

Руководство администратора

Документ содержит инструкции для выполнения ключевых административных задач на платформе Start AWR.

Дата последнего обновления документа: 15.10.2026

Содержание

[Авторизация](#)

[Вход по логину и паролю](#)

[Вход через LDAP](#)

[Вход через SSO](#)

[Меню для быстрой навигации](#)

[Раздел «Настройки»](#)

[Вкладка «Администраторы»](#)

[Профиль администратора](#)

[Часовой пояс](#)

[Двухфакторная аутентификация \(2FA\)](#)

[Лицензия](#)

[Учетные записи администраторов](#)

[Роли администраторов](#)

[Вкладка «Работа с сотрудниками»](#)

[Профили LDAP](#)

[Профили SSO](#)

[Новый сотрудник](#)

[Анонимный режим](#)

[Вкладка «Обучение»](#)

[Вкладка «Почтовый плагин»](#)

[Вкладка «Тренировки»](#)

[Вкладка «Переменные»](#)

[Раздел «Сотрудники»](#)

[Работа с подразделениями](#)

[Создание подразделения](#)

[Редактирование подразделения](#)

[Удаление подразделения](#)

[Добавление сотрудников](#)

[Вручную](#)

[Импорт из файла Excel](#)

[Импорт из LDAP \(например, Microsoft Active Directory\)](#)

[Поиск, фильтры и сортировка сотрудников](#)

[Действия с сотрудниками](#)

[Обучить](#)

[Тренировать](#)

[Выбрать всех остальных, вместо выделенных](#)

[Выгрузить данные сотрудников](#)

[Подготовить отчет по действиям](#)

[Подготовить отчет по обучению](#)

[Подготовить отчет со сводной статистикой по сотрудникам](#)

[Отменить обучение](#)

[Удалить из системы](#)

[Редактировать](#)

[Карточка сотрудника](#)

[Раздел «Тренировки»](#)

[Атака по электронной почте](#)

[Как проходит атака](#)

[Описание интерфейса](#)

[Создание атаки](#)

[Запуск атаки](#)

[Статистика по запускам](#)

[Приостановка атаки \(пауза\)](#)

[Редактирование атаки](#)

[Планирование запуска атаки](#)

[Завершение атаки](#)

[Удаление атаки](#)

[Корзина](#)

[Атака через съемное устройство](#)

[Атака через беспроводную сеть \(Wi-Fi\)](#)

[Раздел «Процессы»](#)

[Описание интерфейса](#)

[Описание интерфейса конструктора процессов](#)

[Событие](#)

[Действие](#)

[Условие](#)

[Создание процесса](#)

[Раздел «Защищенность сотрудников»](#)

[Ключевые показатели](#)

[Индекс защищенности компании](#)

[Переменные](#)

[Виды переменных](#)

[Список переменных](#)

[Стандартные переменные](#)

[Кастомные переменные](#)

[Дашборд в разделе «Ключевые показатели»](#)

[Рейтинг сотрудников](#)

[Формирование рейтинга](#)

[Контроль уязвимостей приложений](#)

[Обучение сотрудников](#)

[Рекомендации по использованию системы](#)

[Почтовый плагин](#)

[Кастомизация внешнего вида плагина](#)

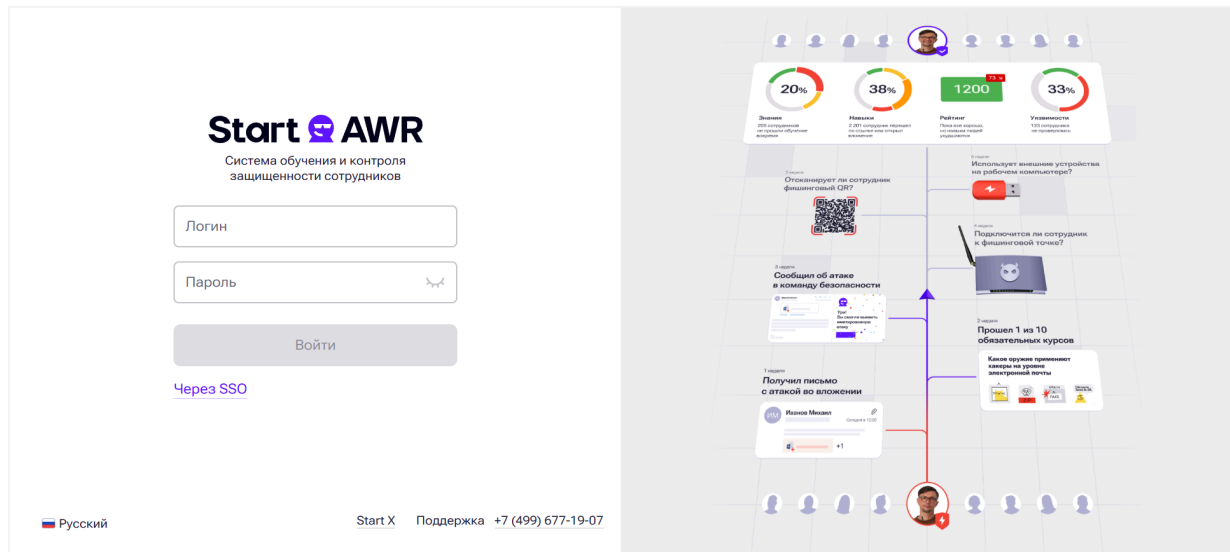
[Отчет по обратной связи от сотрудников](#)

[Планировщик](#)

Авторизация

Все функции Start AWR доступны через панель управления по ссылке

<https://attack.antiphish.ru/login>



Есть несколько способов войти на платформу: по логину и паролю, через LDAP и с помощью SSO.

Вход по логину и паролю

1. Введите логин и пароль.

This is a screenshot of the Start AWR login form. It has the same header as the previous image. The 'Логин' field is pre-filled with 'ivanov@example.com'. The 'Пароль' field is masked with dots. The 'Войти' button is highlighted in blue. The 'Через SSO' link is visible at the bottom.

2. Нажмите кнопку **Войти**.

Готово! Вы вошли на платформу с помощью логина и пароля.

Вход через LDAP

С помощью LDAP-аутентификации администраторы могут входить в систему, используя логин и пароль из корпоративного каталога.

Как настроить

Чтобы настроить вход через LDAP:

1. Добавьте LDAP-профиль.
2. Создайте учетную запись администратора.

Как войти

1. Введите логин и пароль от учетной записи LDAP.
2. Нажмите кнопку **Войти**.

Готово! Вы вошли на платформу с помощью LDAP.

Вход через SSO

SSO-аутентификация по протоколу SAML 2.0 позволяет администраторам входить в систему с помощью корпоративной учетной записи.

Системные требования

- Установленный и настроенный сервис [Microsoft Active Directory Federation Services](#) (AD FS) 3.0 и/или Azure Active Directory (Azure AD);
- Компьютер-сервер на Microsoft Server 2008r2 или 2012/2012r2;
- x509 сертификат, который используется для безопасной подписи всех маркеров при общении с сервером федерации.

Как настроить

Чтобы настроить вход через SSO:

1. Добавьте профиль SSO.
2. Создайте учетную запись администратора.

Как войти

1. Выберите способ авторизации — **Через SSO**.
2. Введите логин от учетной записи администратора — электронную почту.
3. Нажмите кнопку **Войти**.
4. Произойдет переадресация на страницу входа в Microsoft Active Directory Federation Services (AD FS). Авторизуйтесь в нем и система перенаправит вас на сервер Start AWR.

Готово! Вы вошли на платформу с помощью SSO.

Меню для быстрой навигации

Для навигации по платформе администратору доступно меню с разделами:

Start AWR

Securebrand

Ключевые показатели

Сотрудники

Группа риска

Обучение

Тренировки

Уязвимости

Отчеты

Процессы

Защищенность

Все разделы

Настройки

Русский

Иванов Иван

ivanivanov@securebrand.local

Start X

support@startx.team

Сотрудники общим списком

+ Добавить

Не тренировались
94 сотрудника

Все сотрудники в системе
100 сотрудников

Выбрать файлом
Только xls

Сотрудники

изделения, ФИО, email, должность, метка сотрудника

Искать

Фильтровать по обучению, поведению в атаках, рейтингу или по уязвимостям, меткам и новым сотрудникам

Имя и фамилия	Должность и подраздел	Метки	Обучение	Тренировки	Рейтинг
Байрам Ахмад оглы	Frontend-developer	Ежеквартальная п...	Просрочил	Не проверялся	0
Сидорова Евгеньевна	Frontend-developer		Просрочил	Не проверялся	0
Сидорова Евгеньевна	Frontend-developer		Просрочил	Не проверялся	0
Сидорова Евгеньевна	Security Engineer		Просрочил	Выдержал	2
Сидорова Евгеньевна	DevOps		Просрочил	Не проверялся	0

Раздел «Настройки»

В этом разделе доступны основные настройки платформы.

Вкладка «Администраторы»

Настройки

Сохранить отладочную информацию

Обновить систему

Администраторы

Работа с сотрудниками

Обучение

Почтовый плагин

Тренировки

Переменные

Антипов Сергей Петрович

Двухфакторная аутентификация включена

Эл. почта

antipov.s@securebrand.local

Телефон

+7 985 222 33 44

Часовой пояс

GMT+3 Europe - Moscow

Изменить пароль

Лицензия

Чтобы изменить условия лицензии, напишите на support@startx.team

Название

Securebrand

Домены

beresklet.com, borovik.net, dubrovnik.hr, elefant.ro, falconsoft.io, forestcomp.com, intellijoy.com, kaabotech.com

Действует до

30 апр 2027 г.

Поддержка до

12 сен 2026 г.

Сотрудники

6 570 из 10 000, доступно 3 430

Версия

2.6.3

Учетные записи администраторов

Настроить требования к паролю и авторизации

Скачать журнал

+ Новая учетная запись

Здесь вы можете:

- посмотреть данные авторизованного администратора — ФИО, электронную почту и телефон;
- включить или отключить двухфакторную аутентификацию;
- настроить часовой пояс;
- изменить пароль;
- посмотреть информацию о лицензии — до какой даты она действует, какой объем занят или свободен;
- узнать версию платформы;
- создать, изменить или удалить учетные записи администраторов;
- настроить требования к паролю и авторизации;
- скачать журнал действий;
- создать, изменить или удалить роли администраторов.

Профиль администратора

В верхней части страницы находятся фамилия и имя администратора, под учетной записью которого выполнен вход. Здесь же доступны контактные данные администратора — почта и номер телефона.

Часовой пояс

В поле **Часовой пояс** выберите часовой пояс, который будет использоваться при планировании обучения, запуска атак и формировании отчетов.

Часовой пояс
GMT+3 Europe – Moscow

Двухфакторная аутентификация (2FA)

Чтобы дополнительно защитить учетную запись, можно включить двухфакторную аутентификацию. Для этого нажмите **Включить двухфакторную аутентификацию**.

 Доступно только при входе по логину и паролю.

Перед настройкой двухфакторной аутентификации установите на телефон приложение для генерации кодов. После этого выполните действия:

1. Нажмите **Включить двухфакторную аутентификацию**.
2. В открывшемся окне введите пароль от вашей учетной записи.
3. Нажмите кнопку **Продолжить**.
4. В открывшемся окне отсканируйте QR-код с помощью приложения или введите уникальный код, который будет указан ниже.
5. Чтобы завершить настройку, введите в окне код подтверждения из приложения.

Готово! Вы настроили двухфакторную аутентификацию.

Чтобы войти на платформу с помощью 2FA:

1. Введите логин и пароль.
2. Нажмите кнопку **Войти**.
3. Появится поле **Код из приложения**. Введите в нем соответствующий код.
4. Нажмите снова кнопку **Войти**.

Готово! Вы вошли на платформу по логину и паролю с использованием двухфакторной аутентификации.

Лицензия

Лицензия определяет срок использования платформы и максимальное количество сотрудников, которых можно добавить в систему.

Здесь доступна следующая информация:

- **Название** — название компании.
- **Домены** — домены электронной почты, с которыми разрешено добавлять сотрудников на платформу.
- **Действует до** — дата окончания действия лицензии.
- **Поддержка до** — дата окончания действия технической поддержки.
- **Сотрудники** — общее количество сотрудников, доступное в рамках лицензии, и информация о том, сколько мест уже занято и свободно.
- **Версия** — текущая версия платформы.

Учетные записи администраторов

В этом блоке можно управлять учетными записями администраторов, а также настроить требования к паролям и авторизации.

Учетные записи администраторов			
Настроить требования к паролю и авторизации			
		Скачать журнал	+ Новая учетная запись
ФИО	Email	Телефон	Двухфакторная аутентификация
Антипов Сергей Сергеевич	antipov.s@securebrand.local	+7 985 222 33 44	Включена
Константинопольский Кирилл Петрович	konstantinopolsky.k@securebrand.local	+7 926 444 55 66	Выключена
Беляков Алексей Васильевич	belyakov.a@securebrand.local	+7 916 333 44 55	Включена
Соловьев Матвей Александрович	solovyov.m@securebrand.local	+7 903 555 66 77	Выключена

Настройка требований к паролям

Чтобы задать требования к паролям, нажмите **к паролю** под заголовком «Учетные записи администраторов».

[← К настройкам](#)

Требования к паролю

1

Устаревание паролей отключено.

Минимальная длина

символов

Вы можете установить значение от 7 до 999

Включая обязательные символы

☒ Заглавные буквы от А до Z

обязательное условие

☒ Строчные буквы от а до z

обязательное условие

☒ Спецсимволы !@#

обязательное условие

☒ Цифры от 0 до 9, минимум

обязательное условие

символа

Заккрыть

Сохранить

В открывшейся форме можно:

- задать минимальную длину пароля;
- указать обязательные типы символов (цифры, спецсимволы и прочее);
- запретить повторно использовать от пяти и более последних паролей;
- установить срок действия пароля.

Эти требования действуют для вашей учетной записи и для создаваемых учетных записей локальных администраторов.

Настройка требований к авторизации

Здесь можно настроить правила, которые будут действовать при авторизации на платформе:

[← К настройкам](#)

Требования к авторизации

Выйти при бездействии через

минут

Вы можете установить значение от 0 до 999

Лимит ошибок авторизации

попытки

Вы можете установить значение от 0 до 127

Таймаут при превышении лимита

минут

Вы можете установить значение от 0 до 127

Заккрыть

Сохранить

- **Выйти при бездействии через** — укажите количество минут, по истечении которых система автоматически выйдет из учетной записи, если администратор не выполняет никаких действий.
- **Лимит ошибок авторизации** — укажите максимальное количество неудачных попыток входа на платформу. После достижения этого количества доступ к платформе будет временно заблокирован.
- **Таймаут при превышении лимита** — укажите количество минут, в течение которых администратор не сможет войти на платформу после превышения лимита неудачных попыток входа.

Описание интерфейса

Блок «Учетные записи администраторов» представлен в виде таблицы со столбцами:

- ФИО;
- Email;
- Телефон;
- Двухфакторная аутентификация — включена или выключена.

Создание учетной записи

Чтобы добавить учетную запись:

1. Нажмите кнопку **Новая учетная запись**.
2. В открывшейся форме выберите **Тип авторизации***:
 - **Пароль**;
💡 При выборе этого способа появится параметр **Обновить пароль при авторизации**. Если включить его, администратор должен будет изменить пароль при первом входе на платформу.
 - **LDAP**;
 - **SSO**.
3. Заполните остальные поля:
 - **Фамилия***;
 - **Имя***;
 - **Отчество**;
 - **Телефон***;
 - **Роли***;
 - **Вход заблокирован** — включите этот параметр, если нужно запретить вход на платформу для учетной записи. Выберите срок блокировки:
 - **Навсегда** — вход будет запрещен без ограничения по времени;
 - **До** — укажите дату, до которой вход будет запрещен.
4. Нажмите кнопку **Добавить**.

Готово! Вы создали учетную запись.

Редактирование учетной записи

Чтобы изменить данные учетной записи:

1. Нажмите на учетную запись, которую нужно отредактировать.
2. Внесите изменения.
3. Нажмите кнопку **Сохранить**.

Готово! Вы изменили данные учетной записи.

Удаление учетной записи

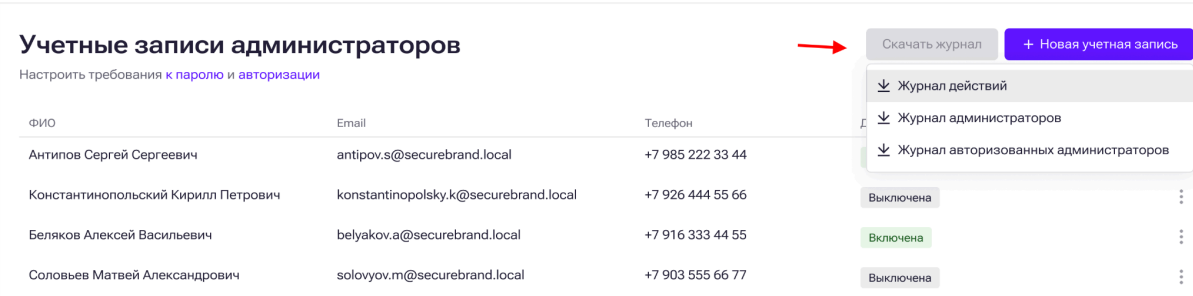
Чтобы удалить учетную запись:

1. Нажмите три точки (⋮) напротив учетной записи, которую нужно удалить.
2. Нажмите **Удалить**.
3. Подтвердите действие.

Готово! Вы удалили учетную запись.

Журналы действий

Журналы содержат информацию о действиях администраторов на платформе. В них можно посмотреть, какие действия ими выполнялись и когда.



Учетные записи администраторов
Настроить требования к [паролю](#) и [авторизации](#)

ФИО	Email	Телефон	Действия
Антипов Сергей Сергеевич	antipov.s@securebrand.local	+7 985 222 33 44	⋮
Константинопольский Кирилл Петрович	konstantinopolsky.k@securebrand.local	+7 926 444 55 66	⋮
Беляков Алексей Васильевич	belyakov.a@securebrand.local	+7 916 333 44 55	⋮
Соловьев Матвей Александрович	solovyov.m@securebrand.local	+7 903 555 66 77	⋮

Скачать журнал + Новая учетная запись

- ⬇ Журнал действий
- ⬇ Журнал администраторов
- ⬇ Журнал авторизованных администраторов

Выключена
Включена
Выключена

Чтобы скачать журнал, нажмите **Скачать журнал** и выберите нужный тип:

- **Журнал действий** (можно выбрать период);
- **Журнал администраторов** (формируется только за весь период);
- **Журнал авторизованных администраторов** (формируется только за весь период).

Формат скачанного файла — *CSV.

Роли администраторов

Роли определяют, какие разделы и функции платформы доступны администратору. С их помощью можно настроить права доступа в зависимости от задач администратора.

Роли администраторов						+ Новая роль
Название	Профили LDAP	Группы пользователей			Частота синхронизации	Синхронизация
Только просмотр	Профиль №1	Финансы	Кадры	Разработчики	Каждый 1 час	▶ Запустить
Особый доступ		Отдел обучения	Логистика		Каждый 1 час	▶ Запустить
		Прочие сотрудники				
Администратор	LDAP-BOSS	Кадры	Прочие сотрудники			▶ Запустить
		Администраторы				

На платформе есть возможность связать роли администраторов Start AWR с группами в LDAP. Тогда система будет автоматически назначать роли пользователям, которые входят в указанные LDAP-группы.

Описание интерфейса

Блок «Роли администраторов» представлен в виде таблицы со столбцами:

- **Название** — название роли.
- **Профили LDAP** — LDAP-профили, с которыми связана роль
- **Группы пользователей** — группы пользователей из LDAP, которым назначена роль.
- **Частота синхронизации** — если настроена синхронизация по расписанию, показывает, с какой периодичностью она происходит.
- **Синхронизация** — показывает, какой способ синхронизации выбран для роли (при использовании LDAP-профиля). Возможны два варианта:
 - **Вручную** — администратор запускает синхронизацию самостоятельно в любое время.
 - **По расписанию** — синхронизация выполняется автоматически по заданному расписанию.

Особенности работы прав доступа у ролей

- Если администратору назначены несколько ролей, он получает все права из них. Например, одна роль дает доступ к просмотру отчетов, а другая — к скачиванию. При назначении обеих ролей администратор сможет и просматривать, и скачивать отчеты.
- Роль можно назначить нескольким группам.
- Группе можно назначить несколько ролей.

Создание роли

⚡ У администратора, который создает роль, должен быть включен доступ «Роли администраторов» в настройках роли.

Для создания роли:

1. Нажмите кнопку **Новая роль**.
2. В открывшемся окне заполните поля:

- **Название*** — укажите название для новой роли.
- **Страница по умолчанию** — выберите раздел, который будет открываться у администратора при входе на платформу.
- **Профиль LDAP** — при необходимости выберите LDAP-профиль для автоматического назначения роли пользователям.
 - **Группы** — выберите LDAP-группы, пользователям которых будет назначена роль при синхронизации.
 - **Синхронизация** — выберите, как будет выполняться синхронизация:
 - **Вручную** — синхронизация будет выполняться только после того, как администратор запустит ее самостоятельно.
 - **По расписанию** — синхронизация будет выполняться автоматически с заданной периодичностью.
- **Доступы** — отметьте доступы, которые будут разрешены администратору с этой ролью.

3. Нажмите кнопку **Добавить**.

Готово! Вы создали новую роль.

Редактирование роли

1. Нажмите на роль, которую нужно отредактировать.
2. Внесите изменения.
3. Нажмите кнопку **Сохранить**.

Готово! Вы изменили параметры роли.

Удаление роли

 Нельзя удалить системные роли «Только просмотр» и «Администратор». Для удаления доступны только пользовательские роли.

Чтобы удалить роль:

1. Нажмите три точки (⋮) напротив роли, которую нужно удалить.
2. Нажмите **Удалить**.
3. Подтвердите действие.

Готово! Вы удалили роль.

Вкладка «Работа с сотрудниками»

Настройки

Сохранить отладочную информацию Планировщик Обновить систему

Администраторы **Работа с сотрудниками** Обучение Почтовый плагин Тренировки Переменные

Профили LDAP

Журнал синхронизаций + Новый профиль LDAP

Название	URL	DN	Частота синхронизации	Синхронизация
Профиль №1	win1.antph.local	DC=antph,DC=local	Вручную	▶ Запустить
Профиль №2	win2.antph.local	DC=antph,DC=local	Вручную	▶ Запустить
Профиль №1	win3.antph.local	DC=antph,DC=local	Вручную	▶ Запустить

Профили SSO

+ Новый профиль SSO

Название
Профиль SSO 1

Здесь вы можете:

- создать, изменить или удалить профиль LDAP;
- скачать журнал синхронизаций;
- создать, изменить или удалить профиль SSO;
- указать количество дней, в течение которых сотрудник будет считаться новым;
- включить или отключить анонимный режим, который позволяет скрывать данные сотрудников в интерфейсе и отчетах.

Профили LDAP

LDAP-профиль используется для загрузки сотрудников из корпоративного каталога на платформу Start AWR.

Поддерживается подключение к следующим службам каталогов:

- Active Directory;
- OpenLDAP;
- FreeIPA.

Здесь вы можете создавать, изменять и удалять LDAP-профили, а также формировать отчет о синхронизациях за выбранный период.

Описание интерфейса

Блок «Профили LDAP» представлен в виде таблицы со столбцами:

- **Название** — имя профиля LDAP.
- **URL** — адрес, по которому система подключается к LDAP.
- **DN** — путь к подразделению или группе в структуре LDAP.
- **Частота синхронизации:**
 - если настроена синхронизация **по расписанию**, здесь отобразится периодичность ее запуска — например, каждые 7 дней;
 - если выбрана синхронизация **вручную**, отобразится значение «Вручную».
 - **Синхронизация** — отображается кнопка **Запустить**, которая позволяет запустить синхронизацию независимо от выбранного способа (вручную или по расписанию).

Создание профиля LDAP

Подробнее узнать о том, как создать LDAP-профиль, можно в разделе «[Импорт из LDAP](#)».

Редактирование профиля LDAP

1. Нажмите на LDAP-профиль, который нужно отредактировать.
2. Внесите изменения.
3. Нажмите кнопку **Сохранить**.

Готово! Вы изменили параметры LDAP-профиля.

Удаление профиля LDAP

Чтобы удалить LDAP-профиль:

1. Нажмите три точки (⋮) напротив профиля, который нужно удалить.
2. Нажмите **Удалить**.
3. Подтвердите действие.

Готово! Вы удалили профиль LDAP.

Журнал синхронизаций

Журнал синхронизаций позволяет получить подробный отчет о выполненных синхронизациях в формате CSV. В нем содержится информация о том, когда и каким способом выполнялась синхронизация, а также какие изменения произошли в данных сотрудников.

Журнал содержит следующую информацию:

- **Дата** — дата выполнения синхронизации.
- **Время** — время выполнения синхронизации.
- **LDAP-профиль** — имя профиля, с помощью которого выполнялась синхронизация.

- **Способ синхронизации** — вручную или автоматически (по расписанию).
- **Статус** — результат выполнения синхронизации.
- **Пользователь** — пользователь, который запустил синхронизацию.
- **Всего выбрано** — общее количество сотрудников, выбранных для синхронизации.
- **Добавлено** — количество добавленных после синхронизации сотрудников.
- **Обновлено** — количество сотрудников, данные которых обновлены в результате синхронизации.
- **Без изменений** — количество сотрудников, данные которых не изменились в результате синхронизации.
- **Не найдены в LDAP** — количество сотрудников, которые не найдены в корпоративном каталоге.
- **Удалено** — количество удаленных в результате синхронизации сотрудников.
- **Не синхронизировано** — количество сотрудников, для которых синхронизация не выполнена.

Профили SSO

Блок предназначен для настройки входа на платформу Start AWR через корпоративную систему аутентификации (SSO). Здесь можно создавать, изменять и удалять профили SSO.

Описание интерфейса

В блоке отображается список созданных SSO-профилей. Для каждого профиля указано его **Название**.

Добавление профиля SSO

Чтобы добавить профиль на платформу:

1. Нажмите кнопку **Новый профиль SSO**.
2. Заполните поля:
 - **Имя профиля SSO** — введите название, по которому профиль будет легко найти и отличить от других.
 - **MetaData URL** — укажите адрес для подключения к поставщику аутентификации. Например, в Microsoft Entra ID это значение находится в поле «App Federation Metadata Url».
3. Нажмите кнопку **Сохранить**.

Готово! Вы добавили профиль SSO на платформу.

Редактирование профиля SSO

1. Нажмите на профиль SSO, который нужно отредактировать.
2. Внесите изменения.

3. Нажмите кнопку **Сохранить**.

Готово! Вы изменили параметры профиля SSO.

Удаление профиля SSO

Чтобы удалить профиль:

1. Нажмите три точки (⋮) напротив профиля, который нужно удалить.
2. Нажмите **Удалить**.
3. Подтвердите действие.

Готово! Вы удалили профиль SSO.

Новый сотрудник

Здесь можно указать количество дней, в течение которых сотрудник будет считаться новым после добавления на платформу.

Новый сотрудник

Считать сотрудника новым в течение

дней

Вы можете установить значение от 1 до 999

Сохранить

В течение этого срока рядом с его именем будет отображаться метка «Новый».

Сотрудники **общим списком** ▾

+ Добавить

Не обучались
84 сотрудника

Не тренировались
55 сотрудников

Пользуются уязвимы...
9 сотрудников

Все сотрудники в сис...
114 сотрудников

Выбрать файлом
Только xlsx

Все сотрудники

березнякова × **Искать**

Выбрать найденных Фильтровать по обучению, поведению в атаках, рейтингу или по уязвимостям, меткам и новым сотрудникам

Сначала от А до Я фамилии ↑↓

Обучение

Тренировки

☐ ФИО и email	Должность и подраздел... Метки	Статус	Итоги последней атаки	Рейтинг
☐ Березнякова Олеся Викторовна Новый berezniakova@antph.local	Менеджер по обучению Обучение	Не обучался	Не проверялся	0

Метка помогает быстро находить и фильтровать новых сотрудников, например,

чтобы назначить им обучение или отправить атаку.

Анонимный режим

При включении анонимного режима данные сотрудников в интерфейсе и отчетах отображаются в обезличенном виде.

Анонимный режим

Скрывает данные сотрудников в интерфейсе и отчетах

Включен

Выключен

Вкладка «Обучение»

Настройки

АдминистраторыРабота с сотрудникамиОбучениеПочтовый плагинТренировкиПеременные

Курсы

Статистика по обучению+ Новый курс

Сначала видно в системе ↑↓

☐ Название	Владелец	Роль	Статус	Видно в системе	
☐ Основы информационной безопасности	Константинопольский Кирилл	Суперадминистратор Администратор	Назначен	☒	⋮
☐ Защита конфиденциальных данных	Константинопольский Кирилл	Суперадминистратор	Назначен	☒	⋮
☐ Защита персональных данных	Ахмадуллина Лейсан	Администратор	Назначен	☐	⋮
☐ Работа с электронной подписью	Константинопольский Кирилл	Суперадминистратор	Назначен	☐	⋮
☐ Создание и хранение паролей	Константинопольский Кирилл	Администратор	Назначен	☒	⋮
☐ Безопасная работа с электронной почтой	Кузнецов Владимир	Суперадминистратор	Назначен	☒	⋮

Сертификаты

Архив сертификатов сотрудников

Название	
Сертификат об успешном прохождении обучения 2026 По умолчанию	⋮
Сертификат об успешном прохождении обучения 2025	⋮
Сертификат об успешном прохождении обучения 2024	⋮

Уведомления

Здесь вы можете:

- добавлять, редактировать и удалять курсы;
- скачивать статистику по обучению за период;
- посмотреть список загруженных сертификатов об обучении сотрудников;
- загрузить сертификаты на других языках;
- скачать архив с сертификатами;
- создавать уведомления об обучении с нуля или на основе шаблона;
- запускать или останавливать работу уведомлений и напоминаний об обучении;
- кастомизировать личный кабинет сотрудника — настроить логотип, контактные данные и другие элементы, чтобы интерфейс соответствовал

внутренним требованиям и брендбуку компании.

