Анализ эффективности учебных фишинговых кампаний как инструмента повышения киберграмотности сотрудников

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 09.04.2025
Принята 29.05.2025
Опубликована 30.06.2025

УДК 302.342:658.562.3
DOI 10.25726/i8766-9360-6591-s
EDN ZUMFHD
ВАК 5.8.1. Общая педагогика, история педагогики и образования (педагогические науки)
OECD 05.03.HA. EDUCATION & EDUCATIONAL RESEARCH

Аннотация

Регулярное развертывание имитационных фишинговых атак является эффективным способом проверки знаний сотрудников и реагирования на реальные угрозы. Эти симуляции дают представление об уязвимостях в организации и помогают определить области, требующие улучшения. Имитируя реальные попытки фишинга, организации могут усилить обучение и подготовить сотрудников к распознаванию и адекватному реагированию на аналогичные угрозы в реальной жизни. Учебные фишинговые кампании являются важным инструментом повышения киберграмотности сотрудников организаций. Они помогают выявлять уязвимости и обучать персонал распознавать различные виды кибератак. Эффективность таких кампаний оценивается через анализ процента успешных атак, количества сообщений о подозрительных письмах, времени реакции на угрозу, а также путем проведения опросов и тестирования знаний. Регулярные учебные атаки, адаптация содержания и интеграция с обучающими программами способствуют повышению общей киберграмотности сотрудников и снижению рисков кибербезопасности. Для повышения уровня киберграмотности сотрудников организации целесообразно провести анализ результатов учебного фишинга с целью выявления слабых мест и разработки эффективных мер по их устранению. В рамках данного исследования предлагается оценить уровень осведомленности персонала о существующих угрозах информационной безопасности через моделирование атак типа "фишинг". Анализ полученных данных позволит определить наиболее уязвимые категории сотрудников и разработать персонализированные программы обучения, направленные на повышение их компетентности в области защиты от цифровых угроз. В статье мы описали подход к анализу результатов, полученных в ходе экспериментальной фишинговой атаки.

Ключевые слова

социальная инженерия, фишинг, анализ эффективности, обучение, безопасность, результат, защита информации.

Введение

Учебные кампании по кибербезопасности являются важными инициативами, направленными на повышение осведомленности сотрудников и реагирования на киберугрозы в организациях (Ан, 2025). По мере роста распространенности кибератак важность оснащения сотрудников навыками и знаниями для снижения этих рисков становится первостепенной. Исследования показывают, что человеческая ошибка является основной причиной нарушений безопасности, что подчеркивает необходимость эффективных программ обучения, которые способствуют культуре осведомленности и соответствия кибербезопасности (Другач, 2024). Примечательно, что такие обучающие инициативы могут значительно сократить случаи нарушения безопасности, в конечном итоге защищая организации от существенного финансового и репутационного ущерба.

Эти обучающие кампании обычно охватывают различные методы, включая очные семинары, онлайн-модули, имитацию фишинговых атак и игровые обучающие мероприятия. Каждый подход направлен на вовлечение сотрудников при устранении конкретных угроз, таких как фишинг и утечки данных. Успешная программа обучения кибербезопасности не только обучает, но и дает сотрудникам возможность выступать в качестве критической линии защиты от потенциальных угроз (Захарова, 2022). Однако такие проблемы, как невовлеченность сотрудников, ограничения по времени и сложность измерения долгосрочной эффективности, создают значительные препятствия для успешной реализации этих программ (Абитов, 2020).

Споры вокруг обучения кибербезопасности часто вращаются вокруг баланса между образованием, ориентированным на соответствие, и поощрением подлинного вовлечения среди сотрудников. Критики утверждают, что чрезмерно предписывающее обучение может привести к менталитету галочек, когда сотрудники выполняют требования к обучению, не понимая и не применяя полученные уроки. Напротив, сторонники подчеркивают важность релевантного, увлекательного контента, который резонирует с повседневными обязанностями сотрудников, тем самым улучшая как сохранение, так и практическое применение знаний (Вилкова, 2020).

Поскольку нормативно-правовая база, окружающая конфиденциальность и безопасность данных, развивается, интеграция обучения с соблюдением требований по кибербезопасности становится все более важной (Зуфарова, 2024). Организации, которые эффективно сочетают навыки соответствия и практические навыки по кибербезопасности, могут гарантировать, что сотрудники не только понимают свои юридические обязанности, но и оснащены для навигации по сложностям современных киберугроз (Жданова, 221).

В целом, постоянная разработка и оценка этих учебных программ имеют важное значение для формирования проактивной культуры безопасности и снижения рисков в постоянно меняющейся цифровой среде (Козлова, 2019).

Материалы и методы исследования

Пошагово распишем процесс организации и анализа фишинговой кампании (Павлов, 2020). В нашем исследовании участвовала хабаровская компания по продажи цветов «Город цветов».

На первом шаге нужно решить организационно-технические вопросы для проведения тестовой фишинговой атаки. Это лучше поручить специалистам в сфере информационной безопасности или знающему человеку в этой области. Масштаб работ при подготовке IT-инфраструктуры в каждой компании может быть разным. Задачи, стоящие на этом этапе: выбрать хостинг, который предоставит IP-адреса, не находящиеся в спам-базах; настроить сервер, домен; создать список адресов «жертв»; продумать правдоподобный сценарий; создать письма для рассылок, фишинговые страницы и вложения (Климов, 2019; Сливинский, 2023).

Компании, которые обладают соответствующей IT-инфраструктурой и в штате которых трудятся специалисты в сфере информационной безопасности, смогут организовать учебную фишинг-атаку для своих коллег самостоятельно. Также инсценировать ее помогут автоматизированные ресурсы или сторонние специалисты. Если решите воспользоваться их услугами, то штатным специалистам не придется настраивать домены и придумывать сценарии атак, а в некоторых случаях аутсорсинг даже поможет проанализировать результаты эксперимента (Штайгер, 2018). Запускаем симуляцию фишинговых атак и получаем результаты.

В нашем эксперименте участвовал работник в сфере информационной безопасности и специализированная платформа StopPhish. Она занималась рассылкой фишинговых сообщений, моделировала реальные сценарии угроз и отслеживала поведение пользователей, составляя отчеты данных, которые можно легко выгружать (рис. 1).

