УДК 33

Исследование эффективности комплексных методов социотехнического пентестинга, направленных на выявление уязвимостей человеческого фактора в корпоративных системах безопасности

Невзорова Алёна Денисовна

Студент,
Московский государственный технический университет им. Н.Э. Баумана,
105005, Российская Федерация, Москва, ул. 2-я Бауманская, 5;
e-mail: renynevzorova@yandex.ru

Овчинников Павел Романович

Студент,
Московский государственный технический университет им. Н.Э. Баумана,
105005, Российская Федерация, Москва, ул. 2-я Бауманская, 5;
e-mail: pasha20030610@gmail.com

Шепелев Денис Сергеевич

Студент,
Московский государственный технический университет им. Н.Э. Баумана,
105005, Российская Федерация, Москва, ул. 2-я Бауманская, 5;
e-mail: denishepelev4002@gmail.com

Моторин Данил Алексеевич

Студент,
Московский государственный технический университет им. Н.Э. Баумана,
105005, Российская Федерация, Москва, ул. 2-я Бауманская, 5;
e-mail: mda44@list.ru

Аннотация

Статья посвящена исследованию эффективности комплексных методов социотехнического пентестинга, направленных на выявление уязвимостей, связанных с человеческим фактором, в системах корпоративной безопасности. Актуальность работы обусловлена тем, что, несмотря на развитие технологических средств защиты, ошибки сотрудников остаются критическим звеном в цепи кибербезопасности, активно эксплуатируемым злоумышленниками через методы социальной инженерии. Авторы подчеркивают необходимость мультидисциплинарного подхода, интегрирующего знания из кибербезопасности, психологии, социологии и теории коммуникаций для создания реалистичных сценариев тестирования. В исследовании подробно рассматриваются

применяемые методики, включая моделирование фишинговых рассылок, телефонных атак с использованием претекстинга, внедрение вредоносных физических носителей и атак через мессенджеры. Особый акцент делается на комплексности тестирования, охватывающего различные каналы взаимодействия и учитывающего специфику организационной структуры, корпоративной культуры и удаленных форматов работы. Важными аспектами методологии признаются этическая корректность, предварительный анализ инфраструктуры компании и обеспечение конфиденциальности процесса для объективности результатов. Основные результаты работы выявили ключевые проблемы: недостаточную эффективность разовых тренингов по безопасности, сложность оценки реальной устойчивости персонала исключительно через количественные метрики (например, процент «клюнувших» на фишинг), влияние групповой динамики и организационной иерархии на поведение сотрудников, а также риски, связанные с гибридной работой и использованием личных устройств. Авторы показывают, что упрощенный подсчет ошибок менее информативен, чем анализ скорости и правильности реакции на инциденты, а также качественная оценка причин уязвимостей. Подчеркиваются важность прозрачной отчетности, ориентированной не только на ИТ-специалистов, но и на менеджмент, и необходимость использования результатов тестов для непрерывного совершенствования политик безопасности и программ обучения. Выводы исследования подтверждают, что комплексный социотехнический пентестинг является мощным инструментом для формирования устойчивой культуры безопасности. Его эффективность напрямую зависит от регулярности проведения, адаптации сценариев к эволюции угроз, учета психологических и организационных факторов, а также интеграции обратной связи в процессы обучения и управления. Авторы утверждают, что инвестиции в такие тесты – это вклад не только в снижение рисков, но и в повышение цифровой грамотности и коллективной ответственности сотрудников, превращающей человеческий фактор из слабого звена в активный элемент защиты.

Для цитирования в научных исследованиях

Невзорова А.Д., Овчинников П.Р., Шепелев Д.С., Моторин Д.А. Исследование эффективности комплексных методов социотехнического пентестинга, направленных на выявление уязвимостей человеческого фактора в корпоративных системах безопасности // Экономика: вчера, сегодня, завтра. 2025. Том 15. № 4А. С. 760-770.

Ключевые слова

Социотехнический пентестинг, человеческий фактор, корпоративная безопасность, фишинг, уязвимости.