Курсы

Описание интерфейса

Блок «Курсы» представлен в виде таблицы со столбцами:

- **Название** — название курса.
- **Владелец** — имя администратора, который загрузил курс на платформу.
- **Роль** — роль администратора, который загрузил курс на платформу.
- **Статус** — текущее состояние курса.
- **Видно в системе** — показывает, доступен ли курс сотрудникам.

Доступ администраторов к курсам

В зависимости от настроек роли администратору могут быть доступны все курсы или только те, которые он самостоятельно загрузил на платформу. От настроек роли зависит и то, какие действия он может с ними выполнять:

- Администратор со **включенным** параметром «Все курсы» — может выполнять все действия со всеми курсами, кроме редактирования и удаления. Редактировать и удалять он может только те курсы, которые загрузил самостоятельно.
- Администратор с **отключенным** параметром «Все курсы» — может выполнять все действия, но только с курсами, которые загрузил самостоятельно.
- Суперадминистратор — может выполнять все действия со всеми курсами на платформе.
 При добавлении курса суперадминистратором, курс появится у всех администраторов, у которых включена галочка «Все курсы».

Добавление курса

Чтобы загрузить курс на платформу, выполните следующие действия:

1. Подготовьте zip-архив с курсом и обложкой.
 Название курса состоит из порядкового номера, темы и проходного балла курса. Пример: «7. Безопасная работа с паролями 80». Эти данные пригодятся на этапе загрузки файла в систему.
2. Нажмите кнопку **Новый курс**.
3. В верхней части формы отобразятся вкладки с языками. В каждой из них вы можете загрузить курс на выбранном языке и задать для него собственные настройки.

Чтобы добавить курс, выберите вкладку с нужным языком и загрузите

zip-архив с курсом.

[← К настройкам](#)

Новый курс

* поля обязательные для заполнения

Русский English Italiano Português (BR) Français Deutsch Español O'zbekcha

☒ Язык по умолчанию

Загрузите файл с курсом

Подойдет только файл в формате .zip

Выбрать файл

Заккрыть

Добавить

4. Отредактируйте параметры загружаемого курса:

Русский English Italiano Português (BR) Français Deutsch Español O'zbekcha

☒ Язык по умолчанию

ZIP

3_RU_Zashchita_personalnykh_dannykh_scorn_75.zip

Удалить

Название*

Защита персональных данных

Защита персональных данных: как соблюдать закон и не нарушать права клиентов и коллег

→ Какие действия могут привести к утечке

→ Почему важно помнить о принципах обработки

→ Как безопасно работать с персональными данными

Итоговый тест

20 минут

Обложка 2604 x 912 px

Удалить

Проходной балл

75

%

☐ Можно изучать самостоятельно

Сертификат*

Default.htm

▼

Срок действия сертификата

180

дней

Заккрыть

Добавить

- **Язык по умолчанию*** — выберите язык, на котором сотрудники увидят курс, если у них в карточке не выбран язык, или курс на этом языке отсутствует в системе.

💡 Пример:

В системе есть курсы только на русском и английском языках. Язык по умолчанию — английский. У сотрудника в карточке выбран итальянский, но курса на этом языке нет, поэтому ему будет доступен курс на английском языке.

- **Название*** — укажите название курса. Оно будет отображаться у сотрудников и администраторов системы.
- **Обложка курса** — загрузите изображение, которое будет отображаться в карточке курса. Оно должно соответствовать требованиям:
 - формат — JPG, PNG или GIF,
 - соотношение сторон — 16:6,
 - минимальная ширина — 780 пикселей.
- **Проходной балл** — укажите проходной балл, который был указан в названии курса.
- **Можно изучать самостоятельно** — позволит сотрудникам проходить курс в любое время и не ждать, пока администратор назначит обучение. Если функция выключена, курс будет доступен только после назначения обучения.
- **Сертификат*** — выберите шаблон сертификата, который будет использоваться для этого курса.
- **Срок действия сертификата** — укажите количество дней, в течение которого будет действовать сертификат об обучении.

5. Нажмите кнопку **Добавить**.

Готово! Вы загрузили курс на платформу Start AWR.

Замена курса

Если нужно обновить содержание курса, выполните следующие действия:

1. Нажмите на курс, который нужно заменить.

2. Удалите старый файл с курсом.

← К настройкам

Редактирование курса

* поля обязательные для заполнения

Русский English Italiano Português (BR) Français Deutsch Español O'zbekcha

☒ Язык по умолчанию

ZIP 02_Bezopasnaya_rabota_s_parolyami SCORM.zip **Удалить**

Название*
Безопасная работа с паролями

Загрузите обложку курса
Подойдет только файл в формате .png или .gif. Соотношение сторон изображения 16:6, минимальная ширина 780px

Выбрать файл

Закрыть Сохранить

3. Добавьте новый курс.

Удаление курса

⚡ Удаление курса влечет за собой потерю всей статистики. Если вы хотите сохранить эти данные, рекомендуем не удалять курс, а заменить его.

1. Нажмите три точки (⋮) напротив профиля, который нужно удалить.
2. Нажмите **Удалить**.
3. Подтвердите действие.

Готово! Курс удален.

В течение нескольких секунд можно отменить удаление курса. Для этого нажмите кнопку **Отменить удаление** на уведомлении.

Сертификаты

В этом блоке представлен список сертификатов, загруженных на платформу.

Сертификаты		Архив сертификатов сотрудников
Название		
Сертификат об успешном прохождении обучения 2026	По умолчанию	⋮
Сертификат об успешном прохождении обучения 2025		⋮
Сертификат об успешном прохождении обучения 2024		⋮

Описание интерфейса

Блок «Сертификаты» представлен в виде списка с названиями загруженных сертификатов.

Также здесь доступна кнопка **Архив сертификатов сотрудников**, которая позволяет скачать сертификаты сотрудников за выбранный период.

Добавление сертификата

Чтобы загрузить сертификат на платформу, обратитесь в службу поддержки Start AWR.

Редактирование сертификата

Если нужно заменить шаблон сертификата, добавить версию на другом языке или обновить настройки:

1. Нажмите на необходимый сертификат в списке.
2. Внесите изменения.
3. Нажмите кнопку **Сохранить**.

Готово! Вы внесли изменения в карточку сертификата об обучении.

Удаление сертификата

 Нельзя удалить сертификат, который выбран по умолчанию.

Для удаления сертификата выполните шаги:

1. Нажмите три точки (⋮) напротив сертификата, который нужно удалить.
2. Нажмите **Удалить**.
3. Подтвердите действие.

Готово! Вы удалили сертификат с платформы.

Уведомления

В этом блоке собраны уведомления об обучении, которые платформа отправляет сотрудникам. При необходимости в них можно изменить текст и оформление, а также добавить переменные.

Уведомления				
По обучению				
Название		Статус	Действие	
Назначен на курс		Запущено	▶ Запустить	⋮
Назначен на несколько курсов		Остановлено	▶ Запустить	⋮
Не прошел курс вовремя		Остановлено	▶ Запустить	⋮
Не прошел несколько курсов вовремя		Запущено	▶ Запустить	⋮
Сертификат об окончании курса		Запущено	▶ Запустить	⋮
Ссылка для входа		Запущено	▶ Запустить	⋮
Напоминания об обучении				
Название		Статус	Действие	
Для одного курса		Запущено	▶ Запустить	⋮
Для нескольких курсов		Остановлено	▶ Запустить	⋮
Пользовательские				+ Новое уведомление
Название	Курсы	Действие с сотрудником	Статус	Действие
Не прошел несколько курсов вовремя — копия	Атаки через картинки	Не прошел курс вовремя	Остановлено	▶ Запустить
Сертификат об окончании курса — копия	Мобильная безопасность в эпоху VPN Безопасность на рабочем месте, скрытая угроза	Не прошел несколько курсов вовремя	Остановлено	▶ Запустить
Кастомное уведомление для новых сотрудников	Атаки через картинки Email атаки в 2026 — новые схемы	Назначен на курс	Запущено	▶ Запустить

Настроить правила отправки уведомлений можно через инструменты «Процессы» или «Планировщик».

В системе существует несколько типов уведомлений:

- **По обучению** — шесть стандартных уведомлений, связанных с обучением сотрудников. Их можно редактировать, копировать и восстанавливать до исходного состояния, но нельзя удалять.

По умолчанию в системе предусмотрены следующие уведомления:

- Назначен на курс;
- Назначен на несколько курсов;
- Не прошел курс вовремя;
- Не прошел несколько курсов вовремя;
- Сертификат об окончании курса;
- Ссылка для входа.
- **Напоминания об обучении** — уведомления, которые напоминают сотрудникам о дедлайне по курсу. Доступны два вида напоминаний:
 - Для одного курса;
 - Для нескольких курсов.

Чтобы руководители могли следить за обучением сотрудников и при необходимости напоминать им о приближающихся сроках, включите параметр **Отправлять копию руководителю** в настройках напоминания.

Копии напоминаний будут отправляться руководителю, указанному в карточке сотрудника.

- **Пользовательские** — уведомления, которые создает администратор или копирует из существующих.

Создание уведомления

Чтобы создать новое уведомление, выполните шаги:

1. Нажмите кнопку **Новое уведомление**.
2. Заполните следующие поля:
 - **Язык*** — выберите вкладку с нужным языком.
Заполнять все вкладки не обязательно. Если в компании сотрудники используют только один язык (например, русский), достаточно заполнить только соответствующую вкладку.
Если уведомление не настроено на языке сотрудника, система отправит его на том языке, который выбран по умолчанию.
 - **Название*** — укажите название уведомления. Например, «Напоминание о прохождении курса» или «Отправка сертификата».
 - **Тема письма*** — укажите тему, которая отобразится в списке писем электронной почты у получателя. Например, «Вам назначен новый курс» или «Поздравляем! Вы получили сертификат».
 - **Отправитель*** — выберите, от чьего имени будет отправлено уведомление. Например, «Отдел обучения» или «HR-служба».
 - **Электронная почта*** — укажите электронный адрес, с которого придет письмо.
 - **Домен*** — укажите домен, с которого придет письмо.
 - **Текст письма*** — оформите текст письма с помощью редактора, переменных или исходного кода.
 - **Действие*** — выберите из списка событие, при котором будет отправляться уведомление.
3. Нажмите кнопку **Добавить**.

Готово! Уведомление создано, оно отобразится в списке пользовательских уведомлений.

Редактирование уведомления

Если нужно изменить какие-либо параметры уведомления, вы можете отредактировать его. Для этого:

1. Нажмите на необходимое уведомление.
2. Внесите изменения.
3. Нажмите кнопку **Сохранить**.

Готово! Вы отредактировали уведомление.

Запуск и остановка уведомления

Для уведомления, к которому привязаны действие и один или несколько курсов, доступны кнопки **Запустить** и **Остановить**. Они позволяют включать и приостанавливать отправку уведомления сотрудникам.

💡 После запуска пользовательского уведомления система перестает отправлять стандартное (системное) уведомление с тем же действием.

Для того, чтобы настроить правило отправления уведомления, к которому не прикреплены курс или курсы, нужно воспользоваться инструментом

Планировщик:

1. Перейдите в **Меню** и нажмите **Планировщик** в правом верхнем углу.
2. Нажмите кнопку **Добавить**.
3. В открывшемся окне заполните поля:
 - **Название** — укажите название правила, чтобы его было легче найти в списке.
 - **Что случилось** — выберите триггер, который запустит правило.
 - **Что нужно сделать** — укажите действие, которое выполнит система при срабатывании триггера.
 - **Выполнить** — настройте время выполнения правила: сразу, с задержкой или не чаще, чем.
 - **Применить** — выберите, на кого распространяется правило.
💡 По умолчанию выбрано значение «Применить». Для изменения на «Не применять», нажмите на слово «Применить».

Доступны следующие варианты:

- **Применить** — правило сработает для выбранных сотрудников.
 - **Не применять** — правило не будет действовать для выбранных сотрудников.
 - **Ко всем сотрудникам** — правило применится ко всем сотрудникам без исключения.
 - **Инвертировать выбор** — правило сработает для всех, кроме выбранных сотрудников.
4. Нажмите кнопку **Сохранить**.

Готово! Правило создано. После запуска правила платформа будет автоматически отправлять уведомление при срабатывании триггера.

Удаление уведомления

💡 Удалить можно только пользовательские уведомления.

Чтобы удалить уведомление:

1. Нажмите три точки (⋮) напротив уведомления, которое нужно удалить.
2. Выберите **Удалить**.
3. Подтвердите действие.

Готово! После удаления уведомления (или правила с ним) система автоматически возобновит отправку стандартного уведомления.

Система электронного обучения

Администратор может настроить логотип, контактные данные и другие элементы личного кабинета, чтобы интерфейс соответствовал внутренним требованиям и брендбуку компании.

Система электронного обучения

* поля обязательные для заполнения

Встроенная

Внешняя

Адрес

http://

https://

Адрес*

Загрузите логотип

Подойдет файл в формате .png .jpg или .gif
Рекомендуемая ширина 248 px, высота 40—80 px

Выбрать файл

Название

Небольшой комментарий под логотипом

Описание

Ссылка на копирайта

http://

https://

Адрес

Телефон поддержки

Язык
Русский

На прохождение курсов

2

Дня

Недели

Вы можете установить значение от 1 до 999

Тип авторизации

Токен

LDAP

Токен/SSO

LDAP/SSO

Ссылка на обучение

Бессрочная

Одноразовая

Сохранить настройки

По умолчанию платформа Start AWR использует стандартные значения, которые можно заменить на свои. Заполните поля, которые хотите изменить:

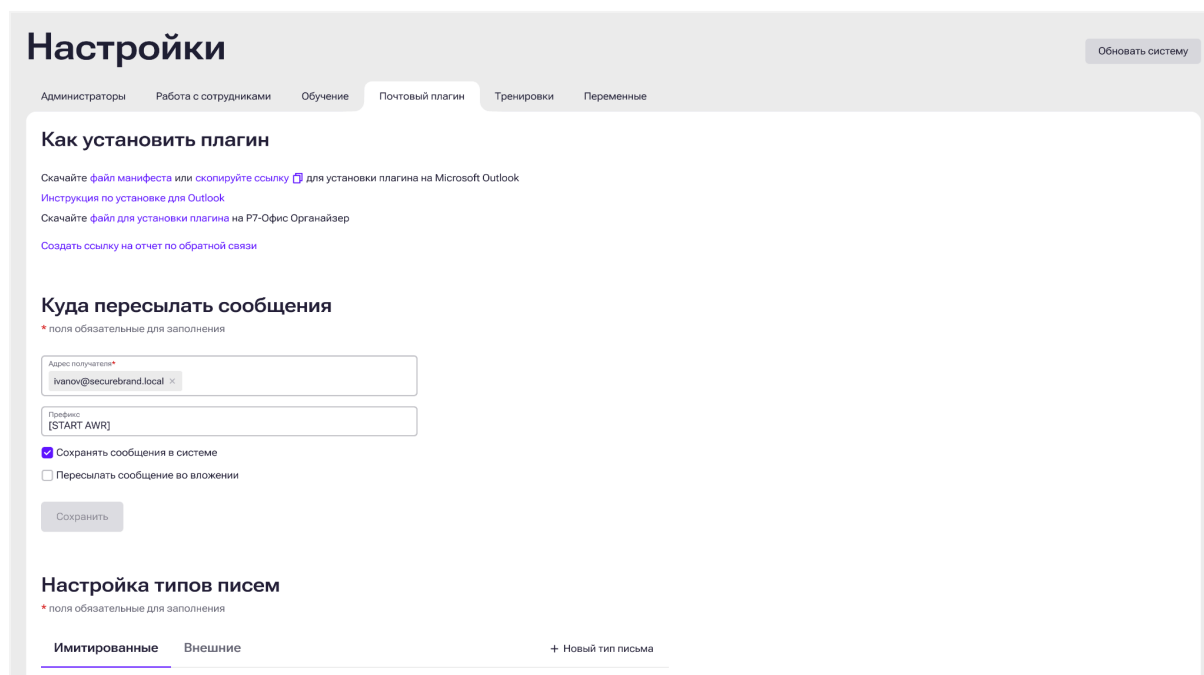
- **Адрес** — укажите адрес системы обучения. По умолчанию здесь указан адрес, который подтягивается из настроек сервера вашей компании.
 - **Логотип** — загрузите изображение в формате .jpeg или .png, которое будет отображаться в верхней части страницы.
 - **Название** — введите текст, который будет отображаться на вкладке браузера (рядом с фавиконом).
 - **Описание** — добавьте краткий текст, который поможет сотрудникам понять, для чего предназначен личный кабинет.
 - **Ссылка на копирайта** — укажите веб-адрес страницы, которую вы хотите разместить внизу личного кабинета. Это может быть сайт компании, внутренний документ или другая полезная ссылка.
 - **Телефон поддержки** — укажите номер телефона или электронную почту, по которым сотрудник может обратиться с вопросами.
💡 Номер телефона можно вводить в любом формате.
 - **Язык** — выберите язык, на котором по умолчанию будет отображаться интерфейс личного кабинета у сотрудников.
 - **На прохождение курсов** — укажите количество дней или недель, которое дается сотруднику на прохождение курса.
💡 Указанное количество будет по умолчанию подставляться при назначении новых курсов. При необходимости администратор сможет изменить этот срок.
 - **Тип авторизации** — выберите, каким способом сотрудники будут входить в личный кабинет. Доступны два варианта:
 - **Токен** — вход по уникальной ссылке, которая приходит сотруднику на электронную почту;
 - **LDAP** — вход с использованием корпоративного логина и пароля;
 - **Токен/SSO** — вход с использованием уникальной ссылки на электронную почту и через корпоративную учетную запись (SSO).
 - **LDAP/SSO** — вход с использованием корпоративных данных с помощью LDAP или через SSO.
 - **Ссылка на обучение** — укажите тип ссылки для входа сотрудника в систему:
 - **Бессрочная** — ссылка действует без ограничений по времени и может использоваться многократно. Ссылка становится бессрочной, если выбран способ авторизации через LDAP или SSO.
 - **Одноразовая** — по такой ссылке можно войти только один раз. После первого входа она будет активной в том браузере, где была открыта. В другом браузере или после очистки кэша ссылка станет нерабочей.
⚡ Доступно только для типа авторизации «Токен».
- Что будет, если после генерации ссылки переключить тип ссылки с «Одноразовая» на «Бессрочная» (и наоборот):

- Если по одноразовой ссылке уже входили, переключение типа на «Бессрочная» не сделает ее активной.
- Если по одноразовой ссылке еще не входили, после переключения типа на «Бессрочная» ссылка станет бессрочной.
- После переключения бессрочной ссылки на тип «Одноразовая», ссылка станет одноразовой.

 Формат бессрочной и одноразовой ссылки одинаковый.

После внесения всей необходимой информации нажмите **Сохранить настройки**.

Вкладка «Почтовый плагин»



Настройки Обновить систему

Администраторы Работа с сотрудниками Обучение **Почтовый плагин** Тренировки Переменные

Как установить плагин

Скачайте [файл манифеста](#) или [скопируйте ссылку](#) для установки плагина на Microsoft Outlook
[Инструкция по установке для Outlook](#)
 Скачайте файл для установки плагина на P7-Офис Органайзер
[Создать ссылку на отчет по обратной связи](#)

Куда пересылать сообщения

* поля обязательные для заполнения

Адрес получателя*
 ivanov@securebrand.local x

Префикс
 [START AWR]

☒ Сохранять сообщения в системе
☐ Пересылать сообщение во вложении

Сохранить

Настройка типов писем

* поля обязательные для заполнения

Имитированные Внешние + Новый тип письма

Здесь содержатся параметры для настройки плагина Start AWR, который позволяет сотруднику сообщать об атаках по электронной почте прямо из почтового клиента Microsoft Outlook. Подробнее о настройке можно узнать в разделе «Почтовый плагин».

Вкладка «Тренировки»

Настройки

АдминистраторыРабота с сотрудникамиОбучениеПочтовый плагиинТренировкиПеременные

Беспроводные сети

⚡ К тренировкам + Новое устройство

Устройство	IP-адрес	Статус	Тренировка
Бесплатный Wi-Fi, работает без VPN	255.233.254.229	Подключено	Бесплатный Wi-Fi без VPN и СМС
Платный доступ в интернет, требуется авторизация	192.168.1.1	Ошибка авторизации	Платный интернет с личным кабинетом
Гостевая сеть, ограниченная скорость	10.0.0.5	Подключено	Гостевая Wi-Fi сеть с ограничениями
Сеть для сотрудников, доступ по паролю	172.16.0.10	Подключено	Закрытая сеть для сотрудников

Шаблоны из электронной почты

+ Новый почтовый сервер

Импортируйте шаблоны email-атак из почтового ящика. При включенной двухфакторной аутентификации импорт может быть ограничен

Название	Адрес сервера	Пользователь
Корпоративные шаблоны	ldap.secure@securebrand.com	secureuser@securebrand.com
Рассылки	admin.secure@securebrand.com	guest.secure@securebrand.com
Зона доступа с оповещениями	alert.secure@securebrand.com	monitor.secure@securebrand.com

Беспроводные сети

Блок предназначен для настройки точек доступа, которые используются для проведения имитированных атак по Wi-Fi. Такие атаки помогают научить сотрудников распознавать угрозы при подключении к посторонним Wi-Fi-сетям и соблюдать необходимые меры предосторожности.

Здесь администратор может добавить, изменить или удалить устройство, а также скопировать его токен для настройки.

Описание интерфейса

Блок «Беспроводные сети» представлен в виде таблицы со столбцами:

- **Устройство** — название устройства для имитации Wi-Fi атаки.
- **IP-адрес** — IP-адрес устройства, которое используется для имитации Wi-Fi атаки.
- **Статус** — текущее состояние устройства.
- **Тренировка** — атака, в которой используется устройство.

Добавление устройства

1. Нажмите кнопку **Новое устройство**.
2. Заполните поля:
 - **Название*** — укажите название устройства, по которому его будет легко найти в системе Start AWR. Сотрудники его не увидят.
 - **IP*** — введите IP-адрес устройства, которое будет использоваться для имитации Wi-Fi атаки.

- **Имя сети*** — укажите название сети (SSID), которое сотрудники будут видеть в списке доступных сетей Wi-Fi.
- **Логин*** — укажите логин устройства.
- **Пароль*** — укажите пароль устройства.

← К настройкам

Новое устройство

* поля обязательные для заполнения

Название*

IP*

В IP допускаются символы: 0.0.0.0 – 255.255.255.255

Имя сети: SSID*

Сотрудник увидит название в списке доступных беспроводных сетей

Данные для входа

Проверьте, что логин и пароль совпадают с настройками роутера

Логин*

Пароль*

👁

Заккрыть

Сохранить

3. Нажмите кнопку **Сохранить**.

Готово! После сохранения система проверит подключение к устройству. Если проверка пройдет успешно, устройство будет добавлено в список со статусом «Подключено».

Редактирование устройства

💡 Редактировать можно только то устройство, которое не используется в активной атаке.

1. Нажмите на устройство, параметры которого нужно изменить.
2. Внесите изменения.
3. Нажмите кнопку **Сохранить**.

Удаление устройства

💡 Перед удалением устройства остановите атаку, в которой оно используется.

Чтобы удалить устройство:

1. Нажмите три точки (⋮) напротив устройства, которое нужно удалить.
2. Выберите **Удалить**.
3. Подтвердите действие.

Шаблоны из электронной почты

В Start AWR есть возможность выгружать письма из корпоративной почты на платформу и использовать их для подготовки имитированных атак. Например, письмо из рабочей переписки можно взять за основу атаки и сохранить как шаблон для дальнейшего использования.

В блоке «Шаблоны из электронной почты» администратор может настроить подключение к корпоративной почте, а также изменить параметры или удалить.

Описание интерфейса

Блок «Шаблоны из электронной почты» представлен в виде таблицы со столбцами:

- **Название** — название подключения к почте.
- **Адрес сервера** — адрес почтового сервера.
- **Пользователь** — учетная запись, с которой выполняется подключение к почте.

При нажатии на подключение откроется список импортированных шаблонов писем.

Добавление сервера для шаблонов

1. Нажмите кнопку **Новый почтовый сервер**.
2. Заполните поля:
 - **Название*** — введите название подключения.
 - **Тип шифрования*** — выберите один из вариантов: Нет шифрования, SSL или TLS.
 - **Порт*** — укажите порт почтового сервера
 - **Адрес сервера*** — укажите адрес почтового сервера.
 - **Имя пользователя*** — введите имя пользователя для подключения к почтовому серверу.
 - **Пароль*** — пароль пользователя для подключения к почтовому серверу.
3. Нажмите кнопку **Добавить**.

Готово! Подключение настроено. Список импортированных шаблонов будет доступен внутри подключения.

Чтобы использовать шаблон, откройте подключение и выберите нужное письмо. Откроется форма создания атаки, где можно настроить ее параметры.

Редактирование сервера для шаблонов

Чтобы отредактировать параметры сервера:

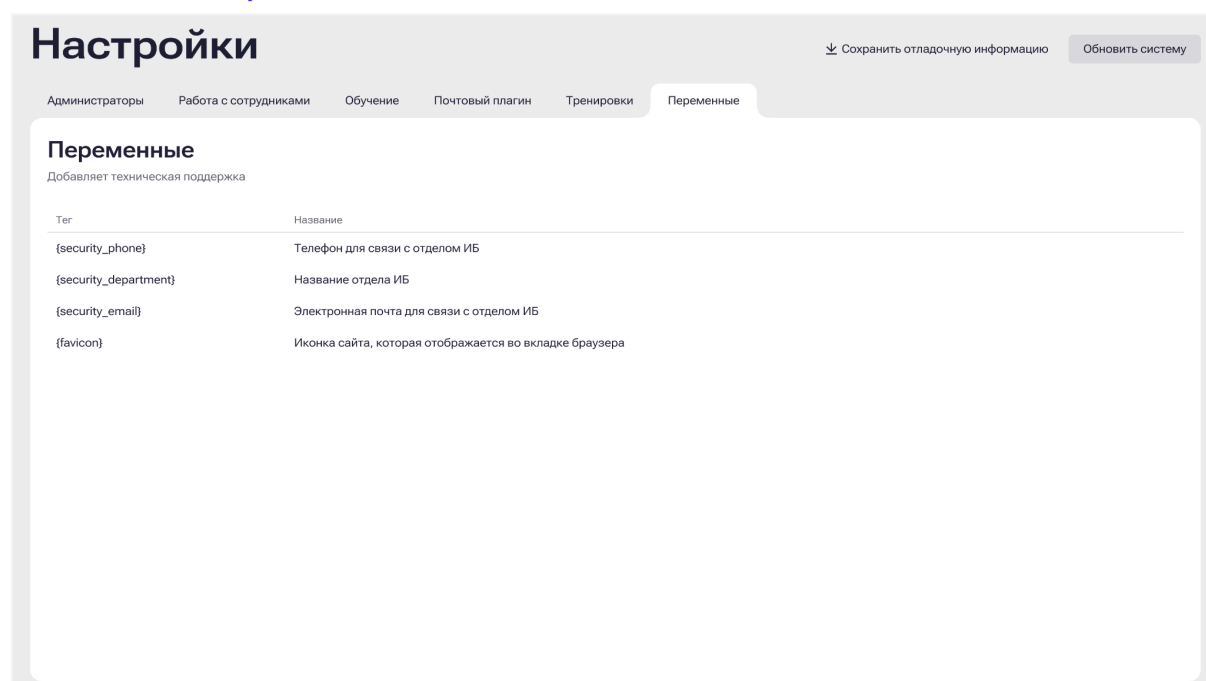
1. Нажмите на подключение, параметры которого нужно изменить.
2. Внесите изменения.
3. Нажмите кнопку **Сохранить**.

Удаление сервера для шаблонов

Чтобы удалить подключение:

1. Нажмите три точки (⋮) напротив подключения, которое нужно удалить.
2. Выберите **Удалить**.
3. Подтвердите действие.

Вкладка «Переменные»



Переменные помогают персонализировать имитированные атаки и сделать письма более похожими на реальные. Их можно использовать в шаблонах писем, вложениях, а также на фишинговой и финальной страницах. Во время рассылки переменные автоматически заменяются на нужные значения.

Во вкладке «Переменные» доступны кастомные переменные. Для них значение задается вручную и подставляется везде, где используется переменная. Добавить такую переменную можно через обращение в техническую поддержку Start AWR.

💡 Ознакомиться со списком доступных переменных можно в главе «[Переменные](#)».

Раздел «Сотрудники»

Расскажем, как работать с подразделениями и сотрудниками, а также, как упростить повседневные рабочие задачи с помощью различных функций системы.

Работа с подразделениями

Создание подразделения

1. Перейдите в **Меню** → **Сотрудники**.

Подразделение	Обучение	Тренировки	Рейтинг
Сотрудники	57	47	44
Системное администрирование	15	0	48
Маркетинг	9	7	1

2. Нажмите кнопку **Добавить** и выберите **Подразделение**.

Подразделение	Обучение	Тренировки	Рейтинг
Сотрудники	57	47	44
Системное администрирование	15	0	48
Маркетинг	9	7	1

3. Заполните поля:

← К сотрудникам

Новое подразделение

* поля, обязательные для заполнения

Название*
SEO

Внутри подразделения
Маркетинг

Заккрыть

Добавить

- **Название*** — укажите название подразделения.
 - **Внутри подразделения** — выберите подразделение, в составе которого будет новое.
- 💡 Если оставить поле пустым, подразделение сохранится как корневое.

