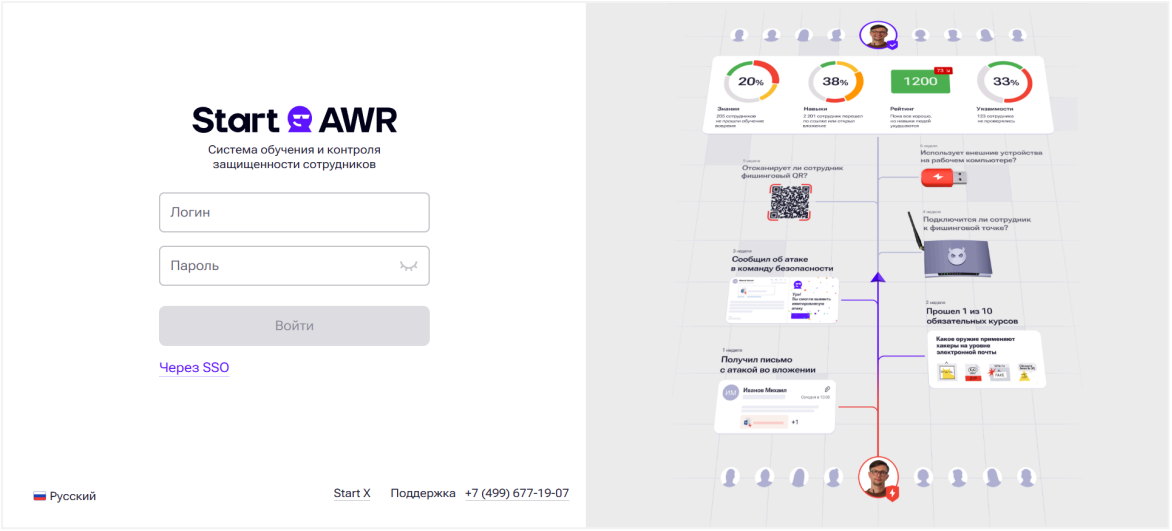
Инструкция по началу работы

Авторизация

Все функции Start AWR доступны через панель управления по ссылке https://attack.antiphish.ru/login.



Вход в систему возможен несколькими способами:

- по логину и паролю,
- через LDAP,
- с помощью SSO.

👉 При первом входе в систему нужно использовать логин и пароль. После этого можно настроить авторизацию через LDAP или SSO.

Вход по логину и паролю

1. В адресной строке браузера введите ссылку для входа в систему Start AWR.

2. Введите логин и пароль.

3. Нажмите кнопку **Войти**.

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

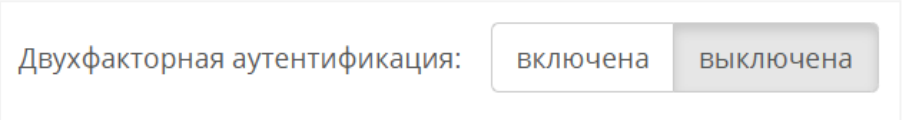
Двухфакторная аутентификация (2FA)

2FA позволяет повысить безопасность учетной записи, добавив второй шаг при входе. После ввода логина и пароля потребуется подтвердить вход кодом из приложения.

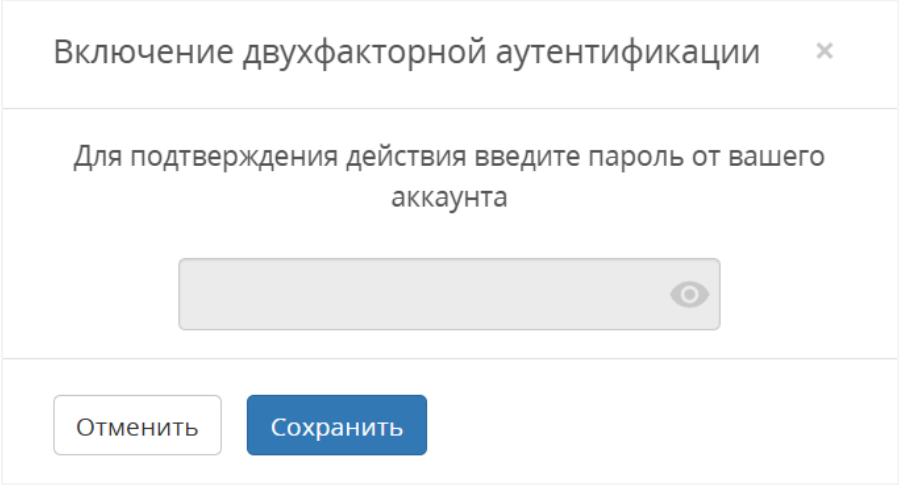
☝ Двухфакторная аутентификация доступна только для входа по логину и паролю. При включенной авторизации через LDAP или SSO второй фактор система не запрашивает.

Настройка
Перед настройкой двухфакторной аутентификации установите приложение для генерации кодов, например, Google Authenticator. Далее выполните шаги:

1. Перейдите в **Меню** → **Настройки**.
   Найдите пункт **Двухфакторная аутентификация** и нажмите **Включена**.



2. В открывшемся окне введите пароль от вашего аккаунта.



3. Нажмите кнопку **Сохранить**.
4. В открывшемся окне отсканируйте QR-код с помощью приложения или введите уникальный код, который будет указан ниже.

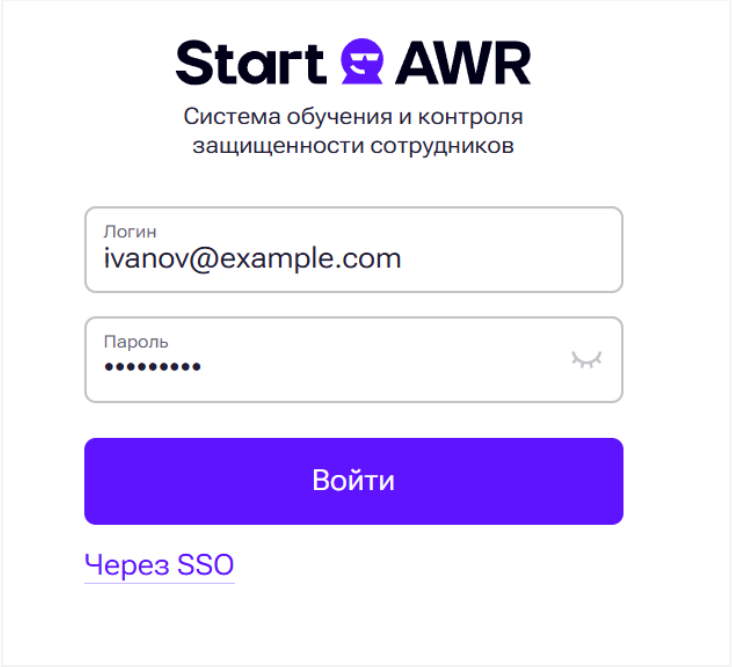
5. Чтобы завершить настройку, введите в окне код подтверждения из приложения.

   Готово! Вы настроили двухфакторную аутентификацию.

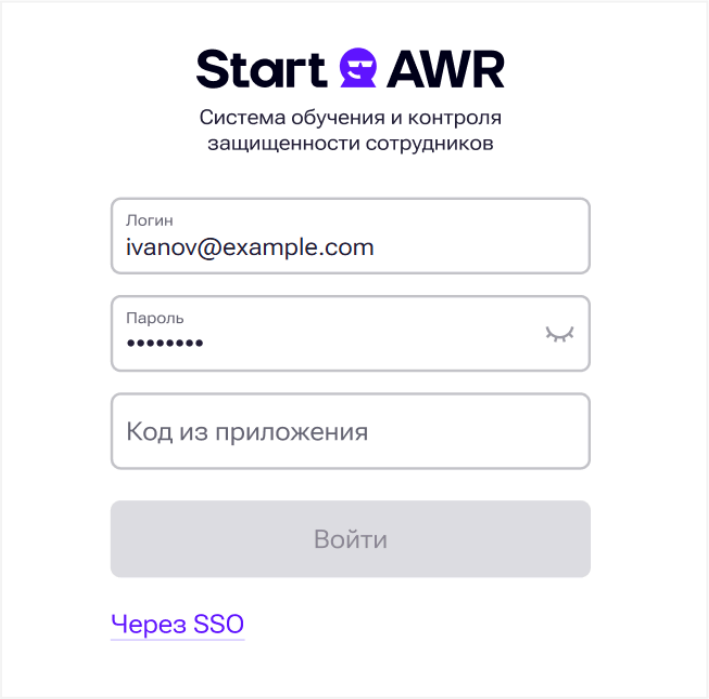
Как войти

Чтобы войти на платформу с помощью 2FA:

1. Откройте страницу входа в Start AWR.
2. Введите логин и пароль.



3. Нажмите кнопку **Войти**.
4. Появится поле **Код из приложения**. Введите в нем соответствующий код.



5. Нажмите снова кнопку **Войти**.

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

Вход по LDAP

LDAP-аутентификация позволяет входить в систему с логином и паролем из корпоративного каталога.

Настройка
Перед тем, как использовать этот способ входа:

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

Как войти

1. В адресной строке браузера введите ссылку для входа в интерфейс Start AWR.
2. Введите логин и пароль от учетной записи LDAP.
3. Нажмите кнопку **Войти**.

   Готово! Вы вошли на платформу с помощью LDAP.

Вход по SSO

SSO-аутентификация по протоколу SAML 2.0 позволяет 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.

Настройка

Перед тем, как использовать этот способ входа:

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

Как войти

1. В адресной строке браузера введите ссылку для входа в интерфейс Start AWR.
2. Выберите способ авторизации — **Через SSO**.
3. Введите логин от учетной записи администратора — электронную почту.
4. Нажмите кнопку **Войти**.
5. 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.

Роли администраторов

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

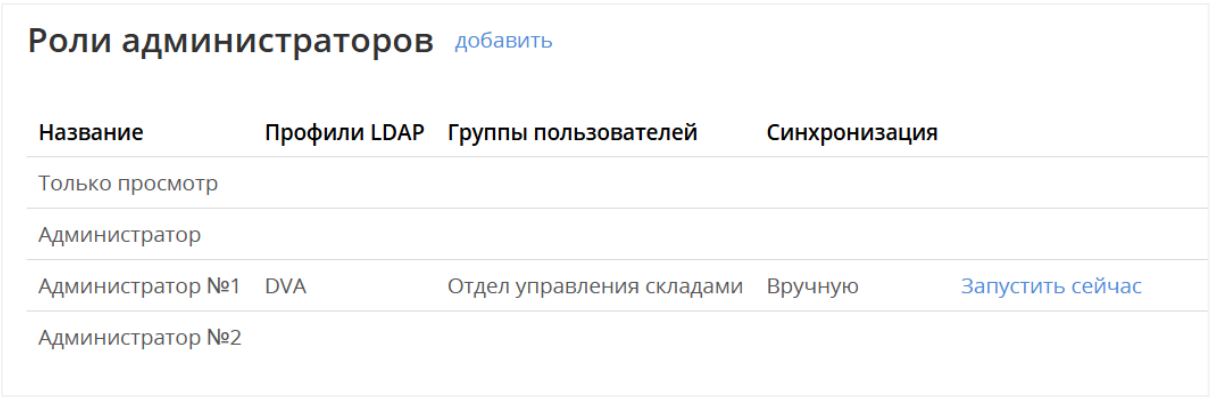
По умолчанию на платформе доступны две системные роли:

- **Администратор** — может делать в системе почти всё: настраивать, управлять сотрудниками и организовывать их обучение и прочее. Исключение — не может создавать роли и учетные записи для других администраторов.
- **Только просмотр** — для этой роли доступен просмотр данных по сотрудникам и атакам, а также сохранение отчетов.

☝ Изменение прав для системных ролей недоступно.

Описание интерфейса

Чтобы увидеть список всех ролей, перейдите в **Меню** → **Настройки** → **Роли администраторов**.



Для просмотра прав нажмите на нужную роль в списке.

Блок **Роли администраторов** представлен в виде таблицы со столбцами:

- **Название** — название ролей администраторов.
- **Профили LDAP** — профили LDAP, из которых система получает данные о группах пользователей.
- **Группы пользователей** — LDAP-группы, с которыми связана роль. Пользователям из этих групп доступны права этой роли.
- **Синхронизация** — тип синхронизации роли с LDAP: вручную или автоматически. Также рядом с этим столбцом отображается дата и время последней синхронизации.

Создание новой роли

☝ Для создания новой роли необходимо, чтобы у администратора в настройках роли были активированы доступы — **Учетные записи администраторов** и **Роли администраторов**.

Особенности прав доступа:

- Если администратору назначено несколько ролей, его права суммируются. Он получает доступ ко всем функциям, которые входят хотя бы в одну из ролей. Пример:

Права роли №1	Права роли №2
— просмотр отчетов, — добавление сотрудников.	— просмотр отчетов, — скачивание отчетов

Если назначить администратору обе роли, он сможет просматривать и скачивать отчеты, а также добавлять сотрудников.

- Одну роль можно назначить нескольким группам пользователей.
- Одна группа может входить сразу в несколько ролей. В этом случае права из всех ролей для этой группы суммируются.

Для создания новой роли:

1. Нажмите кнопку **Добавить**.
2. В открывшемся окне заполните следующие поля:
    - **Название*** — укажите название новой роли.
    - **Страница по умолчанию** — выберите страницу, которая будет открываться как начальная после входа в систему.
    - **Профиль LDAP** — выберите профиль LDAP, из которого система будет получать данные о группах пользователей. Если нужно добавить несколько профилей LDAP, нажмите на иконку плюса.
    - **Группы пользователей** — выберите LDAP-группы, с которыми будет связана роль.
    - **Доступы** — выберите права, которые будут доступны новой роли.
3. Нажмите кнопку **Добавить**.

    Готово! Вы создали новую роль. Назначить ее администратору можно в блоке **Учетные записи**.

Редактирование роли

Чтобы изменить параметры роли:

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

Готово! Вы изменили параметры роли.

Удаление роли

☝ Для удаления доступны созданные пользователем роли.

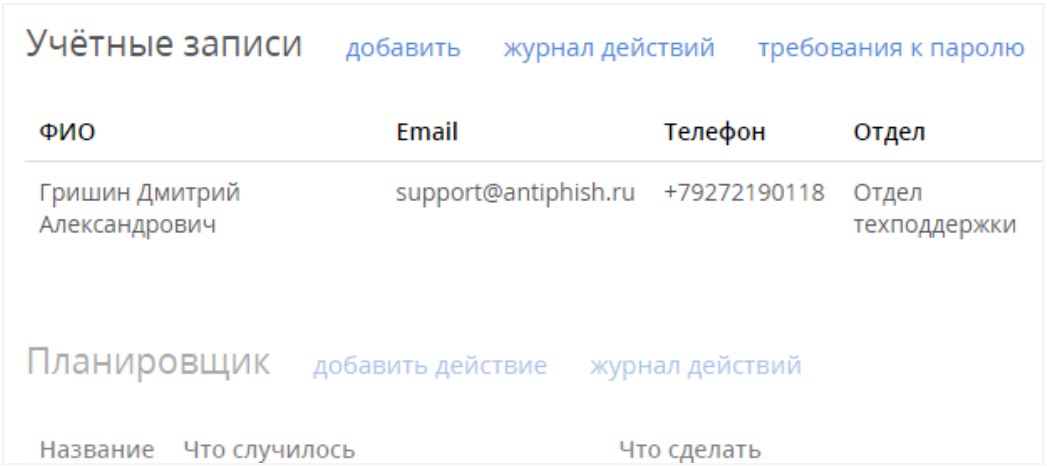
Чтобы удалить роль:

1. Наведите курсор на роль, которую нужно удалить.
2. Возле последнего столбца нажмите на значок корзины.
3. Подтвердите удаление.

    Готово! Вы удалили роль из системы.

Учетные записи

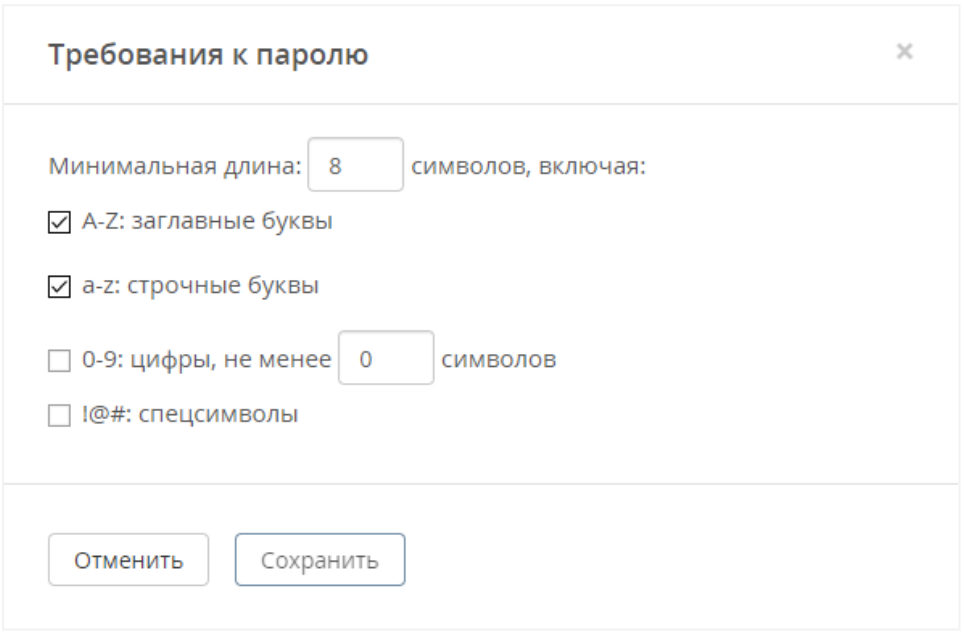
В настройках Start AWR можно создавать локальные учетные записи. Каждый администратор может работать в системе под индивидуальной учетной записью.



По всем учетным записям доступен журнал действий в системе.