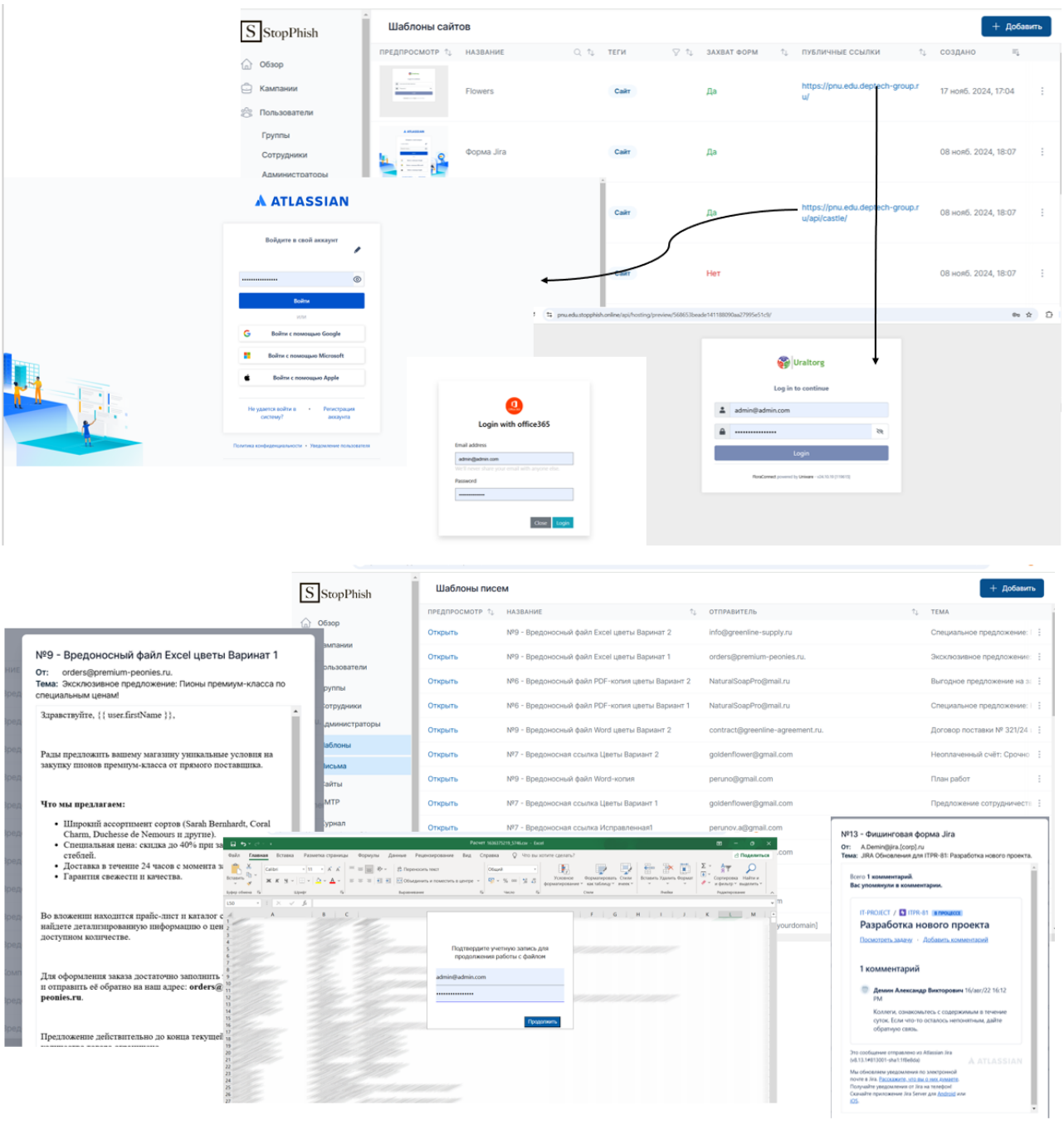


Рисунок 1. Запуск фишинговых кампаний

На шаге втором распределяем «жертв» на группы. Полученные результаты нужно обработать, чтобы лучше понять актуальность проведения учебной фишинговой атаки в организации. Затем необходимо проанализировать ситуацию, что сократит время на обучение по реагированию на такие инциденты, и выработать действительно полезные рекомендации. Советуем распределить коллег на группы «жертв».

Результаты и обсуждение

В процессе проведения экспериментального тестирования с использованием симулированных фишинговых атак и последующего анализа полученных данных было установлено, что всех участников исследования, которые выступали в роли потенциальных "жертв" киберпреступлений, можно классифицировать на пять основных категорий в соответствии с их поведенческими паттернами и реакциями на поддельные электронные сообщения. Данная классификация была разработана на основе углубленного анализа результатов кратковременного опроса, направленного на выявление и изучение специфических реакций персонала организации на фишинговые письма различного типа (Иванов, 2020; Сливинский, 2023).

Первая категория (Группа A) представляет собой наиболее уязвимую часть коллектива - сотрудники, которые продемонстрировали полное отсутствие настороженности и осуществили все действия, предписанные злоумышленниками в поддельном письме. К таким действиям относится переход по подозрительным гиперссылкам, загрузка файлов неизвестного происхождения на рабочие устройства, а также предоставление конфиденциальной информации, включая логины, пароли и другие персональные данные. Именно данная группа сотрудников становится основным объектом для детального анализа, поскольку их поведение демонстрирует те самые нежелательные реакции, которые могут привести к серьезным инцидентам информационной безопасности. Установление точного процентного соотношения таких сотрудников в различных организациях представляет значительную сложность, поскольку данный показатель находится в прямой зависимости от множества внутренних и внешних факторов, включая уровень образования персонала, специфику организационной культуры, индивидуальные психологические особенности каждого работника, его когнитивные способности, а также базовые личностные характеристики и склонности.

Вторая категория (Группа B) включает в себя сотрудников, которые по различным причинам полностью проигнорировали тестовое фишинговое сообщение. Это может быть связано как с невнимательностью и рассеянностью, так и с сознательным решением не открывать электронные письма от неизвестных отправителей. С точки зрения обеспечения кибербезопасности, данная группа представляет особую опасность и требует пристального внимания, поскольку их будущее поведение в условиях реальных киберугроз остается абсолютно непредсказуемым. Существует высокий риск того, что даже при наличии в организации разработанных протоколов реагирования на подозрительные сообщения и соответствующих технических средств защиты, представители этой группы могут не следовать установленным процедурам при столкновении с настоящими фишинговыми атаками (Богданова, 2019; Яковлева, 2021).

