Общество с ограниченной ответственностью
«МультиТек Инжиниринг»

Программный комплекс
по обучению, тренировке навыков и контролю знаний
сотрудников по информационной безопасности

Минск 2021

Содержание

1. Общие сведения

Данный документ содержит описание Программного комплекса по обучению, тренировке навыков и контролю знаний сотрудников по информационной безопасности «Антифишинг» (далее – Система, «Антифишинг»).

Цель документа – предоставить заинтересованным предприятиям и организациям (далее – заказчики) информацию, позволяющую сделать осознанный выбор решения для обеспечения требуемого уровня осведомленности и навыков безопасной работы сотрудников.

Разработчиком Системы является ООО «Антифишинг» – российская исследовательская компания и разработчик программного обеспечения.

ООО «Антифишинг» (далее – производитель) работает на рынке с 2016 года, специализируясь на решении проблем человеческого фактора в информационной безопасности. В штате компании – специалисты по практической безопасности, разработчики, тестировщики, аналитики, психолог, редакторы и методологи.

Производитель ведёт собственные исследования, развивает уникальную классификацию цифровых атак на людей и поддерживает её в «Антифишинге».

ООО «МультиТек Инжиниринг» является официальным партнером ООО «Антифишинг» в Республике Беларусь, имеет в штате обученных специалистов, что позволяет обеспечить высокое качество настройки, интеграции и технической поддержки Системы.

При возникновении вопросов по Системе, не нашедших отражение в настоящем документе, а также при желании провести пилотный проект Системы, необходимо направить электронное письмо на адрес info@mte-cyber.by.

2. Назначение, условия применения и поставки Системы

«Антифишинг» предназначен для автоматизации следующих процессов:

- обучение сотрудников основам информационной безопасности;
- контроль уровня знаний сотрудников;
- тренировка и формирование навыков безопасной работы;
- отслеживание уязвимостей в клиентских приложениях (операционных системах, браузерах, офисных пакетах) с привязкой к небезопасным действиям и выдача рекомендаций по устранению уязвимостей.

В настоящем документе рассматривается «Антифишинг» в исполнении On Premise STANDARD, работающий внутри периметра безопасности заказчика.

Система предоставляет возможность интеграции с системами обучения WebTutor и Moodle и позволяет, помимо использования собственных обучающих курсов, загружать любые курсы обучения в виде SCORM-пакетов.

Панель мониторинга («дашборд») Системы позволяет отслеживать, как изменяются знания и навыки сотрудников. Кроме того, всем сотрудникам, подразделениям и заказчику в целом присваивается рейтинг в зависимости от безопасности их действий.

Система лицензируется по количеству пользователей (минимальное количество – 300) и сроку применения. Возможна поставка лицензии на 1 год или на несколько лет.

В стоимость лицензии «Антифишинга» включены стоимость работ по адаптации курсов по требованиям политик безопасности заказчика, брендирование и замена контактной информации, а также стоимость технической поддержки.

Система поставляется в подготовленном к настройке состоянии в виде виртуальной машины с установленной операционной системой CentOS 7.

Минимальные технические требования к серверу:

- 2 CPU;
- 4 Гбайт RAM;
- 60 Гбайт HDD.

Весь контент, а также интерфейсы Системы доступны на русском, английском и итальянском языках.

3. Функции Системы

Система обеспечивает:

- автоматизацию процессов обучения и контроля защищённости сотрудников;
- имитацию целевых атак через электронную почту, ссылки, вложения различных типов, фишинговые сайты и USB-устройства;
- возможность создания заказчиком собственных шаблонов атак;
- проведение имитаций атак по различным технологическим и психологическим векторам;
- контроль уровня осведомлённости и уровня навыков сотрудников;
- контроль уязвимостей приложений;
- собственные электронные курсы и их бесплатную адаптацию под требования заказчика;
- регулярные обновления материалов для обучения и тренировки навыков;
- использование планировщика для полной автоматизации процессов;
- API для интеграции с другими процессами и системами безопасности.

4. Архитектура Системы

Система состоит из следующих основных компонент:

– **Attack** – компонент тренировки навыков (отправка атак);
– **Edu** – компонент управления обучением (прохождение курсов обучения и сдача зачетов);
– **Mail** – внутренний почтовый сервер (отправка уведомлений об обучении и имитированных атак).

Общая схема работы Системы представлена на рис.1.

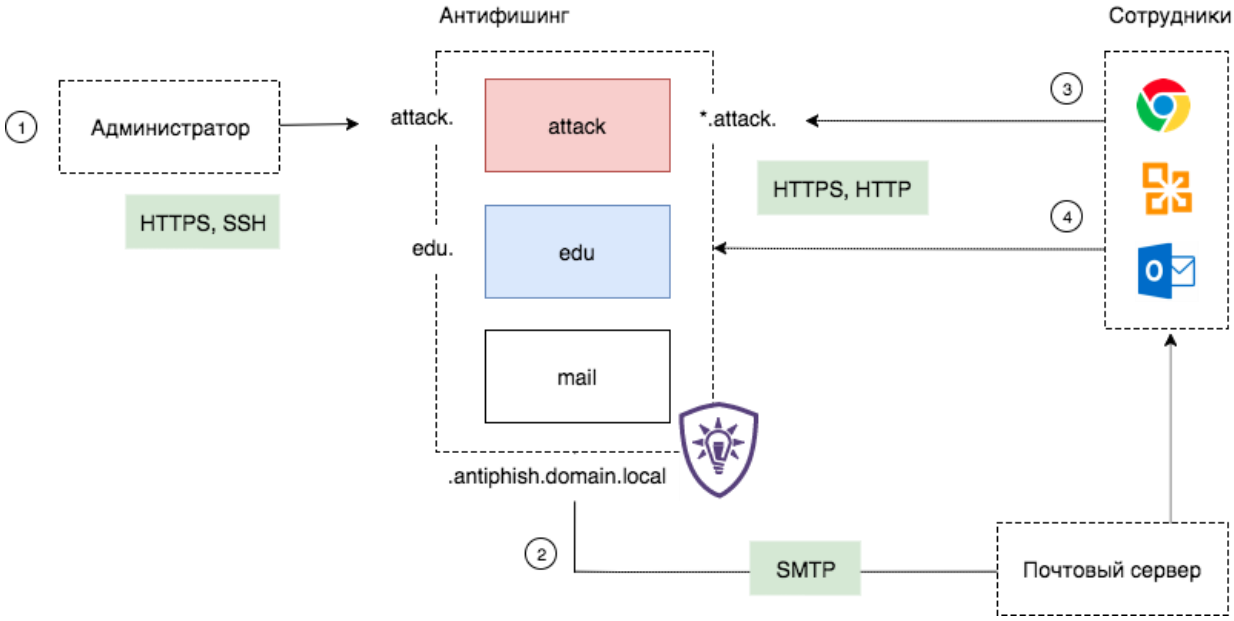

Рисунок 1. Общая схема работы Системы

5. Настройка Системы

Для того, чтобы начать работу, необходимо войти в консоль администрирования (административный интерфейс) Системы (рис. 2).

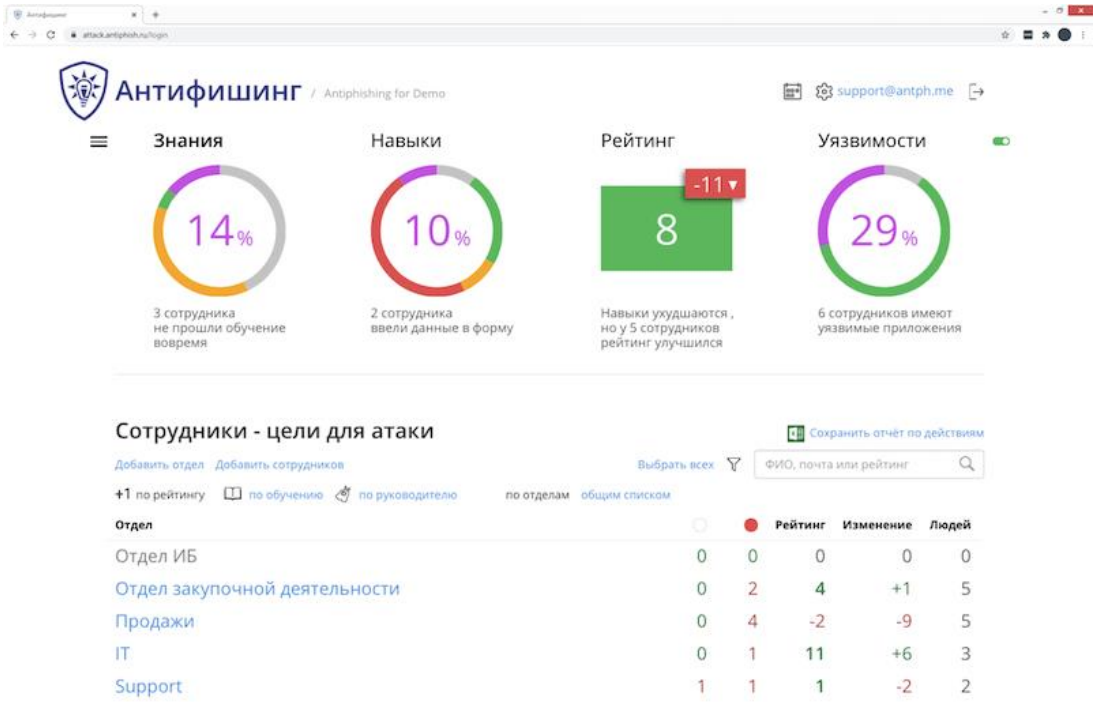

Рисунок 2. Консоль администрирования

Консоль администрирования предлагает следующие возможности:

- раздел «Знания»: отслеживание уровня знаний сотрудников, создание новых учебных атак;
- раздел «Навыки»: отслеживание навыков сотрудников, запуск учебных атак;
- раздел «Рейтинг»: отображение рейтинга по сотрудникам и отделам, вся отчётность;
- раздел «Уязвимости»: выявление программных брешей в пользовательских приложениях на основе небезопасных действий сотрудников;
- раздел «Настройки»: определение всех параметров Системы;
- раздел «Планировщик»: автоматизация и управление задачами по расписанию.

Кроме того, предоставляется возможность просмотра на одной странице всех функций одновременно – путём нажатия на кнопку классического меню в верхнем левом углу.

Одновременно в Системе могут работать несколько сотрудников – менеджеры и специалисты по безопасности, аудиторы, HR-специалисты и

администраторы информационной безопасности.

Встроенная ролевая модель и многопользовательский режим позволяют назначить каждому сотруднику только необходимые права доступа (рис. 3).