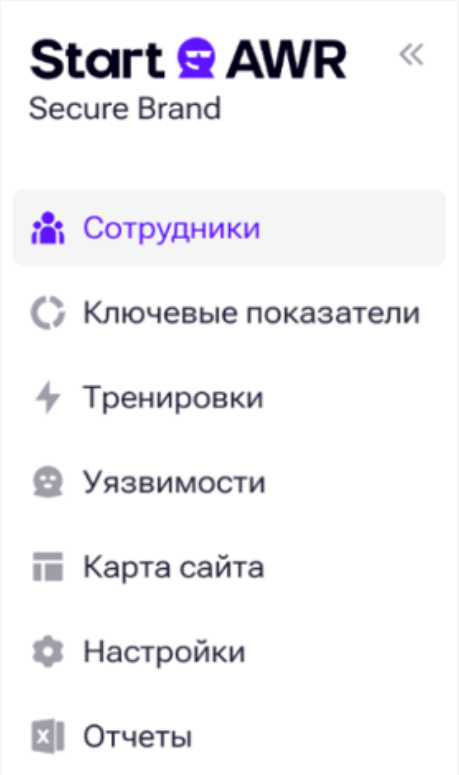
Парольная политика

Главный администратор Start AWR может устанавливать политику требований к паролям как для своей учетной записи, так и для создаваемых учетных записей локальных администраторов.



Меню для быстрой навигации

Для навигации по интерфейсу администратор всегда имеет под рукой все главные разделы:



Добавление сотрудников

Добавить сотрудников в систему можно тремя способами:

- вручную,
- через импорт из файла Excel,
- с помощью LDAP.

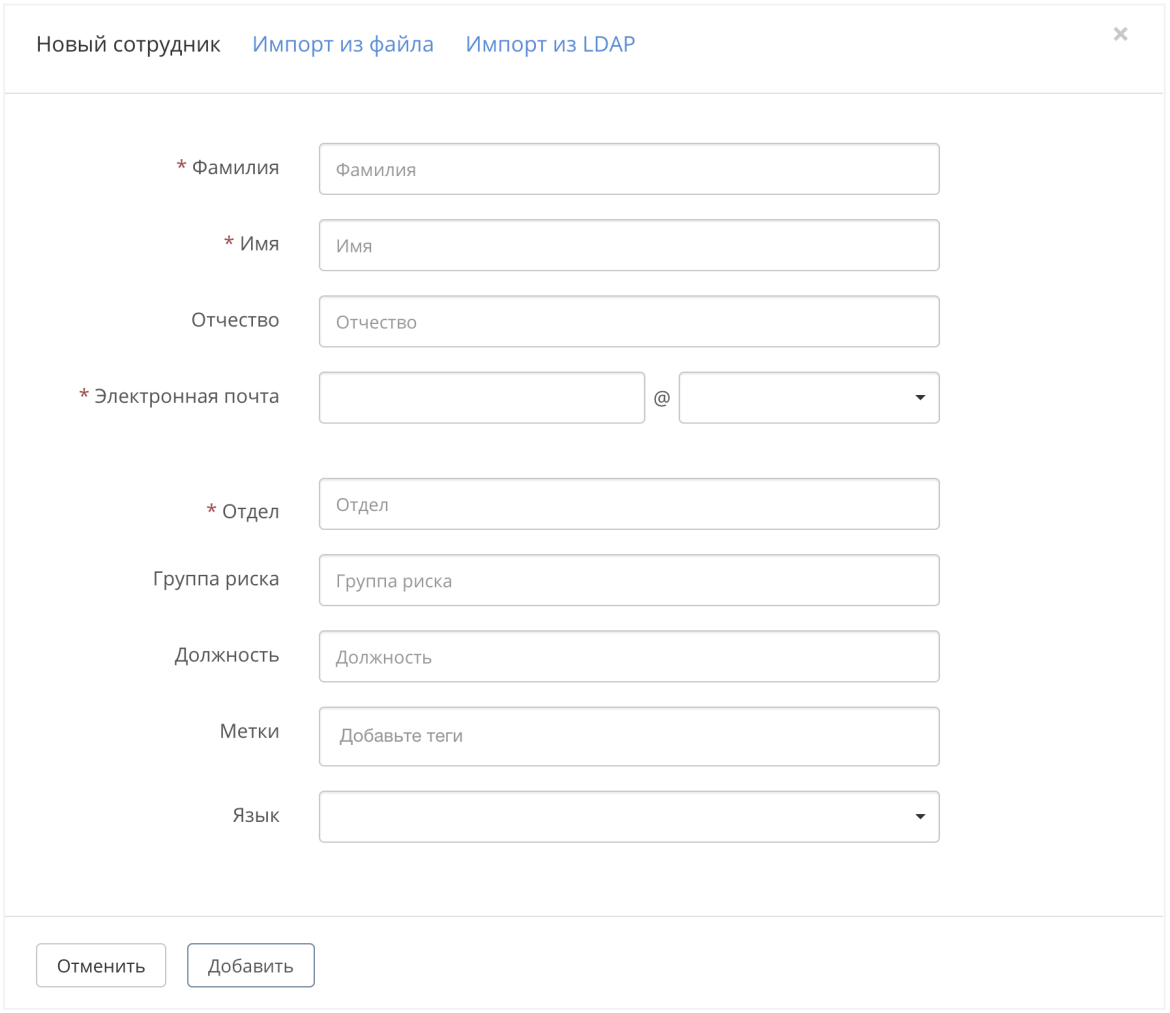
Выберите подходящий вариант в зависимости от ваших задач.

Вручную

Этот способ позволяет добавлять в систему по одному сотруднику.

1. Перейдите в **Меню** → **Сотрудники**.
2. Нажмите кнопку **Добавить сотрудников**.

3. Во вкладке **Новый сотрудник** заполните поля:



- **Фамилия***
- **Имя***
- **Отчество**
- **Электронная почта***
- **Отдел*** — если в системе нет нужного отдела, вы можете создать его, введя название нового отдела в этом поле.
- **Группа риска**
- **Должность**
- **Метки**
- **Язык**

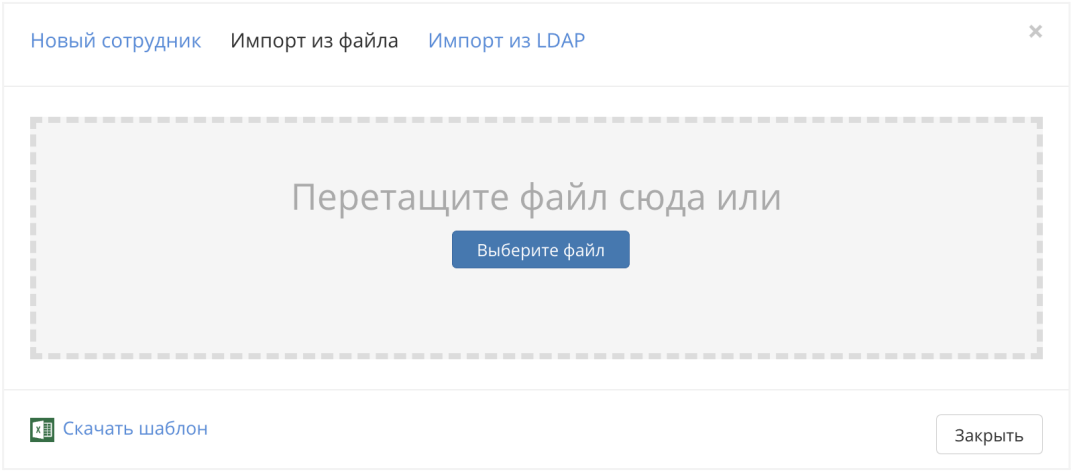
4. Нажмите кнопку **Добавить**.

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 сотрудников.

1. Перейдите в **Меню** → **Сотрудники**.
2. Нажмите кнопку **Добавить сотрудников**.
3. Выберите вкладку **Импорт из файла**.



4. Скачайте шаблон.
5. Заполните скачанный шаблон:
   - **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» — отделом второго уровня (вложенным).
   - **Метки** — укажите текстовую метку, которая поможет 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 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.

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

6. Загрузите заполненный шаблон в систему.
7. После обработки файла система покажет итоги импорта. При наличии ошибки будет указана ее причина — например, если пропущено обязательное поле. В этом случае внесите изменения в файл и загрузите его повторно.

   Готово! Вы добавили сотрудников из файла Excel в систему.

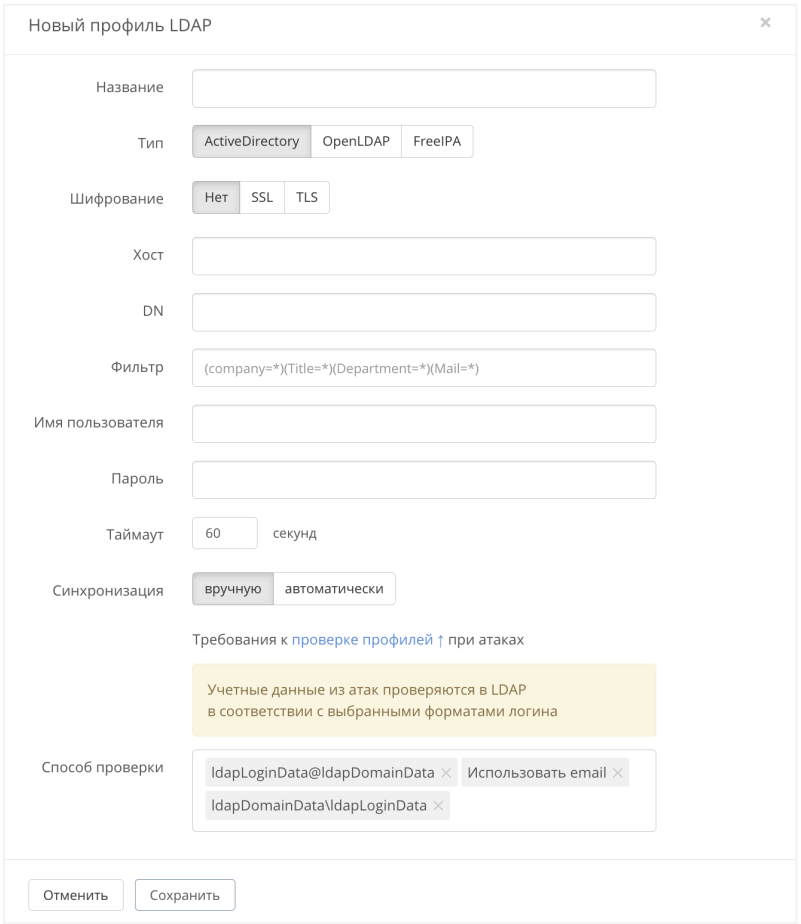
Импорт из LDAP (например, Microsoft Active Directory)

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

☝️ Рекомендуем импортировать не более 1000 сотрудников за один раз.

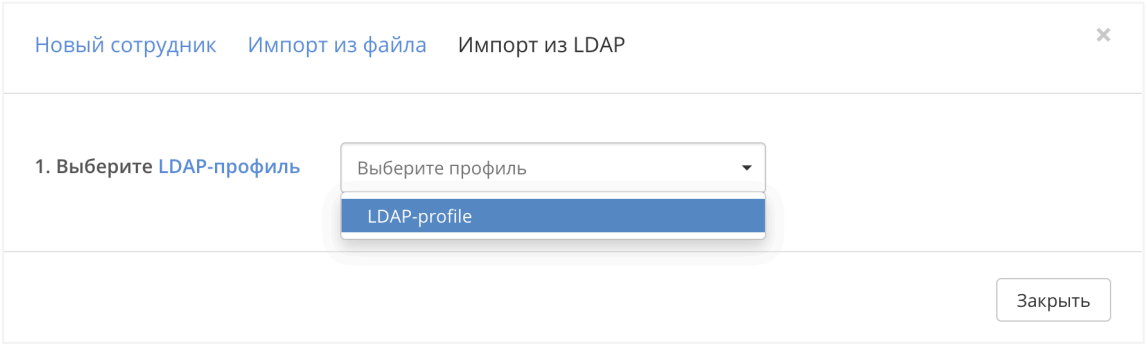
Для импорта сотрудников в систему:

1. Перейдите в **Меню → Настройки → Профили LDAP.**
2. Нажмите кнопку **Добавить**.
3. Заполните поля:



- **Название*** — укажите имя профиля LDAP для удобного поиска в системе.
- **Тип** — выберите один из вариантов: Active Directory, OpenLDAP или FreeIPA.
- **Шифрование** — выберите способ защиты соединения: нет, SSL или TLS.
- **Хост*** — 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.
  ☝ Фильтр должен соответствовать команде ldapsearch и службе каталогов, которую вы используете.
- **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.
- **Синхронизация** — выберите способ обновления данных: вручную или автоматически по расписанию.
- **Требования к проверке профилей 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.

4. Нажмите кнопку **Сохранить**.
5. Перейдите в **Меню** → **Сотрудники**.
6. Нажмите кнопку **Добавить сотрудников**.
7. Перейдите во вкладку **Импорт из LDAP**.
8. Выберите ранее добавленный LDAP-профиль.

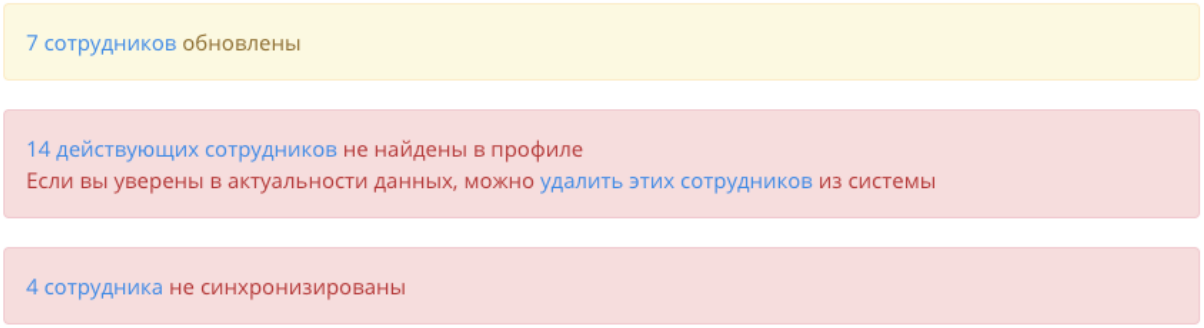


9. Заполните параметры:
   - фильтр по группам Active Directory.
   - соответствие полей определенным LDAP-атрибутам.
10. Выберите, каких сотрудников нужно импортировать — **всех** или **конкретных**.
11. Дополните информацию о сотрудниках. При необходимости укажите:

- **Метки** — текстовые метки, которые помогут сгруппировать сотрудников по каким-либо признакам. Например: «На удаленке», «Офис Москва», «Стажировка».
- **Язык** — на выбранном языке сотрудники будут получать уведомления, курсы и сертификаты об обучении.
- **Группу риска** — если нужной группы нет, введите название новой группы в этом поле. Она появится в системе после сохранения настроек импорта.

12. Нажмите кнопку **Сохранить настройки импорта**.

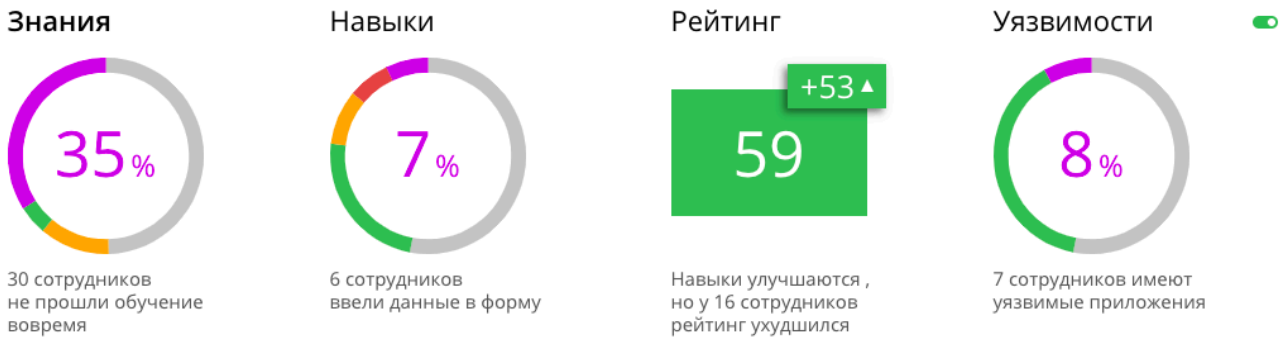
Готово! После завершения синхронизации система покажет итоги импорта по всем сотрудникам.



☝ 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.

Дашборд

Помогает видеть текущий уровень знаний, навыков, рейтинг и уязвимости сотрудников. С помощью него удобно отслеживать прогресс в обучении и тренировках. Состоит дашборд из нескольких диаграмм:



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, кто входит в сектор — кликните на него и нажмите на ссылку с количеством сотрудников под диаграммой. Откроется список, в котором можно использовать фильтры, чтобы искать определенные группы сотрудников. Например, вы можете отобрать только тех, кто работает в финансовом отделе, чтобы посмотреть информацию только о них.

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 сиреневый сектор.

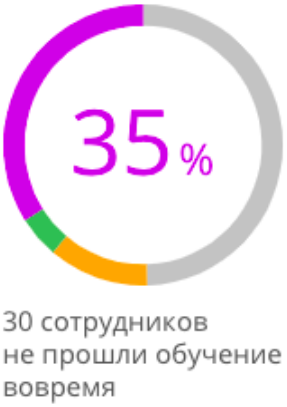


Диаграмма делится на следующие секторы:

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.

