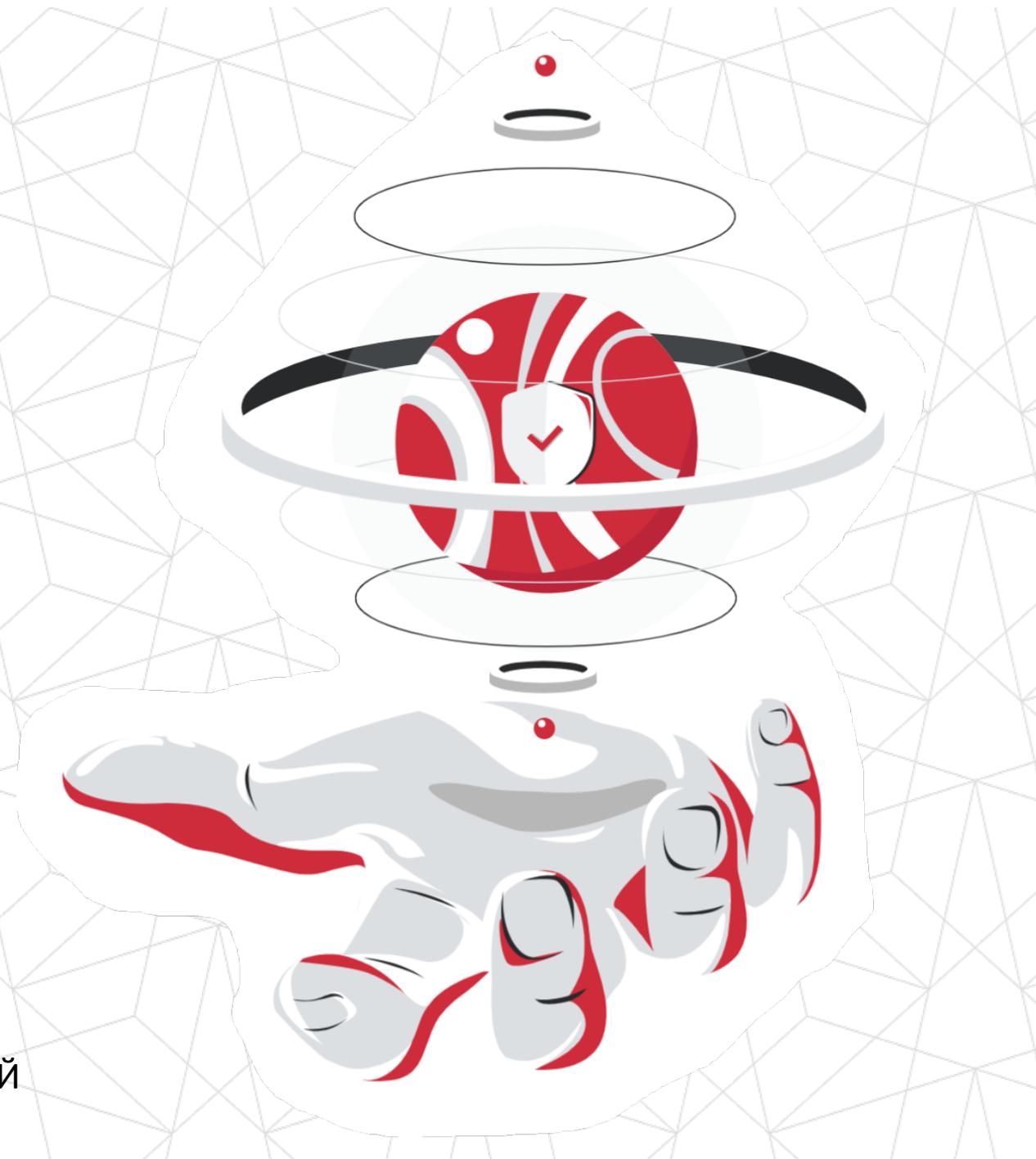




КИБЕРГРАМОТНОСТЬ
СОТРУДНИКОВ И
АВТОМАТИЗАЦИЯ
ПРОЦЕССА ОБУЧЕНИЯ



СИСТЕМА ПОВЫШЕНИЯ ОСВЕДОМЛЁННОСТИ ПОЛЬЗОВАТЕЛЕЙ



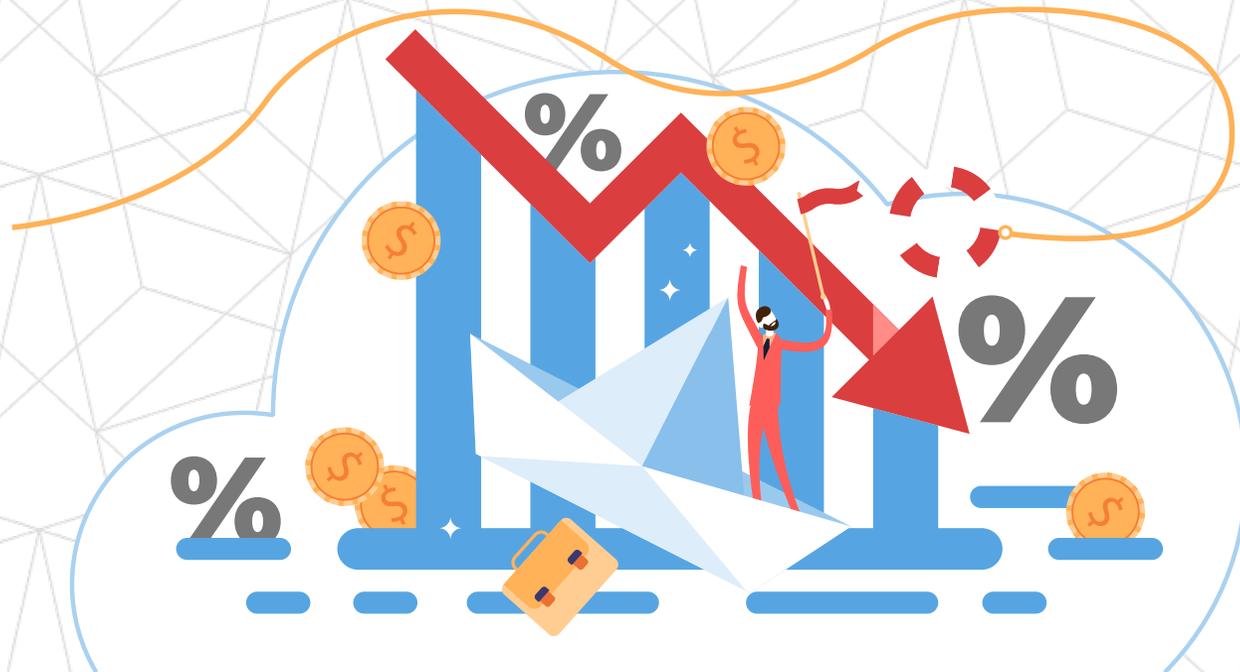
Слабая осведомленность
пользователей в вопросах ИБ