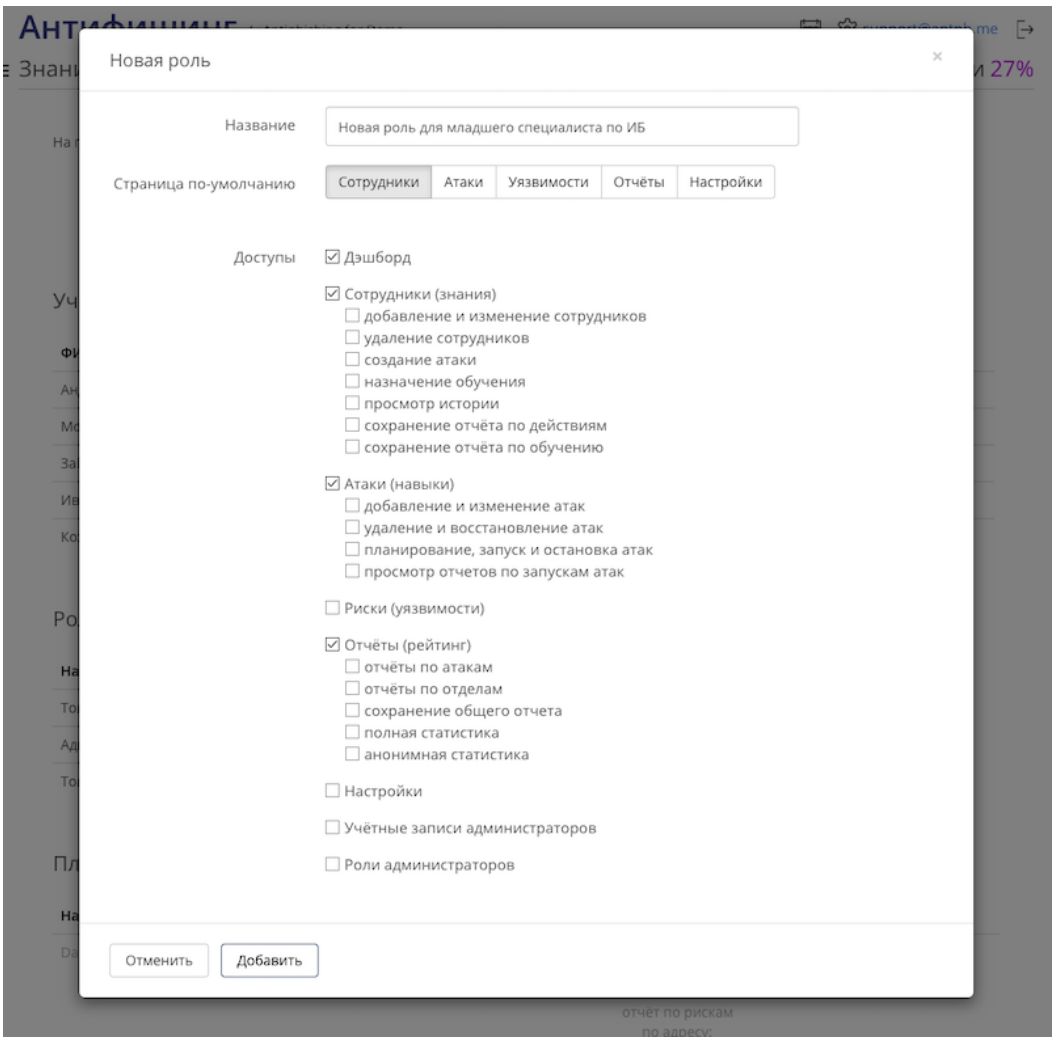

Рисунок 3. Создание новой роли

В разделе «Знания» можно добавлять учётные записи сотрудников, группировать их в подразделения – как в ручном режиме, так и с помощью импорта из файла формата XLS, из Active Directory, через API (рис. 4).

Для более удобного отображения информации доступна сортировка по сотрудникам, отделам или руководителям. В дальнейшем можно назначать сотрудникам атаки и курсы обучения, просматривать историю действий сотрудников, удалять или изменять учётные записи.

Рисунок 4. Отображение списка сотрудников в разделе «Знания»

В разделе «Навыки» отображаются подготовленные ранее учебные атаки (рис. 5). Здесь можно производить запуск этих атак сразу же или через заданный промежуток времени, используя планировщик.

Каждая атака размечается по атрибуции и психологическим векторам в соответствии с классификацией производителя.

Кроме того, есть возможность скопировать атаку и внести практически любые изменения в её шаблон. Отсюда же можно сохранять отчёты о проведённых тренировках.

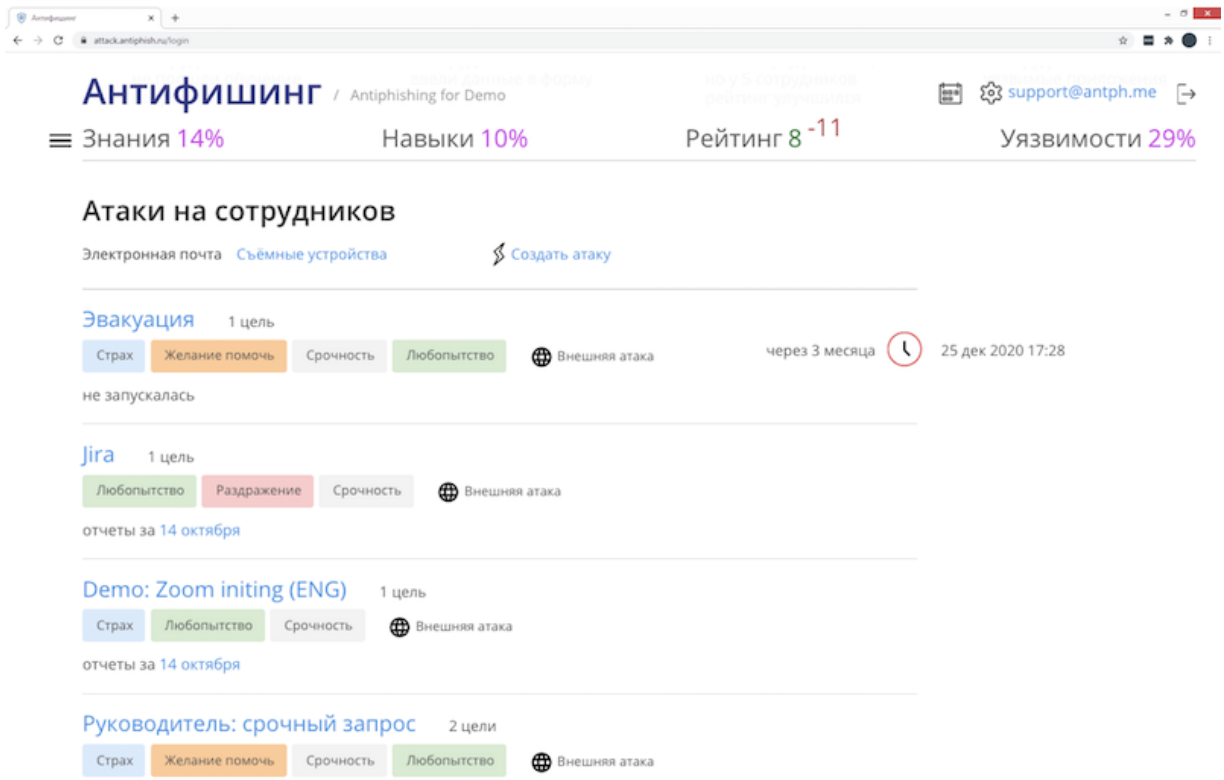

Рисунок 5. Список учебных атак в разделе «Навыки»

В разделе «Уязвимости» (рис. 6) можно посмотреть найденные проблемы и риски: бреши в операционных системах, браузерах, офисных пакетах, почтовых

клиентах и других приложениях, с которыми работают сотрудники и которые Система определяет, как уязвимые, анализируя актуальность версий и их обновлений.

Отчёт из этого раздела можно передавать коллегам для повышения приоритетов патч-менеджмента, а устранённые уязвимости можно отмечать – они исчезнут из этого представления.

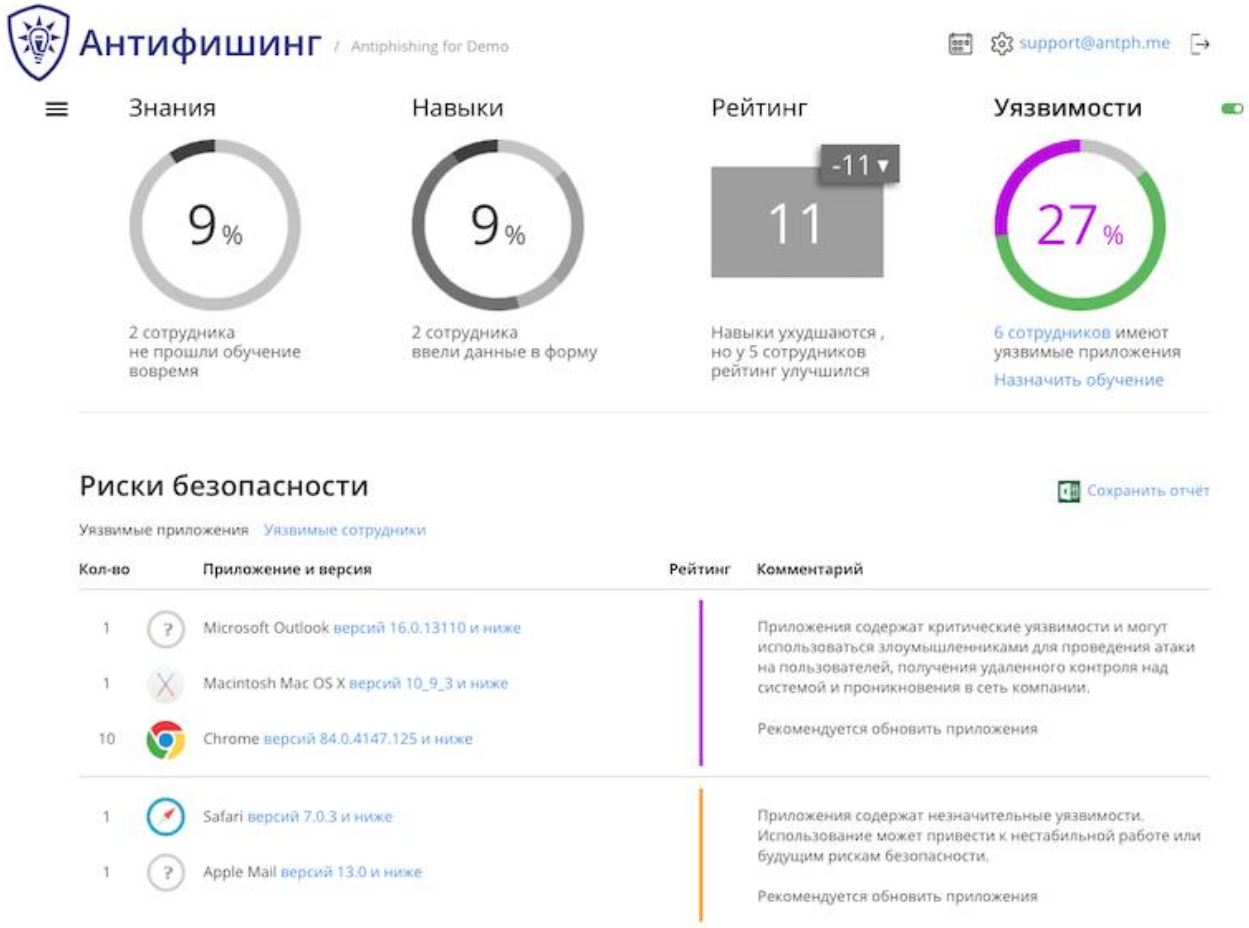

Рисунок 6. Информация в разделе «Уязвимости»

Через раздел «Настройки» (рис. 7) задаются различные параметры Системы – учётные записи администраторов, конфигурация уведомлений и системы обучения, импорт из LDAP и другие.

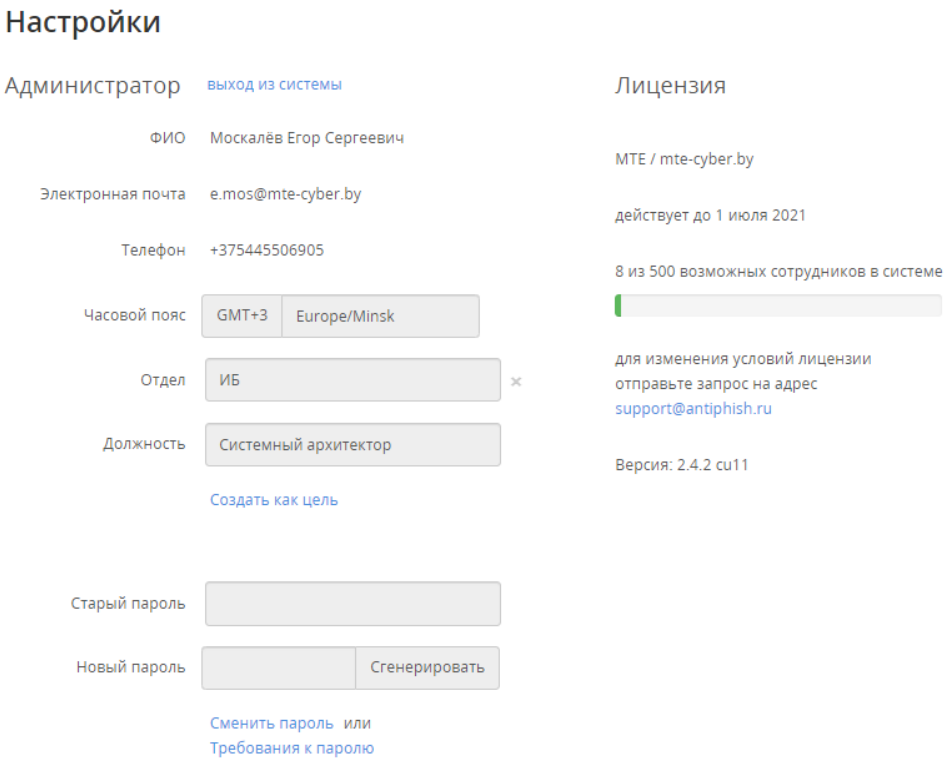

Рисунок 7. Перечень параметров лицензии из раздела «Настройки»

Планировщик позволяет автоматизировать процессы обучения и тренировки навыков, а также формирования и отправки отчётности. При этом можно создавать сложные конструкции с использованием логических элементов «и»/«или», а также планировать различные действия с задержкой по времени, сразу или с определённой частотой выполнения (рис. 8).