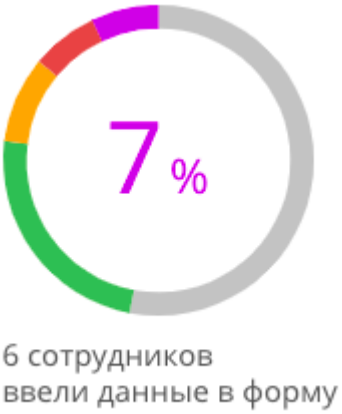
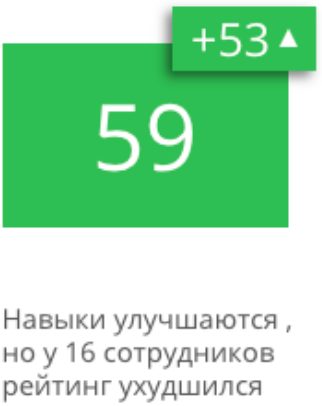


Диаграмма делится на следующие секторы:

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



Уязвимости

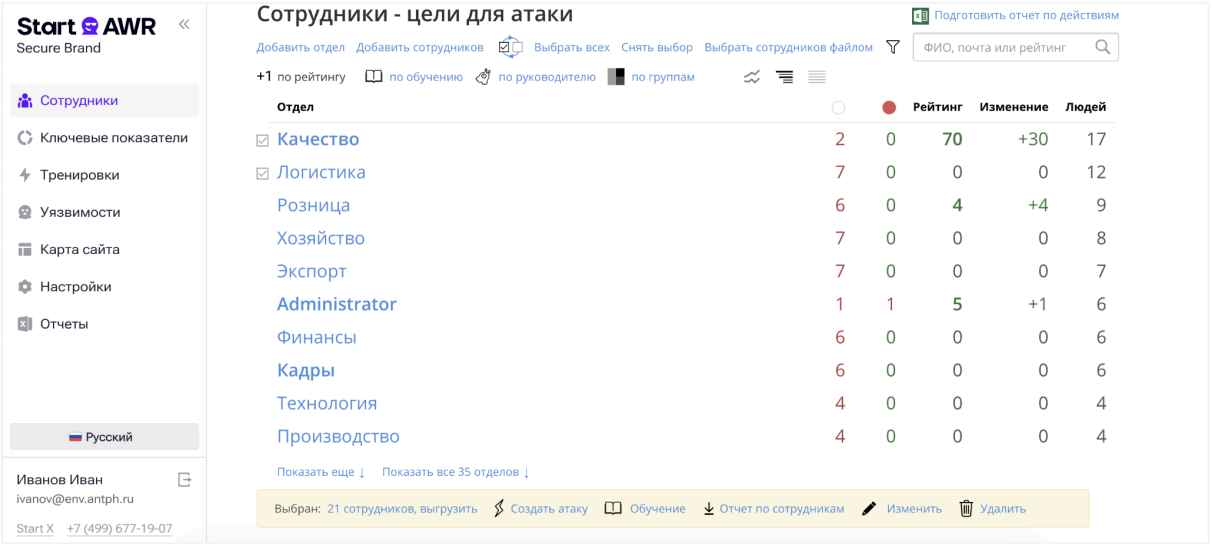
Диаграмма показывает статистику о программных уязвимостях, которые были найдены у сотрудников, когда они совершали небезопасные действия в имитированных атаках.

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».

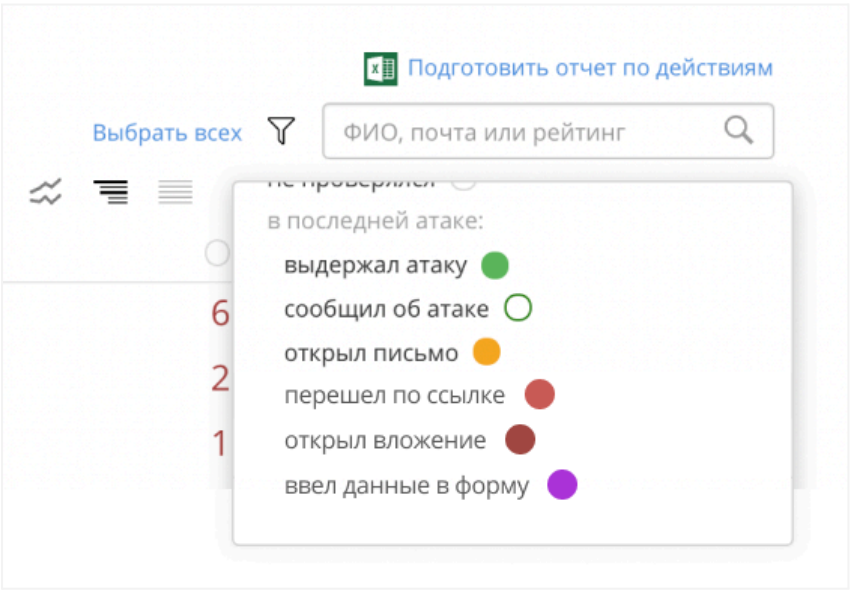
Работа со списком сотрудников

Список сотрудников доступен в разделе **Знания**.



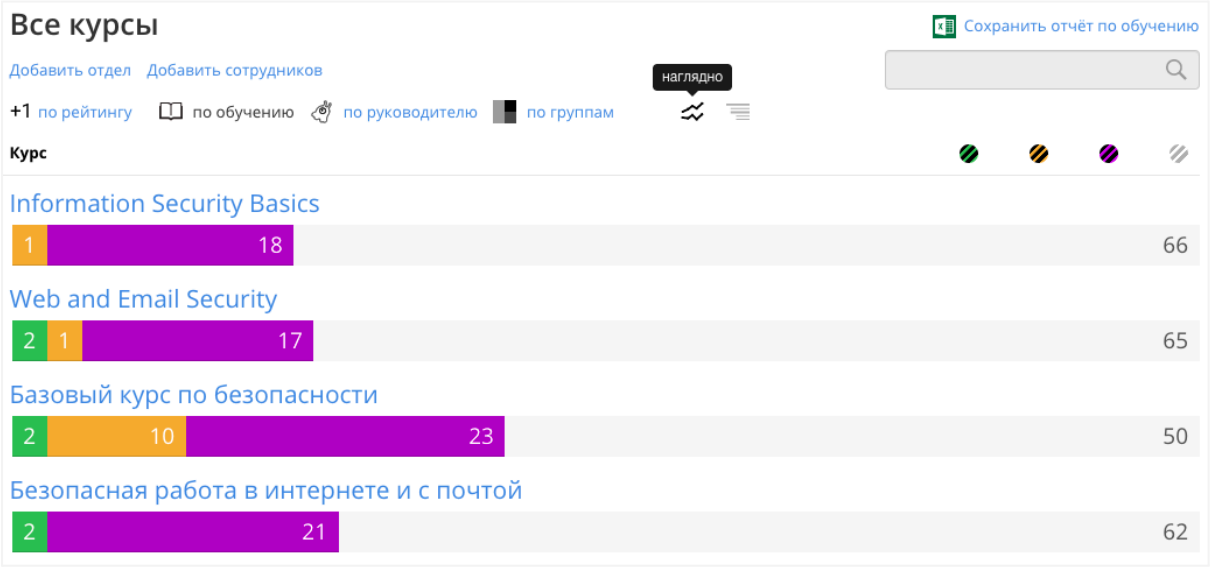
В нем можно использовать поиск по ФИО, почте или рейтингу, и фильтры для быстрого выбора сотрудников:

- по результатам атак,
- по результатам обучения,
- по изменению рейтинга,
- по наличию уязвимостей и другим состояниям.

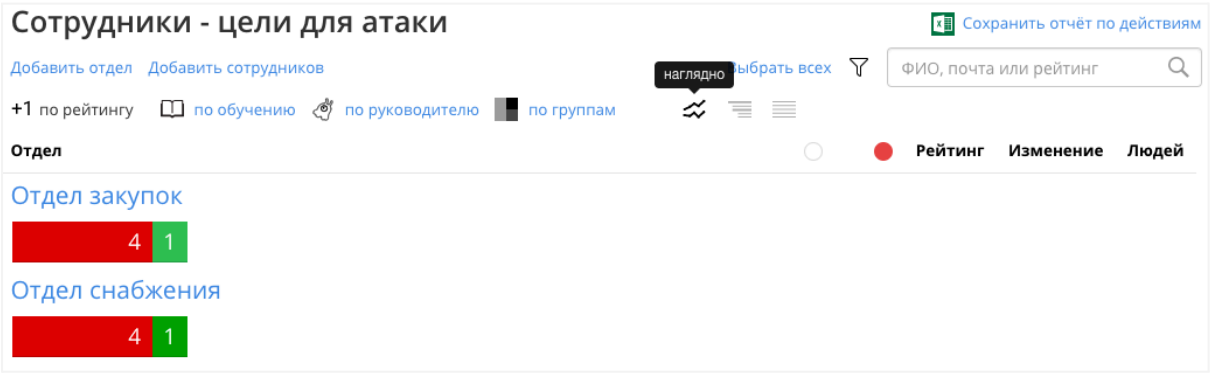


Наглядная статистика позволяет быстро оценить эффект от обучения и тренировки навыков, чтобы принять решение о дальнейших действиях в отношении сотрудников.

Представление по знаниям сотрудников:



Представление по навыкам сотрудников:

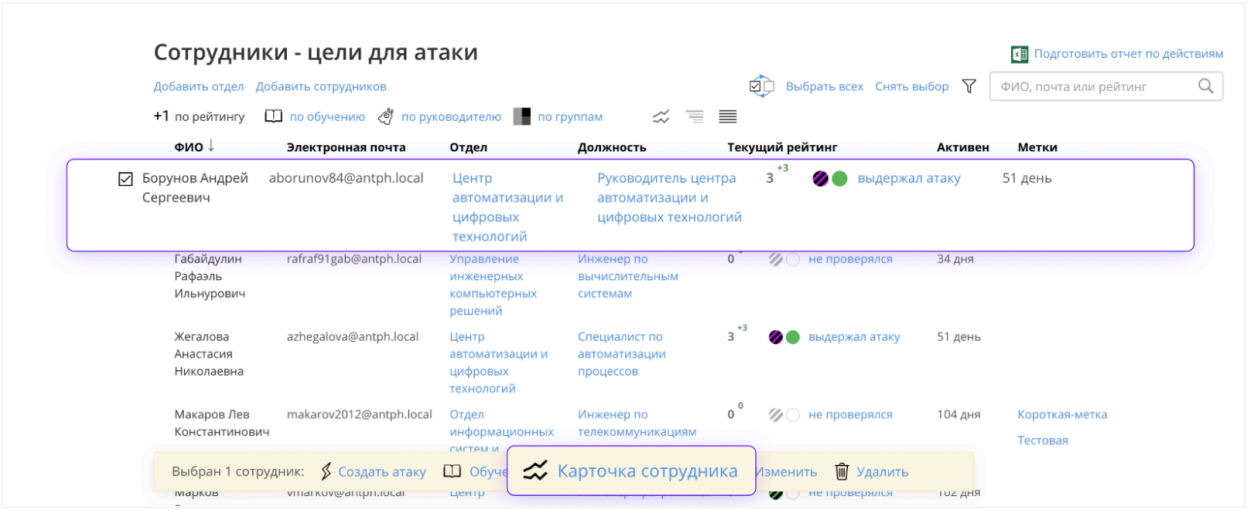


Карточка сотрудника

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, выберите его в списке и в контекстом меню нажмите **Карточка сотрудника**.



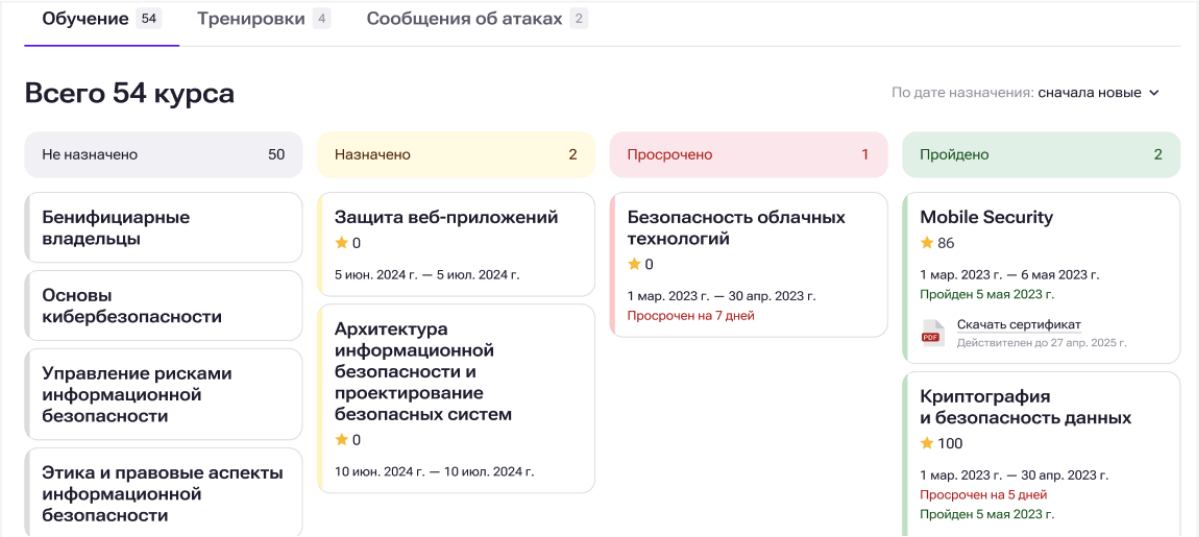
Общие сведения

На странице отображаются:

- **Статус сотрудника** — статус сотрудника в системе.
- **Рейтинг по атакам** — текущий рейтинг и динамика сотрудника. Рейтинг растет, 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 присвоены сотруднику.

Вкладка «Обучение»

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



При необходимости отсортируйте все курсы по дате назначения.

В этом разделе отображаются курсы с разделением по статусам:

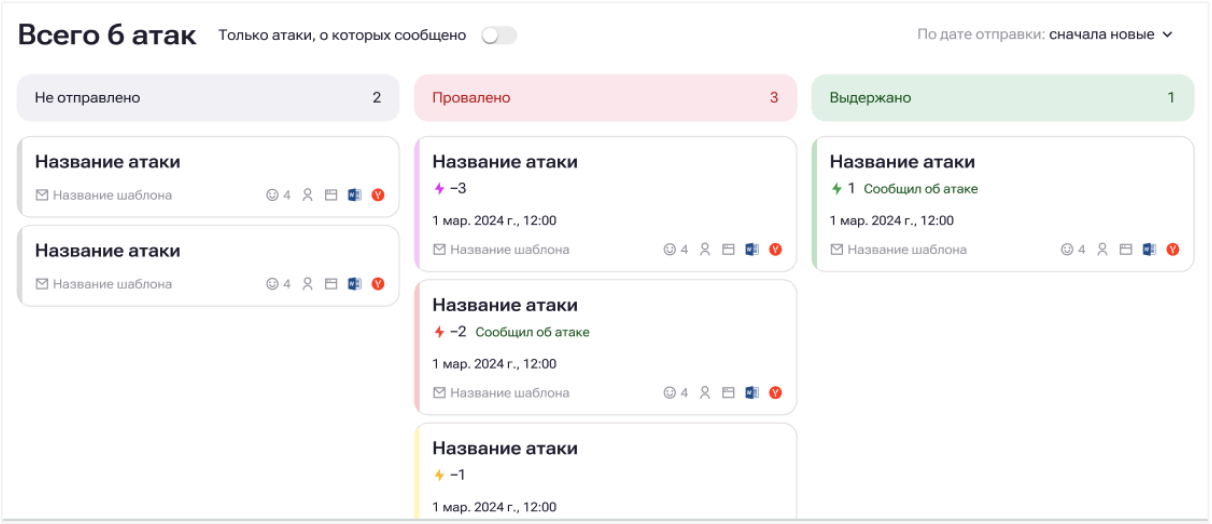
Статус обучения	**Какие курсы отображаются в столбце**	**Что отображается в карточке курса**
Не назначено	Курсы, которые еще не назначены сотруднику.	— Название курса.
Назначено	Назначенные на сотрудника курсы или те курсы, которые он начал проходить.	— Название курса. — Баллы, набранные в последней 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.



Здесь отображаются атаки с разделением по статусам:

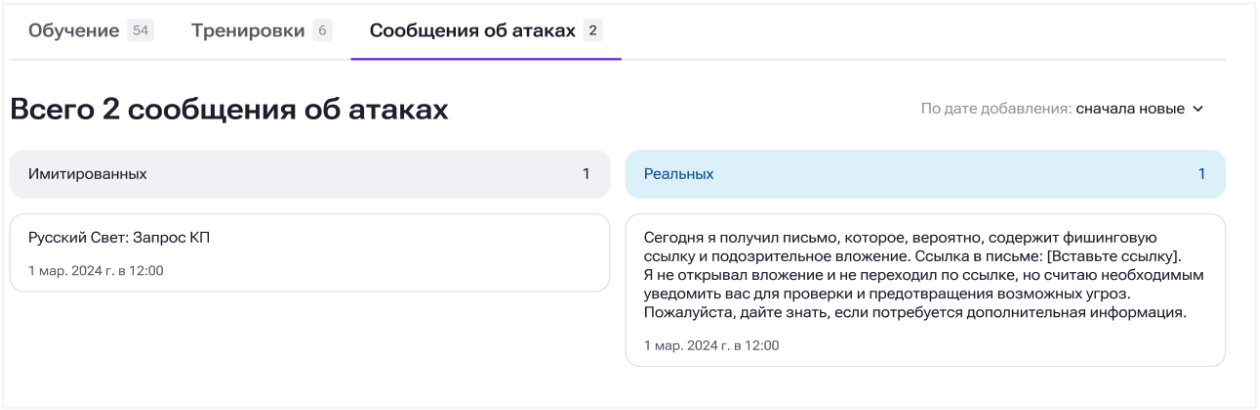
Статус атак	**Какие атаки отображаются в столбце**	**Что отображается в карточке атаки**
Не отправлено	Атака, которую еще не назначили сотруднику.	— Название атаки. — Название шаблона. — Психологические векторы атаки. — Тип сообщения — Ссылка на финальную страницу — Тип файла во вложении. — Название фишинговой страницы. — Название финальной страницы.
Провалено	Атака, в которой сотрудник совершил опасное	— Название атаки. — На сколько изменился рейтинг после

	действие. Например, перешел по ссылке или открыл вложение.	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.