Введение

Социотехнический пентестинг, ставший одной из ключевых методик проверки безопасности корпоративных систем, ориентирован не только на технологические аспекты, но и на психологические факторы, влияющие на поведение сотрудников в условиях потенциальной угрозы. Взаимодействие человека и технологии оказывается более сложным, чем может показаться на первый взгляд, потому что элементы социальной инженерии способны преодолевать наиболее надежные механизмы защиты за счет незаметных манипуляций или

обмана. При этом разработка интегрированных методов социотехнического пентестинга требует сочетания гибких сценариев, четкого планирования экспериментов и последующего анализа поведения участников с целью выявления слабых мест в системе защиты корпоративных данных. В начале таких исследований эксперты фокусировались в основном на технической стороне, однако со временем пришло понимание, что человеческий фактор нередко создает наиболее уязвимые точки, которые могут использовать злоумышленники. Поэтому комплексный подход к тестированию позволяет на практике проверить согласованность различных элементов системы безопасности и способность сотрудников противостоять социально инжинированным атакам. Развитие технологий и рост осведомленности о возможностях киберпреступников стимулируют компании усиливать обучение персонала, но без правильного моделирования реальных угроз проверить эффективность такого обучения оказывается сложно. Настоящий текст призван рассмотреть особенности комплексных методов социотехнического тестирования, а также те аспекты, которые делают человеческий фактор столь существенным в современных корпоративных средах.

Комплексность в социотехническом пентестинге проявляется во взаимодействии нескольких дисциплин: кибербезопасности, психологии, теории коммуникаций, этики и даже социологии. Каждый из этих компонентов дополняет общее представление о том, как люди реагируют на те или иные вызовы [Мельников, 2024]. Более того, важным является учет организационной культуры: компании с жесткой иерархической структурой могут по-разному реагировать на угрозы, нежели организации со свободным стилем управления. Исследователи в области социотехнического пентестинга стремятся не только выявить слабые места, но и понять, как участники теста осознают собственную ответственность за безопасность. Нередко формальные регламенты не гарантируют реальной устойчивости к социальной инженерии, так как пользователи склонны следовать привычкам или верить авторитетным фигурам. Следовательно, необходимость развивать критическое мышление и соответствующие когнитивные навыки в рабочем коллективе выходит на первый план. Все эти аспекты подчеркивают важность многостороннего анализа, который лежит в основе комплексного тестирования.

Материалы и методы исследования

В рамках социотехнического пентестинга исследователи часто прибегают к методу имитации фишинговых рассылок, так как электронная почта продолжает оставаться одним из самых распространенных каналов для атак. Цель подобных экспериментов – определить, насколько сотрудники готовы распознавать признаки фишинга, такие как подозрительные ссылки, необычные адреса отправителей или сомнительные вложения [Михалёва, 2023]. Однако рассылка писем – лишь часть возможных сценариев: практикуются также телефонные звонки с манипулятивными требованиями, социальная инженерия в мессенджерах, использование вредоносных USB-накопителей и прочие векторы. При этом координация всех каналов взаимодействия помогает выявить системные проблемы, ведь, если сотрудники не справляются с подобными угрозами в одном формате, велика вероятность, что аналогичные уязвимости возникнут и при иных методах воздействия. Проанализировав результаты таких тестов, компания может скорректировать инструкции и обучающие материалы, устранив основные пробелы в понимании сотрудниками собственной роли в обеспечении безопасности и снижении рисков. Технические меры защиты, такие как фильтры спама и системы обнаружения

вторжений, безусловно важны, но их работа нередко предполагает, что пользователь проявляет бдительность и не создает ненужных лазеек для злоумышленника. Отсюда берется идея интегрировать человеческий фактор в общую цепь киберзащиты.