4. Нажмите кнопку **Добавить**.

Готово! Вы создали подразделение.

Редактирование подразделения

1. Перейдите в **Меню → Сотрудники**.

Start AWR Securebrand

Ключевые показатели

Сотрудники

Группы риска

Обучение

Тренировки

Уязвимости

Отчеты

Все разделы

Настройки

Русский

Иванов И.
ivanivanov@securebrand.local
Start X +7 (499) 677-19-07

Сотрудники по подразделениям

+ Добавить

Не тренировались 54 сотрудника

Пользуются уязви... 2 сотрудника

Все сотрудники в с... 81 сотрудник

Выбрать файлом Только xlsx

Подразделения

Подразделения, ФИО, email, должность, метка сотрудника

Искать

Сотрудников по обучению, поведению в атаках, рейтингу или по уязвимостям, меткам и новым сотрудникам

Выбрать всех

Подразделения	Сотрудники	Обучение		Тренировки		Рейтинг
		Не обучались	Просрочили	Не проверялись	Провалили	
Подразделение	57	4	37	47	0	44 ↑
Министрирование	15	3	11	0	0	48 ↑
Подразделения	9	1	8	7	1	1 ↑

2. В верхней части интерфейса выберите отображение списка сотрудников

— по подразделениям.

Сотрудники по подразделениям ▾ + Добавить

Не обучались 8 сотрудников Не тренировались 54 сотрудника Пользуются уязви... 2 сотрудника Все сотрудники в с... 81 сотрудник Выбрать файлом Только xlsx

Все подразделения

Название подразделения, ФИО, email, должность, метка сотрудника 🔍 Искать

Показать сотрудников по обучению, поведению в атаках, рейтингу или по уязвимостям, меткам и новым сотрудникам [Выбрать всех](#)

Сначала крупные подразделения ↑↓	Сотрудники	Обучение	Тренировки	Рейтинг
☐ Название и вложенность		Не обучались Просрочили	Не проверялись Провалили	
☐ DevOps 6 вложенных подразделений	57	4 37	47 0	44 ↑ ⋮
☐ Системное администрирование Нет вложенных подразделений	15	3 11	0 0	48 ↑ ⋮
☐ Маркетинг 3 вложенных подразделения	9	1 8	7 1	1 ↑ ⋮

3. Найдите в списке нужное подразделение. Нажмите напротив него на три точки (⋮) и **Редактировать**.

Сотрудники по подразделениям ▾ + Добавить

Не обучались 8 сотрудников Не тренировались 54 сотрудника Пользуются уязви... 2 сотрудника Все сотрудники в с... 81 сотрудник Выбрать файлом Только xlsx

Все подразделения

Название подразделения, ФИО, email, должность, метка сотрудника 🔍 Искать

Показать сотрудников по обучению, поведению в атаках, рейтингу или по уязвимостям, меткам и новым сотрудникам [Выбрать всех](#)

Сначала крупные подразделения ↑↓	Сотрудники	Обучение	Тренировки	Рейтинг
☐ Название и вложенность		Не обучались Просрочили	Не проверялись Провалили	
☐ DevOps 6 вложенных подразделений	57	4 37	47 0	44 ↑ ⋮
☐ Системное администрирование Нет вложенных подразделений	15	3 11	0 0	48 ↑ ⋮
☐ Маркетинг 3 вложенных подразделения	9	1 8	7 1	1 ↑ ⋮

Редактировать

4. Внесите необходимые изменения.

💡 Если оставить поле **Внутри подразделения** пустым, подразделение сохранится как корневое. Чтобы переместить подразделение, обязательно выберите нужное из выпадающего списка.

← К сотрудникам

Редактирование подразделения

* поля, обязательные для заполнения

Название*
Маркетинг и PR

Внутри подразделения
Команда 1

Заккрыть Сохранить

5. Нажмите кнопку **Сохранить**.

Готово! Вы отредактировали карточку подразделения.

Удаление подразделения

💡 При удалении подразделения сотрудники внутри него тоже удалятся. Если вы хотите сохранить сотрудников в системе, перенесите их в другое подразделение.

1. Перейдите в **Меню** → **Сотрудники**.

Start AWR Securebrand

Ключевые показатели

Сотрудники ←

Группы риска

Обучение

Тренировки

Уязвимости

Отчеты

Все разделы

Настройки

Русский

Иванов И.
ivanivanov@securebrand.local

Start X +7 (499) 677-19-07

Сотрудники по подразделениям

+ Добавить

Не тренировались 54 сотрудника

Пользуются уязви... 2 сотрудника

Все сотрудники в с... 81 сотрудник

Выбрать файлом Только xlsx

Подразделения

Подразделения, ФИО, email, должность, метка сотрудника

Искать

Сотрудников по обучению, поведению в атаках, рейтингу или по уязвимостям, меткам и новым сотрудникам

Выбрать всех

Подразделения	Сотрудники	Обучение		Тренировки		Рейтинг
		Не обучались	Просрочили	Не проверялись	Провалили	
Подразделений	57	4	37	47	0	44 ↑
министрирование	15	3	11	0	0	48 ↑
х подразделений	9	1	8	7	1	1 ↑

2. В верхней части интерфейса выберите отображение списка сотрудников — по подразделениям.

The interface shows a sidebar with navigation icons and a main content area titled 'Сотрудники по подразделениям'. At the top, there are filters: 'Не обучались' (9 employees), 'Не тренировались' (55 employees), 'Пользуются уязви...' (2 employees), 'Все сотрудники в с...' (82 employees), and 'Выбрать файлом' (Only xlsx). Below these is a search bar and a 'Показать сотрудников' section with links for 'по обучению, поведению в атаках, рейтингу или по уязвимостям, меткам и новым сотрудникам' and a 'Выбрать всех' button. The main table lists departments with columns for 'Сотрудники', 'Обучение' (Не обучались, Просрочили), and 'Тренировки' (Не проверялись, Провалили, Рейтинг). The departments listed are DevOps, Системное администрирование, Маркетинг, and Техническая поддержка.

Сначала крупные подразделения ↑↓	Сотрудники	Обучение		Тренировки		
☐ Название и вложенность		Не обучались	Просрочили	Не проверялись	Провалили	Рейтинг
☐ DevOps 6 вложенных подразделений	57	4	37	47	0	44 ↑
☐ Системное администрирование Нет вложенных подразделений	15	3	11	0	0	48 ↑
☐ Маркетинг 3 вложенных подразделения	9	1	8	7	1	1 ↑
☐ Техническая поддержка 2 вложенных подразделения	2	2	0	2	0	0

3. Найдите в списке нужное подразделение и отметьте его галочкой.
💡 Чтобы удалить пустое подразделение, нажмите на три точки рядом с ним и выберите **Удалить**.

The interface is the same as the previous screenshot, but the 'Техническая поддержка' department is now selected with a blue checkmark. A red arrow points to this checkmark. At the bottom, a notification bar says 'Вы выбрали: 2 сотрудника' and there are buttons for 'Обучить' and 'Тренировать'.

Сначала крупные подразделения ↑↓	Сотрудники	Обучение		Тренировки		
☒ Название и вложенность		Не обучались	Просрочили	Не проверялись	Провалили	Рейтинг
☐ DevOps 6 вложенных подразделений	57	4	37	47	0	44 ↑
☐ Системное администрирование Нет вложенных подразделений	15	3	11	0	0	48 ↑
☐ Маркетинг 3 вложенных подразделения	9	1	8	7	1	1 ↑
☒ Техническая поддержка 2 вложенных подразделения	2	2	0	2	0	0

4. В нижней части появится контекстное меню. Нажмите на нем три точки.

Сотрудники по подразделениям ▾ + Добавить

Все подразделения

Название подразделения, ФИО, email, должность, метка сотрудника 🔍 Искать

Показать сотрудников по обучению, поведению в атаках, рейтингу или по уязвимостям, меткам и новым сотрудникам [Выбрать всех](#)

Сначала крупные подразделения ↑↓		Обучение		Тренировки		
Название и вложенность	Сотрудники	Не обучались	Просрочили	Не проверялись	Провалили	Рейтинг
☐ DevOps 6 вложенных подразделений	57	4	37	47	0	44 ↑
☐ Системное администрирование Нет вложенных подразделений	15	3	11	0	0	48 ↑
☐ Маркетинг 3 вложенных подразделения	9	1	8	7	1	1 ↑
☒ Техническая поддержка 2 вложенных подразделения	2	2	0	2	0	0

Вы выбрали: 2 сотрудника ×

Обучить Тренировать ...

5. Выберите пункт **Удалить из системы**.

Сотрудники по подразделениям ▾ + Добавить

Все подразделения

Название подразделения, ФИО, email, должность, метка сотрудника 🔍 Искать

Показать сотрудников по обучению, поведению в атаках, рейтингу или по уязвимостям, меткам и новым сотрудникам [Выбрать всех](#)

Сначала крупные подразделения ↑↓		Обучение		Тренировки		
Название и вложенность	Сотрудники	Не обучались	Просрочили	Не проверялись	Провалили	Рейтинг
☐ DevOps 6 вложенных подразделений	57	4	37	47	0	44 ↑
☐ Системное администрирование Нет вложенных подразделений	15	3	11	0	0	48 ↑
☐ Маркетинг 3 вложенных подразделения	9	1	8	7	1	1 ↑
☒ Техническая поддержка 2 вложенных подразделения	2	2	0	2	0	0

Вы выбрали: 2 сотрудника ×

Обучить Тренировать ...

- Выбрать всех остальных, вместо выделенных
- Выгрузить данные сотрудников
- ☒ Подготовить отчет по действиям
- ☒ Подготовить отчет по обучению
- ☒ Подготовить отчет со сводной статистикой по сотрудникам
- Отменить обучение
- Удалить из системы**
- Редактировать

⚡ Вся статистика по подразделению безвозвратно удалится из системы и отчетов. Если в нем есть другие подразделения — они тоже будут удалены.

6. Появится список с сотрудниками из этого подразделения. Нажмите кнопку **Удалить**.

Сотрудники по подразделениям

Все подразделения

Название подразделения, ФИО, email, должность, метка сотрудника

Показать сотрудников по обучению, поведению в атаках, рейтингу или по уязвимостям, меткам и новым сотрудникам

Сначала крупные подразделения ↑↓	Сотрудники	Обучение		Тренировки
		Не обучались	Просрочили	
☐ DevOps 6 вложенных подразделений	57	4	37	47
☐ Системное администрирование Нет вложенных подразделений	15	3	11	0
☐ Маркетинг 3 вложенных подразделения	9	1	8	7
☒ Техническая поддержка 2 вложенных подразделения	2	2	0	2

Вы выбрали 2 сотрудников

Сбросить выбор

Митрофанов Игорь Родионович ×
Вторая линия тех. поддержки

Морозов Алексей Романович ×
Первая линия тех. поддержки

Вы собираетесь безвозвратно удалить сотрудников

Вся информация об этих сотрудниках, включая историю обучения и тренировок, будет удалена из системы.

Удалить **Не удалять**

Готово! Вы удалили подразделение.

Добавление сотрудников

Добавить сотрудников в систему можно тремя способами:

- вручную,
- из файла Excel в формате xlsx,
- с помощью LDAP.

Выберите подходящий вариант в зависимости от ваших задач.

Вручную

Этот способ позволяет добавлять в систему по одному сотруднику.

1. Перейдите в **Меню** → **Сотрудники**.

2. В правом верхнем углу нажмите кнопку **Добавить** и выберите **Сотрудников**.

Сотрудники по подразделениям

Не обучались: 8 сотрудников | Не тренировались: 54 сотрудника | Пользуются уязви...: 2 сотрудника | Все сотрудники в с...: 81 сотрудник

Выбрать с... Только xlsx | Подразделение

Все подразделения

Название подразделения, ФИО, email, должность, метка сотрудника

Показать сотрудников по обучению, поведению в атаках, рейтингу или по уязвимостям, меткам и новым сотрудникам | Выбрать всех

Сначала крупные подразделения ↑↓	Обучение	Тренировки	Рейтинг		
☐ Название и вложенность	Не обучались	Просрочили	Не проверялись	Провалили	
☐ DevOps 6 вложенных подразделений	57	4 37	47	0	44 ↑
☐ Системное администрирование Нет вложенных подразделений	15	3 11	0	0	48 ↑
☐ Маркетинг 2 вложенных подразделения	9	1 8	7	1	1 ↑

3. Во вкладке **Вручную** заполните поля:

← К сотрудникам **Добавление сотрудников**

* поля обязательные для заполнения

Вручную | Из файла | Из LDAP-профиля

Фамилия*
Городищев

Имя*
Петр

Отчество
Александрович

Электронная почта*
p.gorodishev @ Домен*
securebrand.local

Подразделение*
Маркетинг

Руководитель
Романов Станислав Игоревич

Группа риска
Средний уровень риска

Должность
SEO-специалист

Метки
Стажировка × Удаленка ×

Используйте метки, чтобы легко находить и объединять сотрудников по нужным критериям

Язык
Русский

Заккрыть | **Добавить**

- **Фамилия***
- **Имя***

- **Отчество**
- **Электронная почта***
- **Домен***
- **Подразделение***
- **Руководитель**
- **Группа риска**
- **Должность**
- **Метки** — укажите текстовые метки, которые помогут сгруппировать сотрудников по каким-либо признакам. Например: «На удаленке», «Офис Москва», «Стажировка».
- **Язык** — укажите язык, на котором сотрудник будет получать уведомления, курсы и сертификаты об обучении.

4. Нажмите кнопку **Добавить**.

Готово! Вы добавили нового сотрудника в систему. Он отобразится в общем списке.

Импорт из файла Excel

Этот способ позволяет добавить большое количество сотрудников и отделов одновременно. Также с помощью него удобно обновлять общие сведения о сотрудниках.

1. Перейдите в **Меню** → **Сотрудники**.

The screenshot displays the 'Сотрудники' (Employees) management interface. The sidebar menu on the left includes options like 'Ключевые показатели', 'Сотрудники' (highlighted with a red arrow), 'Группы риска', 'Обучение', 'Тренировки', 'Уязвимости', 'Отчеты', 'Все разделы', and 'Настройки'. The main content area shows a header with a search bar and a '+ Добавить' button. Below the header, there are four summary cards: 'Не тренировались' (54 сотрудника), 'Пользуются уязви...' (2 сотрудника), 'Все сотрудники в с...' (81 сотрудник), and 'Выбрать файлом' (Только xlsx). The main table displays employee data categorized by department (подразделения) and training status (Обучение, Тренировки). The table includes columns for 'Сотрудники', 'Не обучались', 'Просрочили', 'Не проверялись', 'Провалили', and 'Рейтинг'.

подразделения ↑↓	Сотрудники	Обучение		Тренировки		Рейтинг
Должность		Не обучались	Просрочили	Не проверялись	Провалили	
подразделений	57	4	37	47	0	44 ↑
министрирование	15	3	11	0	0	48 ↑
х подразделений	9	1	8	7	1	1 ↑

2. В правом верхнем углу нажмите кнопку **Добавить** и выберите **Сотрудников**.

Сотрудники по подразделениям

+ Добавить

Не обучались 8 сотрудников | Не тренировались 54 сотрудника | Пользуются уязви... 2 сотрудника | Все сотрудники в с... 81 сотрудник

Выбрать с... Только xlsx | **Сотрудников** | Подразделение

Все подразделения

Название подразделения, ФИО, email, должность, метка сотрудника

Показать сотрудников по обучению, поведению в атаках, рейтингу или по уязвимостям, меткам и новым сотрудникам | Выбрать всех

Сначала крупные подразделения ↑↓	Обучение	Тренировки	Рейтинг		
☐ Название и вложенность	Не обучались	Просрочили	Не проверялись	Провалили	
☐ DevOps 6 вложенных подразделений	57	4 37	47	0	44 ↑
☐ Системное администрирование Нет вложенных подразделений	15	3 11	0	0	48 ↑
☐ Маркетинг 2 вложенных подразделения	9	1 8	7	1	1 ↑

3. Выберите вкладку **Из файла**.

Добавление сотрудников

* поля обязательные для заполнения

☒ Вручную | **Из файла** | ☐ Из LDAP-профиля

Фамилия*

Имя*

Отчество

Электронная почта* @ Домен*

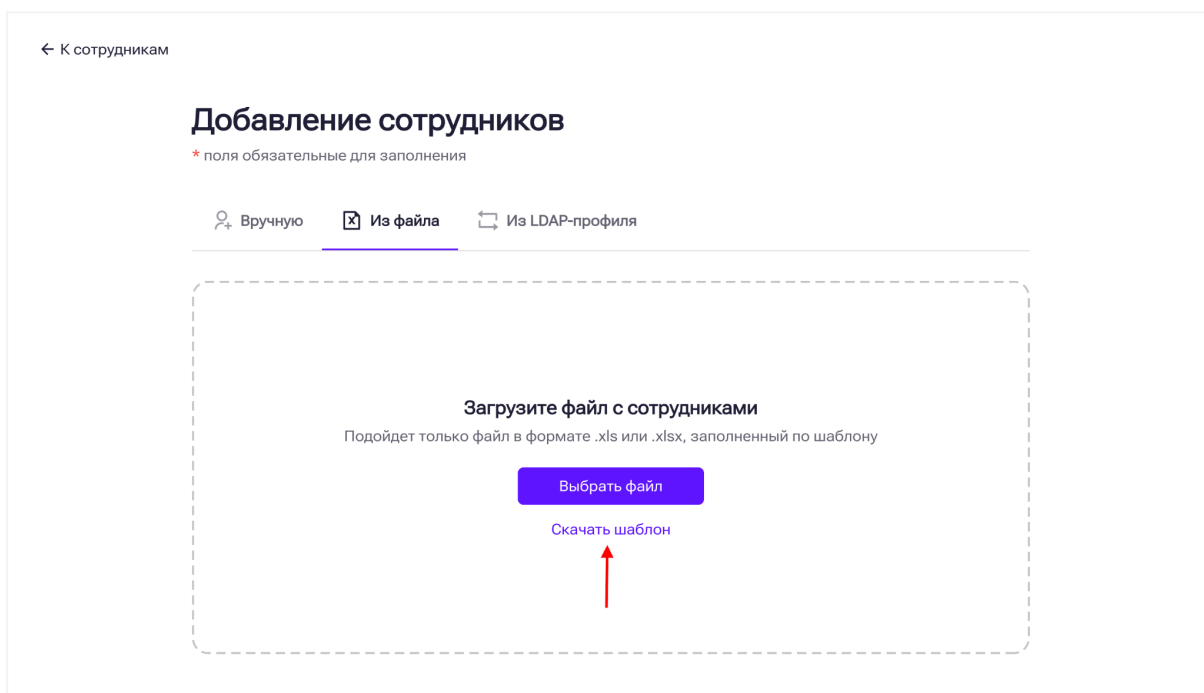
Подразделение*

Руководитель

Группа риска

Заккрыть | Добавить

4. Скачайте шаблон.



5. Заполните скачанный шаблон:

⚡ Столбцы в файле должны быть расположены строго в том порядке, как в скачанном шаблоне. Если порядок нарушен, импорт может пройти некорректно.

- **Email***
- **Фамилия***
- **Имя***
- **Отчество***
- **Должность**
- **Отдел*** — укажите название подразделения или команды. Чтобы создать вложенный отдел, укажите его название через слеш (/). Например: ИТ-отдел/Команда разработки. В этом случае «ИТ-отдел» будет отделом первого уровня (родительским), а «Команда разработки» — вложенным отделом второго уровня.
- **Метки** — укажите текстовые метки, которые помогут сгруппировать сотрудников по каким-либо признакам. Например: «На удаленке», «Офис Москва», «Стажировка». Чтобы добавить несколько меток, перечислите их в одной ячейке через точку с запятой и пробел. Например: первая метка; вторая метка; третья метка.
- **Группа риска** — укажите название группы, которая поможет объединить сотрудников по уровню безопасности и ответственности. Чтобы создать вложенную группу риска, укажите ее название через слеш (/). Например: Высокий риск/Работа с оборудованием.
- **Язык** — укажите язык, на котором сотрудник будет получать уведомления, курсы и сертификаты об обучении.

- **Руководитель** — укажите электронную почту руководителя импортируемого сотрудника.

Пример заполненного шаблона:

Email*	Фамилия*	Имя*	Отчество*	Должность
m.krylova@securebrand.local	Крылова	Мария	Сергеевна	Контент-маркетолог
a.zakharov@securebrand.local	Захаров	Алексей	Петрович	SEO-специалист
e.melnik@securebrand.local	Мельникова	Елена	Андреевна	SEO-специалист
d.sysoev@securebrand.local	Сысоев	Дмитрий	Олегович	SEO-специалист

Отдел*	Метки	Группа риска	Язык	Руководитель
Маркетинг/SMM	Удаленка; Стажировка	Средний уровень	Русский	s.ivanov@securebrand.local
Маркетинг/SEO	Удаленка	Средний уровень	Русский	
Маркетинг	Удаленка	Средний уровень	Русский	s.ivanov@securebrand.local
Маркетинг/SEO	Удаленка	Средний уровень	English	

6. Загрузите заполненный шаблон в систему.

← К сотрудникам

Добавление сотрудников

* поля обязательные для заполнения

Вручную

Из файла

Из LDAP-профиля

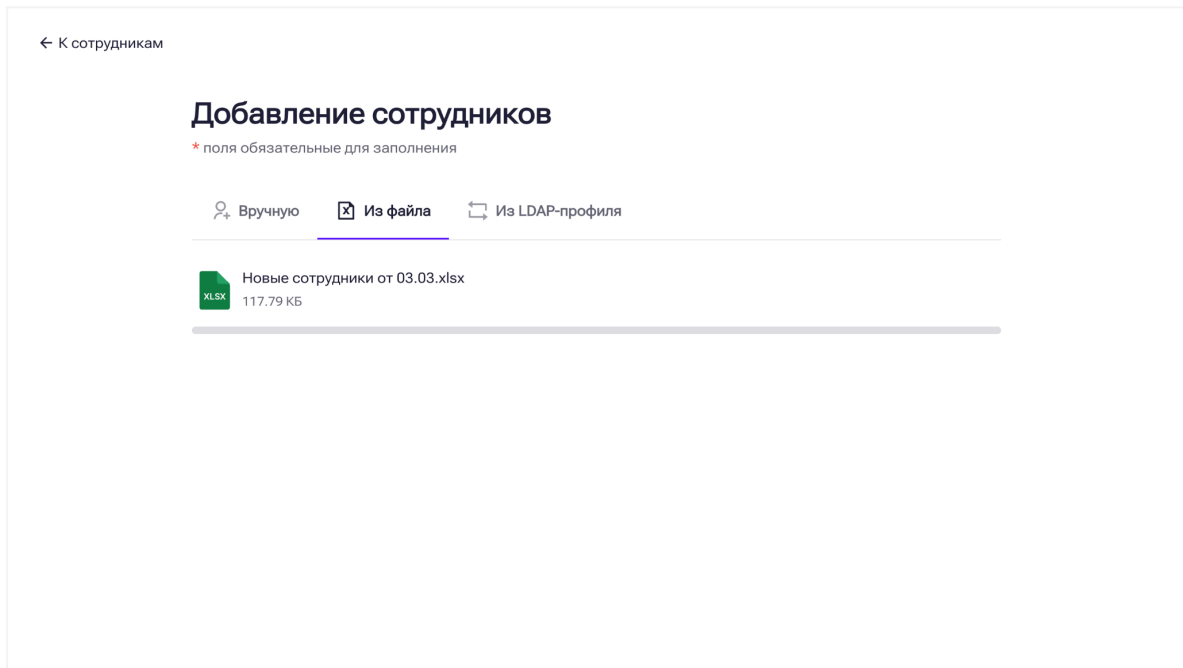
Загрузите файл с сотрудниками

Подойдет только файл в формате .xls или .xlsx, заполненный по шаблону

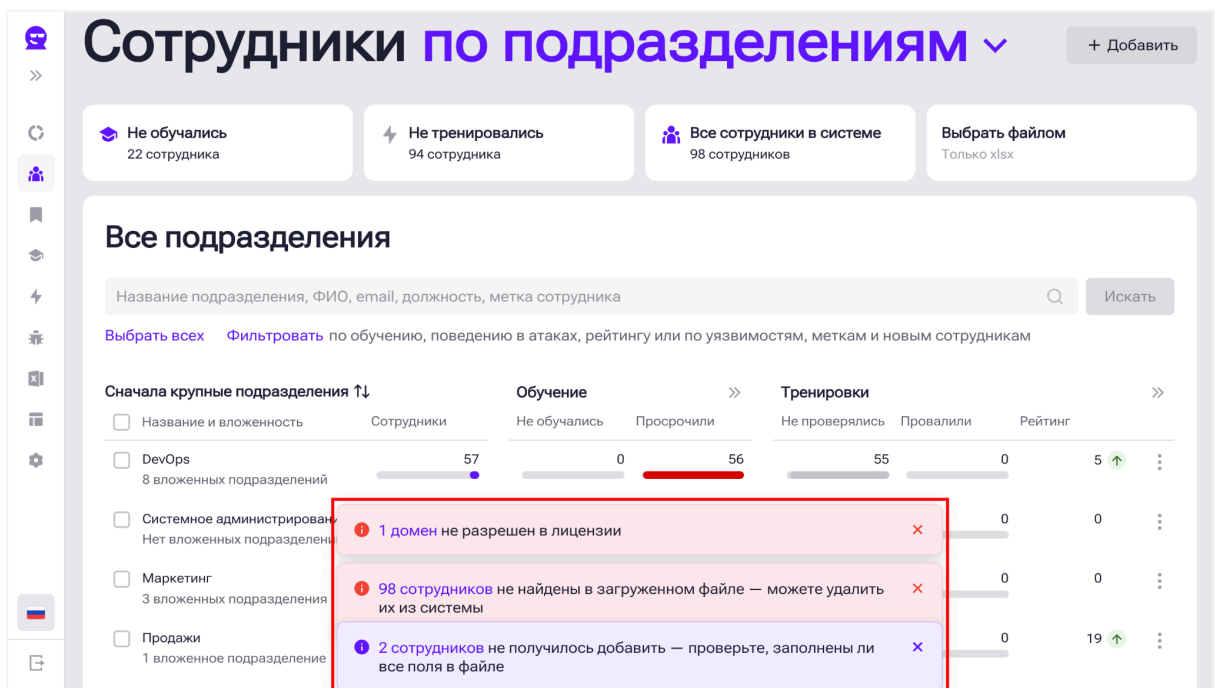
Выбрать файл

Скачать шаблон

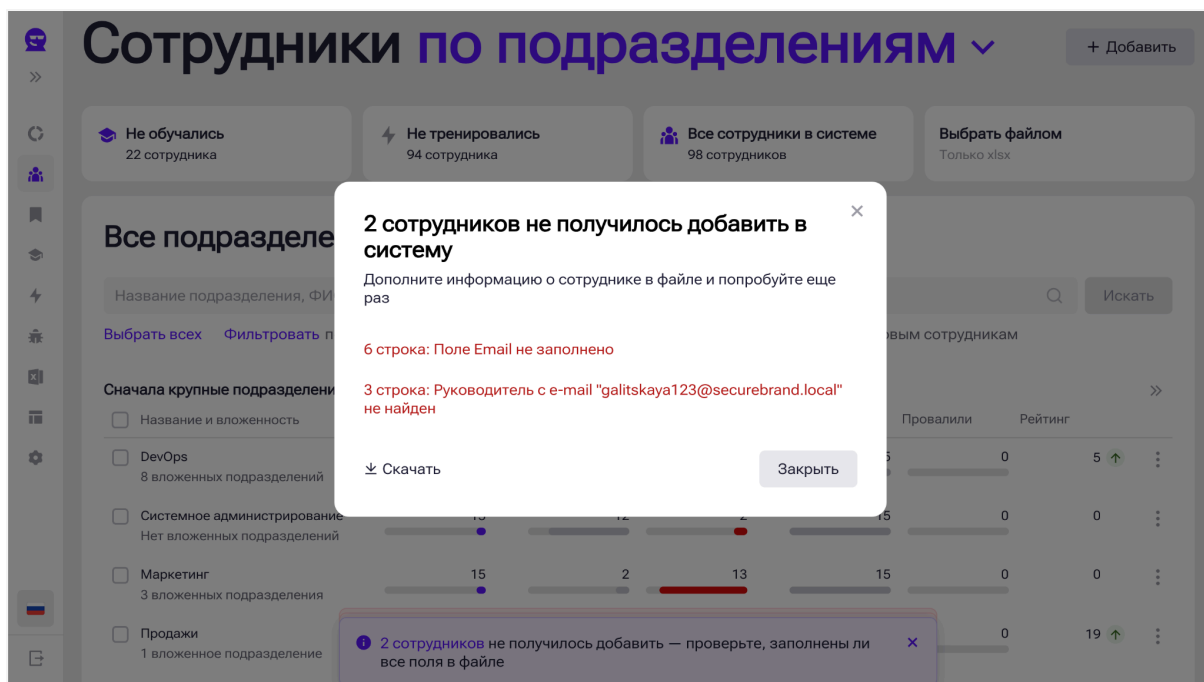
7. Дождитесь окончания импорта.



8. После обработки файла система покажет итоги импорта. Если кто-то из сотрудников в файле не загрузится в систему, отобразится уведомление с причиной и количеством таких сотрудников.



Чтобы посмотреть список сотрудников, которые не загрузились в систему, нажмите на число в уведомлении. При необходимости скачайте список.



Готово! Вы добавили сотрудников из файла Excel в систему.

