

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на систему повышения осведомленности и навыков информационной безопасности пользователей

1. Общие сведения

Настоящее техническое задание (далее – ТЗ) определяет функциональные и технические требования к программному обеспечению для повышения осведомленности и навыков кибербезопасности пользователей.

2. Полное наименование системы и ее условное обозначение

Полное наименование: программное обеспечение для повышения осведомленности и навыков информационной безопасности пользователей (далее – Система).

3. Сведения о заказчике

Заказчик: _____

4. Плановые сроки начала и окончания работ

Дата начала: _____

Дата окончания: _____

5. Назначение и цели системы

5.1. Назначение системы

- Повышение уровня осведомленности работников Заказчика в области информационной безопасности и формирование необходимых навыков безопасного поведения в информационном пространстве.
- Формирование культуры информационной безопасности.
- Получение измеримых результатов по итогам обучения работников.

5.2. Цели и задачи Системы

- Снижение рисков информационной безопасности, связанных с небезопасными действиями сотрудников.
- Повышение интереса и участия пользователей в обеспечении информационной безопасности организации.
- Автоматизация процессов повышения осведомленности сотрудников посредством имитации учебных атак и своевременного обучения правилам кибербезопасности.
- Получение измеримых результатов по итогам обучения работников.

6. Требования к Системе

6.1. Общие требования

- Система должна предоставлять веб-интерфейсы для работы администраторов и пользователей.
- Должна быть предусмотрена возможность использования функций Системы без доступа в сеть Интернет.
- Должен поддерживаться вариант развертывания On-Premise.
- Система должна поставляться в формате виртуальных машин и/или в виде дистрибутива, устанавливаемого на поддерживаемую операционную систему.
- Должна предоставляться техническая документация пользователя и администратора Системы.
- Система не должна нарушать работоспособность и целостность других систем Заказчика и должна быть совместима с применяемыми у Заказчика средствами и системами информационной безопасности.
- Консоль администрирования Системы должна функционировать в актуальных версиях Chromium-совместимых браузеров.
- В течение согласованного срока предоставления Системы должны быть доступны обновления программного обеспечения и обучающих материалов.
- Должна быть предусмотрена методология повышения осведомленности пользователей.

6.2. Обучение

- Встроенная LMS и возможность интеграции с LMS Заказчика.
- Личный кабинет пользователя с разделами для обучения и навыков, достижений и сертификатов, а также полезных материалов.
- Отображение назначенных курсов, сроков их прохождения, статусов обучения и прогресса пользователя в личном кабинете.
- Игровые механики повышения вовлеченности: десять уровней пользователей, начисление баллов за успешное прохождение курсов и сообщения о подозрительных письмах, значки достижений, рейтинги пользователей внутри подразделений и по организации, соревнования между подразделениями; возможность исключать выбранные подразделения из рейтингов.
- Возможность редактирования текстов уведомлений LMS.
- Настройка расписания отправки уведомлений в LMS.
- Автоматическая отправка уведомлений пользователям о назначенных курсах.
- Автоматическая отправка уведомлений пользователям с незавершенными курсами и приближающимся сроком окончания обучения.

- Управление порталом обучения через веб-интерфейс и программный интерфейс (REST API).
- Возможность авторизации пользователей без ручного ввода логина и пароля при использовании поддерживаемых механизмов единого входа.
- Возможность интеграции и запуска курсов в iSpring.
- Возможность интеграции и запуска курсов в Equeo.
- Видеоконтент в курсах с примерами реальных атак.
- Голосовое сопровождение контента в курсах.
- Интерактивные модули и элементы в курсах.
- Возможность обновления курсов с учетом появления новых типов атак и актуальных угроз.
- Возможность загрузки произвольного контента в список обучающих материалов.
- Размещение в личном кабинете пользователя памяток, полезных ссылок и файлов, опубликованных администратором; возможность автоматического добавления наименования организации в PDF-файлы полезных материалов.
- Управление внутренними и подключенными внешними курсами из единого интерфейса, включая добавление курсов и перевод неактуальных курсов в архив.
- Электронные обучающие курсы и тесты, доступные без дополнительных плагинов в актуальных версиях браузеров для ПК и мобильных устройств.
- Возможность адаптации курсов и тестов под требования Заказчика.
- Возможность создания шаблонов писем для всех пользователей и отдельных шаблонов для пользователей, систематически допускающих нарушения в определенной области.
- Конструктор курсов с созданием электронных курсов с нуля через веб-интерфейс; поддержка формата слайдов и лонгрида; выгрузка курсов в SCORM для последующего добавления в LMS.
- Возможность отменить или отредактировать назначение обучения.
- Планировщик назначения учебных курсов отдельным пользователям и группам с учетом вложенных групп: немедленное назначение либо назначение на заданные дату и время, в том числе на несколько дат; отображение статусов «Не назначен», «Запланировано», «Назначено».
- Массовое планирование программы обучения из нескольких курсов с настройкой последовательности, интервала отправки в днях и дня недели.
- Настройка при назначении курсов количества попыток прохождения, срока завершения обучения и отправки уведомления пользователю.
- Автоматическое подтверждение прохождения обучающего курса сотрудником с выдачей сертификата и настройкой срока его действия.