Крайне высокий риск возникновения
инцидентов социальной инженерии



Значительные финансовые
и репутационные потери
для организации





Кого именно обучать?



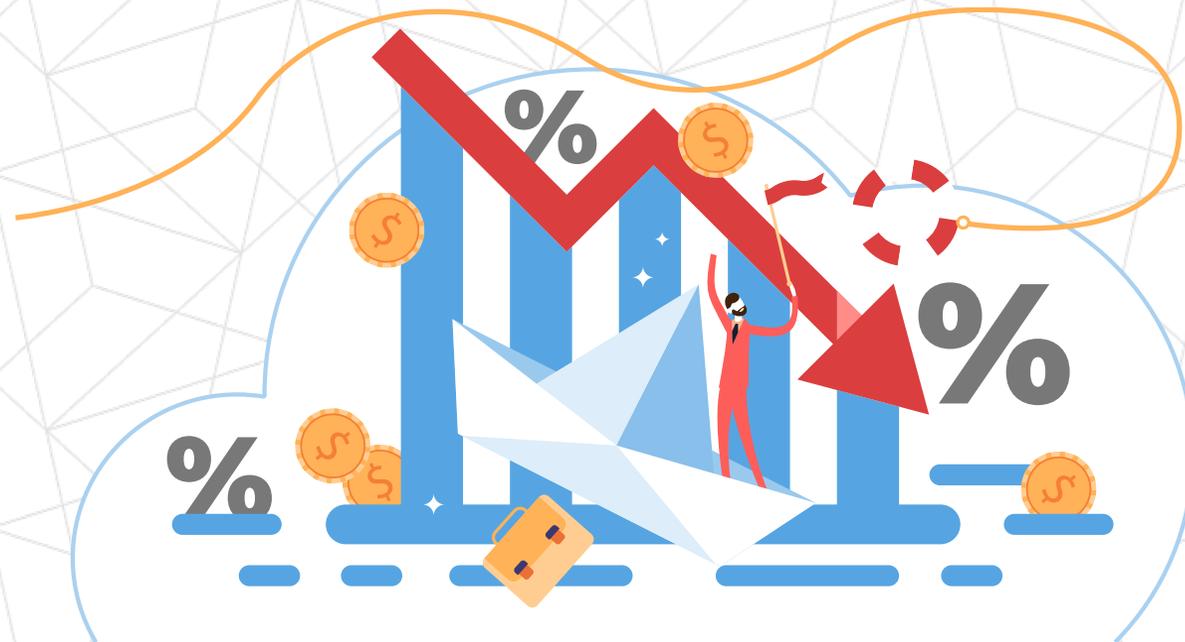
Какие курсы необходимы
сотруднику?