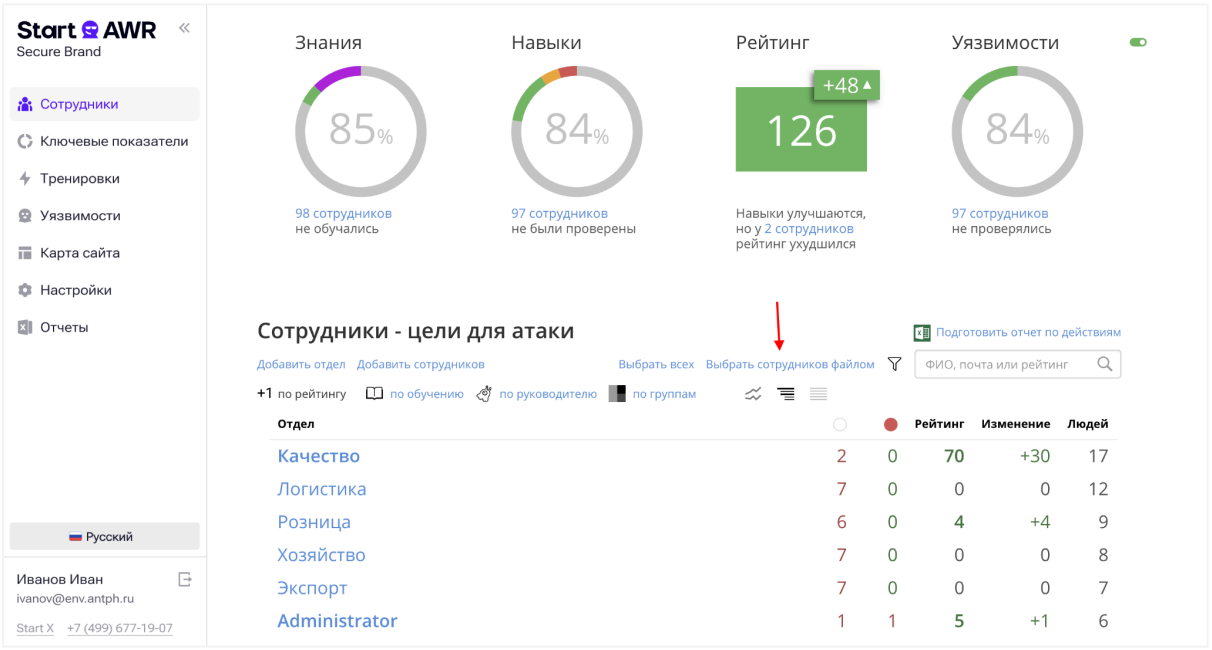
Выделение группы сотрудников через импорт файла со списком

Чтобы упростить поиск сотрудников и не искать каждого вручную, вы можете загрузить файл со списком сотрудников, и система выделит всех, кто в нем есть. Этот способ будет полезен, если нужно выполнить какие-либо действия с большим количеством сотрудников, например:

- Отредактировать сведения о них — отдел, группу, должность или другие данные.
- Создать имитированную атаку.
- Назначить обучение.
- Сформировать отчет.

Для выделения группы сотрудников через импорт файла со списком:

1. Перейдите в **Меню** → **Сотрудники** и нажмите **Выбрать сотрудников файлом.**



2. Скачайте шаблон и заполните его.
3. Нажмите **Выберите файл** и загрузите заполненный шаблон в систему.

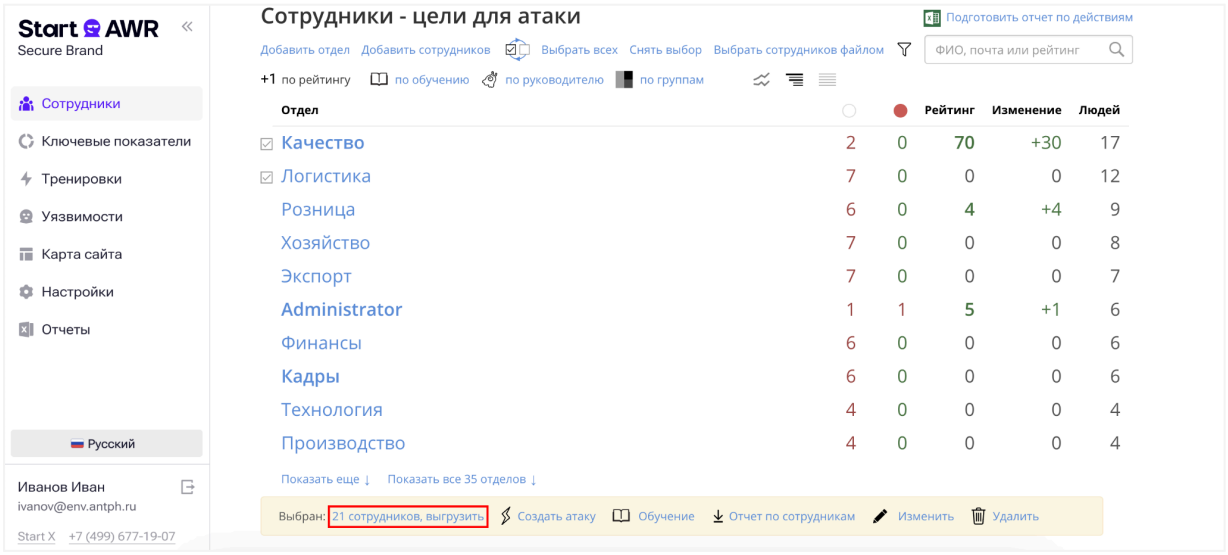
   Готово! Система выделит в списке сотрудников, которые есть в файле.

Выгрузка сотрудников в файл Excel

Выгрузка сотрудников в файл Excel позволяет скачать список сотрудников из системы. Это удобно, если нужно внести массовые правки — например, в персональные данные сотрудников. После редактирования файл можно загрузить обратно через импорт, и все изменения отобразятся в системе.

☝ Для выгрузки списка в настройках роли администратора должен быть разрешен доступ к сотрудникам.

Чтобы скачать список с данными сотрудников, отметьте нужных сотрудников и нажмите **Выгрузить** на нижней панели.



Проверка и тренировка навыков

Навыки в системе можно проверять и тренировать через имитированные атаки по нескольким технологическим векторам:

Электронная почта

- Открытие потенциально опасных электронных писем.
- Переходы по ссылкам в письмах.
- Открытие вложенных файлов в письмах.

Сайты

- Заполнение и отправка данных на мошеннических (фишинговых) сайтах.
- Загрузка и установка вредоносных браузерных расширений.
- Загрузка и запуск потенциально вредоносных исполняемых файлов.
- Сбор данных об установленных программах и их версиях.

Офис, рабочие помещения

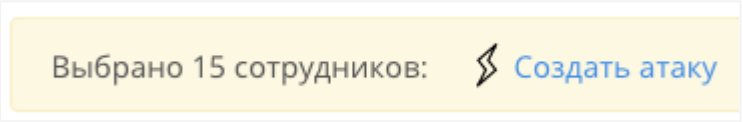
- Подключение недоверенных съемных устройств в рабочий компьютер.
- Подключение к недоверенным Wi-Fi сетям.

Подробнее по ссылке [Start AWR — Классификация цифровых атак на сотрудников]

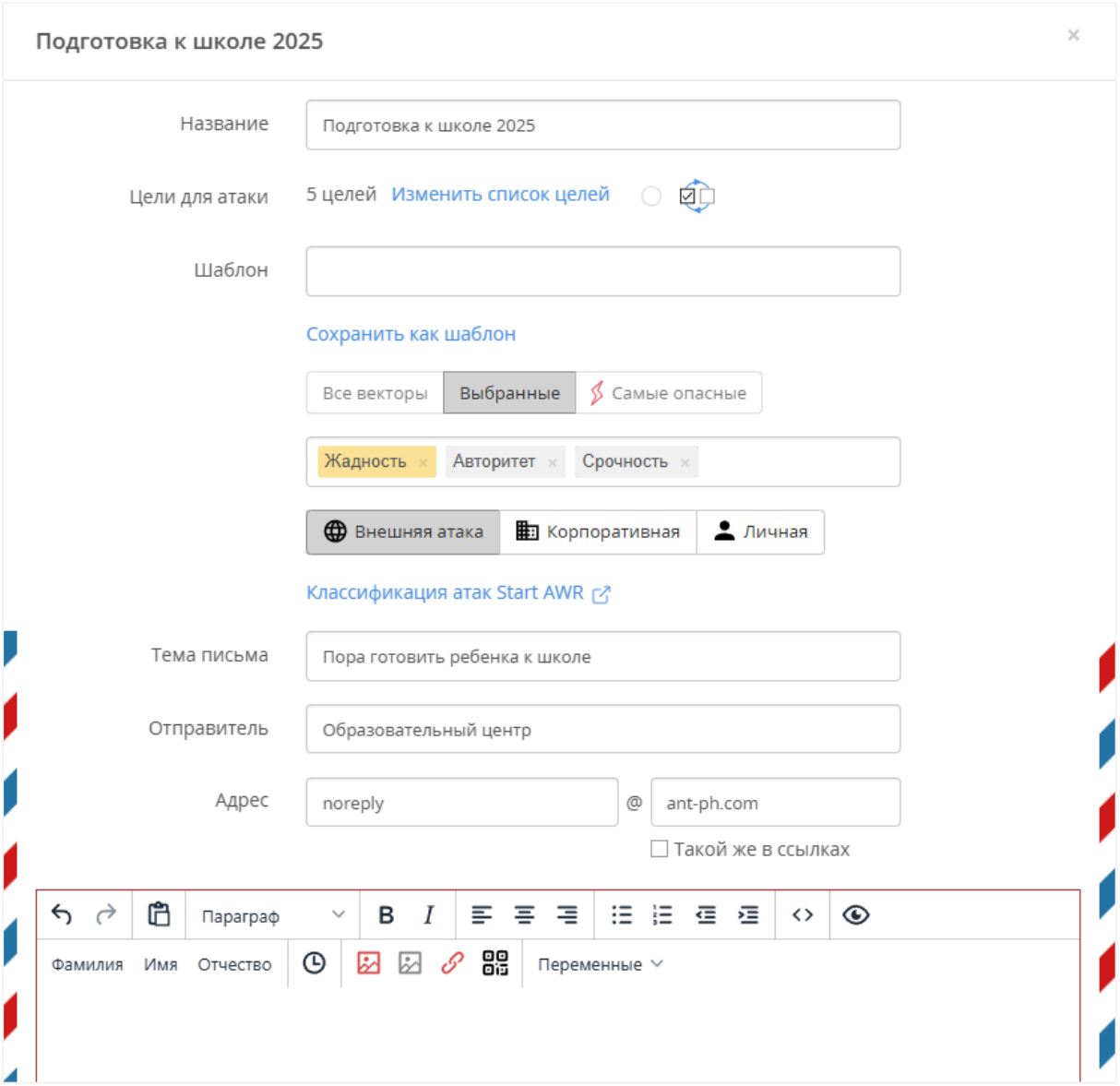
Атаки по электронной почте

Для создания имитированной атаки:

1. Перейдите в **Меню** → **Сотрудники**.
2. Выделите в списке сотрудников, которым нужно отправить атаку.
3. В нижней части экрана появится панель. Нажмите на ней **Создать атаку**.



4. Укажите название атаки. Это нужно для внутреннего поиска в системе. Получатели атаки его не увидят.



5. При необходимости измените список сотрудников, которым отправится имитированная атака.
6. Выберите готовый шаблон письма или создайте свой.
7. Укажите тему письма.
8. Укажите имя отправителя, которое сотрудники увидят в поле «От кого».

9. Введите адрес отправителя, от которого придет письмо.
10. При необходимости:
    - отредактируйте шаблон,
    - добавьте ссылку в виде QR-кода.
    - прикрепите файлы: запакованные в zip-архив, zip с паролем, ISO, LNK файлы.
    - добавьте ссылку в письмо,
    - выберите фишинговую страницу, которая имитирует реальный сайт, и на которую сотрудник будет перенаправлен при переходе по ссылке из письма.
    - укажите финальную страницу, на которую сотрудники будут перенаправлены после действий на фишинговых страницах или сразу при переходе по ссылкам.
11. Нажмите кнопку **Сохранить**.

Готово! Вы создали имитированную атаку. Созданную атаку можно сохранить и запустить сразу, либо запланировать на любой день и время.

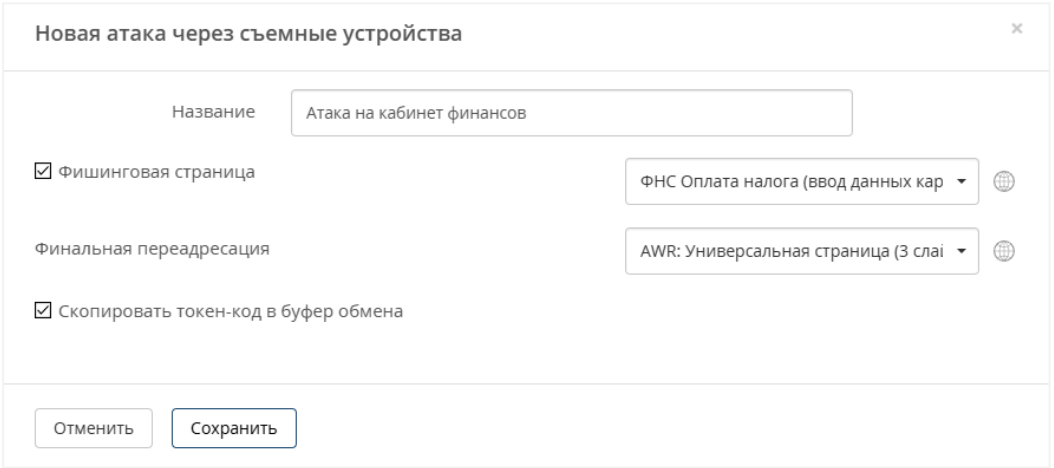
☝ Изменять параметры атаки можно в любое время, но до первого запуска. Параметры запущенной атаки изменять нельзя — это может привести к некорректному сравнению статистики поведения сотрудников в разных запусках.

Атаки через съемные устройства

Атаки через съемные устройства помогут имитировать и отслеживать статистику по подключению недоверенных USB-устройств.

Для создания имитированной атаки:

1. Перейдите в **Меню** → **Сотрудники** → **Навыки** → **Съемные устройства**.
2. Нажмите **Создать атаку**.
3. Укажите параметры атаки.



4. Нажмите кнопку **Сохранить.**

В результате будет создан уникальный токен-код. Его нужно передать специалисту, который будет прошивать устройство.

Специалист изготавливает и программирует с использованием токен-кода необходимое количество USB-устройств, которые затем могут быть оставлены в любых помещениях, где бывают сотрудники.

Технически каждое такое устройство является USB-клавиатурой.

При подключении к компьютеру оно инициирует открытие браузера и ввод детектирующего URL с заранее определенным токен-кодом, например: https://attack.antiphish.ru/payload/openUsb?computername=win10&token=ya4g4kerd&userdomain=domain&username=test

По атакам, в которых были зафиксированы подключения USB-устройств, отобразится статистика:

- Дата и время подключения.
- Домен и имя рабочей станции.
- Имя пользователя.
- Операционная система.

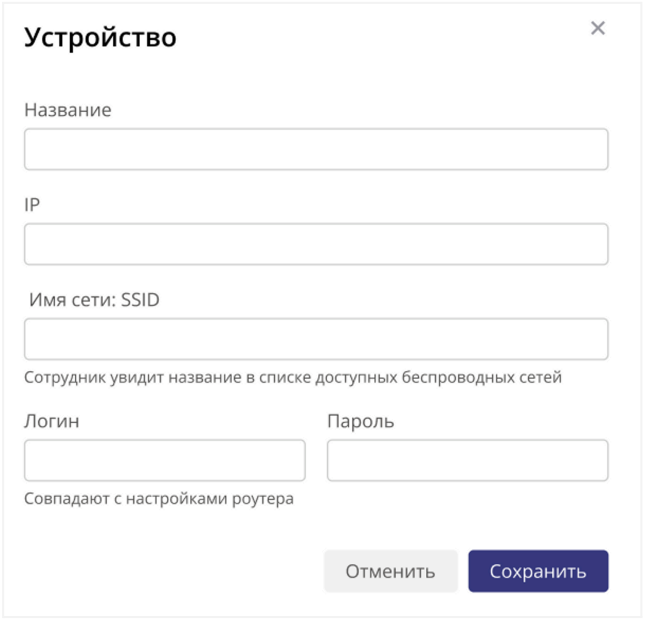
Атаки через беспроводные сети

Атаки через беспроводные поддельные точки доступа помогут имитировать небезопасные Wi-Fi сети, тем самым обучая сотрудников оценивать угрозу использования бесплатных Wi-Fi сетей.

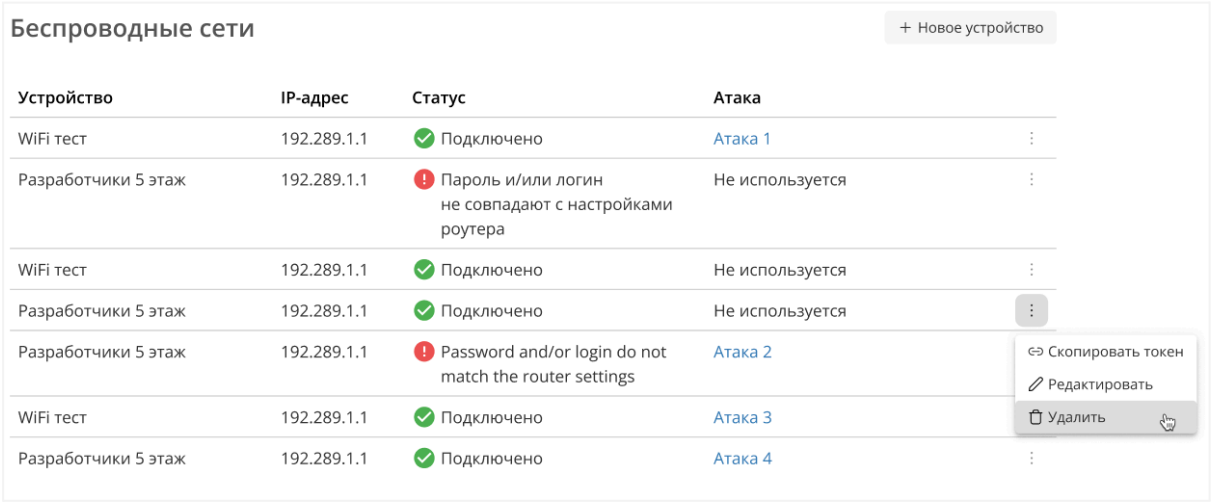
Для создания имитированной атаки:

1. Перейдите в **Меню** → **Настройки** → **Беспроводные сети**.