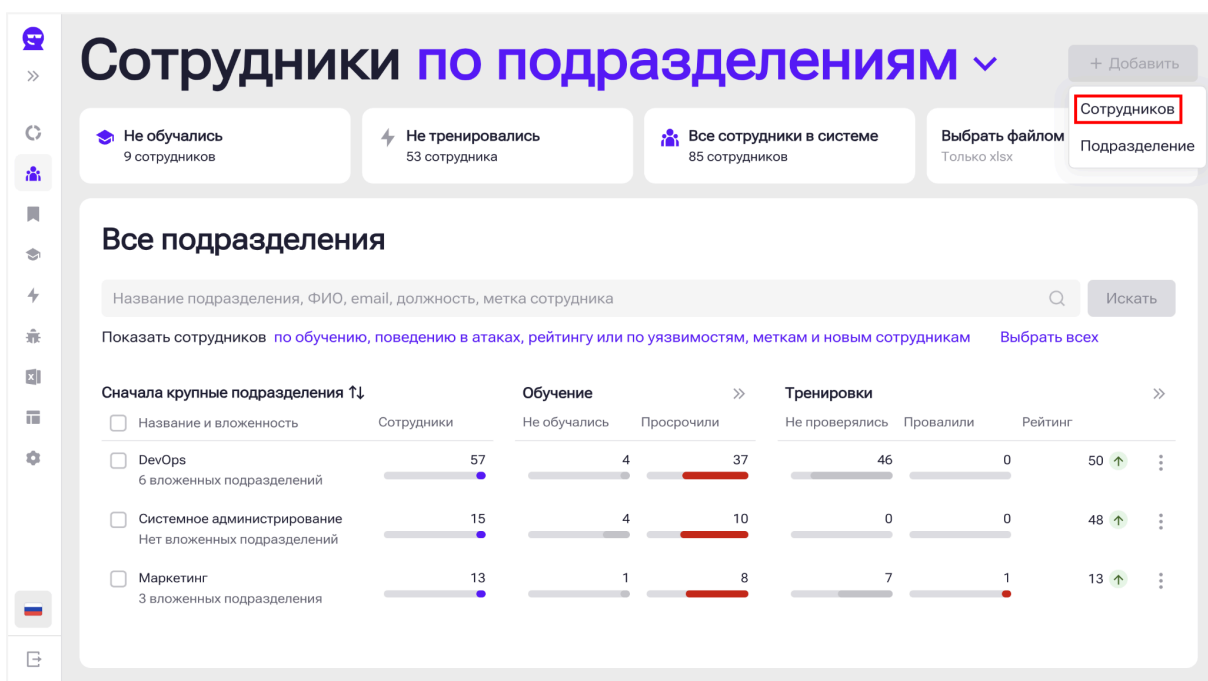
Импорт из LDAP (например, Microsoft Active Directory)

Этот способ позволяет добавить сотрудников и отделы из служб каталогов Active Directory, FreeIPA или OpenLDAP.

⚡ Рекомендуем импортировать не более 1000 сотрудников за один раз.

Для импорта сотрудников в систему:

1. Перейдите в **Меню** → **Сотрудники**.
2. В правом верхнем углу нажмите **Добавить** и выберите **Сотрудников**.



3. Перейдите во вкладку **Из LDAP-профиля**.

← К сотрудникам

Добавление сотрудников

* поля обязательные для заполнения

Вручную Из файла Из LDAP-профиля

Фамилия*

Имя*

Отчество

Электронная почта* @ Домен*

Подразделение*

Руководитель

Группа риска

Должность

Заккрыть Добавить

4. Чтобы создать новый LDAP-профиль, нажмите кнопку **Добавить новый**.

← К сотрудникам

Добавление сотрудников

* поля обязательные для заполнения

Вручную Из файла Из LDAP-профиля

Профиль LDAP*

Добавить новый

Заккрыть

5. Заполните поля:

Новый профиль LDAP

* поля обязательные для заполнения

Название*

Профиль 2

Не более 64 символов

ActiveDirectory

OpenLDAP

FreeIPA

Нет шифрования

SSL

TLS

Адрес сервера*

win.secure.local

DN*

DC=secure,DC=local

Фильтр

В формате: (company=*)(Title=*)(Department=*)(Mail=*)*

Имя пользователя*

ldaprofile

Пароль*

.....

60

секунд таймаута

☐ Синхронизировать по расписанию

Соответствие полей

Фамилия*

SN

Имя*

GIVENNAME

Отчество

Объединить ФИО в одно поле

Электронная почта*

MAIL

Подразделение*

DEPARTMENT

Должность

TITLE

Группа риска

Руководитель

MANAGER

Требования к проверке профиля при атаках

Учетные данные из имитированных атак проверяются в LDAP по выбранным форматам логина

☒ IdapLoginData@ldapDomainData

☒ Использовать email

☒ IdapDomainData\ldapLoginData

Заккрыть

Добавить

Новый профиль LDAP

- **Название*** — укажите имя профиля LDAP для удобного поиска в системе.
- **Служба каталогов** — выберите один из вариантов: Active Directory, OpenLDAP или FreeIPA.
- **Тип шифрования** — выберите один из вариантов: Нет шифрования, SSL или TLS.
- **Адрес сервера*** — введите адрес, по которому система подключится к LDAP.
- **DN*** — укажите путь к подразделению или группе в структуре LDAP.
- **Фильтр** — укажите одно или несколько условий, которые помогут исключить из выгрузки ненужных пользователей. Например, по отделу или должности.
- **Имя пользователя*** — введите логин от профиля LDAP.
- **Пароль*** — введите пароль от профиля LDAP.
- **Таймаут** — укажите время ожидания ответа от LDAP в секундах. По умолчанию указано 60 секунд.
- **Синхронизировать по расписанию** — включите параметр, чтобы данные обновлялись по заданному расписанию автоматически. Если параметр отключен, синхронизацию нужно будет запускать вручную.

Соответствие полей

- **Фамилия*** — укажите атрибут LDAP, из которого будут извлекаться фамилии сотрудников.
- **Имя*** — укажите атрибут LDAP, из которого будут извлекаться имена сотрудников.
- **Отчество** — укажите атрибут LDAP, из которого будут извлекаться отчества сотрудников.
- **Объединить ФИО в одно поле** — выберите этот параметр, если ФИО сотрудников хранятся в одном атрибуте LDAP. В этом случае фамилия, имя и отчество будут извлекаться из одного поля.
- **Электронная почта*** — укажите атрибут LDAP, из которого будут извлекаться электронные адреса сотрудников.
- **Подразделение*** — укажите LDAP-атрибуты, из которых будет построена структура подразделений сотрудников на платформе.
 Если выбрать `DISTINGUISHEDNAME`, структура будет сформирована на основе организационных единиц (OU), указанных в `DISTINGUISHEDNAME` сотрудника.
Если структура подразделений хранится в других LDAP-полях, выберите их вручную и задайте порядок, в котором они будут использоваться для построения структуры. Первое выбранное

поле будет основным подразделением, второе — его дочерним подразделением и так далее.

- **Группа риска** — укажите атрибут LDAP, из которого будут извлекаться информация о группах риска сотрудников.
- **Руководитель** — укажите атрибут LDAP, из которого будут извлекаться ФИО руководителей сотрудников.

Требования к проверке профиля при атаках

- **Требования к проверке профиля при атаках** — выберите один или несколько форматов логина LDAP. С помощью этой функции можно избежать ложных срабатываний системы безопасности и блокировки учетных записей при вводе данных на имитированной фишинговой странице.

6. Нажмите кнопку **Добавить**. Созданный LDAP-профиль будет автоматически выбран в форме добавления сотрудников.

7. В открывшейся форме заполните поля:

[← К сотрудникам](#)

Добавление сотрудников

* поля обязательные для заполнения

Вручную Из файла **Из LDAP-профиля**

Профиль LDAP*
Профиль 2

Добавить новый

1 Данные сотрудников из Профиль 2 будут соответствовать полям:

- Фамилия — SN
- Имя — GIVENNAME
- Электронная почта — MAIL
- Подразделение — DEPARTMENT
- Должность — TITLE
- Руководитель — MANAGER

[Изменить профиль или соответствие полей](#)

Только из групп

Уточните группы или будут добавлены все сотрудники профиля

Группы

Отдел розничной сети × Отдел инновационных технологий ×

Администраторы основного уровня ×

Добавить сотрудникам

Метки

Работают с ПДн × Стандартный доступ ×

Не более 30 знаков в метке

Группа риска

Средний уровень риска

Язык

Русский

Каких сотрудников

Всех

Некоторых

Только из групп

- **Группы** — укажите, какие группы сотрудников нужно загрузить из LDAP в систему.
⚡ Если оставить поле пустым, будут добавлены все сотрудники.

Добавить сотрудникам

- **Метки** — укажите текстовые метки, которые помогут сгруппировать сотрудников по каким-либо признакам. Например: «На удаленке», «Офис Москва», «Стажировка».
- **Язык** — выберите язык, на котором сотрудники будут получать уведомления, курсы и сертификаты об обучении.
- **Группа риска** — выберите группу риска, к которой будут относиться импортируемые сотрудники.

Каких сотрудников

Выберите, каких сотрудников нужно импортировать:

- **Всех** — выберите этот пункт, если нужно добавить всех сотрудников из выбранных групп. Если группы не указаны, будут добавлены все сотрудники из LDAP-профиля.
- **Некоторых** — выберите этот пункт, если нужно добавить только часть сотрудников из выбранных групп.

Каких сотрудников

Всех

Некоторых

Сотрудники по подразделениям ▾

Все подразделения

Название подразделения, ФИО, email, должность

Сбросить

Выбрать всех

Сначала крупные подразделения ↕

Название и вложенность

Сотрудники

☒ Разработка

нет вложенных подразделений

115

☒ Тестирование

2 вложенных подразделения

5

☒ Логистика

нет вложенных подразделений

1

☐ Трейдинг

нет вложенных подразделений

1

☐ АХО

нет вложенных подразделений

1

☐ Тестирования

нет вложенных подразделений

1

☐ Бухгалтерия

нет вложенных подразделений

1

☒ Кадры

нет вложенных подразделений

1

☒ Охрана труда

1 вложенное подразделение

1

10 на странице ▾

< Назад

1

2

Вперед >

Сохранить настройки импорта

Сбросить

Добавить 124 сотрудника

Заккрыть

8. Нажмите кнопку **Сохранить настройки импорта**.

Готово! После завершения синхронизации система покажет итоги импорта по всем сотрудникам.

← К сотрудникам

Не более 30 знаков в метке

Группа риска

Язык

Каких сотрудников

Всех Некоторых

100 сотрудников добавлены в систему

14 сотрудников обновлены

6 сотрудников остались без изменений

1 сотрудник не найден в профиле

3 сотрудника не синхронизированы

Сохранить настройки импорта

Добавить всех

Заккрыть

💡 При импорте каждый сотрудник загружается с уникальным номером (SID, GUID или UUID). При синхронизации система проверяет этот уникальный номер и электронную почту. Если таких нет, добавляет нового сотрудника. Если данные из LDAP-профиля не совпадают с данными в системе Start AWR, то данные в системе Start AWR обновляются в соответствии с данными в выбранной службе каталогов (AD, FreeIPA и прочие).

Поиск, фильтры и сортировка сотрудников

Отображение сотрудников

💡 Система запоминает выбранный способ отображения и использует его при последующем открытии раздела.

В верхней части интерфейса можно выбрать, как показывать список сотрудников:

- **по подразделениям** — список сотрудников группируется по отделам или подразделениям. Чтобы увидеть, кто находится в отделе, нажмите на его название.

»

↺

👤

📖

⚡

🔍

⚙️

🇷🇺

📄

Сотрудники по подразделениям ▾

🎓 Не обучались
13 сотрудников

⚡ Не тренировались
57 сотрудников

👤 Все сотрудники в системе
85 сотрудников

📄 Выбрать файлом
Только xlsx

Все подразделения

Название подразделения, ФИО, email, должность, метка сотрудника 🔍

Искать

Показать сотрудников по обучению, поведению в атаках, рейтингу или по уязвимостям, меткам и новым сотрудникам [Выбрать всех](#)

Сначала крупные подразделения ↑↓

Обучение

Тренировки

☐ Название и вложенность	Сотрудники	Не обучались	Просрочили	Не проверялись	Провалили	Рейтинг	
☐ DevOps 6 вложенных подразделений	57	4	36	46	0	50 ↑	⋮
☐ Системное администрирование Нет вложенных подразделений	15	3	11	0	0	48 ↑	⋮
☐ Маркетинг 3 вложенных подразделения	13	5	8	11	1	1 ↑	⋮

Чтобы увидеть вложенные подразделения (если они есть), кликните на необходимое подразделение.

»

↺

👤

📖

⚡

🔍

⚙️

🇷🇺

📄

Все подразделения

DevOps

Название подразделения, ФИО, email, должность, метка сотрудника 🔍

Искать

Показать сотрудников по обучению, поведению в атаках, рейтингу или по уязвимостям, меткам и новым сотрудникам [Выбрать всех](#)

Вложенные подразделения

Сначала крупные подразделения ↑↓

Обучение

Тренировки

☐ Название и вложенность	Сотрудники	Не обучались	Просрочили	Не проверялись	Провалили	Рейтинг	
☐ Frontend 3 вложенных подразделения	18	4	13	16	0	6 ↑	⋮
☐ Инфраструктура Нет вложенных подразделений	10	0	6	5	0	30 ↑	⋮
☐ Backend Нет вложенных подразделений	0	0	0	0	0	0	⋮

Корневое подразделение

Сначала от А до Я фамилии ↑↓

Обучение

Тренировки

☐ ФИО и email	Должность и подраздел...	Метки	Статус	Итоги последней атаки	Рейтинг
☐ Александр Степанов Петрович stepanov.alexandr@secur ebrand.local	Data Engineer DevOps		Просрочил	Не проверялся	0

- **общим списком** — все сотрудники отображаются одним списком без какой-либо группировки.

»

🔄

👤

📅

⚡

🔍

📄

⚙️

🇷🇺

📄

Сотрудники **общим списком** ▾

🎓 Не обучались
13 сотрудников

⚡ Не тренировались
57 сотрудников

👤 Все сотрудники в системе
85 сотрудников

📄 Выбрать файлом
Только xlsx

Все сотрудники

Название подразделения, ФИО, email, должность, метка сотрудника 🔍 Искать

Показать сотрудников по обучению, поведению в атаках, рейтингу или по уязвимостям, меткам и новым сотрудникам [Выбрать всех](#)

Сначала от А до Я фамилии ↑↓			Обучение	Тренировки	
☐ ФИО и email	Должность и подраздел...	Метки	Статус	Итоги последней атаки	Рейтинг
☐ Абдукаримов Байрам Ахмад оглы abdubayram@securebrand.local	Frontend-developer Frontend		Просрочил	Не проверялся	0
☐ Бабичев Антон Павлович babichevantont@securebrand.local	SMM-маркетолог Маркетинг		Просрочил	Выдержал	3 ↑
☐ Белова Анастасия Дмитриевна belova.anastasia@securebrand.local	Старший системный администратор Системное администрирование		Просрочил	Выдержал	3 ↑

- **по руководителям** — список сотрудников группируется по их руководителям.

💡 Общее количество сотрудников в столбце «Сотрудники» отображается с учетом руководителя. Например, если у руководителя в подчинении 9 сотрудников, в столбце будет указано 10 человек.

»

🔄

👤

📅

⚡

🔍

📄

⚙️

🇷🇺

📄

Сотрудники **по руководителям** ▾

🎓 Не обучались
9 сотрудников

⚡ Не тренировались
53 сотрудника

👤 Все сотрудники в системе
85 сотрудников

📄 Выбрать файлом
Только xlsx

Все руководители

Сначала больше подчиненных ↑↓

ФИО и количество подчиненных	Сотрудники	Тренировки		Рейтинг
		Не проверялся	Провалили	
Григорьев Владимир Игоревич 9 подчиненных	10	4	0	15 ↑
Дашина Вера Сергеевна 1 подчиненный	2	1	1	-2 ↓

Чтобы посмотреть список подчиненных, нажмите на ФИО руководителя.

При переключении режимов отображения сотрудников меняется состав таблицы и доступные параметры сортировки.

Быстрые фильтры

Ниже отображаются **быстрые фильтры**, с помощью которых система автоматически объединяет сотрудников по определенным признакам:

- **Не обучались** — сотрудники, которым не назначали ни одного курса.
- **Не тренировались** — сотрудники, которым не отправляли ни одной

атаки.

- **Пользуются уязвимыми приложениями** — сотрудники, у которых система обнаружила уязвимые приложения.
- **Все сотрудники в системе** — весь список сотрудников.

Нажмите на нужную плитку, чтобы выделить группу.

💡 Быстрый фильтр появляется только в случае, если в системе есть сотрудники, подходящие под один из вышеперечисленных признаков.

Расположение быстрых фильтров может меняться в зависимости от ширины экрана:

- при ширине от 1280 до 1600 пикселей, они будут находиться в верхней части экрана;

Сотрудники по подразделениям ▾ + Добавить

Не обучались 8 сотрудника | Не тренировались 54 сотрудника | Пользуются уязви... 2 сотрудника | Все сотрудники в с... 81 сотрудник | Выбрать файлом Только xlsx

Все подразделения

Название подразделения, ФИО, email, должность, метка сотрудника 🔍 Искать

Показать сотрудников по обучению, поведению в атаках, рейтингу или по уязвимостям, меткам и новым сотрудникам [Выбрать всех](#)

Сначала крупные подразделения ↑↓	Сотрудники	Обучение		Тренировки		Рейтинг
		Не обучались	Просрочили	Не проверялись	Провалили	
☐ DevOps 6 вложенных подразделений	57	4	37	47	0	44 ↑
☐ Системное администрирование Нет вложенных подразделений	15	3	11	0	0	48 ↑
☐ Маркетинг 3 вложенных подразделения	9	1	8	7	1	1 ↑

- при ширине от 1600 пикселей — в правой части.

Сотрудники по подразделениям ▾ + Добавить

Все подразделения

Название подразделения, ФИО, email, должность, метка сотрудника 🔍 Искать

Показать сотрудников по обучению, поведению в атаках, рейтингу или по уязвимостям, меткам и новым сотрудникам [Выбрать всех](#)

Сначала крупные подразделения ↑↓	Сотрудники	Обучение		Тренировки		Рейтинг
		Не обучались	Просрочили	Не проверялись	Провалили	
☐ DevOps 6 вложенных подразделений	57	4	37	46	0	50 ↑
☐ Системное администрирование Нет вложенных подразделений	15	4	10	0	0	48 ↑
☐ Маркетинг 3 вложенных подразделения	13	1	8	7	1	13 ↑

Рекомендуем начать работу с этих групп сотрудников:

- Не обучались 9 сотрудников
- Не тренировались 53 сотрудника
- Все сотрудники в системе 85 сотрудников

Найти и выбрать сотрудников быстро — через файл

Загрузите xlsx файл с данными сотрудников, которых хотите найти в системе

[Выбрать файл](#)

[Скачать шаблон](#)

Выделение сотрудников через импорт файла со списком

Если у вас есть готовый список сотрудников, можно загрузить его в формате `xlsx`, и система автоматически выделит в разделе «Сотрудники» всех, кто находится в файле.

Этот способ будет полезен, если нужно выполнить какие-либо действия с большим количеством сотрудников, например, назначить обучение или отправить атаку.

Чтобы выделить сотрудников с помощью импорта файла:

1. Перейдите в **Меню** → **Сотрудники**.
2. Нажмите на плитку **Выбрать файлом**.

The screenshot shows the 'Сотрудники' (Employees) management interface. At the top, there are three summary cards: 'Не обучались' (13 employees), 'Не тренировались' (57 employees), and 'Все сотрудники в системе' (85 employees). To the right of these cards is a button labeled 'Выбрать файлом' (Select by file) with the subtext 'Только xlsx'. This button is highlighted with a red rectangular box. Below the cards is a search bar and a table of employees. The table has columns for selection, personal data, training status, and rating.

Сначала от А до Я фамилии ↑↓	Обучение	Тренировки	Рейтинг
☐ ФИО и email	Статус	Итоги последней атаки	
☐ Абдукаримов Байрам Ахмад оглы abdubayram@securebrand.local	Просрочил	Не проверялся	0
☐ Бабичев Антон Павлович babichevanton@securebrand.local	Просрочил	Выдержал	3 ↑
☐ Белова Анастасия Дмитриевна belova.anastasia@securebrand.local	Просрочил	Выдержал	3 ↑

3. Нажмите кнопку **Выбрать файл** и загрузите файл со списком.

This screenshot shows the same interface as the previous one, but with a modal dialog box open. The dialog is titled 'Найти и выбрать сотрудников быстро — через файл' (Find and select employees quickly — through a file). It contains the instruction 'Загрузите xlsx файл с данными сотрудниками, которых хотите найти в системе' (Load an xlsx file with the data of the employees you want to find in the system). There are two buttons in the dialog: a purple 'Выбрать файл' (Select file) button and a blue 'Скачать шаблон' (Download template) link. The background interface is dimmed.

Если готового файла нет, можно воспользоваться шаблоном. Для этого нажмите **Скачать шаблон**. Заполните файл и загрузите его в систему.

4. Готово! Сотрудники из файла отмечены в списке.

Сотрудники

общим списком

+ Добавить

Все сотрудники

Название подразделения, ФИО, email, должность, метка сотрудника

Искать

Показать сотрудников по обучению, поведению в атаках, рейтингу или по уязвимостям, меткам и новым сотрудникам

Выбрать всех

Сначала от А до Я фамилии	Обучение	Тренировки	Рейтинг		
ФИО и email	Должность и подраздел...	Метки	Статус	Итоги последней атаки	Рейтинг
☐ Абдукаримов Байрам Ахмад оглы abdubayram@securebrand.local	Frontend-developer Frontend	Просрочил	Не проверялся	0	
☒ Бабичев Антон Павлович babichevantont@securebrand.local	SMM-маркетолог Маркетинг	Просрочил	Выдержал	3 ↑	
☐ Белова Анастасия Дмитриевна belova.anastasia@securebrand.local	Старший системный администратор Системное администрирование	Просрочил	Выдержал	3 ↑	
☐ Бородина Алёна Сергеевна borodina.alyona@securebrand.local	Frontend-developer Frontend	Просрочил	Не проверялся	0	

Вы выбрали: 13 сотрудников

Обучить

Тренировать

...

Поиск

Поиск доступен по названию подразделения, ФИО, email, должности и метке сотрудника.

Сотрудники

общим списком

+ Добавить

Не обучались
13 сотрудников

Не тренировались
57 сотрудников

Все сотрудники в системе
85 сотрудников

Выбрать файлом
Только xlsx

Все сотрудники

Название подразделения, ФИО, email, должность, метка сотрудника

Искать

Показать сотрудников по обучению, поведению в атаках, рейтингу или по уязвимостям, меткам и новым сотрудникам

Выбрать всех

Сначала от А до Я фамилии	Обучение	Тренировки	Рейтинг		
ФИО и email	Должность и подраздел...	Метки	Статус	Итоги последней атаки	Рейтинг
☐ Абдукаримов Байрам Ахмад оглы abdubayram@securebrand.local	Frontend-developer Frontend	Просрочил	Не проверялся	0	
☐ Бабичев Антон Павлович babichevantont@securebrand.local	SMM-маркетолог Маркетинг	Просрочил	Выдержал	3 ↑	
☐ Белова Анастасия Дмитриевна belova.anastasia@securebrand.local	Старший системный администратор Системное администрирование	Просрочил	Выдержал	3 ↑	

Фильтры

Отфильтровать сотрудников в списке можно несколькими способами:

- нажать на метку, статус обучения или итог последней атаки — выбранное значение автоматически добавится в поле поиска, и список сотрудников отфильтруется;

The screenshot shows the 'Сотрудники общим списком' (Employees in general list) interface. At the top, there are filter buttons: 'Не обучались' (84 employees), 'Не тренировались' (55 employees), 'Пользуются уязвимы...' (9 employees), 'Все сотрудники в сис...' (114 employees), and 'Выбрать файлом' (Only xlsx). Below these is a search bar with the text 'Название подразделения, ФИО, email, должность, метка сотрудника' and a search button. The main table lists employees with columns for 'Сначала от А до Я фамилии', 'Должность и подраздел...', 'Метки', 'Обучение', 'Тренировки', and 'Рейтинг'. The table contains four rows of employee data. Red boxes highlight specific filters: 'Удаленка' and 'Работа с персон...' under 'Метки', 'Просрочил' under 'Обучение', and 'Ввел данные в форму' and 'Уязвимое приложение' under 'Тренировки'.

- открыть панель фильтров и выбрать нужные условия фильтрации.

The screenshot shows the 'Все сотрудники' (All employees) interface with the filter panel open. The panel is titled 'Показать сотрудников' (Show employees) and contains several sections: 'По обучению' (By training), 'По тренировкам' (By training), 'По рейтингу' (By rating), 'По динамике рейтинга' (By rating dynamics), and 'Дополнительно' (Additional). Each section contains radio buttons for different filter conditions. The 'По обучению' section has four conditions: 'Не обучались', 'Просрочили курсы', 'Проходят курсы', and 'Прошли курсы'. The 'По тренировкам' section has four conditions: 'Не тренировались', 'Выдержали', 'Провалили последнюю атаку', and 'Открыли письмо'. The 'По рейтингу' section has two conditions: 'Положительный' and 'Отрицательный'. The 'По динамике рейтинга' section has two conditions: 'Растет' and 'Падает'. The 'Дополнительно' section has two conditions: 'Новые сотрудники' and 'Без меток'. A 'Заккрыть' (Close) button is at the bottom right of the panel. At the bottom of the interface, there is a pagination bar showing '10 на странице' and a set of navigation buttons: '< Назад', '1', '2', '3', '...', '11', 'Дальше >'.

💡 При выборе некоторых фильтров часть других может стать недоступна. Например, если выбрать «Новые сотрудники», фильтры по атакам будут неактивны.

Отфильтровать сотрудников по следующим параметрам:

По статусу обучения

- **Не обучались** — нет назначенных курсов.
- **Просрочили курсы** — не прошел хотя бы один назначенный курс вовремя.
- **Проходят курсы** — у сотрудника есть хотя бы один назначенный курс, срок прохождения которого еще не истек.
- **Прошли курсы** — сотрудник прошел все назначенные ему курсы.

По статусу тренировок

- **Не тренировались** — не получали имитированные атаки.
- **Выдержали** — не было опасных действий в последней атаке.

По самому опасному действию в последней атаке

- **Открыли письмо**
- **Перешли по ссылке**
- **Перешли по ссылке в QR**
- **Открыли файл по ссылке**
- **Открыли вложение**
- **Ввели данные в форму**
- **Сообщали об атаке**
- **С уязвимыми приложениями**

По рейтингу

- **Положительный**
- **Отрицательный**

По динамике рейтинга

- **Растет**
- **Падает**

Дополнительно

- **Новые сотрудники**
- **Без меток**

Чтобы снять выбор с примененных фильтров, нажмите на крестик или кнопку **Сбросить фильтр**.

Сортировка

Доступные варианты сортировок зависят от того, какой выбран способ отображения сотрудников:

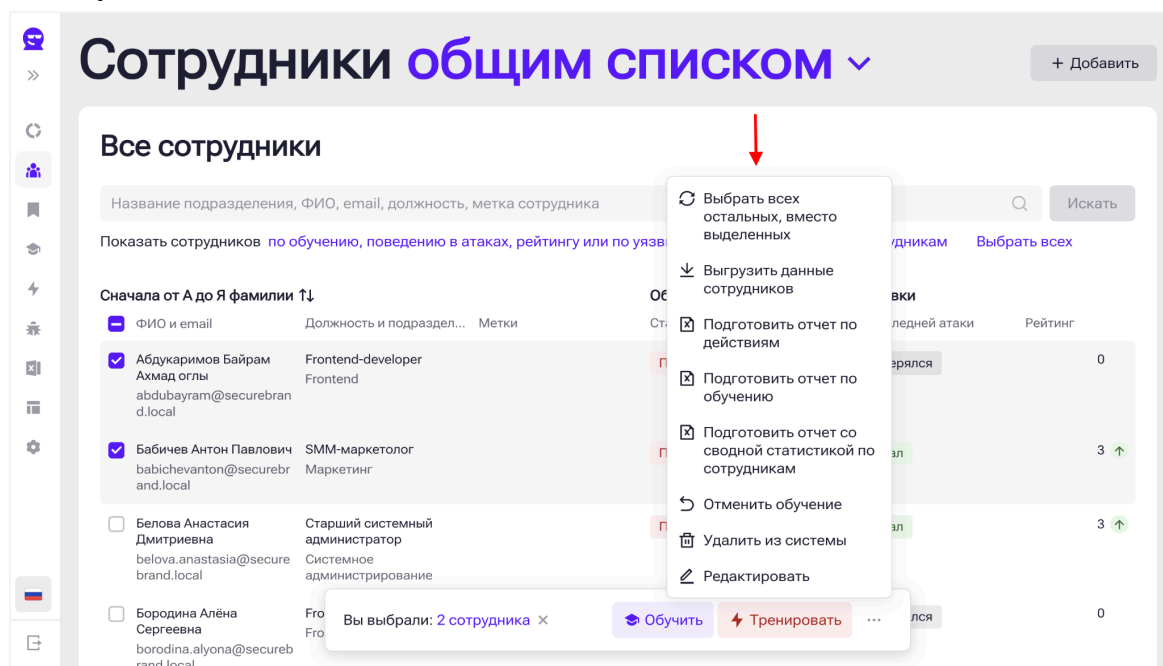
- **По подразделениям** — сортировка доступна по размеру подразделений, количеству необученных/не обученных вовремя/обученных/в процессе

обучения, не проверенных атакой/проваливших атаку/выдержавших атаку и по рейтингу.

