



ANGARA

professional assistance

ANTIFISHING

**Повышение осведомленности
работников по информационной
безопасности**

WWW.ANGARAPRO.RU

Антифишинг – это информационная система непрерывного обучения и контроля защищенности сотрудников компании. Она является «облачным» решением и позволяет через web-интерфейс работать в единой системе как пользователям, так и администраторам.

ПРЕИМУЩЕСТВА РЕШЕНИЯ

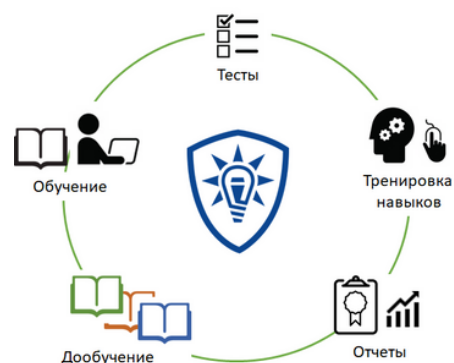
- Снижение рисков ИБ.
- Решение задач в области повышения знаний сотрудников в вопросах ИБ.
- Снижение числа типовых нарушений информационной безопасности.
- Формирование у сотрудников понимания важности действующих мер по ИБ.
- Автоматизация процессов выявления низкой осведомленности сотрудников, выстраивание процесса обучения.
- Предустановленный набор отчетов и возможность их доработки под имеющиеся особенности бизнеса.
- Поддержка собственного программного интерфейса (REST API), который позволяет управлять всеми заявленными функциями и получать всю статистику по работе решения.
- Наличие реализованной интеграции с системами класса IR (Incident Response) или SGRC (Security Governance, Risk Management and Compliance).
- Собственный портал обучения.

ОСОБЕННОСТИ ПОРТАЛА

Портал обучения содержит предустановленные курсы по вопросам ИБ, которые можно дорабатывать и корректировать, а также создавать новые курсы, в зависимости от специфики бизнес-процессов и действующих регламентов ИБ.

Предустановленные курсы по вопросам ИБ включают следующие темы:

- Базовый курс (угрозы, ответственность, работа с паролями и конфиденциальной информацией, реагирование на инциденты).
- Безопасная работа в интернете и с электронной почтой (спам и целевой фишинг, email, психологические приемы).
- Мобильная безопасность (взлом устройств, работа с приложениями, физическая защита, блокировка и поиск потерянных устройств).
- Индивидуальные планы обучения.



- 🛡️ Физическая безопасность (кража пропуска, проход в офис посторонних, неформальное общение с коллегами).
- 🛡️ Безопасная удаленная работа (работа через мобильный интернет, использование VPN, проверка сертификатов сайтов).

ВЕРСИИ АНТИФИШИНГА

Base:

- 🛡️ Версия подойдет компаниям, в которых не было организованных процессов обучения и тренировок сотрудников.
- 🛡️ Базовая функциональность платформы для имитации атак и контроля защищенности сотрудников.
- 🛡️ Изменение рейтингов сотрудников.
- 🛡️ Имитация атак через электронную почту со ссылками и файлами.
- 🛡️ Имитация атак через имитированные фишинговые сайты.
- 🛡️ Базовый набор обучающих курсов Антифишинга.
- 🛡️ Базовая функциональность определения уязвимых программ, плагинов и фреймворков на стороне пользователей.

STD:






- 🛡️ Имитация атак через съемные устройства (**HID**).
- 🛡️ Ежеквартальная разработка до 5 целевых шаблонов атак по актуальным векторам, фишинговых страниц и другого контента для проверки навыков сотрудников.
- 🛡️ Ежеквартальные обновления обучающих курсов.
- 🛡️ Ежеквартальные обновления правил определения уязвимых программ, плагинов и фреймворков на стороне пользователей.
- 🛡️ Базовые правила автоматизированного управления процессами обучения и контроля защищенности на основе методологии Антифишинга.
- 🛡️ Базовая функциональность учета обратной связи от сотрудников и отображения ее в рейтинговой модели Антифишинга.
- 🛡️ Программный интерфейс Антифишинга (**REST API**) для интеграции, управления и получения данных из любых внешних систем.
- 🛡️ Модуль интеграции с системой обучения ВебТьютор и Moodle.
- 🛡️ Многопользовательский режим Антифишинга, парольная политика, таймауты для выхода из системы и блокировки при множественных попытках входа.

ENT:

-  Ежеквартальные обновления обучающих курсов и тестов.
-  Ежемесячные информационные дайджесты по безопасности.
-  Имитация атак через съемные устройства (накопители).
-  Имитация атак через прием ответных исходящих писем от сотрудника.
-  Имитация атак через загрузку и запуск вредоносных файлов.
-  Имитация атак через загрузку и установку браузерных плагинов.
-  Плагин для почтовых программ MS Office.
-  Сбор и хранение действий администраторов системы.
-  Ежеквартальная актуализация базы уязвимых приложений и правил автоматизации.
-  Автоматизация импорта и синхронизация сотрудников из LDAP с учетом структуры компании.

