ОРГАНИЗАЦИЯ ИНФОРМАЦИОННОЙ РАБОТЫ

УДК 004.056

Л.В. Астахова, И.А. Медведев

Информационное средство повышения устойчивости сотрудников организации к социоинженерным атакам*

Выявлен рост количества атак социальной инженерии на пользователей защищенных информационных систем организаций и снижение устойчивости пользователей к ним. Обоснована необходимость разработки инструментов для защиты организаций от социально-инженерных атак и рассмотрена возможность решения этой проблемы с использованием технологий машинного обучения. Описаны результаты разработки сканера устойчивости – программного приложения для тестирования сотрудников организации с целью повышения их устойчивости к атакам социальной инженерии. Показана его полифункциональность (обнаружение уязвимости пользователей, повышение их вовлеченности в процесс обнаружения атак социальной инженерии и в формирование культуры информационной безопасности организации) и перспективы дальнейшего развития.

Ключевые слова: *информационная безопасность, социальная инженерия, организация, сотрудник, уязвимости, сканирование, тестирование, устойчивость, программный продукт, культура информационной безопасности*

DOI: 10.36535/0548-0019-2021-01-2

ВВЕДЕНИЕ

Человек как источник инцидентов информационной безопасности изучается много лет, но остается критическим объектом теоретических и эмпирических исследований. Согласно аналитическим отчетам, уже четыре года подряд доля внутренних утечек информации от общего числа утечек остается в диапазоне 53-61%, т. е. все эти годы более половины утечек, зафиксированных в мире, происходит не по причине воздействия внешних хакеров, а из-за ошибок или умышленных действий сотрудников организаций [1]. Впервые с 2004 г. внутренние утечки информации показали более высокую «мощность», чем внешние – в среднем большее количество данных было скомпрометировано в результате одной внутренней утечки, чем в результате внешней. Согласно отчету PriceWaterhouseCoopers, внутренние утечки произошли по вине занятых (30%) и бывших (27%) сотрудников организаций [2].

При атаках на клиентов (юридических лиц) финансовых учреждений злоумышленники, как правило, не используют сложные технические средства, а больше внимания уделяют методам социальной инженерии. По данным Group-IB, в России более 80% краж средств у клиентов банков осуществляется этими методами. В течение 2018 г. банки ежемесячно сталкивались в среднем с тремя тысячами подобных атак. Таким образом было обнаружено более 1,9 млн уникальных фишинговых ссылок, что на 85% больше, чем в 2017 г. [3].

Повышенная опасность атак с использованием методов социальной инженерии требует от работодателей усилий по повышению устойчивости работников к такого рода атакам. Мир уже приобрел некоторый опыт в повышении осведомленности сотрудников банковской среды в области информационной безопасности, а за рубежом и в развитии культуры кибербезопасности, но число социоинженерных атак все еще растет. Это указывает на необходимость использования технических средств для мониторинга устойчивости персонала к этим атакам и определяет цель настоящей статьи – представить программный инструмент (сканер),

* Статья подготовлена при поддержке Правительства РФ (Постановление № 211 от 16.03.2013 г.), соглашение № 02. A03.21.0011.

разработанный на основе машинного обучения, для тестирования сотрудников организации, чтобы повышать их устойчивость к социоинженерным атакам различных типов и форм и развивать их культуру информационной безопасности.

УГРОЗЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ КАК ПРОБЛЕМА ТЕОРИИ И ПРАКТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Социальная инженерия стала серьезной угрозой в виртуальных сообществах и является эффективным инструментом для атаки на информационные системы, поэтому активно изучается в науке и практике. Эволюция концепции социальной инженерии в политике и кибербезопасности в 1990-х – 2017 гг. рассмотрена в [4]. Наиболее распространенным предметом исследования является классификация атак с помощью методов социальной инженерии в области информационной безопасности [5, 6]; многоаспектная классификация представлена в [7]. Такие атаки классифицируются по различным критериям в зависимости: от того, как они организованы (через человека или программное обеспечение); от того, как осуществляется атака (социальные, технические и физические атаки); от направления воздействия – прямое (через физический контакт или зрительный контакт или голос взаимодействия, присутствие злоумышленника в рабочей зоне жертвы для проведения атаки) и косвенное (может быть запущено удаленно с использованием вредоносного программного обеспечения, передается по электронной почте или через SMS). Прямые атаки – это физический доступ, серфинг на плечах, дайвинг, телефон и т. д., косвенные – фишинг, фальшивое программное обеспечение, всплывающие окна, вымогательство, рассылка SMS-сообщений, социальная инженерия онлайн и обратная социальная инженерия.