- **Общим списком** — сортировка доступна по фамилии, электронному адресу, названию подразделения, должности и по рейтингу.
- **По руководителям** — сортировка доступна по количеству подчиненных, фамилии, непроверенных атакой/проваливших атаку и по рейтингу.

Действия с сотрудниками

После выбора сотрудников в нижней части интерфейса появится панель с доступными для них действиями.



Чтобы убрать сотрудника из выделенного списка, нажмите крестик рядом с его именем или снимите галочку в основном списке. Чтобы очистить весь выбор сразу, используйте кнопку **Сбросить выбор**.

Обучить

Это действие позволяет назначить обучающие курсы выбранным сотрудникам. Чтобы отправить сотрудников на обучение:

1. Отметьте сотрудников и нажмите кнопку **Обучить**.

Сотрудники по подразделениям ▾ + Добавить

Все подразделения > Маркетинг

SEO

Название подразделения, ФИО, email, должность, метка сотрудника 🔍 Искать

Показать сотрудников по обучению, поведению в атаках, рейтингу или по уязвимостям, меткам и новым сотрудникам

Сначала от А до Я фамилии ↑↓				Обучение	Тренировки	
☒ ФИО и email	Должность и подраздел...	Метки		Статус	Итоги последней атаки	Рейтинг
☒ Городищев Семён Александрович s.gorodishchev@securebrand.local	SEO-специалист SEO	Удаленка		Не обучался	Не проверялся	0
☒ Захаров Алексей Петрович a.zakharov@securebrand.local	SEO-специалист SEO	Удаленка		Не обучался	Не проверялся	0
☒ Сысоев Дмитрий Олегович d.sysoev@securebrand.local	SEO-специалист SEO	Удаленка		Не обучался	Не проверялся	0
☒ Филиппова Ирина Сергеевна	Специалист					0

Вы выбрали: 4 сотрудника × → **Обучить** ⚡ Тренировать ...

2. В открывшемся окне:

- выберите один или несколько курсов, которые нужно назначить сотрудникам.

← К сотрудникам **Отправить обучаться**

4 сотрудников [показать список](#) [изменить](#)

На 2 курса [показать только выбранные](#)

Поиск 🔍

☒ Название курса

- ☒ 1. Основы информационной безопасности 100.zip
- ☐ 11. Защита от дипфейков как распознать подделку и защитить свою цифровую личность 66.zip
- ☐ 2. Защита информации 80.zip
- ☒ 3. Защита персональных данных 80.zip
- ☐ 4. Работа с электронной подписью 80.zip
- ☐ 5. Безопасная работа с сайтами и веб-сервисами 80.zip
- ☐ 6. Безопасная работа с паролями 80.zip
- ☐ 7. Безопасная работа с электронной почтой 75.zip

Закрыть **Все верно, отправить**

- укажите, за какой срок сотрудники должны пройти обучение. Например, за одну неделю или в конкретный период.

← К сотрудникам

Название курса

☒ 1. Основы информационной безопасности 100.zip
 ☐ 11. Защита от дипфейков как распознать подделку и защитить свою цифровую личность 66.zip
 ☐ 2. Защита информации 80.zip
 ☒ 3. Защита персональных данных 80.zip
 ☐ 4. Работа с электронной подписью 80.zip
 ☐ 5. Безопасная работа с сайтами и веб-сервисами 80.zip
 ☐ 6. Безопасная работа с паролями 80.zip
 ☐ 7. Безопасная работа с электронной почтой 75.zip

В ближайшие

День

Неделя

Точные даты

1

Заккрыть

Все верно, отправить

- Чтобы назначить обучение, нажмите **Все верно, отправить**.

Готово! Сотрудники получают уведомление с информацией о назначенных курсах.

Все подразделения > Маркетинг

SEO

Название подразделения, ФИО, email, должность, метка сотрудника

Искать

Показать сотрудников по обучению, поведению в атаках, рейтингу или по уязвимостям, меткам и новым сотрудникам

Сначала от А до Я фамилии ↑↓			Обучение	Тренировки	
☒ ФИО и email	Должность и подраздел...	Метки	Статус	Итоги последней атаки	Рейтинг
☒ Городищев Семён Александрович s.gorodishchev@securebrand.local	SEO-специалист SEO	Удаленка	На обучении	Не проверялся	0
☒ Захаров Алексей Петрович a.zakharov@securebrand.local	SEO-специалист SEO	Удаленка	На обучении	Не проверялся	0
☒ Сысоев Дмитрий Олегович d.sysoev@securebrand.local	SEO-специалист SEO	Удаленка	На обучении	Не проверялся	0
☒ Филиппова Ирина Сергеевна i.fillipova@securebrand.local	Специалист по безопасности SEO	Удаленка	На обучении	Не проверялся	0

Отправка уведомлений о новом обучении. Отправлено 0 из 4

Вы выбрали: 4 сотрудника

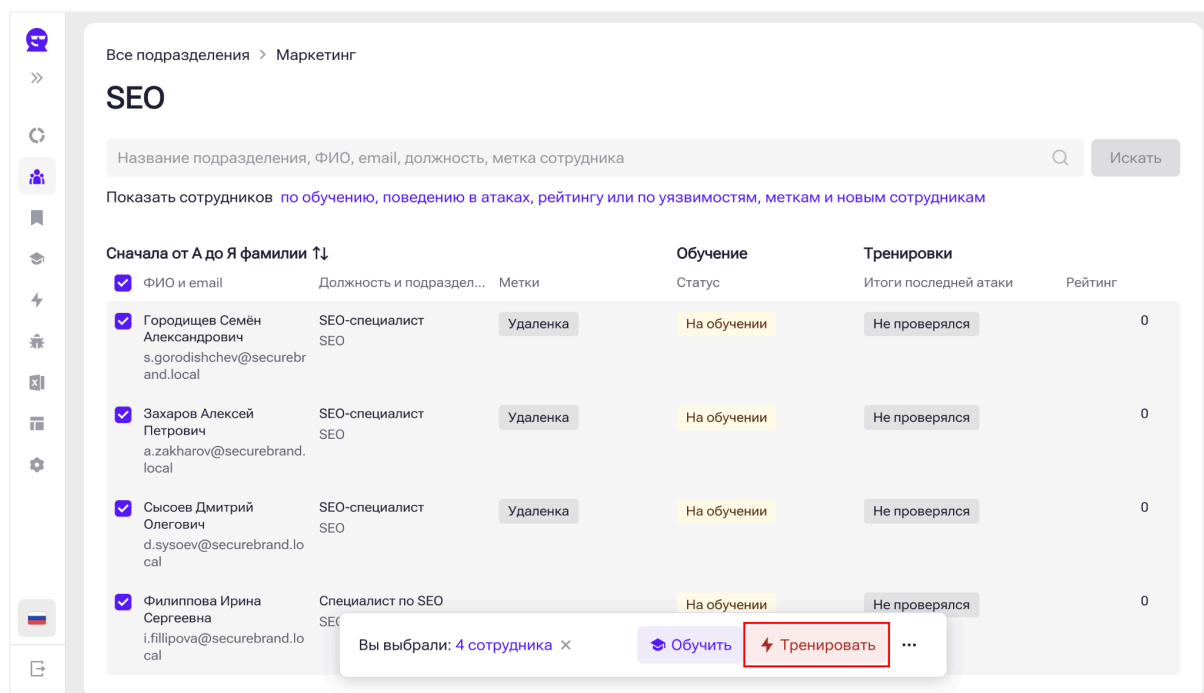
Назад

Продолжить

Тренировать

Это действие позволяет отправить имитированную атаку по электронной почте на выбранных сотрудников. Чтобы назначить атаку, отметьте сотрудников

и нажмите кнопку **Тренировать**. Подробная инструкция по работе с атакой находится в главе «[Атака по электронной почте](#)».



Выбрать всех остальных, вместо выделенных

Это действие позволяет снять выделение с текущих сотрудников и выделить всех остальных в списке.

Выгрузить данные сотрудников

Это действие позволяет выгрузить файл со списком сотрудников в формате xlsx.

Название файла с отчетом — *targets-list_ГГГГММДД*

⚡ Важное про работу отчетов:

Сформированный отчет можно скачать сразу из уведомления или позже в разделе «Отчеты». После скачивания отчет исчезает из списка и повторно скачать его нельзя, можно только сформировать заново.

Подготовить отчет по действиям

В отчете содержится информация о том, как сотрудник взаимодействовал с имитированными атаками:

- история запусков атак, где указаны названия атак, которым подвергался сотрудник и его ответные действия на них;
- история действий сотрудников;
- уязвимости сотрудника.

Название файла с отчетом — *employee-ГГГГ-ММ-ДД*

Подготовить отчет по обучению

Отчет содержит полную статистику по пройденным и назначенным курсам.

Название файла с отчетом — *education-ГГГГ-ММ-ДД*

Подготовить отчет со сводной статистикой по сотрудникам

Отчет помогает оценить, как сотрудники справляются с обучением и тренировками. Содержит общую статистику и сводки по обучению и атакам.

Название файла с отчетом — *summary-by-employees-ГГГГ-ММ-ДД*

Отменить обучение

Это действие позволяет отменить ранее назначенные курсы для выбранных сотрудников.

Удалить из системы

Это действие позволяет удалить из системы сотрудника и всю информацию о нем, включая историю обучения и тренировок.

Редактировать

Это действие позволяет изменить данные одного или нескольких сотрудников. Например, ФИО, должность, отдел и прочее.

Карточка сотрудника

Карточка сотрудника — это инструмент для быстрого доступа к ключевой информации о сотруднике. В ней содержится несколько блоков:

- **Общие сведения** — ФИО, контактные данные, должность, отдел и прочее.
- **Обучение** — текущие статусы по всем курсам и выданные сертификаты об обучении.
- **Тренировки** — детализация по всем имитированным атакам, которые назначали на сотрудника.
- **Сообщения об атаках** — обратная связь сотрудника об атаках.

Чтобы посмотреть информацию о сотруднике, нажмите на его ФИО в списке.

Общие сведения

На странице отображаются:

- **Статус сотрудника** — текущий статус сотрудника в системе.
- **Рейтинг по атакам** — текущий рейтинг и динамика сотрудника. Рейтинг растёт, если сотрудник сообщает об атаках и не совершает в них опасных действий. Опасные действия приводят к падению рейтинга.
- **ФИО** — фамилия, имя и отчество сотрудника.
- **Эл. почта** — корпоративная почта сотрудника.
- **Дата добавления** — дата добавления сотрудника в систему.
- **Язык** — на этом языке сотрудник получает уведомления, курсы и сертификаты об обучении.
- **Подразделение** — отдел, в котором работает сотрудник.
- **Должность** — кем работает сотрудник в компании.
- **Руководитель** — ФИО руководителя сотрудника.
- **Группа риска** — группа риска, в которой находится сотрудник.
- **Метки** — метки, которые присвоили сотруднику.

Вкладка «Обучение»

Здесь можно отслеживать прогресс по обучению в разрезе каждого курса и скачивать сертификаты по пройденным курсам.

Обучение 54Тренировки 4Сообщения об атаках 2

Всего 54 курса

По дате назначения: сначала новые

Не назначено50

Назначено2

Просрочено1

Пройдено2

Бенефициарные владельцы

Основы кибербезопасности

Управление рисками информационной безопасности

Этика и правовые аспекты информационной безопасности

Защита веб-приложений

Архитектура информационной безопасности и проектирование безопасных систем

Безопасность облачных технологий

Mobile Security

Криптография и безопасность данных

При необходимости отсортируйте все курсы по дате назначения.

В этом разделе отображаются курсы с разделением по статусам:

Статус обучения	Какие курсы отображаются в столбце	Что отображается в карточке курса
Не назначено	Курсы, которые еще не назначены сотруднику.	— Название курса.

Назначено	Назначенные на сотрудника курсы или те курсы, которые он начал проходить.	— Название курса. — Баллы, набранные в последней попытке. При наведении можно увидеть количество попыток. — Срок на прохождение курса.
Просрочено	Курсы, которые сотрудник не успел пройти вовремя.	— Название курса. — Баллы, набранные в последней попытке. При наведении можно увидеть количество попыток. — Срок на прохождение курса. — На сколько дней сотрудник просрочил курс.
Пройдено	Успешно пройденные курсы.	— Название курса. — Баллы, набранные в последней попытке. При наведении можно увидеть количество попыток и время прохождения. — Срок на прохождение курса. — На сколько дней сотрудник просрочил курс. Значение отобразится в случае, если пройденный курс был просрочен. — Ссылка на скачивание сертификата. — Срок действия сертификата.

Вкладка «Тренировки»

Здесь отображаются все отправленные и неотправленные атаки на сотрудника, а также действия, которые он в них совершил.

При необходимости можно отобразить только те атаки, о которых сообщил сотрудник. Также доступен фильтр по дате отправки атак — от новых к старым или наоборот.

Обучение 54
Тренировки 6
Сообщения об атаках 2

Всего 6 атак
Только атаки, о которых сообщено
По дате отправки: сначала новые

Не отправлено 2

Провалено 3

Выдержано 1

Вакцинация от клещей
Свой шаблон. Клещи
4

Запрос КП
Запрос КП
4

Положение о премировании
-3
14 июл 2025 г., 10:37
4

Обращение в Help Desk создано
-2 Сообщил об атаке
2 июл 2025 г., 15:03
4

ДТП рядом с офисом!
-1

Поиск людей для написания платных отзывов
1 Сообщил об атаке
1 мар. 2024 г., 12:00
4

Здесь находятся атаки с разделением по статусам:

Статус атак	Какие атаки отображаются в столбце	Что отображается в карточке атаки
Не отправлено	Атака, где сотрудник выбран целью, но которую еще не запустили.	— Название атаки. — Название шаблона. — Психологические векторы атаки. — Тип сообщения — Ссылка на финальную страницу — Тип файла во вложении. — Название фишинговой страницы. — Название финальной страницы.
Провалено	Атака, в которой сотрудник совершил опасное действие. Например, перешел по ссылке или открыл вложение.	— Название атаки. — На сколько изменился рейтинг после провала атаки. — Когда была отправлена атака. — Название шаблона атаки. — Психологические векторы атаки. — Тип коммуникации (например, от имени коллег или руководителей).
Выдержано	Атака, в которой сотрудник не совершил опасных действий. Например, не перешел по ссылке или не открыл вложение.	— Название атаки. — На сколько изменился рейтинг после провала атаки. — Когда была отправлена атака. — Название шаблона атаки. — Психологические векторы атаки. — Тип коммуникации (например, от имени коллег или руководителей).

Вкладка «Сообщения об атаках»

Здесь хранится история сообщений об имитированных и реальных атаках, про которые сообщил сотрудник.

При необходимости сообщения можно отсортировать по дате добавления — от новых к старым и наоборот.

Обучение 54

Тренировки 6

Сообщения об атаках 2

Всего 2 сообщения об атаках

По дате добавления: сначала новые

Имитированных 1

Реальных 1

Запрос КП

1 мар. 2024 г., в 12:00

Сегодня я получил письмо, которое, вероятно, содержит фишинговую ссылку и подозрительное вложение. Ссылка в письме: [Вставьте ссылку]. Я не открывал вложение и не переходил по ссылке, но считаю необходимым уведомить вас для проверки и предотвращения возможных угроз. Пожалуйста, дайте знать, если потребуется дополнительная информация.

1 мар. 2024 г., в 12:00

Раздел «Тренировки»

Предназначен для управления имитированными атаками, которые используются в рамках тренировки навыков безопасного поведения сотрудников.

Имитированные атаки — это тренировки, которые проводятся для обучения сотрудников распознаванию и противодействию реальным киберугрозам. Они похожи на настоящие атаки, но без вредоносного содержимого.

Цель таких атак — научить сотрудников быть бдительными и правильно реагировать на подозрительные сообщения или действия.

На платформе Start AWR доступны следующие виды имитированных атак:

- по электронной почте;
- через съемные устройства (HID и накопители);
- через беспроводные точки доступа (Wi-Fi).

Основные понятия

Письмо — отправная точка сценария, которая погружает сотрудника в контекст и побуждает совершить небезопасное действие. Например, перейти по ссылке или открыть вложение.



Письмо можно создать на основе шаблона или самому с нуля.

Небезопасное действие — действие сотрудника, которое нарушает правила информационной безопасности. Платформа Start AWR фиксирует следующие небезопасные действия:

- переход по фишинговой ссылке;
- ввод данных на фишинговой странице;
- открытие файла по ссылке;
- открытие вложение;
- переход по фишинговому QR-коду.

Вложение или **ссылка** — элемент атаки, с которым взаимодействует сотрудник. Может вести на фишинговую или финальную страницу. Позволяет проверить, совершит ли сотрудник небезопасное действие.

Фишинговая страница — страница, которая имитирует реальный сайт и используется для проверки действий сотрудника после перехода по ссылке или открытия вложения. Например, введет ли он логин и пароль.

Финальная страница — это страница, которую сотрудник видит после перехода по фишинговой ссылке. Она завершает сценарий и используется для обратной связи.

На странице сотруднику сообщается, что это была имитация атаки, объясняется, в чем заключалась ошибка, и даются рекомендации по безопасной работе с электронной почтой.

Атака по электронной почте

Как проходит атака

Во время атаки сотрудник получает письмо, которое выглядит как настоящее фишинговое. Если он откроет письмо, перейдет по ссылке или совершит другое небезопасное действие, эти события отобразятся на платформе Start AWR.

В дальнейшем эта информация поможет администратору оценить, насколько сотрудники умеют распознавать фишинговые письма.

Атака состоит из нескольких этапов:

1. Создание атаки

Администратор настраивает параметры атаки и выбирает сотрудников, которым она отправится.

2. Запуск атаки

Администратор выбирает конкретные дату и время или задает период, в течение которого нужно отправить атаку.

3. Получение письма

На электронную почту сотрудника приходит письмо. В зависимости от сценария атаки он может совершить одно или несколько небезопасных действий.

4. Фиксация небезопасных действий сотрудника

Платформа Start AWR фиксирует действия сотрудника — результаты отображаются на дашбордах и в отчетах.

5. Завершение атаки

После совершения небезопасного действия сотрудник видит финальную страницу. На странице ему сообщается, что это была имитация атаки, объясняется, в чем заключалась ошибка, и даются рекомендации по безопасной работе с электронной почтой.

Описание интерфейса

Вкладка «Через почту» представлена в виде таблицы со столбцами:

- **Название** — содержит название атаки. Под названием отображается количество сотрудников, выбранных в качестве целей атаки.

💡 Под активными атаками дополнительно отображается индикатор выполнения, показывающий количество сотрудников, которым отправлены письма.

- **Статус** — отображает текущее состояние атаки. Ниже приведено описание каждого статуса:

Название	Описание
Черновик	Атака создана, но еще не запущена. Можно изменить любые параметры атаки и список сотрудников.
Запустится 29 марта, 11:10	Запуск атаки запланирован на указанную дату и время. До запуска можно изменить параметры атаки и список сотрудников.
В работе	Атака запущена, происходит рассылка писем сотрудникам. Пока атака активна, изменить ее параметры или список сотрудников нельзя. Для этого нужно сначала приостановить атаку.
Приостановлена	Администратор временно приостановил отправку писем. Нельзя изменить параметры атаки, но можно изменить список сотрудников. В любой момент отправку писем можно продолжить.
Завершена	Атака может быть завершена по разным причинам: ● письма отправлены всем выбранным сотрудникам; ● администратор остановил ее вручную. После завершения атаки можно изменить ее параметры и список сотрудников, а затем при необходимости запустить снова.

- **Запуски** — показывает дату и время каждого запуска атаки.
- **Что делать с атакой** — содержит список доступных действий для выбранной атаки. Например, запустить, редактировать и прочие. Доступные действия зависят от статуса атаки.

Создание атаки

Чтобы создать атаку по электронной почте, выполните следующие шаги:

1. Нажмите кнопку **Новая атака**.

2. В открывшейся форме заполните параметры атаки:

← К тренировкам

Новая атака

* поля обязательные для заполнения

На 2 сотрудников

[показать список](#)

[изменить](#)

По шаблону

Поиск

Q

Новая атака

Актуализированы правила использования печатной инфраструктуры

Необходимо пройти диспансеризацию

Изменения в использовании банковских сервисов (Банк России)

Обновляем вендинговые аппараты

Запуск системы обратной связи «360 градусов»

Рассылка от маркетплейса

Оценка уровня стресса и эмоционального состояния

Заккрыть

Создать атаку

← К тренировкам

Письмо от внешних партнеров, подрядчиков

Письмо от имени коллег или руководителей

Личное сообщение, не связанное с работой

Психологические векторы

▼

Классификация атак

Тема письма*

Отправитель*

Адрес*

@

test.test

▼

☐ Такой же в ссылках

Arial

▼

15

▼

B

I

U

A

↶

↷

☰

▼

☰

☰

▼

☒

Добавить переменную:

Фамилия

Имя

Дата

...

или

🔗 Фишинговая ссылка

📄 Фишинговый QR

Текст письма

Заккрыть

Создать атаку

← К тренировкам

Приложить:

☒ Файл

☐ Ссылку на файл в тело письма

Все

320 файлов

.xlsx

76 файлов

.docx

126 файлов

.pptx

10 файлов

.rtf

6 файлов

▶

Файл в приложении

universal.pdf

▼

Название файла, которое увидит сотрудник

universal

Заархивировать файл:

☒ Нет

☐ ZIP

☐ ZIP с паролем

☐ ISO

Фишинговая страница

▼

Предпросмотр

Финальная перенадресация

ФНС Новое налоговое уведомление

▼

Предпросмотр

Сохранить как новый шаблон

Придумайте название атаке

Название*

Новая атака

Заккрыть

Создать атаку

- **Сотрудники** — выберите сотрудников, которым нужно отправить атаку.
- **Шаблон** — выберите, каким способом вам удобнее создать атаку:
 - **С нуля** — пропустите поле «Шаблон» и заполните все параметры атаки вручную.
 - **На основе шаблона** — выберите готовый шаблон, чтобы автоматически заполнить параметры атаки.
При необходимости измените их.
- **Источник атаки** — показывает, какой источник имитирует письмо в атаке. Эта информация может быть полезна при анализе результатов атаки.

При выборе шаблона, поле заполнится автоматически. Если создаете атаку с нуля, при необходимости выберите подходящий источник:

- **Письмо от внешних партнеров, подрядчиков** — имитирует письмо от внешнего отправителя, например, партнера или популярных сервисов.
- **Письмо от имени коллег или руководителей** — имитирует письмо от внутренних корпоративных источников, например, HR или IT-службы.
- **Личное сообщение, не связанное с работой** — имитирует личное сообщение, например, уведомление о посылке или сообщение из социальной сети.
- **Психологические векторы** — показывают, какую реакцию пытается вызвать письмо у сотрудников. Например, чувство страха, жадности и прочее.

При выборе шаблона, поле заполнится автоматически. Если создаете атаку с нуля, при необходимости выберите подходящие психологические векторы: страх, раздражение, невнимательность, любопытство, жадность, желание помочь, авторитет, срочность.

- **Тема письма** — укажите тему письма, которая отобразится в письме с атакой.
- **Отправитель** — укажите имя отправителя, которое отобразится в письме с атакой.
- **Адрес** — введите электронную почту отправителя, которая отобразится в письме с атакой.
- **Домен** — выберите домен, с которого будет отправлено письмо с атакой.
💡 Перед отправкой атаки убедитесь, что домен корректно настроен. Подробнее в инструкции «Домены».
- **Такой же в ссылках** — включите параметр, если необходимо использовать выбранный домен в имитированных фишинговых

ссылках внутри письма.

3. Оформите письмо с помощью встроенного визуального редактора. В нем вы можете:

- добавлять текст и настраивать форматирование (шрифт, размер, цвет и другое);
- вставлять изображения, ссылки и QR-коды;
- использовать переменные;
- работать с HTML-кодом письма.

4. При необходимости добавьте к письму **Вложение** или **Ссылку на скачивание файла**. Для этого настройте параметры:

- **Приложить** — выберите элемент, который нужно добавить в атаку:
 - **Файл** — позволит добавить вложение в виде файла к письму.
 - **Ссылку на файл в тело письма** — позволит добавить в текст письма ссылку на скачивание вложения. Ссылка вставляется в письмо в виде переменной.

После выбора элемента атаки появится фильтр по вложениям. Выберите в нем нужный формат (PDF, DOC и другие), чтобы отфильтровать список.

Далее заполните следующие поля:

- **Файл в приложении** — выберите вложение, которое нужно добавить в письмо.
- **Название файла, которое увидит сотрудник** — укажите отображаемое имя файла:
 - Если выбран вариант **Файл** — указанное название отобразится в имени файла.
 - Если выбран вариант **Ссылка на файл в тело письма** — указанное название отобразится при наведении курсора на ссылку.
- **Заархивировать файл** — укажите, нужно ли упаковать вложение в архив и какой формат использовать: **ZIP**, **ZIP с паролем** или **ISO**. Если архив не нужен, выберите **Нет**.
 При выборе варианта «ZIP с паролем», для передачи пароля в письме используйте переменную {password} — она сгенерирует пароль в тексте при рассылке атаки.

5. При необходимости выберите **Фишинговую страницу** в соответствующем поле.

 Использование фишинговой страницы не обязательно — при необходимости сотрудника можно сразу направить на финальную

страницу.

Чтобы посмотреть, как выглядит фишинговая страница, нажмите **Предпросмотр**.

После выбора фишинговой страницы становится доступен параметр **Проверить в LDAP**. Он позволяет определить, использует ли сотрудник реальные корпоративные учетные данные при вводе на странице.

⚡ Не все фишинговые страницы поддерживают LDAP-проверку — обычно такие страницы помечены соответствующим признаком в названии.

💡 Проверка доступна только для сотрудников, добавленных в систему из LDAP-профиля.

6. В поле **Финальная переадресация** выберите **Финальную страницу**, на которую будет перенаправлен сотрудник после выполнения небезопасного действия.

Чтобы посмотреть, как выглядит финальная страница, нажмите **Предпросмотр**.

7. При необходимости вы можете сохранить атаку как шаблон, чтобы использовать его повторно. Для этого нажмите кнопку **Сохранить как новый шаблон**.

После сохранения он появится в общем списке шаблонов и будет доступен для выбора.

8. Введите **Название** атаки.

9. После заполнения всех полей нажмите кнопку **Сохранить**.

Готово! Вы создали имитированную атаку. Запустите ее сразу или запланируйте на нужную дату и время.

Запуск атаки

⚡ Изменять параметры атаки можно только до первого запуска. При этом список сотрудников можно редактировать в любое время.

Чтобы запустить атаку:

1. Нажмите кнопку **Запустить** в столбце **Что делать с атакой**.
2. Подтвердите действие.

Готово! Вы запустили атаку. Ее статус изменится на «В работе».

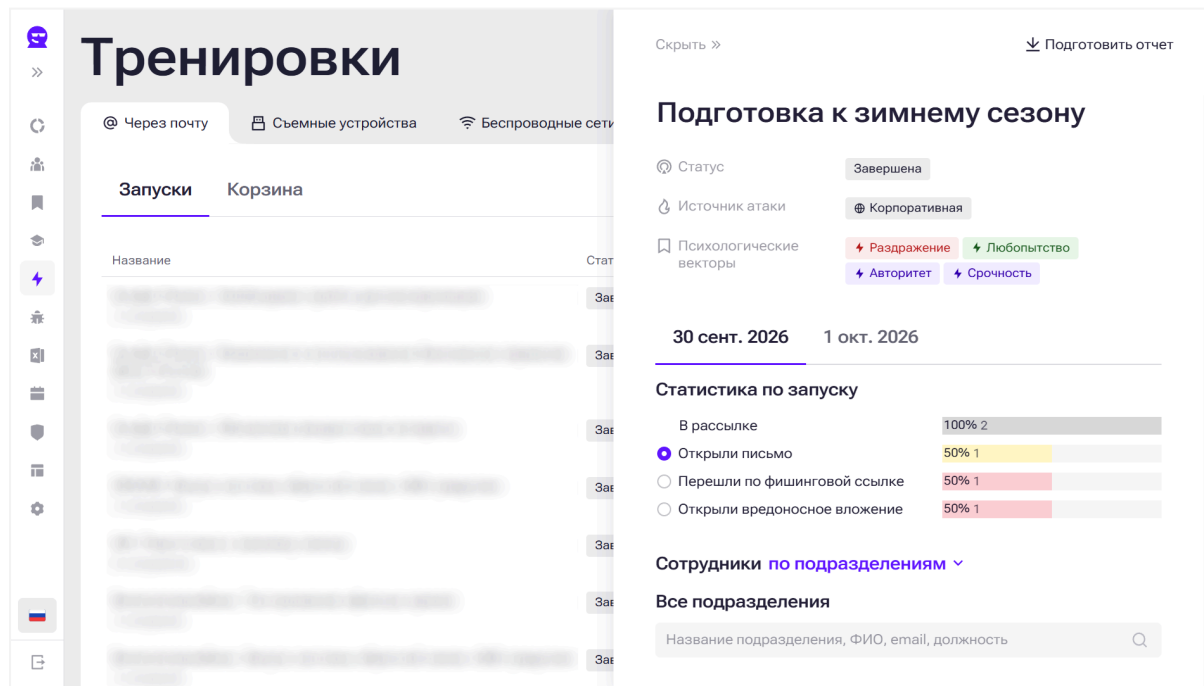
Отслеживать процесс рассылки писем можно с помощью индикатора

под названием атаки. Он показывает, скольким сотрудникам уже отправлены письма.

Статистика по запускам

Чтобы открыть статистику по атаке, нажмите на нужную атаку в списке.

В верхней части страницы отображается общая информация об атаке: статус, источник атаки и психологические векторы.