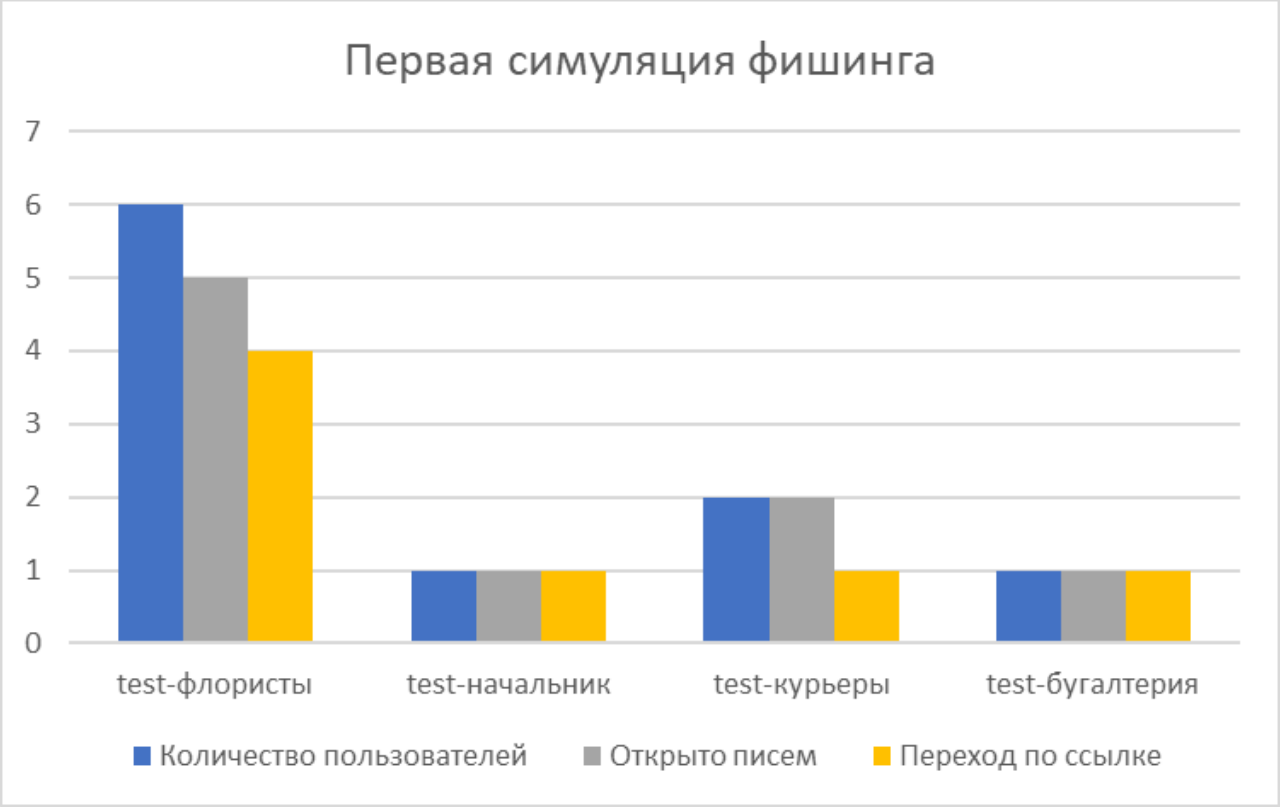
Третья категория (Группа C) объединяет сотрудников, которые внимательно изучили содержание подозрительного письма, однако проявили здоровую осторожность и воздержались от выполнения каких-либо действий из-за неуверенности в легитимности сообщения или недостаточного понимания требований отправителя. Работа с данной группой персонала требует системного и последовательного подхода к образовательному процессу. Первоначально необходимо обеспечить доступное и понятное объяснение сущности фишинговых атак, их технических механизмов и основных целей киберпреступников. Только после формирования базового понимания угроз следует переходить к детальному изучению алгоритмов правильного реагирования на подозрительные сообщения.

Четвертая категория (Группа D) представлена наиболее подготовленными с точки зрения кибербезопасности сотрудниками, которые не только тщательно проанализировали полученное сообщение, но и смогли правильно идентифицировать его как потенциальную угрозу. Представители данной группы продемонстрировали осознанное и взвешенное поведение, самостоятельно приняв

решение о нейтрализации угрозы путем удаления письма, помещения его в папку спама или блокировки отправителя. Образовательный процесс для этой категории сотрудников не потребует значительных временных и ресурсных затрат, поскольку им будет достаточно ознакомления с обновленными корпоративными рекомендациями и протоколами действий в различных ситуациях.

Пятая категория (Группа F) включает наиболее ответственных и социально активных сотрудников, которые при обнаружении подозрительного сообщения незамедлительно информировали о потенциальной угрозе свое непосредственное руководство, обратились за консультацией к более опытным коллегам в рамках своего структурного подразделения или направили уведомление непосредственно в службу информационной безопасности организации. Представителей данной группы настоятельно рекомендуется подвергнуть повторному детальному интервьюированию с целью получения максимально подробной информации о том, какие именно элементы письма вызвали у них подозрения и сомнения в его подлинности. Также крайне важно зафиксировать пошаговое описание всех действий, которые они предприняли после первичного анализа сообщения. Собранная таким образом информация станет бесценным ресурсом для разработки оптимального сценария действий при обнаружении реальных фишинговых атак, который будет максимально адаптирован к специфическим условиям конкретной организации, ее филиалов или отдельных структурных подразделений. Согласно актуальным статистическим данным, лишь 39% от общего числа сотрудников различных организаций заявляют о своей готовности сообщить о выявленных проблемах, связанных с нарушениями информационной безопасности, в случае их обнаружения (Ефимов, 2024).

На заключительном, третьем этапе исследования необходимо провести комплексный анализ поведенческих паттернов всех категорий сотрудников и сформировать детальный отчет с рекомендациями по повышению уровня кибербезопасности. В рамках нашего исследования был проведен углубленный анализ результатов проведенных симуляций фишинговых атак, результаты которого представлены в графическом виде (рис. 2).