При планировании комплексного социотехнического пентеста учитывается не только выбор сценариев, но и корректное моделирование угроз с учетом уникальных характеристик компании. Это предполагает сбор базовой информации об организационной структуре, изучение доступа сотрудников к различным ресурсам и анализ уже существующих политик информационной безопасности. На практике иногда оказывается, что политики формально прописаны, но не привиты в реальной практике либо быстро устаревают, не соответствуя меняющимся условиям [Потапова, 2020]. Исследователи, работающие в области пентестинга, уделяют особое внимание тому, чтобы тестовые сценарии максимально приближались к реальным, а результаты позволяли внести конкретные рекомендации по устранению недостатков. Важным моментом остается и этическая сторона: должна быть четко оговорена цель, круг вовлеченных лиц и методы, которые не причинят вреда ни инфраструктуре, ни персоналу. Более того, грамотно построенный процесс тестирования должен предусматривать, что некоторые сотрудники будут знать о проведении эксперимента, но не должны раскрывать его деталей коллегам, иначе результаты окажутся не вполне объективными. Когда компания придерживается подобного формата, она может быть уверена, что итоги теста отразят фактический уровень подготовки коллектива.

Результаты и обсуждение

В некоторых случаях эффективный социотехнический пентест включает не только внешних экспертов, но и внутренние ресурсы, чтобы обеспечить более масштабный охват. При этом возможны конфликты интересов, ведь внутренние специалисты могут неосознанно смягчать сценарии, избегая слишком провокационных методов. С другой стороны, их участие помогает более точно воспроизвести реальные условия, в которых работают сотрудники на постоянной основе [Краснянская, Тылец, 2022]. Оптимальным решением становится совместная работа внешней команды пентестеров и внутренних специалистов, где каждая группа вносит свою экспертизу. Ключевым моментом здесь остается предварительная договоренность о границах тестирования, четко прописанные цели и методология. Если подобные аспекты не уточнить заблаговременно, результаты окажутся смазанными. Таким образом, когда формируется единая рабочая группа, удается глубоко проработать возможные сценарии атак, включающие как технические, так и поведенческие модели взлома. Согласование действий всех участников позволяет комплексно взглянуть на потенциальные уязвимости и на то, каким образом их можно своевременно выявлять и устранять.

Сложность человеческого поведения проявляется в том, что люди, даже обладая знаниями о методах социальной инженерии, не всегда соблюдают правила информационной безопасности. Психологический фактор доверия и желания помочь остается сильным мотиватором. Некоторые исследования показывают, что сотрудники быстро забывают инструктаж, если не сталкиваются с реальными инцидентами или не видят наглядных последствий невнимательности [Барышников, 2024]. Поэтому одним из актуальных направлений становится организация периодических проверок, когда в разные промежутки времени актуализируются фишинговые рассылки и функциональные тесты на бдительность персонала. Такие проверки помогают поддерживать уровень внимательности и формируют

привычку критически оценивать входящую информацию. В этом контексте важно, чтобы руководство компании не сводило всю политику карательными мерами в случае нарушения. Гораздо эффективнее срабатывает разъяснительная работа, обучение и награждение лучших практик. Метод кнута и пряника здесь должен основываться на тонком психологическом понимании корпоративной культуры. К тому же необходимо учитывать постоянный цикл обучения, чтобы люди воспринимали кибербезопасность не как разовую акцию, а как элемент повседневной деятельности.

Расширение масштабов удаленной работы и облачных сервисов внесло дополнительные нюансы в социотехнический пентестинг. Если ранее значительная часть коммуникаций проходила внутри офисных сетей, то теперь сотрудники могут пересылать конфиденциальные данные по личной почте или пользоваться незащищенными Wi-Fi-сетями [Челейкина, Хромова, 2024]. Отсюда возникает потребность моделировать атаки, ориентированные на удаленных сотрудников: от перехвата данных в публичных точках доступа до целевых фишинговых попыток, связанных с инструментами совместной работы. Администраторам необходимо понимать, какие слабые места присутствуют в инфраструктуре, чтобы вовремя вводить многофакторную аутентификацию, шифрование и дополнительные проверки подлинности. Параллельно сотрудникам нужно регулярно напоминать, что их домашние устройства тоже могут стать объектом атаки, и объяснять, почему важно соблюдать рекомендации по обновлению операционных систем и использованию надежных паролей. Комплексный социотехнический пентест учитывает все эти аспекты для обеспечения целостного анализа. При этом рынок предлагает широкий ассортимент программного и аппаратного обеспечения, способствующего контролю удаленного доступа и минимизации риска утечек. Однако никакие технические средства не заменят человеческую ответственность и осознанное отношение к корпоративной безопасности со стороны каждого участника процесса.