Ниже приведена статистика по каждому запуску атаки. В ней показано, сколько сотрудников совершили каждое небезопасное действие.

💡 В показателе «В рассылке» отображается количество сотрудников, которым уже отправлено письмо.

Чтобы посмотреть, какие именно сотрудники совершили действие, нажмите переключатель рядом с действием.

💡 Если сотрудник совершил несколько небезопасных действий, он отобразится в статистике по всем действиям, которые он совершил.

Например, если сотрудник открыл письмо, перешел по ссылке и открыл вложение, он будет учтен в статистике по каждому из этих действий.

Приостановка атаки (пауза)

Чтобы поставить рассылку на паузу:

1. Нажмите кнопку **Приостановить** в столбце **Что делать с атакой**.
2. Подтвердите действие.

Готово! Рассылка писем приостановлена. Статус атаки изменится на «Приостановлена».

Редактирование атаки

💡 Если атака ни разу не запускалась, можно изменить любые параметры. После первого запуска доступно только редактирование списка сотрудников.

Чтобы отредактировать атаку:

1. Напротив нужной атаки нажмите три точки (⋮) и выберите **Редактировать**.
2. Внесите необходимые изменения в параметры атаки.
3. Нажмите кнопку **Сохранить**.

Готово! Параметры атаки изменены.

Планирование запуска атаки

💡 Планирование запуска доступно для атак в статусе «Черновик» и «Завершена».

Чтобы запланировать запуск атаки:

1. Напротив нужной атаки нажмите три точки (⋮) и выберите **Запланировать**.
2. В открывшемся окне выберите **Часовой пояс**, в котором нужно запустить атаку, и способ рассылки:
 - **Одновременно** — письма будут отправлены всем выбранным сотрудникам в указанную дату и время.
 - **Постепенно** — письма будут отправляться выбранным сотрудникам в течение указанного периода.
3. Нажмите кнопку **Запланировать**.

Готово! Атака запланирована. Ее статус изменится на «Запланирована». При необходимости вы сможете изменить дату и время запуска.

Завершение атаки

Чтобы полностью остановить атаку, нажмите три точки (⋮) возле нее и выберите **Остановить**.

Готово! После остановки:

- если атака еще ни разу не запускалась, статус изменится на «Черновик»;
- если атака уже запускалась, статус изменится на «Завершена».

Удаление атаки

💡 Удаление доступно для атак со статусами «Черновик» и «Завершена».

Чтобы удалить атаку:

1. Нажмите три точки (⋮) возле атаки и выберите **Удалить**.
2. В открывшемся окне подтвердите действие, нажав **Удалить**. Атака переместится в корзину, откуда ее при необходимости можно восстановить.

Если нужно удалить атаку навсегда вместе со статистикой, нажмите **Удалить атаку навсегда вместе со статистикой**. После этого восстановить атаку будет нельзя.

Корзина

В корзине хранятся удаленные атаки вместе со статистикой по их запускам.

Атаки можно восстановить или удалить навсегда. Действия применяются ко всем атакам в корзине одновременно.

Атака через съемное устройство

💡 Инструкция находится в разработке. Подробное описание будет добавлено позже.

Атака через беспроводную сеть (Wi-Fi)

💡 Инструкция находится в разработке. Подробное описание будет добавлено позже.

Раздел «Процессы»

Инструмент «Процессы» помогает автоматизировать рутинные задачи администратора: назначение сотрудников на обучение, отправку имитированных атак, выгрузку отчетов и прочие. Также с помощью него можно создавать нестандартные процессы под задачи компании.

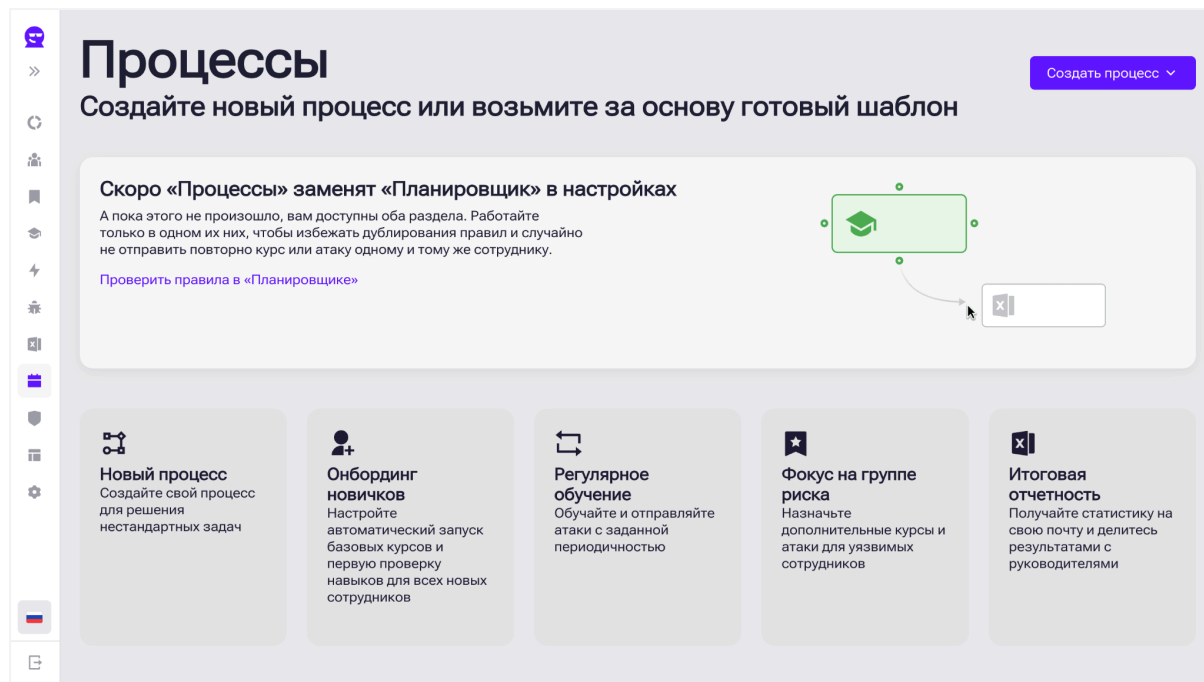
Процесс — это набор шагов, по которым система автоматически выполняет действия в ответ на события и соблюдение условий.

Каждый процесс состоит из трех элементов:

- **Событие** — определяет, когда запускается процесс.
- **Условие** — проверяет, нужно ли выполнять дальнейшие шаги.
- **Действие** — определяет, что система должна сделать.

Описание интерфейса

В разделе отображаются все созданные процессы, а также доступные инструменты для их создания, запуска и управления.

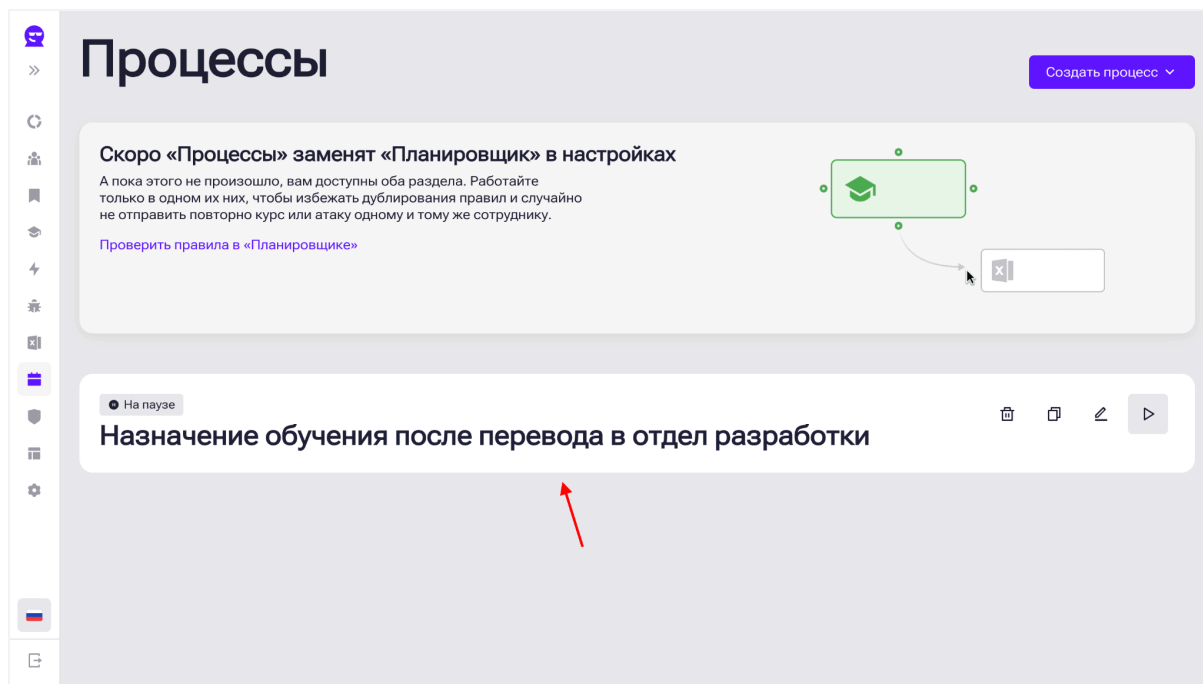


В верхней части страницы расположена кнопка **Создать процесс**, которая позволяет создать новый процесс с нуля или использовать готовый шаблон. При нажатии доступны следующие варианты:

- **Новый процесс** — создание процесса с нуля.
- **Онбординг новичков** — шаблон для назначения базовых курсов и первой проверки навыков у новых сотрудников.
- **Регулярное обучение** — шаблон для назначения обучения и отправки атак с заданной периодичностью.
- **Фокус на группе риска** — шаблон для назначения дополнительных курсов и атак для уязвимых сотрудников.
- **Итоговая отчетность** — шаблон для отправки отчетов на электронную почту.

💡 До создания первого процесса шаблоны отображаются на странице в виде отдельных плиток. После создания первого процесса они будут доступны только через кнопку **Создать процесс**.

После создания процесс отображается в виде отдельной карточки с названием и доступными действиями.



Для каждого процесса отображается текущий статус:

- **На паузе** — обозначает, что выполнение процесса остановлено.
💡 После создания процесс автоматически ставится на паузу.
При необходимости вы можете запустить его вручную.
- **Работает** — обозначает, что процесс запущен и выполняется системой.

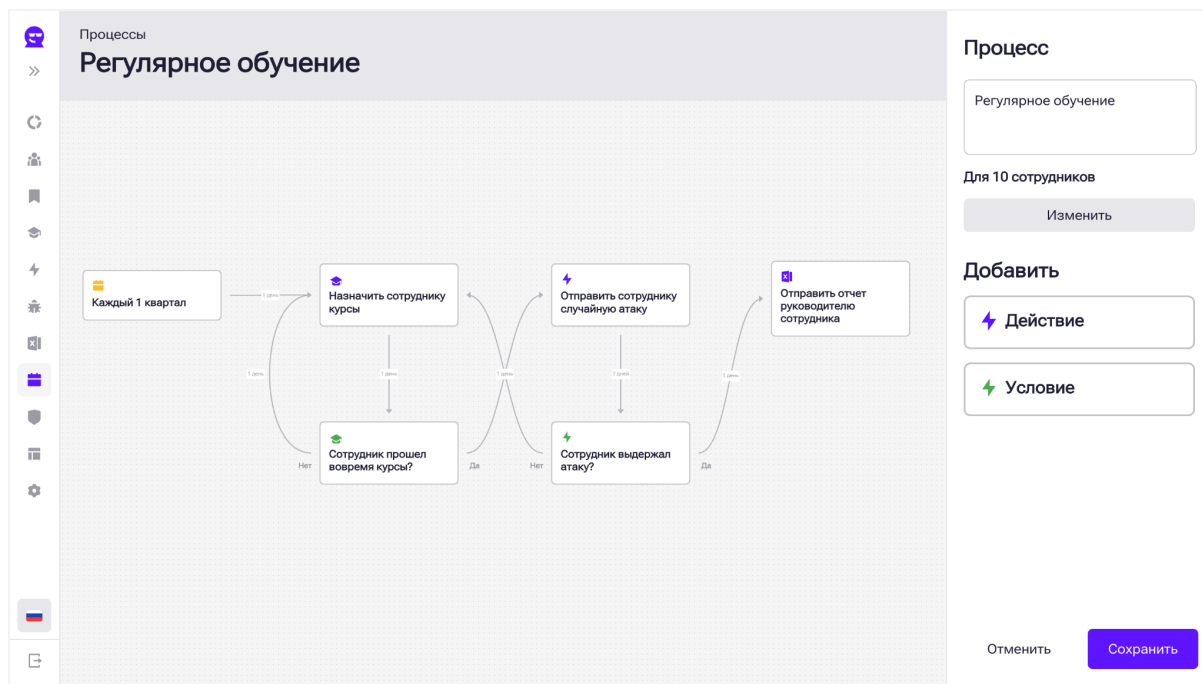
Также для каждого процесса доступны следующие действия:

- **Запустить / Поставить на паузу** — запускает выполнение процесса или временно останавливает его.
- **Редактировать** — позволяет изменить настройки процесса.
⚡ Редактировать настройки можно только до первого запуска процесса.
- **Копировать** — создает дубликат процесса со всеми его настройками (событиями, условиями и действиями). Перед запуском процесса копию можно изменить.
- **Удалить** — удаляет процесс из системы.

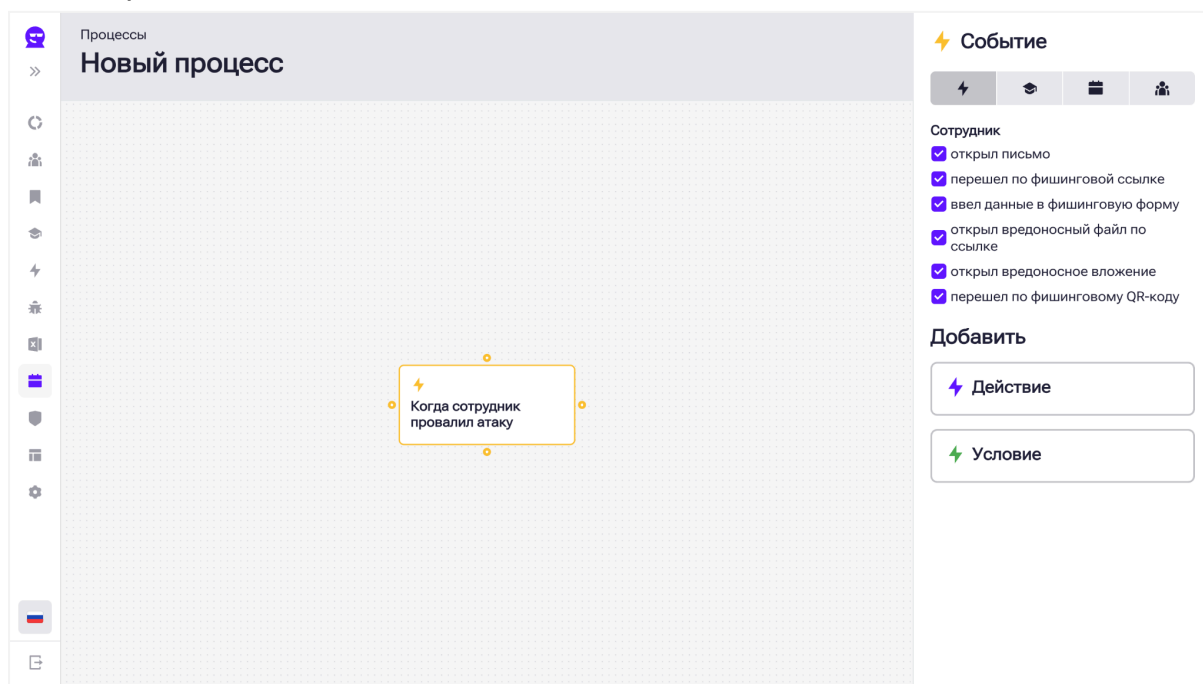
Описание интерфейса конструктора процессов

Конструктор состоит из двух частей: рабочего поля и панели с настройками.

Рабочее поле занимает основную часть экрана. Здесь размещаются элементы процесса и соединяются между собой линиями, которые задают порядок выполнения.



Справа расположена панель, на которой находятся доступные настройки для выбранного элемента.



Для перемещения по схеме и изменения масштаба используйте мышь, тачпад или горячие клавиши.

Событие

Событие определяет, когда запускается процесс. После добавления блока «Событие» справа открывается панель настройки, в которой необходимо выбрать тип события и заполнить параметры.

Типы событий

Во время атаки

Процесс запускается при действиях сотрудника в рамках имитированной атаки.

Доступные триггеры:

- открыл письмо;
- перешел по фишинговой ссылке;
- ввел данные в фишинговую форму;
- открыл вредоносный файл по ссылке;
- открыл вредоносное вложение;
- перешел по фишинговому QR-коду.

Во время обучения

Процесс запускается в зависимости от того, прошел сотрудник курс вовремя или нет.

Доступные триггеры:

- сотрудник прошел курс вовремя;
- сотрудник не прошел курс вовремя.

После выбора триггера укажите один или несколько курсов, при прохождении которых будет запускаться процесс.

В заданное время

Процесс запускается по указанному времени или расписанию.

Доступные варианты запуска:

- один раз;
- по расписанию — каждые неделю, месяц или квартал.

При кадровых изменениях

Процесс запускается при изменениях данных у сотрудника.

Доступные триггеры:

- добавлен в систему;
- переведен на новую должность — выберите одну или несколько должностей, при переводе на которые будет запускаться процесс;
- переведен в новый отдел — выберите один или несколько отделов, при переводе в которые будет запускаться процесс;
- добавлен в группу риска — выберите одну или несколько групп, при добавлении в которые будет запускаться процесс.

Действие

Определяет, что система выполнит после срабатывания события или выполнения условий (при наличии).

Типы действий

Отправить атаку

Позволяет отправить сотруднику имитированную атаку по электронной почте.

Доступные варианты:

- Случайная атака из базы — система случайным образом выберет для отправки одну атаку. При необходимости можно ограничить список шаблонов атак по следующим признакам:
 - с фишинговой ссылкой;
 - с вложением;
 - с фишинговой страницей;
 - со ссылкой для скачивания вложения;
 - с QR-кодом;
 - с вложением в zip-архиве;
 - новые для сотрудника.
- Конкретная атака — система создаст атаку на основе выбранного администратором шаблона.

Назначить курсы

Позволяет назначить сотруднику один или несколько курсов.

Выберите курсы и укажите срок прохождения обучения:

- в ближайшие дни;
- в ближайшие недели;
- в точную дату или период.

Отправить отчет

Позволяет отправить отчет выбранным получателям.

Укажите, кому нужно отправить отчет:

- руководителю сотрудника;
- администратору — выберите одного или несколько;
- на почту — укажите адрес электронной почты, на который нужно отправить отчет.

Выберите один или несколько видов отчетов:

Отчет по сотруднику (формируется по сотрудникам, участвующим в процессе)

- по обучению (по выборке сотрудников);
- по действиям;
- по отделу сотрудника;
- сводный.

Общий отчет (формируется по всем сотрудникам компании)

- основной;
- по рискам;
- сводный по компании.

Добавить в группу риска

Позволяет при срабатывании события или выполнения условия добавить сотрудника в выбранную группу риска.

Условие

Условие используется для ветвления процесса. После срабатывания события условие определяет, по какому сценарию процесс продолжит выполнение.

Доступные условия:

- **Сотрудник выдержал последнюю атаку** — проверяет, успешно ли сотрудник выдержал последнюю атаку, отправленную в рамках процесса. От условия можно настроить два варианта перехода:
 - Да — если сотрудник успешно выдержал атаку;
 - Нет — если сотрудник провалил атаку.
- **Сотрудник прошел вовремя курсы** — проверяет, завершил ли сотрудник обучение в установленный срок. Для настройки условия выберите один или несколько курсов, прохождение которых будет проверяться.

 Если обучение было назначено в рамках этого процесса, соответствующие курсы будут автоматически выбраны в условии.

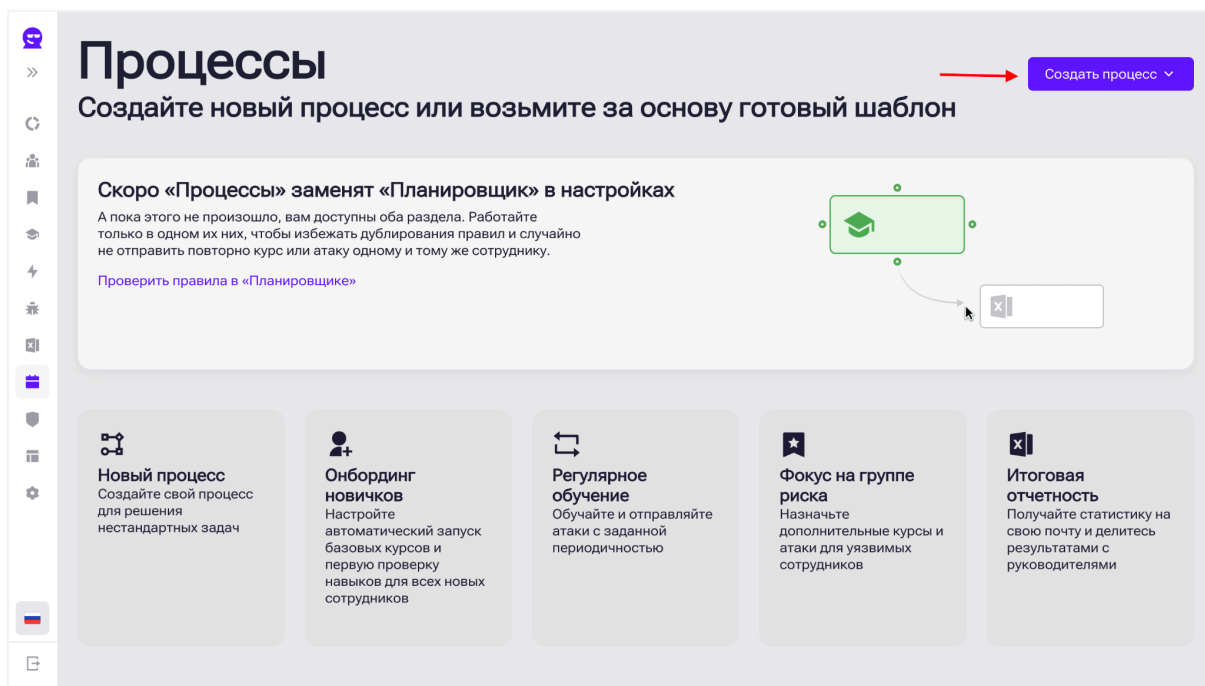
От условия можно настроить два варианта перехода:

- Да — сотрудник прошел курсы вовремя;
- Нет — сотрудник не прошел курсы вовремя.

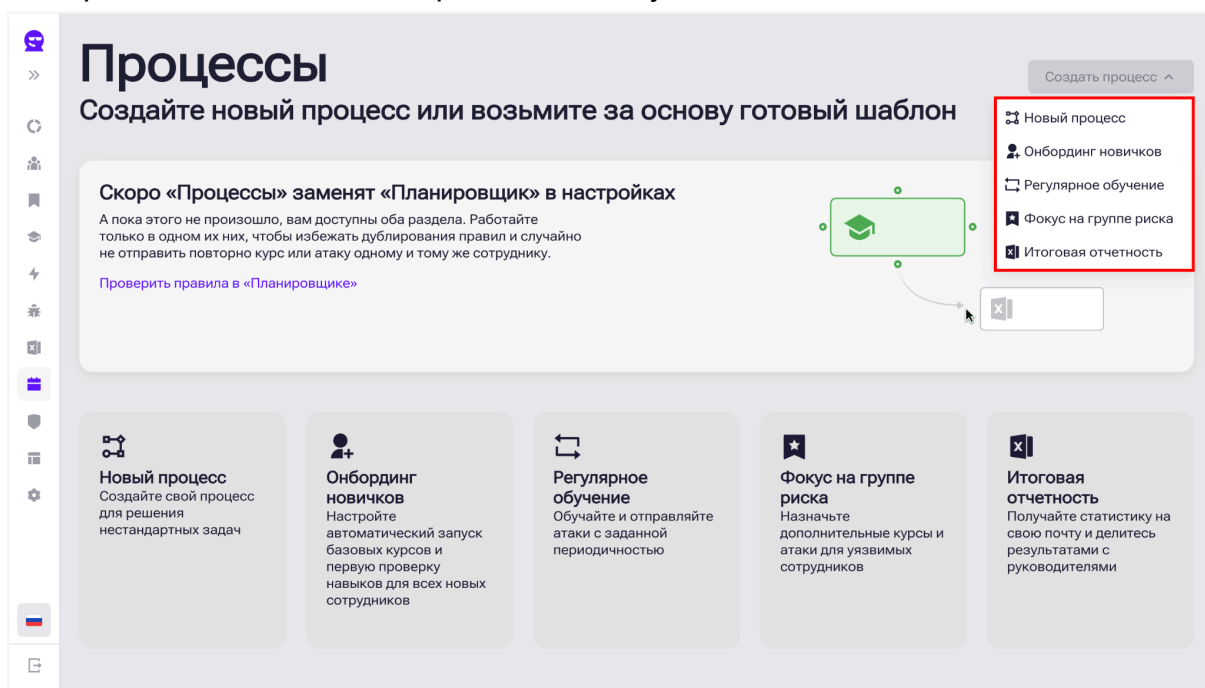
Создание процесса

Чтобы создать процесс:

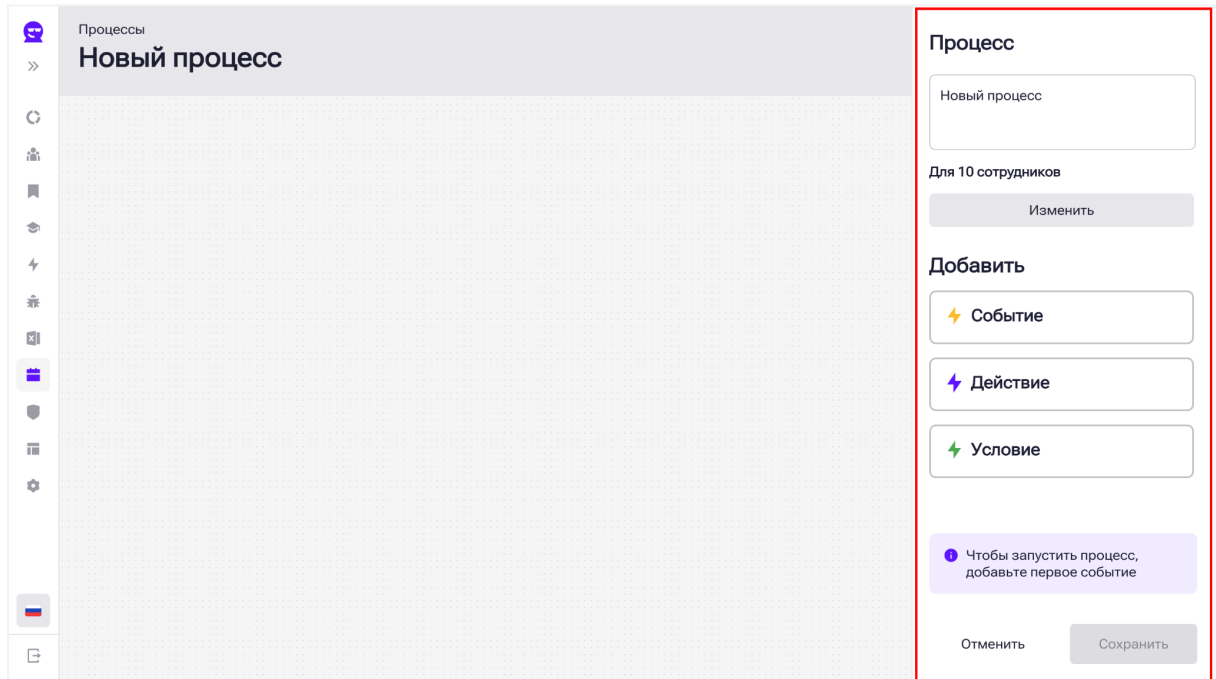
1. Нажмите кнопку **Создать процесс**.



2. Выберите способ создания процесса — с нуля или на основе шаблона.



