ПРОГРАММНАЯ ПЛАТФОРМА ДЛЯ ФИШИНГОВЫХ СИМУЛЯЦИЙ

Биюмен Е.А., студент гр.361401

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Белоусова Е.С. – канд. тех. наук, доцент

Аннотация. В статье анализируется статистика угроз методами социальной инженерии в корпоративном секторе за 2025–2026 годы. Рассматриваются когнитивные факторы, влияющие на успешность целевых атак, и приводится количественное обоснование неэффективности классических методов обучения. Предложена архитектура программной платформы для фишинговых симуляций, автоматизирующая процессы аудита информационной безопасности посредством модулей копирования веб-ресурсов и отслеживаемых электронных документов.

Ключевые слова. информационная безопасность; социальная инженерия; когнитивная уязвимость; фишинговые симуляции; непрерывное обучение; автоматизация аудита.

Социальная инженерия в 2025–2026 годах является доминирующим вектором первоначального проникновения в корпоративные информационные системы. По данным аналитических центров, количество писем с признаками манипуляции в корпоративных почтовых системах выросло в три раза по сравнению с показателями предыдущего года [1].

Традиционные средства контентной фильтрации демонстрируют резкое снижение эффективности. Например, в строительной отрасли доля вредоносных писем, отклоненных на этапе базовой технической проверки, снизилась с 38% до 4,5% [1]. Данный факт обусловлен массовым использованием нарушителями скомпрометированных легитимных учетных записей партнеров. В условиях, когда программно-аппаратные барьеры пропускают подавляющее большинство целевых атак, критичным элементом системы защиты становится способность самого сотрудника выявлять аномалии.

Успешность социальной инженерии базируется на эксплуатации нейробиологических особенностей распределения внимания. Нарушители конструируют сообщения таким образом, чтобы адресат обрабатывал информацию рефлекторно, исключая аналитический подход. Детальный анализ позволяет выделить ключевые параметры писем, преодолевающие когнитивные барьеры:

1 Использование реальных персональных данных и точное копирование корпоративных интерфейсов активируют эффект внутригруппового искажения. Мозг воспринимает визуально знакомую среду как безопасную, блокируя механизмы скептицизма [1].

2 Письма, доставляемые в периоды пиковых нагрузок, эксплуатируют усталость от принятия решений: способность к критическому анализу снижается, и действия выполняются автоматически [1]. Согласно аналитике, фишинговые атаки имеют недельную сезонность: пик активности нарушителей приходится на среду (22,1%) и вторник (20,9%), когда загрузка сотрудников максимальна. К концу недели наблюдается спад с минимумом в воскресенье (1,2%) [2]. Описанная сезонность активности нарушителей проиллюстрирована на рисунке 1.

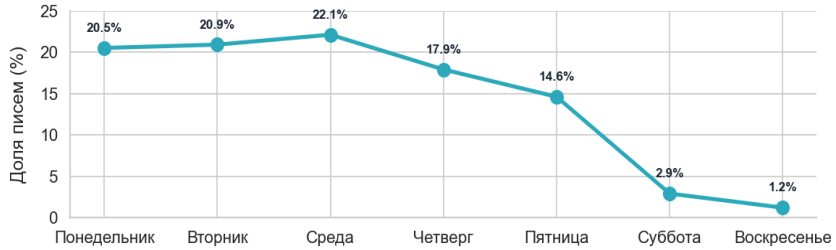


Рисунок 1 – График доли фишинговых писем в зависимости от дня недели в 2024 году

3 Использование QR-кодов в теле письма вынуждает пользователя перейти с рабочего компьютера на личный смартфон. Это выводит сотрудника из защищенной корпоративной среды и притупляет привычную настороженность [3].

4 Чаще всего ошибки возникают при маскировке фишинга под рутинные бизнес-процессы (акты сверок, уведомления систем документооборота). Из-за привыкания сотрудники обрабатывают такие письма рефлекторно. Число подобных атак кратно возросло в отраслях с интенсивным внешним документооборотом: в сфере профессиональных услуг – более чем в 8 раз, в логистике – в 3 раза, в здравоохранении – в 2 раза [1].

5 Применение факторов авторитетности (сообщения от имени руководства) и срочности провоцирует стресс. Это переключает мозг в режим быстрого реагирования, заставляя сотрудника фокусироваться исключительно на немедленном выполнении требований [4].