Другая проблема, возникающая при организации пентестов, связана с оценкой эффективности проведенных мероприятий. В некоторых компаниях принято сводить итоги к простому подсчету числа сотрудников, которые «повелись» на фишинговую рассылку или проговорились во время телефонной социнжиниринговой атаки. Однако такой упрощенный подход не всегда дает полную картину. Более показательной метрикой признается анализ того, насколько быстро сотрудники сообщили о подозрительном письме в службу безопасности, либо вовремя ли уведомили системного администратора о нетипичном запросе доступов. Психологический контекст здесь важен: люди могут не только ошибаться, но и успешно противодействовать попыткам манипуляции. Построение системы показателей, отражающих реальную устойчивость коллектива к социально инжинированным атакам, требует внимательного подхода и зачастую опирается на качественные критерии. Некоторые компании инвестируют в специализированные платформы, которые помогают собирать автоматическую статистику по инцидентам во время тестов. Важно, чтобы руководство осознавало: одной лишь метрики «процент спровоцированных сотрудников» недостаточно для принятия осмысленных управленческих решений. Куда более эффективно совмещать количественные параметры с качественным анализом кейсов и мнением независимых экспертов.

Распространенная ошибка при реализации социотехнических пентестов – отсутствие продуманной стратегии обучения и реагирования на результаты. Проведя один раз фишинговую кампанию, некоторые специалисты считают задачу выполненной и не придают особого значения полученным статистическим данным. Однако, если не использовать результаты для корректировки программ обучения, аналитики и пересмотра политик, то ценность тестирования

резко снижается [Котляр, Мещеряков, Бугаев, 2021]. Существенное значение имеет и тайминговый аспект: повторные тесты желательно проводить через определенные промежутки времени, чтобы отследить динамику изменений. Если показатель взаимодействия с фишинговыми письмами снижается, значит принятые меры приносят плоды. Если же сотрудники продолжают допускать одни и те же ошибки, стоит задуматься над коренными причинами. Возможно, инструкции формальные и невнятные, или сотрудники попросту перегружены информацией и не успевают усвоить материал. Комплексные методы подразумевают непрерывное совершенствование: от планирования и реализации до анализа и внедрения корректив.

Важнейшим этапом в социотехническом пентесте считается заключительная фаза, связанная с подготовкой отчетов. Эти отчеты не должны быть сугубо техническими, так как их целевая аудитория – не только ИТ-специалисты, но и менеджеры, принимающие решения об инвестициях в безопасность. Помимо цифровых показателей, вроде количества открытых фишинговых писем и времени реакции, в документах важно отражать поведенческие аспекты, указывая, какие именно уязвимости повлияли на результаты [Feotkulov, Maslova, 2024]. Изложение результатов должно дать исчерпывающее понимание того, какие ошибки совершают сотрудники, почему они их совершают, и какие меры помогут минимизировать подобное в будущем. При этом важна корректная формулировка: отчет – не способ указать на виновных, а метод повышения осведомленности и эффективности всей системы защиты. Результаты тестирования дают возможность показать сотрудникам, что их действия непосредственно влияют на общую безопасность организации. И если люди видят, что руководство не использует отчеты для наказания, а принимает конкретные шаги к улучшению корпоративной культуры в сфере защиты данных, то это стимулирует более внимательное отношение к безопасности в повседневной деятельности.

Если говорить о практических инструментах, то комплексный социотехнический пентест может включать несколько этапов: сбор и анализ открытой информации о сотрудниках и компании, подготовку персонализированных сценариев атаки, внедрение тестовых векторов (фишинговые письма, звонки, физический доступ), фиксацию результатов каждой попытки и их структурированный анализ. В отличие от чисто технического пентеста, социально ориентированные методы предполагают тонкую настройку психологической составляющей. Задача – не только проникнуть в систему, но и выяснить, как именно человек поддается на манипуляции [Гельфанд, Кузнецов, Анучин, 2024]. К примеру, один сотрудник может ответить на подозрительную почту, другой – сообщить внутренние данные по телефону якобы коллеге из соседнего отдела, а кто-то третьий – пропустить незнакомца в офис под предлогом срочности. Эти эпизоды складываются в общую картину уязвимостей, которые нужно исправлять. Важно понимать, что такой пентест, проводимый без должной подготовки и этических норм, способен нанести ущерб доверительным отношениям внутри компании. Поэтому четкие правила игры и прозрачность целей особенно значимы.