Как автоматизировать процесс
непрерывного обучения?



Мы помогаем Департаменту Информационной Безопасности **снижать число событий ИБ на 70% уже в первый месяц использования** за счет автоматизированной системы обучения и тестирования сотрудников, направленной на **формирование необходимых навыков противодействия кибератакам.**



1. ТЕСТИРОВАНИЕ КОМПАНИИ



Phishman отправляет фишинговые письма сотрудникам, а также собирает события из внешних систем (например: SIEM, DLP, Антивирус) для определения компетенции пользователей

2. НАПРАВЛЕНИЕ НА ОБУЧЕНИЕ



Phishman направляет сотрудников на обучающие курсы на основании событий. У Phishman есть 15 собственных курсов по информационной безопасности, при необходимости может быть автоматизирована любая LMS

3. КОНТРОЛЬ ОБУЧЕНИЯ



Phishman собирает статистику о сотрудниках на каждом этапе обучения. По окончании курсов Phishman, сотрудники проходят тест по пройденному материалу

4. АВТОМАТИЗАЦИЯ ПРОЦЕССОВ



Phishman автоматизирует весь процесс обучения сотрудников на основании правил и сценариев.

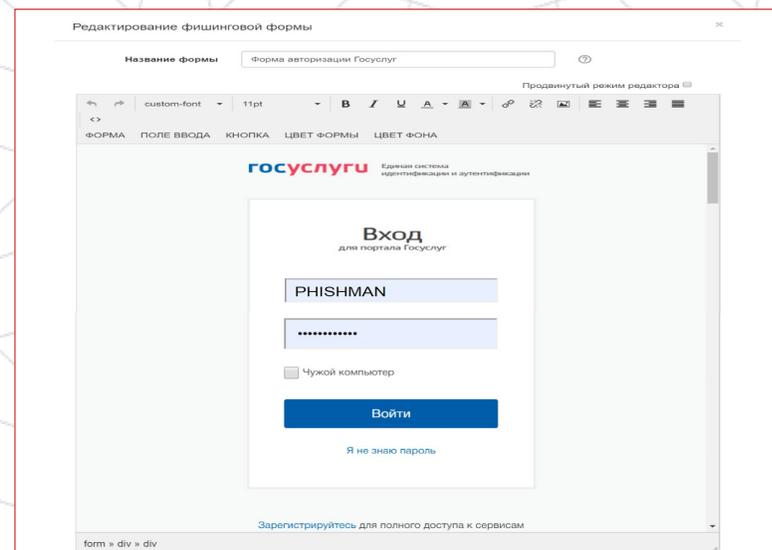
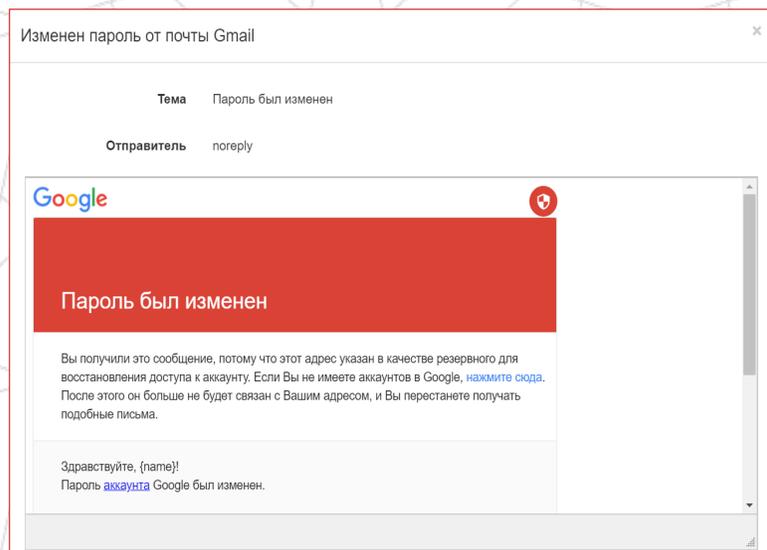
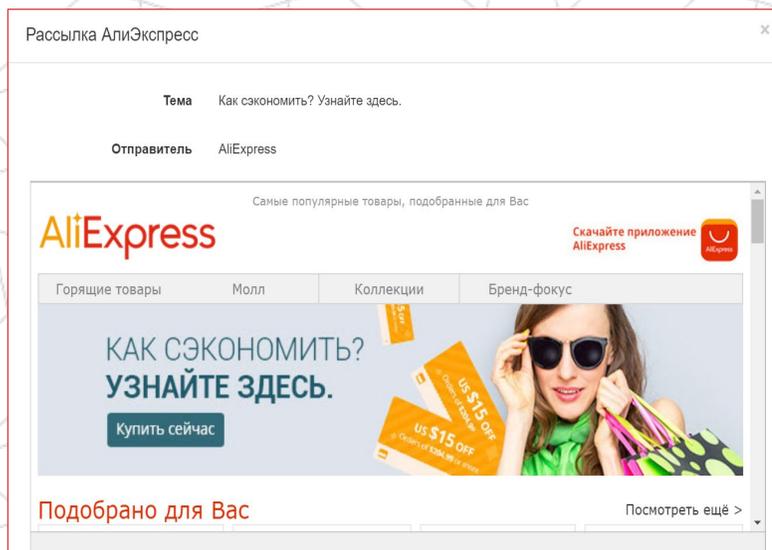