- Возможность редактирования шаблона сертификата о прохождении обучающего курса.
- Отображение действующих и истекших сертификатов в личном кабинете пользователя.
- При включении функции проверки прохождения курсов — определение учетной записи Windows и имени компьютера при открытии курса, начале и завершении попытки, сопоставление учетной записи с адресом электронной почты пользователя и ведение журнала проверки. При расхождении прохождения не блокируется, сведения о проверке отражаются в сертификате.
- Наличие предустановленных курсов по вопросам информационной безопасности с возможностью их доработки и корректировки, а также импорта новых курсов в формате SCORM.

Минимальный перечень курсов и тем:

- Вводный курс по четырем основным типам онлайн-атак.
- Базовые правила работы с конфиденциальной информацией в организации.
- Безопасная работа с персональным компьютером в организации.
- Безопасная работа с электронной подписью в организации.
- Безопасное хранение пароля.
- Блокировка экрана компьютера и негативные последствия при нарушении правил работы с ПК.
- Правила информационной безопасности на рабочем месте.
- Выявление вредоносных вложений в официальной переписке.
- Выявление фишинга в официальной переписке.
- Обзор угроз работнику при нарушении регламентов и правил информационной безопасности.
- Обзор сложных многоходовых атак на пользователей и методов формирования доверия.
- Виды маскировки отправителя фишинговых писем и признаки подмены.
- Личная информационная безопасность и угрозы для личных устройств сотрудника, используемых на рабочем месте.
- Мобильная безопасность в личной и корпоративной среде.
- Опасность найденных USB-устройств и типовые сценарии их использования злоумышленниками.
- Признаки подделки официальной переписки и анализ текста письма.
- Политика чистого стола и риски ее несоблюдения.

- Противодействие сценариям с побуждением к самостоятельному поиску вредоносной нагрузки через поисковые системы.
- Базовые правила информационной безопасности в организации.
- Мошенничество в социальных сетях и мессенджерах.
- Безопасность на удаленной работе.
- Эффективное управление паролями.
- Безопасная работа с сайтами и веб-ресурсами.
- Пропускной режим и правила использования бейджей.
- Информационная безопасность для руководителей и иных лиц с повышенными полномочиями или публичным статусом.
- Безопасное использование ИИ в работе, включая риски передачи конфиденциальной информации.
- Интерактивный тренажер по распознаванию фишинга.
- Интерактивный тренажер по атакам в мессенджерах, включая распознавание дипфейков и иных сообщений злоумышленников.
- Обучающая игра по сбору информации, подготовке фишинговой атаки и распознаванию примененных злоумышленником приемов.
- Интерактивный тренажер-квест по выявлению нарушений информационной безопасности в офисных ситуациях.

6.3. Дополнительные возможности

- Загрузка пользователей через XLSX, CSV, TXT, LDAP, LDAPS.
- Автоматическая синхронизация пользователей по протоколу OData V2.
- Произвольная группировка пользователей.
- Возможность исключения пользователя из отдельной группы без удаления его учетной записи из Системы.
- Создание произвольных email-уведомлений для пользователей.
- Выгрузка действий пользователей в кампаниях.
- Сортировка по числовым значениям в таблицах с результатами атак и обучения.
- Произвольная выборка пользователей при назначении кампаний.