С точки зрения корпоративной культуры на этапе результатов возникает еще одна тонкость: некоторые менеджеры опасаются, что тестирование создаст в коллективе атмосферу подозрительности и сократит желание поддерживать открытую коммуникацию. Реально подобный риск существует, если применяются жесткие или провокационные сценарии, и методика не сопровождается разъяснением. Однако грамотное внедрение, основанное на идее общего вклада в безопасность, обычно наоборот повышает уровень доверия, так как люди

осознают, что уязвимые места есть везде, и цель пентеста – научить их вовремя определять угрозы. Прозрачно представленные итоги демонстрируют, что кибербезопасность – это командная игра, где каждый берет на себя часть ответственности. Важно, чтобы менеджмент делился обратной связью и достижениями компании в противодействии атакам, демонстрируя положительный эффект от обучения. Тогда даже те сотрудники, которые ошибались во время теста, увидят в этом процессе не угрозу, а возможность прокачать компетенции.

Роль психологических методов в пентестинге не ограничивается манипулятивными техниками. Исследователи также учитывают аспекты социальной идентичности и групповой динамики. Например, сотрудники могут испытывать давление со стороны неформальных лидеров или следовать общепринятым нормам, если в коллективе сформировалась привычка некритично пропускать письма от неизвестных адресатов или делиться паролями. В таких условиях внедрять изменения и обучать персонал приходится с учетом особенностей поведения группы. Более того, если организация распределена по разным странам и культурам, одни и те же методы социальной инженерии могут работать по-разному. Учет этого фактора помогает более точно создавать сценарии пентеста, ориентированные на реальные коммуникативные стили и традиции взаимодействия внутри коллектива. Это еще раз указывает на важность системного подхода, когда эксперты по безопасности, психологи и социологи совместно формируют концепцию тестирования.

Заключение

Перспективы развития также включают более тесную кооперацию между разными отраслями, обмен опытом и создание лучших практик. Корпорации, однажды столкнувшиеся с утечками, зачастую более охотно делятся методологиями. Социотехнические пентесты могут стать обязательной частью аудита безопасности в ряде высокорисковых секторов, включая финансовый, энергетический и государственный [Потапова, 2020]. Комплексный характер подхода становится своеобразным стандартом, так как без анализа человеческих факторов невозможно понять истинную картину защищенности. Исследователи и практики все активнее интегрируют данные из социальных сетей, бизнес-процессов и закрытых корпоративных каналов, моделируя сценарии, максимально приближенные к реальности. Именно такая детализация позволяет подметить тонкие аспекты взаимодействия сотрудников, для которых традиционные техничные пентесты не дают ответов. При этом, благодаря развитию облачных решений и инструментов аналитики больших данных, появляется шанс глубже анализировать результаты, выявляя закономерности и тренды, которые были незаметны ранее.

Таким образом, эффективность комплексных методов социотехнического пентестинга напрямую связана с мультидисциплинарным и многоуровневым подходом. При одновременном учете психологических, организационных и технологических факторов становится возможным более тонко и объективно оценивать уровень защищенности корпоративных систем. Регулярные тестирования, продуманные программы обучения и прозрачная отчетность ведут к формированию устойчивой культуры безопасности, где каждый сотрудник понимает, что он – часть общей системы защиты, а не пассивное звено [Мельников, 2024]. Несмотря на то, что технический прогресс делает системы все более надежными, ошибка пользователя по-прежнему остается фактором риска, и именно поэтому тесты, учитывающие человеческий аспект, актуальны как никогда. Проведение же комплексных методов социотехнического пентестинга

требует не только компетенций, но и дальновидного менеджмента, готового инвестировать в долгосрочную безопасность и развитие сотрудников.

