альфаинтенсив

Комплексное решение для повышения уровня киберграмотности сотрудников организации и подготовки кадров в области информационной безопасности



ПОЧЕМУ ПОВЫШАТЬ КИБЕРГРАМОТНОСТЬ СОТРУДНИКОВ ВАЖНО?



сотрудников в государственных учреждениях и 61% сотрудников частных компаний имеют **плохой или средний уровень знаний по ИБ**



компаний уже сталкивались с утечками данных — чаще всего по вине **невнимательных или неосведомленных сотрудников**



хакерских групп начинают свои атаки с **фишинга** — самого простого, но эффективного способа проникновения



всех успешных кибератак происходят из-за **ошибок сотрудников**



ежегодный рост числа **фишинговых писем**

Сложившийся контекст	Риски	Последствия
Сложность и многочисленность законодательных требований	Нарушение требований законода-тельства	Штрафы, приостановка деятельности
Низкая осведомленность сотрудников, обрабатывающих информацию	Финансовые и репутацион-ные потери	Срыв бизнес процессов, потеря доверия клиентов и партнеров, издержки и убытки
Отсутствие стуктурированной системы обучения	Уязвимость организации к кибератакам	Атаки, утечки информации, компрометация данных и систем
Недостаточно высокий уровень квалификации будущих кадров в вузах и СПО в сфере ИБ	Снижение эффективности внутренних процессов	Отсутствие контроля знаний, повышение нагрузки на ИБ-специалистов

Законодательные требования



ПОВЫШЕНИЕ ОСВЕДОМЛЕННОСТИ СОТРУДНИКОВ И ИХ ОБУЧЕНИЕ

Федеральный закон № 152-ФЗ от 27.07.2006 г. «О персональных данных»

- Статья 6
- Статья 7
- Статья 8
- Статья 19

Федеральный закон № 187-ФЗ от 26.07.2017 г. «О безопасности критической информационной инфраструктуры Российской Федерации»

- Статья 9, пункт 1.4
- Статья 11, пункт 1.1

Приказ ФСТЭК России № 117 от 11.04.2025 г.

- Пункты 5-6
- Пункты 9-10
- Пункт 13
- Пункты 21-23
- Пункт 34
- Пункты 56-57

Приказ ФСТЭК России № 239 от 25.12.2017 г.

- Пункт 13.6
- Пункт 13.7
- Пункт 22

Приказ ФСТЭК России № 31 от 14.03.2014 г.

- Пункт 15.2
- Пункт 16
- Пункт 18

ПРИОБРЕТЕНИЕ ПРАКТИЧЕСКИХ НАВЫКОВ И ПРОВЕДЕНИЕ ТРЕНИРОВОК

Федеральный закон № 152-ФЗ от 27.07.2006 г. «О персональных данных»

- Статья 6
- Статья 7
- Статья 8
- Статья 19

Федеральный закон № 187-ФЗ от 26.07.2017 г. «О безопасности критической информационной инфраструктуры Российской Федерации»

- Статья 9, пункт 1.4
- Статья 11, пункт 1.1

Приказ ФСТЭК России № 117 от 11.04.2025 г.

- Пункт 10
- Пункты 21-23
- Пункт 34
- Пункты 56-57

Приказ ФСТЭК России № 239 от 25.12.2017 г.

- Пункт 13.6
- Пункт 13.7
- Пункт 22

Приказ ФСТЭК России № 31 от 14.03.2014 г.

- Пункт 15.2
- Пункт 16
- Пункт 18

ПОДГОТОВКА СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Федеральный закон от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации»

- Статья 11, пункт 2
- Статья 12, пункт 1
- Статья 28, пункт 3

Федеральный государственный образовательный стандарт (ФГОС) для направлений, связанных с ИБ