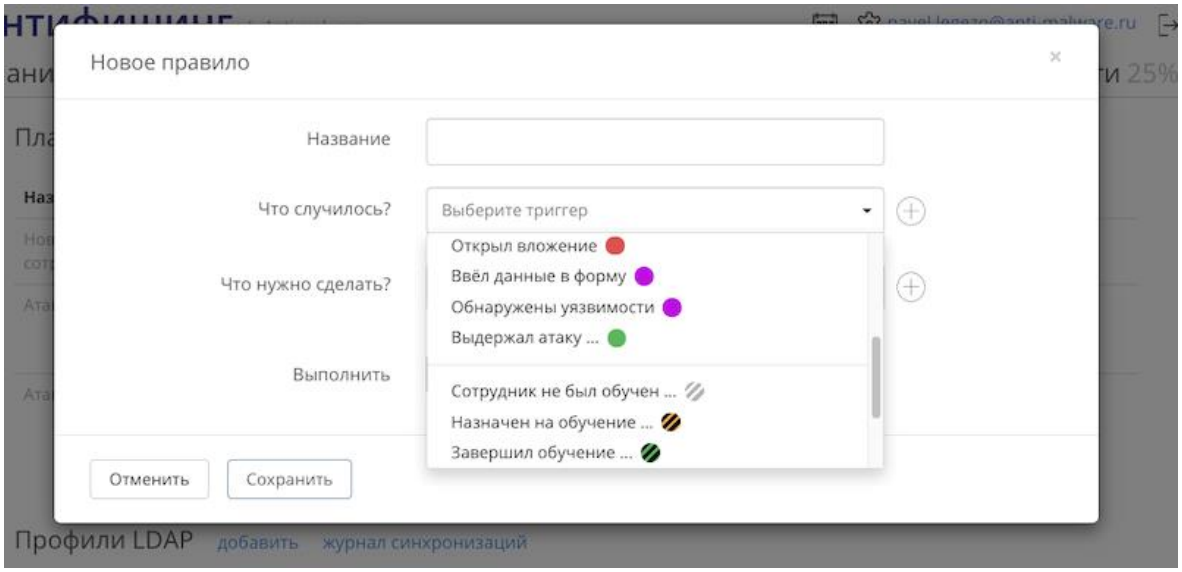

Рисунок 8. Пример триггеров планировщика — возможных состояний, на основе которых автоматизируются процессы

Производитель поставляет и в рамках технической поддержки на основе

методологии «Антифишинга» ежеквартально обновляет базовые правила (пример правила приведен на рис. 9), которые создаются с помощью планировщика.

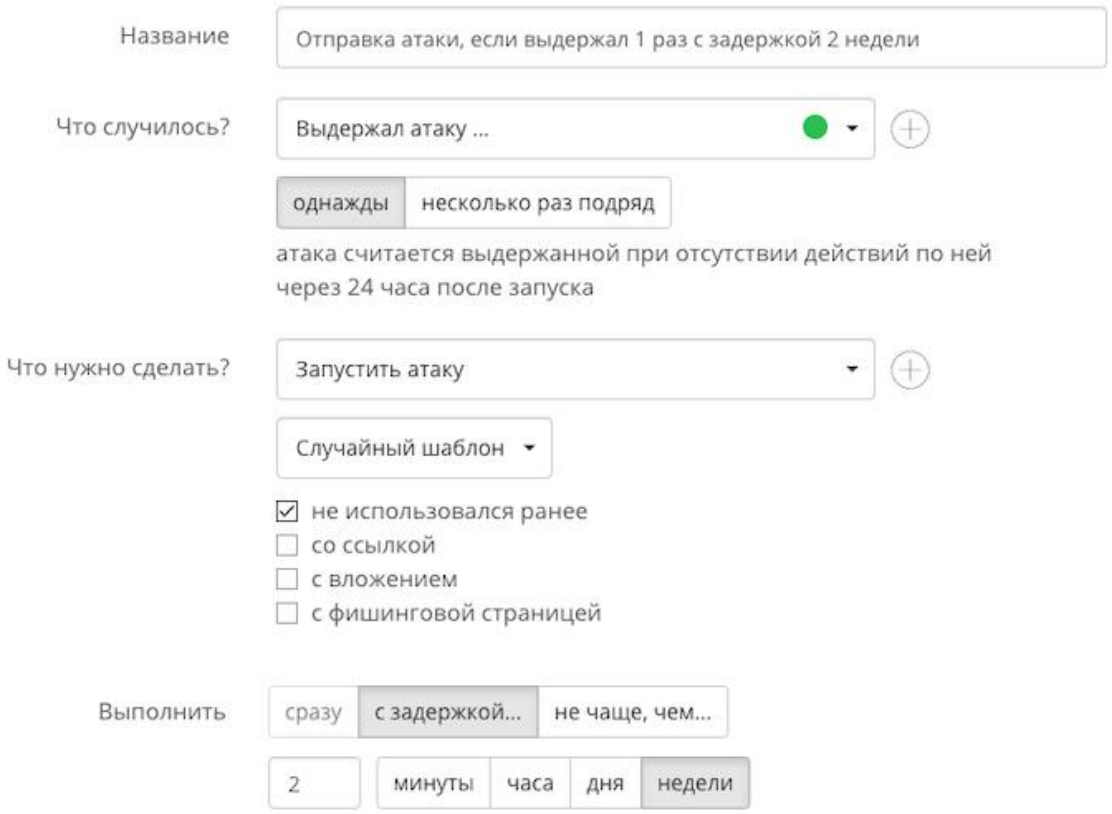

Рисунок 9. Пример правила в планировщике

6. Подготовка шаблонов для атак

Производитель в рамках технической поддержки занимается созданием шаблонов целевых атак для каждого заказчика.

Эта работа основана на собственных психологических и технических исследованиях, которые производитель проводит с 2017 года (собирает и публикует еженедельную аналитику по фишингу и другим цифровым атакам на людей, участвует в информационном обмене с ФинЦЕРТ Банка России и др.), что позволяет ему предлагать заказчикам самые актуальные целевые атаки (пример сценария атаки приведен на рис. 10) и обучающие материалы.

Сценарии соответствуют классификации Антифишинга

Ид	Сценарий	Вектора атаки	Технологии
1	Письмо от вендора ([redacted]), который предлагает провести обзор новой версии Web application firewall. Во вложении ReleaseNotes, компания [redacted] готова предоставить оборудование для тестирования в течение двух дней.	Внешняя Персональная Любопытство Желание помочь	Эл. письмо Вложение MS Word
2	Независимый эксперт отправляет статью для публикации по теме "Влияние Искусственного интеллекта на жизнь безопасника". Статья находится во вложении.	Внешняя Анонимная Любопытство	Эл. письмо Вложение pdf
3	Письмо от Генерального директора, в котором он обращается к сотруднику по имени и требует срочно проверить, кто согласовал эту новость на корпоративном сайте.	Корпоративная Персональная Страх Срочность Авторитет	Эл. письмо Ссылка
4	Письмо от Госуслуг, в котором к сотруднику обращаются по имени, сообщают о правонарушении и приводят подробности (адрес недалеко от офиса, другие детали). Там же указана сумма штрафа. Предлагается посмотреть подробности по ссылке и оплатить штраф со скидкой 50% до конца недели.	Личная Персональная Раздражение Жадность Срочность Авторитет	Эл. письмо Ссылка Фишинговая gosuslusi.ru
5	Письмо от сотрудника, который просит срочно подключиться к его видеоконференции по ссылке (Zoom, Google Meet, Skype for business) для помощи по важному проекту. Фишинговая страница запрашивает доступ к камере.	Корпоративная Персональная Желание помочь Страх Срочность Авторитет	Эл. письмо Ссылка Фишинговая ссылка Zoom/Google Meet/Skype for business
6	Рассылка от информационной системы об учащении случаев мошенничества и проведении профилактических мероприятий, необходимо в ближайшее время сменить	Корпоративная Анонимная Страх Срочность Авторитет	Эл.письмо Ссылка Фишинговое окно блокировки ОС

Рисунок 10. Пример сценария имитированных атак

После согласования сценария с заказчиком производитель разрабатывает шаблон атаки (в виде писем со всем оформлением: ссылками, вложениями, фишинговыми страницами) для внесения изменения в Систему.

7. Подготовка новой атаки

Для того, чтобы подготовить новую проверку, необходимо нажать на кнопку «Создать атаку»; появится окно для определения параметров.

В качестве примера выбран шаблон атаки от имени компании, которая приглашает работников на международный форум. (рис. 11).

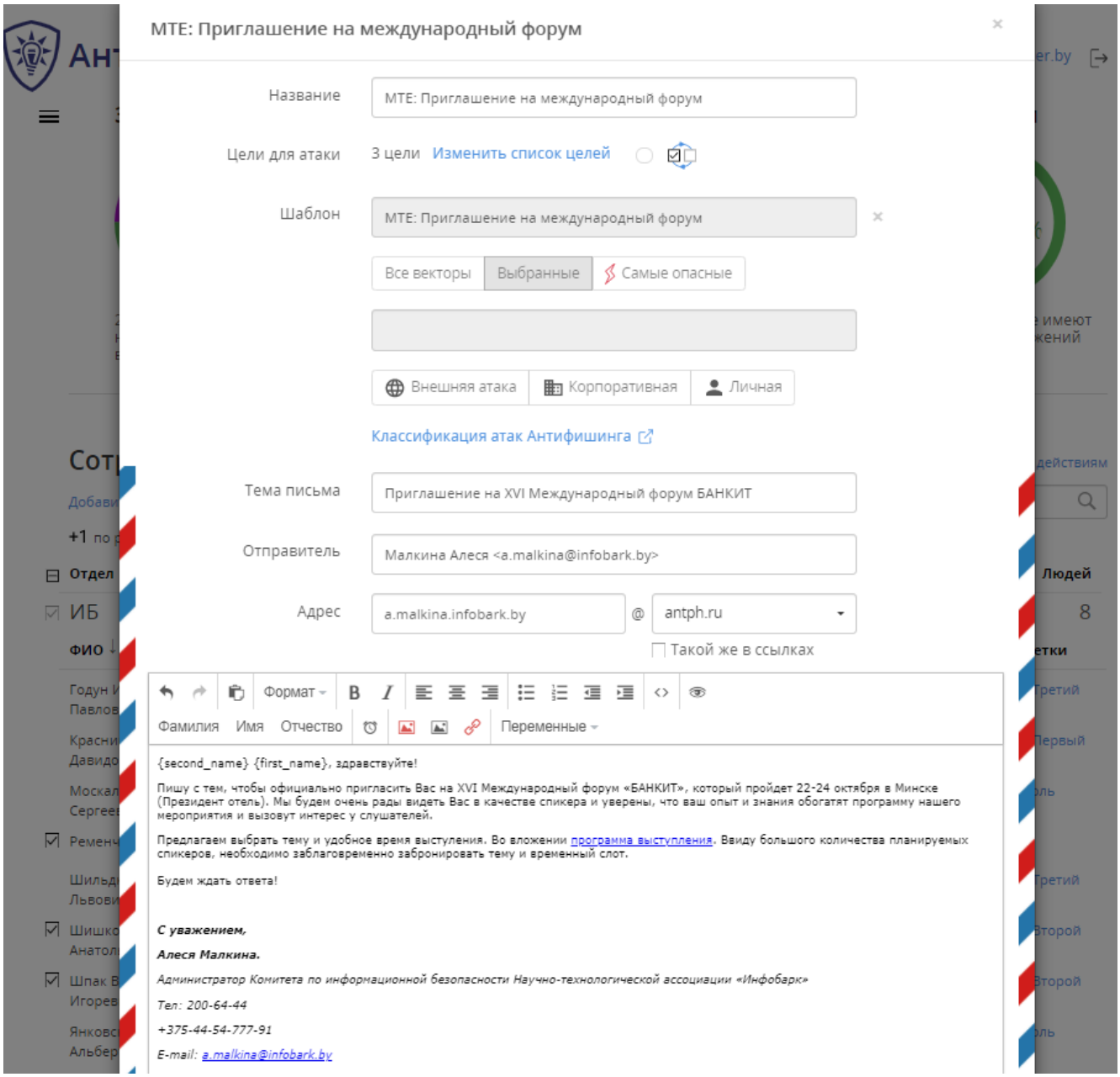

Рисунок 11. Создание новой учебной атаки

По классификации производителя у этой атаки будут следующие параметры:

- атрибуция: корпоративная атака;
- психологические векторы и усилители: страх, авторитет, срочность;
- персонификация: есть.