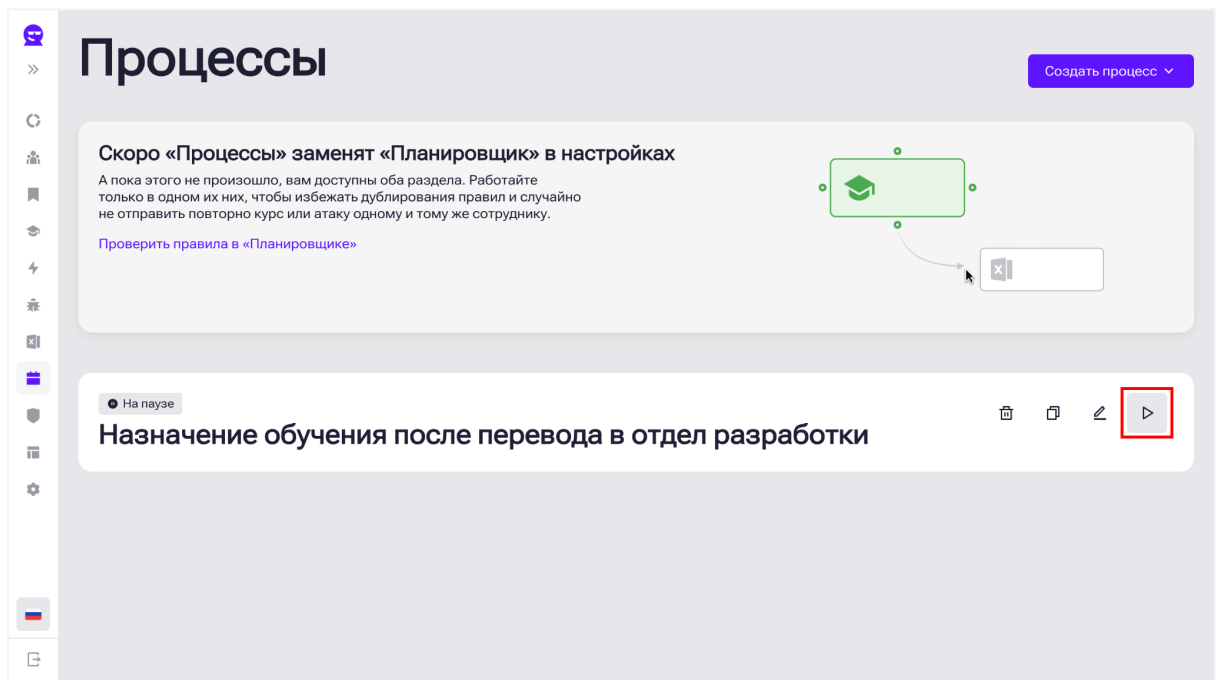
3. В открывшейся панели настроек выполните следующие действия:



- укажите **Название** процесса;
- выберите сотрудников, которые будут участвовать в процессе;
- настройте логику процесса — добавьте событие, действие и при необходимости условие.

4. После завершения настройки нажмите кнопку **Сохранить**.

💡 Новый процесс будет создан в статусе «На паузе». Чтобы начать выполнение, нажмите **Запустить**.



Раздел «Защищенность сотрудников»

Раздел «Защищенность сотрудников» помогает оценивать уровень защищенности компании от угроз, связанных с человеческим фактором, а также отслеживать ключевые показатели безопасности.

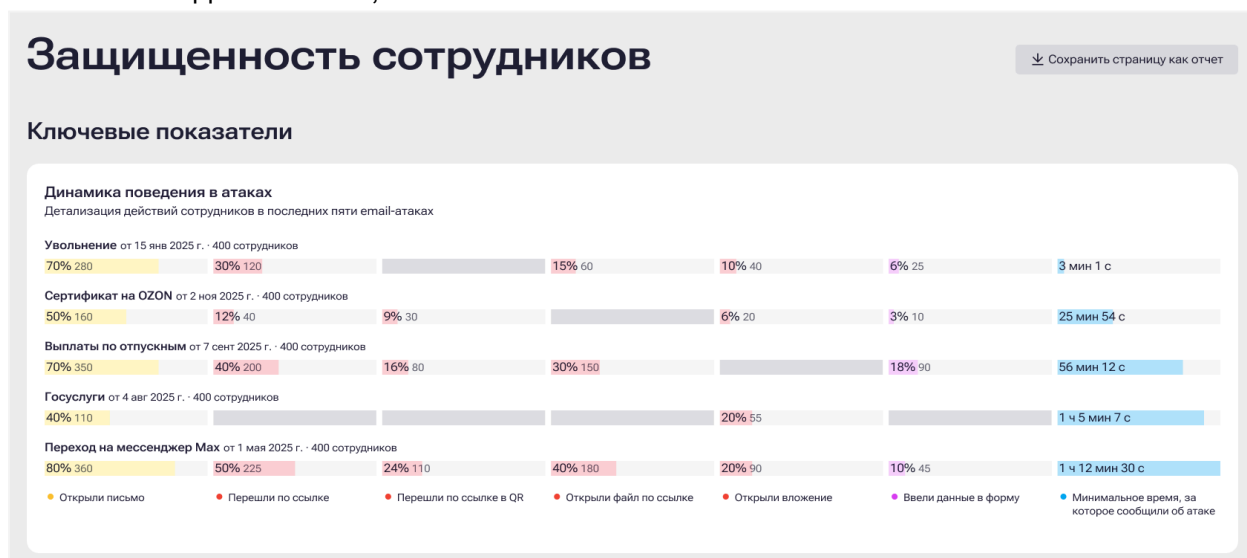
Раздел состоит из двух блоков:

- Ключевые показатели;
- Индекс защищенности компании.

Ключевые показатели

Показывает детализацию поведения сотрудников и подразделений в разных сценариях безопасности. Здесь можно отследить следующие показатели:

- **Динамика поведения в атаках** — какие действия совершали сотрудники в пяти последних атаках;



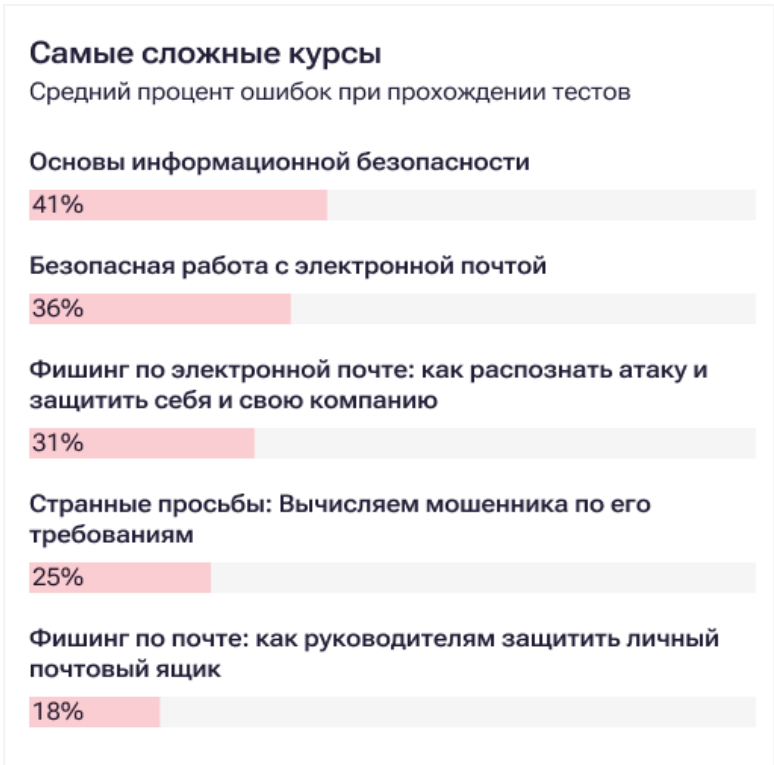
- **Статус прохождения обязательного курса;**



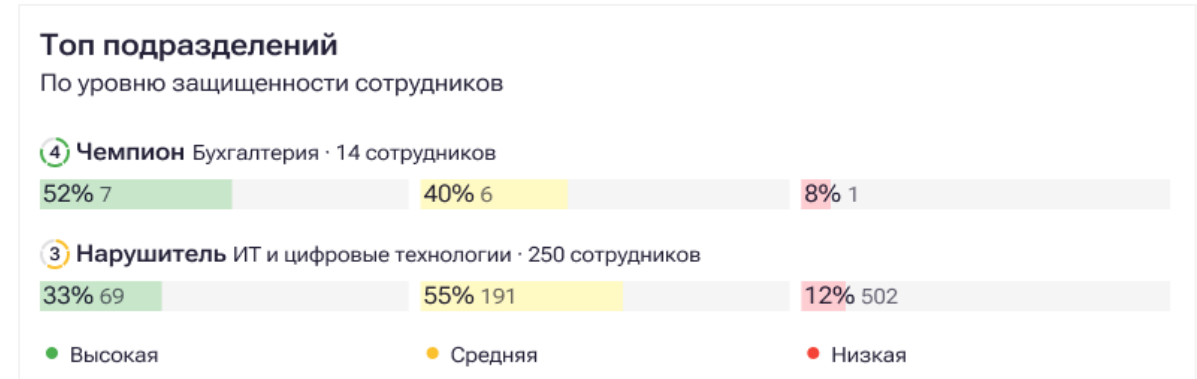
- **Влияние обучения на устойчивость к атакам** — как действовали обученные и необученные сотрудники в последней атаке;



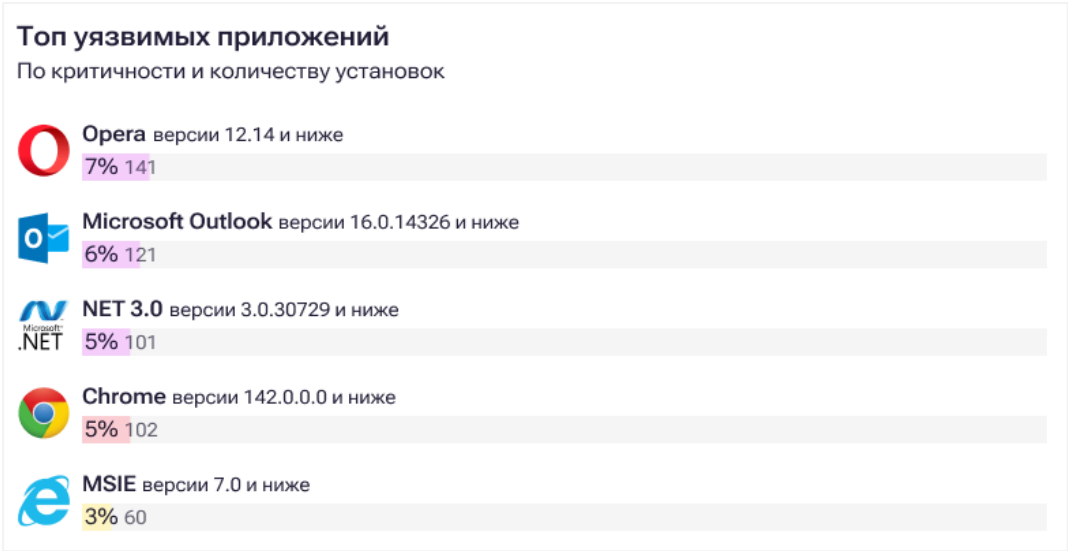
- **Самые сложные курсы** — показывает средний процент ошибок при прохождении тестов;



- **Топ подразделений** по уровню защищенности сотрудников;

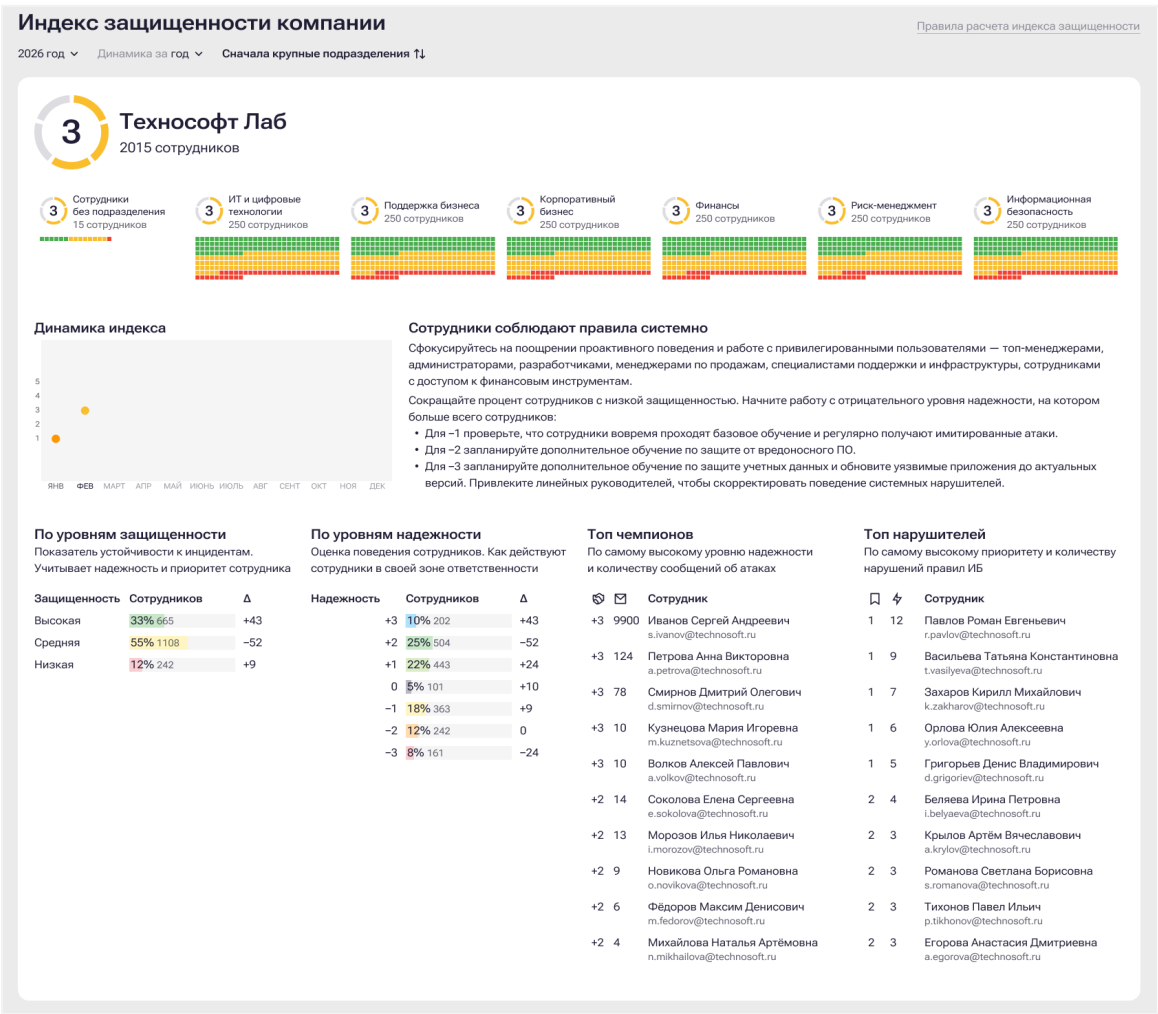


- **Топ уязвимых приложений** по критичности и количеству установок.



Индекс защищенности компании

Показывает общую оценку уровня безопасности компании. Объединяет ключевые метрики в общий индекс и помогает быстро понять общий уровень защищенности и распределение сотрудников по уровню риска.



Здесь можно отследить следующие показатели:

- уровень защищенности компании от угроз, связанных с человеческим фактором;
- уровень надежности сотрудников и соблюдения ими правил ИБ;
- топ чемпионов — сотрудников с высоким уровнем надежности и наибольшим количеством успешных сообщений об атаках;
- топ нарушителей — сотрудников с самым высоким приоритетом и наибольшим количеством нарушений правил ИБ.

💡 Узнать, как рассчитываются показатели защищенности компании можно на странице «Правила расчета индекса защищенности».

[← К защищенности](#)

Правила расчета индекса защищенности

Надежность сотрудника

Показатель устойчивости сотрудника к атакам мошенников. Рассчитывается на основе суммы его действий и бездействий в отношении политики информационной безопасности компании.

+3

Сообщил хотя бы об 1 атаке за последние 30 дней

+2

Выдержал последние 3 атаки за последние 90 дней
И проходит вовремя или прошел все назначенные курсы

+1

Получил или выдержал хотя бы 1 атаку за последние 30 дней
И назначен на обязательный курс — или прошел его вовремя за последние 365 дней

0

Новый сотрудник — добавлен в систему в течение последних 30 дней

-1

Не получил или провалил хотя бы 1 атаку за последние 30 дней

Заккрыть

Применить

Также в разделе доступны следующие функции:

- просмотр показателей по всей компании и подразделениям;
- динамика изменений за период — год, квартал, месяц;
- сквозная навигация по иерархии подразделений;
- выгрузка страницы с показателями в виде отчета в формате PDF.

Переменные

Использование переменных делает письмо персонализированным и повышает эффективность атаки. Их можно использовать в шаблоне письма, вложениях, а также на фишинговой и финальной страницах. Переменные автоматически заполнятся нужными значениями во время проведения рассылки с имитированной атакой.

Например, если на финальных страницах используется номер телефона

отдела ИБ, вам не нужно менять его вручную на каждой странице. Достаточно один раз обновить значение переменной `{security_phone}` в настройках — и новый номер автоматически появится во всех письмах и страницах.

Виды переменных

В системе есть стандартные и кастомные переменные. При необходимости список переменных можно расширить через обращение в техническую поддержку Start AWR.

Список переменных

Стандартные переменные

Значение подставляется системой автоматически.

Название	Переменная
Дата	
Текущая дата (ДД.ММ.ГГ)	{dmy}
Текущая дата (ДД.ММ.ГГ) +/- N дней	{dmy+N}
Полная дата (ДД месяц ГГГГ)	{date}
Полная дата (ДД месяц ГГГГ) +/- N дней	{date+N}
Полная дата (ДД месяц ГГГГ) +/- N дней с заданным языком	{date+N lang:ru}
День (ДД)	{day}
День (ДД) +/- N дней	{day+N}
Месяц (ММ)	{month}
Месяц (ММ) +/- N месяцев	{month+N}
Месяц (ММ) +/-N месяцев с заданным языком	{month+N lang:ru}
Год (ГГ)	{year}
Год (ГГ) +/- N лет	{year+N}
Случайные числа	
Случайное число с заданным разрядом	{rand:N}
Сотрудник	
Фамилия	{last_name}

Имя	{name}
Отчество	{middle_name}
Электронная почта	{email}
Подразделение	{department}
Должность	{position}
<i>Администратор</i>	
Фамилия	{admin_last_name}
Имя	{admin_name}
Отчество	{admin_middle_name}
Электронная почта	{admin_email}
Номер телефона	{admin_phone}
Название компании	{admin_company}
Подразделение	{admin_department}
Должность	{admin_position}
<i>Атака</i>	
Сгенерированный пароль	{password}
Код шаблона	{templateCode}
Домен отправителя	{domain}
Уникальный код письма	{payload}

Кастомные переменные

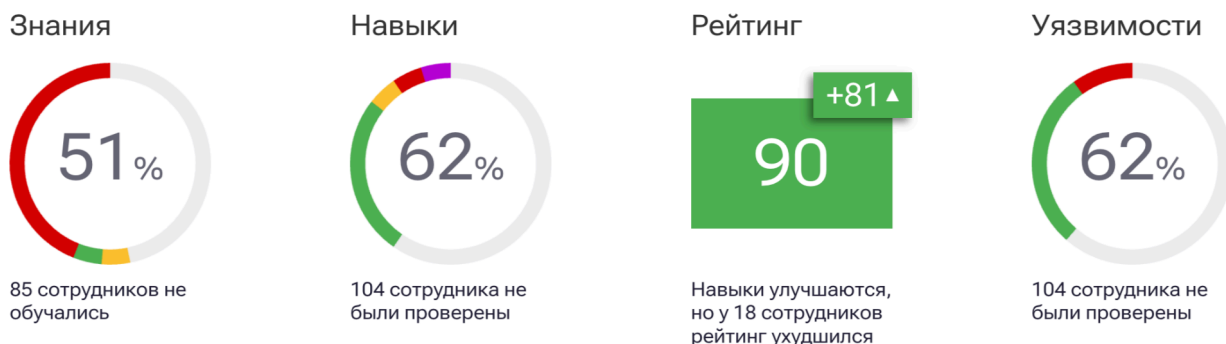
Значение задается вами и подставляется везде, где используется переменная. При необходимости значение можно изменить.

Название	Переменная
Название отдела ИБ для финальной страницы	{security_department}
Номер телефона отдела ИБ для финальной страницы	{security_phone}
Электронная почта отдела ИБ для финальной страницы	{security_email}

Логотип компании в формате Base64	{logo-b64}
Название проекта в уведомлениях об обучении	{project_name}
Включение переадресации на финальную страницу со всех ссылок на фишинговой странице	{enable_links_on_pages}
Фавикон финальной страницы	{favicon}

Дашборд в разделе «Ключевые показатели»

Ключевые показатели защищенности всегда доступны на дашборде. Он помогает видеть текущий уровень знаний, навыков, рейтинг и уязвимости сотрудников, а также с помощью него удобно отслеживать прогресс в обучении и тренировках. Дашборд состоит из нескольких диаграмм:



Где находится

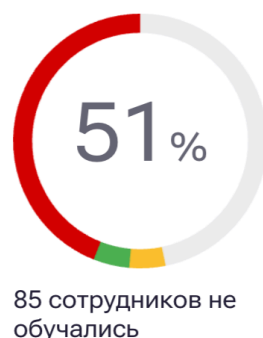
Меню → Ключевые показатели.

Как работает

- Все диаграммы (кроме рейтинга) разделены на секторы.
- Каждый сектор имеет свой цвет, который соответствует определенной категории сотрудников.
- Если нажать на сектор, внутри диаграммы отобразится процент сотрудников, который относится к этой категории.
- Чтобы узнать, сколько сотрудников относится к конкретному сектору — кликните на него.

Знания

Диаграмма показывает текущую статистику по обучению сотрудников.



Сотрудник может находиться только в одном секторе, который определяется исходя из худшего статуса по всем курсам.

Например, если сотрудник изучает пять курсов и один не завершает вовремя — худший статус по всем курсам будет «Не прошел обучение вовремя», сотрудник попадет в **красный** сектор.

Диаграмма делится на следующие секторы:

Название сектора	Цвет	Кто входит в сектор
Не обучались		Сотрудники, которые еще не начали проходить курсы.
На обучении		Сотрудники: — на которых назначили хотя бы один курс, — у которых нет статуса «Не прошел обучение вовремя» ни по одному курсу.
Прошли обучение		Сотрудники, которые успешно прошли все назначенные курсы.
Не прошли обучение вовремя		Сотрудники, которые не прошли вовремя хотя бы один курс.

Навыки

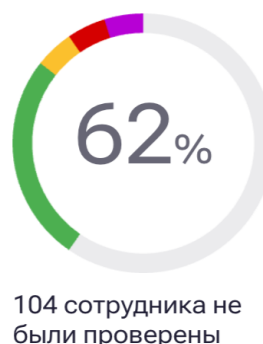
Диаграмма показывает текущую статистику по действиям сотрудников в последней имитированной атаке.

Сотрудник может находиться только в одном секторе, который определяется исходя из самого небезопасного действия в последней атаке.

Например, если сотрудник откроет письмо и перейдет по ссылке, он попадет в **красный** сектор «Перешли по ссылке или по ссылке в QR», а не в **оранжевый** «Открыли письмо», так как переход по фишинговой ссылке более опасное действие, чем открытие письма.

Диаграмма делится на следующие секторы:

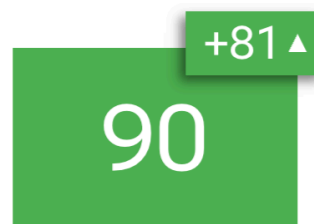
Название сектора	Цвет	Кто входит в сектор
Не проверялись		Сотрудники, которым не отправлялась ни одна имитированная атака.
Выдержали		Сотрудники, которые не совершали опасных



атаку		действий в последней атаке.
Открыли письмо		Сотрудники, которые открыли письмо с атакой, но при этом не совершили небезопасные действия: — не переходили по фишинговой ссылке или QR-коду, — не открывали вложение или файл по ссылке, — не вводили данные в форму.
Перешли по ссылке или по ссылке в QR		Сотрудники, которые перешли по фишинговой ссылке или ссылке из QR-кода, но при этом: — не открывали вложение или файл по ссылке, — не вводили данные в форму, — не совершали другие небезопасные действия.
Открыли вложение или открыли файл по ссылке		Сотрудники, которые открыли вложение или файл по ссылке, но при этом: — не вводили данные в форму, — не совершали другие небезопасные действия.
Ввели данные в форму		Сотрудники, которые вводили данные в форму.

Рейтинг

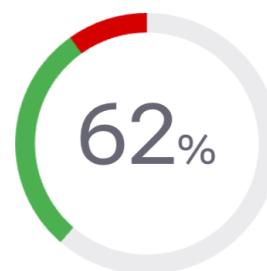
Диаграмма показывает общий рейтинг и как он изменился в последней имитированной атаке.



Навыки улучшаются, но у 18 сотрудников рейтинг ухудшился

Уязвимости

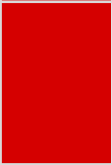
Диаграмма показывает статистику о программных уязвимостях, которые были найдены у сотрудников, когда они совершали небезопасные действия в имитированных атаках.



104 сотрудника не были проверены

Диаграмма состоит из секторов:

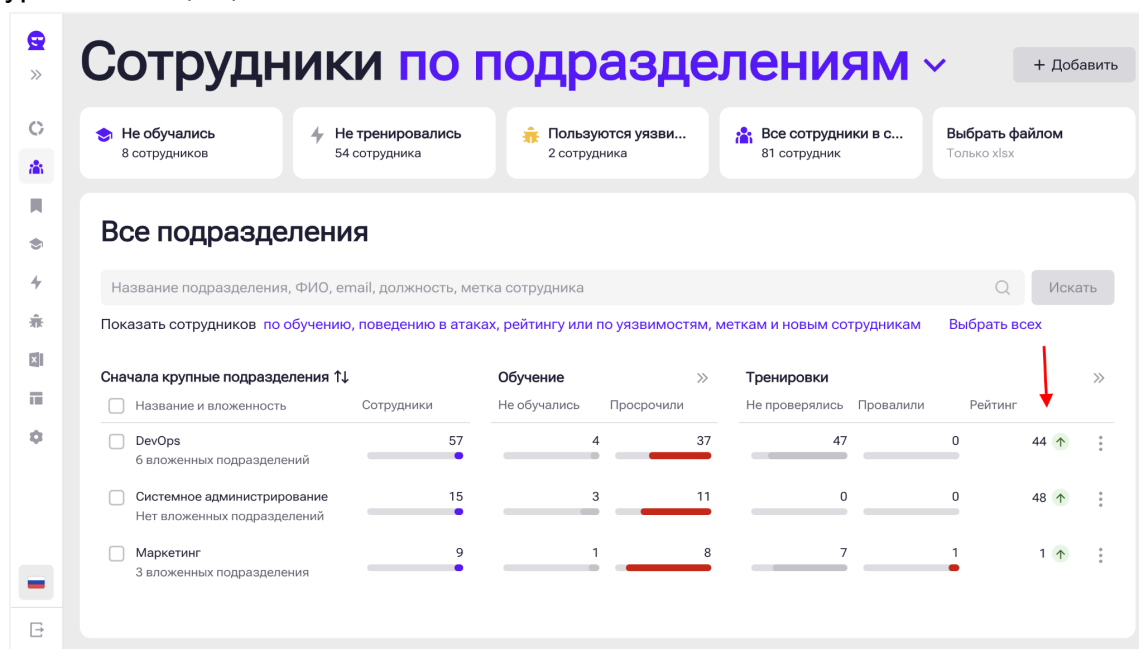
Название сектора	Цвет	Кто входит в сектор
Не проверялись		Сотрудники, которые еще не участвовали в атаках.

Не имеют уязвимых приложений		Сотрудники, у которых не нашли программных уязвимостей.
Имеют уязвимые приложения		Сотрудники, у которых нашли программные уязвимости. После устранения уязвимостей сотрудники перемещаются в сектор «Не имеют уязвимых приложений».

Также статистику поведения сотрудников можно увидеть в разделе **Сотрудники**.

Рейтинг сотрудников

В результате каждого действия по каждой имитированной атаке у сотрудника накапливается рейтинг — число, означающее одновременно его опыт и общий уровень защищенности.



Отрицательный рейтинг означает, что в большинстве имитированных атак сотрудник совершал небезопасные действия.

Формирование рейтинга

Рейтинг сотрудника характеризуют его навыки и действия в атаке. Обучение и наличие уязвимостей в ПО сотрудника не учитываются в начислении рейтинга.

При формировании рейтинга учитываются все небезопасные действия сотрудника, которые проверяются в атаках и показывают его навыки:

- открыл письмо (-1)
- перешел по ссылке (-1)

- перешел по ссылке в QR (-1)
- открыл вложение (-1)
- открыл вложение по ссылке (-1)
- ввел данные в фишинговую форму (-1)

Если сотрудник совершил хоть одно небезопасное действие в атаке, рейтинг в этой атаке автоматически становится отрицательным, так как атака считается не выдержанной.

То есть, если сотрудник открыл письмо, но не скачал файл или не перешёл по фишинговой ссылке, его рейтинг будет -1, а плюсовые значения по другим действиям уже не будут учтены.

Если человек выдержал атаку, т.е. не совершил ни одного опасного действия, ему присваивается статус «Выдержал атаку» и максимально возможный положительный рейтинг по данной атаке. Например, если атака содержала ссылку и вложение, сотруднику присваивается рейтинг +3 за атаку — он не открыл письмо, не перешел по ссылке и не открыл вложение.

Также сотрудник имеет возможность получить дополнительный +1 балл, если сообщит об имитированной атаке через плагин, или если администратор при редактировании этого сотрудника в системе укажет, что сотрудник сообщил об имитированной атаке.

Если внутри письма нет детектирующей ссылки, а сотрудник просто открыл письмо и не перешел по ссылке, то его рейтинг не изменится.

Контроль уязвимостей приложений

Для сотрудников, которые совершили небезопасное действие в имитированной атаке, Start AWR определяет версии их браузеров, плагинов, офисных программ и операционных систем.

Чтобы просмотреть наличие таких рисков, перейдите в **Меню** → **Уязвимости**.

Уязвимости

Подготовить отчет по уязвимостям

Уязвимые приложения Уязвимые сотрудники

Кол-во	Приложение и версия	Рейтинг	Комментарий
6	Chrome версии 145.0.0.0 и ниже	[Red bar]	Приложения содержат уязвимости, которые могут использовать злоумышленники для проведения атак на пользователей и получения скрытого удаленного доступа в сеть компании. Рекомендуется обновить приложения
3	Android версии 6 и ниже		
1	iOS mobile OS версии 16_5_1 и ниже		
2	Firefox версии 147.0 и ниже		
1	Edge версии 113.0.1774.50 и ниже	[Yellow bar]	Приложения содержат незначительные уязвимости. Использование может привести к нестабильной работе или будущим рискам безопасности. Рекомендуется обновить приложения

Уязвимости в этих версиях считаются дополнительным риском безопасности, и классифицируются в зависимости от рейтинга уязвимости (CVSS Score). Статистика по таким рискам доступна в отдельном разделе, с группировкой по приложениям и сотрудникам.