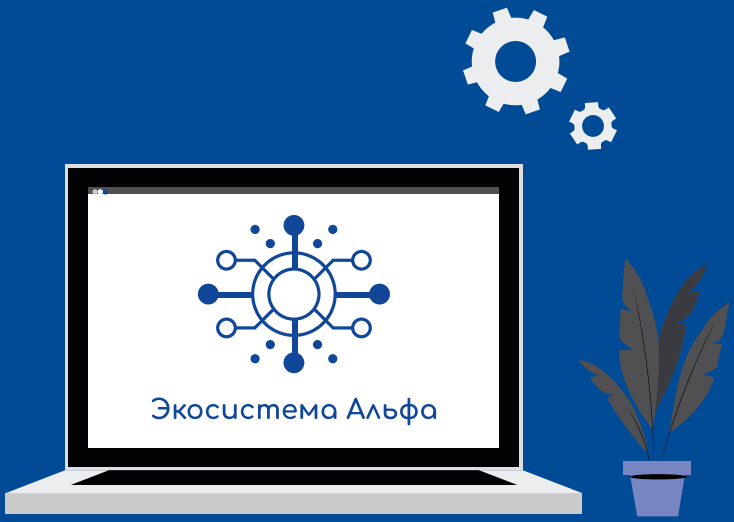
- ФГОС ВО 10.03.01 «Информационная безопасность»
- ФГОС ВО 10.05.01 «Компьютерная безопасность»
- ФГОС ВО 10.05.05 «Безопасность информационных технологий в правоохранительной сфере»
- ФГОС ВО 09.03.01 «Информатика и вычислительная техника»
- ФГОС ВО 09.03.02 «Информационные системы и технологии»
- ФГОС ВО 09.03.04 «Программная инженерия»

Профессиональные стандарты

- «Специалист по безопасности информации»
- «Специалист по защите информации в автоматизированных и информационных системах»

альфа|интенсив

приложение экосистемы «Альфа»



Помогаем повышать уровень осведомленности сотрудников и готовить кадры в области информационной безопасности

Система управления обучением (LMS)

Собственная платформа для обучения сотрудников с возможностью создавать собственные обучающие курсы или импортировать готовые материалы

Готовые курсы

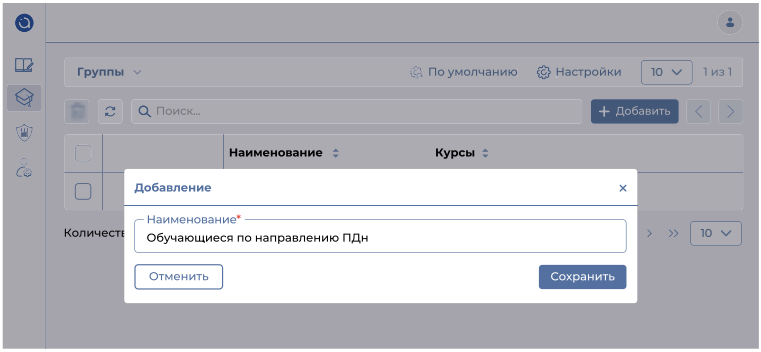
Актуальные курсы по основным направлениям защиты информации для сотрудников и студентов

Платформа для имитации фишинговых атак

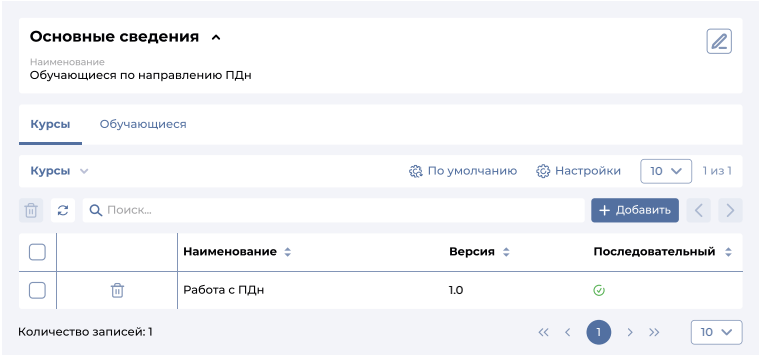
Проверка реакции сотрудников на фишинг с последующим обучением и закреплением навыков