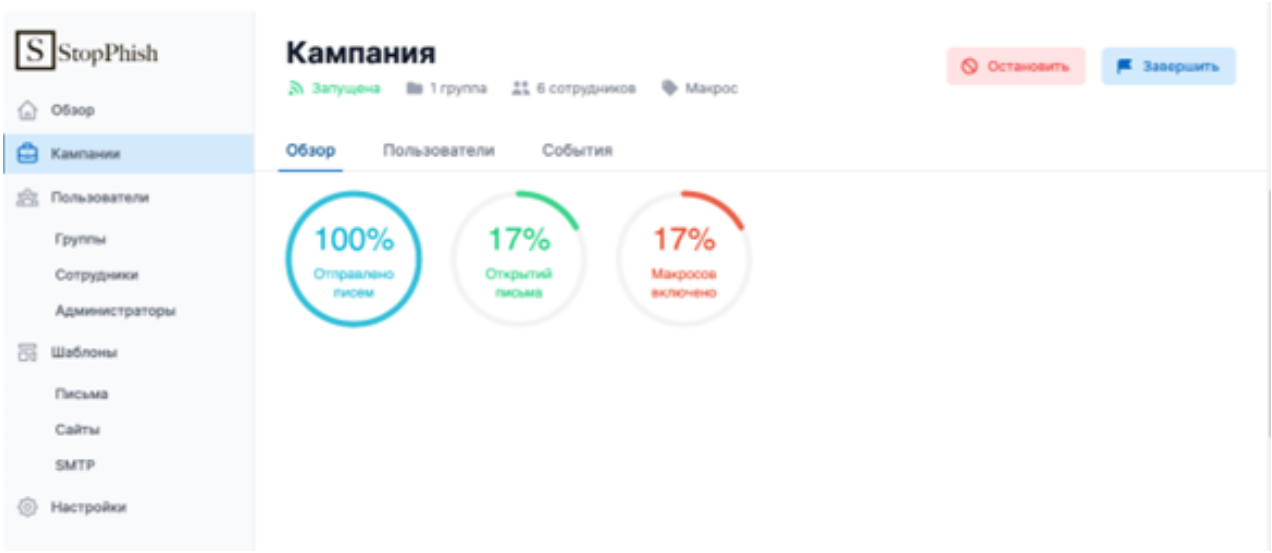


Рисунок 2. Отчет и результаты первой симуляции

Для обеспечения максимальной эффективности использования полученных в ходе исследования данных и результатов проведенного анализа крайне важно тщательно продумать и разработать оптимальную структуру представления информации, а также определить наиболее удобный формат ее визуализации. Рекомендуется организовать итоговый документ таким образом, чтобы он содержал несколько логически связанных между собой разделов, каждый из которых выполняет определенную функциональную роль.

Первый раздел документа должен содержать исчерпывающую общую информацию, включающую детальное описание причин инициации эксперимента, четкое определение поставленных целей и задач, а также обоснование необходимости проведения данного исследования в контексте обеспечения информационной безопасности организации. В этом же разделе целесообразно разместить полный комплекс технических характеристик проведенного тестирования, включая используемые методики, программные средства, временные рамки, а также детальные информационные сведения о параметрах эксперимента. Такой подход к структурированию информации обеспечит возможность точного воспроизведения аналогичного тестирования в будущем, что может потребоваться для проведения повторных измерений эффективности мер по повышению уровня кибербезопасности спустя определенный период времени или для сравнительного анализа динамики изменений в поведении сотрудников. В последующих тематических разделах документа рекомендуется представить детальную обезличенную характеристику поведенческих паттернов каждой из выявленных групп потенциальных "жертв" фишинговых атак. При этом крайне важно обеспечить полную анонимность участников исследования, исключив любую возможность идентификации конкретных сотрудников, что соответствует этическим принципам проведения подобных исследований и требованиям защиты персональных данных.

Заключительная часть аналитического отчета должна содержать обобщающие выводы, основанные на полученных результатах, а также подробные практические рекомендации по оптимизации и совершенствованию алгоритмов реагирования персонала на фишинговые атаки. Эти рекомендации должны быть ориентированы на повышение общего уровня кибербезопасности в конкретной организации и учитывать ее специфические особенности.

Временные параметры реализации проекта и формирование рабочей группы

Определение точных временных рамок, необходимых для полноценного осуществления всего комплекса мероприятий по тестированию и анализу уровня защищенности от фишинговых атак, представляет значительную сложность и не может быть унифицировано для всех типов организаций. Продолжительность реализации проекта находится в прямой зависимости от множества факторов, включая масштаб организации, сложность ее организационной структуры, географическое

распределение подразделений, уровень технической оснащенности, а также готовность персонала к участию в подобных мероприятиях.

Для крупных холдинговых структур с разветвленной сетью филиалов, насчитывающих тысячи сотрудников и функционирующих в различных часовых поясах, даже трехмесячный период может оказаться недостаточным для проведения качественного и всестороннего анализа. В таких случаях необходимо учитывать время на координацию действий между различными подразделениями, согласование методик тестирования с региональными представительствами, а также обеспечение единообразия подходов во всех структурных единицах организации. В то же время для небольших компаний, штат которых составляет порядка 30-50 человек, недельного периода может быть вполне достаточно для проведения всех необходимых процедур, включая подготовку тестовых материалов, проведение симуляции фишинговой атаки, сбор и анализ полученных данных, а также формирование итогового отчета с рекомендациями. Ключевым фактором успешной реализации проекта является организация эффективной командной работы, предполагающей привлечение специалистов различных профилей и уровней компетенции. В состав рабочей группы должны входить не только профессиональные специалисты в области информационной безопасности, обладающие необходимыми техническими знаниями и практическим опытом, но также ответственные представители всех филиалов и структурных подразделений организации, которые смогут обеспечить эффективное взаимодействие с персоналом на местах и учет специфических особенностей функционирования каждого отдела. Особое значение имеет включение в рабочую группу квалифицированных специалистов HR-отдела, которые обладают глубоким пониманием психологических аспектов поведения сотрудников, корпоративной культуры организации, а также имеют практический опыт в области обучения и развития персонала (Прохоров, 2023; Богданова, 2019).

На четвертом этапе реализации проекта критически важно придать конкретную, практически применимую форму тем желаемым реакциям и алгоритмам действий, которые должны демонстрировать сотрудники при столкновении с потенциальными фишинговыми угрозами. Этот процесс требует трансформации теоретических знаний и абстрактных рекомендаций в четкие, понятные и легко выполнимые инструкции, которые смогут использовать работники различных уровней подготовки и технической грамотности. Итоговый отчет о результатах проведенной фишинговой кампании, в котором детально отражены все аспекты анализа тестовой атаки, настоятельно рекомендуется дополнить практическим приложением прикладного характера. Данное приложение должно представлять собой комплексный справочный материал, содержащий систематизированную информацию по всем ключевым аспектам противодействия фишинговым атакам. В практическом приложении должны быть зафиксированы следующие критически важные элементы: исчерпывающий перечень характерных признаков и индикаторов, позволяющих своевременно идентифицировать фишинговые письма среди легитимной корреспонденции; пошаговый алгоритм действий для ситуаций, когда у сотрудника возникают подозрения относительно подлинности полученного сообщения; детальные инструкции по экстренному реагированию в случаях, когда конфиденциальные данные уже были введены в формы на поддельных веб-ресурсах; процедуры уведомления соответствующих служб о выявленных угрозах; рекомендации по минимизации последствий в случае компрометации учетных данных. Информация в практическом приложении может быть представлена в различных форматах, каждый из которых имеет свои преимущества и области применения. Это может быть интерактивная карта действий с визуальными элементами, подробная пошаговая инструкция с иллюстрациями, краткие рекомендации для быстрого ознакомления, формализованные правила поведения в различных ситуациях, а также практические чек-листы для самостоятельной проверки подозрительных сообщений (рисунок 3).