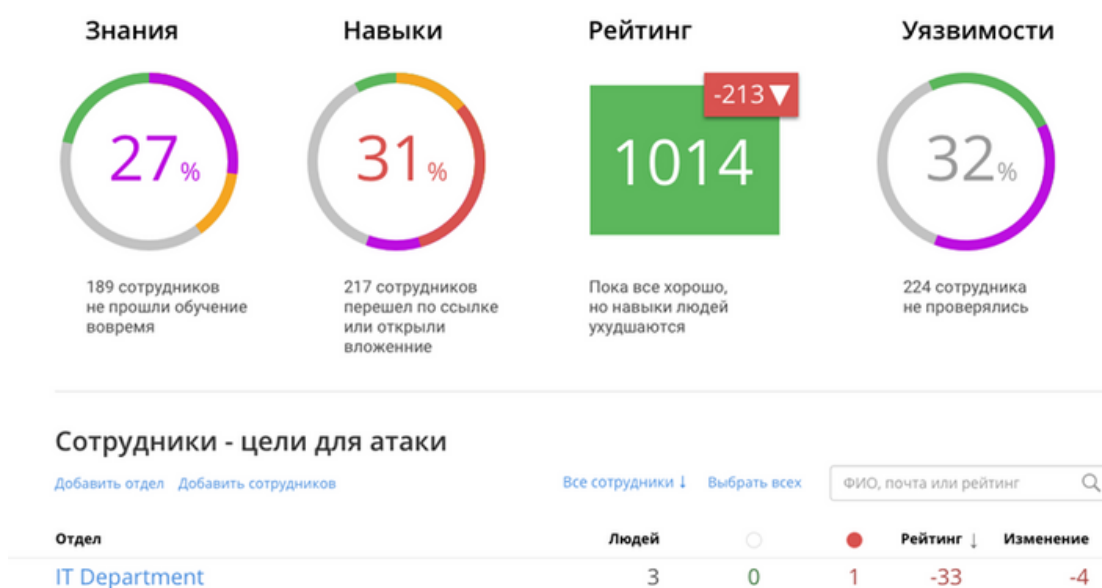
Также подготовлена англоязычная версия Антифишинга, переведены курсы и тесты, шаблоны имитированных атак и ежемесячные закрытые дайджесты.

ОСОБЕННОСТИ ОПРЕДЕЛЕНИЯ УЯЗВИМОСТЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

-  Наличие функций определения версий браузеров, плагинов, офисных программ, операционных систем, включая мобильные версии, у тех сотрудников, которые совершают небезопасные действия, а также программных уязвимостей в версиях указанного ПО.
-  Классификация уязвимостей в соответствии с рейтингом CVSS.
-  Учет уязвимостей в статистике небезопасных действий по сотрудникам и в отдельном разделе решения.
-  Возможность отметить уязвимости как исправленные и исключить их из статистики.
-  Обновляемая база и правила определения уязвимостей.

ШИРОКИЕ ВОЗМОЖНОСТИ ФУНКЦИОНАЛА ОТЧЕТОВ

- 🛡️ Статистика по каждой выполненной имитированной атаке.
- 🛡️ Статистика по отделам, выбранным сотрудникам.
- 🛡️ Статистика по всем уязвимостям ПО с детализированными данными.
- 🛡️ Возможность выгружать отчеты в формате XLSX.
- 🛡️ Наличие журнала с каждым небезопасным действием.



АЛГОРИТМ ОКАЗАНИЯ УСЛУГИ

Подготовка. Заказчик загружает в систему необходимое количество e-mail сотрудников, которые будут проверяться на осведомленность по ИБ при помощи фишинговых рассылок. С нашей стороны предоставляется логин и пароль для доступа к платформе Антифишинг для администратора системы. Далее Заказчику предлагается три сценария атаки на согласование. Как только сценарии утверждены, заказчику направляются шаблоны данных атак. После их согласования мы загружаем их в платформу Антифишинг. Далее сотрудник ИБ в планировщике атак выбирает шаблон атаки, сотрудников и даты фишинговой атаки.

Проверка пользователей. Антифишинг, притворяясь нарушителем, отправляет электронные письма с различными ловушками и оценивает действия пользователя.

Обучение. Если пользователь «попался», то система фиксирует его действия и подбирает для него индивидуальную обучающую программу, направляя уведомление об этом ответственному руководителю.

Тестирование. По итогам обучения программа тестирует пользователя.

БИЗНЕС-МИШЕНИ ФИШИНГОВЫХ АТАК Q1 2019 (%)



ИСТОЧНИК KASPERSKY LAB



ANGARA

professional assistance

Контакты

**121096, г. Москва, ул. Василисы Кожиной,
д.1, к.1. БЦ «Парк Победы»
Телефон/факс: +7 (495) 269 26 07
E-mail: info@angarapro.ru**

WWW.ANGARAPRO.RU