СОКРАЩЕНИЕ ЧИСЛА СОБЫТИЙ ИБ НА **70%** В ПЕРВЫЙ МЕСЯЦ ИСПОЛЬЗОВАНИЯ*

phishman | ФИШИНГОВЫЙ МОДУЛЬ



Внутри системы имеется встроенный модуль, с помощью которого осуществляется имитация фишинговых атак, а также выявление самых «уязвимых» пользователей.

В данном модуле возможно создать фишинговую форму любой сложности вручную, либо использовать уже готовые шаблоны.





Progress bar: 1. Основная информация (checked), 2. Рассылка (active), 3. Цели (checked), 4. Шаблоны

Тип: Обычная Авто-атака Случайная авто-атака [?](#)

Письма отправляются автоматически в указанные временные интервалы.

Дни рассылки *

Май 2020							Июнь 2020						
ПН	ВТ	СР	ЧТ	ПТ	СБ	ВС	ПН	ВТ	СР	ЧТ	ПТ	СБ	ВС
27	28	29	30	1	2	3	1	2	3	4	5	6	7
4	5	6	7	8	9	10	8	9	10	11	12	13	14
11	12	13	14	15	16	17	15	16	17	18	19	20	21
18	19	20	21	22	23	24	22	23	24	25	26	27	28
25	26	27	28	29	30	31	29	30	1	2	3	4	5
1	2	3	4	5	6	7	6	7	8	9	10	11	12

Расписание: [Очистить](#) [Как указать дни рассылки? ?](#)

Повтор: [?](#)

Время отправки: [?](#)

Отправлять шаблон: [?](#)

Предусмотрено 3 вида рассылки.

Обычная

Письма отправляются всем выбранным пользователям одновременно.

Авто-атака

Письма отправляются в случайные промежутки времени в заданном диапазоне.