Наименование данного документа может варьироваться в зависимости от корпоративной культуры и принятых в организации стандартов документооборота. Главным критерием при выборе формата и названия должна служить максимальная понятность и удобство использования для всех категорий сотрудников. Только при соблюдении принципа доступности и практической применимости предпринятые усилия принесут ожидаемую пользу: персонал организации сможет успешно усвоить и применять на практике желаемые алгоритмы реагирования и действий при столкновении с

фишинговыми атаками. При наличии технических и ресурсных возможностей настоятельно рекомендуется разработать специализированную информацию, адаптированную для конкретных структурных подразделений с учетом специфики их деятельности. Например, при подготовке образовательных материалов для сотрудников бухгалтерии и финансовых служб особое внимание следует уделить вопросам безопасности при работе с платежными системами, банковскими сервисами, а также процедурам верификации финансовых операций и запросов на перевод средств.

Для обеспечения максимальной эффективности внедрения разработанных мер и гарантии их неукоснительного соблюдения всеми сотрудниками организации крайне важно придать новым процедурам и алгоритмам действий официальный статус. С этой целью настоятельно рекомендуется оформить и утвердить разработанную стратегию противодействия фишинговым атакам в виде официального распорядительного документа, который будет иметь обязательную силу для всех работников организации независимо от их должностного положения и структурной принадлежности. Процедура ознакомления с утвержденным документом должна быть организована таким образом, чтобы гарантировать получение каждым сотрудником полной и достоверной информации о новых требованиях и процедурах. Для этого необходимо обеспечить персональное ознакомление всех работников с содержанием документа под личную подпись, что позволит зафиксировать факт получения информации и создаст правовую основу для последующего контроля соблюдения установленных требований.

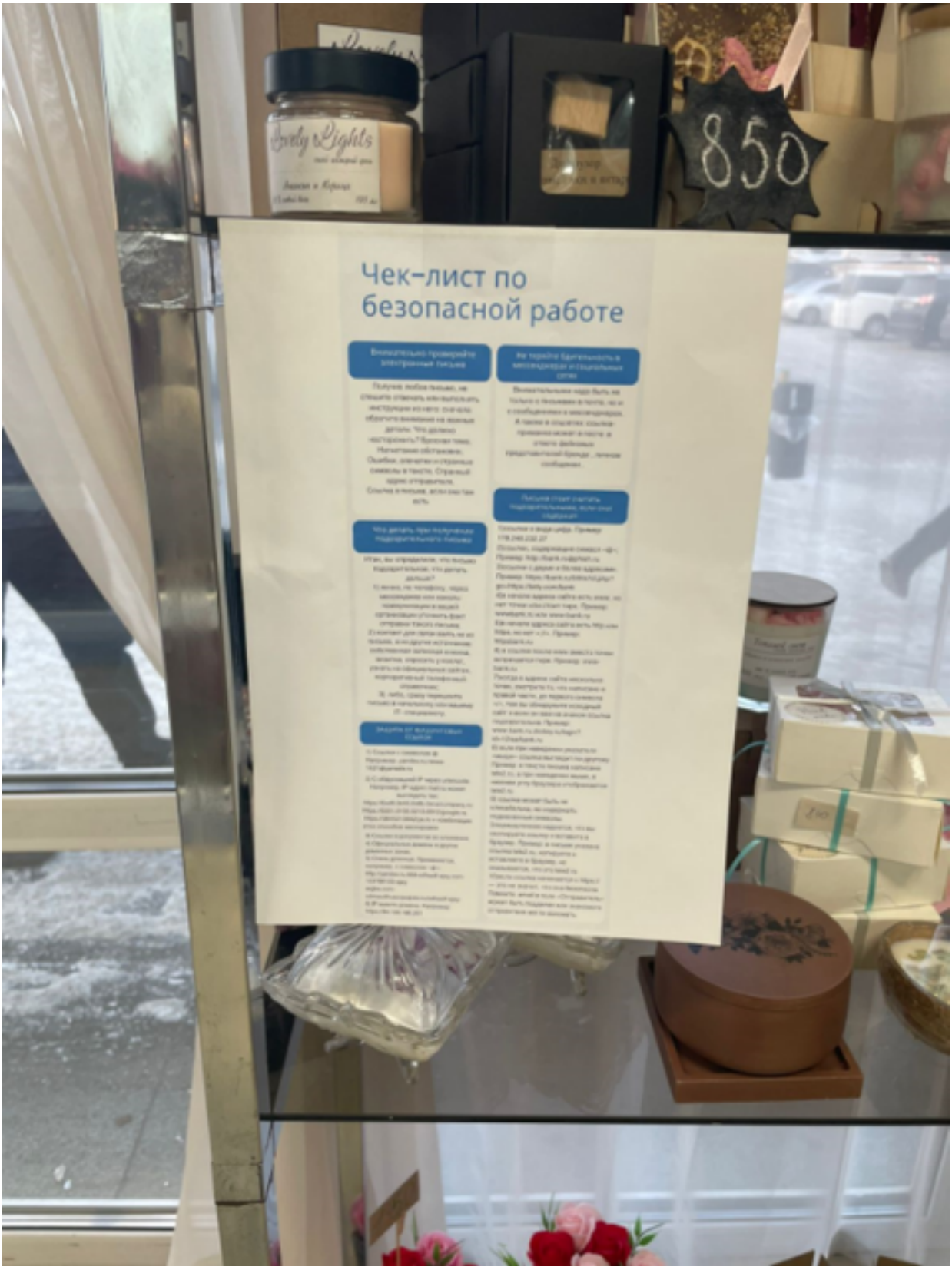


Рисунок 3. Обучающие чек-листы

На пятом шаге организуйте эффективное обучение сотрудников. Несмотря на то, что все поставят свою подпись об ознакомлении с нововведениями, только это не окажет должного эффекта. Рекомендуем сформировать обучающую программу (Зуфарова, 2024). Вам решать, какая информация там должна быть и сколько времени нужно отвести на обучение. Интересными кажутся результаты

недавнего исследования, в котором утверждается, что если сотрудники обучаются три месяца, то это приведет к снижению успеха фишинговых атак с 31.4% до 16.4%, а если обучение продлить на год, то этот результат снизится до 4,8% (Баиева, 2017).