2. Добавьте новое устройство.

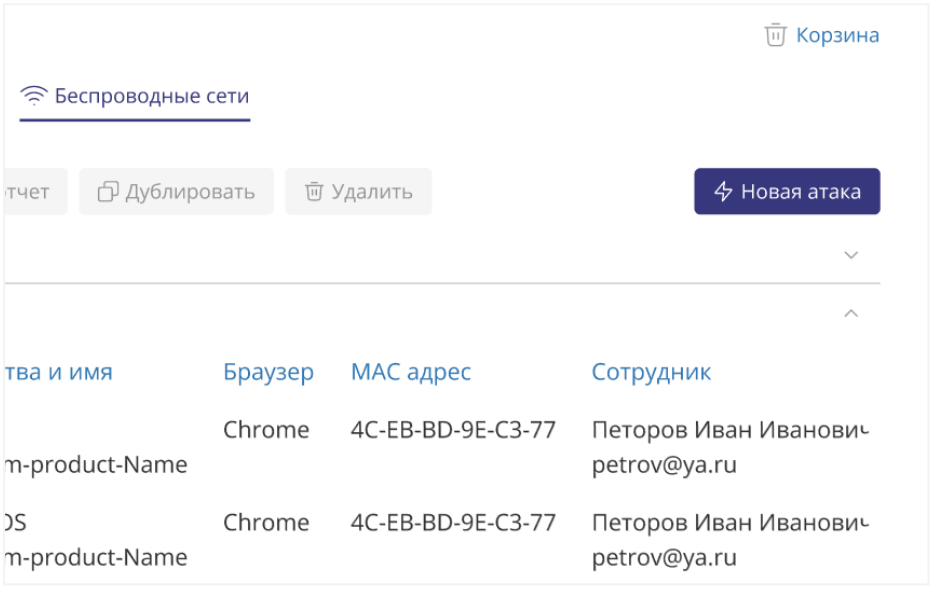


3. В результате будет добавлено беспроводное устройство. Система проверит подключение и отобразит в его списке устройств с соответствующим статусом.

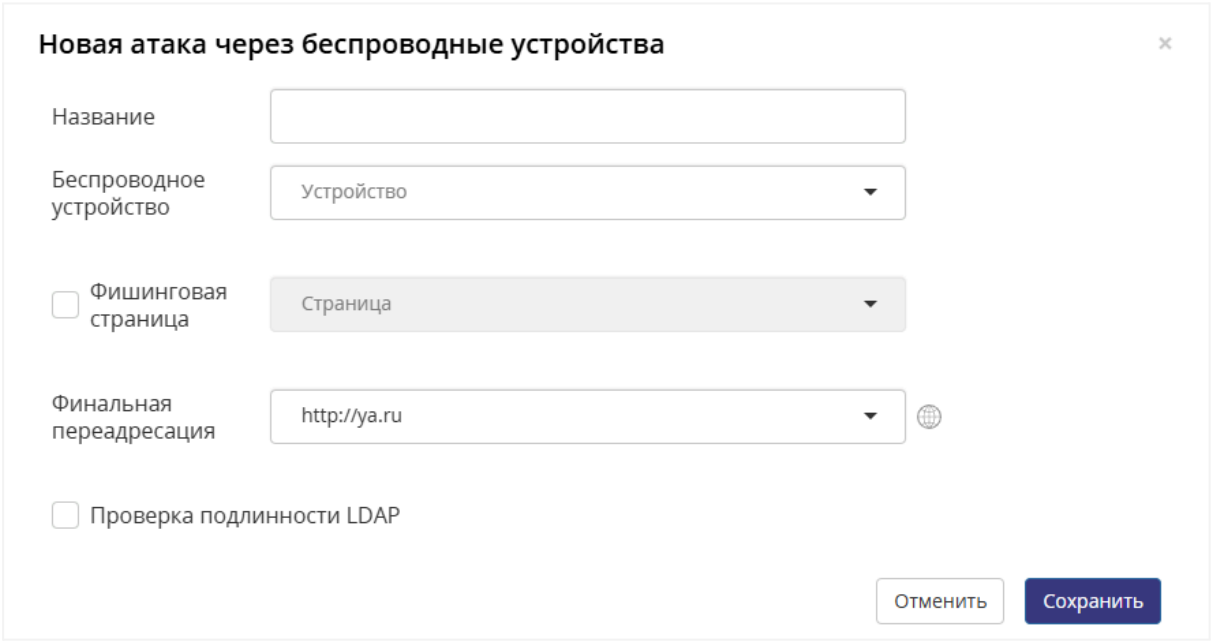


4. Для создания атаки перейдите в **Меню** → **Настройки** → **Навыки** → **Беспроводные сети**.

5. Нажмите кнопку **Новая атака**.



6. Укажите параметры атаки.

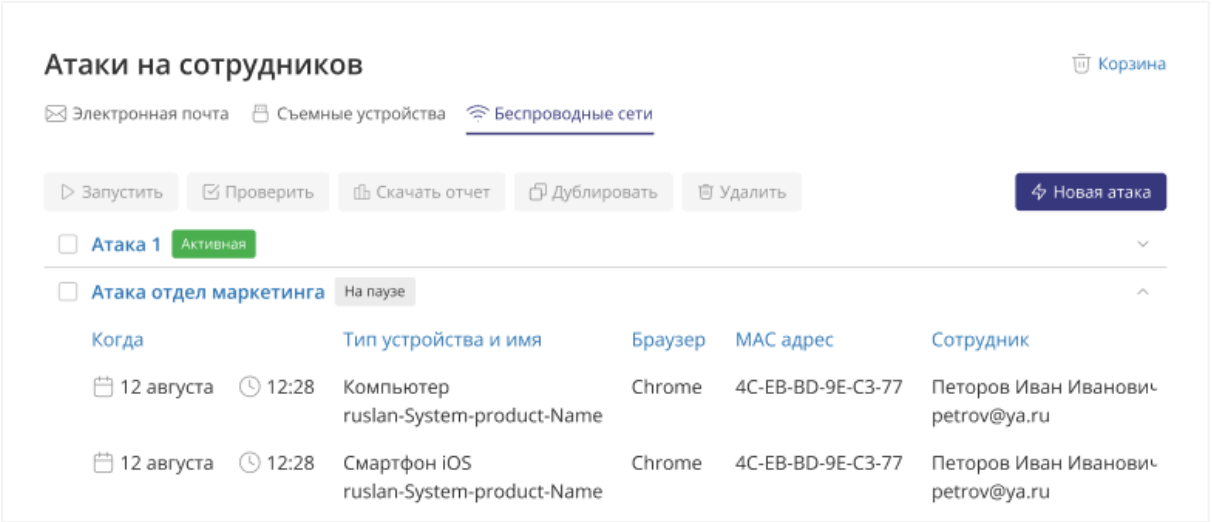


7. Нажмите кнопку **Сохранить**.

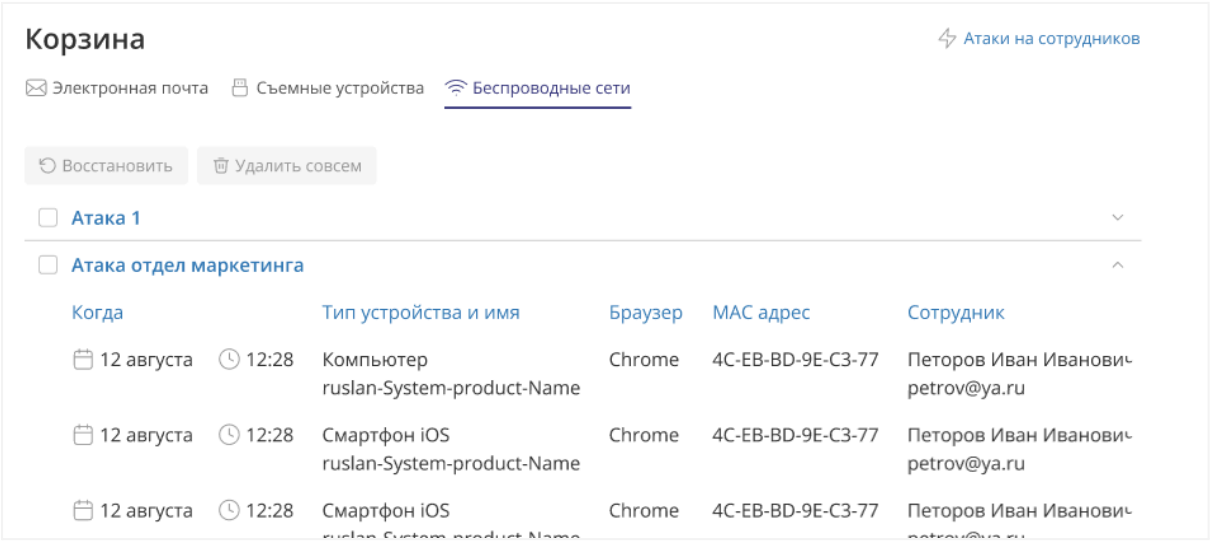
Готово! Вы создали имитированную атаку. Созданную атаку можно сохранить и запустить сразу, либо запланировать на любой день и время.

☝ Изменять параметры атаки можно в любое время, но до первого запуска.
После сохранения атаки система отображает ее статус как «Новая», после дальнейших действий с ней ее статус может меняться на «Активная» или «Остановленная».
Сохраненную атаку можно запустить сразу или в другое время.

Администратор может посмотреть статистику по подключениям в атаке, развернув пункт с нужной атакой. Также при необходимости можно скачать подробный отчет по атакам.



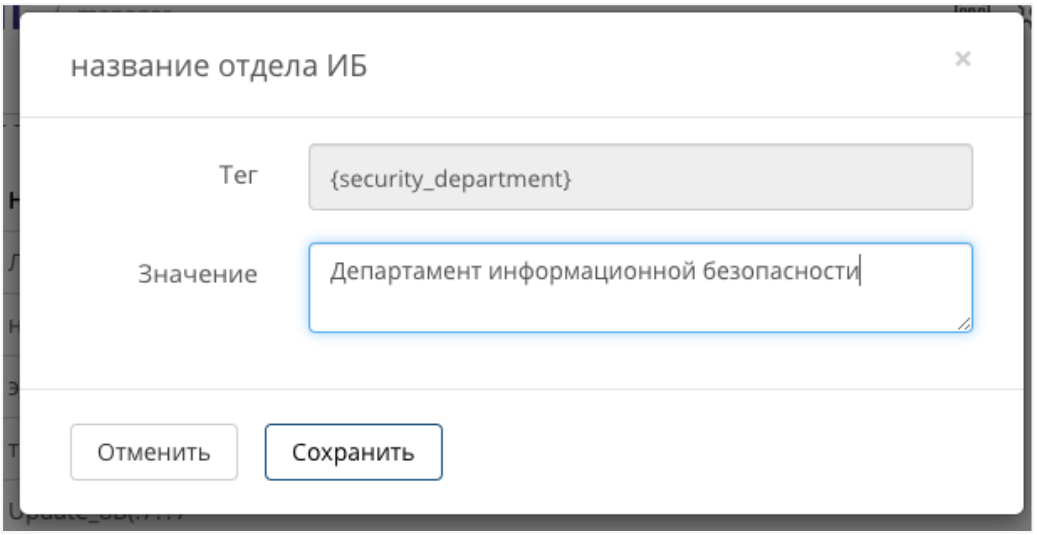
Администратор может удалить атаку, после чего она будет отображаться в разделе «Корзина», откуда ее можно восстановить или удалить навсегда, при этом статистика по ней сохранится.



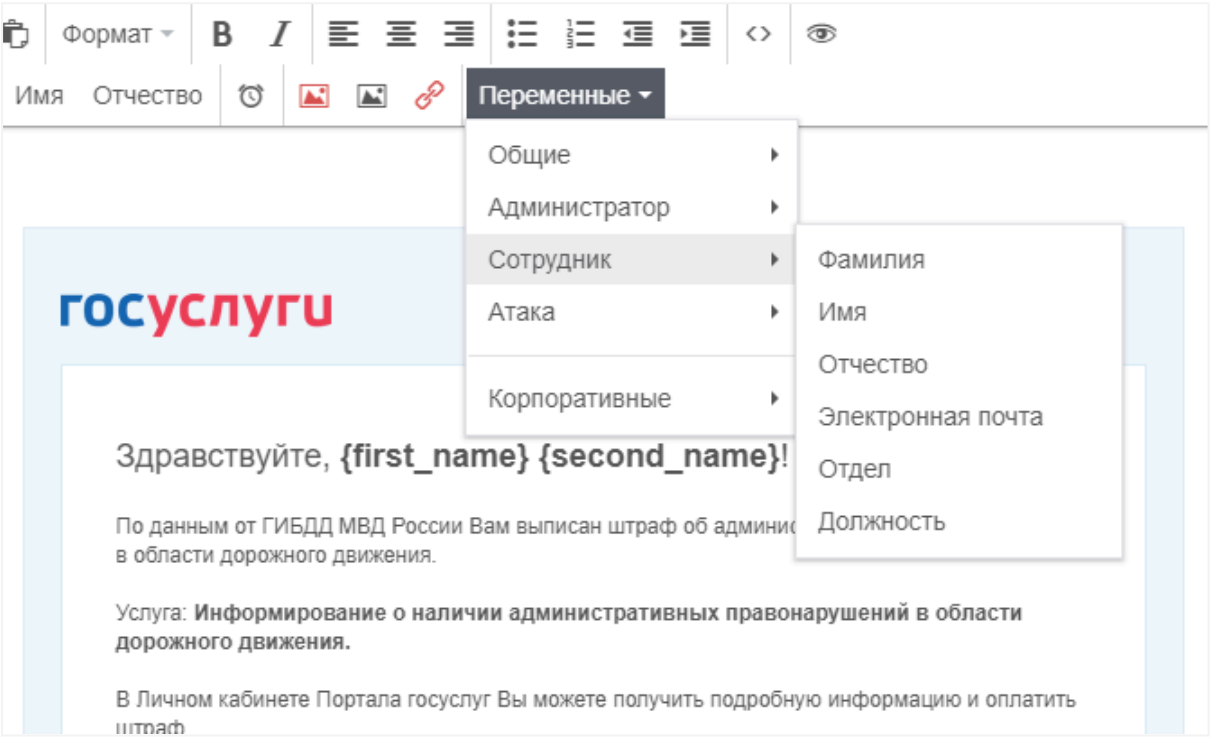
Целевые атаки с использованием переменных

В шаблоне атаки, на фишинговой и финальной странице можно использовать переменные, которые будут автоматически заполнены при исполнении атаки по данным конечного пользователя или другим, в соответствии со значением переменной. Это позволяет создавать еще более эффективные, персонифицированные и актуальные целевые атаки:

Для того чтобы задать или изменить значение пользовательских переменных, необходимо перейти в раздел **Настройки** → **Переменные**, нажать на выбранную переменную и в модальном окне указать значение.



При использовании в атаке переменные можно выбирать из меню редактора и использовать в любой части шаблона.



Контроль защищенности сотрудников

Ключевые показатели защищенности всегда доступны на дашборде. Его подробное описание можно изучить в разделе Дашборд.

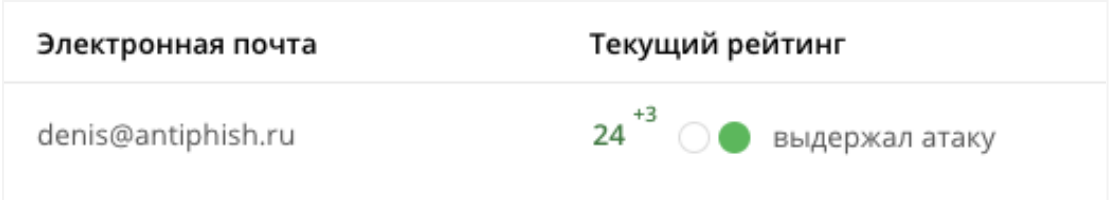
Статистику поведения сотрудников можно увидеть в разделе **Рейтинг** → **Отчеты** с группировкой по отделам и выполненным атакам. Вы увидите, как действовали сотрудники — кто именно и когда открывал имитированные фишинговые письма, переходил по ссылкам или открывал вложения.

Любые отчеты и статистику можно сохранить в формате файла Excel.

Рейтинг сотрудников

Представление данных

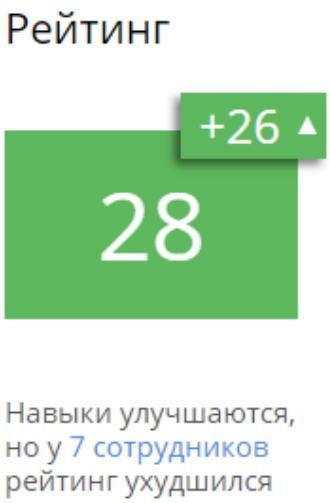
В результате каждого действия по каждой имитированной атаке у сотрудника накапливается рейтинг — число, означающее одновременно его опыт и общий уровень защищенности:



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

Степень в рейтинге и комментарий означают последние изменения: насколько ухудшилось или улучшилось поведение сотрудника, и что именно он сделал в последней имитированной атаке.

Общий рейтинг и его изменение по всем сотрудникам является ключевым показателем защищенности и отображается на главной странице.



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.