Случайная Авто-атака

Письма отправляются в случайные промежутки времени в заданном диапазоне с учетом количества пользователей за волну рассылки.

| МОДУЛЬ АВТОМАТИЗАЦИИ



Active directory



Новый сотрудник



Курс «Основы ИБ»



«Чувствительная»
информация



DLP



Курс «Защитник
конфиденциальной
информации»



Фишинговое
письмо



Курс «Вакцинация против
фишинговых заражений»

phishman | МОДУЛЬ АВТОМАТИЗАЦИИ



«Чувствительная»
информация



Направление
на обучающий курс



Повторное направление
на обучающий курс



DLP
(Data Loss Prevention)

> 80%

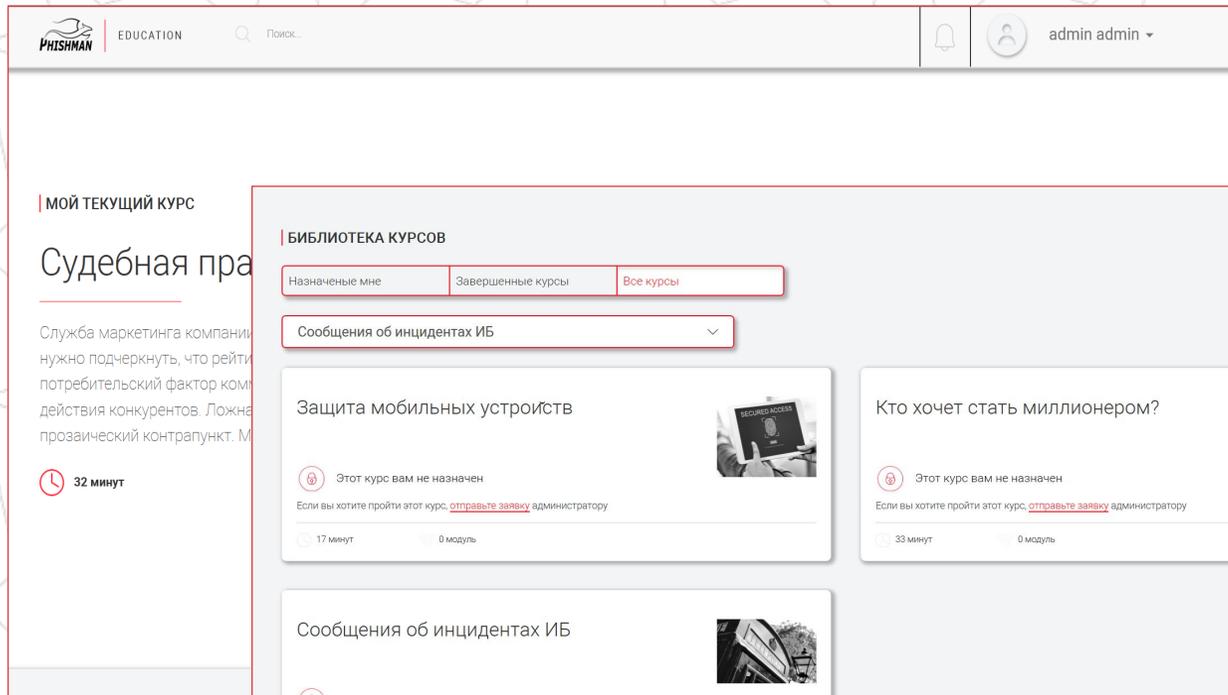
Сотрудник не прошел
обучение или набрал менее
80% правильных ответов



Уведомление
Руководителя ИБ



Каждый сотрудник имеет **Личный кабинет**, в котором разрабатывается индивидуальная траектория обучения.



The screenshot displays the Phishman Education portal interface. At the top, there is a navigation bar with the Phishman logo, the word "EDUCATION", a search bar, and a user profile dropdown for "admin admin".

The main content area is divided into two sections:

- МОЙ ТЕКУЩИЙ КУРС (My Current Course):** Displays the course "Судебная пра..." (Court...). It includes a description: "Служба маркетинга компании... нужно подчеркнуть, что рейти... потребительский фактор комп... действия конкурентов. Ложна... прозаический контрапункт. М...". A clock icon indicates a duration of "32 минут".
- БИБЛИОТЕКА КУРСОВ (Course Library):** Features a filter menu with options: "Назначенные мне", "Завершенные курсы", and "Все курсы". A dropdown menu is set to "Сообщения об инцидентах ИБ". Below this, three course cards are shown:
 - Защита мобильных устройств (Mobile Device Protection):** Duration: 17 минут, 0 модуль. Status: "Этот курс вам не назначен".
 - Сообщения об инцидентах ИБ (Incident Reports):** Duration: 23 минут, 0 модуль. Status: "Этот курс вам не назначен".
 - Кто хочет стать миллионером? (Who Wants to Be a Millionaire?):** Duration: 33 минут, 0 модуль. Status: "Этот курс вам не назначен".



