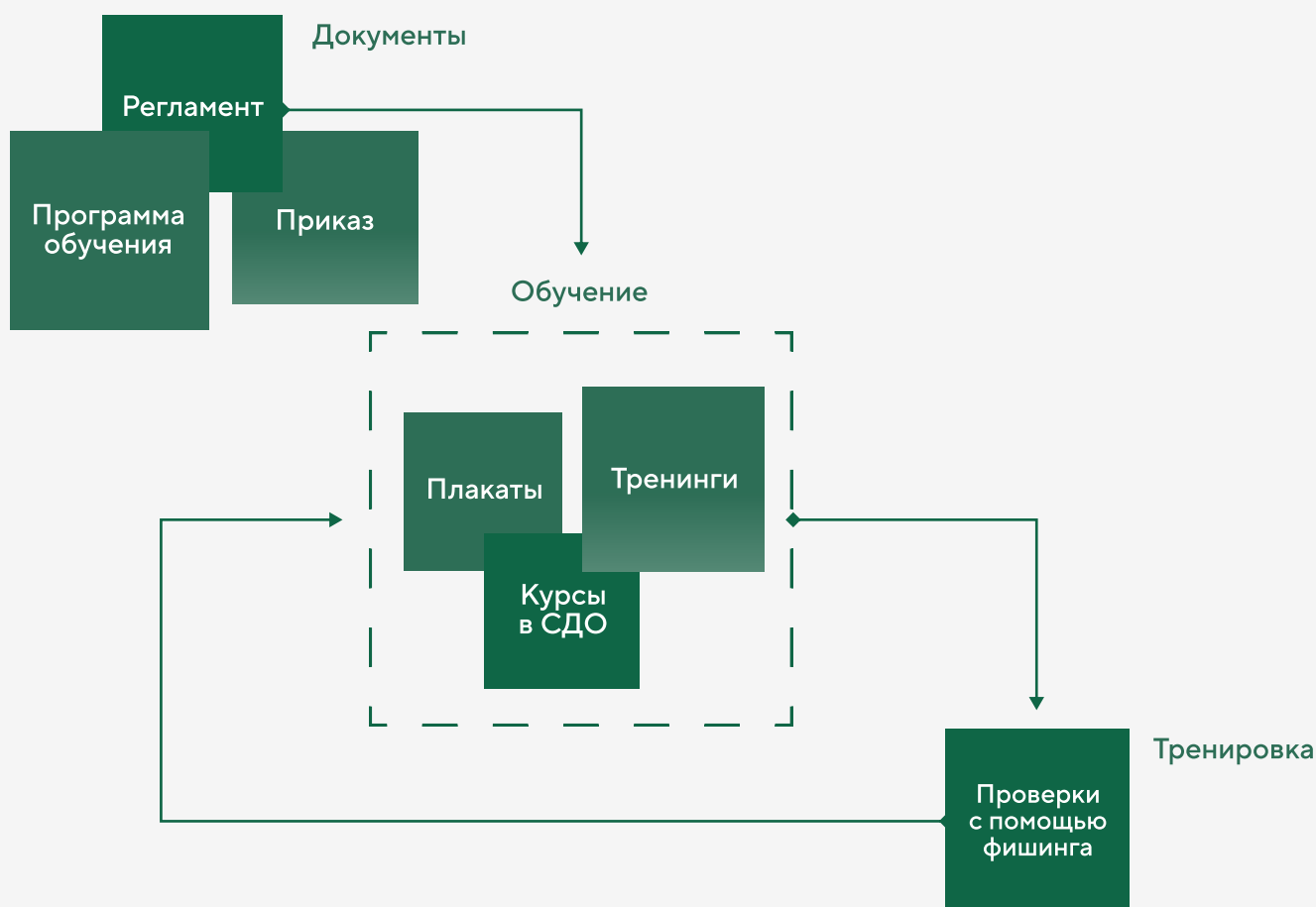


# Чек-лист стратегии по повышению осведомленности в области ИБ: общий трек



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

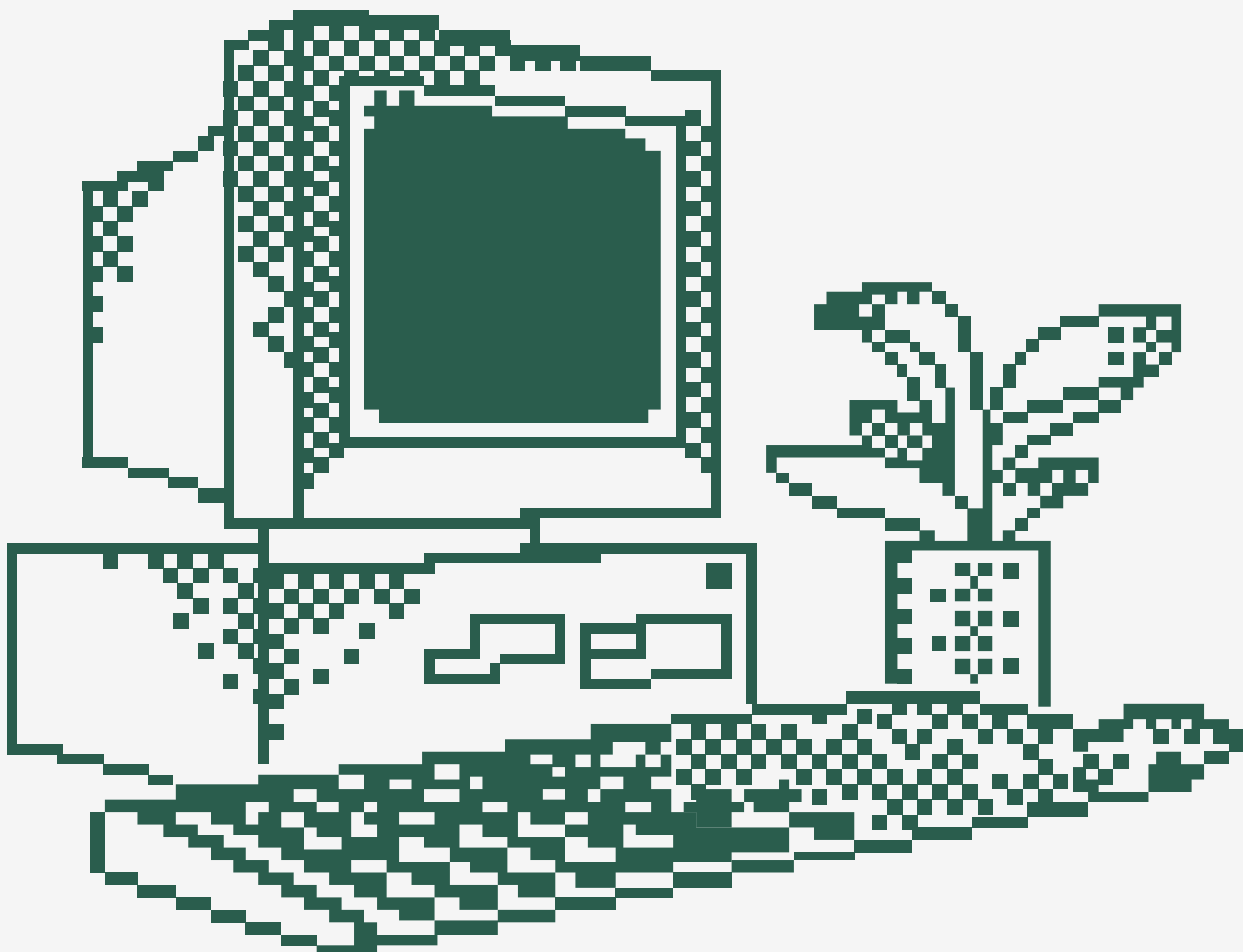
Для организации рекомендуется использовать систему Security Awareness, систему дистанционного обучения или open-source фишинговый тренажер.

#### 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 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;
- Положения ЦБ РФ № 382-П, № 719-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»

### 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. Инцидент 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 2. Регламент по обучению и проверке знаний

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

По результатам обучения должно проводиться тестирование для определения уровня освоения учебного материала. Работники, не набравшие необходимые для успешного прохождения тестирования баллы, должны пройти обучение и тестирование повторно.

С установленной периодичностью отделом «» проводятся проверки осведомленности персонала о правилах безопасной работы, основных угрозах, правилах и проблемах информационной безопасности.

3.4. Профессионально-техническое обучение в области ИБ проводится для работников отдела «».

Сведения о проведенных обучении и инструктажах работников подлежат учету и должны актуализироваться на регулярной основе.