Сегодня встречается все больше громких случаев мошенничества с использованием разных видов атак с помощью методов социальной инженерии [8], поэтому большое внимание уделяется способам и средствам защиты от них. Прежде всего эти атаки рассматриваются в контексте проблемы снижения человеческих угроз информационной безопасности. В процессе ее решения принято понятие «повышение осведомленности в области информационной безопасности», которое включено в число требований международных и национальных стандартов [9, 10]. Однако во многих странах уже давно используется другое понятие – культура информационной безопасности (кибербезопасности, цифровой безопасности и т. д.), что стало ключевым объектом и науки, и практики. Появились обобщающие исследования этой проблемы в виде обзоров. Так, ученые провели изучение культуры информационной безопасности в периоды 2000 – 2013 гг. [11], 2003 – 2016 гг. [12], 2000 – 2017 гг. [13].

Столь большое внимание, уделяемое культуре информационной безопасности связано с тем, что меры по повышению осведомленности сотрудников организаций далеко не всегда эффективны. Например, в Нидерландах была экспериментально доказана неэффективность метода повышения осведомленности об опасностях социальных и кибератак [14]. Российские эксперты также все чаще приходят к выводу, что повышение осведомленности – это наиболее пассивное и зачастую бесполезное средство противодействия атакам социальной инженерии, так как большинство людей просто игнорирует предупреждения об угрозе независимо от формы их представления. Что касается культуры информационной безопасности, то в нормативных документах российских государственных регуляторов и в стандартах по информационной безопасности она не упоминается, а ее инициативное развитие требует гораздо большего времени и усилий, по сравнению с осведомленностью. Поэтому культура информационной безопасности организаций в России – это дело будущего, и, рассматривая антропогенную защиту от атак, сегодня имеют в виду недостаточную эффективность именно метода повышения осведомленности.

В связи с этим сфера защиты информации обращается к инструментальным средствам, к которым относятся сканеры уязвимостей (программные или аппаратные). Они используются для диагностики и мониторинга сетевых компьютеров, позволяют сканировать сети, компьютеры и приложения на предмет возможных проблем безопасности, оценивать и исправлять уязвимости. Тестирование на проникновение угроз является относительно зрелой отраслью. Его самая большая задача сегодня – использовать потенциал искусственного интеллекта для улучшения тестирования на проникновение и выявления уязвимостей системы [15].

Появился интерес и к инструментальным средствам защиты от социоинженерных атак. Так, зарубежные эксперты показали, что, используя только ту информацию, которая видна удаленному злоумышленнику, можно автоматически идентифицировать сотрудников организации. Исходя из этого, авторы [16] предложили применять автоматический сканер уязвимостей для проверки устойчивости организации к потенциальным атакам социальной инженерии, возникающим в результате использования открытых источников. Другие авторы [17] обращают внимание на возможность использования социальных сетей как часть теста на проникновение с помощью социальной инженерии.

Проблемы социоинженерных атак изучают и российские ученые [18]. Концепция программного пакета для автоматизированной системы анализа защиты пользователей компьютерных сетей от атак социальной инженерии представлена в [19]. Разработана формальная модель злоумышленника и модель его профиля компетенции, что позволяет оценивать безопасность информационной системы от социоинженерных атак, выявлять наиболее уязвимые звенья в системе и своевременно принимать необходимые меры для обеспечения защиты информации [20, 21].

По мере накопления опыта тестирования сотрудников организации на устойчивость к атакам социальной инженерии стали обсуждаться этические проблемы этого процесса [22]. Мы согласны с экспертами, утверждающими, что психологический стресс или вред работникам организации, вызванный этими атаками, должен быть ограничен. Обращает на себя внимание, что исследователи призывают ис-

пользовать потенциал человека как эффективного субъекта выявления атак социальной инженерии. Например, зарубежные эксперты разработали «human-as-a-security sensor platform» (платформу «человек как датчик безопасности») и внедрили ее в виде CogniSense – приложения-прототипа Microsoft Windows, предназначенного для активного обнаружения атак социальной инженерии и сообщении о них. Экспериментальная оценка пользователей, использующих CogniSense на своих персональных компьютерах в течение 45 дней, показала, что человек как датчик неизменно превосходит технические системы безопасности [23].