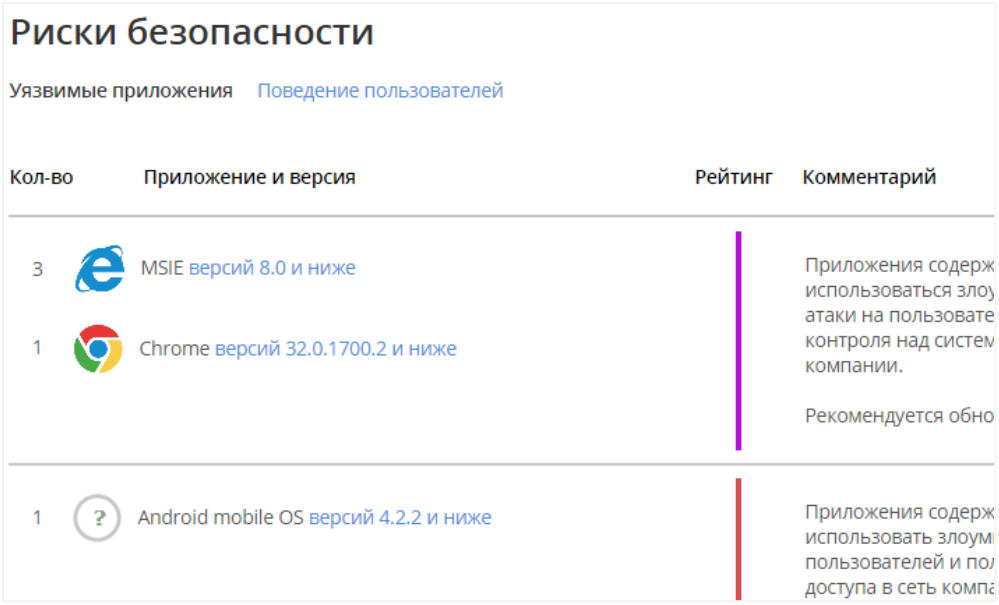
Если человек выдержал атаку, т.е. не совершил ни одного опасного действия, ему присваивается статус «Выдержал атаку» и максимально возможный положительный рейтинг по данной атаке. Например, если атака содержала ссылку и вложение, сотруднику присваивается рейтинг +3 за атаку — он не открыл письмо, не 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 продемонстрировали небезопасное поведение — открывали имитированные фишинговые письма, переходили по ссылкам или открывали вложения, Start AWR определяет версии браузеров, плагинов, офисных программ и операционных систем.



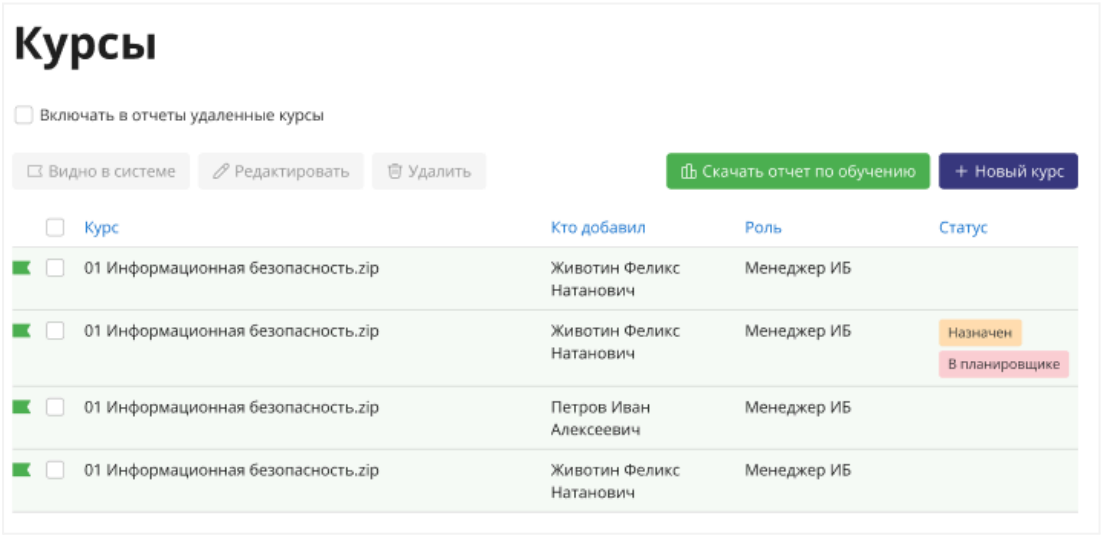
Уязвимости в этих версиях считаются дополнительным риском безопасности, и классифицируются в зависимости от рейтинга уязвимости (CVSS Score). Статистика по таким рискам доступна в отдельном разделе, с группировкой по приложениям и сотрудникам.

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

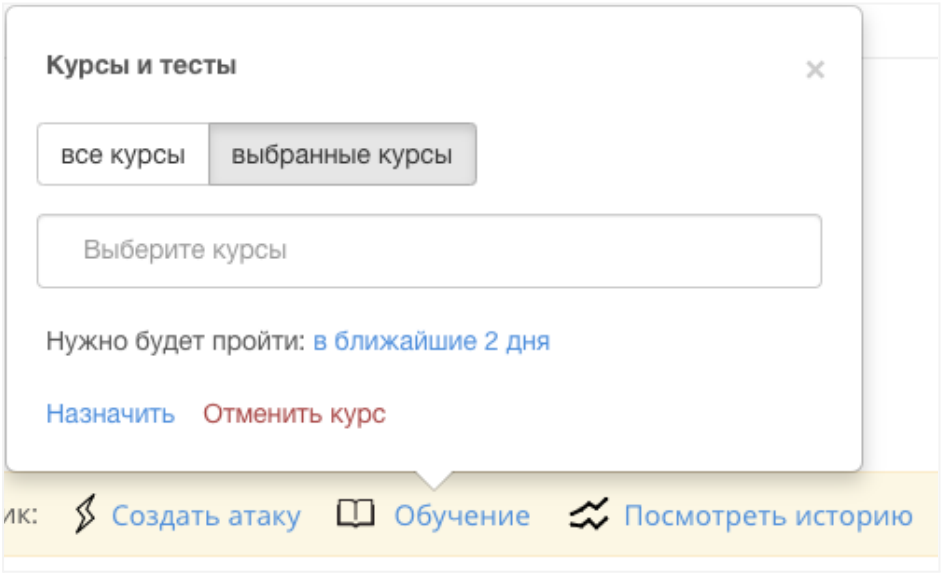
Уязвимости, которые были устранены на рабочем месте сотрудника или определены как ложное срабатывание, можно исключить из статистики Start AWR.

Обучение сотрудников

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



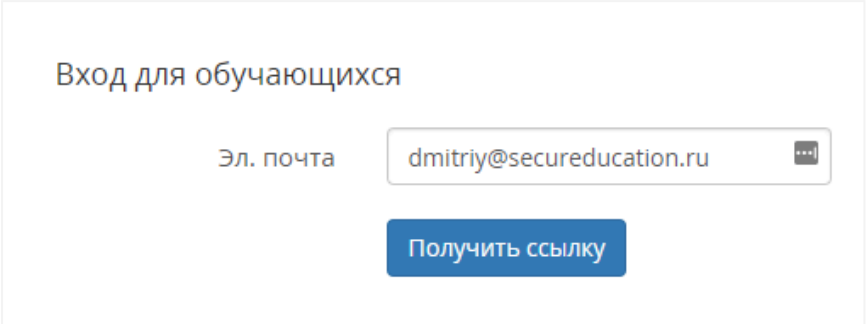
Из интерфейса можно выбрать сотрудников и отправлять их на один или несколько курсов.



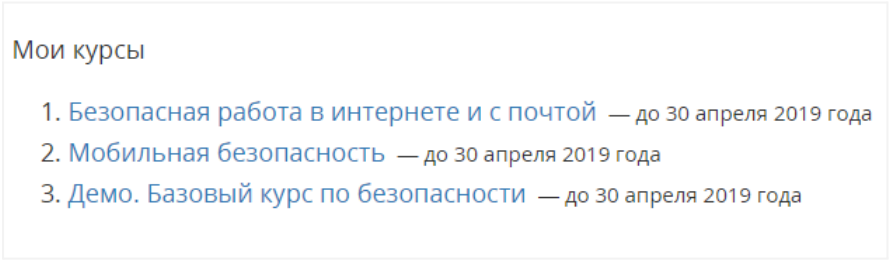
Для автоматизации этих процессов рекомендуем использовать планировщик. Подробнее о нем в разделе Планировщик.

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.

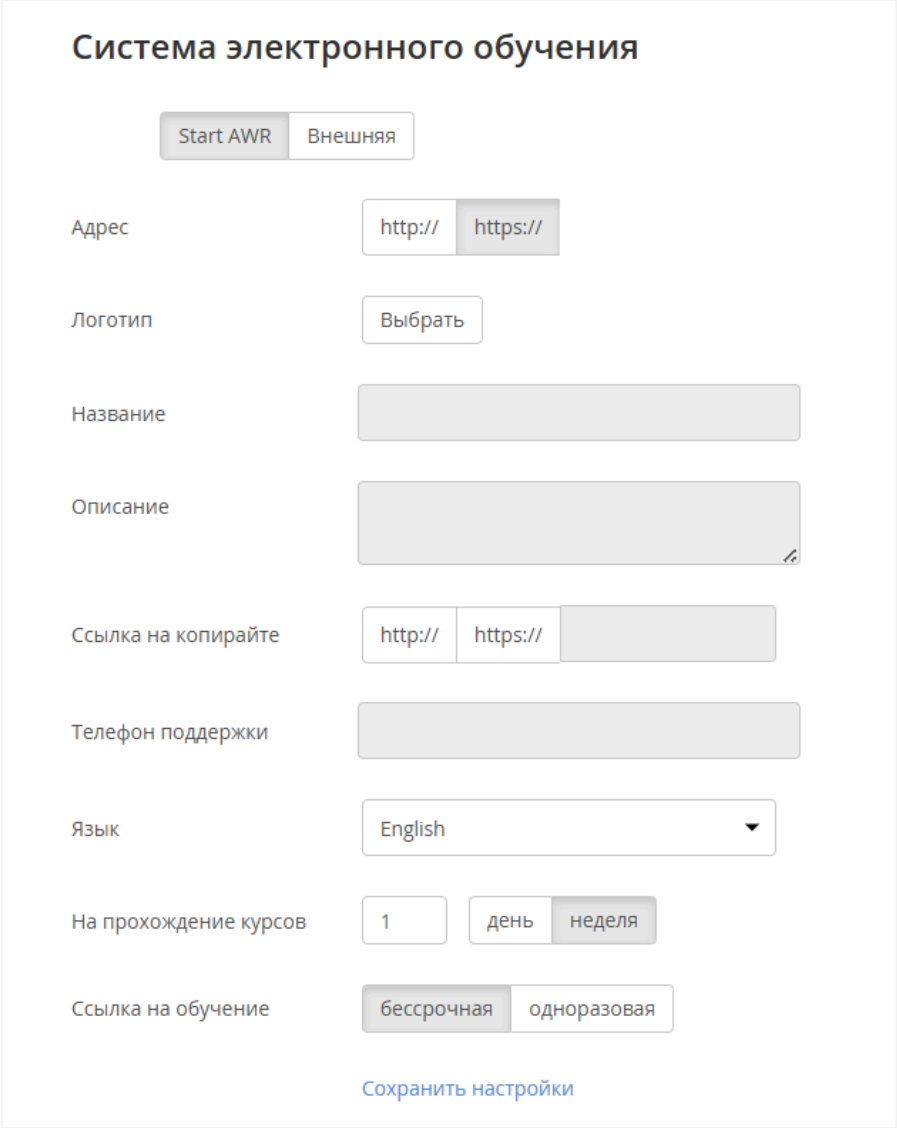
Даже если письмо со ссылкой будет утеряно, назначенный на курс сотрудник в любой момент сможет получить доступ к системе обучения через страницу авторизации обучающей системы.



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

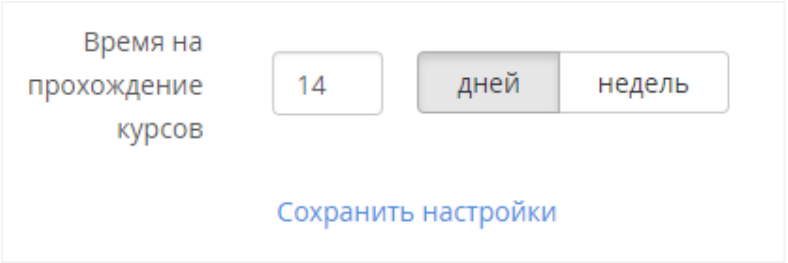


Администратор может заменить логотип, подпись, а также контактные данные, которые будут отображаться у сотрудников в интерфейсе системы обучения.



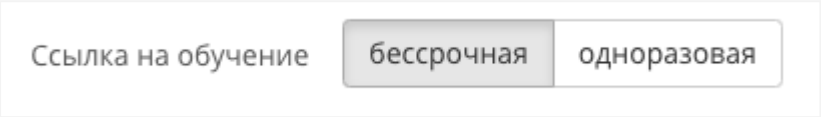
Курс будет считаться пройденным после просмотра всех слайдов и сдачи встроенного в курс теста.

Время на прохождение обучения можно задать в настройках:



Администратор может выбирать тип ссылки на обучение — бессрочная или одноразовая:

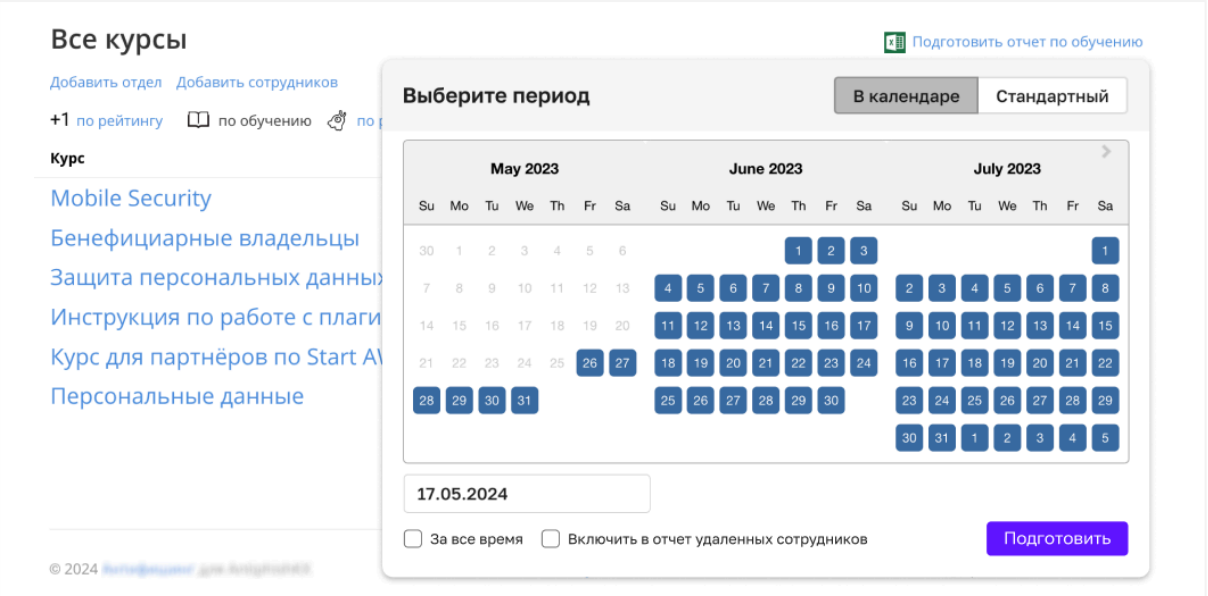
- Если ссылка одноразовая, при переходе по ней можно авторизоваться в системе обучения один раз, после чего при новых переходах по этой же ссылке новые авторизации (например, с новых устройств) не сработают.
- Если ссылка была одноразовая и по ней был совершен переход, после переключения на режим «Бессрочная», ссылка не будет активна. Если по одноразовой ссылке не совершили переход, после переключения на режим «Бессрочная» ссылка будет активна и начнет работать как бессрочная.
- Если ссылка выдана как бессрочная, после перехода по такой ссылке устаревание не происходит.
- После переключения бессрочной ссылки на режим «Одноразовая», ссылка в письме станет одноразовой.



Формат бессрочной или одноразовой ссылки на обучение одинаковый.

Вся статистика по обучению доступна в представлении сотрудников по обучению, 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 всё время использования системы. Всех прошедших обучение сотрудников рекомендуется включать в приоритетные цели имитированных атак для тренировки и проверки навыков.



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.

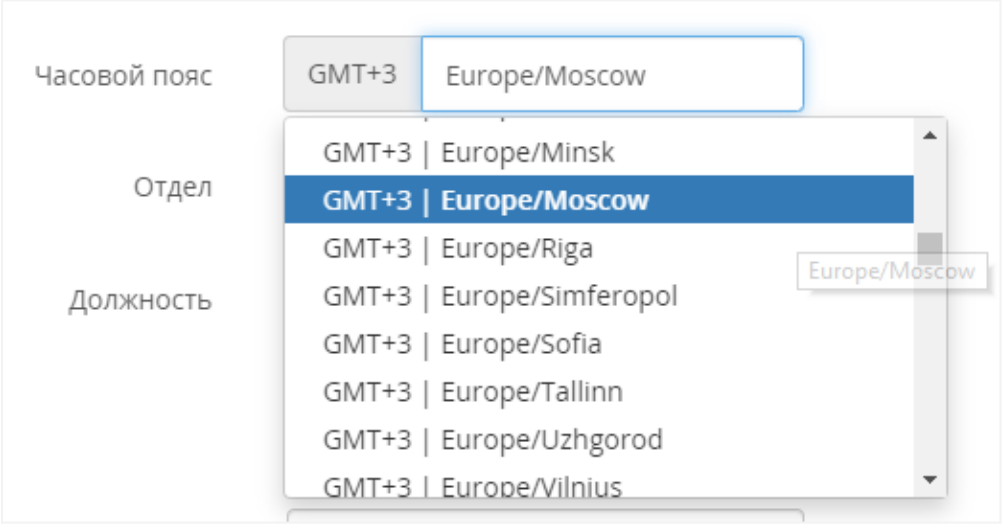
Ежемесячно — 60 минут

- 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.

