DOI 10.36622/VSTU.2022.25.1.006
УДК 378:004.056.57

СОЦИОТЕХНИЧЕСКОЕ ТЕСТИРОВАНИЕ В УСЛОВИЯХ ПОДГОТОВКИ БУДУЩИХ СПЕЦИАЛИСТОВ СФЕРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ЭТАПЫ ПРОВЕДЕНИЯ И СЦЕНАРИИ АТАК

З.В. Семенова, Н.А. Моисеева, Е.В. Толкачева, Д.А. Бибик

В статье представлен анализ современного состояния проблемы атак на основе социальной инженерии. Рассматриваются методы и средства формирования иммунитета к атакам социальной инженерии вообще и фишинговым атакам, в частности. Проведен анализ современных подходов, отражающих основные этапы и сценарии проведения социотехнического тестирования, а также анализ терминологии в этой области. Обосновывается необходимость проведения социотехнических учений (Social Engineering Penetration Testing) для 100% студентов высших учебных заведений. Выявлены особенности учебного процесса, которые существенным образом влияют на подготовку и проведение социотехнического тестирования. Предложены техническая и программная инфраструктуры социотехнического тестирования. Подробно описаны пять сценариев, которые предлагается реализовать в рамках социотехнического тестирования. Кроме того, представлены ряд ограничений применения сценариев, совокупность созданных сервисов, обеспечивающих реализацию предложенных сценариев социотехнического тестирования и условия проведения подготовительных работ.

Ключевые слова: информационная безопасность, кибератака, атака социальной инженерии, социотехническое тестирование, тестирование на проникновение в социальную инженерию.

Введение

На фоне развития и массового внедрения технических и программных средств защиты информации наблюдается рост инцидентов информационной безопасности (ИБ), обусловленных атаками социальной инженерии (СИ) [1, 3-8]. Эта проблема характерна для различных сфер деятельности: от финансовой и научной до медицины и образования.

Данные, заслуживающие пристального внимания, приводит румынская компания Bitdefender, занимающаяся разработкой программного обеспечения в области киберзащиты. Проведенный ею опрос более 6,5 тысяч руководителей и сотрудников департаментов ИБ и ИТ-подразделений из 10 стран различных континентов свидетельствует, что самое большое количество респондентов (26%) указывает на рост в 2020 г. количества фишинговых атак.

По данным аналитического отчета центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) Департамента ИБ Банка России в 2020 г. наблюдалось существенное увеличение количества фишинговых ресурсов, связанных с финансовой поддержкой населения в связи с COVID-19. Пик их появления в русскоязычном сегменте приходится на июль 2020, когда злоумышленниками было создано и размещено в сети интернет более 20000 таких ресурсов.

Согласно отчету мирового лидера в области решений для защиты корпоративных данных и кибербезопасности Trend Micro [9] вредоносные программы, фишинг и фишинговые атаки, целью которых являются учетные данные пользователей, резко выросли в 2020 г. Как правило, фишинговые атаки, при которых злоумышленники крадут учетные данные электронной почты сотрудников, реализуются через поддельные страницы входа.

Данные Trend Micro Cloud App Security показывают, что в 2020 г. было обнаружено и заблокировано 5 465 969 фишинговых атак с использованием учетных данных, что на 14% больше, чем годом ранее. При этом, как следует из отчета, 94% целевых электронных писем используют вложения вредоносных файлов или источника заражения. Остальные 6% используют альтернативные методы, такие как установка вредоносных программ по вредоносным ссылкам [9].

Специалисты в области ИБ все чаще указывают на то, что одним из самых эффективных способов формирования устойчивых навыков противостояния атакам СИ является проведение социотехнических тестирований (тренингов).