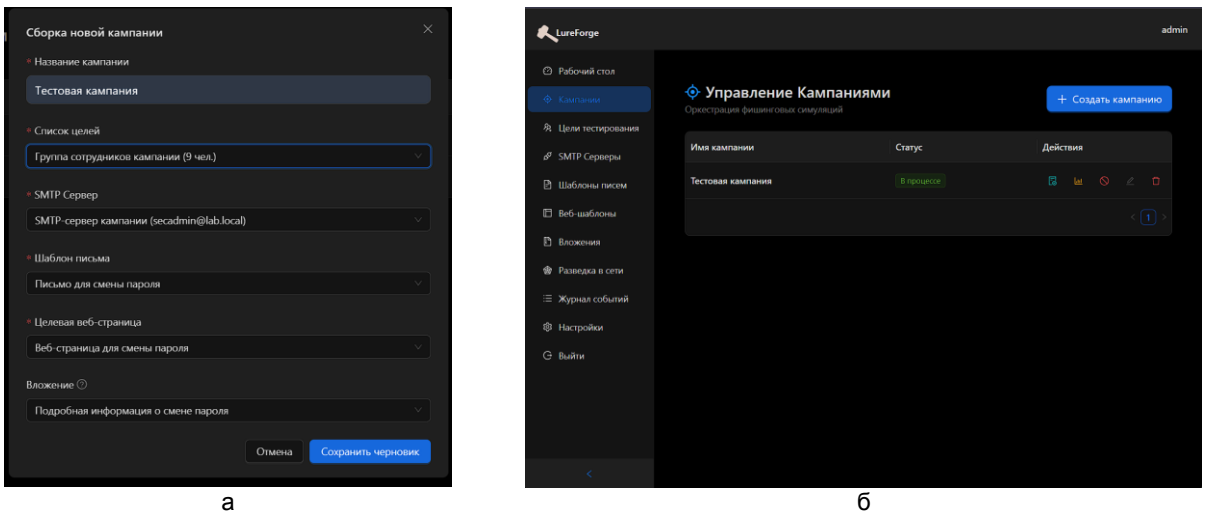
Традиционный подход к повышению осведомленности персонала, опирающийся на теоретические инструктажи и нормативный контроль, демонстрирует низкую продуктивность. Масштабные контролируемые исследования подтверждают полное отсутствие статистически значимой корреляции между тем, насколько недавно сотрудник прошел лекционное обучение, и его способностью противостоять реальным целевым атакам [5]. Пользователи, недавно завершившие теоретический курс, поддаются на социальную инженерию с той же вероятностью, что и лица, не проходившие его более года [5]. Теоретические знания не конвертируются в защитные рефлексы без регулярного практического закрепления.

В противовес лекционному подходу, методология регулярных фишинговых симуляций доказывает высокую результативность. Практическое погружение сотрудника в контролируемую среду учебной симуляции позволяет объективно выявить реальные поведенческие уязвимости [5]. В перспективе эффективность таких тренировок планируется усилить концепцией «моментальной обратной связи» (когда разбор ошибки предоставляется сразу после ее совершения) [6].

Важным фактором эффективности симуляций является их ролевая релевантность, использующая эффект семантического предшествования. Учебный сценарий должен строго соответствовать должностным обязанностям (например, имитация финансовых документов для бухгалтерии). Системный переход от разовых инструктажей к непрерывным релевантным симуляциям позволяет снизить базовый процент уязвимости персонала с 33,1% до 4,7% в течение одного года работы [6].

Для практической реализации описанной методологии разработана программная платформа для фишинговых симуляций. Подробная микросервисная архитектура комплекса, включающая изолированное ядро рассылок, модуль автоматизированной разведки и модуль фильтрации машинного трафика, была детально представлена в ранее опубликованной работе [7].

Процесс проведения учебной симуляции на базе разработанной платформы состоит из последовательных этапов, объединяющих работу графического интерфейса пользователя и скрытых технических механизмов. На этапе конфигурации администратор задает базовые параметры через форму сборки (рисунок 2, а). Процесс начинается с подготовки материалов: система позволяет создавать пользовательские шаблоны электронных писем и осуществлять точное копирование (клонирование) целевых веб-ресурсов для повышения реалистичности сценария. Формирование целевых групп тестируемых сотрудников реализуется двумя способами: путем прямого импорта списков или с использованием встроенного модуля автоматизированной разведки по открытым источникам. Данный модуль применяет средства морфологического анализа для извлечения персональных данных из текстовых массивов. По завершении настройки новая кампания сохраняется в статус «Черновика», а после подтверждения (нажатия кнопки запуска кампании) переходит в активный статус и отображается в общей панели управления (рисунок 2, б).



а б

Рисунок 2 – Запуск и управление фишинговыми симуляциями (кампаниями)

После запуска инициируется процесс генерации писем и подстановки данных. Ключевую технологическую роль на данном этапе выполняет модуль промежуточного проксирования почтового трафика, который перехватывает исходящие сообщения до их выхода во внешнюю сеть. Промежуточный узел решает две задачи. Во-первых, осуществляется подмена технических заголовков письма для имитации легитимных корпоративных почтовых программ, что позволяет обходить базовые средства фильтрации. Во-вторых, в сообщение динамически внедряется отслеживаемое электронное вложение. Техническая реализация такого вложения базируется на внедрении связи с внешним ресурсом во внутреннюю разметку документа (стандарта Office Open

XML). Только после завершения сборки промежуточный узел маршрутизирует полностью готовое письмо на реальный почтовый шлюз для доставки адресатам.