В настоящее время на российском рынке существуют продукты тестирования сотрудников организации на предмет выявления их восприимчивости к социальной инженерии (например, Phishman, Antiphishing, Kaspersky Awareness, Syssoft Security Awareness и т. д.). Аналогичные продукты предлагают поставщики услуг информационной безопасности Ростелеком-Солар и Сбербанк-Бизон. Многие организации создают свои собственные системы. Результаты выполненных проектов – положительные, например, проект по проверке состояния безопасности информационной системы ОАО «Уралкалий» с помощью дистанционного теста на проникновение с элементами социальной инженерии [24].

ПОЛИФУНКЦИОНАЛЬНОЕ СРЕДСТВО ПОВЫШЕНИЯ УСТОЙЧИВОСТИ ПОЛЬЗОВАТЕЛЕЙ К СОЦИОИНЖЕНЕРНЫМ АТАКАМ

Каждая организация сталкивается со специфическими проблемами от внешних информационных воздействий и защиты от них. По заявке малого предприятия с ограниченными ресурсами, предоставляющего ИТ-услуги, в связи с ростом фишинговых атак на его сотрудников, нами разработан сканер устойчивости – программное приложение для сотрудников организации с целью повышения их устойчивости к атакам социальной инженерии. Прототип приложения (сканера) имеет следующие функциональные возможности: оценка уровня уязвимости пользователя к социоинженерным атакам, обучение сотрудников противодействию атакам социальной инженерии, текущий контроль уровня осведомленности сотрудников в области информационной безопасности.

Сканер является веб-приложением для более удобного развертывания на любом АРМ или сервере. Основной язык программирования, используемый при написании приложения, – Python, также использовался JavaScript. В качестве фреймворка для веб-приложения был выбран Django, так как он обладает широким функционалом и легко изменяем. Поскольку Python – это кроссплатформенный язык программирования, он одинаково хорошо работает как на Windows, так и на Unix подобных системах. Оболочка в виде Docker контейнера позволяет без каких-либо проблем развертывать приложения на любой операционной системе. Сохранение данных реализовано на основе MariaDB – легковесной СУБД, что позволяет обеспечивать высокую скорость взаимодействия веб-приложения и базы данных. Для выявления психотипа человека используется коммерческий проект DataFuel, а для определения конечной оценки уровня уязвимости – логистическая регрессия.

Минимальные требования к оборудованию для установки приложения: процессор Intel с частотой 2ГГц или более; не менее 2 ГБ оперативной памяти; не менее 2 ГБ свободного места на жестком диске; клавиатура, мышь Microsoft Mouse или совместимое указывающее устройство; видеокарта и монитор, поддерживающие режим Super VGA с разрешением не менее чем 1024x768 точек.

Работа с программой выглядит следующим образом. При приеме нового сотрудника специалист по информационной безопасности на предприятии распознает его психотип, используя сканер приложения DataFuel [25]. Этот сканер, основанный на модели Больших Данных, анализирует страницу нового сотрудника в социальной сети и, в результате, отображает его психотип в соответствии с типологией Майерс-Бриггс (рис. 1), а также его возможные стимулы.

Такой метод оценки предназначен для исследования личности определенного человека. Типологический индикатор состоит из восьми букв: S, E, T, J, N, I, F, P, каждая соответствует особенностям и качествам характер и имеет своё значение. Например, буква E означает, что руководитель принадлежит к экстравертному типу (Extraverted), получает энергию от внешних источников. А буква F в комбинации психотипа свидетельствует о том, что перед нами человек «чувствующего» типа (Feeling). Он принимает решения на основании субъективной системы ценностей, а также личностных приоритетов.

Парные сочетания букв в разных комбинациях присущи определенному человеку.

Эта технология широко используется во всем мире и очень хорошо подходит для классификации сотрудников в бизнесе. В дальнейшем для повышения валидности оценок мы планируем использовать для этой цели методы дифференциальной психологии и психометрии. На выходе сканера специалист получает диаграмму с распределением вероятностей по возможным психотипам.

Эта информация сохраняется в приложении и впоследствии используется классификационной моделью для определения уязвимости сотрудника по отношению к социальной инженерии и другим типам угроз. В первые рабочие дни сотрудник обучается основам защиты информации на предприятии с помощью видеоуроков и в зависимости от специфики предприятия получает инструкции от специалиста по информационной безопасности. По завершении обучения сотрудник выполняет серию тестов, которые определяют уровень его знаний о том, как хранить личные данные, что такое атаки социальной инженерии и т. д.

