

Симуляция фишинговых атак как метод повышения киберграмотности и подготовки к реагированию на угрозы

Дмитрий Станиславович Ан

Студент

Тихоокеанский государственный университет

Хабаровск, Россия

2019100305@togudv.ru

ORCID 0000-0000-0000-0000

Анна Сергеевна Зуфарова

Старший преподаватель кафедры Математических методов защиты информации и компьютерной безопасности

Тихоокеанский государственный университет

Хабаровск, Россия

006694@togudv.ru

ORCID 0000-0000-0000-0000

Поступила в редакцию 10.04.2025

Принята 30.05.2025

Опубликована 30.06.2025

УДК 004.052.6

DOI 10.25726/b2476-6563-8129-i

EDN ZBCSVM

БАК 5.8.1. Общая педагогика, история педагогики и образования (педагогические науки)

OECD 05.03.HA. EDUCATION & EDUCATIONAL RESEARCH

Аннотация

Несмотря на наличие современных технологий защиты, успешность атак часто зависит от уровня подготовки сотрудников. Неправильное поведение при столкновении с киберугрозами может привести к серьезным последствиям, таким как утечка данных или нарушение работы организации. Фишинговые атаки являются одной из наиболее распространенных угроз кибербезопасности. Они представляют собой попытку обмануть пользователей с целью получения конфиденциальной информации, такой как пароли, данные банковских карт, «секретная» информация и другая личная информация. Повышение киберграмотности сотрудников является ключевым элементом защиты от фишинга. Один из эффективных методов повышения осведомленности – проведение симуляций фишинговых атак. Симуляция фишинговых атак – это эффективный метод повышения киберграмотности сотрудников и подготовки их к реагированию на реальные угрозы. Этот подход позволяет имитировать атаки, которые могут произойти в реальной жизни, и дает возможность сотрудникам тренироваться в безопасной среде, что способствует развитию необходимых навыков и повышению осведомленности о рисках. Цель данного исследования заключается в изучении эффективности симуляции фишинговых атак, как метода повышения уровня киберграмотности и подготовки сотрудников к реагированию на реальные угрозы. Мы рассмотрим основные аспекты проведения таких симуляций, их влияние на поведение пользователей и возможные улучшения в процессе обучения. Произведем сравнительный анализ существующих обучающих платформ. Рассмотрим алгоритм проведения симуляций атак и выделим основные цели и задачи симуляций атак с помощью реально эксперимента, проведенного на фирме. Обозначим педагогическую ценность симуляций фишинговых атак.

Ключевые слова

социальная инженерия, симуляция фишинговых атак, обучение, безопасность, e-mail рассылки, письма, обучающие платформы.

Введение

В современном мире информационные технологии занимают центральное место в деятельности организаций, государств и частных лиц. Цифровая трансформация бизнеса и широкое распространение интернета привели к тому, что информация стала одним из самых ценных ресурсов. Однако с ростом зависимости от технологий также увеличивается количество угроз, связанных с кибербезопасностью. Одной из наиболее опасных и распространенных угроз является социальная инженерия. С 2022 года Россия остается самой атакуемой страной в мире, становясь основной целью для хакеров (Другач, 2024). Новые угрозы и тактики злоумышленников ставят под удар компании, госсектор и обычных пользователей.

Актуальность темы работы обусловлена растущим числом инцидентов, связанных с атаками социальной инженерии, которые становятся все более изощренными и сложно обнаружимыми. Согласно исследованиям, более 70% успешных кибератак связаны с использованием методов социальной инженерии (Иванов, 2020).

Симуляции атак выступают эффективным инструментом обучения, который помогает моделировать реальные сценарии и отрабатывать на практике действия при выявлении угроз. Такой подход не только выявляет слабые звенья в компании, но и позволяет сотрудникам развивать устойчивость к различным видам социальной инженерии.

Проведение симуляций позволяет организациям оценить текущий уровень осведомленности, своевременно выявить уязвимости и предложить меры по их устранению. Этот метод сочетает теоретическое обучение с практическими навыками, что делает его ключевым элементом в построении системы защиты от социальной инженерии.

Материалы и методы исследования

Существует множество реальных успешных практик в образовательном процессе по симуляции атак. «CyberPatriot» международная программа организует соревнования по кибербезопасности, где команды школьников решают задачи, связанные с защитой сетей и обнаружением уязвимостей, включая фишинговые атаки. Проект «No More Ransom», это совместная инициатива правоохранительных органов и частных компаний, направленная на борьбу с программами-вымогателями. В рамках проекта проводится обучение и распространение учебных материалов, включая симуляции фишинговых атак. «Simulated Phishing Attacks in Schools», школы проводят регулярные симуляции фишинговых атак, чтобы повысить уровень кибербезопасности среди учащихся и сотрудников. Результаты симуляций используются для разработки рекомендаций и учебных курсов (Ефимов, 2024).

В России существует множество обучающих платформ по информационной безопасности включая и симуляцию фишинговых атак, например Phishman, Secure-T, StartX, StopPhish. Эти обучающие платформы помогают обучать персонал фирм, организаций в сфере информационной безопасности, в частности социальной инженерии.

Результаты и обсуждение

Симуляции атак представляют собой практический инструмент, направленный на имитацию реальных угроз информационной безопасности для проверки готовности сотрудников и уровня их осведомленности о киберугрозах. Этот подход основан на создании реалистичных сценариев кибератак, которые включают фишинг, вишинг, смишинг и другие методы социальной инженерии.

Симуляции позволяют выявить слабые места в поведении сотрудников и организационных процессах, а также способствуют формированию навыков и привычек, необходимых для противодействия угрозам. Особенностью симуляций является их проведение в условиях, максимально

приближенных к реальным, что исключает формальность обучения и стимулирует сотрудников к внимательности и ответственному отношению к информационной безопасности (Другач, 2024).