Библиография

1. Абрамов М.В., Тулупьева Т.В., Тулупьев А.Л., Бушмелев Ф.В. Цифровизация публичного управления: социоинженерные риски // Научные труды Северо-Западного института управления РАНХиГС. 2022. Т. 13. № 1 (53). С. 5-16.
2. Барышников П.В. Социальная инженерия и человеческий фактор в информационной безопасности: угрозы и защита // Научный Альманах ассоциации France-Kazakhstan. 2024. № 2. С. 268-272.
3. Виноградова В.Л., Милованова Л.Р. Социальная инженерия в киберпространстве: манипулируя человеческим фактором // Наукосфера. 2024. № 1-2. С. 157-161.
4. Гельфанд А.М., Кузнецов С.А., Анучин К.Н. Совершенствование защиты от социальных атак в области информационной безопасности // Международный журнал информационных технологий и энергоэффективности. 2024. Т. 9. № 4 (42). С. 89-94.
5. Котляр Е.О., Мещеряков М.О., Бугаев К.Г. Методы социальной инженерии как инструмент хищения конфиденциальных данных пользователей // Охрана, безопасность, связь. 2021. № 6-2. С. 223-230.
6. Краснянская Т.М., Тылец В.Г. Факторы угрозы корпоративной безопасности: систематизация подходов и определение их признаков // Институт психологии Российской академии наук. Социальная и экономическая психология. 2022. Т. 7. № 4 (28). С. 122-143.
7. Мельников А.И. Социальная инженерия в цифровой эпохе: анализ методов манипуляции человеческим фактором в целях кибератак // Социально-гуманитарные знания. 2024. № 1. С. 50-54.
8. Михалёва У.А. Претекстинг и способы противодействия ему // Вестник Дагестанского государственного технического университета. Технические науки. 2023. Т. 50. № 2. С. 109-116.
9. Останина Е.А. Counteraction to methods of social engineering as one of the areas of information protection of organizations with varying degrees of state participation // Amazonia Investiga. 2021. Т. 10. № 38. С. 123-129.
10. Останина Е.А. Обучение как противодействие методам социальной инженерии // Человеческий капитал. 2021. № 3 (147). С. 172-180.
11. Потапова К.А. Политика противодействия атакам, совершённым с использованием социальной инженерии в корпоративной среде // ИТ-Стандарт. 2020. № 4 (25). С. 31-37.
12. Санина Л.В., Чепинога О.А., Ржепка Э.А., Палкин О.Ю. Деструктивная социальная инженерия как угроза экономической безопасности: масштабы явления и меры предотвращения // Baikal Research Journal. 2021. Т. 12. № 2. С. 1-10.
13. Хлобыстова А.О., Абрамов М.В. Адаптация модели многоходовых социоинженерных атак с учётом информационного влияния // Международная конференция по мягким вычислениям и измерениям. 2021. Т. 1. С. 65-68.
14. Челейкина С.З., Хромова А.В. Социальная инженерия в сфере корпоративной безопасности: анализ угроз, предупреждение инцидентов и стратегии защиты // Информационные войны. 2024. № 1 (69). С. 74-79.
15. Feotkulov S.A.S., Maslova O.V. Analysis of the influence of the human factor on effectiveness of the scenario approach // Молодежь. Общество. Современная наука, техника и инновации. 2024. № 23. С. 131-133.

Research on the effectiveness of comprehensive sociotechnical penetration testing methods aimed at identifying human factor vulnerabilities in corporate security systems

Alena D. Nevzorova

Student,
Moscow State Technical University named after N.E. Bauman,
105005, 5 2-ya Baumanskaya str., Moscow, Russian Federation;
e-mail: renynevzorova@yandex.ru

Pavel R. Ovchinnikov

Student,
Moscow State Technical University named after N.E. Bauman,
105005, 5 2-ya Baumanskaya str., Moscow, Russian Federation;
e-mail: pasha20030610@gmail.com

Denis S. Shepelev

Student,
Moscow State Technical University named after N.E. Bauman,
105005, 5 2-ya Baumanskaya str., Moscow, Russian Federation;
e-mail: denishepelev4002@gmail.com

Danil A. Motorin

Student,
Moscow State Technical University named after N.E. Bauman,
105005, 5 2-ya Baumanskaya str., Moscow, Russian Federation;
e-mail: mda44@list.ru