Настройки

Часовой пояс

Выберите корректный часовой пояс для своего аккаунта. Планирование атак и обучения, а также отчетность будет выполняться в выбранном часовом поясе.

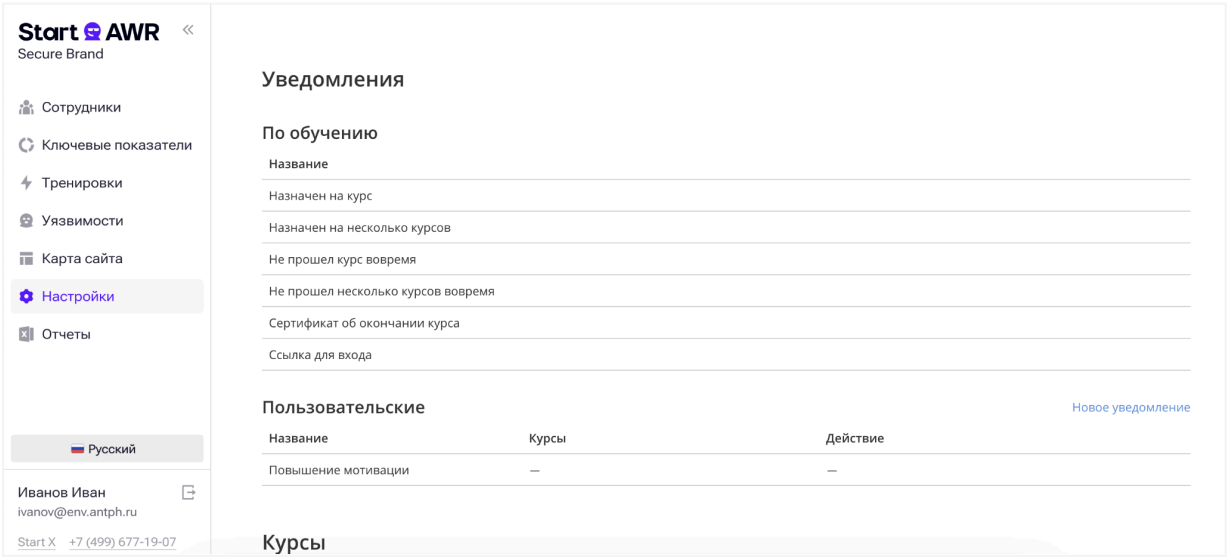


Настройка уведомлений системы обучения

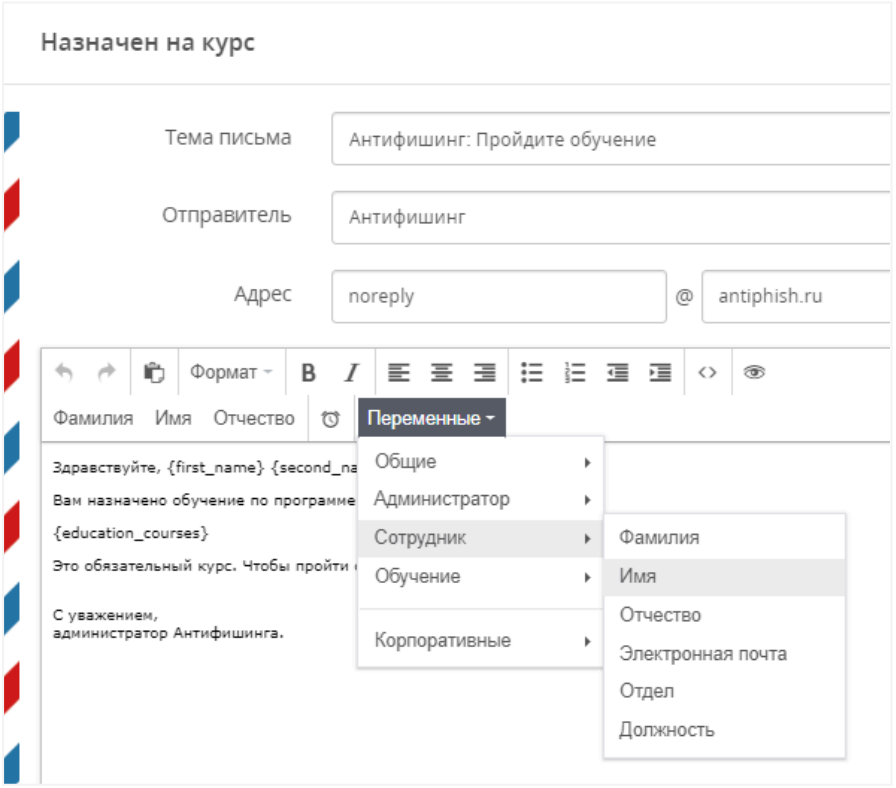
В системе существует два типа уведомлений:

По обучению — это шесть уведомлений, которые есть в системе по умолчанию. Их можно редактировать, копировать и восстанавливать до первоначальной редакции, но нельзя удалять.

Пользовательские — уведомления, создаваемые и настраиваемые администратором.



Все уведомления, которые будет отправлять сотруднику система обучения, можно изменить с применением корпоративного стиля. Так же, как и при создании атак, в редакторе уведомлений можно использовать переменные.



Для настройки правила отправления уведомления администратор может создать правило внутри редактора уведомлений или воспользоваться планировщиком.
При создании правила через планировщик администратору будут доступны все уведомления, у которых нет прикрепленных действия и курса/курсов.

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 попадаются на фишинговые атаки. Они становятся более внимательными и осторожными при работе с письмами.
2. Повышается культура информационной безопасности в компании. Сотрудники активно участвуют в защите информации и осознают важность собственного вклада в безопасность компании.
3. Сокращается время обнаружения инцидента. Фишинговая атака

выявляется практически сразу после получения письма, еще до момента ее обнаружения техническими средствами защиты и системами мониторинга.

Системные требования

Плагин можно установить для почтовых клиентов:

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

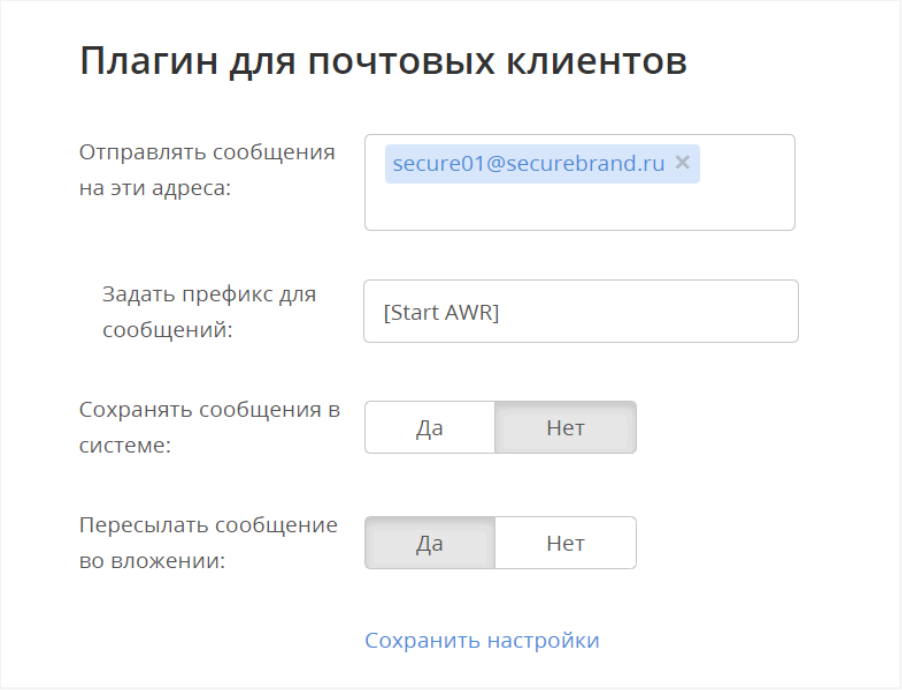
Также они должны работать с почтовым сервером Microsoft 365, Exchange Online, Exchange Server или другими, которые поддерживают Exchange Web Services (EWS).

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.

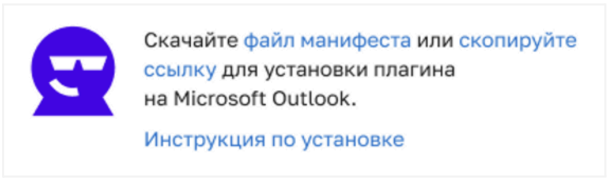
Настройка в Start AWR

1. Откройте платформу Start AWR.
2. Перейдите в раздел **Настройки** → **Плагин для почтовых клиентов**.



3. Заполните поля:
    - **Отправлять сообщения на эти адреса** — введите один или несколько электронных адресов, на которые будут поступать письма, отмеченные сотрудниками, как фишинговые.
      По умолчанию здесь указан электронный адрес ответственного за систему.
    - **Задать префикс для сообщений** — 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).

4. Скачайте файл манифеста или скопируйте ссылку на него.



Готово! Переходите к этапу установки плагина в Microsoft Outlook.

Установка

Есть два способа установить плагин:

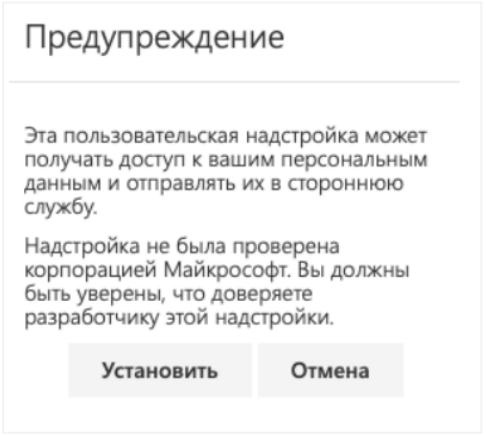
- **Локально**
  Плагин устанавливается вручную на каждый компьютер.
- **Централизованно**
  Плагин устанавливается через почтовые серверы Microsoft Exchange Online, Exchange Server и Microsoft 365. Централизованная установка упрощает управление и обновление плагина, так как изменения вносятся централизованно.

Локально

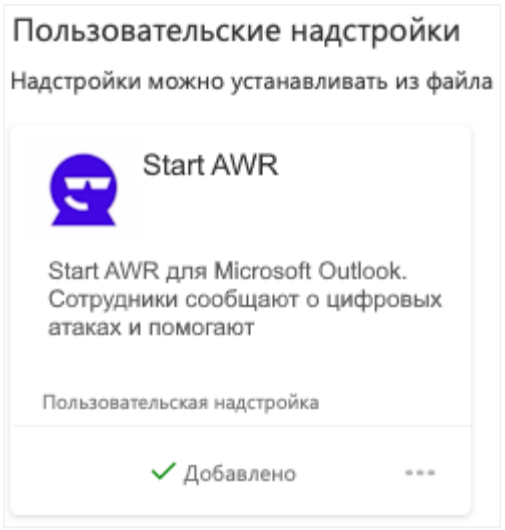
1. В главном разделе Microsoft Outlook нажмите **Получить надстройки**.
2. В открывшемся окне **Надстройки для Outlook** выберите **Мои**

надстройки → Добавить пользовательскую надстройку.

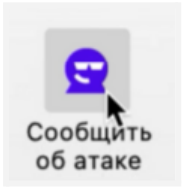
3. Добавьте ранее скачанный файл манифеста любым удобным способом — через загрузку файла или с помощью ссылки.
   Если появится предупреждение, нажмите кнопку **Установить**.



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.**

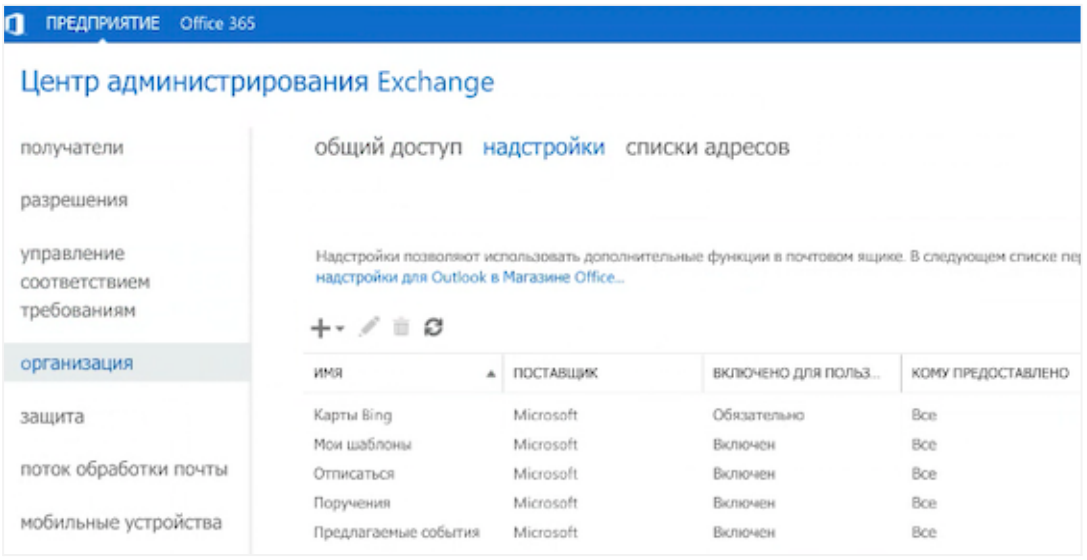


Централизованно

Алгоритм установки рассмотрим на примере Microsoft Exchange Server:

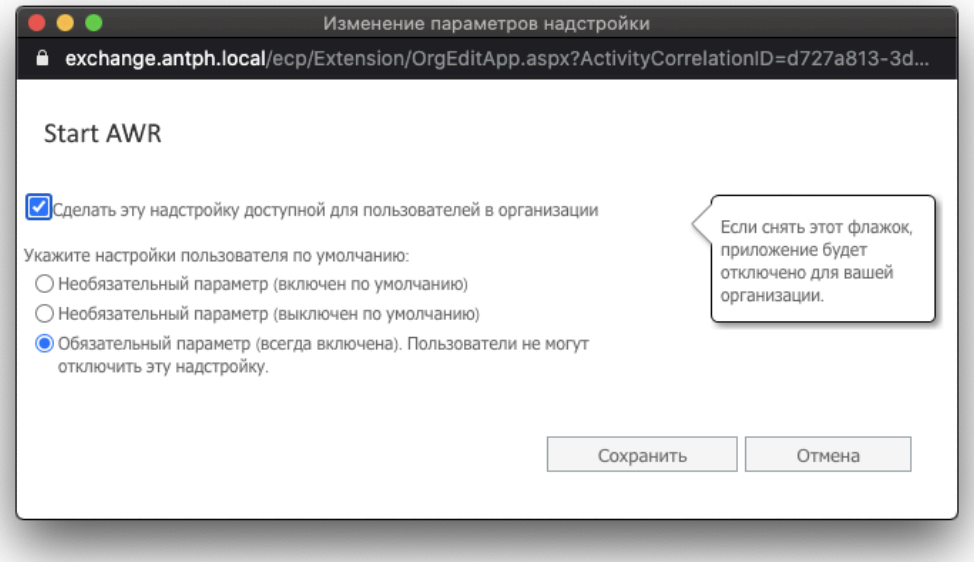
1. Войдите на портал администратора вашего почтового сервера.

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.

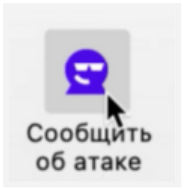
4. На некоторых версиях может появится подобное окно. Отметьте в нем пункты:
   - Сделать надстройку доступной для пользователей в вашей организации
   - Обязательный параметр (всегда включена). Пользователи не могут отключить эту надстройку.



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.

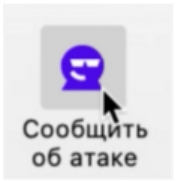
   На верхней панели Microsoft Outlook появится плагин Start AWR с кнопкой **Сообщить об атаке**.



Работа плагина

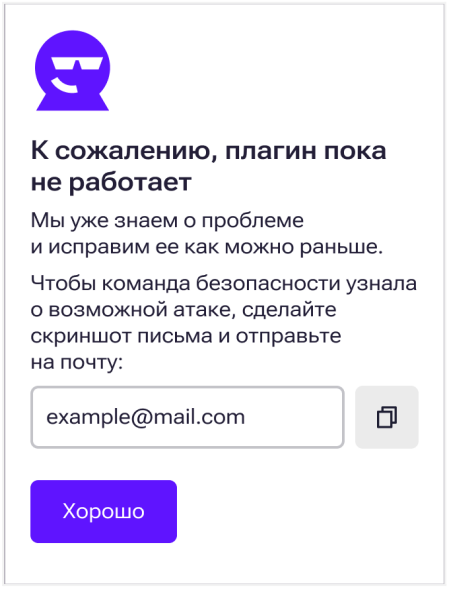
После открытия письма:

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

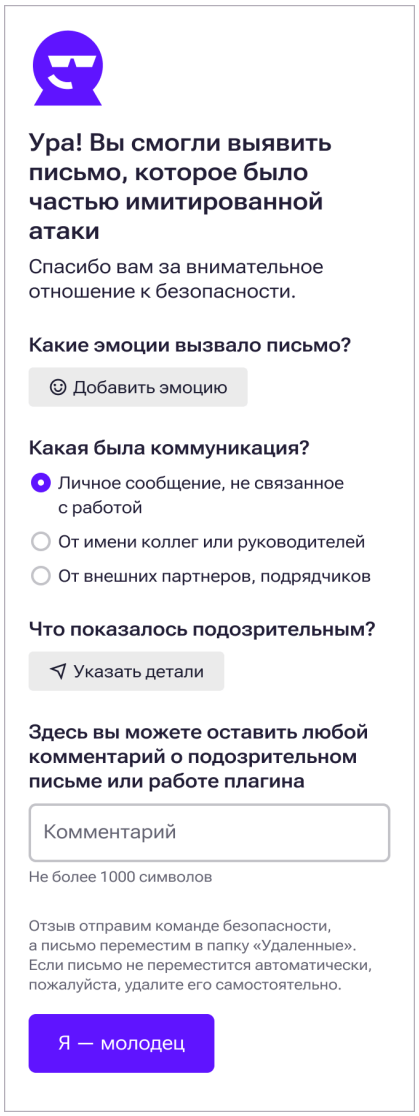


2. Подождите, пока плагин проанализирует письмо и определит тип атаки — реальная или имитированная.