Нами был произведен сравнительный анализ обучающих платформ для борьбы с фишингом. Обучение сотрудников является важнейшим элементом защиты от киберугроз. Современные вызовы требуют комплексного подхода, включающего разработку специализированных программ, использование интерактивных методов обучения и регулярное обновление учебных материалов. Вовлечение руководства, формирование культуры безопасности и международное сотрудничество способствуют повышению эффективности обучения и снижению рисков.

Security Awareness (осведомленность в области безопасности) – это важный компонент комплексной стратегии информационной безопасности, направленный на обучение сотрудников правилам и практикам защиты данных. В России существует ряд платформ, которые помогают организациям развивать культуру безопасности и повышать осведомленность сотрудников о киберугрозах. Так же большинство компаний разрабатывают свою комплексы (Козлова, 2019).

Для повышения осведомленности сотрудников воспользуемся готовой обучающей платформой. Однако, прежде чем сделать выбор, необходимо провести тщательный анализ существующих решений, чтобы определить наиболее подходящую и эффективную платформу для нашей организации. Рассмотрим следующие платформы, которые нужны для нашего исследования Phishman, Secure-T, StartX, StopPhish.

Phishman – эта платформа подходит для организаций различного масштаба и отраслевой принадлежности, стремящихся повысить уровень подготовки сотрудников в вопросах распознавания и предотвращения различных форм социальной инженерии. Помимо традиционных фишинговых рассылок, Phishman способен моделировать более сложные формы атак, такие как vishing (телефонная социальная инженерия), spear phishing (таргетированные фишинговые атаки) и атаки через социальные сети. Важной особенностью является возможность адаптации учебных сценариев под конкретные потребности компании, включая выбор тематик, персонализацию сообщений и определение целевой аудитории среди сотрудников. Достоинства Phishman заключаются в широком диапазоне симулируемых угроз и высокой степени гибкости настроек сценариев (рис. 1).

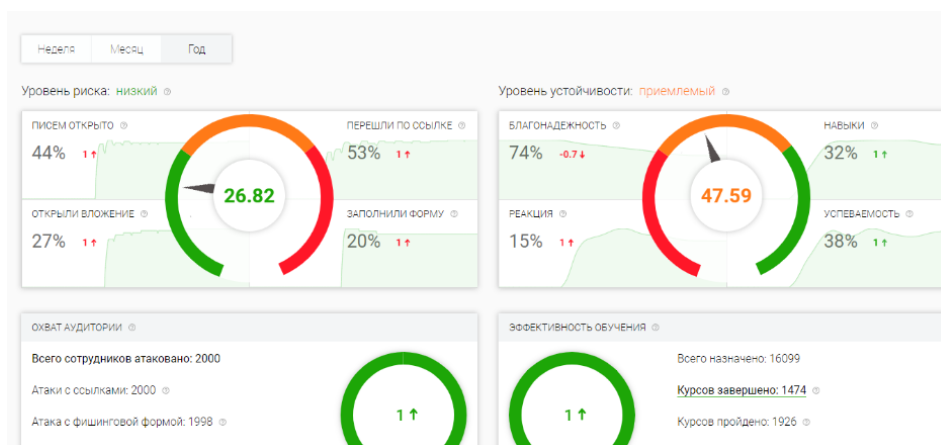


Рисунок 1. Платформа Phishman

Обучающая платформа Secure-T, ориентирована на обучение сотрудников преимущественно методам противодействия фишинговым атакам. Secure-T акцентирует внимание на имитации различных сценариев фишинга, включая фальшивые электронные письма и вредоносные веб-ресурсы. Платформа предоставляет широкие возможности для кастомизации учебного контента и проведения тестов, учитывающих специфику бизнеса клиента. Ключевыми преимуществами Secure-T являются простота интерфейса и наличие эффективных инструментов мониторинга прогресса пользователей (рис. 2).

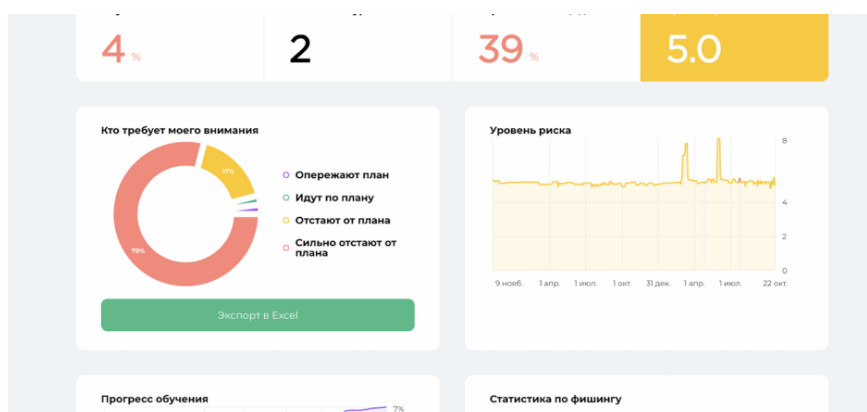


Рисунок 2. Платформа Secure-T

Платформа StartX предназначена для организаций любых масштабов, заинтересованных в повышении устойчивости сотрудников к различным видам фишинга и социальной инженерии. StartX предлагает симуляции фишинговых атак, а также тестирование на устойчивость к другим видам социальной инженерии, таким как телефонные мошенничества. Платформу отличает высокая степень адаптивности сценариев обучения и тестирования, что делает ее удобной для реализации индивидуальных требований заказчиков. Среди преимуществ StartX стоит отметить удобный интерфейс и высокую гибкость настроек (рис. 3).