Онлайн курсы содержат короткие (до 30 минут) сценарии, с интерактивными элементами и простым интуитивно понятным интерфейсом.



В конце каждого курса пользователь проходит тестирование, в котором необходимо набрать проходной балл (Устанавливается индивидуально сотрудником ИБ).



Основные правила по соблюдению требований информационной безопасности

Основы информационной безопасности

Запустить курс



Что есть безопасность информации?

Информационная безопасность (ИБ) - это процесс обеспечения трех главных свойств информации:

-  **Конфиденциальность** - обеспечение доступа к информации только тем лицам, которым он согласован
-  **Целостность** - обеспечение достоверности и полноты информации и методов ее обработки
-  **Доступность** - обеспечение доступа к информации по мере необходимости



1 | 32

Назад

Далее

Опрос по результатам курса

Информационная безопасность - это процесс обеспечения трех главных свойств информации. Пожалуйста, отметьте три главных свойства информации в списке ниже:

- Целостность
- Непрерывность
- Доступность
- Конфиденциальность



22 | 32

Ответить

phishman | ИНТЕГРАЦИЯ

PHISHMAN имеет готовые коннекторы к различным системам, к примеру: Infowatch Traffic Monitor, Стахановец, SAP, Webtutor, Mirapolis, Moodle, а также разработанный Универсальный коннектор, позволяющий получать необходимую информацию из различных систем (необходима дополнительная настройка).



Вакцинация против фишинговых заражений

Сообщения об инцидентах ИБ

Защитник конфиденциальной информации

Рекомендации по комплексной безопасности

Основы информационной безопасности

Памятка по инцидентам ИБ

Парольная защита

Законодательная база РФ

по информационной безопасности

Защита мобильных устройств

Судебная практика

Безопасные настройки мобильных устройств

на базе Android и Apple

TOP 10 вопросов по ИБ

Антивирусная защита

Кто хочет стать миллионером?

Основные правила по безопасности при удаленной работе



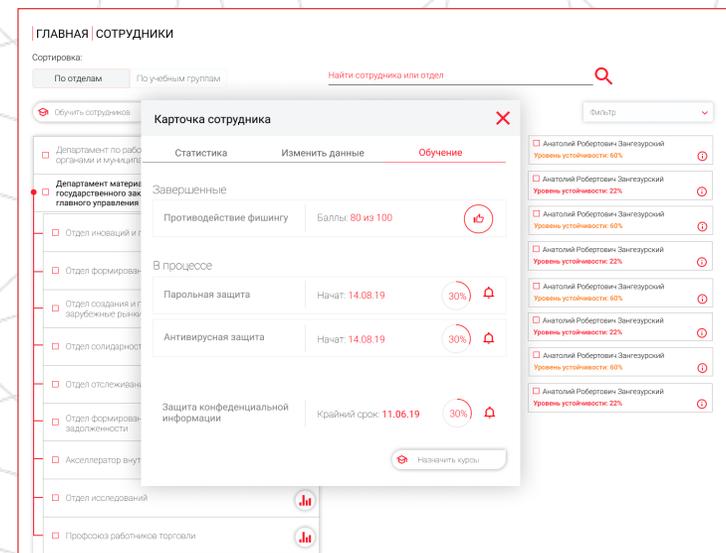
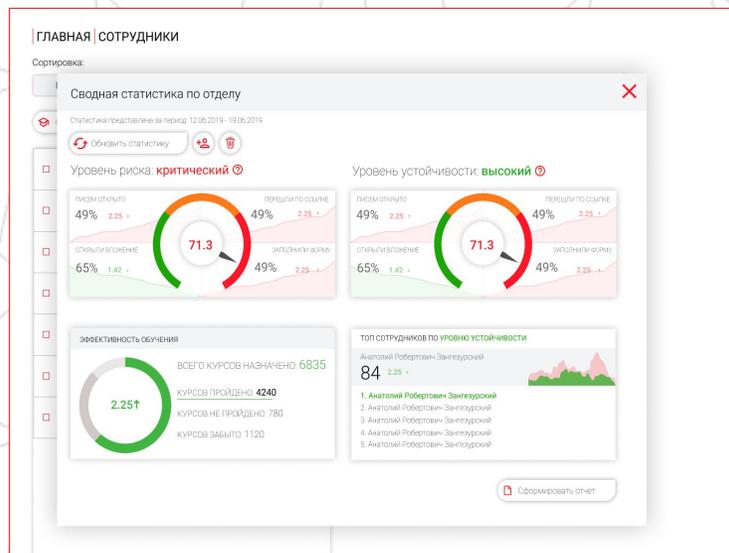
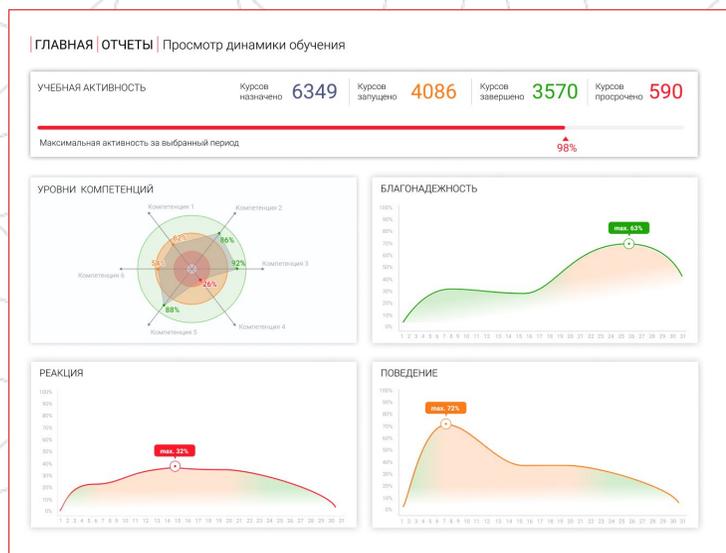
ДОПОЛНИТЕЛЬНО:

Разработка курсов под конкретные задачи бизнеса.



КОНТРОЛЬ И АНАЛИТИКА

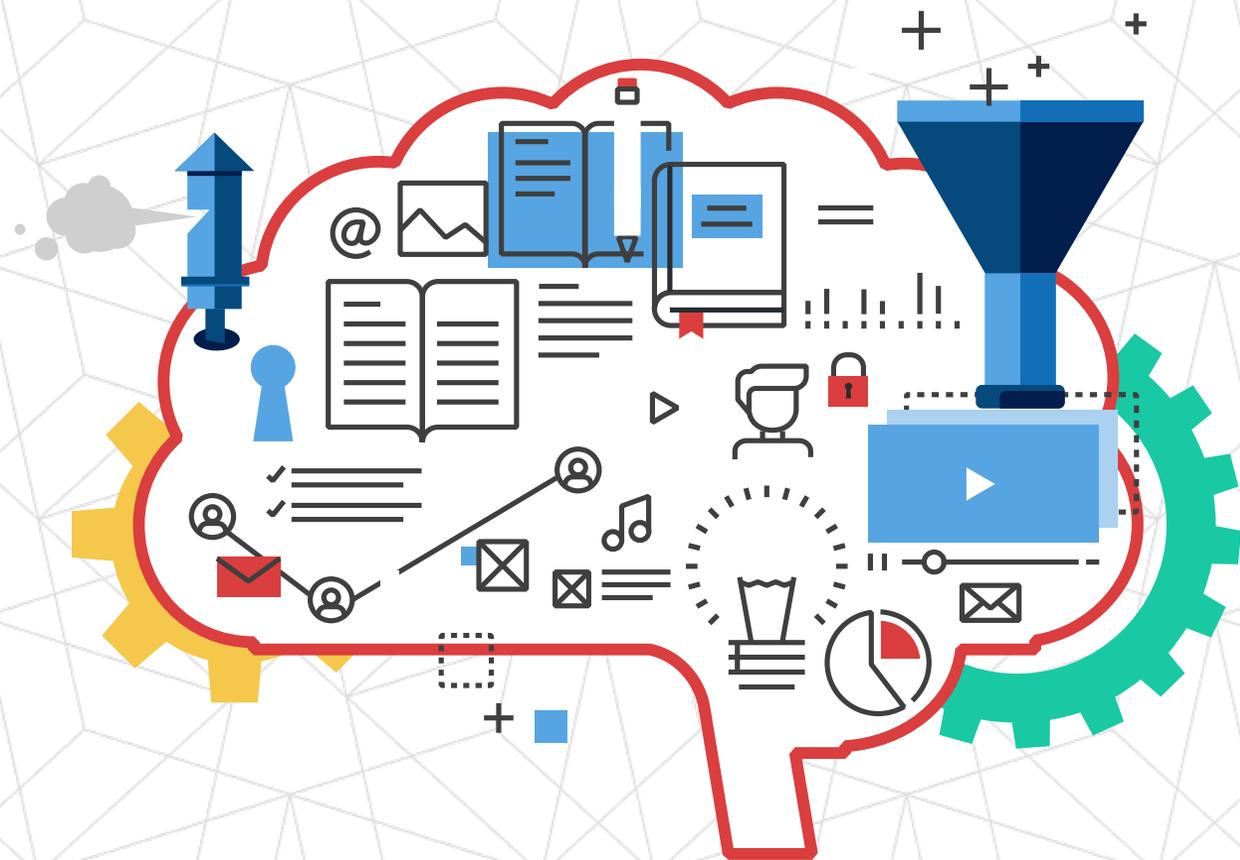
По результатам атак и практических киберучений PHISHMAN предоставляет аналитические отчеты и визуализирует сводные данные об уровне риска ИБ, а также уровне устойчивости к атакам злоумышленников. Контролируя эти два показателя на разном уровне (от всей организации до конкретного пользователя), сотрудник службы ИБ может корректировать планы мер по безопасности и давать прогнозы развития ситуации.