ПОВЫШЕНИЕ ОСВЕДОМЛЕННОСТИ

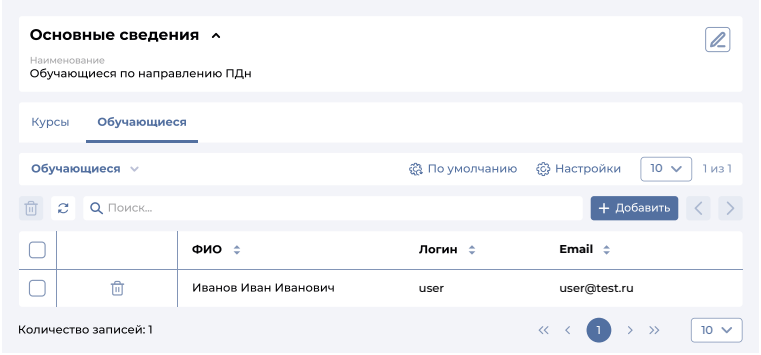
1. Создание группы обучения



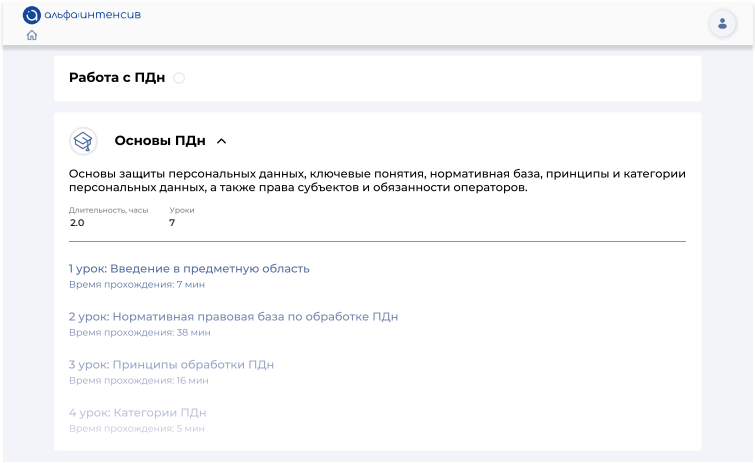
2. Выбор направления обучения



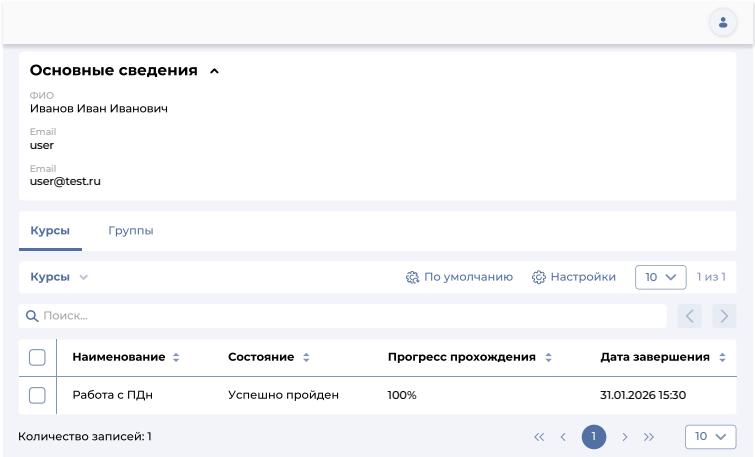
3. Выбор участников



4. Прохождение обучения