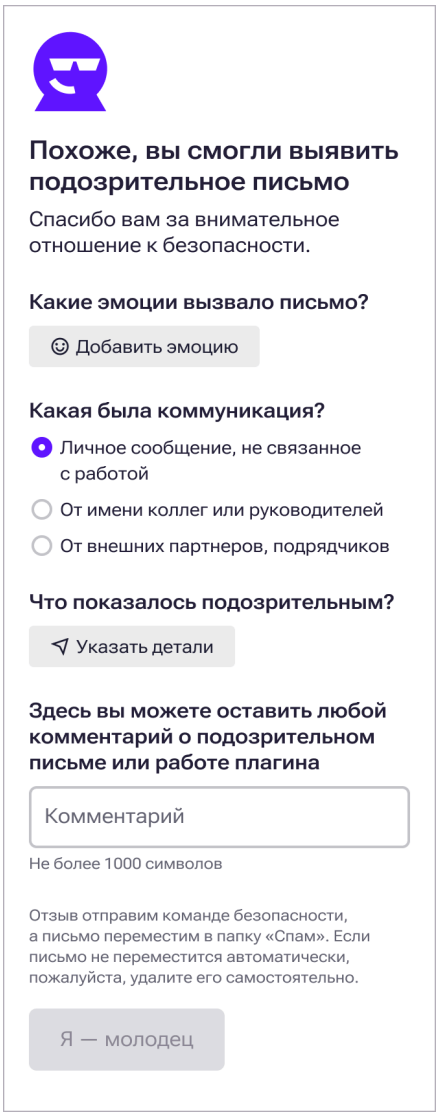
Если плагин не работает — сделайте скриншот письма и отправьте на почту, указанную в этом окне:



3. Заполните форму обратной связи:



Имитированная атака



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.

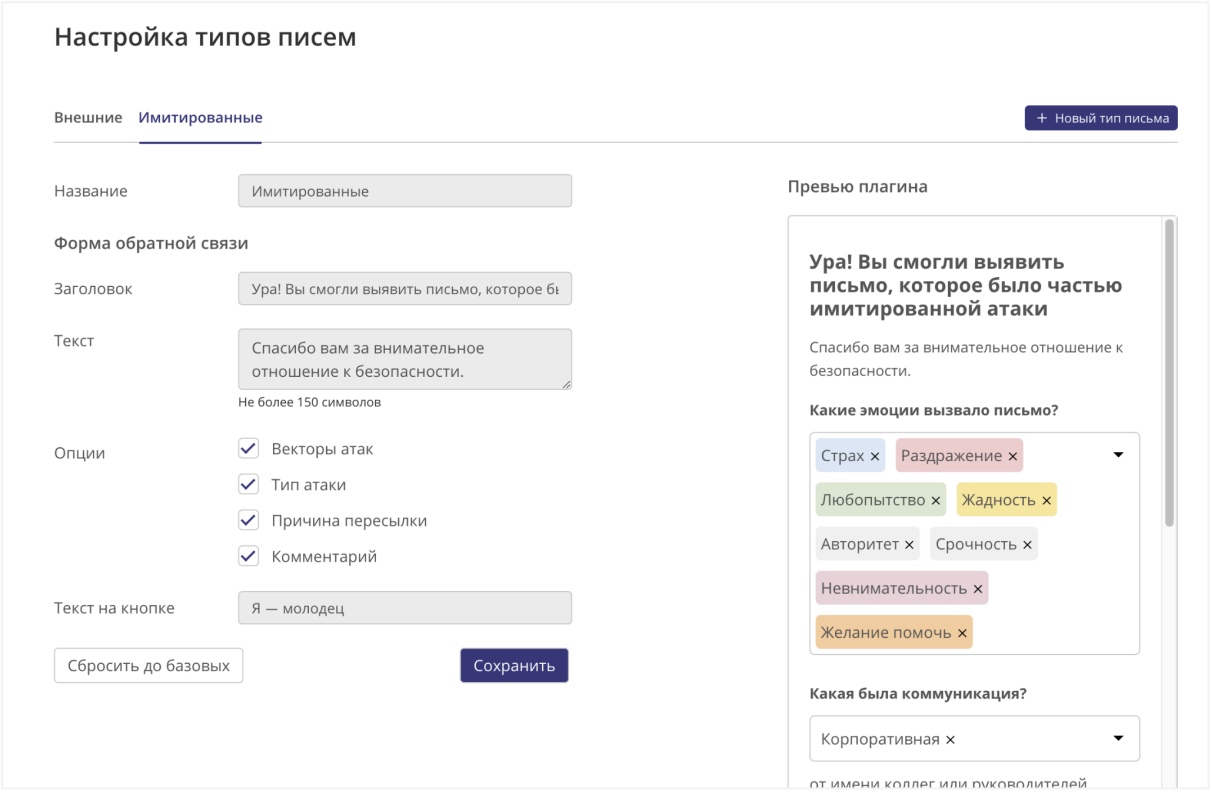
4. После заполнения формы обратной связи, нажмите кнопку **Я – молодец**.

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** → **Настройка типов писем**. Доступ к этому разделу можно редактировать с помощью ролевой модели.



Типы писем по умолчанию

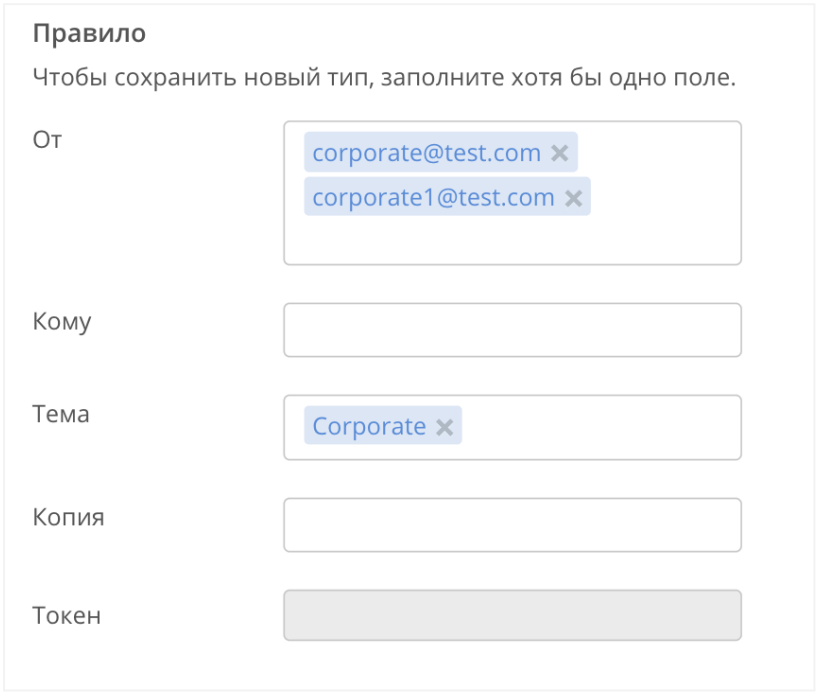
По умолчанию в системе есть два видам писем:

- **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

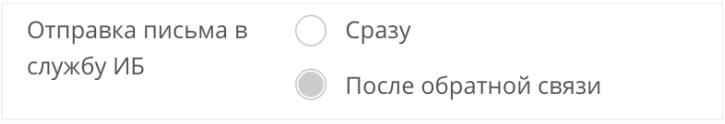
Кроме двух типов по умолчанию можно создавать собственные типы и задавать для них вид формы ОС.

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 оператор 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.



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.

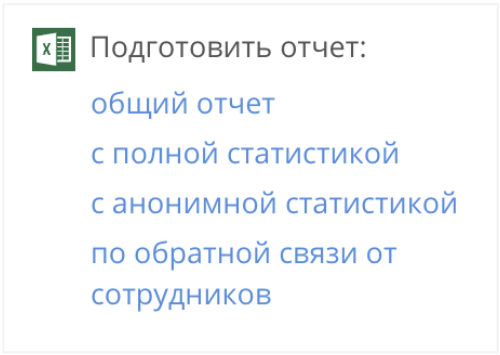
- **После обратной связи**
  Логика работы:
  Сотрудник нажал на «Сообщить об атаке» в плагине → Сотруднику открывается форма ОС → Сотрудник заполняет поля → Нажал на «Я – молодец!» → Сообщение отправлено в службу ИБ. В пересланном сообщении выведены заполненные данные по вектору, типу атаки, причине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

Предварительный просмотр формы ОС

С помощью окна **Превью 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

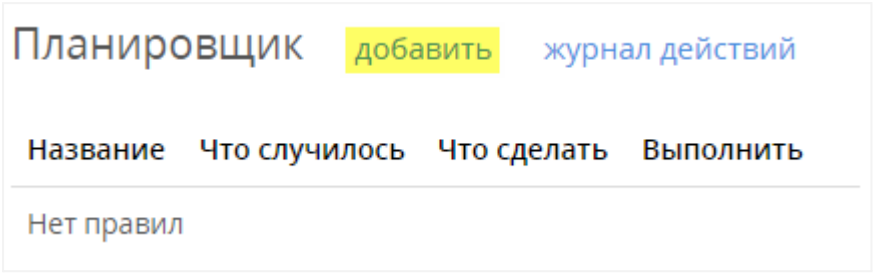
В меню и в разделе **Рейтинг** есть отчет **По обратной связи от сотрудников**. Он формируется в формате csv и содержит данные, которые собирает плагин.



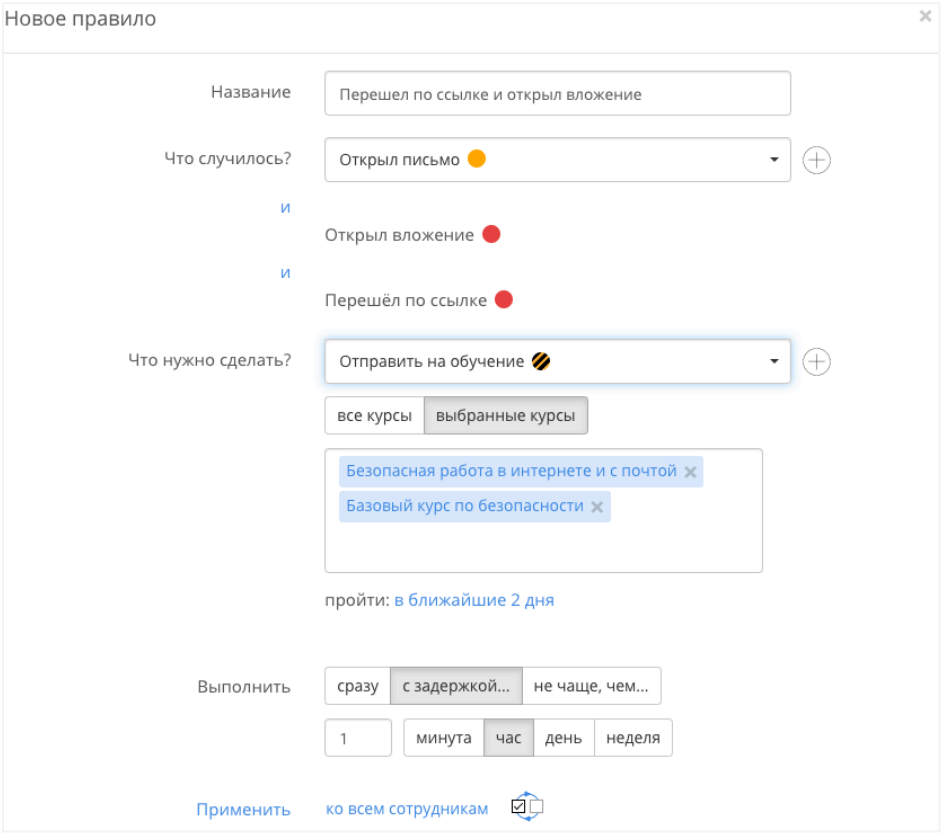
Планировщик

Планировщик поможет полностью автоматизировать процессы в системе: отправку на обучение, имитированные атаки на сотрудников, выгрузку отчетности.

Добавить новое правило для планировщика можно в разделе **Настройки** → **Планировщик**.

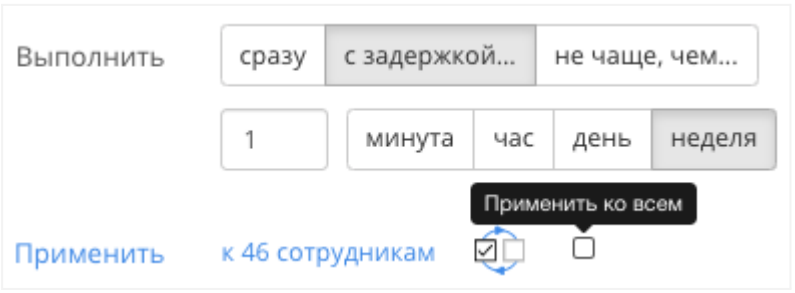


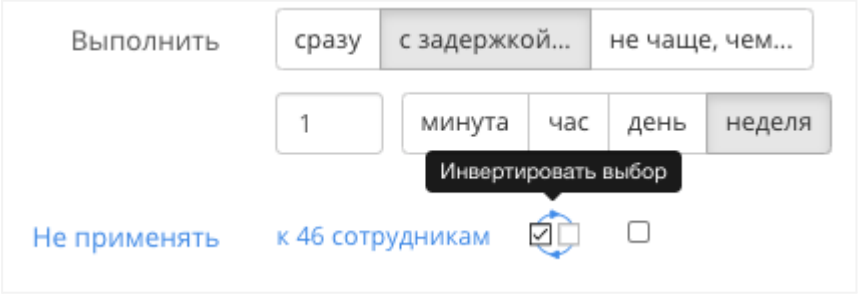
Можно добавить несколько событий-триггеров и действий, которые должны произойти по этим событиям:



Выбор целей в планировщике

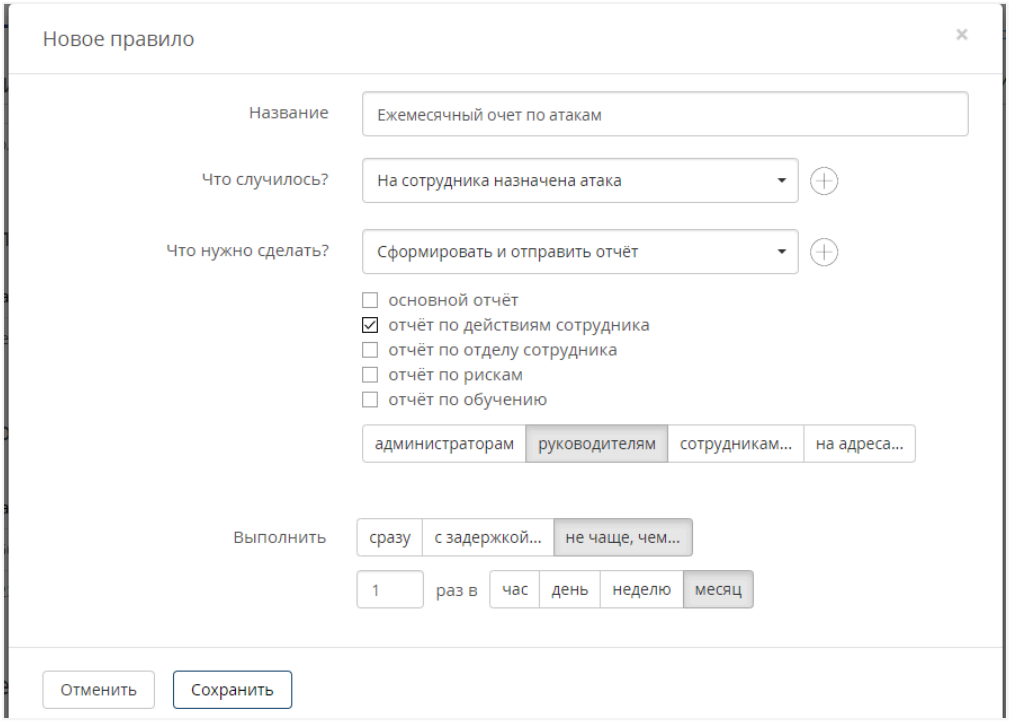
При создании правила планировщика можно выбрать конкретных сотрудников, для которых правило будет применено или наоборот, к которым оно применяться не будет.



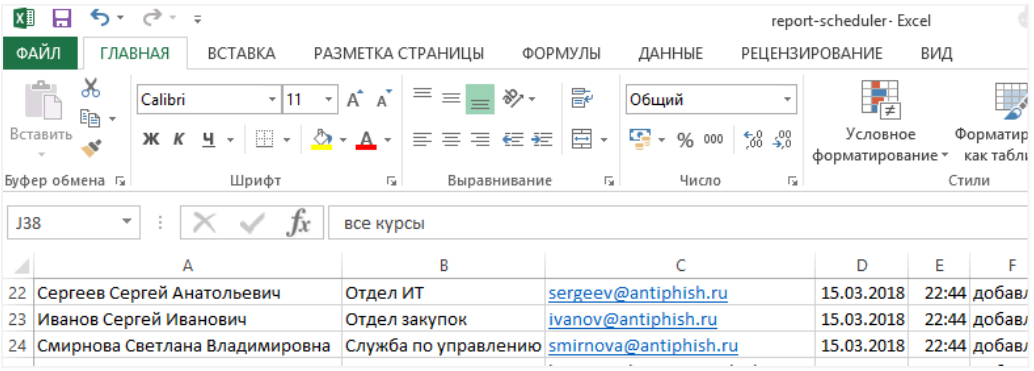


Отчеты

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



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



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