- Привязка нескольких фишинговых доменов.
- Разграничение прав доступа для разделения кабинетов и проведения отдельных кампаний по дочерним организациям.
- Проверка прав доступа на стороне сервера при выполнении действий в Системе; ограничение области работы администратора назначенными ему группами пользователей.
- Добавление сертификата для доменов через интерфейс Системы.
- Логирование действий в журнал и syslog.
- Формирование файлов аудита для передачи в системы мониторинга и анализа событий информационной безопасности (SIEM).
- Возможность хранения значений, введенных пользователями в формы учебных фишинговых страниц, в зашифрованном виде при включенной настройке шифрования.
- Ручная отправка напоминаний пользователям с не начатыми или незавершенными курсами.
- Просмотр и изменение назначений по курсам.
- Двухфакторная аутентификация по модели TOTP.
- Интеграция с сервисами, используемыми Заказчиком, при наличии соответствующего API или поддерживаемого протокола.
- Добавление пользовательских полей для разметки и сегментации.
- Вложенные группы с возможностью воспроизведения организационной структуры.
- Создание произвольных полей в карточке пользователя.
- Настройка элементов визуального оформления Системы.
- Создание сегментов на основе действий пользователей.

6.4. Учебные атаки

- Возможность проведения атак, при которых домен фишинговой ссылки отличается от домена отправителя электронного письма.
- Создание фишинговых кампаний со страницы пользователей.
- Планирование расписания учебных атак.
- Пакетная отправка учебных атак с настройкой количества писем в пакете и временного интервала.
- Привязка рассылки учебных атак новой кампании к результатам предыдущих кампаний с сегментацией по инцидентам, статусам обучения и типу атаки.

- Распределение кампаний по группам и пользователям, генерация персонализированного контента и наличие репозитория шаблонов писем.
- Расширенный выбор аудитории учебной кампании путем включения и исключения отдельных пользователей и групп; предварительный подсчет количества включенных, исключенных и фактических получателей с указанием причин исключения, в том числе для кампаний по группам с числом получателей более 1000.
- Каталог готовых сценариев учебных атак, объединяющих учебное письмо, фишинговую страницу и обучающий курс, с возможностью отбора по сложности, курсу и вектору атаки (ссылка, форма, макрос, PDF), а также создания собственных сценариев.
- Создание черновика учебной кампании на основе выбранного сценария с последующим выбором профиля SMTP и получателей.
- Проверка навыков пользователей посредством имитированных атак по электронной почте с использованием различных векторов: ссылки; вложенные файлы не менее 15 типов, включая офисные документы; архивированные вложения; архивированные вложения с паролем, указанным в письме; ввод учетных данных на фишинговых страницах; имитация скачивания вредоносного файла с поддельного сайта.
- Наличие не менее 40 готовых шаблонов учебных писем и не менее 20 шаблонов сайтов.
- Классификация шаблонов учебных писем по типам атак (вредоносная ссылка, файл Word, файл PDF, обучение через LMS, фишинговая форма), поиск и фильтрация по типам и вложениям, предварительный просмотр шаблонов и массовые действия с ними.
- Конструктор для создания учебных фишинговых писем и сайтов.
- Инструменты для переноса структуры сайтов и форм авторизации в учебные сценарии.
- Возможность загрузки сайта учебной фишинговой страницы из ZIP-архива.
- Возможность создания учебных атак с использованием USB- и HID-устройств.
- Возможность генерации ссылок для учебных атак через QR-коды на бумажных носителях.
- Возможность генерации ссылок для таргетированных учебных атак через социальные сети и мессенджеры.
- Возможность настройки отображаемых параметров отправителя электронного письма в рамках разрешенных учебных сценариев.
- Поддержка списков исключений/блокировок для управления учебными кампаниями.
- Автоматизация назначения учебных курсов по заданным правилам.

6.5. Плагины и расширения

- Плагин для отправки уведомлений о подозрительных письмах в службу информационной безопасности, включая сбор исходного сообщения, с поддержкой согласованных почтовых клиентов.
- Поддержка надстройки для отправки сообщений о подозрительных письмах в Microsoft Outlook на macOS и в веб-версии Outlook, а также самостоятельной отправки таких сообщений из почтовых клиентов P7 Органайзер и Thunderbird.
- Синхронизация данных плагина с Системой и учет сообщений о подозрительных письмах в отчетах.
- Расширение для Chromium-совместимых браузеров, уведомляющее подразделение информационной безопасности о вводе учетных данных на фишинговых сайтах.
- Возможность настройки и редактирования текстовых полей, уведомлений и всплывающих сообщений, включая адрес подразделения информационной безопасности, текст подтверждения пользователю и тело сообщения, отправляемого в подразделение информационной безопасности.

