ООО «АВАТЕК»
677000, Республике Саха (Якутия),
г. Якутск, 202-й микрорайон, 12, корп. 2
тел. 8 (4112) 31-80-31
ИНН 1435293280, ОГРН 1151447003289

AVAREANGE

Документация, содержащая описание функциональных характеристик экземпляра программного обеспечения, предоставленного для проведения экспертной проверки

2024

1. Термины и определения

В настоящем документе используются следующие термины и сокращения:

- Владелец (Holder) - представитель компании, которая приобрела услуги системы AVAREANGE. Владелец выполняет роль главного руководителя и отвечает за организацию процесса обучения сотрудников внутри своей компании;
- Участник (Participant) - пользователь системы, который активно участвует в обучении и тестировании. Принимает участие в образовательных программах, таких как курсы, тесты и кампании, назначенные Владельцем;
- Гость (Guest) - пользователь, который имеет доступ к публичной части сайта системы AVAREANGE, но не зарегистрирован и не имеет доступа к функциональности, предназначенной для Владельцев и Участников;
- Фишинговая кампания (Campaigns) - учебное мероприятие, симулирующее реальные фишинговые атаки, с целью тестирования навыков сотрудников в области кибербезопасности;
- Курс (Course) - серия учебных занятий с расписанием, направленных на обучение линейного персонала организации по темам кибербезопасности;
- Тест (Test) - один из атрибутов курса или отдельная сущность, предназначенная для проверки знаний. Тест может быть связан с темой курса или использоваться для оценки знаний по другим темам в системе;
- Сертификат (Certificate) - документ, подтверждающий успешное завершение курса;
- Геймификация (Gamification) - внедрение игровых элементов в процесс обучения для повышения мотивации и вовлеченности участников;
- Статусы испытаний (Test status) - показатели, отражающие уровень успешности сотрудника в прохождении фишинговых симуляций;
- Ачивки (Achievements) - виртуальные награды, которые сотрудники получают за успешное прохождение тестов.

2. Назначение документа

Настоящий документ описывает функциональные характеристики программного обеспечения платформы AVAREANGE и предназначен для ознакомления с основными функциями и возможностями системы.

3. Уровень подготовки пользователей

Для работы с платформой AVAREANGE пользователям не требуется специальное обучение. Достаточно базовых навыков, включающих:

- уверенное владение персональным компьютером и умение работать с операционными системами (использование клавиатуры и мыши, управление окнами и приложениями, работа с файловой системой);
- знание основ работы с веб-браузерами (настройка типичных параметров, подключение к интернету, переход на веб-сайты, навигация, заполнение форм и работа с другими интерактивными элементами веб-интерфейсов).

4. Требования к рабочей станции пользователя

Для работы с платформой AVAREANGE пользователю необходимо иметь стабильное подключение к сети Интернет, его компьютер должен соответствовать системным требованиям, указанным в таблице 1, и использовать один из рекомендуемых современных веб-браузеров, указанных в таблице 2

Таблица 1 – Рекомендованные системные требования

	Рекомендуемые требования
Процессор	Тактовая частота 2,3 ГГц и выше
Оперативная память	DDR4 от 8 Гб и более
Операционная система	Windows 8/ 8.1 / 10, MacOS 10.11 и новее

Таблица 2 – Список подходящих для работы браузеров

Компонент	Конфигурация
Браузер	Google Chrome 80+, Yandex Browser 20+, Mozilla Firefox 73+, Microsoft Edge 80+, Opera 67+

5. Общие положения

Платформа для повышения кибербезопасности сотрудников компаний AVAREANGE (далее – платформа, AVAREANGE) предназначена для использования уполномоченными сотрудниками компаний и организаций, заинтересованных в снижении рисков, связанных с киберугрозами, и в повышении уровня осведомленности сотрудников о методах защиты от фишинговых атак.

Цель работы платформы состоит в проведении оценки киберрисков организации, предоставлении обучающих материалов по кибербезопасности и в тестировании навыков сотрудников в условиях имитации реальных угроз.