Abstract

This article is devoted to studying the effectiveness of comprehensive sociotechnical penetration testing methods aimed at identifying vulnerabilities related to the human factor in corporate security systems. The relevance of the work is due to the fact that despite the advancement of technological protection measures, employee errors remain a critical link in the cybersecurity chain, actively exploited by attackers through social engineering techniques. The authors emphasize the need for a multidisciplinary approach that integrates knowledge from cybersecurity, psychology, sociology, and communication theory to create realistic testing scenarios. The study examines in detail the applied methodologies, including modeling phishing mailings, telephone attacks using pretexting, introducing malicious physical media, and attacks via messaging apps. Special attention is paid to the comprehensiveness of testing, covering various communication channels and taking into account the specifics of the organizational structure, corporate culture, and remote work formats. Ethical correctness, preliminary analysis of the company's infrastructure, and ensuring the confidentiality of the process for objective results are recognized as important methodological aspects. The main results of the work identified key issues: the insufficient effectiveness of one-off security trainings, the difficulty of assessing personnel's real resilience solely through quantitative metrics (for example, the percentage of those who "fell for" phishing), the influence of group dynamics and organizational hierarchy on employee behavior, as well as risks associated with hybrid work and the use of personal devices. The authors argue that a simplified count of mistakes is less informative than analyzing the speed and accuracy of incident responses, as well as qualitatively assessing the root causes of vulnerabilities. The importance of transparent reporting geared not only to IT specialists but also to management, and the need to use test results for the continuous improvement of security policies and training programs, is emphasized. The study's conclusions confirm that comprehensive sociotechnical penetration testing is a powerful tool for shaping a sustainable security culture. Its effectiveness directly depends on the regularity of testing, the adaptation of

scenarios to the evolution of threats, the consideration of psychological and organizational factors, and the integration of feedback into training and management processes. The authors assert that investments in such tests are not only a contribution to reducing risks but also to improving digital literacy and collective responsibility among employees, turning the human factor from a weak link into an active element of defense.

For citation

Nevzorova A.D., Ovchinnikov P.R., Shepelev D.S., Motorin D.A. (2025) Issledovanie effektivnosti kompleksnykh metodov sotsiotekhnicheskogo pentestinga, napravlennykh na vyyavlenie uyazvimostei chelovecheskogo faktora v korporativnykh sistemakh bezopasnosti [Research on the effectiveness of comprehensive sociotechnical penetration testing methods aimed at identifying human factor vulnerabilities in corporate security systems]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 15 (4A), pp. 760-770.

Keywords

Sociotechnical penetration testing, human factor, corporate security, phishing, vulnerabilities