6.6. Автоматизация

- Автоматическая синхронизация списка пользователей по LDAP с сохранением иерархии групп.
- Автоматическое назначение руководителей групп по сведениям из каталога LDAP.
- Автоматическое уведомление пользователей о событиях, связанных с обучением: назначении курсов, приближении крайнего срока и необходимости завершить обучение.
- Автоматизация рассылок учебных атак и назначения курсов.
- Автоматическая досылка учебных атак новым пользователям.
- Автоматический выпуск SSL-сертификатов при наличии соответствующей технической возможности.
- Авторизация пользователей в LMS по модели SSO на базе SAML 2.0.
- Автоматическая настройка сервера отправки и приема писем после добавления электронной почты и домена.
- Автоматическая отправка отчетов руководителям подразделений и администратору.
- Формирование автоматических правил по итогам действий сотрудников: назначение обучающих курсов, назначение повторного обучения, включение сотрудников в учебные группы, отправка уведомлений руководителям и по электронной почте.
- Назначение обучающих курсов новым сотрудникам для автоматизации вводного обучения.
- Маркировка новых сотрудников с настройкой периода, в течение которого сотрудник считается новым.

- Уведомление сотрудников службы информационной безопасности о повторяющихся инцидентах.
- Информирование администратора Системы или иных ответственных лиц о срабатывании правила с указанием условий срабатывания и пользователей, попавших под действие правила.
- Поддержка условий автоматизации, включая: переход по ссылке не менее X раз за последние X дней; открытие вложения не менее X раз за последние X дней; заполнение фишинговой формы не менее X раз за последние X дней; обнаружение фишинга при настроенном расширении; добавление сотрудника в Систему за последние X дней.

6.7. Отчетность

- Визуальные отчеты о результатах учебных атак и обучения с отображением динамики.
- Единая аналитическая панель состояния осведомленности с показателями риска пользователей, обучения и учебных фишинговых кампаний за выбранный период, отображением даты актуальности данных, обновлением показателей и пояснениями к методике их расчета.
- Разграничение видимости аналитической панели по ролям: данные всей организации для главного администратора и наблюдателя, данные назначенных групп, включая вложенные, для администратора.
- Отображение среднего риск-балла, его динамики, количества пользователей с высоким уровнем риска и распределения пользователей по уровням риска, а также расшифровка факторов риск-балла для отдельного пользователя.
- Сводные показатели обучения: статусы назначений, ход прохождения курсов, ближайшие сроки завершения и корректирующие назначения по результатам инцидентов.
- Сводные показатели фишинговых кампаний: число кампаний, отправленных писем и инцидентов, доля инцидентов и распределение действий пользователей по видам.
- Статистика по каждой учебной атаке: процент небезопасных действий, количество пользователей, открывших письмо, перешедших по ссылке, выполнивших небезопасное действие с файлом и заполнивших фишинговую форму.
- Статистика по динамике обучения: количество, процент сотрудников, прошедших каждый курс.
- Выгрузка отчетов в CSV, PDF и XLSX.
- Интеграция с SIEM посредством syslog.
- Сводный отчет по состоянию организации.
- Формирование автоматических правил по итогам действий сотрудников.