Показательным являются результаты таких тренингов, организованные и проведенные службой киберкультуры Сбербанка. Ее руководитель К. Лопатина высоко оценивает их результаты. Акцентируя внимание на широком охвате тренингов (около 300 тысяч сотрудников центрального офиса и филиалов), руководитель отмечает, что регулярность их проведения позволила существенно снизить процент сотрудников, которые не смогли противостоять атаке СИ с 48% (в 2016 г.) до 1,6% (в 2018 г.) [2].

Сегодня на ИТ-рынке достаточное количество компаний, предлагающих услугу по проведению социотехнического тестирования (СТТ) для предприятий малого и среднего бизнеса. Однако отметим, что на сегодняшний день нельзя говорить о широкой практике таких тренингов. Значительно чаще происходит лишь повышение осведомленности сотрудников в области кибербезопасности вообще и в области социальной инженерии (СИ), в частности. Используемые подходы традиционные - лекции, семинары, беседы и т.п. При этом успех тем выше, чем более подходящий для конкретного индивида применяется метод влияния. Ряд специалистов подчеркивают, что зачастую страх используется как метод убеждения в сфере кибербезопасности.

Эксперты сферы кибербезопасности убедительно обосновывают необходимость проведения СТТ на регулярной основе. Ш. Давидофф, являющаяся экспертом в области тестирования на проникновение, а также автором книги Philosecurity, указывает на такую важнейшую роль СТТ, как возможность выявить сильные и слабые стороны отдельных сотрудников или целых подразделений, что позволяет планировать обучающие семинары и пр. При этом и само по себе СТТ, по мнению Ш. Давидофф "... является ключевым компонентом обучения по вопросам ИБ и помогает закрепить позитивное поведение" [4].

Авторы данной статьи вслед за многими экспертами убеждены, что уже в средней школе необходимо формировать навыки противостояния атакам СИ. При этом обучение целесообразно проводить на основе активных методов: лишь просветительская работа не способна обеспечить значимый результат.

Если в отношении школьников проведение СТТ является желательным, то для студентов высших учебных заведений и колледжей такие тренинги обязательны, в чем мы глубоко убеждены. Еще одним из важнейших аргументов в пользу этого является то, что исследования S. M. Albladi и G. R.Weir показали, что именно молодые люди наиболее уязвимы атакам СИ, именно они чаще всего становятся жертвами фишинговых атак [5].

Постановка задачи

Многочисленные исследования и опыт проведения СТТ в различных организациях убедительно свидетельствуют о том, что оно является одним из самых эффективных способов формирования устойчивого иммунитета против атак СИ. В высших учебных заведениях, как уже подчеркивалось выше, такие тестирования должны охватывать 100% обучаемых. Здесь возникает ряд проблем, требующих решения. Прежде всего - это невозможность без модификации использовать методику, которой придерживаются компании, предлагающие в качестве услуги проведение СТТ сотрудников той или иной организации. Во-вторых, вся инфраструктура СТТ (техническое и программное обеспечение) требует учитывать специфику функционирования образовательного учреждения. Кроме того, важно определить каковы особенности разработки сценариев таких тренингов.

Теория

Эксперты и специалисты сферы ИБ до сих пор, говоря об активных методах формировании навыков противодействия атакам СИ, используют различающиеся между собой термины. J. M. Archibald и K. Renaud, подчеркивая необходимость проведения СТТ, рассматривают его в рамках тестирования на проникновение и используют для его обозначения такой термин, как "пентестинг человека в социотехнической системе" [6]. Многочисленные компании, оказывающие услуги по проверке того, как в организации обеспечивается соблюдение сотрудниками

стандартов безопасности, как правило, используют термин “Social Engineering Penetration Testing”. Одна из ведущих консалтинговых компаний, работающая в области обучения по ИБ Social-Engineer (LLC, США) и ее директор, автор научных книг по вопросам СИ Кристофер Хаднаги использует такое словосочетание, как Adversarial Simulation. Учебный центр Сибирской Академии ИБ (Россия) наряду с термином “социотехническое тестирование” использует термин “Имитированные массовые и таргетированные фишинговые рассылки по запросу”.