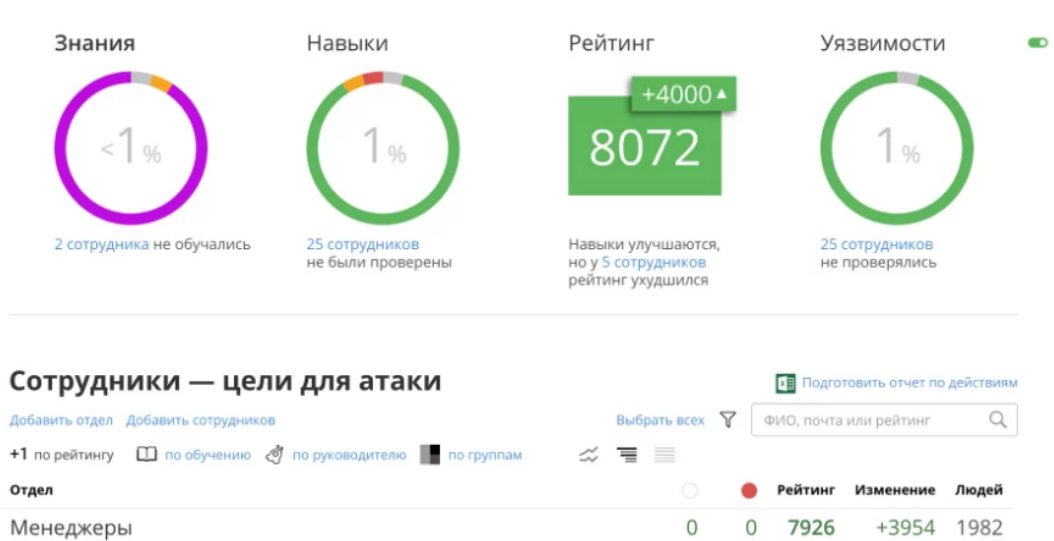


Рисунок 3. Платформа StartX

StopPhish, особенно полезна для компаний, которые хотят сосредоточиться на обучении сотрудников по распознаванию и предотвращению фишинговых атак. Платформа специализируется на симуляциях фишинговых атак с широким спектром сценариев, включая электронные письма, веб-сайты и сообщения в социальных сетях, и позволяет настраивать сценарии атак в соответствии с потребностями организации, включая выбор тематики и создание персонализированных сообщений.

Преимущества StopPhish – это простота в использовании и эффективные методы обучения (рис. 4).

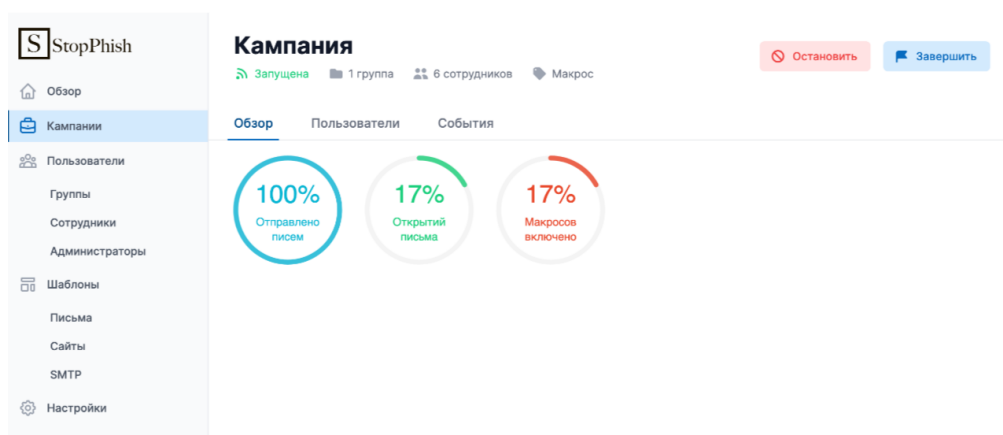


Рисунок 4.1 Платформа StopPhish

StopPhish была выбрана как наиболее подходящая платформа для обучения сотрудников благодаря ее узкой специализации на фишинговых атаках, простом использовании и гибкости. Платформа предлагает широкий спектр сценариев, включая имитации атак через электронную почту, веб-сайты и социальные сети, что полностью охватывает ключевые угрозы для обучения сотрудников, а также эффективные методы обучения и аналитические инструменты позволяют не только повышать осведомленность сотрудников, но и оперативно выявлять уязвимости. С учетом высокого качества функционала и доступной стоимости StopPhish стала оптимальным выбором.

Рассмотрим алгоритм проведения симуляций атак.

1. Разработка реалистичных сценариев. Основой эффективной симуляции является создание сценариев, которые соответствуют реальным угрозам, с которыми может столкнуться организация. Например, сотрудникам может быть отправлено электронное письмо от имени «службы IT-поддержки» с просьбой подтвердить данные для обновления доступа. Разработка индивидуальных сценарии тестовой атаки с учетом специфики исследуемой компании представлена на рисунке 5 или можно воспользоваться генератором сценариев (рис. 6). В первую очередь идет сбор нужных данных для атаки (происходит разведка, OSINT). Можно использовать различные другие инструменты поиска информации. Собирают: доменные почту сотрудников, социальные сети, хобби, интересы, доверенные ресурсы компании и многое другое (Прохоров, 2023). После сбора актуальных данных, происходит обработка и анализ данных. Вырабатывается нужная стратегия для обучения и запускается фишинговая кампания.