Можно купить для компании общий курс по информационной безопасности, самостоятельно составить теоретический блок конкретно о фишинге, периодически устраивать повторные тренировочные фишинг-атаки, проводить тематические тесты или, к примеру, предложить сотрудникам пройти обучающую игру о фишинге (рисунок 4). Вариантов много. Если есть возможность, предоставьте коллегам выбор и остановитесь на том решении, которое понравится большинству. У кого есть ресурсы – персонализируйте программу. Результативней будет то решение, которое сориентировано на конкретную проблему в конкретной среде. Например, можно работать отдельно с каждой разделенной группой по уязвимостям. Также можно объединить представителей разных групп (например, первую и вторую; третью и четвертую). Еще вариант – адаптировать программу для каждого структурного подразделения (Захарова, 2022).

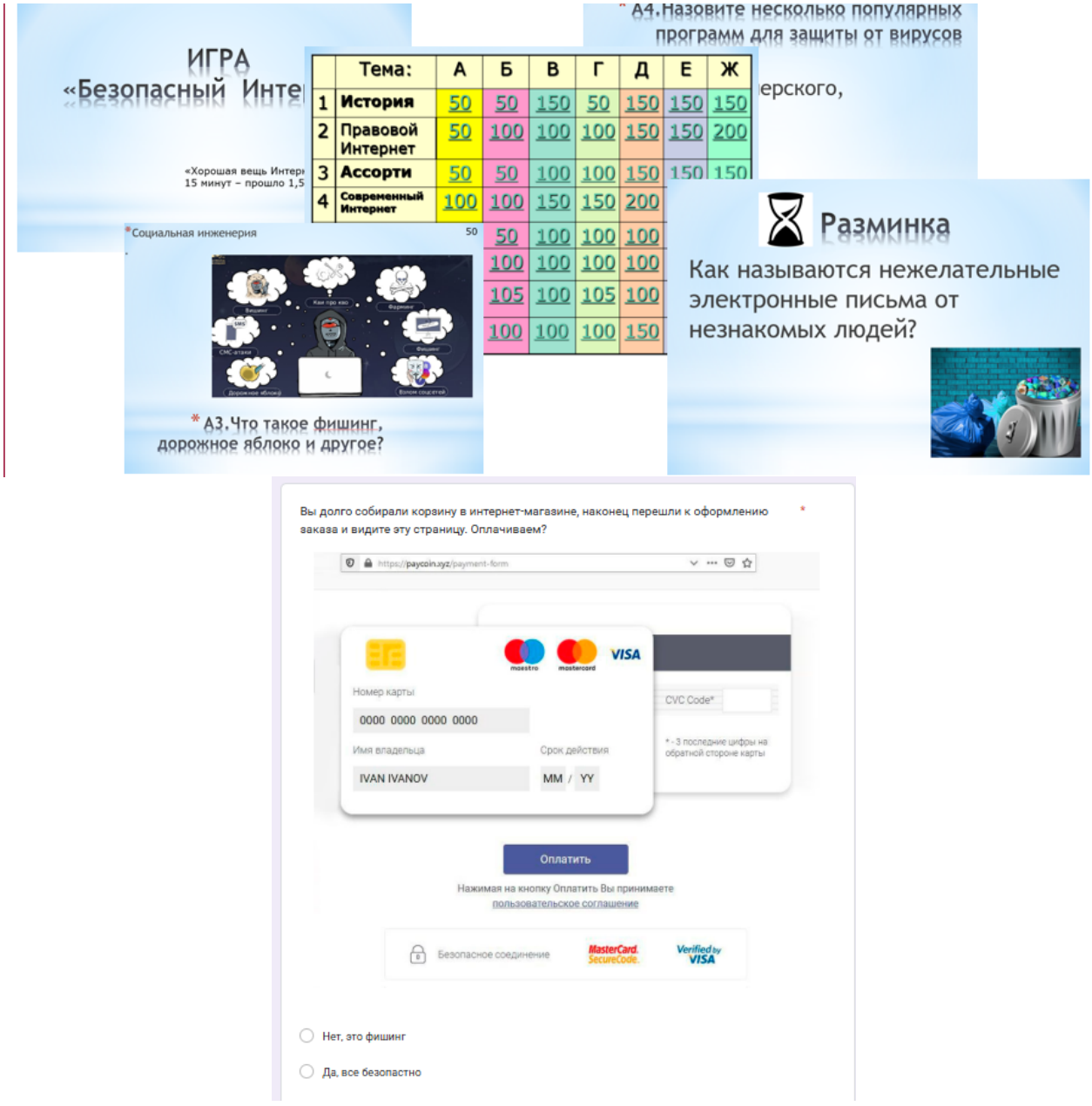


Рисунок 4. Обучающие семинары, тесты

На шаге шестом, защитите компанию от угроз с помощью программного обеспечения, т.е. произвести техническую защиту. Не имеет значения, о каких компаниях идет речь – крупных холдингах или ИП в защите нуждаются все. Исследование профессора Стэнфордского университета установило: каждый четвертый нанятый работник когда-нибудь нажимал на фишинговое электронное письмо на рабочем месте (Васильева, 2020).

Сегодня один из самых эффективных способов защититься от утечек информации – контролировать все каналы коммуникации компании с «внешним миром». Существуют системы способны запретить посещать пул не доверенных сайтов, фиксировать попытку отправки важных корпоративных данных и прерывать этот процесс, и также поможет предотвратить хищение информации при попытке получения доступа к рабочей станции посредством подключения внешних накопителей. Также система способна провести расследование и найти путь, по которому данные могли попасть к злоумышленникам. На рисунке 5 представлено внедрение технических решений для минимизации риска. Надеемся, организация и анализ тестовой фишинг-атаки, а также последующее обучение сотрудников будет положительным опытом для вашей компании и действительно снизит риски утечек данных.