В зависимости от сценария в атаку могут добавляться файлы различных типов, фишинговые страницы и финальные страницы с обратной связью для пользователей (рис. 12).

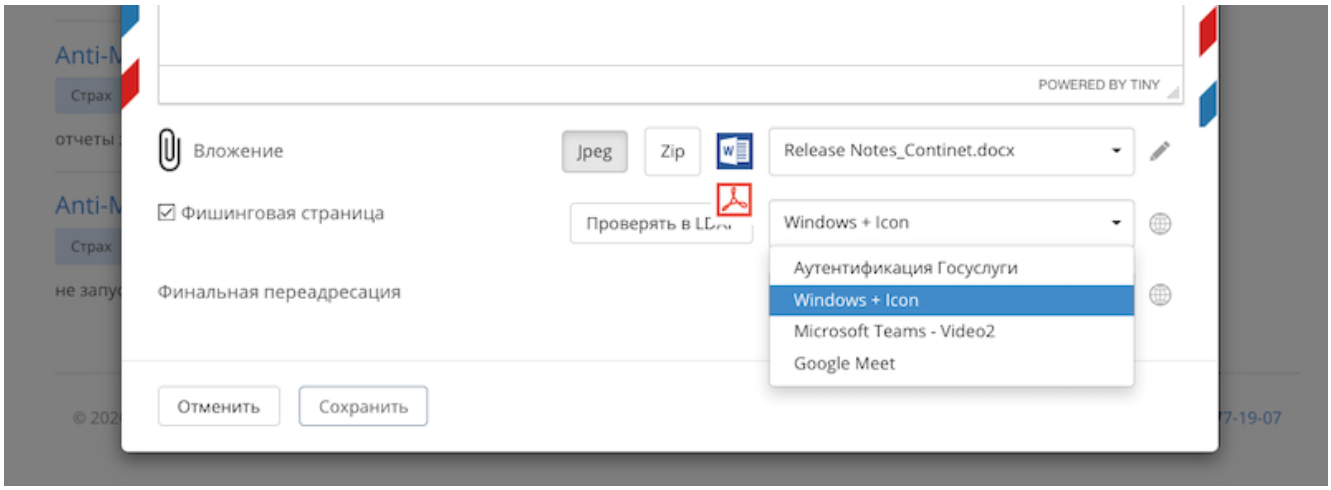

Рисунок 12. Внесение изменений в учебную атаку

После того как учебная атака будет создана и назначена сотрудникам, она отобразится в списке атак раздела «Навыки» (рис. 13).

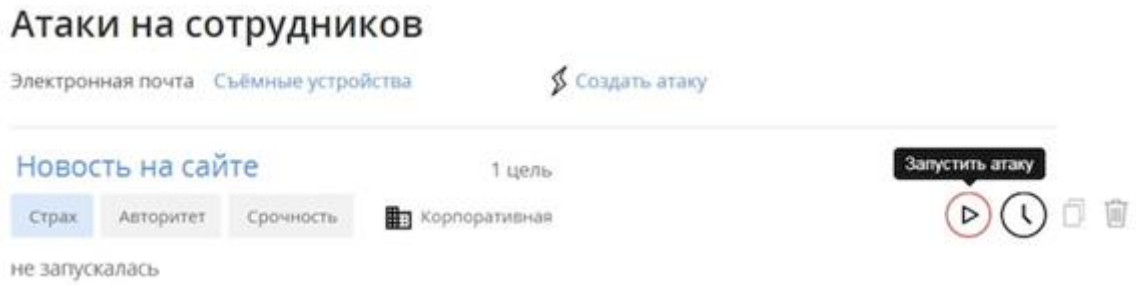

Рисунок 13. Подготовленная учебная атака на сотрудников

Атаку можно выполнить немедленно или в запланированный момент времени, а также удалить её либо скопировать, после чего внести в сделанную копию изменения (например, поменять текст письма, адрес и имя отправителя, тему, финальную страницу, вложение и т. д.).

8. Выполнение учебных атак и тренировка навыков

Атаки после запуска приходят сотрудникам, а Система фиксирует возможные небезопасные действия – загрузку внешнего содержимого, открытие файлов и отключение защищённого режима (для офисных документов), переходы по ссылкам и ввод паролей, или, например, разрешение на доступ к камере и микрофону (рис. 14).

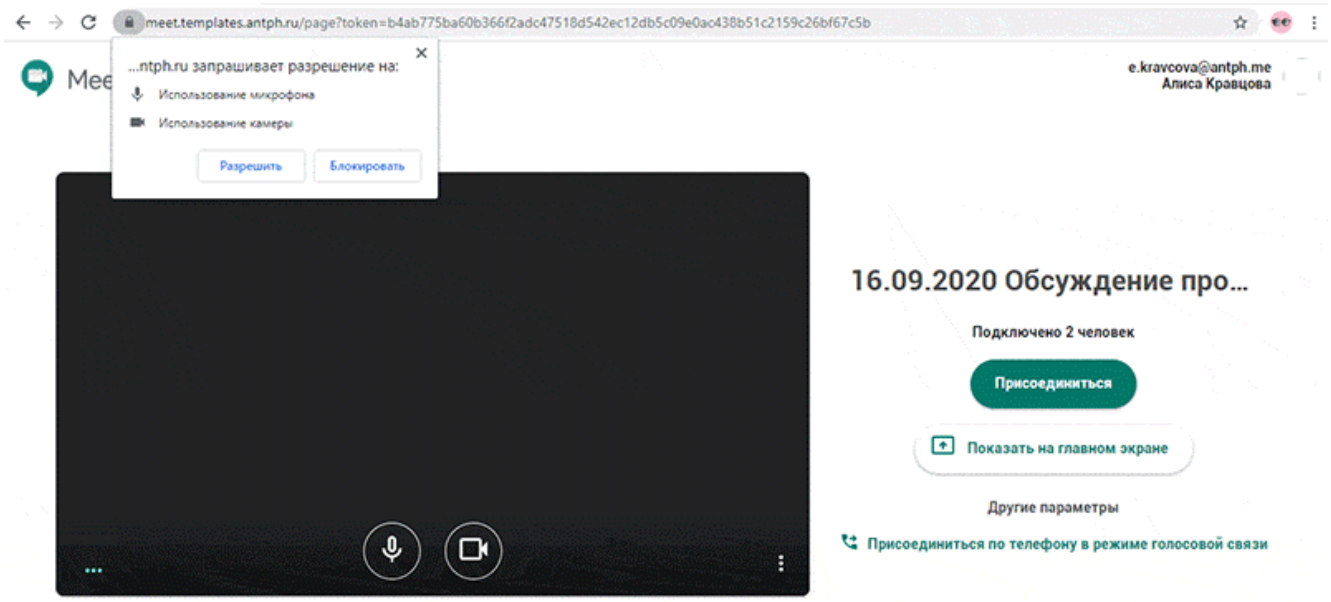

Рисунок 14. Проведение учебной атаки через доступ к камере и микрофону

Как только сотрудник совершает небезопасное действие, Система показывает ему эмоциональную обратную связь и тут же объясняет, как нужно действовать безопасно в подобной ситуации.

Другая атака выглядит для пользователя как ошибка, которая появляется в операционной системе. Язык, текст и внешний вид ошибки адаптируются под операционную систему и действующие параметры пользователя (рис. 15).

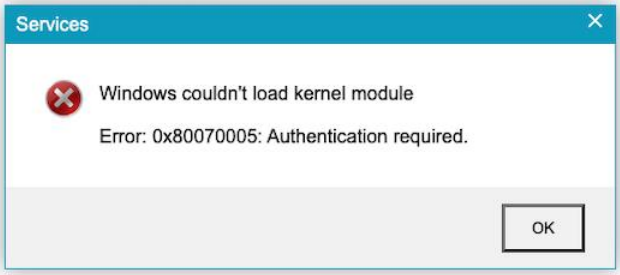

Рисунок 15. Ложная ошибка в операционной системе

После нажатия на любой элемент окна экран пользователя блокируется (рис. 16) — вместо браузера и интерфейса операционной системы пользователь видит знакомый экран блокировки. Оформление, шрифты и другие параметры подбираются в соответствии с действующими групповыми политиками.

Рисунок 16. Экран блокировки рабочего стола в Системе

При попытке «разблокировать» компьютер пользователь видит свои имя и фамилию, адрес электронной почты и даже свою фотографию, если он авторизован на одном из популярных сайтов, которые проверяет производитель (рис. 17).

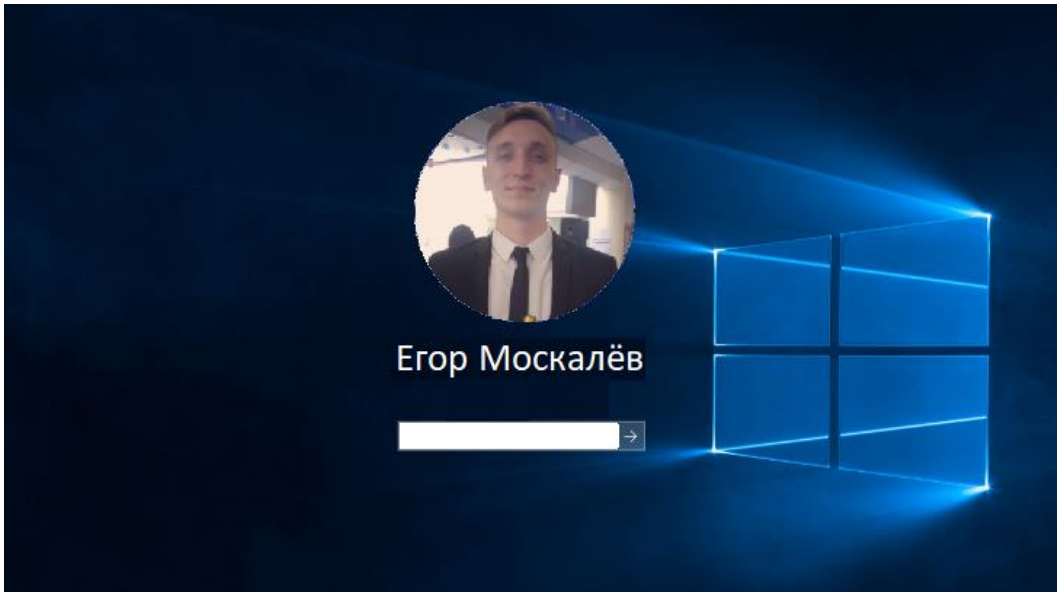

Рисунок 17. Ложное окно авторизации

Пароль может сверяться с действующим доменным паролем учётной записи пользователя, если в Системе включена синхронизация с LDAP, и администратор выбрал соответствующий пункт в параметрах атаки (рис. 18).