Сегодня практически все эксперты сферы кибербезопасности констатируют тот факт, что самым слабым звеном в кибербезопасности компании является сотрудник. Они подчеркивают, что как никогда важно развивать культуру коллективной кибербезопасности и корпоративной ответственность. Компании предпринимают разные подходы, готовя своих сотрудников противостоять атакам социальной инженерии. Мы условно разделяем эти подходы на 4 группы: пассивные, полуактивные, активные и сверхактивные.

Среди пассивных подходов: пассивное обучение сотрудников (беседы, лекции, семинары); подход, основанный на правилах (для сотрудников составляются инструкции, которые рекомендуется неукоснительно выполнять). Данные подходы малоэффективны. Для повышения эффективности в рамках обучающих семинаров акцентируют внимание на возможном финансовом ущербе, который может наступить из-за некорректных действий конечного пользователя. Таким образом, главный мотив - это чувство страха принести ущерб компании, в которой работает пользователь.

К полуактивным методам мы относим тренинги, которые подразумевают на фоне информированности сотрудником о проверке их устойчивости к атакам СИ проведение викторин интерактивных лекций использование интернет-ресурсов на распознавание, например, фишинга.

СТТ - один из самых эффективных активных методов. Эксперты подчеркивают, что многие пользователи с трудом противостоят фишинговым атакам до тех пор, пока не станут жертвой атаки СИ. Важно подчеркнуть, что тестируемые заранее не осведомлены, что будет реализована управляемая атака СИ. В этом случае каждый тестируемый поступает исходя из своего опыта, уровня осознанности своих действий и осведомленности в области СИ. Если управляемая атака завершается успешно, то это фиксируется и затем подлежит тщательному разбору. Таким образом, индивид приобретает негативный опыт, важную роль здесь играет видимость реальных условий и фактор легкого стресса.

Накоплен колоссальный теоретический и практический опыт проведения таких управляемых атак. Специалисты предлагают подробное описание всех этапов проведения СТТ [7], которое начинается с этапа разведки и может заканчиваться формированием отчетности (рис. 1).

Рис. 1. Этапы СТТ

Множество работ специалистов описывают в целом единый подход к разработке сценариев атак СИ. Так, например, в работе [8] представлен типовой шаблон сценария атаки, включающий в себя 6 шагов (табл. 1)

Если для компании, заказавшей СТТ, все этапы реализуются стандартно, то в системе высшего образования при главной целевой установке - повышение уровня противостояния атакам СИ для каждого студента, отдельные этапы претерпевают существенную модификацию.

Следует обратить внимание на то, что ряд экспертов считает, что высшая школа особенно уязвима для атак СИ. Так, в частности, T. Nguyen и S. Bhatia [1] указывают на то, что: “Высшие учебные заведения - главная цель миссий по СИ”. Это,

по мнению авторов, обусловлено тем, что именно в высшей школе наблюдается массовые притоки и оттоки студентов, преподавателей и сотрудников, которые так или иначе влияют на ИТ-экосистему учебного заведения. Именно эти трансферы добавляют от сотен до тысяч динамических уязвимостей их ИТ-экосистемы и ИБ. Авторы предлагают использовать регулярные тренинги, включая СТТ..

Таблица 1

Шаги типового шаблона сценария атаки СИ

Шаг	Состав шага
Шаг 1. Формулировка цели атаки	1.1. Определение цели. 1.2. Идентификация объектов и субъектов цели.
Шаг 2. Сбор информации	2.1. Определение потенциальных источников. 2.2. Сбор информации из источников. 2.3. Оценка собранной информации.
Шаг 3. Подготовка атаки	3.1. Анализ собранной информации. 3.2. Развитие вектора атаки.
Шаг 4. Установление контактов	4.1. Налаживание коммуникации. 4.2. Установление взаимопонимания.
Шаг 5. Использование контактов	5.1. Предварительная подготовка к запросу на доступ к объекту цели. 5.2. Запрос на доступ к объекту цели.
Шаг 6. Подведение итогов	6.1. Уведомление субъектов цели об успешном выполнении запроса на доступ к объекту цели. 6.2. Получение несанкционированного доступа к объекту цели. 6.3. Достижение цели.