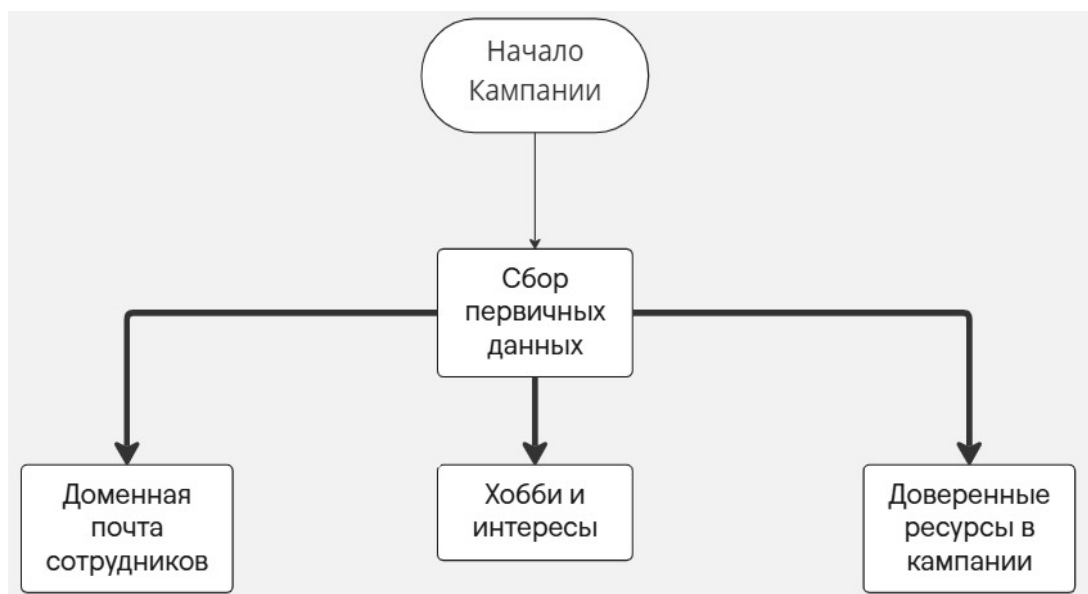


Рисунок 5. Разработка фишинговых сценариев

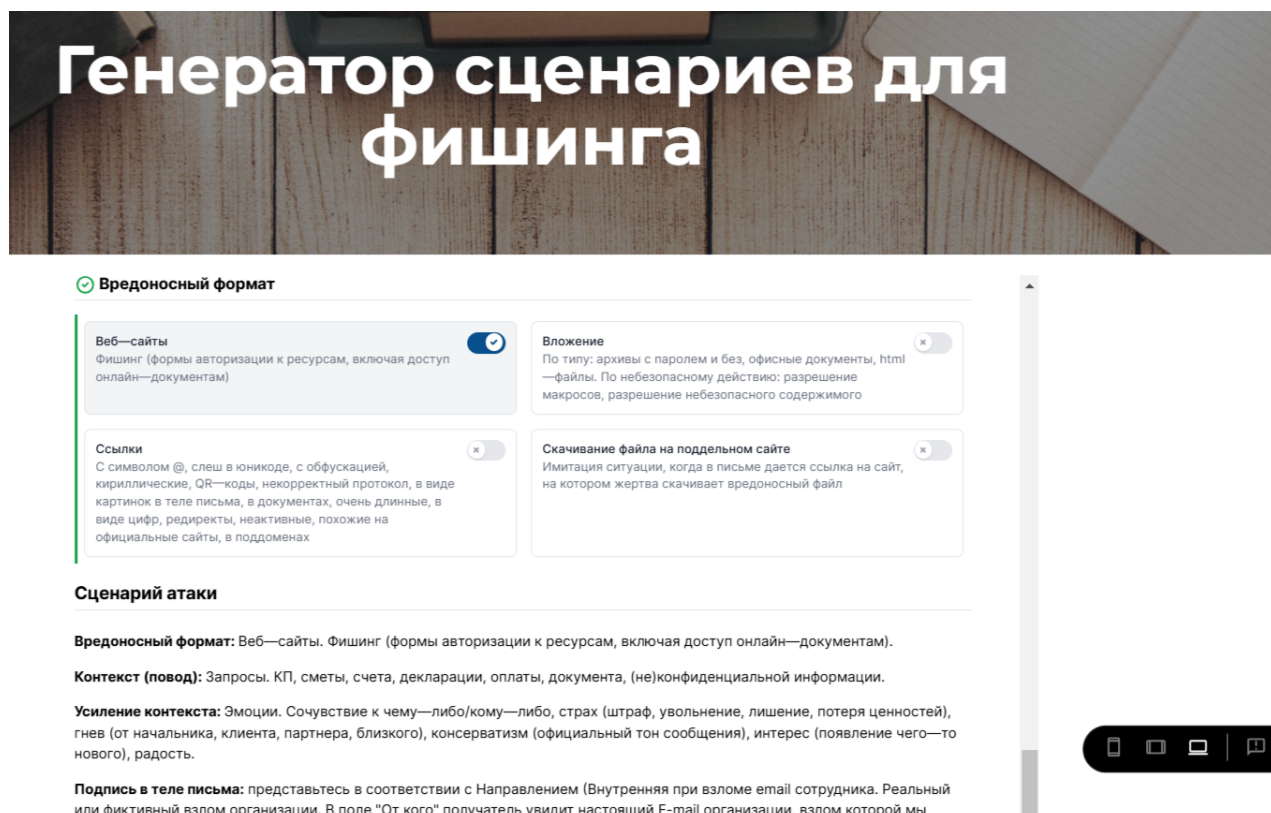


Рисунок 6. Генератор сценариев

2. Проведение обучающей симуляции. Сценарий разворачивается в контролируемой среде, а сотрудники взаимодействуют с ним без предварительного уведомления. Это позволяет объективно оценить их реакцию (Бачиева, 2017). Например, при симуляции вишинга сотруднику может поступить звонок от якобы «банковского сотрудника», запрашивающего данные учетной записи. Можно сгенерировать фишинговый сайт и отправить ссылку на него в электронном письме создать разнообразные вложения для электронных писем (файл pdf, макросы, QR коды и другое). Запуск учебной фишинговой кампании представлен на рисунке 7.