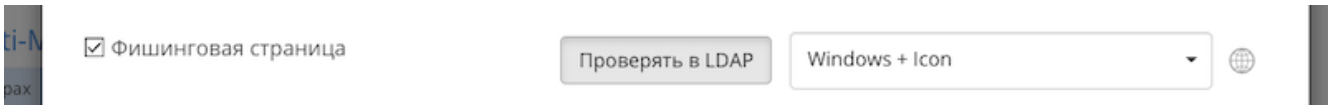

Рисунок 18. Включение синхронизации с LDAP

Также Система может фиксировать безопасное поведение сотрудников – например, умение выявить атаку и сообщить о ней через плагин в почтовом клиенте (рис. 19).

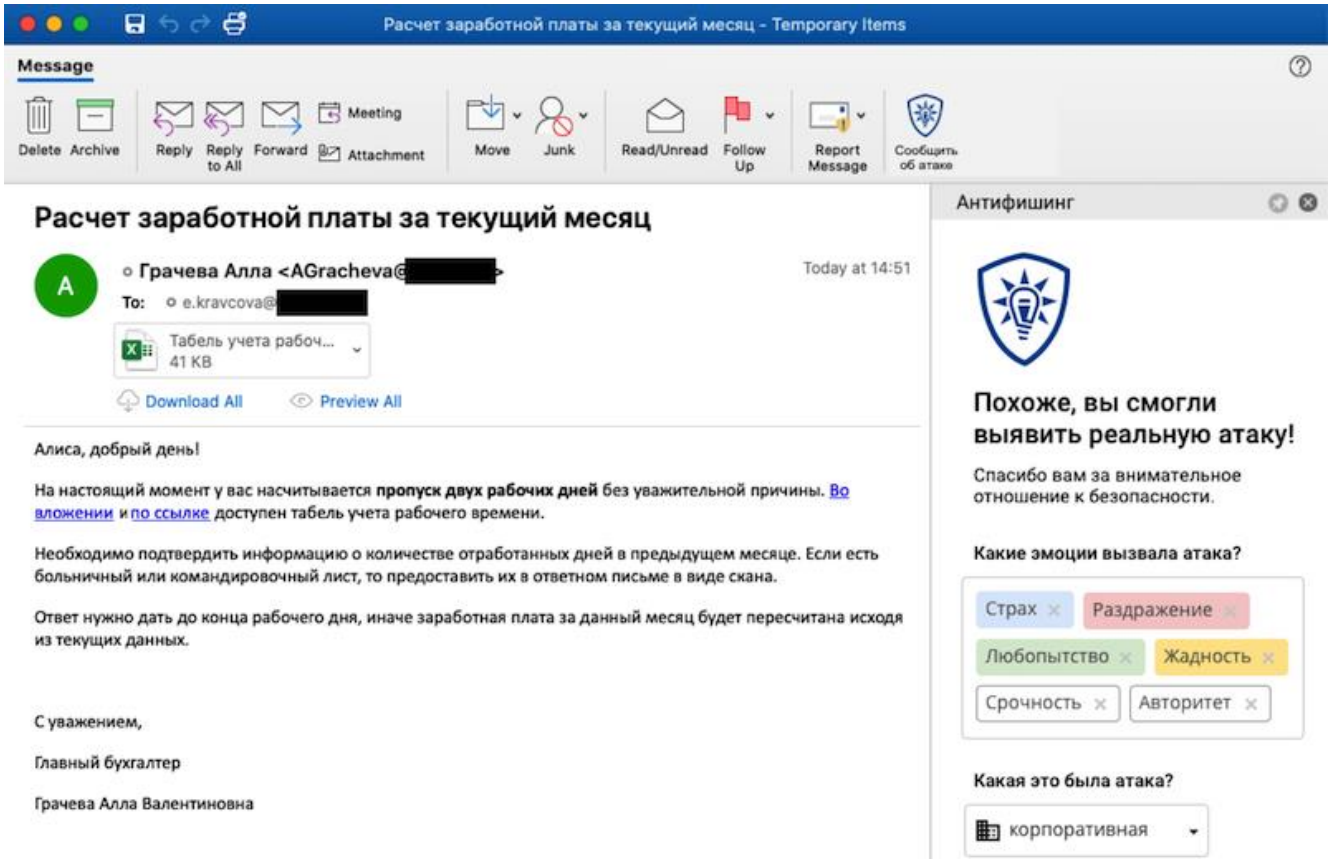

Рисунок 19. Выявление реальной фишинговой атаки

Эта функциональность позволяет не только формировать навыки сотрудников, но и побуждать их к безопасному поведению, а также собирать внутренние киберразведывательные (Threat Intelligence) данные по социальной инженерии: техническую и психологическую аналитику по реальным атакам, которые выявили сотрудники.

Использование плагина доступно в Системе, начиная с версии 2.4.3.

9. Результаты учебных атак

В результате каждого действия по каждой имитированной атаке у сотрудника накапливается рейтинг – число, означающее одновременно его опыт и общий уровень защищённости (рис. 20).

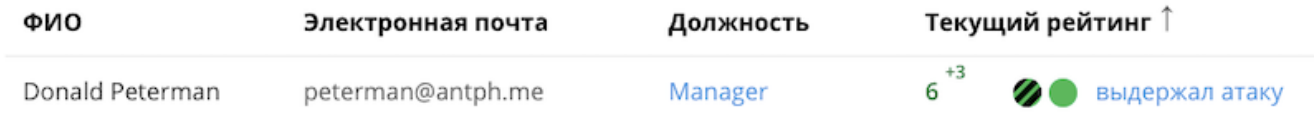

Рисунок 20. Отображение текущего рейтинга сотрудника

Отрицательный рейтинг означает, что в большинстве имитированных атак сотрудник совершал небезопасные действия (рис. 21).

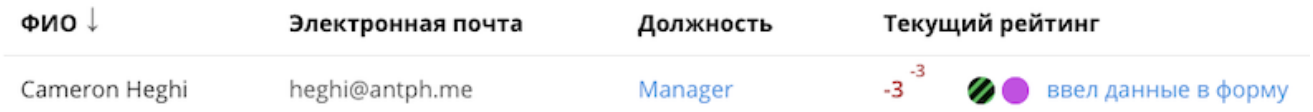

Рисунок 21. Отображение текущего рейтинга сотрудника

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 вкупе с его изменением по всем сотрудникам является ключевым показателем защищённости и отображается на главной странице «Антифишинга» (рис. 22).

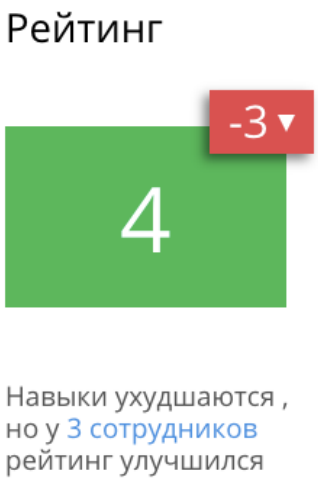

Рисунок 22. Отображение общего рейтинга сотрудников на главной странице

10. Формирование рейтинга

В случае, если сотрудник совершил хоть одно небезопасное действие в атаке, рейтинг в ней автоматически становится отрицательным, так как атака считается не выдержанной.

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

11. История действий

Через «Историю действий» можно посмотреть, как действовал сотрудник (или любая группа коллег) на протяжении времени. Графики наглядно покажут все совершённые операции и изменения рейтинга (рис. 23).

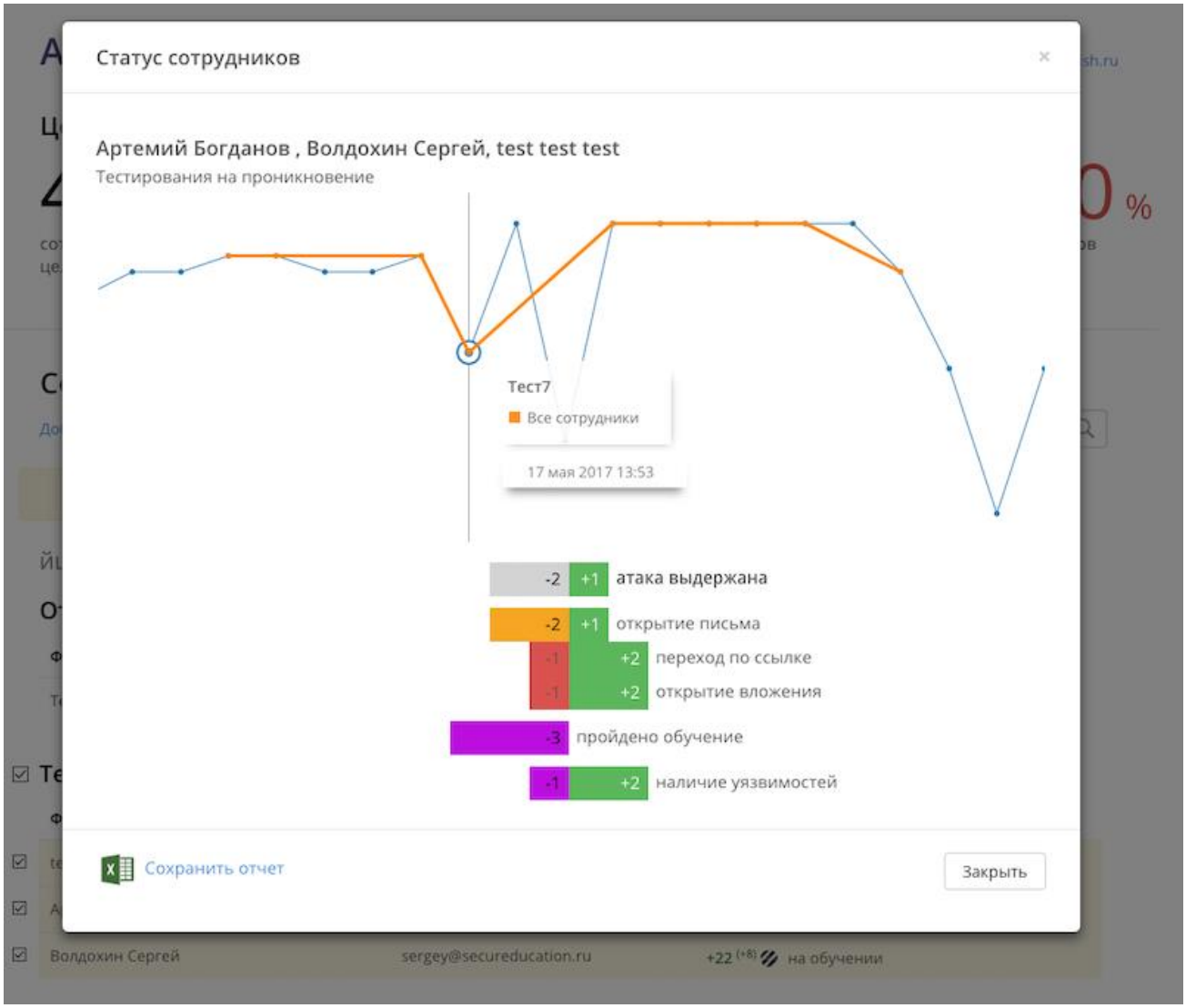

Рисунок 23. Отображение истории действий сотрудников на графиках

Оранжевый график показывает имитированные атаки и статистику, общую для всех выбранных сотрудников.

Синий график показывает статистику по подмножеству выбранных сотрудников (не все выбранные пользователи могли одновременно участвовать в одних и тех же имитированных атаках).

Статистика по обучению и обнаружению уязвимых приложений показана для тех же сотрудников справочно и не влияет на изменение рейтинга.