Результаты теста заносятся в базу данных организации, а также используются классификационной моделью для определения уровня уязвимости сотрудников к угрозам. Статистическая модель, используемая для предсказания вероятности возникновения интересующего события с помощью логистической функции, представляет собой логистическую регрессию, её относят к моделям бинарного выбора. Регрессионная модель бинарного выбора – это модель, в которой

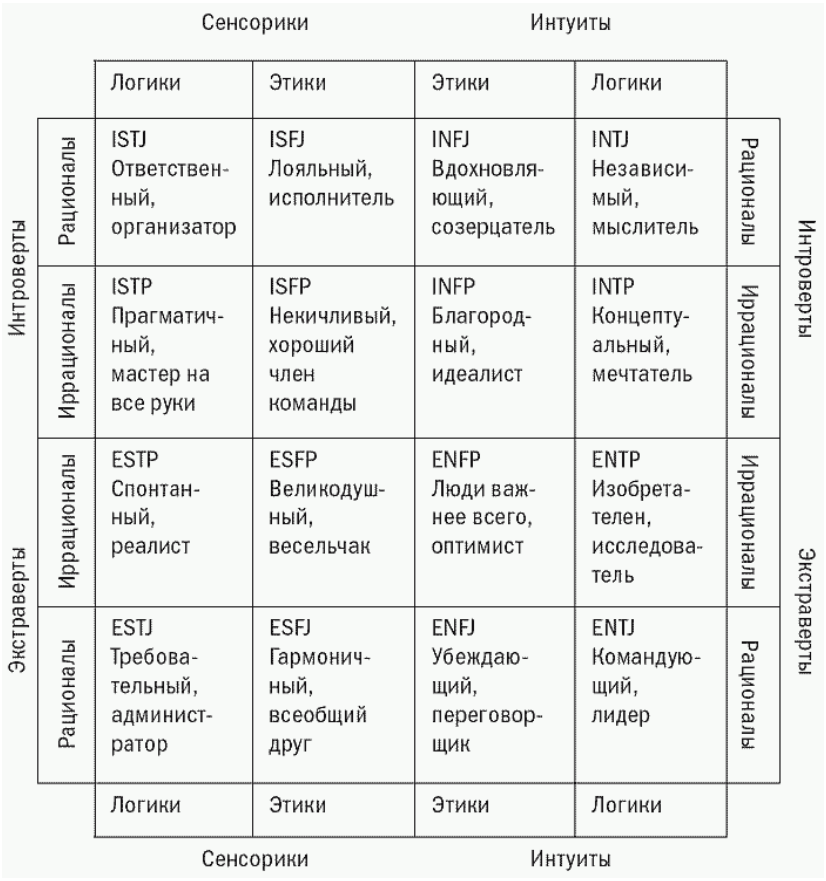

Рис. 1. Психотипы по Майерс-Бриггс [25]

зависимая переменная дихотомическая (бинарная), она может принимать лишь два значения: в нашем случае – уязвим сотрудник к информационным атакам или нет.

Для моделирования вероятности дихотомической зависимой переменной подбирают специальную монотонно возрастающую функцию, которая может принимать значения только от 0 до 1. Такая классификация, основанная на некоторых личных показателях (возраст, пол, психотип, а также результаты тестов и наблюдения инструктора), может довольно точно предсказывать вероятность уязвимости пользователя для информационных атак.

Администратор приложения может запланировать обучение персонала, выборочные тесты на основе своих предпочтений или рекомендаций «Программы повышения осведомленности о безопасности», в которой он должен указать количество сотрудников на предприятии, специфику предприятия, приблизительный уровень осведомленности сотрудников об информационных угрозах, желаемую конечную степень осведомленности, а также адреса электронной почты сотрудников для различных проверок. Пример теста в приложении Phishing – один из самых популярных методов атаки, направленных на получение информации по фишинговым ссылкам, которые отправляются сотрудникам по электронной почте. Цель этого теста – не дать сотрудникам переходить по подозрительным ссылкам и передавать любую информацию. Это может быть выполнено как стандартными методами (например, поддельной ссылкой, ведущей в социальную сеть с поддельной формой авторизации), так и с использованием социальной инженерии.