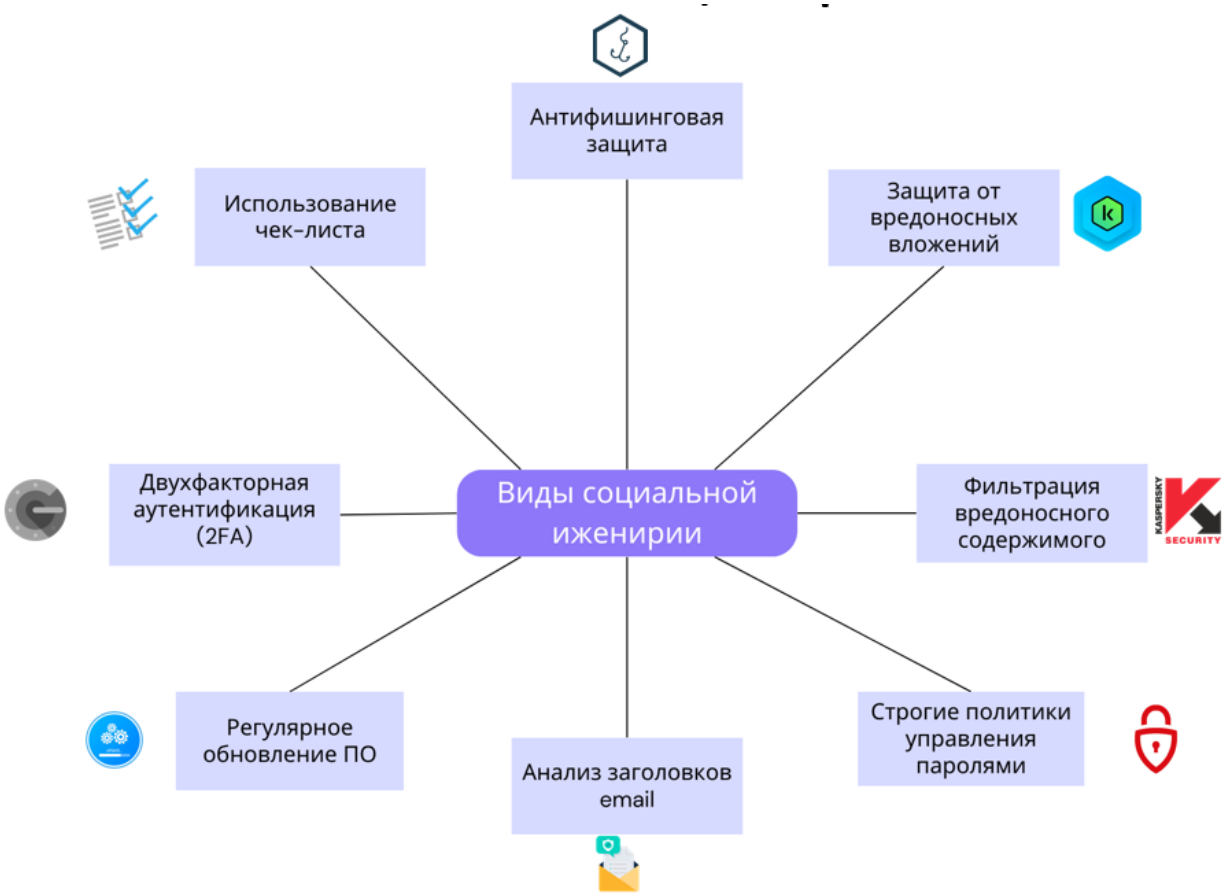


Рисунок 5. Технические решения для минимизации риска

На шаге седьмом можно провести повторную симуляцию фишинга, чтоб убедиться в правильности выбранной стратегии. Спустя определенное время, после внедрения комплекса мер по повышению осведомленности сотрудников о киберугрозах, можно произвести вторая и последующие симуляции фишинговой атаки.

Основной целью данного этапа стало это оценка эффективности предпринятых ранее образовательных инициатив и других профилактических мероприятий. Результаты нашей второй симуляции продемонстрировали заметные улучшения (рис. 6).

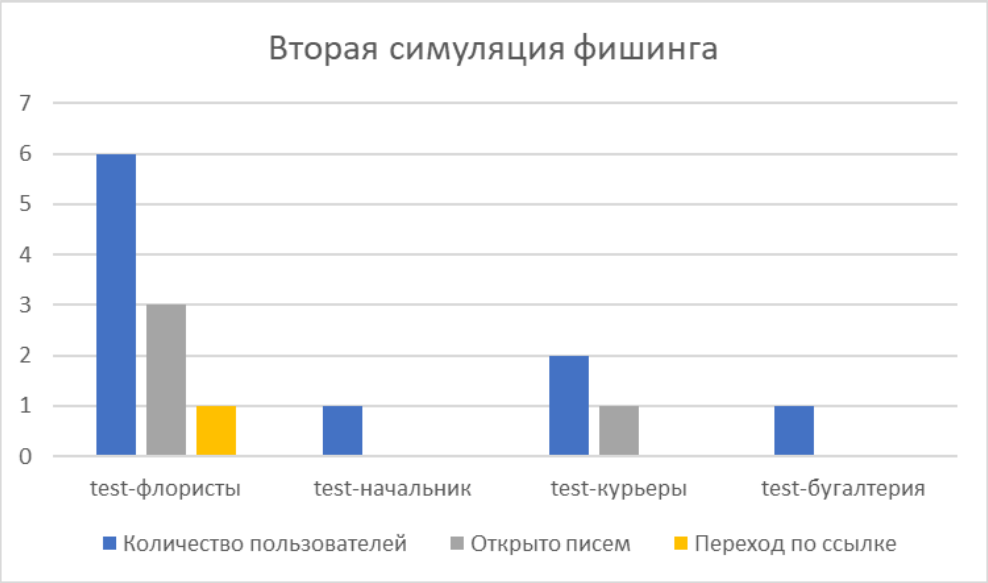


Рисунок 6. Результаты второй симуляции

Мы заметили, что 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. Такой результат свидетельствует о том, что образовательные меры, включающие проведение вебинаров и размещение чек-листов на рабочих местах, оказались действенными (Нечипуровский, 2024).

На восьмом этапе можно сделать сравнительный анализ всех симуляций и на основе нее сделать отчет для начальства и для итогового отчета (рис. 7).

Рисунок 7. Анализ симуляции фишинговых атак

Понятно, что проверить реакцию сотрудников можно в симуляции, но нам предоставили настоящую ситуацию. В числе недавних инцидентов после обучения стоит отметить проведение на нас DDoS-атаки с последующим шантажом, целью которого было получение выкупа. Скрин атаки предоставлен на рисунке 8. Однако благодаря осведомленности, которую мы повысили за счет

регулярных тренингов, и хладнокровию наших сотрудников, ситуация была успешно разрешена, что предотвратило денежные риски.