12. Обучение сотрудников

В Системе есть встроенная система обучения и несколько курсов по вопросам информационной и физической безопасности, которые следует знать сотруднику (рис. 24).

После отправки на обучение (вручную, через планировщик, или через API) пользователю приходит приглашение. Перейдя по ссылке в нём, сотрудник попадает в личный кабинет, где будут отображены все назначенные ему курсы.

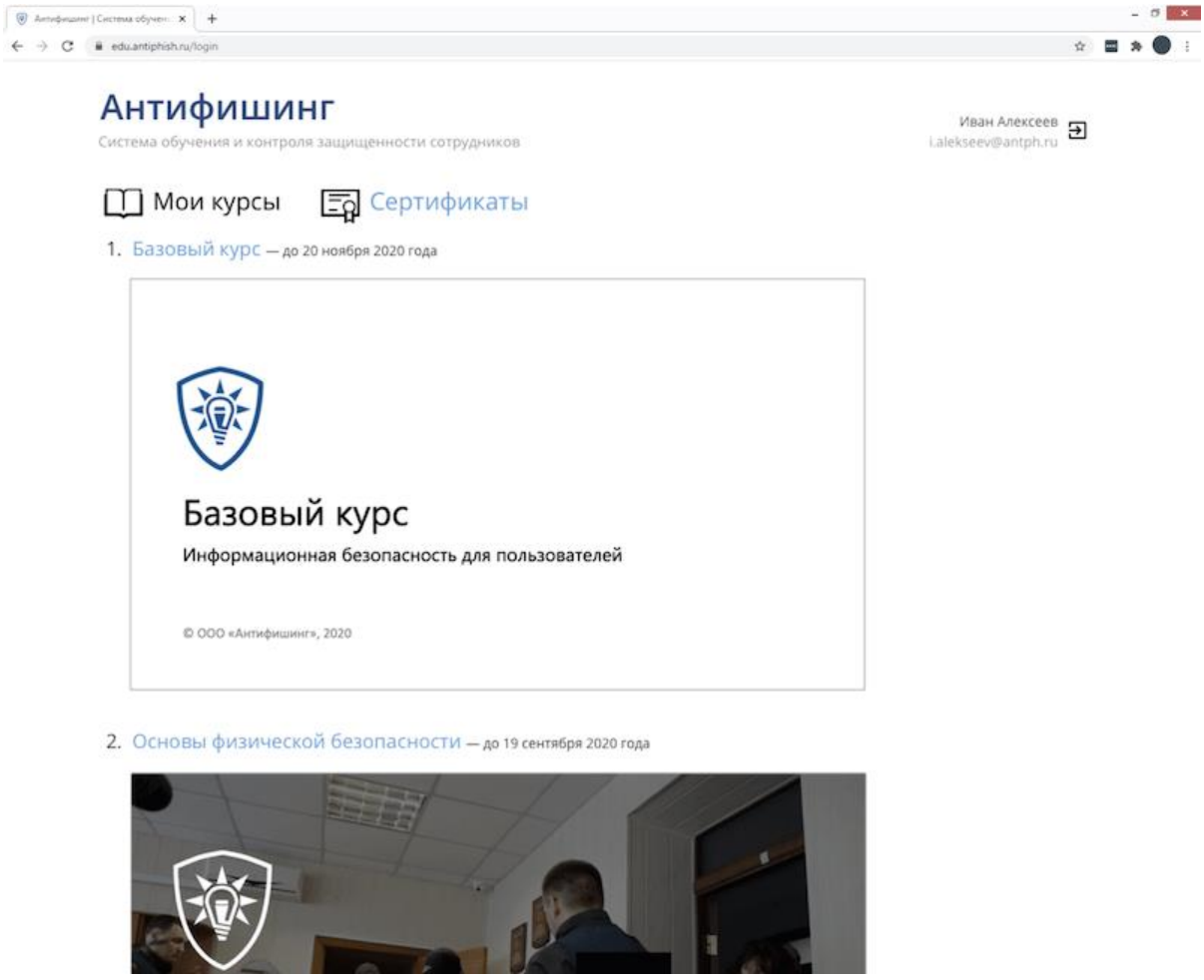

Рисунок 24. Раздел обучения

Часть курсов может быть доступной для самостоятельного изучения и будет отображаться без установленного срока прохождения.

Каждый курс состоит из теории и обязательного тестирования.

По большей части материал подаётся в виде жизненных случаев – примеров реальных ситуаций и атак, которые могут встретиться сотруднику, и конкретных практических рекомендаций о том, как действовать в этих ситуациях.

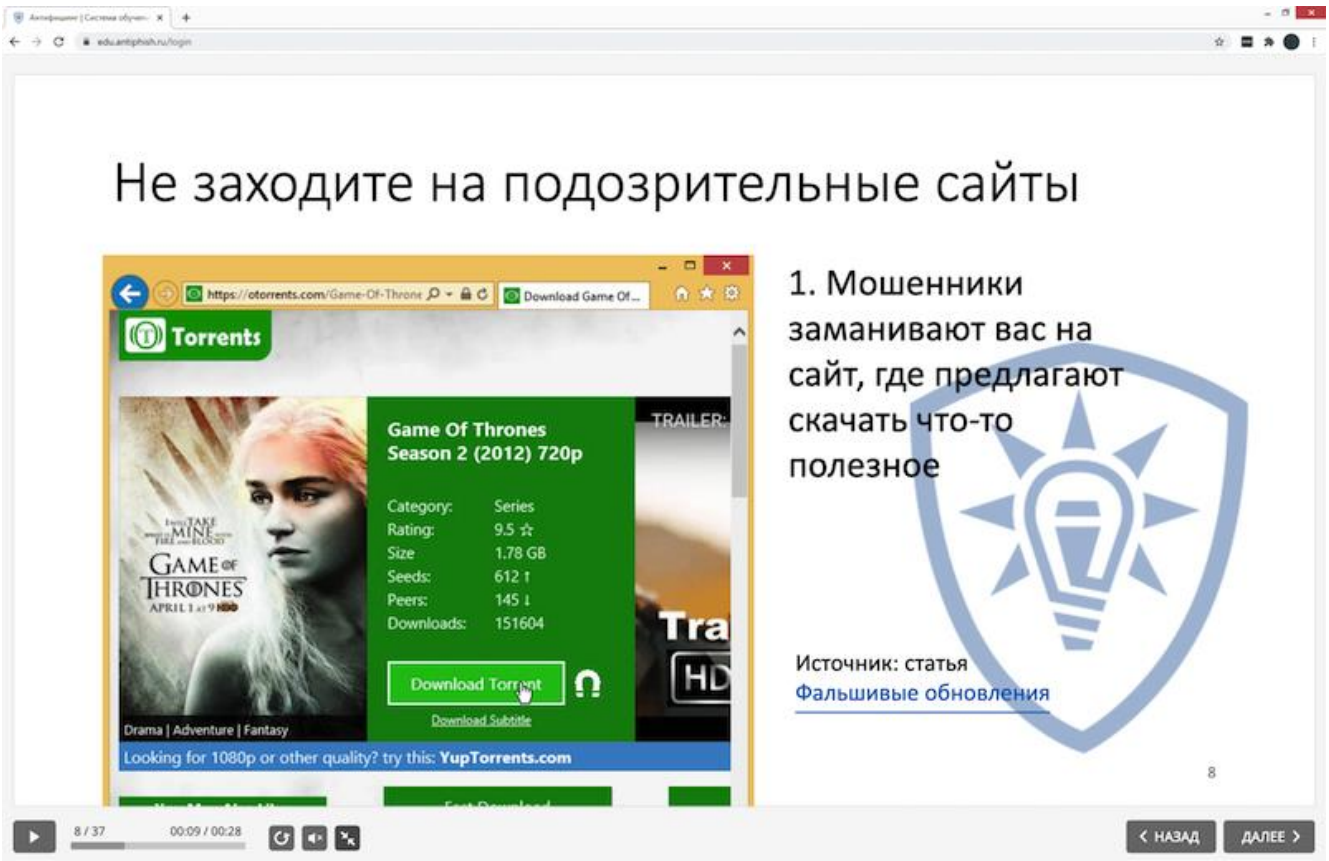

Рисунок 25. Слайд из курса «Безопасная работа в интернете и с электронной почтой»

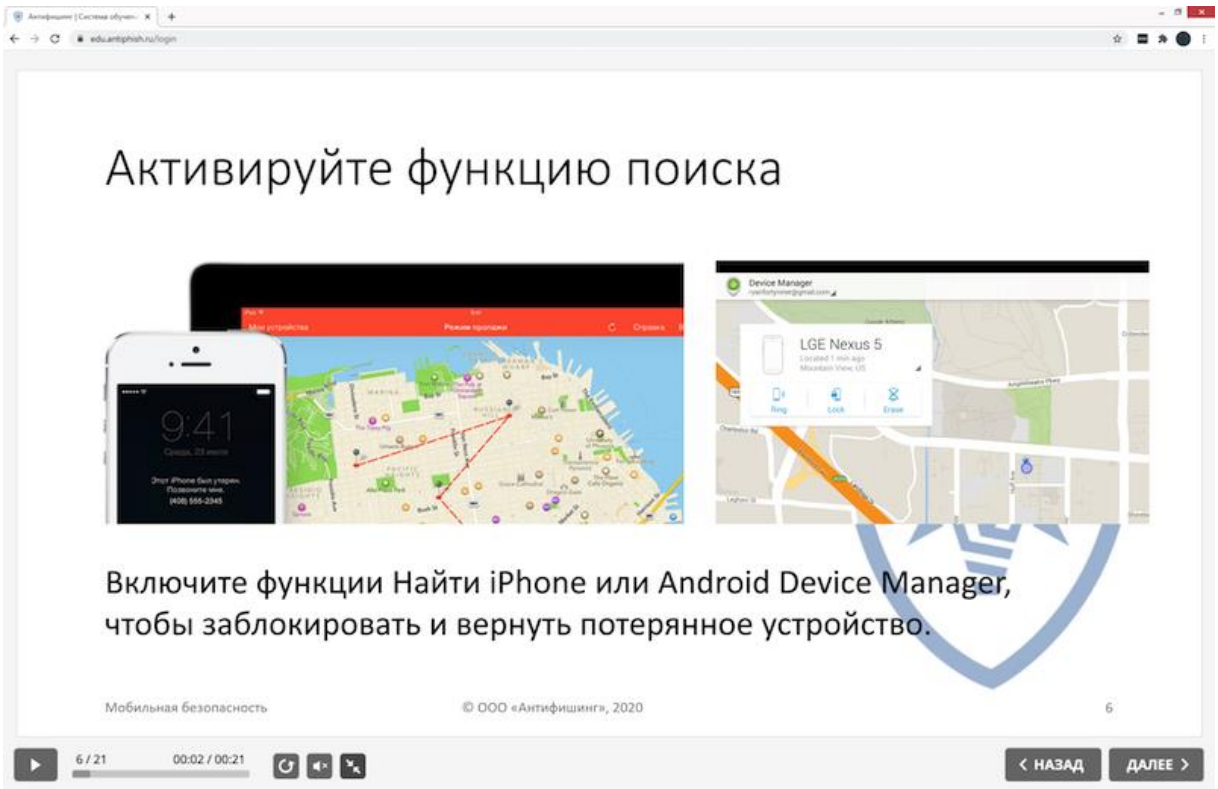

Рисунок 26. Слайд из курса обучения «Мобильная безопасность»