В ходе активной фазы кампании подсистема журналирования и аналитики непрерывно фиксирует этапы взаимодействия пользователя с полученным сообщением, сохраняя каждое событие в централизованном журнале аудита. Регистрация факта открытия письма происходит при загрузке почтовым клиентом скрытого графического маркера, интегрированного в тело сообщения. Факт взаимодействия с вложением фиксируется в момент, когда текстовый редактор пользователя инициирует обращение к серверу платформы для загрузки внешнего элемента, программно внедренного в документ. При переходе по ссылке в письме система регистрирует обращение к поддельному веб-ресурсу. Для защиты от систем автоматического анализа применяются технологии генерации запутанных сетевых адресов. В случае ввода учетных данных на поддельной странице информация безопасно перехватывается с помощью обратного прокси-сервера, алгоритмы которого настроены на асинхронную потоковую передачу для предотвращения перегрузки вычислительных мощностей.

Вся собираемая статистика и записи системного журнала обрабатываются в режиме реального времени и агрегируются в виде графиков и сводных таблиц на рабочем столе администратора платформы (рисунок 3). Полученные метрики объективно отражают последовательность действий каждого тестируемого субъекта на всех этапах инцидента, предоставляя профильным подразделениям обоснованную базу для принятия решений о необходимости корректирующего обучения.

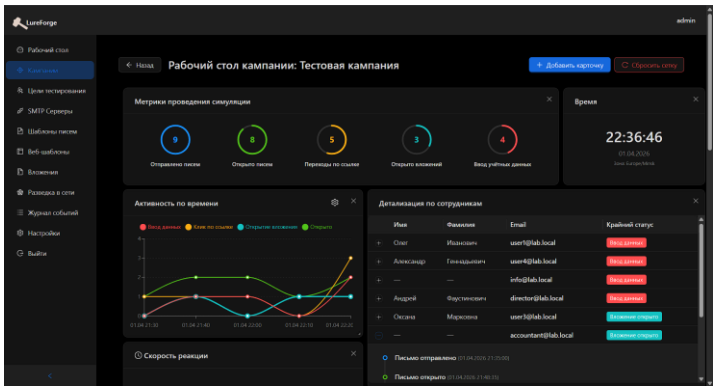


Рисунок 3 – Внешний вид рабочего стола в процессе симуляции

Проведенный анализ доказывает неэффективность теоретического обучения на фоне усложнения атак методами социальной инженерии. Предложенная платформа решает эту проблему, переводя подготовку персонала в практическую плоскость и автоматизируя аудит безопасности. Дальнейшее развитие комплекса направлено на интеграцию генеративного искусственного интеллекта с целью автоматического конструирования писем и веб-ресурсов. Дополнительно будет внедрена система «моментальной обратной связи» для проведения персонального инструктажа непосредственно в момент совершения ошибки, а также расширен спектр отслеживаемых вложений (PDF-документы, электронные таблицы, архивы) для тестирования устойчивости сотрудников к комплексным векторам компрометации.

Список использованных источников:

1. Фишинг в 2025 году стал основной угрозой для корпоративной почты [Электронный ресурс] // SecPost : аналитический портал. – Режим доступа: https://secpost.ru/fishing-v-2025-godu-stal-osnovnoj-ugrozoj-dlya-korporativnoj-pochty. – Дата доступа: 29.03.2026.

2. Фишинг в России [Электронный ресурс] // TAdviser : портал выбора технологий и поставщиков. – Режим доступа: https://www.tadviser.ru/index.php/Статья:Фишинг_в_России. – Дата доступа: 01.04.2026.

3. Phishing Activity Trends Reports (Q4 2025) [Electronic resource] // Anti-Phishing Working Group (APWG). – Режим доступа: https://docs.apwg.org/reports/apwg_trends_report_q4_2025.pdf. – Дата доступа: 29.03.2026.

4. Kaspersky spam and phishing report for 2025 [Electronic resource] // Securelist by Kaspersky. – Режим доступа: https://securelist.com/spam-and-phishing-report-2025/118785/. – Дата доступа: 29.03.2026.

5. IEEE Symposium on Security and Privacy 2025: Controlled study at UC San Diego Health [Electronic resource] // Scribd. – Режим доступа: https://www.scribd.com/document/908754843/ieee-25. – Дата доступа: 29.03.2026.

6. Phishing By Industry Benchmarking Report 2025 [Electronic resource] // KnowBe4. – Режим доступа: https://www.knowbe4.com/resources/reports/phishing-by-industry-benchmarking-report. – Дата доступа: 29.03.2026.

7. Архитектура платформы автоматизации аудита информационной безопасности / Е.А. Биюмен, К.Ц. Маршалова // Технические средства защиты информации: матер. XXIV Междунар. науч.-техн. конф., 2026. – С. 199–202.