Потенциальными пользователями платформы AVAREANGE являются сотрудники компаний, соответствующие следующим требованиям:

- Занимаются поддержкой информационной безопасности в компании;
- Несут ответственность за защиту данных, управление киберрисками и контроль доступа к корпоративным системам;
- Отвечают за повышение квалификации и обучение сотрудников в области защиты данных и киберугроз;
- Обладают необходимыми знаниями для управления процессом обучения в сфере информационной безопасности;
- Знакомы с процедурами идентификации, обработки и устранения фишинговых и других киберугроз;

6. Функциональные возможности системы

Процесс подачи заявок и управления доступом:

- Подача заявки: Гостевой пользователь подает заявку на доступ. После ее обработки Владелец получает временные учетные данные для входа и проходит процедуру первичной настройки.

Административное управление (для Владельцев):

- Онбординг: Введение во все основные разделы и функции системы при первом входе в платформу;
- Управление структурой и пользователями: Добавление участников в платформу, создание отделов и распределение пользователей по подразделениям.

Образовательный контент:

- Курсы: Поддержка создания курсов с уникальным материалом (PDF, видеоконтент) и фишинговыми испытаниями, а также возможность использования системных курсов для назначения участникам;
- Тесты: Возможность создания собственных тестов, включая настройку типов вопросов и минимального порога прохождения, или использование системных тестов для назначения участникам.

Фишинговые кампании и микротренинги:

- Настройка кампаний по фишинговым испытаниям: Создание фишинговых кампаний с использованием системных шаблонов, настройка условий успеха, частоты отправки писем, временной зоны и других параметров;
- Микротренинги: Автоматическое назначение коротких обучающих тестов после неудачного прохождения фишингового испытания для повышения уровня знаний участников.

Прохождение обучения и кампаний (для Участников):

- Доступ к назначенному контенту: Участники получают доступ к назначенным курсам и тестам в личном кабинете;
- Уведомления о назначениях: Участники получают уведомления о новых курсах и тестах;

- Прохождение курсов и тестов: Обучение через образовательные материалы и тестирование знаний, где успех или неудача фиксируются в общей статистике;
- Участие в фишинговых кампаниях: Прохождение фишинговых испытаний, назначенных Владельцем, для оценки уровня подготовки к реальным киберугрозам;
- Получение микротренингов: Автоматическое назначение кратких обучающих тестов при неудачном прохождении фишингового испытания для повышения устойчивости к атакам.

Дашборд и статистика:

- Владелец мониторит прогресс по курсам, тестам и фишинговым кампаниям в режиме реального времени;
- Поддержка вывода статистики по назначенным задачам, прогрессу и результатам в диаграммах на дашборде;
- Статусы испытаний: Показатели, отражающие уровень успешности сотрудников в прохождении фишинговых симуляций. Владелец видит количество участников с различными статусами испытаний;
- Ачивки: Виртуальные награды, которые сотрудники получают за успешное прохождение тестов. Под каждой ачивкой отображается количество участников, которые ее имеют на данный момент.

Геймификация обучения (для Участников):

- Первичный тест оценки знаний: Участник проходит тест и получает ачивку, влияющий на доступность курсов и тестов;
- Статусы испытаний: Участники получают уровни в зависимости от успешности прохождения фишинговых симуляций и тестов, что мотивирует их к повышению квалификации;
- Отслеживание прогресса: Участник видит статистику по завершенным курсам, тестам и микротренингам;
- Сертификаты за успешное прохождение курсов: В случае успеха Участник получает электронные сертификаты, доступные для скачивания.

Редактирование и управление данными пользователей:

- Владелец может обновлять информацию о пользователях и отделах (должности, отдел);
- Участники имеют возможность редактировать свои данные (ФИО, аватар) через личный кабинет.

7. Входные данные

- Информация о сотрудниках (ФИО, должность, email и т.д.);
- Содержание курсов и тестов (загружаемые файлы для курсов и вопросы тестов);
- Настройки фишинговых кампаний.

8. Выходные данные

- Информация о прогрессе пользователей по курсам, тестам и фишинговым кампаниям, доступная для Владельца;
- Данные о полученных ачивках пользователями и их успехах в прохождении фишинговых испытаний;
- Электронные сертификаты, подтверждающие знания в области кибербезопасности.

Служба технической поддержки

Если у вас возникли вопросы по работе платформы AVAREANGE или любые технические проблемы, Вы можете обратиться в нашу службу технической поддержки.

Адрес: Республика Саха (Якутия), Якутск, мкр. 202 корпус 12/2 (9:00 – 18:00, UTC+9:00)

Контактный телефон: +74112318031

Электронная почта: help@avareange.ru

Telegram-бот: https://t.me/AvareangeBot

WhatsApp-бот: +7 (914) 101-93-33