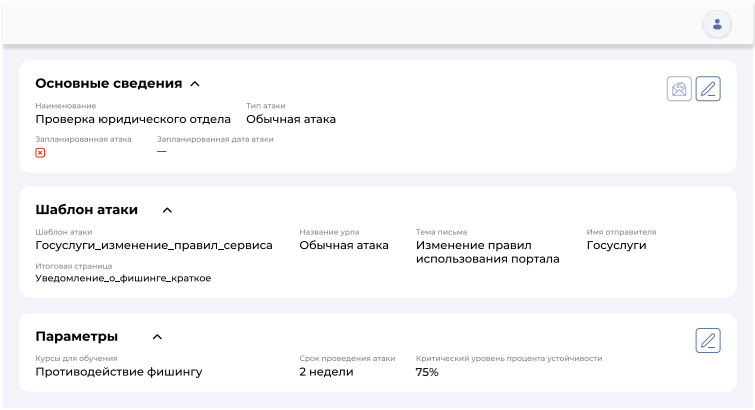


5. Подведение итогов

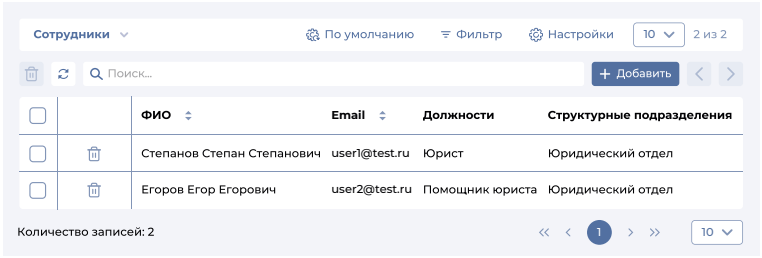


ИМИТАЦИЯ ФИШИНГОВЫХ АТАК

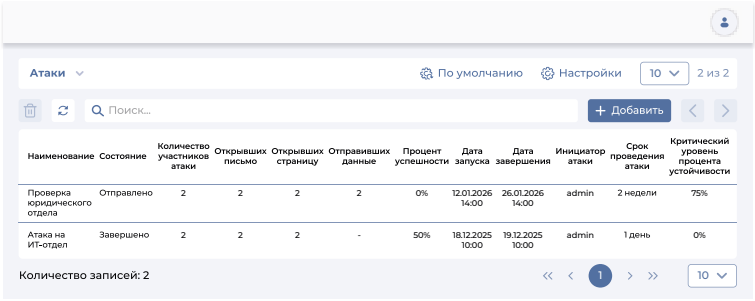
1. Подготовка к имитации фишинговой атаки



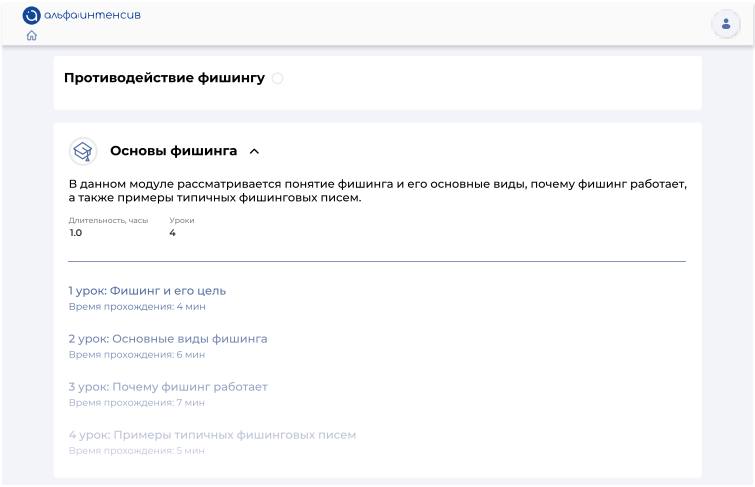
2. Определение участников и запуск атаки