Положительные результат обучения студентов СИ на примере СТТ представлен в работе американских специалистов A. Luse и J. Burkman [6]. В этом исследовании подробно описывается проект образовательного назначения, в котором студенты реализовали тренинг фишинговой атаки в реальной обстановке, т. е. на реальную компанию. Авторами представлен подробный сценарий фишинговый атаки и описана ее реализация. Участие студентов в подобных проектах можно отнести к сверхактивным методом обучения противостояния атакам СИ. В процессе проведения проекта использовались активные методы обучения в интерактивном режиме – активное взаимодействие всех участников проекта, интерактивная техническая фишинговая среда и оперативная обратная связь между студентами и сотрудниками компании. В качестве технической фишинговой среды использовалось свободно распространяемое программное обеспечение Gophish с открытым исходным кодом (https://getgophish.com/).

Благодаря активному взаимодействию с внешним корпоративным партнером студенты изучили правовые, технические, поведенческие, аналитические и отчетные аспекты социальной инженерии. Результат предоставил как полезные данные для реальной компании, так и уникальный ценный образовательный опыт для будущих специалистов в ИБ сфере.

К сожалению, описанный уникальный опыт, полученный в этой работе, распространяется не на всех обучающихся студентов, а факультативно. т. е. на часть студентов.

При этом многочисленные исследователи подчеркивают, что активное обучение устойчивым навыкам противостояния атакам СИ должно охватывать 100% молодых людей, поскольку возраст от 17 до 24 лет является наиболее уязвимым для атак СИ [5], [12].

Уже на первом курсе подготовки будущего специалиста любого направления и специальности и, особенно - сферы ИБ, следует проводить первое СТТ. При этом при подготовке и проведении данного тестирования важно учесть ряд особенностей протекания учебного процесса, а традиционные для рядовых компаний сценарии необходимо адаптировать.

Обсуждение результатов

Процесс обучения в вузе имеет ряд особенностей, приводящих к необходимости корректировки типовых этапов и шаблонов сценариев атак для проведения СТТ. В табл. 2 представлен перечень модификаций типового

подхода к подготовке и проведению СТТ с учетом выявленных особенностей.

Таблица 2

Влияние особенностей процесса обучения на структуру типового подхода к подготовке и проведению СТТ

№ п/п	Рабочий процесс в компании	Образовательный процесс в вузе	Особенности подготовки и проведения СТТ
1.	Сотрудники проходят СТТ выборочно.	Необходимо обеспечить возможность тестирования всех обучающихся.	Этап формирования базы сотрудников исключается, СТТ проводится для всех обучающихся.
2.	СТТ проводится на рабочих сервисах.	Не целесообразно вмешательство в образовательный процесс. Необходимо сохранение целостности образовательного процесса.	Этап формирования списка сервисов заменяется на этап проектирования, разработки и развертывания отдельных сервисов для проведения СТТ.
3.	Сотрудник имеет свое рабочее место и использует его в течение всего рабочего дня.	Конкретный обучающийся не привязан к рабочему месту.	Необходимо предусмотреть этап вовлечения обучающихся в использование разработанных сервисов, не связанных с образовательным процессом.
4.	Сотрудник любой компании использует корпоративные ресурсы в рамках своего функционала.	Основной функционал обучающихся - выполнение учебных заданий и задач и ведение портфолио личных достижений.	В качестве сервисов для проведения СТТ могут быть реализованы сервисы для работы с корпоративной электронной почтой и для работы с распорядительной документацией.
5.	СТТ не ограничено по времени.	СТТ должно быть ограничено по времени (1-2 пары).	В сценарии атак целесообразно исключить шаг налаживания контактов, а для сокращения времени атаки рассылать фишинговые письма от имени лиц, с которыми контакт ранее установлен.
6.	Устранение контролируемых последствий СТТ не ограничено по времени.	По окончании тестирования рабочие места должны быть до конца занятия возвращены в исходное состояние.	Необходимо предусмотреть в составе инфраструктуры наличие виртуальных машин и подконтрольного сегмента локальной вычислительной сети вуза.
7.	СТТ может проводиться при участии сторонних организаций.	СТТ проводят сотрудники вуза и обучающиеся старших курсов.	Из шаблона сценариев целесообразно исключить предварительный сбор информации и установление контактов с субъектами атак.
8.	Сотрудники различных подразделений подвергаются типовым атакам СИ.	Целесообразно использовать индивидуальный подход при выборе атаки СИ.	Требуется более широкий спектр легенд для атак СИ, учитывающих индивидуальные особенности обучающихся, выявляемые в ходе предварительной индивидуальной работы с обучающимися.