Статистику по уязвимостям можно использовать для улучшения процессов управления уязвимостями, например, объединяя со статистикой внутренних систем сканирования.

Уязвимости, которые были устранены на рабочем месте сотрудника или определены как ложное срабатывание, можно исключить из статистики Start AWR.

Обучение сотрудников

Start AWR позволяет обучать сотрудников. Все курсы доступные администратору отображаются на странице настроек.

Настройки

Сохранить отладочную информацию

Обновить систему

Администраторы

Работа с сотрудниками

Обучение

Почтовый плагин

Тренировки

Переменные

Курсы

Статистика по обучению

Новый курс

Сначала видно в системе ↑↓

☐ Название

Владелец

Роль

Статус

Видно в системе

☐ Основы информационной безопасности

Константинопольский Кирилл

Суперадминистратор

Назначен

☒

☐ Защита конфиденциальных данных

Константинопольский Кирилл

Суперадминистратор

Назначен

☒

☐ Защита персональных данных

Ахмадулина Лейсан

Администратор

Назначен

☐

☐ Работа с электронной подписью

Константинопольский Кирилл

Суперадминистратор

Назначен

☐

☐ Создание и хранение паролей

Константинопольский Кирилл

Администратор

Назначен

☒

☐ Безопасная работа с электронной почтой

Кузнецов Владимир

Суперадминистратор

Назначен

☒

Сертификаты

Архив сертификатов сотрудников

Название

Сертификат об успешном прохождении обучения 2026

По умолчанию

Сертификат об успешном прохождении обучения 2025

Сертификат об успешном прохождении обучения 2024

Уведомления

При добавлении нового курса система отображает ФИО того, кто добавил курс и его роль. Чтобы избежать случайного удаления курса, который используется в обучении, система отображает статус у каждого задействованного в процессе курса.

Из интерфейса можно выбрать сотрудников и отправлять их на один или несколько курсов. Ознакомиться подробнее с тем, как назначить обучение сотрудникам, можно в разделе «Обучить».

Для автоматизации процессов обучения рекомендуем использовать инструмент «Процессы». Подробнее о нем в разделе «[Процессы](#)».

При использовании встроенной системы обучения Start AWR сотруднику не нужно вводить логин и пароль: уникальная ссылка из письма-приглашения авторизует его и даст доступ в любой из назначенных курсов.

Даже если письмо со ссылкой будет утеряно, назначенный на курс сотрудник в любой момент сможет получить доступ к системе обучения через страницу авторизации обучающей системы.

Start AWR
Система обучения и контроля защищенности сотрудников

Получить ссылку

Русский

Start X Поддержка: [+7 \(499\) 677-19-07](#)

Общий список назначенных курсов для сотрудника доступен на главной странице системы обучения.

Start AWR

[Мои курсы](#) [Сертификаты](#)

Егорова Анна Ивановна
egorova@securebrand.local

Всего 3 курса

По статусу: сначала просроченные ▾

Курс	Статус обучения	Пройти до	Проходной балл	
Работа с электронной подписью	Пройти сегодня	28 июля 2025 г.	92.5%	>
Безопасная работа с электронной почтой	Пройти сегодня	28 июля 2025 г.	92.5%	>
Вы уже обучились				
Мини-курс «Атаки через картинки»	Пройден			>

Русский

Start X Поддержка: [+7 \(499\) 677-19-07](#)

Администратор может заменить логотип, подпись, а также контактные данные, которые будут отображаться у сотрудников в интерфейсе системы обучения.

Система электронного обучения

* поля обязательные для заполнения

Встроенная

Внешняя

Адрес

http://

https://

Адрес*
https://edu.your-company.ru/

Загрузите логотип

Подойдет файл в формате .png .jpg или .gif

Рекомендуемая ширина 248 px, высота 40—80 px

Выбрать файл

Название

Небольшой комментарий под логотипом

Описание

Ссылка на копирайте

http://

https://

Адрес

Телефон поддержки

Язык
Русский

На прохождение курсов

2

Дня

Недели

Вы можете установить значение от 1 до 999

Тип авторизации

Токен

LDAP

Токен/SSO

LDAP/SSO

Ссылка на обучение

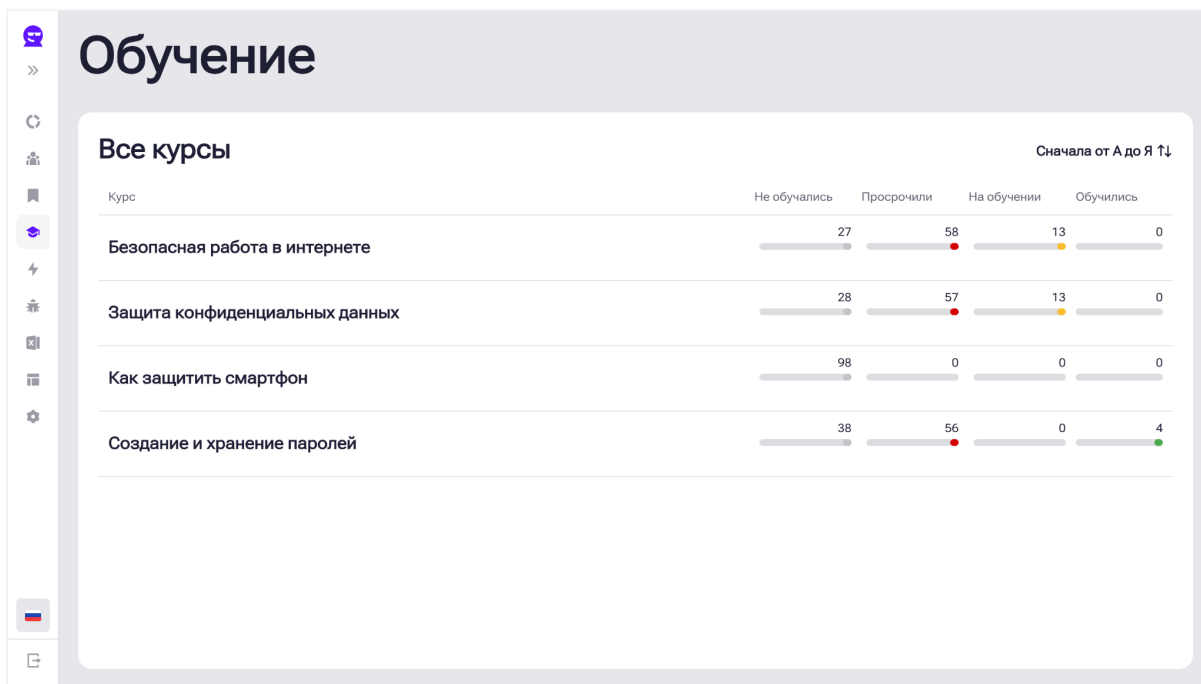
Бессрочная

Одноразовая

Сохранить настройки

Курс будет считаться пройденным после просмотра всех слайдов и сдачи встроенного в курс теста. Время на прохождение обучения можно задать в настройках.

Вся статистика по обучению доступна в разделе **Обучение**, в отчете по обучению, а также в общем отчете.



При подготовке отчета по обучению администратор может выбрать для него период из календаря — стандартный период или период, охватывающий все время использования системы. Всех прошедших обучение сотрудников рекомендуется включать в приоритетные цели имитированных атак для тренировки и проверки навыков.

Отчеты

Подготовить

Общий
по активным сотрудникам.xlsx
по всем, включая удаленных.xlsx

Со сводной статистикой
по сотрудникам.xlsx
по компании.xlsx

Готовые

Обучение
статистика по обучению.xlsx

Другое
полная статистика.csv
истика.zip
сотрудников.csv

Выберите период формирования отчета

☐ За все время ☐ Включить в отчет удаленных сотрудников

Фев. 2026							Мар. 2026						
пн	вт	ср	чт	пт	сб	вс	пн	вт	ср	чт	пт	сб	вс
26	27	28	29	30	31	1	23	24	25	26	27	28	1
2	3	4	5	6	7	8	2	3	4	5	6	7	8
9	10	11	12	13	14	15	9	10	11	12	13	14	15
16	17	18	19	20	21	22	16	17	18	19	20	21	22
23	24	25	26	27	28	1	23	24	25	26	27	28	29
							30	31	1	2	3	4	5

01 фев. 2026 - 01 мар. 2026

Подготовить

хотите подготовить

Также при необходимости в отчет можно включить удаленных сотрудников. Если сотрудник удален из системы, в отчете у него будет статус «Неактивен».

Рекомендации по использованию системы

Start AWR позволяет автоматизировать процессы обучения и контроля защищенности сотрудников. Для эффективного использования системы рекомендуем выполнять следующие процедуры:

Ежедневно — 15 минут

- Проводить синхронизацию сотрудников — через выгрузку из кадровой системы, каталога или другого достоверного источника информации об активных сотрудниках.
- Отправлять на обучение всех новых сотрудников.
- Проверять навыки всех новых сотрудников на актуальных имитированных шаблонах.

Два раза в месяц — 30 минут

- Обновлять базу уязвимостей (для локальной версии);
- Выявлять критические уязвимости и отправлять отчеты в ИТ, принимать отчеты и корректировать уязвимости в системе.
- Выявлять сотрудников с наихудшим рейтингом, не прошедших обучение вовремя, отправлять на дообучение или применять к таким сотрудникам дисциплинарные меры.

Ежемесячно — 60 минут

- Принимать обновление системы (для локальной версии).
- Принимать новые шаблоны, планировать имитированные атаки для актуальных групп сотрудников.
- Принимать новые учебные материалы, отправлять актуальные группы сотрудников на дообучение.
- Выгружать и анализировать отчеты по процессам обучения, проверки навыков и устранения уязвимостей.

Почтовый плагин

Почтовый плагин Start AWR — это дополнение к почтовому клиенту Microsoft Outlook, которое позволяет сотруднику сообщить вашей команде безопасности о подозрительном письме.

Главная ценность — плагин помогает сотрудникам быстро сообщать об атаках и защищать организацию. В результате:

1. Сотрудники меньше попадают на фишинговые атаки. Они становятся более внимательными и осторожными при работе с письмами.
2. Повышается культура информационной безопасности в компании. Сотрудники участвуют в защите информации и осознают важность

собственного вклада в безопасность компании.

3. Сокращается время обнаружения инцидента. Атака выявляется практически сразу после получения письма, еще до момента ее обнаружения техническими средствами защиты.

Системные требования

Плагин можно установить для почтовых клиентов:

- Windows — Outlook 2013 или более поздней версии,
- Mac — Outlook 2016 или более поздней версии.

Также они должны работать с почтовым сервером Microsoft 365, Exchange Online, Exchange Server или другими, которые поддерживают [Exchange Web Services](#) (EWS).

Язык

По умолчанию в плагине установлен язык, который выбран у сотрудника в настройках Start AWR.

Если в настройках Start AWR не выбран язык или выбран неподдерживаемый — в плагине установится язык из настроек браузера.

Если язык в браузере не определился или он не поддерживается платформой Start AWR — плагин будет на английском языке.

Настройка в Start AWR

1. Перейдите в раздел **Настройки** → **Почтовый плагин**.
2. Настройте параметры:

Куда пересылать сообщения

* поля обязательные для заполнения

Адрес получателя*

test@antph.local ×

▼

Префикс

[STARTX]

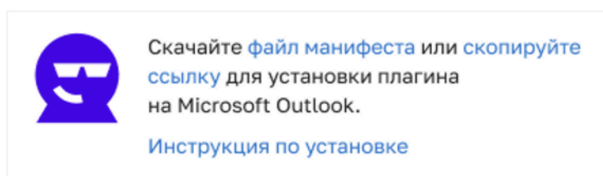
☒ Сохранять сообщения в системе

☐ Пересылать сообщение во вложении

Сохранить

- **Адрес получателя*** — введите один или несколько электронных адресов, на которые будут поступать письма, отмеченные сотрудниками, как фишинговые. По умолчанию здесь указан электронный адрес ответственного за систему.
- **Префикс** — введите префикс, который будет отображаться в теме каждого письма с обратной связью от сотрудников.
- **Сохранять сообщения в системе** — при включении этого параметра в базе данных будут сохраняться заголовки и содержимое писем.
- **Пересылать сообщение во вложении** — при включении этого параметра на электронные адреса из поля «Отправлять сообщения на эти адреса» будут поступать заголовки и содержимое писем в формате eml или txt (в зависимости от размера письма).

3. Скачайте файл манифеста или скопируйте ссылку на него.



Готово! Переходите к этапу установки плагина в Microsoft Outlook.

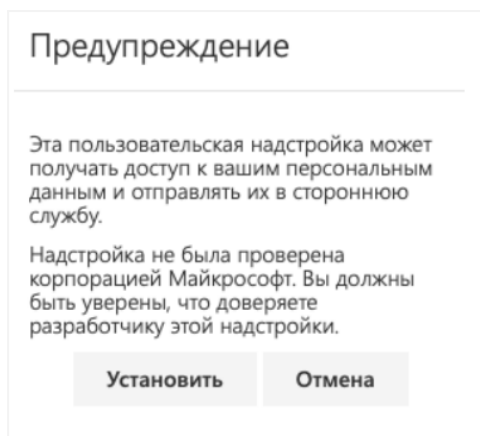
Установка

Есть два способа установить плагин:

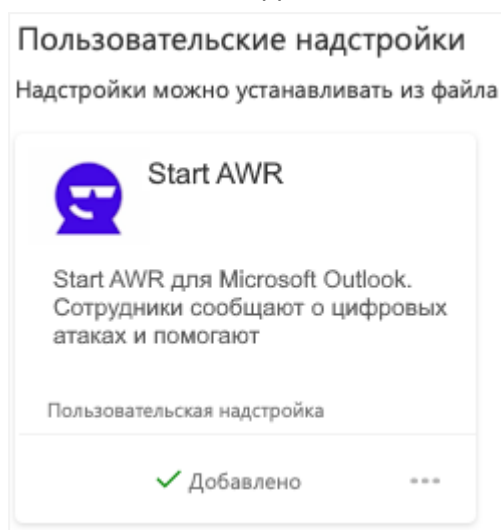
- **Локально**
Плагин устанавливается вручную на каждый компьютер.
- **Централизованно**
Плагин устанавливается через почтовые серверы Microsoft Exchange Online, Exchange Server и Microsoft 365. Централизованная установка упрощает управление и обновление плагина, так как изменения вносятся централизованно.

Локально

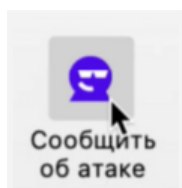
1. В главном разделе Microsoft Outlook нажмите **Получить надстройки**.
2. В открывшемся окне **Надстройки для Outlook** выберите **Мои надстройки** → **Добавить пользовательскую надстройку**.
3. Добавьте ранее скачанный файл манифеста любым удобным способом — через загрузку файла или с помощью ссылки.
Если появится предупреждение, нажмите кнопку **Установить**.



4. Готово! После установки в пользовательских надстройках появится почтовый плагин для Microsoft Outlook.



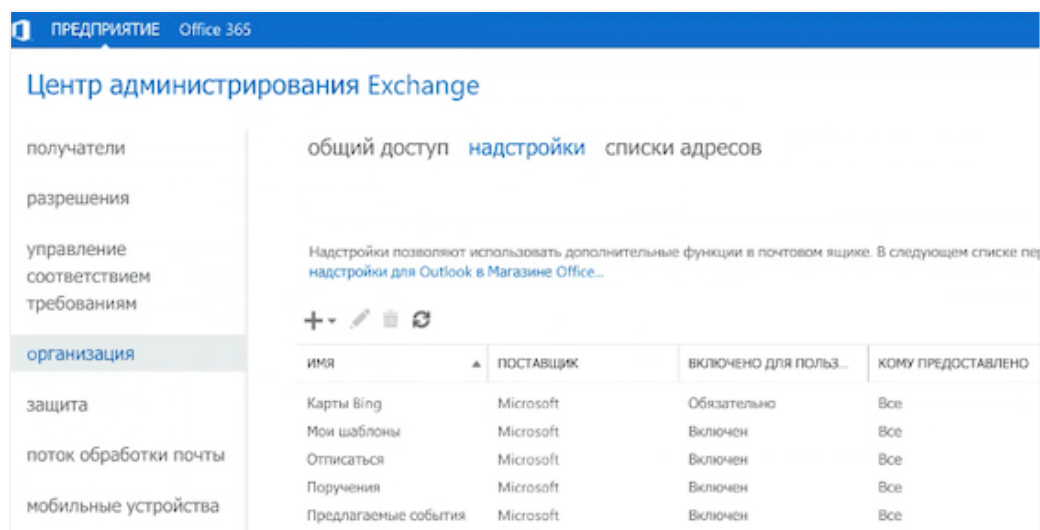
На верхней панели Microsoft Outlook появится плагин Start AWR с кнопкой **Сообщить об атаке**.



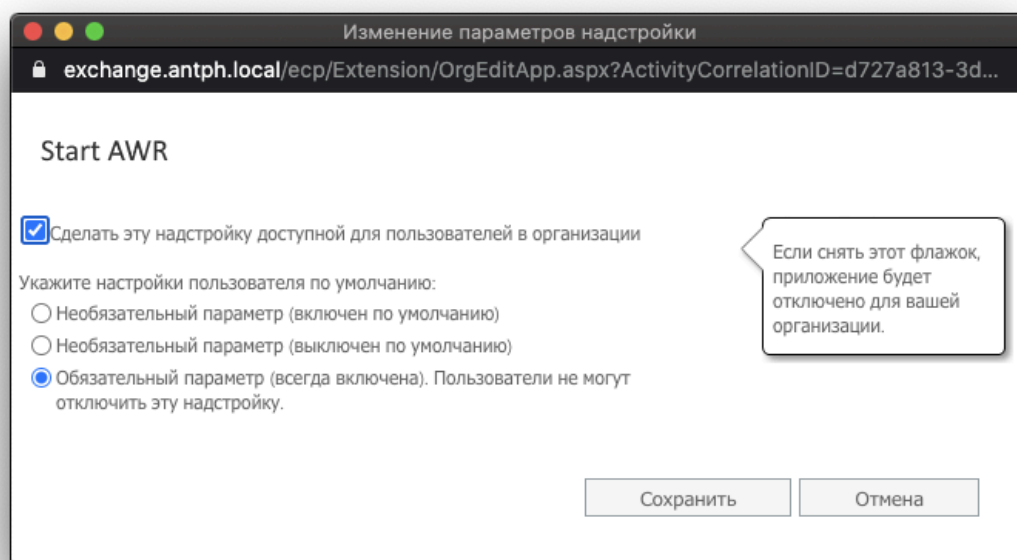
Централизованно

Алгоритм установки рассмотрим на примере Microsoft Exchange Server:

1. Войдите на портал администратора вашего почтового сервера.
2. Перейдите в раздел **Надстройки** или **Управление надстройками** и нажмите кнопку **+**.



3. Добавьте файл манифеста любым удобным способом — по URL-адресу или загрузите из файла.
4. На некоторых версиях может появиться подобное окно.

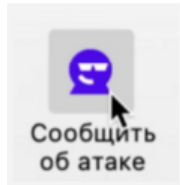


Отметьте в нем пункты:

- Сделать надстройку доступной для пользователей в вашей организации
- Обязательный параметр (всегда включена). Пользователи не могут отключить эту надстройку.

5. Нажмите кнопку **Сохранить** для завершения установки. Убедитесь, что настройки применились корректно и режим «Обязательно» включен.
6. Готово! После установки в списке надстроек появится плагин Start AWR для Microsoft Outlook.

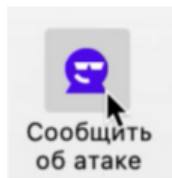
На верхней панели Microsoft Outlook появится плагин Start AWR с кнопкой **Сообщить об атаке**.



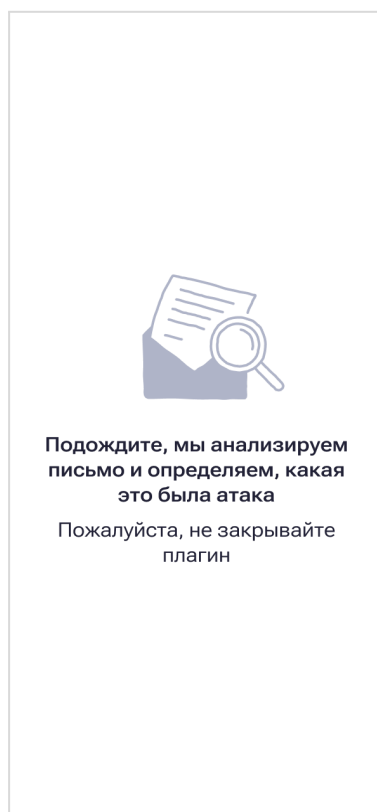
Работа плагина

После открытия письма:

1. Нажмите кнопку **Сообщить об атаке**.



2. Подождите, пока плагин проанализирует письмо и определит тип атаки — реальная или имитированная.



Если плагин не работает — сделайте скриншот письма и отправьте на почту, которая будет указана в этом окне:



К сожалению, плагин пока не работает

Мы уже знаем о проблеме и исправим ее как можно раньше.

Чтобы команда безопасности узнала о возможной атаке, сделайте скриншот письма и отправьте на почту:



Хорошо

3. Заполните форму обратной связи:



Ура! Вы смогли выявить письмо, которое было частью имитированной атаки

Спасибо вам за внимательное отношение к безопасности.

Какие эмоции вызвало письмо?

 Добавить эмоцию

Какая была коммуникация?

☒ Личное сообщение, не связанное с работой

☐ От имени коллег или руководителей

☐ От внешних партнеров, подрядчиков

Что показалось подозрительным?

 Указать детали

Здесь вы можете оставить любой комментарий о подозрительном письме или работе плагина

Не более 1000 символов

Отзыв отправим команде безопасности, а письмо переместим в папку «Удаленные». Если письмо не переместится автоматически, пожалуйста, удалите его самостоятельно.

Я — молодец

Имитированная атака



Похоже, вы смогли выявить подозрительное письмо

Спасибо вам за внимательное отношение к безопасности.

Какие эмоции вызвало письмо?

 Добавить эмоцию

Какая была коммуникация?

☒ Личное сообщение, не связанное с работой

☐ От имени коллег или руководителей

☐ От внешних партнеров, подрядчиков

Что показалось подозрительным?

 Указать детали

Здесь вы можете оставить любой комментарий о подозрительном письме или работе плагина

Не более 1000 символов

Отзыв отправим команде безопасности, а письмо переместим в папку «Спам». Если письмо не переместится автоматически, пожалуйста, удалите его самостоятельно.

Я — молодец

Реальная атака

Какие эмоции вызвало письмо:

- Страх,
- Раздражение,
- Любопытство,
- Жадность,
- Авторитет,
- Срочность,
- Невнимательность,
- Желание помочь.

Какая была коммуникация:

- Личное сообщение, не связанное с работой
- От имени коллег или руководителей
- От внешних партнеров, подрядчиков

Что показалось подозрительным:

- Адрес отправителя,
- Вложение,
- Ссылка в письме,
- Я не ждал этого письма,
- Свой вариант.

Комментарий — оставьте любой комментарий о подозрительном письме или работе плагина. Длина комментария должна быть не более 1000 символов.

4. После заполнения формы обратной связи, нажмите кнопку **Я – молодец**.
5. Готово! Обратная связь отправлена команде безопасности. Письмо переместится в зависимости от типа атаки:
 - при реальной атаке — в папку «Спам»,
 - при имитированной атаке — в папку «Удаленные».

Кастомизация внешнего вида плагина

Администратор может настраивать вид формы, которую увидит сотрудник компании в почте, в зависимости от типа письма, которое сотрудник помечает как подозрительное.

Редактирование внешнего вида плагина происходит в разделе **Настройки** → **Почтовый плагин**. Доступ к этому разделу можно редактировать с помощью ролевой модели.

Типы писем по умолчанию

По умолчанию в системе есть два вида писем:

- **Имитированные** — преднамеренные угрозы без вредоносного ПО в виде электронных писем, созданные с помощью Start AWR.
- **Внешние** — под этот тип попадают все неимитированные атаки.

Кастомные типы писем

Кроме двух типов по умолчанию можно создавать собственные типы и задавать для них вид формы ОС.

Новый тип задается с помощью раздела **Правило**, в котором необходимо заполнить хотя бы одно поле. Значения из полей **От**, **Кому**, **Тема** и **Копия** система будет искать в заголовках письма, а значение из поля **Токен** — в теле письма. При этом если заполнить несколько полей, правило сработает в том случае, если совпало хотя бы одно из значений в каждом поле (внутри поля значения связаны через ИЛИ, а сами поля связаны через И).

Настройка логики отправки письма в команду безопасности/реагирования на инциденты/SOC компании

Для внешнего типа и для любого нового типа можно выбрать, в какой момент плагин должен отправить письмо команде безопасности.

Отправка письма в службу ИБ

☐ Сразу

☒ После обратной связи

Два возможных варианта:

- **Сразу**

Логика работы:

Сотрудник нажал на «Сообщить об атаке» в плагине → Сообщение отправляется в службу ИБ → Сотруднику открывается форма ОС. При настройке такой логики отправки сообщение в службу ИБ уходит без данных из формы ОС, которые заполнит сотрудник. При этом эти данные будут отражены в отчете по обратной связи от сотрудников.

- **После обратной связи**

Логика работы:

Сотрудник нажал на «Сообщить об атаке» в плагине → Сотруднику открывается форма ОС → Сотрудник заполняет поля → Нажал на «Я – молодец!» → Сообщение отправлено в службу ИБ. В пересланном сообщении выведены заполненные данные по вектору, типу атаки, причине и комментарий.

Предварительный просмотр формы ОС

С помощью окна **Пreview плагина** администратор может увидеть, как будут выглядеть все формы обратной связи у сотрудника с учетом тех данных, которые он внес в поля. Изменения отображаются в превью в реальном времени.

Отчет по обратной связи от сотрудников

Отчет помогает увидеть, как сотрудники распознают подозрительные письма и на что обращают внимание.

Чтобы скачать его, перейдите в раздел **Меню** → **Отчеты** и выберите отчет **Обратная связь от сотрудников**.

В отчете содержится следующая информация:

- ID письма;
- Название имитированной атаки;
- Дата и время получения письма;

- От кого;
- Тема;
- Дата и время пересылки;
- ID сотрудника;
- ФИО сотрудника;
- Эл. почта;
- Должность;
- Отдел;
- Психологические векторы атаки;
- Источники атаки;
- Причина;
- Комментарий.

Планировщик

Чтобы добавить новое правило для планировщика, перейдите в раздел **Меню** → **Настройки** и нажмите **Планировщик**. В открывшейся форме нажмите **Добавить**.

Новое правило

Название

Что случилось?

Перешел по ссылке

Открыл вложение

Открыл письмо

Что нужно сделать?

Отправить на обучение

все курсы

выбранные курсы

Безопасная работа с электронной почтой

Информационная безопасность для пользователей

пройти: в ближайшие 3 дня

Выполнить

сразу

с задержкой...

не чаще, чем...

1

минута

час

день

неделя

Применить

ко всем сотрудникам

Отменить

Сохранить

Можно добавить несколько событий-триггеров и действий, которые должны произойти по этим событиям.

При создании правила планировщика можно выбрать конкретных сотрудников, для которых правило будет применено или наоборот, к которым оно применяться не будет.

Отчеты

Через правило планировщика можно выбрать и назначить руководителя для получения отчета по отделу:

Новое правило

Название

Ежемесячный отчет по атакам

Что случилось?

На сотрудника назначена атака

Что нужно сделать?

Сформировать и отправить отчет

☐ основной отчет
☒ отчет по действиям сотрудника
☐ отчет по отделу сотрудника
☐ отчет по рискам
☐ отчет по обучению

администраторам

руководителям

сотрудникам...на адреса...

Выполнить

сразу

с задержкой...

не чаще, чем...

1

раз в

час

день

неделю

месяц

Применить

к 3 сотрудникам

Отменить

Сохранить

Все действия планировщика записываются и доступны для анализа через журнал действий:

report-scheduler - Excel						
ФАЙЛ ГЛАВНАЯ ВСТАВКА РАЗМЕТКА СТРАНИЦЫ ФОРМУЛЫ ДАННЫЕ РЕЦЕНЗИРОВАНИЕ ВИД						
Общий						
Условное форматирование Форматирование как таблицу						
J38 : ✕ ✓ fx все курсы						
	A	B	C	D	E	F
22	Сергеев Сергей Анатольевич	Отдел ИТ	sergeev@antiphish.ru	15.03.2018	22:44	добавл
23	Иванов Сергей Иванович	Отдел закупок	ivanov@antiphish.ru	15.03.2018	22:44	добавл
24	Смирнова Светлана Владимировна	Служба по управлению	smirnova@antiphish.ru	15.03.2018	22:44	добавл

Чтобы обезопасить данные отчета из планировщика, можно установить пароль на архив. Для этого откройте командную строку на сервере Start AWR и введите:

```
php yii options/report/archive --clientId={clientId} --mode=1
```

clientId — идентификационный номер учетной записи в Start AWR. Его можно уточнить в службе поддержки.

mode — включение (1) и выключение (0).

Появились вопросы?

Мы будем рады помочь. Обратиться к нам можно:

- через портал поддержки <https://startx.support/>
- по электронной почте support@startx.team
- по телефону +7 499 677 19 07