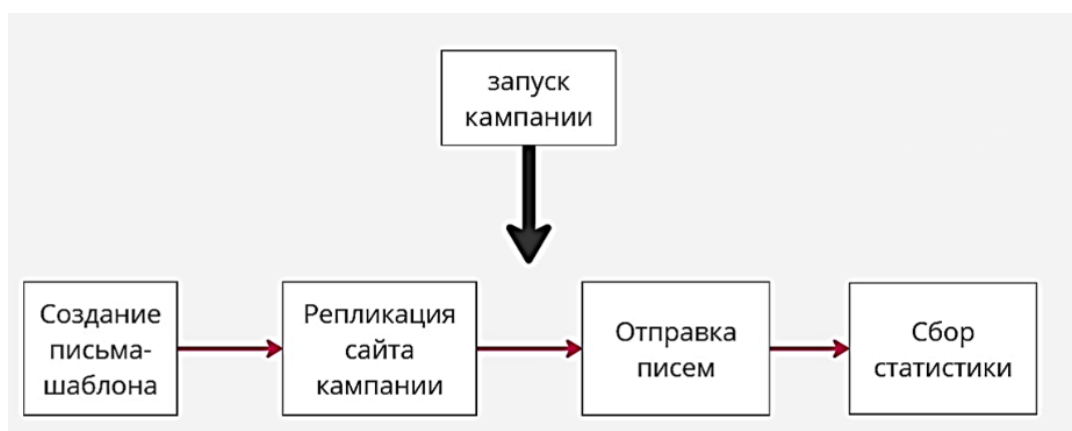


Рисунок 7. Запуск кампании

3. Анализ поведения сотрудников. На этапе анализа фиксируются все действия участников: открытие писем, переходы по подозрительным ссылкам, ввод конфиденциальных данных, реакция на

телефонные звонки и сообщения (Васильева, 2020). Эти данные позволяют определить основные ошибки и уровень готовности сотрудников.

4. Обратная связь и обучение. После завершения симуляции сотрудники получают разъяснения, что они сделали правильно, а где допустили ошибки. Происходит работа над ошибками. Этот этап сопровождается рекомендациями и дополнительным обучением. Например, сотруднику объясняется, как проверить подлинность адреса электронной почты отправителя или распознать подозрительные признаки запроса.

На основе этого алгоритма был проведен эксперимент в хабаровской фирме по продаже цветов. Продукция поставляется как через собственные розничные магазины, так и онлайн-платформу.

Был произведен анализ фирмы с точки зрения информационной безопасности. Рассмотрены уязвимости компании по социальной инженерии: рабочая электронная почта, социальные сети, мессенджеры, телефонные звонки (Захарова, 2022).

После тщательного анализа особенностей деятельности компании и изучения ее ключевых направлений, были разработаны фишинговые сообщения, которые максимально соответствуют интересам и специфике фирмы. В основе составленных писем лежали темы, напрямую связанные с деятельностью компании, что позволяло сделать сообщения более убедительными и убедить сотрудников в их подлинности.

На первом этапе исследования была проведена проверка, целью которой являлось выявление уровня кибербезопасности среди сотрудников компании и их способности распознавать потенциально опасные фишинговые письма. Для достижения этой цели была реализована симуляция, заключающаяся в отправке поддельных фишинговых сообщений.

Эти сообщения были специально составлены так, чтобы имитировать реальные угрозы, с которыми сотрудники могут столкнуться в своей профессиональной деятельности (Абитов, 2020). Письма были разосланы представителям различных отделов компании, включая руководителей, бухгалтеров, курьеров и флористов. Такой выбор был сделан для того, чтобы охватить широкий спектр сотрудников, выполняющих разнообразные функции, и проанализировать их реакцию на подозрительные электронные письма.

Рассылкой фишинговых сообщений занималась специализированная платформа StopPhish, которая позволяет моделировать реальные сценарии угроз и отслеживать поведение пользователей, составляя отчеты данных, которые можно легко выгружать (рис. 8).

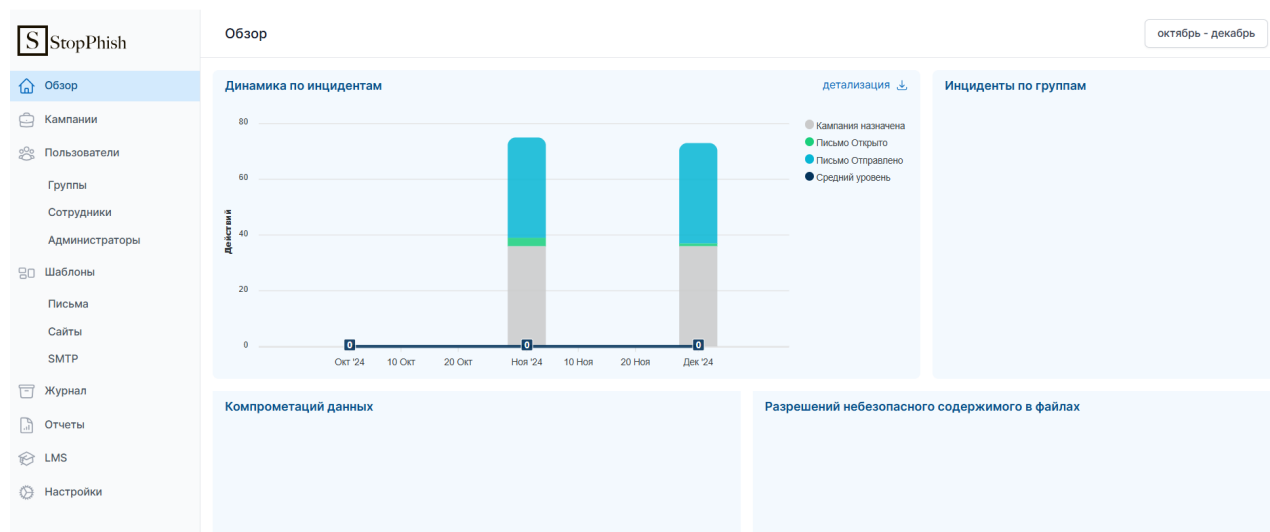


Рисунок 8. Запуск фишинговых кампаний

После рассылки писем начался этап анализа. Особое внимание уделялось тому, открывались ли сообщения сотрудниками и переходили ли они по ссылкам, содержащимся в этих письмах [9]. Эта информация позволила оценить степень осведомленности сотрудников о киберугрозах, их бдительность

и готовность противостоять подобным атакам. Низкие показатели первой симуляции подчеркивают необходимость внедрения обучения. Итоги анализа стали основным фактором для дальнейших мер повышения уровня кибербезопасности от социальной инженерии внутри компании. Для достижения этой цели были тщательно проанализированы доступные подходы к обучению сотрудников, и в результате выбраны методы, которые сочетают в себе информативность и удобство применения. Основное внимание было уделено созданию образовательной программы, которая будет понятной и доступной для всех сотрудников, вне зависимости от их должности и уровня подготовки (Вилкова, 2020).