Совокупность созданных сервисов может образовывать, например, корпоративную информационную систему (КИС), в состав которой входит корпоративная почта, корпоративная система электронного документооборота (СЭД) и сервис для проведения опросов обучающихся для сбора различных сведений по запросам кафедр. На рис. 2 представлен бизнес-процесс взаимодействия пользователей с корпоративной почтой и СЭД.

Для работы с СЭД обучающиеся должны пройти процедуру авторизации. Сервис для сбора сведений об обучающихся не предполагает авторизации, что необходим для проведения анонимных опросов обучающихся, например, об интересующей их тематике кружков и дополнительных спецкурсов (в случае проведения не анонимных опросов в форму опросника добавляются обязательные для заполнения поля ввода сведений, идентифицирующих обучающихся).

ИТ-инфраструктура КИС представляет собой сеть, объединяющую ряд физических и виртуальных серверов, а также физических и виртуальных ПК пользователей, расположенных в локальной сети университета (рис. 3), что позволит учесть все особенности проведения СТТ для обучающихся в вузе, включая виртуализацию и обособленный сегмент локальной сети.

В [10] представлено подробное описание сценариев 5 атак в соответствии с приведенным в работе [8] шаблоном, модифицированном с учетом особенностей,

перечисленных в табл. 1. В настоящей работе приведем краткое описание сценариев атак:

1. Сценарий атаки на электронную почту: с поддельных электронных адресов рассылаются фишинговые письма с уведомлениями о подозрении на компрометацию пароля и со ссылками на поддельные формы смены пароля; в случае перехода обучающегося по ссылке и заполнения им поддельной формы смены пароля осуществляется несанкционированный доступ (НСД) к конфиденциальным учетным данным обучающегося для входа в корпоративную электронную почту.