Каждый сотрудник организации предлагает администратору приложения «облако тегов», представляющее собой список слов, которые чаще всего встречаются на странице сотрудника в социальной сети. Наиболее популярными в этом «облаке» являются слова, отражающие личные интересы сотрудника. Используя эту информацию, администратор может составить фишинговое письмо для каждого сотрудника индивидуально, чтобы повысить эффективность сканирования и добиться более надежных результатов. В результате тестовой проверки программа отображает такие параметры, как «доля ответов» (количество сотрудников, которые кликнули по ссылке на фишинговый сайт от общего числа сотрудников) и «доля ввода» (количество сотрудников, которые ввели свои личные данные в фишинговый веб-сайт). Эти параметры также вводятся в базу данных организации и используются моделью машинного обучения для лучшей оценки её сотрудников.

Функциональность разработанного прототипа не конечна. В стадии разработки авторами настоящей статьи находятся:

- «USB Security test». Специалист по защите информации оставляет в людном месте предприятия флешку, на которой записан специальный файл. Если

какой-либо сотрудник вставит эту флешку в свою рабочую станцию, то файл сообщит об этом на сервер, а результат теста будет признан отрицательным.

- «Тревожная кнопка». У каждого сотрудника в интерфейсе почтового клиента должен быть доступ к этой кнопке. Если сотрудник сомневается в источнике электронного письма, то при нажатии на кнопку это письмо будет перенаправлено в специальный алгоритм, оценивающий вероятность фишинга по ключевым точкам в письме. В результате сотрудник узнает о вероятности того, что данное письмо является информационной атакой.
- «Второй шанс». Этот модуль позволяет пользователю дать второй шанс после клика на подозрительную ссылку или ввода данных в форму. Для этого выводится диалоговое окно, оповещающее пользователя о небезопасности данного действия и о запросе на продолжение операции. Администратор может сам устанавливать фильтры на ссылки, домены и другие опции.

ЗАКЛЮЧЕНИЕ

Проблема социоинженерных атак на пользователей информационных систем организаций становится все более острой и изучается в контексте классификации атак, их принципов, этики и т.д. Антропогенные методы защиты от социоинженерных атак исследуются в рамках осведомленности в области информационной безопасности и культуры кибербезопасности, но их эффективность пока недостаточно высока. Рынок сканеров уязвимостей начинает развиваться, появляются примеры разработки инструментов для сканирования уязвимостей пользователей. Новизна разработанного нами и представленного в настоящей статье программного обеспечения заключается в том, что оно позволяет не только сканировать устойчивость сотрудников организации к атакам социальной инженерии, но и получать от них информацию об обнаруженных атаках, а также быть обучающей системой со сложной обратной связью. Полифункциональные возможности сканера позволили обеспечить технологии машинного обучения, использованные в процессе его разработки. Внедрение этого сканера на предприятиях будет способствовать снижению количества утечек информации, а также повышению осведомленности персонала в области кибербезопасности. Элементы вовлечения сотрудников в обнаружение атак социальной инженерии способны повысить взаимное доверие работодателя и работника, укрепив «человеческий периметр» защиты корпоративной информации.