- Сводный отчет с диаграммами и отслеживанием действий пользователей в кампаниях и курсах: отправлено и открыто писем, переходы по ссылкам, активация PDF, отправка форм, активация макросов, сообщения о фишинге.
- Отчет по кампаниям и группам с разбивкой действий по группам.
- Рейтинг групп по количеству инцидентов на одного сотрудника с численностью группы, общим количеством инцидентов и сравнением с предыдущим периодом; отображение групп с наибольшим риск-баллом с учетом вложенных групп.
- Отдельные списки инцидентов по группам и пользователям с выбором периода, поиском, сортировкой по столбцам и постраничным просмотром.
- Отчет по обучению со статусами пользователей по темам курсов: назначено, пройдено, не пройдено, просрочено, не начато.
- Отчет по уровню риска пользователей и групп.
- Аналитические показатели зрелости: соотношение сообщений сотрудников о фишинге и инцидентов, охват сотрудников учебными симуляциями, количество повторно допускающих небезопасные действия пользователей и доля приходящихся на них инцидентов.
- Анализ воронки учебных кампаний по этапам доставки писем, открытия, перехода по ссылке и заполнения формы с отдельным учетом сообщений о фишинге; анализ изменения распределения пользователей между уровнями риска за период.
- Анализ скорости реакции на учебную атаку: медианное время от доставки письма до первого перехода по ссылке и до первого сообщения о фишинге.
- При наличии LMS — показатели эффекта обучения и повторных инцидентов после прохождения курсов для сопоставления результатов обучения с поведением пользователей в учебных атаках.
- Статистика обучения за выбранный период с разделением по источникам данных (встроенная LMS и подключенные iSpring, WebTutor, Эквио), графиком динамики культуры информационной безопасности и показателями по пользователям.
- Возможность ведения администратором заметок и отображения выбранных заметок отметками на графике динамики культуры информационной безопасности.
- Автоматическая отправка отчетов за заданный период по электронной почте.
- Настройка правил отслеживания действий пользователей и отправки уведомлений администратору.
- Отправка отчетов по заданным правилам.
- Панель операционных событий с отображением количества активных расписаний отчетов и автоматических правил, даты следующего отчета и времени последней проверки правил.

- Быстрый переход с аналитической панели к назначению обучения, созданию кампании, запуску учебной темы, списку просроченных курсов, последней кампании и настройке отчета при наличии соответствующего модуля и прав доступа.

6.8. Требования к технической поддержке

- Техническая поддержка должна предоставляться в течение согласованного срока использования Системы.
- Обращения в техническую поддержку должны приниматься через систему HelpDesk и/или электронную почту.
- Срок первичного ответа на обращение в техническую поддержку – не более 24 часов, если иное не установлено условиями закупки или договором.
- Исполнитель должен обеспечивать актуальность документации по Системе и предоставлять сведения о поддерживаемых версиях программного обеспечения.

6.9. Требования к ИТ-инфраструктуре

- Поддерживаемые операционные системы: Ubuntu Server 22.04 и выше, Astra Linux, Debian 12 и/или иные ОС, согласованные с Заказчиком.
- Выделенный объем оперативной памяти: от 4 ГБ или в соответствии с расчетом ресурсов для заявленного количества пользователей.
- Свободное место на диске: от 50 ГБ или в соответствии с расчетом ресурсов.
- 64-разрядный (x64) процессор с тактовой частотой от 2 ГГц или эквивалентной производительностью.

7. Сервисное сопровождение

- По запросу подготовка периодических отчетов для Заказчика с необходимыми метриками по результатам учебных атак и обучения.
- Подбор и приоритизация актуальных векторов учебных атак с учетом целей и профиля рисков организации.
- Планирование расписания учебных атак.
- Проведение многоуровневых учебных атак по отдельным группам пользователей в пределах согласованных объемов.
- Актуализация обучающих материалов с учетом внутренних регламентов информационной безопасности Заказчика.
- Настройка и адаптация сценариев повышения культуры информационной безопасности пользователей.

- Разработка сценариев работы с пользователями, которые не проходят обучение или игнорируют сообщения службы информационной безопасности.
- Отправка внеплановых курсов по индивидуальному расписанию.
- Возможность применения микро-курсов для сотрудников, допустивших небезопасное действие в ходе учебной атаки.

8. Требования к приемке и проверке соответствия

Соответствие Системы требованиям настоящего ТЗ рекомендуется подтверждать демонстрацией заявленных функций, предоставлением технической документации и проведением согласованных приемочных испытаний.

Перечень функций, подлежащих обязательной проверке, сроки и критерии приемки следует определить Заказчику до заключения договора.

9. Приложения и сведения для адаптации

- Количество пользователей: _____
- Количество администраторов: _____
- Требуемый вариант развертывания: _____
- Используемая ОС: _____
- Используемая LMS: _____
- Требования к интеграциям: _____
- Требования к срокам поддержки: _____
- Требования к отчетности: _____
- Дополнительные требования: _____