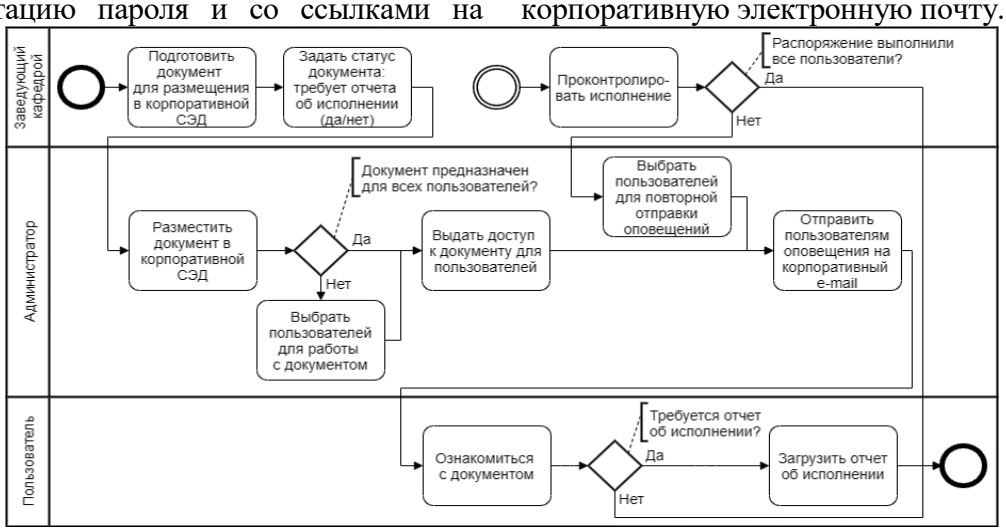

Рис. 2. Схема бизнес-процесса взаимодействия пользователей с сервисами для проведения СТТ

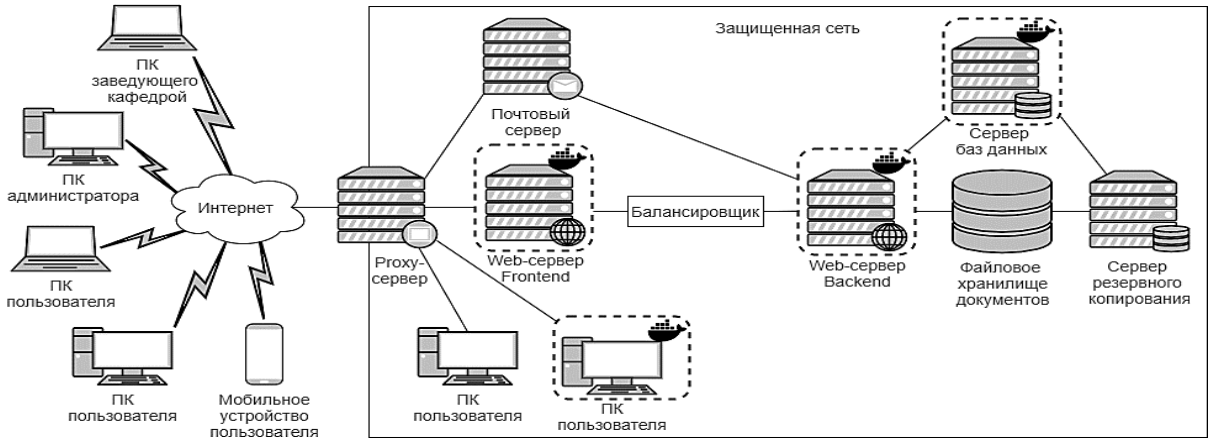

Рис. 3. Схема ИТ-инфраструктуры сервисов для проведения СТТ

2. Сценарий атаки на личный кабинет СЭД: с поддельных электронных адресов рассылаются фишинговые письма с уведомлениями о необходимости ознакомиться с распоряжением по кафедре и со ссылками на сайт-двойник СЭД; в случае перехода обучающегося по ссылке и ввода учетных данных на сайте-двойнике СЭД осуществляется НСД к конфиденциальным учетным данным обучающегося для входа в личный кабинет СЭД.

3. Сценарий атаки на персональные данные: с поддельных электронных адресов рассылаются фишинговые письма со ссылками на поддельные формы опросников для сбора персональных данных обучающихся; в случае перехода обучающегося по ссылке и заполнения формы опросника осуществляется НСД к персональным данным обучающегося.

4. Сценарий атаки на личные файлы: с поддельных электронных адресов рассылаются фишинговые письма с вложениями, содержащими код; в случае открытия вложения осуществляется несанкционированный доступ к личным файлам обучающегося.

5. Сценарий атаки на локальную вычислительную сеть: подбрасываются съемные носители с файлами, содержащими код; в случае открытия съёмного носителя осуществляется блокировка доступа к ресурсам корпоративной вычислительной сети.