СПИСОК ЛИТЕРАТУРЫ

1. InfoWatch. Утечки данных организаций по вине или неосторожности внутреннего нарушителя. Сравнительное исследование. 2013–2019 гг. – URL: https://www.infowatch.ru/ sites/default/files/ analytics/files/InfoWatch_Analytical_Report.pdf (дата обращения: 26.05.2020 г.).
2. PriceWaterhouseCoopers. Обследование глобального состояния информационной безопасности® 2018. – URL: https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html (дата обращения: 26.05.2020 г.).
3. Банк России. FINCERT. Обзор основных типов компьютерных атак в кредитно-финансовой сфере в 2018 году. – URL: https://cbr.ru/Content/ Document/File/72724/ DIB_2018_20190704.pdf (дата обращения: 26.05.2020 г.).
4. Hatfield J.M. Social engineering in cybersecurity: The evolution of a concept // Computers & Security. – 2018. – Vol.73. – P. 102-113.
5. Krombholz K., Hobel H., Huber M., Weippl E. Advanced social engineering attacks // Journal of Information Security and Applications. – 2015. – Vol. 22. – P. 113-122.
6. Abass I.A.M. Social Engineering Threat and Defense: A Literature Survey // Journal of Information Security. – 2018. – № 9. – P. 257-264.
7. Salahdine F., Kaabouch N. Social Engineering Attacks: A Survey // April 2019 Future Internet 11(89). – URL: https://www.researchgate.net/publication/ 332151597_Social_Engineering_Attacks_A_Survey (дата обращения: 26.05.2020 г.)
8. Social engineering scams ensnare Google, Facebook and their users // Network Security. – 2017. – Vol. 2017, Issue 5, May 2017. – P. 1-2. doi.org/10.1016/ S1353-4858(17)30043-0
9. ГОСТ Р ИСО / МЭК 27000–2012. Информационные технологии. Методы защиты. Системы управления информационной безопасностью. Общий обзор и терминология. – URL: http://docs.cntd.ru/ document/1200102762 (дата обращения: 26.05.2020 г.).
10. ISO / IEC 27001: 2013 Информационные технологии. Методы защиты. Системы управления информационной безопасностью. Требования. – URL: https://www.iso.org/ standard/54534.html (дата обращения: 26.05.2020 г.).
11. Karlsson F., Åström J., Karlsson M. Information security culture–state-of-the-art review between 2000 and 2013 // Information & Computer Security. – 2015. – Vol. 23, № 3. – P. 246-285. doi.org/10.1108/ICS-05-2014-0033
12. Mahfuth A., Yussof S., Baker A.A., Ali N. A systematic literature review: Information security culture // 2017 International Conference on Research and Innovation in Information Systems (ICRIIS). – Langkawi, 2017. – P. 1-6. DOI: 10.1109/ ICRIIS.2017.8002442.
13. Nasir A., Arshah R.A., Ab Hamid M.R., Fahmy S. An analysis on the dimensions of information security culture concept: A review // Journal of Information Security and Applications. – 2019. – № 44. – P. 12-22.
14. Junger M., Montoya L., Overink F.-J. Priming and warnings are not effective to prevent social engineering attacks // Computers in Human Behavior. – 2017. – Vol. 66. – P. 75-87.
15. McKinnel D.R., Dargahi T., Dehghantanha A., Choo K.-K.R. A systematic literature review and meta-analysis on artificial intelligence in penetration testing and vulnerability assessment // Computers & Electrical Engineering. – 2019. – Vol.75. – P. 175-188.

16. Edwards M., Larson R., Green B., Rashid A., Baron A. Panning for gold: Automatically analysing online social engineering attack surfaces // Computers & Security. – 2017. – Vol. 69. – P. 18-34.
17. Faircloth J. Chapter 8: Client-side attacks and social engineering // Penetration Tester's Open Source Toolkit (Fourth Edition). – 2017. – P. 273-318.
18. Азаров А.А., Тулупьева Т.В., Суворова А.В., Тулупьев А.Л., Абрамов М.В., Юсупов Р.М. Социально-инженерные атаки: проблемы анализа. – СПб: Санкт-Петербургская издательско-книготорговая компания Наука, 2016. – 349 с.
19. Абрамов М.В. Автоматизация анализа социальных сетей для оценки защищенности от атак социальной инженерии // Автоматизация процессов управления. – 2018. –Вып.1 (51). – С. 34-40.
20. Абрамов М.В., Азаров А.А., Тулупьев Т.В., Тулупьев А.Л. Модель профиля компетентности конкурента в задаче анализа защищенности персонала информационных систем от атак социальной инженерии // Информационно-управляющие системы. – 2016. – Вып. 4(83). – С. 77-84.
21. Абрамов М.В., Тулупьев А.Л., Сулейманов А.А. Задачи для анализа защиты пользователей от атак социальной инженерии: построение социального графа на основе информации из социальных сетей // Научно-технический журнал «Информационные технологии, механика и оптика». – 2018. – Т. 18, № 2. – С. 313-321.
22. Hatfield J.M. Virtuous human hacking: The ethics of social engineering in penetration-testing // Computers & Security. – 2019. – Vol.83. – P. 354-366.
23. Heartfield R., Loukas. G. Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework // Computers & Security. – 2018. – Vol. 76. – P. 101-127.
24. Pentest with elements of social engineering. – URL: https://amonitoring.ru/about/success/prime_group (дата обращения: 26.05.2020 г.).
25. DataFuel. – URL: https://datafuel.me/ (дата обращения: 27.05.2020 г.).

Материал поступил в редакцию 27.05.20.

Сведения об авторах

АСТАХОВА Людмила Викторовна – доктор педагогических наук, профессор, профессор кафедры защиты информации Южно-Уральского государственного университета, Челябинск
e-mail: astakhovalv@susu.ru

МЕДВЕДЕВ Иван Алексеевич – студент кафедры защиты информации Южно-Уральского государственного университета (национального исследовательского университета), г. Челябинск
e-mail: ivanelgran@mail.ru