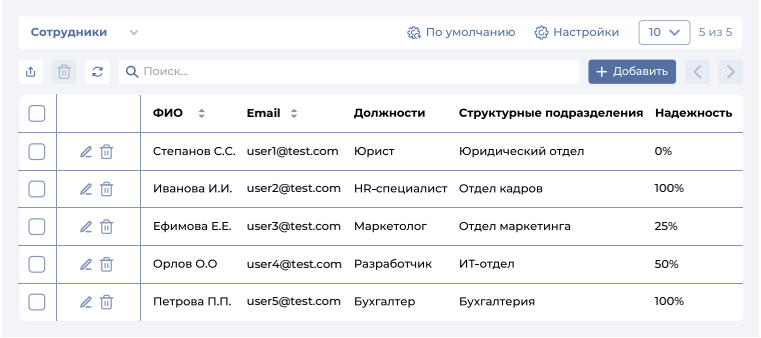
3. Мониторинг и подведение итогов



4. Обучение сотрудников, не прошедших фишинговую проверку



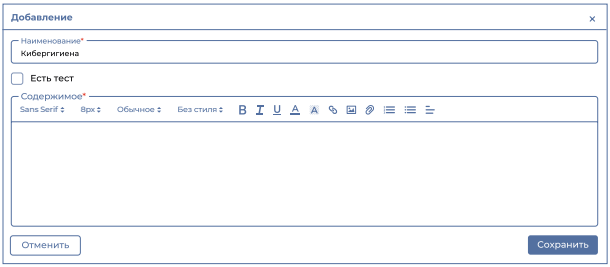
5. Подведение итогов по киберграмотности сотрудников



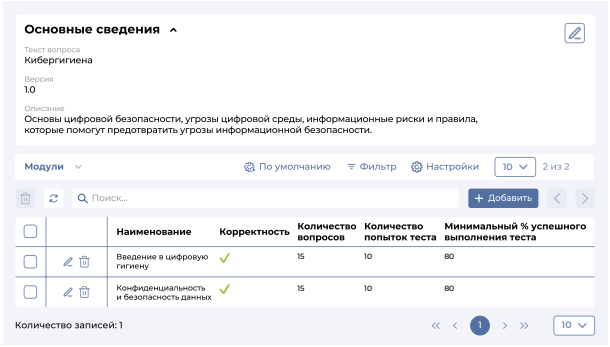
ФИО	Email	Должности	Структурные подразделения	Надежность
Степанов С.С.	user1@test.com	Юрист	Юридический отдел	0%
Иванова И.И.	user2@test.com	HR-специалист	Отдел кадров	100%
Ефимова Е.Е.	user3@test.com	Маркетолог	Отдел маркетинга	25%
Орлов О.О	user4@test.com	Разработчик	ИТ-отдел	50%
Петрова П.П.	user5@test.com	Бухгалтер	Бухгалтерия	100%

ИНСТРУМЕНТ ДЛЯ СОЗДАНИЯ КОНТЕНТА

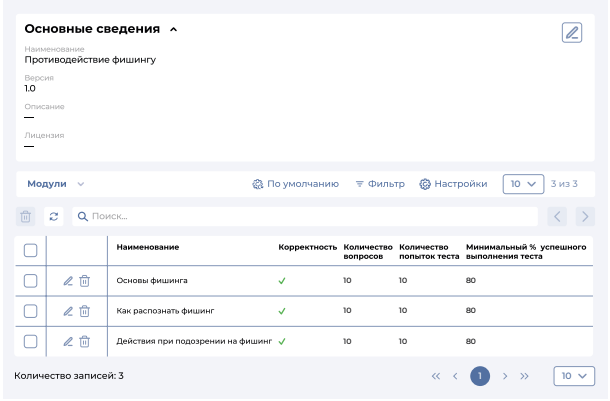
1. Подготовка и оформление учебных материалов



2. Создание тестовой части для проверки знаний



3. Объединение материалов и тестов в единый курс
и определение критериев успешного прохождения обучения



ПОДДЕРЖКА ПОЛЬЗОВАТЕЛЕЙ

Гарантийная поддержка
Входит в состав всех лицензий

- ✓ консультации по функционалу
- ✓ участие в обучающих вебинарах по вопросам эксплуатации системы
- ✓ актуализация документации по установке и настройке
- ✓ консультации в процессе самостоятельной установки, настройки, обновления, переустановки и отладки

Дополнительные услуги
Только для on-premise решений

- \+ разработка дополнительных шаблонов писем и сайтов с учетом специфики организации
- \+ разработка дополнительных курсов и контрольных заданий к ним
- \+ адаптация собственных курсов и контрольных заданий к ним под требования организации

ИНДИВИДУАЛЬНОЕ СОПРОВОЖДЕНИЕ

Дополнительные возможности
Только для on-premise решений

+ поддержание в актуальном состоянии дополнительно разработанных шаблонов писем и сайтов с учетом специфики организации
+ поддержание в актуальном состоянии дополнительно разработанных курсов и контрольных заданий к ним
+ поддержание в актуальном состоянии собственных курсов и контрольных заданий к ним под требования организации
+ удаленное обеспечение работоспособности