Одним из ключевых элементов этой программы стал вебинар, представляющий собой серию лекций, посвященных темам социальной инженерии и киберугроз (Нечипуровский, 2024). Этот формат был выбран из-за его гибкости и возможности охватить одновременно большое количество участников. На вебинаре сотрудники смогут получить не только теоретические знания, но и практические советы по выявлению и предотвращению фишинговых атак.

Дополнительно, чтобы информация оставалась перед глазами сотрудников в их повседневной работе, было решено разместить чек-листы на рабочих местах. Эти чек-листы содержат простые и понятные инструкции, которые помогут быстро проверить, является ли полученное электронное письмо или сообщение безопасным (Богданова, 2019). Таким образом, сотрудники смогут ежедневно обращаться к наглядным рекомендациям и закреплять полученные знания на практике.

Эти меры создают основу для формирования культуры кибербезопасности внутри компании, делая осведомленность о социальной инженерии частью повседневной работы каждого сотрудника.

Через две недели, после внедрения комплекса мер по повышению осведомленности сотрудников о киберугрозах, была проведена вторая симуляция фишинговой атаки. Основной целью данного этапа стало не только повторное тестирование уровня кибербезопасности в компании, но и оценка эффективности предпринятых ранее образовательных инициатив и других профилактических мероприятий.

Результаты второй симуляции продемонстрировали заметные улучшения. Большинство сотрудников стали гораздо более осторожны при работе с подозрительными электронными письмами, что выразилось в снижении числа случаев открытия фишинговых сообщений и переходов по вредоносным ссылкам (Яковлева, 2021). Такой результат свидетельствует о том, что образовательные меры, включающие проведение вебинаров и размещение чек-листов на рабочих местах, оказались действенными. На рисунке 9, представлены результаты двух фишинговых симуляций.

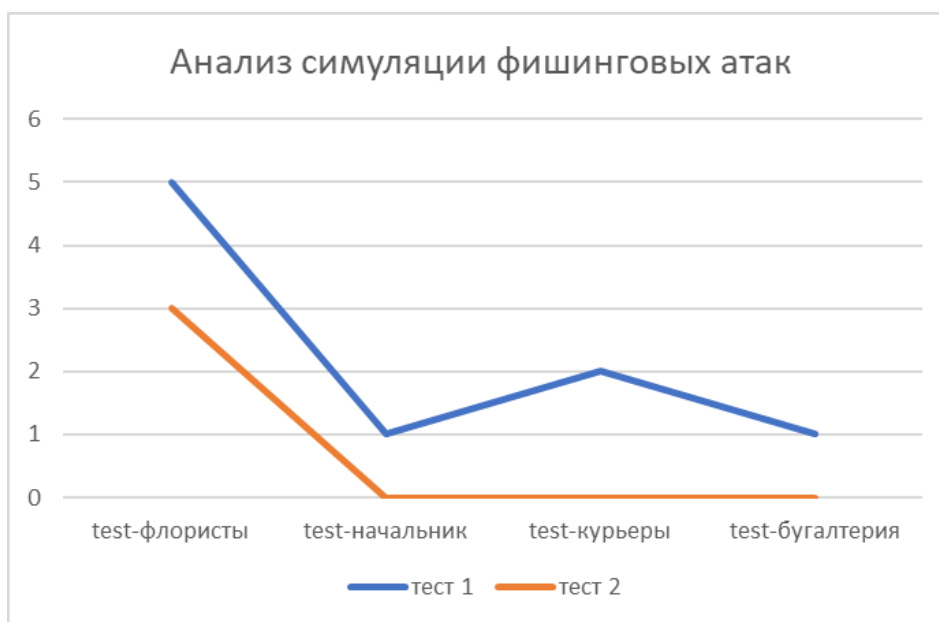


Рисунок 9. Сравнение результатов

Важно отметить, что участники вебинаров отмечали практическую пользу полученной информации, что способствовало более осознанному подходу к вопросам информационной безопасности. Чек-листы, размещенные на рабочих местах, также сыграли свою роль: они напоминали сотрудникам о ключевых правилах безопасности и помогали закрепить полученные знания в повседневной работе.

Из нашего исследования можно выделить основные цели и задачи симуляций атак.

На первом месте повышение осведомленности сотрудников (обучающихся). Фишинговая симуляция наглядно демонстрирует риски, связанные с невнимательностью или недостатком знаний в области информационной безопасности. Обучающие получают практический опыт распознавания угроз, что повышает их бдительность в реальных условиях. Благодаря фишинговым симуляциям, выявляются слабые места. Анализ результатов симуляции позволяет определить основные уязвимости, связанные с человеческим фактором, и скорректировать программы обучения и внутренние политики компании. Благодаря регулярным симуляциям сотрудники учатся правильно реагировать на подозрительные запросы, электронные письма и звонки (Штайгер, 2018). Это минимизирует вероятность успешной атаки. Так же, результаты симуляций показывают, насколько текущие обучающие программы, политики безопасности и технические меры соответствуют требованиям и актуальным угрозам.

Благодаря нашему эксперименту, выявили педагогическую ценность симуляций фишинговых атак.

1. Практический опыт, симуляция фишинговых атак позволяет учащимся получить реальный опыт взаимодействия с вредоносными сообщениями, что способствует лучшему пониманию механизмов мошенничества.

2. Развивает критическое мышления у обучающихся. Учащиеся учатся распознавать подозрительные элементы в электронных письмах и сообщениях, развивая навыки анализа и оценки информации.