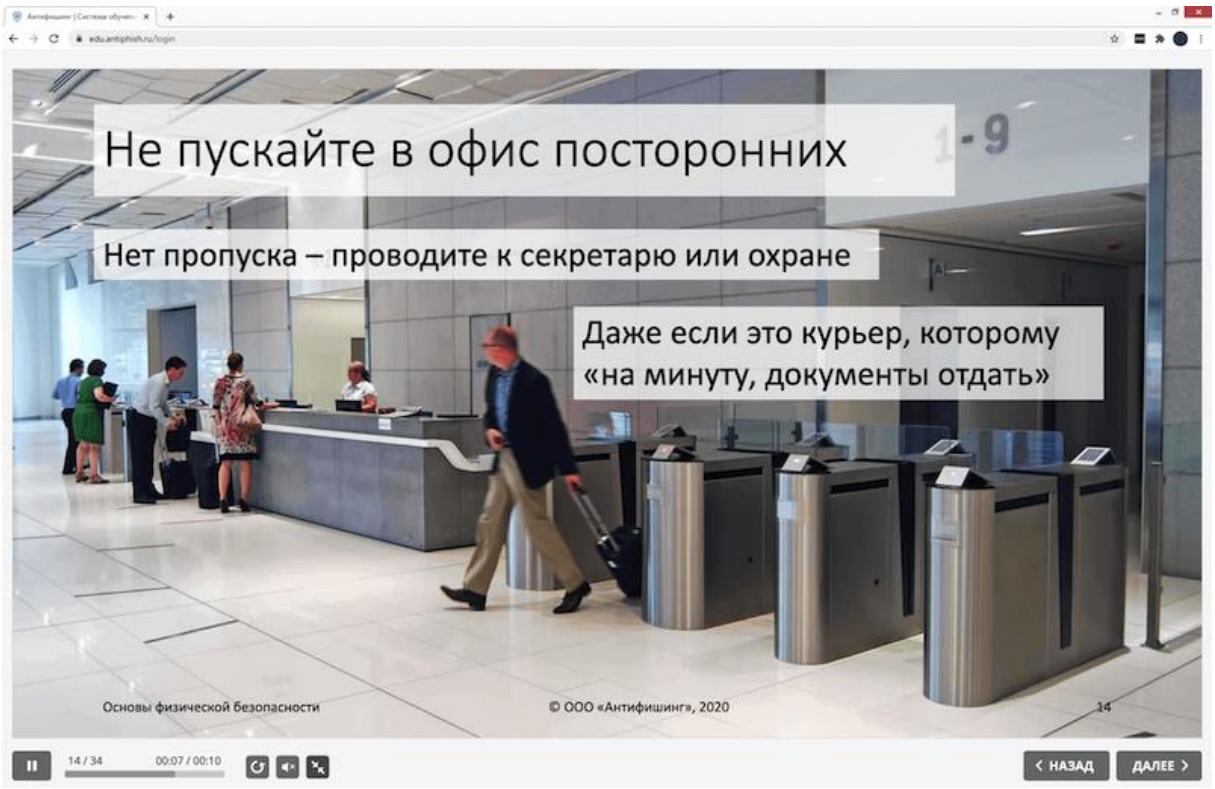

Рисунок 27. Слайд из курса обучения «Физическая безопасность»

Примеры слайдов из курсов обучения Системы приведены на рис. 25-27.

Вторая часть каждого курса представляет собой обязательный тест (рис. 28), в котором необходимо набрать проходной балл для того, чтобы курс был засчитан как пройденный.

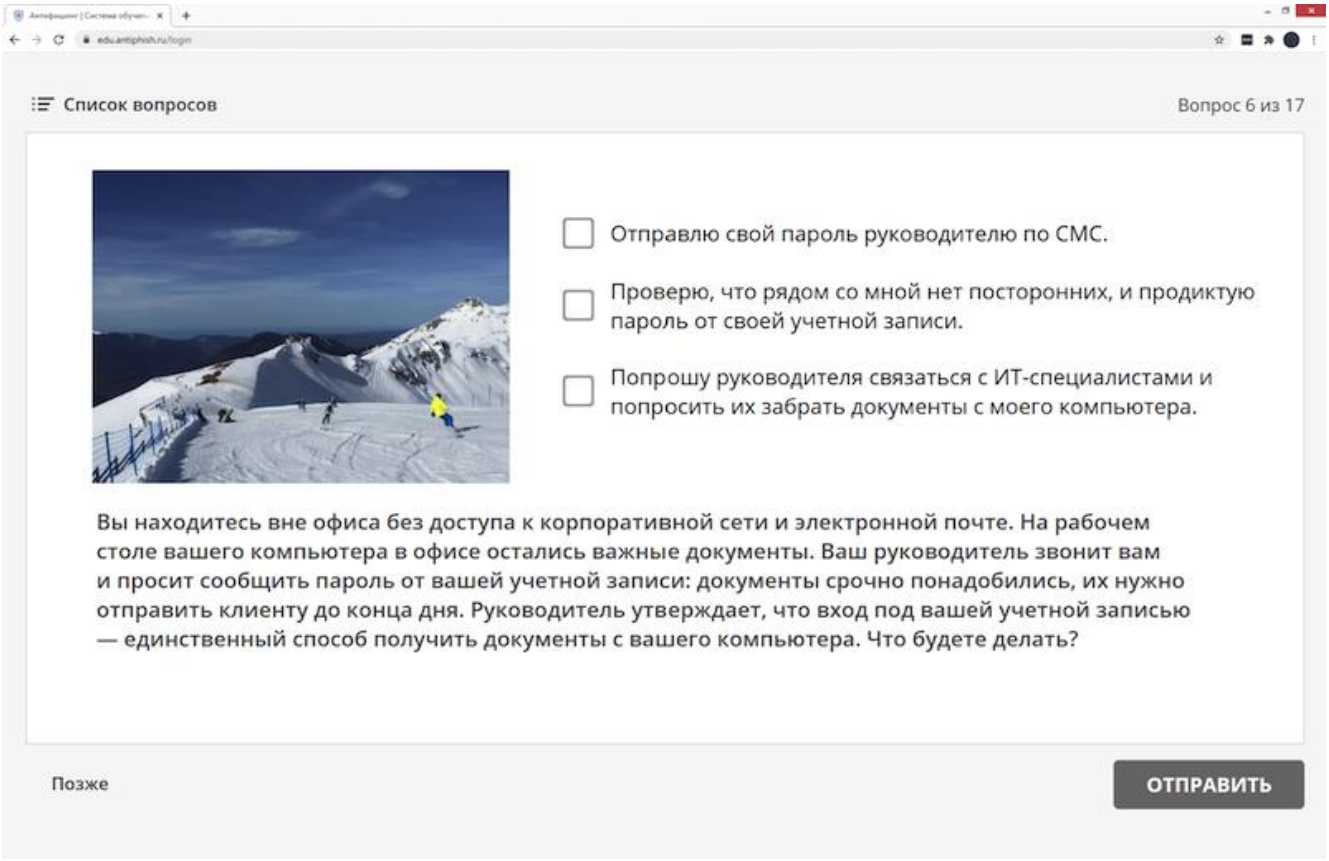

Рисунок 28. Прохождение теста после изучения курса

Все тесты также построены на кейсах — реальных ситуациях, в которых может оказаться сотрудник, и предлагают выбрать правильный вариант действий.

После успешного прохождения обучения каждому сотруднику автоматически выдается сертификат (рис. 29).

Настоящим удостоверяется, что сотрудник:

Иванов Сергей Петрович

прошел обучение и успешно сдал итоговое тестирование по курсу
Базовый курс по информационной безопасности

Общий балл за курс: 93 из 100

Балл за тест: 87 из 100

Сертификат действителен до: 31 декабря 2020 года.

Рисунок 29. Сертификат об успешном прохождении курса

Система предоставляет возможность оформлять сертификаты в соответствие с корпоративным брендбуком.

QR-код на сертификате позволяет проверить актуальность действующего сертификата (если сотрудник допустил нарушения, то его могут назначать на повторное обучение, а старые результаты в таком случае станут недействительными).

В Системе доступны следующие учебные курсы:

- Базовый курс по безопасности;
- Безопасная работа в интернете и с почтой;
- Мобильная безопасность;
- Физическая безопасность;
- Безопасная удалённая работа.

Производитель намеренно не создаёт множества курсов – компактно упакованные знания позволяют не перегружать сотрудников, тратить на обучение оптимальное время.

«Антифишинг» может интегрироваться с внешними системами обучения – «ВебТьютор» и Moodle (рис. 30).

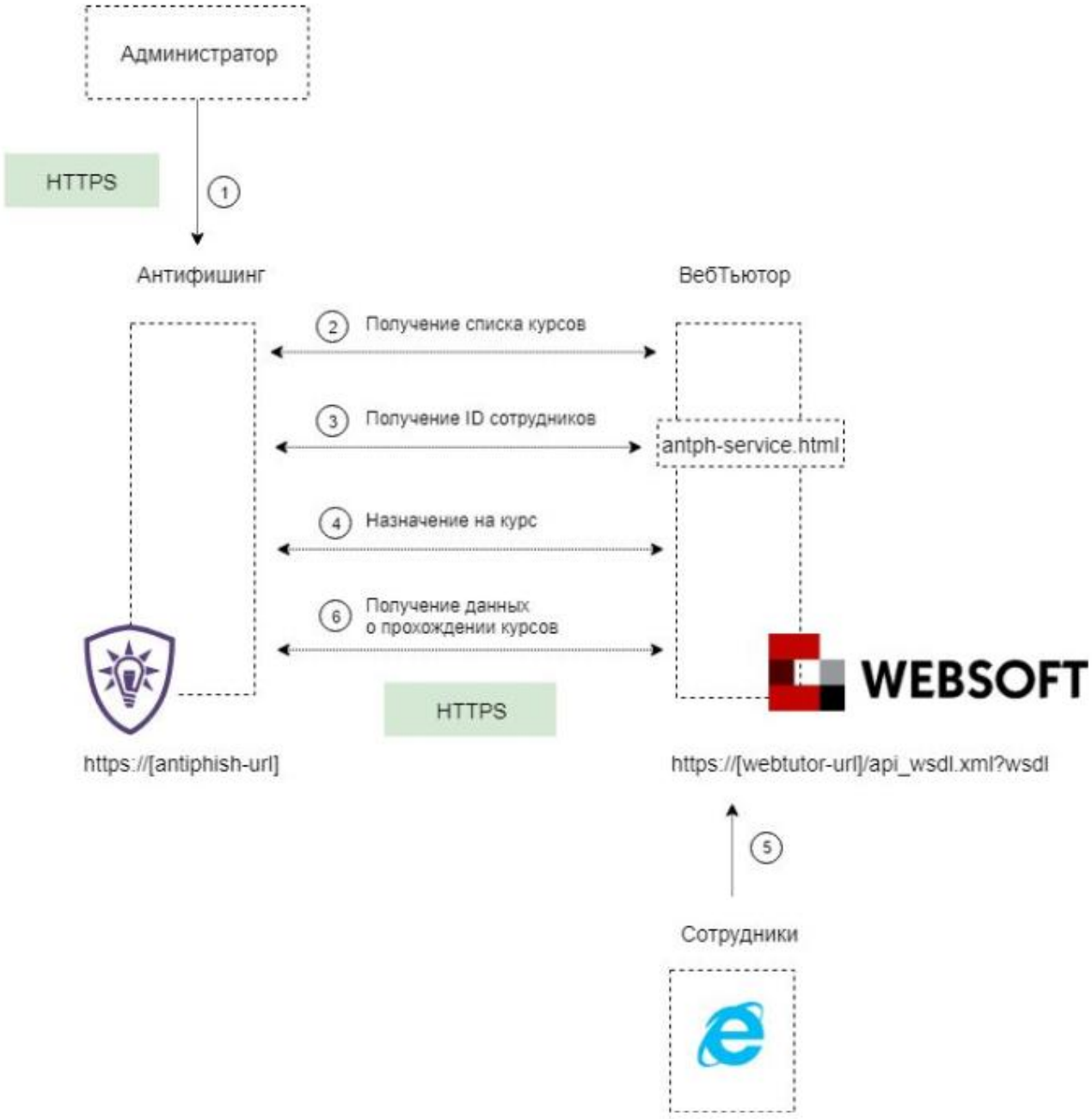

Рисунок 30. Схема интеграции «Антифишинга» с внешними системами обучения

При такой интеграции курсы «Антифишинга» поставляются в систему обучения в формате SCORM, сотрудники проходят обучение в привычной им среде, а вся статистика и управление процессом остаются в «Антифишинге».

13. Работа со статистикой и отчётами

Ключевые показатели защищённости всегда доступны на панели мониторинга (рис. 31).