Свяжитесь с нами удобным для вас способом:

- 8 800 500-52-33
- alfa@npc-ksb.ru

По будням с 8:00 до 18:00 по мск

альфаинтенсив
поможет вам



Соответствовать требованиям законодательства

Выполнять требования федерального законодательства в области информационной безопасности (№ 152-ФЗ, № 187-ФЗ), приказов ФСТЭК России (№ 117, № 239, № 31, № 235)

Провести реальную проверку сотрудников

Выявлять пробелы в знаниях сотрудников, повышать устойчивость персонала к методам социальной инженерии

Создать комплексную систему обучения

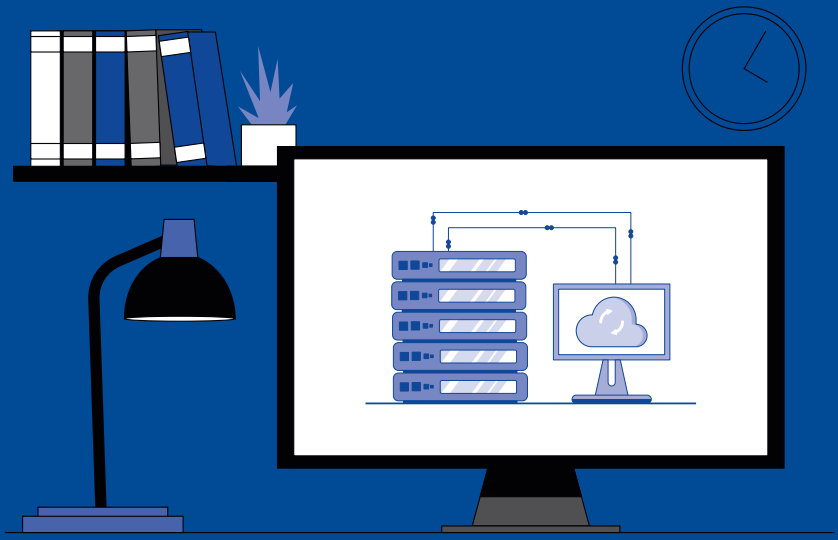
Выстроить систему обучения сотрудников с возможностью создания собственных курсов по защите информации или внедрения сторонних, поддержание высокого уровня кибербезопасности в организации

Подготовить будущие кадры в вузах и СПО

Создать специалистов с практическими навыками и актуальными знаниями в сфере ИБ, увеличивая их конкурентоспособность на рынке труда и престиж учебного заведения

альфа|интенсив

варианты внедрения



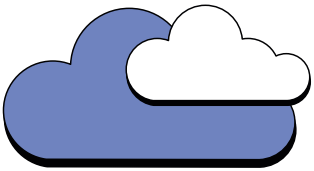
ВАРИАНТЫ ВНЕДРЕНИЯ



On-premise

Серверные мощности пользователя

- Обучение
- Имитация фишинговых атак
- Инструмент для создания курсов



On-cloud

Защищенный ЦОД НПЦ «КСБ»

- Обучение

альфа|интенсив

преимущества



- Интеграция с экосистемой приложений «Альфа»
- 13-летний опыт взаимодействия с государственными регуляторами
- Гибкая ценовая политика
- Внедрение в формате on-premise
- Опыт работы с организациями ключевых отраслей экономики во всех регионах России

альфа



86
субъектов
Российской Федерации

7000+
организаций –
действующих пользователей

1000+
субъектов КИИ

ЗАЙДИТЕ
на сайт alfa-doc.ru

ПРОТЕСТИРУЙТЕ
сервис бесплатно

ВЫБЕРИТЕ
подходящую лицензию

ПОЛУЧИТЕ
консультацию эксперта

№ 20044
в Едином реестре
российских программ
для ЭВМ и баз данных

Совместимость
с отечественными
ОС и пакетами
офисных приложений

Дзен | Rutube | Сайт | ВКонтакте | Telegram | MAX