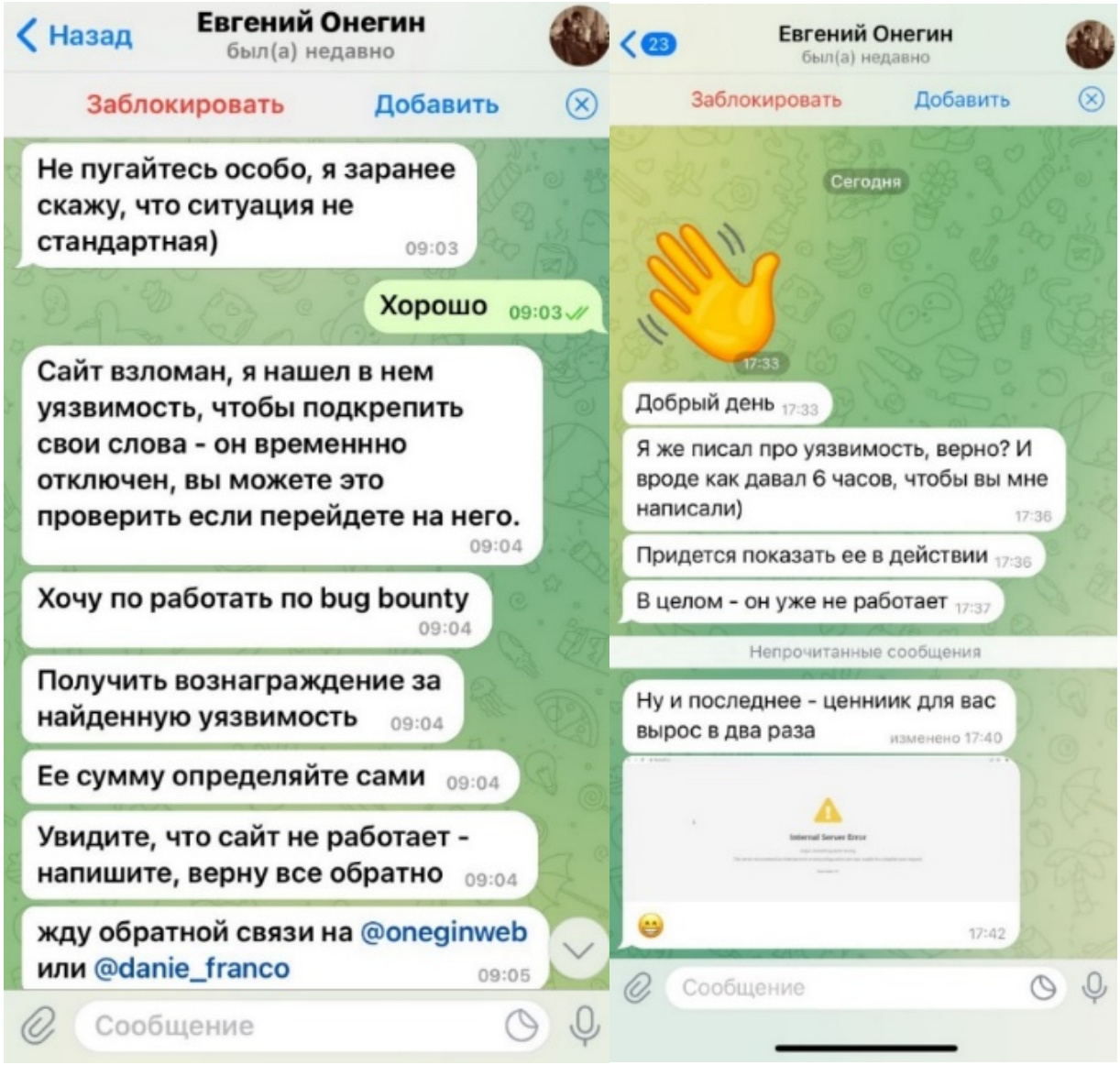


Рисунок 8. Реальная фишинговая атака на компанию

Эти результаты стали весомым доказательством того, что обучение и постоянное напоминание о принципах социальной инженерии способны существенно снизить риски, связанные с фишингом. Улучшения в показателях второй симуляции подчеркивают, что выбранный подход был правильным и эффективным, создавая крепкую основу для дальнейшего укрепления культуры кибербезопасности внутри компании.

Заключение

Таким образом, социальная инженерия нацелена на человеческий фактор, который часто становится самым слабым звеном в системе безопасности организации. Для предотвращения угроз необходимо повышать осведомленность сотрудников, обучая их выявлять и правильно реагировать на попытки манипуляции. Образовательные программы, организованные для служащих, помогают не только укрепить защиту компании, но и формировать культуру ответственности за сохранность информации.

Отметим, что защита от атак социальной инженерии требует комплексного подхода, сочетающего обучение сотрудников, внедрение строгих политик и процедур, а также использование современных технических решений. Таких, как учебная симуляция фишинговых атак, которая представляет собой эффективный педагогический инструмент для повышения уровня киберграмотности и подготовки сотрудников к реагированию на современные киберугрозы. Преимущества такого подхода – это реализм, контроль безопасности, адаптация под угрозы, мотивация сотрудников. Участие в симуляциях формирует у сотрудников более ответственное отношение к вопросам информационной безопасности.

Анализ результатов учебной атаки позволит выявить слабые места в системе информационной безопасности и разработать эффективные меры по предотвращению фишинговых атак. Отчет должен содержать информацию о группах «жертв», их реакциях на фишинговые письма и рекомендациях по повышению уровня осведомленности о фишинге. Только такой подход обеспечит надежную защиту информации и минимизирует риски для вашей организации.

Список литературы

1. Абитов А.А., Тхакахов Р.А., Хачмахова М.З., Сунгуров К.Ш. Защита от фишинга // В сборнике научных трудов: Цифровая трансформация науки и образования. 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.
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-на-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.

Analysis of the effectiveness of educational phishing campaigns as a tool to increase employee cyberbullying

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 09.04.2025
Accepted 29.05.2025
Published 30.06.2025

UDC 302.342:658.562.3
DOI 10.25726/i8766-9360-6591-s
EDN ZUMFHD
VAK 5.8.1. General pedagogy, history of pedagogy and education (pedagogical sciences)
OECD 05.03.HA. EDUCATION & EDUCATIONAL RESEARCH

Abstract

Regular deployment of simulated phishing attacks is an effective way to test employees' knowledge and respond to real threats. These simulations provide insight into vulnerabilities in an organization and help identify areas for improvement. By simulating real phishing attempts, organizations can enhance training and prepare employees to recognize and respond appropriately to similar threats in real life. Educational phishing campaigns are an important tool for improving the cyber literacy of employees in organizations. They help identify vulnerabilities and train staff to recognize different types of cyber attacks. The effectiveness of such campaigns is assessed by analyzing the percentage of successful attacks, the number of suspicious emails reported, the response time to the threat, as well as by conducting surveys and knowledge testing. Regular training attacks,

content adaptation and integration with training programs contribute to improving the overall cyber literacy of employees and reducing cybersecurity risks. To increase the level of cyber literacy of the organization's employees, it is advisable to analyze the results of educational phishing in order to identify weaknesses and develop effective measures to eliminate them. As part of this study, it is proposed to assess the level of staff awareness of existing information security threats through the modeling of phishing attacks. The analysis of the data obtained will make it possible to identify the most vulnerable categories of employees and develop personalized training programs aimed at improving their competence in the field of protection against digital threats. In the article, we described an approach to analyzing the results obtained during an experimental phishing attack.

Keywords
social engineering, phishing, performance analysis, training, security, outcome, information protection.

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.l 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.