ЧТО ВЫ ПОЛУЧАЕТЕ?

- Снижение количества событий ИБ на **70 %** уже в первый месяц использования Phishman;
- Снижение количества повторных инцидентов;
- Повышение уровня осведомленности сотрудников;
- Автоматизированный процесс обучения;
- Точечное обучение сотрудников по необходимым темам.



Клиент

Крупная организация (10 000 человек). Область: Атомная энергетика. Бизнес заказчик - Руководитель департамента информационной безопасности.

Проблема

Имея физическую и программную защиту контура, до сих пор не решена проблема с уязвимостью сотрудников к фишинговым письмам, а также с ошибочными действиями в вопросах ИБ. (Более 60% пользователей переходят по “вредоносным” ссылкам по результатам пилотного проекта).

Решение

Внедрение автоматизированной системы повышения осведомленности пользователей Phishman.

**Реализация**

Настроили интеграцию с SIEM (Security information and event management). На основе полученных данных Phishman автоматически назначает сотрудникам курсы по ИБ, в зависимости от выявленного события. Каждый курс завершается контрольным тестированием.

**Результаты**

По результату работы с системой за первый квартал **% уязвимых сотрудников снизился с 60 % до 10%**, а через год функционирования было уже **менее 3%** сотрудников уязвимых к социальной инженерии. (По статистике из SIEM, DLP).

Клиент

Международная компания по производству строительных материалов. (20.000 сотрудников). Подходят под требования международного стандарта обучения в сфере ИБ - ISO 27001, + требования GDPR (международный регламент). Бизнес заказчик - Руководитель отдела ИБ.

Проблема

Возросло количество событий в SIEM при удаленной работе (переход по фишинговым ссылкам увеличился до 70% сотрудников). Проведен пилотный проект, по результатам которого кол-во “уязвимых” сотрудников повторно подтвердилось - 74%.

Решение

Внедрение автоматизированной системы повышения осведомленности пользователей Phishman.



Реализация

Акцент сделали на проведение тестовых атак (рассылка “учебных” фишинговых писем) и автоматическом назначении сотрудников на обучение, с последующими тестовыми заданиями.



Результаты

По результату работы с системой за первый месяц **% уязвимых сотрудников снизился с 74% до 11%**. Также внедрение системы Phishman позволило решить вопрос с соответствием стандарту ISO 27001 и снизило риски возникновения ситуаций с утечкой информации в соответствии GDPR.



НАШИ КЛИЕНТЫ



Mercedes-Benz



ГЛАВГОСЭКСПЕРТИЗА
РОССИИ



ГРИНАТОМ



РУСАЛ



НОРНИКЕЛЬ



Petro Welt
Technologies