References

1. Abramov M.V., Tulupieva T.V., Tulupiev A.L., Bushmelev F.V. (2022) Tsifrovizatsiya publichnogo upravleniya: sotsioinzhenernye riski [Digitalization of Public Administration: Socio-Engineering Risks]. Nauchnye trudy Severo-Zapadnogo instituta upravleniya RANKhiGS [Scientific Works of the North-Western Institute of Management RANEPA], 13 (1 (53)), p. 5-16.
2. Baryshnikov P.V. (2024) Sotsialnaya inzheneriya i chelovecheskiy faktor v informatsionnoy bezopasnosti: ugrozy i zashchita [Social Engineering and Human Factor in Information Security: Threats and Protection]. Nauchnyy Almanakh assotsiatsii France-Kazakhstan [Scientific Almanac of the France-Kazakhstan Association], 2, p. 268-272.
3. Cheleykina S.Z., Khromova A.V. (2024) Sotsialnaya inzheneriya v sfere korporativnoy bezopasnosti: analiz ugroz, preduprezhdenie intsidentov i strategii zashchity [Social Engineering in Corporate Security: Threat Analysis, Incident Prevention and Protection Strategies]. Informatsionnye voyny [Information Wars], 1 (69), p. 74-79.
4. Feotkulov S.A.S., Maslova O.V. (2024) Analysis of the influence of the human factor on effectiveness of the scenario approach. Molodezh. Obshchestvo. Sovremennaya nauka, tekhnika i innovatsii [Youth. Society. Modern Science, Technology and Innovations], 23, p. 131-133.
5. Gelfand A.M., Kuznetsov S.A., Anuchin K.N. (2024) Sovershenstvovanie zashchity ot sotsialnykh atak v oblasti informatsionnoy bezopasnosti [Improving Protection Against Social Attacks in the Field of Information Security]. Mezhdunarodnyy zhurnal informatsionnykh tekhnologiy i energoeffektivnosti [International Journal of Information Technologies and Energy Efficiency], 9 (4 (42)), p. 89-94.
6. Khlobystova A.O., Abramov M.V. (2021) Adaptatsiya modeli mnogokhodovykh sotsioinzhenernykh atak s uchyotom informatsionnogo vliyaniya [Adaptation of a Model of Multi-Stage Socio-Engineering Attacks Taking into Account Information Influence]. Mezhdunarodnaya konferentsiya po myagkim vychisleniyam i izmereniyam [International Conference on Soft Computing and Measurements], 1, p. 65-68.
7. Kotlyar E.O., Meshcheryakov M.O., Bugaev K.G. (2021) Metody sotsialnoy inzhenerii kak instrument khishcheniya konfidentsialnykh dannykh polzovateley [Social Engineering Methods as a Tool for Stealing Users' Confidential Data]. Okhrana, bezopasnost, svyaz [Security, Safety, Communications], 6-2, p. 223-230.
8. Krasnyanskaya T.M., Tyilets V.G. (2022) Faktory ugrozy korporativnoy bezopasnosti: sistematizatsiya podkhodov i opredelenie ikh priznakov [Threat Factors to Corporate Security: Systematization of Approaches and Definition of Their Characteristics]. Institut psikhologii Rossiyskoy akademii nauk. Sotsialnaya i ekonomicheskaya psikhologiya [Institute of Psychology of the Russian Academy of Sciences. Social and Economic Psychology], 7 (4 (28)), p. 122-143.
9. Melnikov A.I. (2024) Sotsialnaya inzheneriya v tsifrovoy epokhe: analiz metodov manipulyatsii chelovecheskim faktorom v tselyakh kiberatak [Social Engineering in the Digital Age: Analysis of Methods of Manipulating the Human Factor for Cyberattacks]. Sotsialno-gumanitarnye znaniya [Socio-Humanitarian Knowledge], 1, p. 50-54.
10. Mikhaleva U.A. (2023) Preteksting i sposoby protivodeystviya emu [Pretexting and Ways to Counteract It]. Vestnik Dagestanskogo gosudarstvennogo tekhnicheskogo universiteta. Tekhnicheskie nauki [Bulletin of Dagestan State Technical University. Technical Sciences], 50 (2), p. 109-116.
11. Ostanina E.A. (2021) Counteraction to methods of social engineering as one of the areas of information protection of

organizations with varying degrees of state participation. Amazonia Investiga, 10 (38), p. 123-129.
12. Ostanina E.A. (2021) Obuchenie kak protivodeystvie metodam sotsialnoy inzhenerii [Training as a Counteraction to Social Engineering Methods]. Chelovecheskiy kapital [Human Capital], 3 (147), p. 172-180.
13. Potapova K.A. (2020) Politika protivodeystviya atakam, sovershyonnym s ispolzovaniem sotsialnoy inzhenerii v korporativnoy srede [Policy for Countering Attacks Perpetrated Using Social Engineering in the Corporate Environment]. IT-Standart [IT-Standard], 4 (25), p. 31-37.
14. Sanina L.V., Chepinoga O.A., Rzhepka E.A., Palkin O.Yu. (2021) Destruktivnaya sotsialnaya inzheneriya kak ugroza ekonomicheskoy bezopasnosti: masshtaby yavleniya i mery predotvrashcheniya [Destructive Social Engineering as a Threat to Economic Security: Scale of the Phenomenon and Prevention Measures]. Baikal Research Journal, 12 (2), p. 1-10.
15. Vinogradova V.L., Milovanova L.R. (2024) Sotsialnaya inzheneriya v kiberprostranstve: manipuliruya chelovecheskim faktorom [Social Engineering in Cyberspace: Manipulating the Human Factor]. Naukosfera [Science Sphere], 1-2, p. 157-161.