3.5. Повышение осведомленности работников в области ИБ проводится на постоянной основе и включает в себя регулярное информирование об основных угрозах и проблемах безопасности, методиках реагирования на возможные инциденты, изменениях в нормативно-правовых актах и локальных нормативных документах.

### 4. Ответственность

4.1. Требования настоящего Регламента обязательны для выполнения всеми работниками «Компания». В случае нарушения установленных требований работники несут ответственность в порядке, установленном Трудовым кодексом РФ и иными федеральными законами.

4.2. Ответственность за проведение обучения и постоянный контроль выполнения требований настоящего Регламента несет лицо, ответственное за обеспечение информационной безопасности.

Лист ознакомления с Регламентом обучения и повышения осведомленности персонала в сфере информационной безопасности в «Компания»

№ п/п ФИО Должность Дата ознакомления Подпись

| № п/п | ФИО | Должность | Дата ознакомления | Подпись |
|-------|-----|-----------|-------------------|---------|
| 1     |     |           |                   |         |
| 2     |     |           |                   |         |



# 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<br>Персональная ответственность пользователей и соглашение о неразглашении; Охрана коммерческой тайны;<br>Контроль доступа на территорию и правила взаимодействия с посетителями, Использование паролей;<br>Вопросы контроля доступа;<br>Безопасность рабочих мест, Использование сети Интернет;<br>Спам;<br>Правила использования электронной почты |         |      | Курс 2<br>Вопросы социальной инженерии;<br>Появление электронных писем от незнакомых людей и открытие вложений;<br>Защита от вишинга, Использование портативных устройств;<br>Безопасность ноутбуков вне территории организации;<br>Работа из дома и использование корпоративных систем для личных целей, Передача конфиденциальной информации по сети Интернет;<br>Передача информации и оборудования третьим лицам;<br>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<br>Защита от вредоносного ПО;<br>Регулярное обновление корпоративных систем и ПО;<br>Использование лицензионного ПО, Резервное копирование и восстановление информации;<br>Управление инцидентами (кому звонить, что делать);<br>Последствия несоблюдения политики ИБ, Использование корпоративных систем;<br>Использование персонального ПО и АО;<br>Безопасность оборудования от окружающей среды |        |          | Курс 4<br>Распознавание дипфейков; Актуальные угрозы в мессенджерах;<br>Защита персональных данных, Защита конфиденциальной информации;<br>Правила использования электронной почты;<br>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 статистике в будущем он может изменится 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:

$R = 10 * (1 - (a * \Phi + (1 - a) * E))$  где

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 выявил 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

$E = \text{SUM}(T_i) / T_{\text{max}}$  ## от 0 до 1 где

T\_max = SUM(y\_i)

$T_i = d * \max((1 - k * m), 0,5) * y_i$  где

d - признак сданного теста (если сдал, 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\_i - максимальная оценка за тест (пока все y\_i = 1)

# Литература

1. NIST NICE: <https://www.nist.gov/itl/applied-cybersecurity/nice>
2. ENISA: <https://www.enisa.europa.eu/>
3. 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>
4. Security Awareness Program: Project Plan. SANS Security Awareness
5. Cybersecurity training for the real world: <https://www.eccouncil.org/>
6. Elevating Cyber Workforce and Professional Development: <https://www.offsec.com/>
7. Cyber Security Courses, Training, Certifications and Resources: <https://www.sans.org/apac/>
8. Приказы ФСТЭК России № 239, № 17, № 31
9. Указ Президента № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»
10. Федеральные законы: 187-ФЗ, 152-ФЗ, 98-ФЗ
11. ГОСТ 57580.1, ГОСТ Р ИСО/МЭК 27002-2022, ГОСТ Р 56939-2024
12. Положения ЦБ РФ № 382-П, № 719-П
13. ISO/IEC 27001:2013, 27001:2022
14. PCI DSS (Payment Card Industry Data Security Standard)
15. GDPR (General Data Protection Regulation)

# Полезные материалы



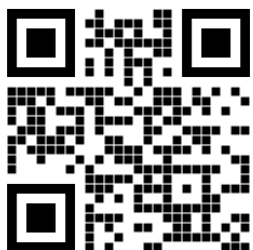
strategy@secure-t.ru

+ 7 (495) 105-54-85

Полезный канал по киберкультуре



Памятка по ИБ для сотрудников



Стратегия: киберкультура для коммерческих организаций

