**ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ**

**закупаемой услуги по повышению осведомленности в области кибербезопасности**

**1. Заказчик:**

ГУ «Отдел внутренней политики акимата Житикаринского района»

**2. Цель работы:**

Предоставление услуги по повышению осведомленности сотрудников

ГУ «Отдел внутренней политики акимата Житикаринского района» в области кибербезопасности.

**3. Представитель Заказчика по согласованию и утверждению необходимых документов:**

Руководитель отдела внутренней политики акимата Житикаринского района;

Главный специалист отдела внутренней политики акимата Житикаринского района (по письменному уведомлению).

**4. Название курса:**

Основы кибербезопасности.

**5. Содержание услуги:**

Повышение осведомленности сотрудников ГУ «Отдел внутренней политики акимата Житикаринского района».

**6. Цель Курса:**

Дать общее представление о безопасности в информационном обществе, и на этой основе сформировать понимание технологий информационной безопасности и умение применять правила кибербезопасности во всех сферах деятельности.

**7. Пользователи курса:**

Сотрудники ГУ «Отдел внутренней политики акимата Житикаринского района».

**8. Формат подачи учебной информации разрабатываемого электронного курса:**

Теоретический материал курса будет представлен в следующих форматах:

* интерактивные слайды;
* обучающие видео.

Практический материал курса будет представлен в следующих форматах:

* интерактивные упражнения;
* тесты.

Структура курса - линейная.

Язык обучения - русский

**9. Информационная структура курса**

|  |  |
| --- | --- |
| **Наименование темы** | **Приобретаемые знания/навыки** |
| Введение в информационную безопасность | * Знать законодательные требования
* Осознавать уровень личной ответственности за нарушение кибербезопасности
 |
| Безопасность паролей | * Уметь создавать надежные пароли и хранить их
 |
| Безопасность при работе с электронной почтой | * Уметь распознавать фишинговые письма и знать, как реагировать на них
 |
| Фишинговые сайты | * Уметь распознавать фишинговые сайты
 |
| Безопасность при посещении страниц Интернет/Безопасность в сети Интернет | * Уметь распознавать веб-страницы
 |
| Антивирусная защита | * Знать как обезопасить устройство от вредоносных программ
 |
| Социальная инженерия | * Знать техники социальной инженерии и способы реагирования
* Знать распространенные мошеннические схемы с использованием дипфейка
 |
| Безопасность при работе с социальными сетями | * Знать как безопасно пользоваться социальными сетями
 |
| Безопасность в офисе | * Знать правило “чистого стола”
 |
| Безопасность при работе с корпоративной информациейв публичных сетях | * Знать о возможных последствиях обсуждения корпоративной информации с третьими лицами (коллегами, родственниками, друзьями)
* Знать основы безопасной работы с корпоративной информацией

в публичных сетях |
| Обеспечение конфиденциальности информации | * Знать основы защиты персональных и корпоративных данных
 |
| Правила защиты мобильных устройств | * Знать основные признаки взлома устройства и как действовать
* Знать основные правила защиты мобильных устройств
 |
| Физическая защита, блокировка и поиск потерянных устройств | * Знать как действовать, в случае потери или кражи устройства
 |
| Повышение культуры безопасности | * Понимать важность поддержания культуры безопасности
 |

Дополнением к курсу будет симуляция фишинговых рассылок на почтовые адреса сотрудников ГУ «Отдел внутренней политики акимата Житикаринского района».

При успешном завершении обучения, ГУ «Отдел внутренней политики акимата Житикаринского района» будет выдан сертификат о прохождении курса.

**10. Функциональные требования**

Курс будет воспроизводиться на системе дистанционного обучения (Система), которая предоставляет следующие возможности:

* Система должна предоставлять доступ к учебным материалам курса через веб-браузер без установки стороннего ПО (Flash, Java, ActiveX и подобные) и быть доступна по протоколу HTTP или HTTPS;
* Система должна иметь возможность соединения со службами каталогов LDAP для синхронизации пользователей, групп пользователей и аутентификации пользователей;
* Система должна предоставлять возможность настройки структуры курса, его материалов и активностей;
* Система должна предоставлять возможность интеграции со сторонними сервисами для проведения вебинаров;
* Система должна запоминать этап прохождения курса и давать возможность пользователю продолжать с места остановки;
* Система должна иметь отчеты о статусе прохождения курса слушателями;
* Система должна предоставлять возможность тестирования только по 100% прохождению лекции и ограниченное количество попыток;
* Система должна предоставлять возможность проходить тестирование независимо от статуса прохождения лекции;
* Система должна иметь возможность формирования и использования банка вопросов;
* Система должна иметь возможность случайной выборки вопросов теста для исключения одинакового состава вопросов в попытках;
* Система должна иметь возможность показа вопросов теста в случайном порядке;
* Система выдает результаты тестирования автоматически после завершения тестирование и не дает возможность исправить результат;
* Система должна иметь встроенные промежуточные отчеты по статусу прохождения тестирования среди всех слушателей курса.
* Система должна предоставлять возможность формировать учебные группы и потоки;
* Система должна иметь возможность записать группу пользователей на курс;
* Система должна иметь отчет по прогрессу прохождения курса группой слушателей - процент прохождения курса каждым слушателем и график прогресса группы по дням;
* Система должна иметь функцию симуляции фишинговых атак;
* Система должна иметь функцию настройки шаблона фишинговой страницы;
* Система должна иметь функцию настройки шаблона фишинговой рассылки;
* Система должна иметь функцию настройки профиля email-рассылки с указанием почтового сервера и отправителя;
* Система должна иметь возможность создания фишинговой кампании с выбором шаблонов фишинговой страницы, рассылки, профиля рассылки и группы пользователей.
* Система должна отслеживать как минимум следующие статусы фишинговой кампании: письмо отправлено пользователю, письмо открыто пользователем, пользователь перешел на фишинговую страницу, пользователь отправил персональные данные;
* Система должна иметь возможность автоматически зачислить пользователя на курс по фишингу в случае если он отправил персональные данные в фишинговой симуляции;
* Система должна предоставлять интерактивный отчет (дэшборд) с информацией по запущенным компаниям в разрезе статусов, как в общем, так и по каждому пользователю;
* Система должна предоставлять возможность создания, запуска и контроля сценариев - выполнение назначенных действий на возникновение определенного события;
* Система должна предоставлять преднастроенные сценарии и возможность создания пользовательских сценариев;
* Система должна предоставлять возможность запуска, приостановки и удаления (архивирования) сценариев;
* Система должна позволять настраивать параметры событий и действий в рамках сценария;
* Система должна уметь обрабатывать событие зачисления пользователя на курс;
* Система должна уметь обрабатывать событие окончания срока доступа к курсу;
* Система должна уметь обрабатывать событие, когда до окончания срока доступа к курсу осталось менее Х часов;
* Система должна уметь обрабатывать событие регистрации нового пользователя в системе;
* Система должна уметь обрабатывать событие выполнения активности курса Х часов назад;
* Система должна уметь обрабатывать событие завершения курса Х часов назад;
* Система должна уметь обрабатывать событие не завершения курса в срок;
* Система должна уметь обрабатывать событие, когда обучающийся не сдал тест (не набран проходной балл);
* Система должна уметь обрабатывать событие передачи персональных данных в фишинговой симуляции;
* Система должна уметь обрабатывать внешние события, возникающие во внешних информационных системах;
* Система должна позволять, в рамках сценария, выполнить отправку настраиваемого уведомления (электронная почта, внутреннее) при срабатывании определенного события;
* Система должна позволять, в рамках сценария, выполнить отправку обобщенного уведомления (по всем затронутым в событии пользователям) при срабатывании определенного события;
* Система должна позволять, в рамках сценария, выполнить зачисление пользователя на определенный курс;
* Система должна позволять, в рамках сценария, выполнить запуск фишинговой симуляции;
* Система должна позволять, в рамках сценария, выполнить блокировку учетной записи пользователя в Active Directory;
* Система должна вести журнал событий сценариев;
* Система должна вести в журнале событий сценариев учет времени возникновения события, вовлеченного пользователя, контекст события, а также подробного описания действия;
* Система должна позволять фильтровать журнал событий сценариев по типу сценария, конкретного сценария, конкретного события, конкретного действия, конкретного пользователя, а также указанному периоду;
* Система должна предоставлять аналитическую панель (дашборд) по выполнению сценариев, с информацией по количеству запусков сценариев, успешности выполнения, среднего времени выполнения. А также должна быть возможность фильтровать по типу сценария, конкретного сценария и периода;

У каждого сотрудника будет логин и пароль для входа в СДО и начала обучения.

Сотрудник должен будет заполнить профиль и начать изучение курса.

**11. Требования к техническим характеристикам**

Для воспроизведения мультимедийного курса, персональный компьютер сотрудника должен соответствовать следующим программным конфигурациям:

* Операционные системы MS Windows 7 и выше;
* Браузер: Internet Explorer 8.0 /Mozilla Firefox 2.0 (или более поздние версии), Google Chrome, Yandex и т.д.;
* MS Office 200x и другое программное обеспечение, необходимое для просмотра дополнительных документов курса;
* Персональные компьютеры не должны использовать беспроводные модемы (2,3,4G) для подключения к интернету для лучшего воспроизведения курсов
* Рекомендация по пропускной способности канала: 100 Мб/сек

**12. Требования к Исполнителю**

1) Иметь как минимум 1 (одного) специалиста с сертификатом от вендора (производителя), подтверждающего возможность обслуживания и сопровождения системы;

2) Иметь авторизационное письмо о партнерском статусе от вендора.

3) Потенциальный поставщик должен обладать опытом поставки товара или услуг не менее одного завершенного договора по закупке аналогичных товаров ил услуг предшествующий текущему году.

Настоящая Техническая спецификация составлена в 2 (двух) экземплярах на русском языке, имеющих одинаковую юридическую силу, один из которых подлежит передаче Поставщику, а второй – хранится у Заказчика.