3. Формирует культуру безопасности в организации. Регулярные тренировки помогают закрепить привычки безопасного поведения в интернете, такие как проверка отправителей сообщений и ссылок перед открытием (Зуфарова, 2024).

4. Фишинговые симуляции позволяют продемонстрировать последствия неправильных действий, стимулируя осознанный подход к защите личной информации, то есть обеспечивает повышение осведомленности в области социальной инженерии.

5. Поддержка междисциплинарного подхода. Работа с социальной инженерии включает в себя элементы информатики, информационной безопасности, юридические науки, психологии. Этот комплекс делает занятия интересными и полезными (Павлов, 2020).

6. Интерактивные форматы обучения, такие как симуляции, привлекают внимание учащихся и способствуют более глубокому усвоению материала. Появляется интерес к обучению, то есть мотивация.

7. Безопасный эксперимент, то есть учащиеся могут совершать ошибки в контролируемых условиях, что снижает риск реальных потерь и последствий. Обучающим не страшно делать ошибки, так как не будет потери конфиденциальной информации.

8. Происходит развитие коммуникативных навыков при анализе, поставленных задач в командной работе.

9. Преподаватели могут использовать результаты и анализ симуляций для создания учебных пособий и кейсов, которые будут полезны для дальнейшего обучения. Так же методы фишинга постоянно совершенствуются, регулярные симуляции помогают поддерживать актуальные знания и навыки учащихся (Козлова, 2019).

Заключение

Преимущества симуляций атак — это реализм, контроль безопасности, адаптация под угрозы, мотивация сотрудников. Сценарии адаптированы под реальную обстановку, что делает обучение практичным и наглядным. Симуляции проводятся в контролируемой среде, где все риски

минимизированы. Сценарии могут быть модифицированы в соответствии с новыми тенденциями в киберугрозах. Участие в симуляциях формирует у сотрудников более ответственное отношение к вопросам информационной безопасности.

У фишинговых симуляций есть три ключевые задачи: первая, это как обучающийся идентифицирует угрозу; вторая задача повышение кибербезопасности и третья создать рекомендации по реагированию на угрозы (Климов, 2019).

Не имеет значения, о каких компаниях идет речь – крупных холдингах или малых субъекта: в защите нуждаются все. Исследование профессора Стэнфордского университета установило: каждый четвертый нанятый работник когда-нибудь нажимал на фишинговое электронное письмо на рабочем месте (Сливинский, 2023).

Симуляция фишинговых атак представляет собой эффективный педагогический инструмент для повышения уровня киберграмотности и подготовки учащихся к реагированию на современные киберугрозы. Комплексный подход, включающий подготовку преподавателей, разработку учебных материалов и интеграцию симуляций в учебный процесс, обеспечивает долгосрочный эффект и способствует формированию устойчивых навыков безопасного поведения в цифровом пространстве (Ан, 2025).

Список литературы

1. Абитов А.А., Тхакахов Р.А., Хачмахова М.З., Сунгуров К.Ш. Защита от фишинга // В сборнике: Цифровая трансформация науки и образования // Сборник научных трудов. 2020. С. 13-17.
2. Ан Д.С., Зуфарова А.С. Влияние интерактивных тренингов на осведомленность сотрудников о фишинговых атаках // ЦИТИСЭ. 2025. № 1. С. 41-52.
3. Бачиева А.В., Бозиев Т.О. Фишинг как один из способов мошенничества в сфере компьютерной информации // В сборнике: Актуальные проблемы юридической науки и практики. 2017. Т. 1. С. 232-235.
4. Богданова Т.М. Повышение безопасности сотрудников через тренировки по фишинговым атакам. М.: РАН, 2019. 153 с.
5. Васильева Н.А. Методы защиты сотрудников от фишинговых атак: роль тренингов и образования. М.: РУДН, 2020. 220 с.
6. Вилкова А.В., Литвишков В.М., Швырев Б.А. Встроенное обучение как элемент непрерывного обучения информационной безопасности // Пенитенциарная наука. 2020. Т. 14. № 1(49). С. 135-141.
7. Другач Ю. С. Контролируемый взлом. Библия социальной инженерии. 2-е изд., перераб. и доп. СПб.: БХВ-Петербург, 2024. 208 с.
8. Ефимов С.А., Пронькин Н.Н. Роль сотрудников в обеспечении информационной безопасности: подходы к повышению осведомленности // Международный журнал профессиональной науки. 2024. № 6-2. С. 40-47. URL:
9. Жданова Д.Е. Технология реверсивного обучения: сочетание мобильного обучения и активных методов обучения // Наукосфера. 2021. № 7-1. С. 55-58.
10. Захарова А.А. Методы обучения персонала в организации // Аллея науки. 2022. Т. 1. № 3 (66). С. 114-120.
11. Зуфарова А.С., Кошелева А.Д. Формирование методики создания интерактивных образовательных web-квестов в условиях школьного образования // Современное педагогическое образование. 2024. № 6. С. 116-120.
12. Иванов П.И. Противодействие фишинговым атакам: обучение пользователей безопасности. М.: Наука, 2020. 256 с.
13. Климов А.А., Заречкин Е.Ю., Куприяновский В.П. Влияние цифровизации на систему профессионального образования // Современные информационные технологии и ИТ-образование. 2019. Т. 15/ № 2. С. 468-476.

14. Козлова О.В. Интерактивные методы обучения для повышения осведомленности о фишинговых атаках. СПб.: Невский университет, 2019. 162 с.
15. Нечипуровский Д.И. Как построить многоуровневую защиту для борьбы с продвинутыми угрозами фишинга // Научный аспект. 2024. Т. 41. № 4. С. 5337-5342.
16. Павлов А.С. Методика оценки эффективности тренингов по фишингу в организациях. М.: Высшая школа экономики, 2020. 276 с.
17. Прохоров А.И., Маркин Е.А., Никеева У.Г. Фишинг-атаки: основные виды и способы защиты от них // Информационные системы, экономика и управление. Ученые записки. Ростов н/Дону, 2023. С. 84-90.
18. Сливинский Д.В., Шишияну К.С. Обучение персонала как технология управления человеческими ресурсами предприятия: основные формы, методы и критические оценки // Инновации и инвестиции. 2023. № 11. С. 78-80.
19. Штайгер А.А. Социальная инженерия на примере фишинга // Вестник современных исследований. 2018. № 6.3(21). С. 612-614.
20. Яковлева М.А. Лидерство в системе наставничества как эффективный инструмент адаптации персонала // Human Progress. 2021. Т. 7. № 1.