Фишинговые письма, которые имеют вложения с документами или исполняемыми файлами, должны содержать код, приводящий к вредоносному воздействию исключительно на виртуальных компьютерах. Исполнение кода должно приводить к запуску заранее запланированного на виртуальной машине вредоносного воздействия (при открытии вложений на личных устройствах обучающихся или на компьютерах в локальной сети вуза вредоносное воздействие невозможно).

Заключение

Прошлый 2020 г. ознаменовался колоссальным ростом атак СИ на все без исключения сферы деятельности человека. Специалисты сферы ИБ и эксперты единодушны в том, что на фоне успехов в области программной и технической защиты информации от вторжений самым уязвимым звеном в защите является человек, чем и пользуются социальные инженеры.

Существуют различные способы подготовки сотрудников к противостоянию атак СИ. Основная масса средств и методов являются пассивными и не способны обеспечить требуемый уровень осведомленности в области защиты информации и, тем более, активного оперирования имеющимися сведениями.

Одной из самых проблемных сфер с точки зрения атак СИ является система высшего образования. В данной статье мы обосновываем необходимость готовить и проводить для 100% студентов 1 курса СТТ, которое является одним из наиболее эффективных активных методов формирования устойчивого иммунитета к атакам СИ. Представленный в статье анализ показал, что в теории и практике наработан существенный опыт проведения социотехнических учений для организаций различного уровня и сферы деятельности. Что же касается системы высшего образования, то здесь опыт не такой обширный и основное ограничение - это особенность образовательного процесса (по сравнению с рабочим процессом той или иной компании).

Мы выявили особенности образовательного процесса, которые влияют на подготовку и проведение СТТ студентов (сохранение целостности образовательного процесса, отсутствие у студента постоянного рабочего места, ограниченность по времени проведения СТТ, необходимость оперативного приведения к исходному состоянию всех рабочих мест, СТТ готовят и проводят сотрудники и старшекурсники, длительный и тщательный подготовительный период и др.). Выбор сценариев атак СИ также учитывают особенности образовательного процесса.

Основная цель дальнейших исследований - особенности организации и проведения учений на основе сверхактивных методов (100% студентов участвуют в подготовке и проведении СТТ).

Список литературы

1. Nguyen T, Bhatia S 2020 Higher Education Social Engineering Attack Scenario,Awareness & Training Model Journal of The Colloquium for Information Systems Security Education, V. 8, No. 1. // URL: https://cisse.info/journal/index.php/cisse/article/view/126/126 (дата обращения: 05.12.2021).

2. Лопатина К. Формирование и повышение культуры кибербезопасности. Опыт Сбербанка. URL: https://lib.itsec.ru/articles2/focus/formirovanie-i-povyshenie-kultury-kiberbezopasnosti-opyt-sberbanka (дата обращения: 05.12.2021).

3. Archibald J and Renaud K 2019 Refining the PoinTER “Human Firewall” pentesting framework. Information & Computer Security 27(2). DOI: 10.1108/ICS-01-2019-0019.

4. Davidoff Sh. 2009 How to prevent phishing attacks with social engineering tests // URL: https://searchsecurity.techtarget.com/tip/How-to-prevent-phishing-attacks-with-social-engineering-tests (дата обращения: 05.12.2021).

5. Albladi S and Weir G 2018 User characteristics that influence judgment of social engineering attacks in social networks. Human-centric Computing and Information Sciences, 8. DOI: 10.1186/s13673-018-0128-7.

6. Luse A and Burkman J 2020. Gophish: Implementing a Real-World Phishing Exercise to Teach Social Engineering, Journal of Cybersecurity Education, Research and Practice: Vol. 2020 : No. 2 , Article 5. Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2020/iss2/5 (дата обращения: 05.12.2021).

7. Этапы проведения социо-технического тестирования // URL:

https://saib.biz/sociotehnicheskoe-testirovanie-sotrudnikov/ (дата обращения: 05.12.2021).