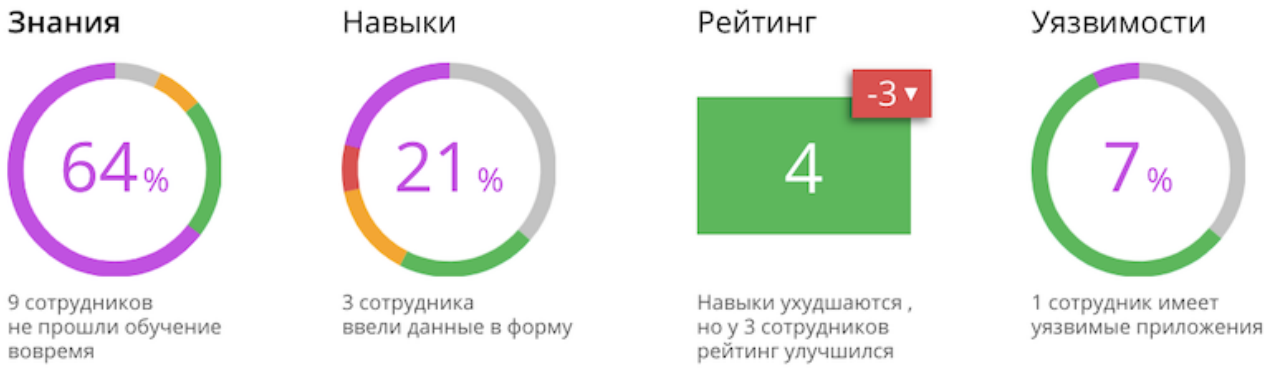

Рисунок 31. Отображение ключевых показателей на панели мониторинга

Расшифровку обозначения каждого сектора можно увидеть при наведении курсора мыши. Статистика по сектору отображается при нажатии на него (рис.32).

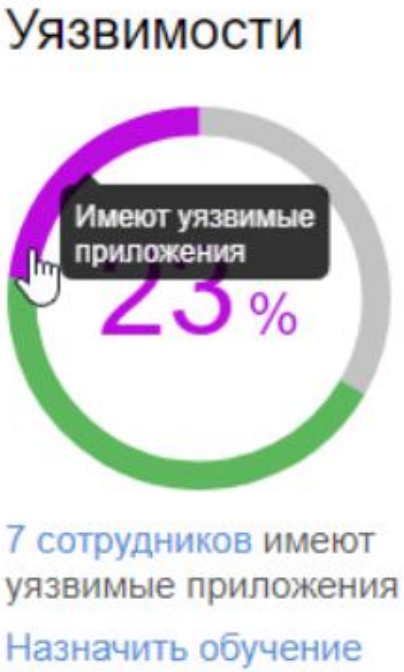

Рисунок 32. Отображение статистики по сектору «Уязвимости»

При нажатии на ссылку информация по соответствующим сотрудникам будет показана в таблице целей. Прямо из панели мониторинга можно выбрать и отправить сотрудников на обучение или проверить их навыки.

Помимо этого, в Системе реализованы возможности по созданию различных отчётов и выгрузке журналов по широкому спектру действий и событий.

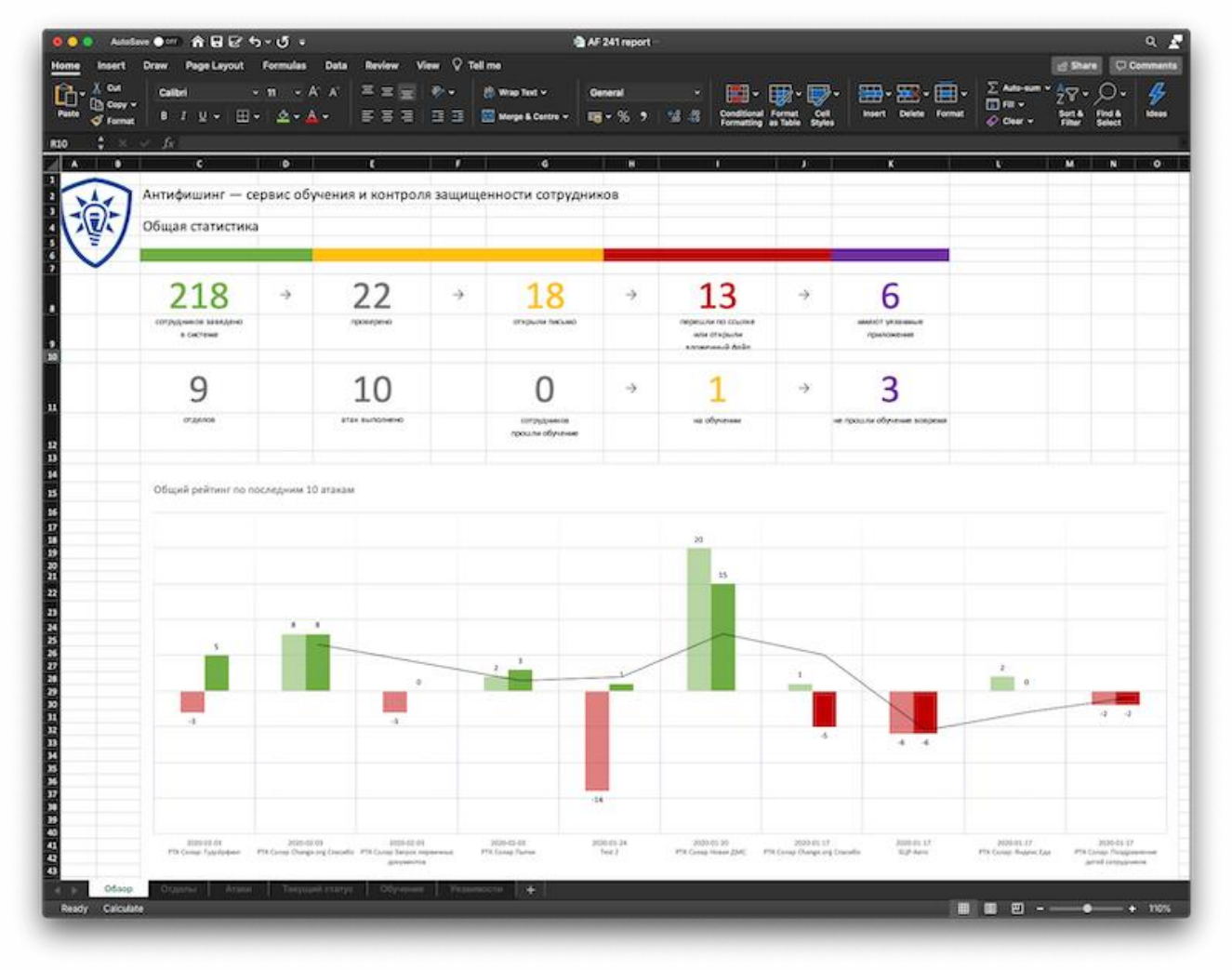

Рисунок 33. Пример главного отчёта

Главный отчёт (рис. 33) содержит общую статистику:

- общее количество сотрудников, отделов — графики и наглядные представления трендов;
- общее количество сотрудников, которые находятся на обучении, прошли его, не прошли вовремя;
- общее количество проведённых атак с информацией о том, сколько сотрудников прошли атаку и с каким результатом;
- количество выполненных атак;
- количество сотрудников, на устройствах которых имеются уязвимости, перечень брешей и степень их серьёзности.

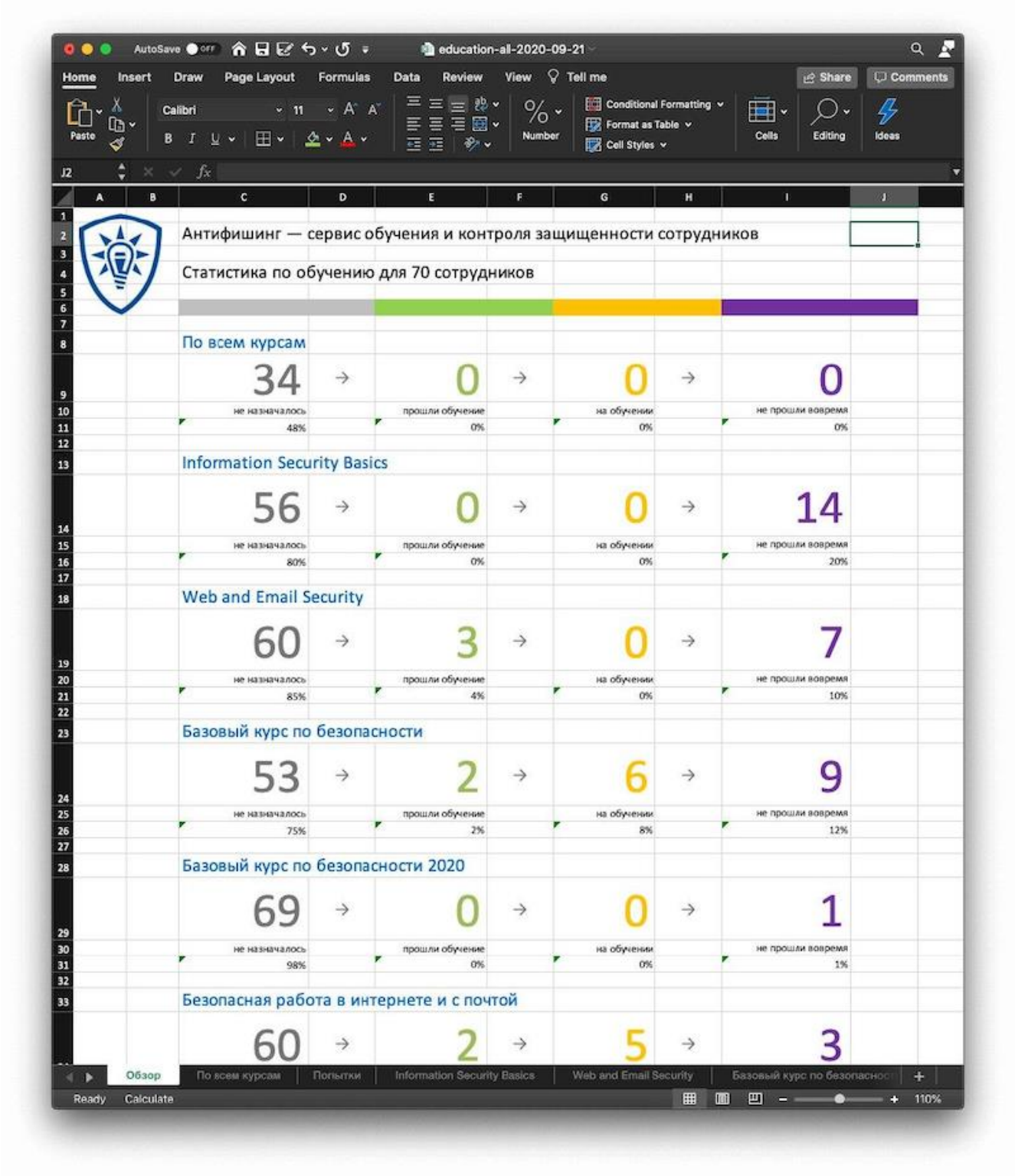

Рисунок 34. Пример отчёта по обучению

Отчёт по обучению (рис. 34) содержит полную статистику по курсам и сотрудникам, которые их проходят:

- статусы по курсу: «прошёл» / «не прошёл» / «отменено»;
- сколько попыток было по каждому курсу;
- детальная отчётность по каждому курсу.

Другие отчёты и журналы действий помогают увидеть всю прочую статистику по процессам в Системе в разных разрезах.

Все журналы и отчёты могут импортироваться в SIEM-систему по протоколу Syslog.

Указанной возможностью пользуются заказчики, которые проводят корреляцию событий из области безопасности, в том числе на основе уровня знаний и поведения сотрудников в имитированных атаках.

Все данные из Системы доступны через API для любых внешних систем, таких, например, как IDM, IRP/SOAR.

Тот же API позволяет управлять процессами из SGRC-решений, таких, например, как R-Vision SGRC.