Simulation of phishing attacks as a method of increasing cyber literacy and preparing to respond to threats

Dmitry S. An

Student

Pacific State University

Khabarovsk, Russia

2019100305@togudv.ru

ORCID 0000-0000-0000-0000

Anna S. Zufarova

Senior Lecturer at the Department of Mathematical Methods of Information Security and Computer Security

Pacific State University

Khabarovsk, Russia

006694@ togudv.ru

ORCID 0000-0000-0000-0000

Received 10.04.2025

Accepted 30.05.2025

Published 30.06.2025

UDC 004.052.6

DOI 10.25726/b2476-6563-8129-i

EDN ZBCSVM

VAK 5.8.1. General pedagogy, history of pedagogy and education (pedagogical sciences)

OECD 05.03.HA. EDUCATION & EDUCATIONAL RESEARCH

Abstract

Despite the availability of modern security technologies, the success of attacks often depends on the level of training of employees. Improper behavior when faced with cyber threats can lead to serious consequences, such as data leakage or disruption of the organization. Phishing attacks are one of the most common threats to cybersecurity. They are an attempt to deceive users in order to obtain confidential information

such as passwords, bank card information, «secret» information and other personal information. Improving employee cybersecurity is a key element of protection against phishing. One of the most effective methods of raising awareness is conducting phishing attack simulations. Simulating phishing attacks is an effective method of increasing employees' cyber literacy and preparing them to respond to real threats. This approach allows you to simulate attacks that can happen in real life, and gives employees the opportunity to train in a safe environment, which helps to develop the necessary skills and raise awareness of the risks. The purpose of this study is to study the effectiveness of phishing attack simulation as a method of increasing cyber literacy and training employees to respond to real threats. We will look at the main aspects of conducting such simulations, their impact on user behavior, and possible improvements in the learning process. Let's make a comparative analysis of the existing training platforms. Let's consider the algorithm for conducting attack simulations and highlight the main goals and objectives of attack simulations using a real experiment conducted at the company. Let's define the pedagogical value of phishing attack simulations.

Keywords

social engineering, phishing attack simulation, training, security, e-mail newsletters, letters, training platforms.

References

1. Abitov A.A., Tkhakakhov R.A., Khachmakhova M.Z., Sungurov K.S. Protection from phishing // In the collection of scientific papers: Digital transformation of science and education. 2020. pp. 13-17.
2. An D.S., Zufarova A.S. The impact of interactive trainings on employee awareness of phishing attacks. 2025. № 1. pp. 41-52.
3. Bachieva A.V., Bosiev T.O. Phishing as one of the methods of fraud in the field of computer information // In the collection: Actual problems of legal science and practice. 2017. Vol. 1. pp. 232-235.
4. Bogdanova T.M. Improving employee security through phishing attack training. M.: RAS, 2019. 153 p.
5. Vasilyeva N.A. Methods of protecting employees from phishing attacks: the role of training and education. M.: Peoples' Friendship University of Russia, 2020. 220 p.
6. Vilkova A.V., Litvishkov V.M., Shvyrev B.A. Embedded learning as an element of continuous information security training // Penal science. 2020. Vol. 14. № 1(49). pp. 135-141.
7. Drugach Yu.S. Controlled hacking. The Bible of social engineering. 2nd ed., revis. and add. SPb.: BHV-Petersburg, 2024. 208 p.
8. Efimov S.A., Pronkin N.N. The role of employees in ensuring information security: approaches to awareness-raising // International journal of professional science. 2024. № 6-2. pp. 40-47.
9. Zhdanova D.E. Technology of reverse learning: a combination of mobile learning and active teaching methods // Sciencesphere. 2021. № 7-1. pp. 55-58.
10. Zakharova A.A. Methods of personnel training in the organization // Alley of science. 2022. Vol. 1. № 3(66). pp. 114-120.
11. Zufarova A.S., Kosheleva A.D. Formation of methods for creating interactive educational web-quests in the context of school education // Modern pedagogical education. 2024. № 6. pp. 116-120.
12. Ivanov P.I. Countering phishing attacks: educating security users. M.: Science, 2020. 256 p.
13. Klimov A.A., Zarechkin E.Yu., Kupriyanovsky V.P. The impact of digitalization on the professional education system // Modern information technologies and IT education. 2019. Vol. 15. № 2. pp. 468-476.
14. Kozlova O.V. Interactive teaching methods to raise awareness of phishing attacks. SPb.: Nevsky University, 2019. 162 p.
15. Nechipurovsky D.I. How to build multilevel protection to combat advanced phishing threats // Scientific aspect. 2024. Vol. 41. № 4. pp. 5337-5342.
16. Pavlov A.S. Methodology for evaluating the effectiveness of phishing trainings in organizations. M.: Higher School of Economics, 2020. 276 p.

17. Prokhorov A.I., Markin E.A., Nikeeva U.G. Phishing attacks: the main types and methods of protection against them // Information systems, economics and management. Scientific notes. 2023. pp. 84-90.
18. Slivinsky D.V., Shishiyanu K.S. Personnel training as a technology for managing human resources of an enterprise: basic forms, methods and critical assessments // Innovations and investments. 2023. № 11. pp. 78-80.
19. Steiger A.A. Social engineering on the example of phishing // Bulletin of modern research. 2018. № 6.3(21). pp. 612-614.
20. Yakovleva M.A. Leadership in the mentoring system as an effective tool for staff adaptation // Human Progress. 2021. Vol. 7. № 1.