8. Mouton F, Leenen L and Venter S 2016 Social engineering attack examples, templates and scenarios. Computers & Security. 59. pp. 186-209. DOI:10.1016/j.cose.2016.03.004

9. Пользователи хотят отказаться от паролей. URL: https://www.azone-it.ru/polzovateli-hotyat-otkazatsya-ot-paroley (дата обращения: 05.12.2021).

10. Гит с атаками. URL: https://gitlab.com/SibADI_InfoSec/Article_Socio-Technical_Testing/ (дата обращения: 05.12.2021).

11. Montañez R, Golob E and Xu S 2020 Human Cognition Through the Lens of Social Engineering Cyberattacks. Front. Psychol. 11:1755. DOI: 10.3389/fpsyg.2020.01755

12. Albladi S.M., Weir G.R.S. 2020 Predicting individuals' vulnerability to social engineering in social networks. Cybersecur 3, 7. DOI: 10.1186/s42400-020-00047-5

Сибирский государственный автомобильно-дорожный университет
The Siberian State Automobile and Highway University

Омский государственный технический университет
Omsk State Technical University

Поступила в редакцию 12.12.2021

Информация об авторах

Семенова Зинаида Васильевна – д-р пед. наук, профессор кафедры информационной безопасности, Сибирский государственный автомобильно-дорожный университет, e-mail: zvs111@gmail.com;

Моисеева Наталья Александровна – канд. пед. наук, доцент кафедры прикладной математики и фундаментальной информатики, Омский государственный технический университет, e-mail: nat_lion@mail.ru

Толкачева Елена Викторовна – канд. техн. наук, доцент кафедры информационной безопасности, Сибирский государственный автомобильно-дорожный университет, e-mail: tolkacheva_ev@mail.ru

Бибик Дмитрий Андреевич – технический директор, ООО «Спички», e-mail: bibik_dima@mail.ru

SOCIO-TECHNICAL TESTING UNDER FUTURE INFORMATION SECURITY SPECIALISTS' TRAINING: STAGES AND ATTACK SCENARIOS

Z.V. Semenova, N.A. Moiseeva, E.V. Tolkacheva, D.A. Bibik

The article presents the analysis of the current state of the problem of attacks based on social engineering. Methods and means of forming immunity to social engineering attacks in general and phishing attacks in particular are considered. The paper presents the analysis of modern approaches reflecting the main stages and scenarios of conducting socio-technical testing, as well as the analysis of terminology in this area. The necessity of Social Engineering Penetration Testing for 100% of higher educational institutions students is justified. The features of the educational process that significantly affect the preparation and conducting Social Engineering Penetration Testing are described. The technical and software infrastructure of socio-technical testing is proposed. Five scenarios that are suggested to be implemented within the framework of socio-technical testing are described in detail. In addition, a number of restrictions on the use of the described scenarios are presented. The description of the created services that ensure the implementation of the proposed scenarios of socio-technical testing and the conditions for conducting preparatory work is presented.

Keywords: Information Security, Cyberattack, Social Engineering Attack, Socio-technical Testing, Social Engineering Penetration Testing.

Submitted 12.12.2021

Information about the authors

Semenova Z. Vasilevna – Dr. of Pedagogy, Professor of Department of Information Security, The Siberian State Automobile and Highway University, e-mail: zvs111@gmail.com;

Moiseeva N. Alexandrovna – Cand. Sc (Pedagogical), Assistant Professor of Department of Applied Mathematics and Fundamental Infornmatics, Omsk State Technical University, e-mail: nat_lion@mail.ru

Tolkacheva E. Victorovna – Cand. Sc (Technical), Assistant Professor of Department of Information Security, The Siberian State Automobile and Highway University, e-mail: tolkacheva_ev@mail.ru

Bibik D. Andreevich – technical director, OOO "Spichki", e-mail: bibik_dima@mail.ru