6. Yantser L. V., Yantser K. E. Questions of teaching mathematical analysis in medical universities. *Kant*, 2021, no. 1, pp. 353—356. (In Russ.)

7. Komarova E. P., Alekseeva G. A. Forming integrated competence of medical students in the smart technologies context. *International Journal of Humanities and Natural Sciences*, 2020, no. 7-3, pp. 106—109. (In Russ.)

8. Shmonova M. A. Forming professional competence of students at medical universities while teaching mathematics. *Yaroslavl pedagogical bulletin*, 2016, no. 2, pp. 54—59. (In Russ.)

9. Shmonova M. A. Formation of professional competence of students of medical universities in the process of teaching mathematics. *Yaroslavl pedagogical bulletin*, 2018, no. 2, pp. 88—94. (In Russ.)

10. Drobot M. V. Business competence as an economic category. *Society: politics, economy, law*, 2013, no. 1, pp. 111—115. (In Russ.)

11. Gerasimenko O. A., Avilova J. N. Key business competences as an economic category. *Vestnik BGTU im. V. G. Shuhova*, 2016, no. 6, pp. 273—277. (In Russ.)

12. Maksimova G. P. Business competences in the teaching process of Russian higher school. In: *Higher school: experience, problems, prospects. Materials of the IX international sci. and pract. conf.* In 2 parts. Moscow, RUDN publ., 2016. Pp. 470—472. (In Russ.)

13. Grozova O. S., Tsvetkova G. S. Business competence as a factor of innovational development of the provincial region. *Trudy Povolzhskogo gosudarstvennogo tehnologicheskogo universiteta. Seriya Social'no-ekonomicheskaya*, 2019, no. 7. pp. 16—23. (In Russ.)

14. Barannikov K. A. *Formation of economic and business competences of students of secondary vocational education and their impact on the economic security of the person. Abstract of diss. of the Cand. of Pedagogy.* Moscow, 2009. P. 23. (In Russ.)

15. Lanina L. V. Orientation of first-year medical students to the study of mathematics in the initial period of study. *Cherepovets State University Bulletin*, 2012, no. 3, vol. 2, pp. 159—162. (In Russ.)

Статья поступила в редакцию 10.04.2022; одобрена после рецензирования 22.04.2022; принята к публикации 29.04.2022.
The article was submitted 10.04.2022; approved after reviewing 22.04.2022; accepted for publication 29.04.2022.

Научная статья
УДК 37.013
DOI: 10.25683/VOLBI.2022.59.258

Oleg Vladimirovich Ostanin
Candidate of Military Sciences,
Associate Professor of the Department of Radio Systems
and Control Systems,
Information Transmission and Information Security,
Moscow Aviation Institute
(National Research University)
Moscow, Russian Federation
kn0377@mail.ru

Олег Владимирович Останин
канд. воен. наук,
доцент кафедры радиосистем
и комплексов управления,
передачи информации и информационной безопасности,
Московский авиационный институт
(национальный исследовательский университет)
Москва, Российская Федерация
kn0377@mail.ru

Elena Anatolyevna Ostanina
Candidate of Pedagogy, Associate Professor,
Associate Professor of the Department of Radio Systems
and Control Systems,
Information Transmission and Information Security,
Moscow Aviation Institute
(National Research University)
Moscow, Russian Federation
neka1818@mail.ru

Елена Анатольевна Останина
канд. пед. наук, доцент,
доцент кафедры радиосистем
и комплексов управления,
передачи информации и информационной безопасности,
Московский авиационный институт
(национальный исследовательский университет)
Москва, Российская Федерация
neka1818@mail.ru

ПОДГОТОВКА ПЕРСОНАЛА ОРГАНИЗАЦИИ ПО ВОПРОСАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

13.00.02 — Теория и методика обучения и воспитания (по областям и уровням образования)

Аннотация. *В статье рассматриваются вопросы подготовки персонала организации к противодействию возникающим информационным угрозам, потребность в которой в настоящее время только возрастает. Повышение уровня защищенности информации в информационных системах организаций, включая телекоммуникационные сети, может быть обеспечено только комплексным применением методов и средств защиты. Наиболее уязвимым звеном в этом случае, по мнению специалистов, является человек.*

В работе приведены и проанализированы данные, характеризующие долю воздействия методами социальной

инженерии на физических и юридических лиц. В России методы социальной инженерии получили достаточно широкое распространение, и их доля в период пандемии показывает устойчивый рост.

Информация в наше время оказывается ключевым ресурсом практически любой организации или сообщества, компании и даже государства в целом. Вследствие этого вопросы защиты информационного ресурса во всем мире выходят на ключевые позиции и требуют тщательного анализа, оценки и оперативного реагирования на современные вызовы.

В рамках данного исследования проведены анализ и оценка значимости человеческого фактора в обеспечении информационной безопасности организации.

Проведенное исследование подтвердило, что наиболее действенным способом защиты от социальной инженерии является обучение работников. Процесс целесообразно организовывать периодически, он может проводиться как в очном, так и в дистанционном формате, адаптируя программу к занимаемой сотрудником должности. Обучение, помимо теоретических занятий по изучению методов и способов защиты, должно содержать активные методы, дискуссии по разбору актуальных инцидентов информационной безопасности и решение кейсовых заданий.

Ключевые слова: *дистанционное обучение, обучение персонала, информационная безопасность, методы противодействия, социальная инженерия, угроза безопасности, информация, подготовка персонала, мошенничество, атака*

Для цитирования: Останин О. В., Останина Е. А. Подготовка персонала организации по вопросам информационной безопасности // Бизнес. Образование. Право. 2022. № 2 (59). С. 340—344. DOI: 10.25683/VOLBI.2022.59.258.

Original article

TRAINING OF THE ORGANIZATION'S PERSONNEL ON INFORMATION SECURITY ISSUES

13.00.02 — Theory and methodology of education and upbringing (by areas and levels of education)

Abstract. *The article discusses the issues of training the organization's personnel to counter emerging information threats, the need for which is currently only increasing. Increasing the level of information security in the information systems of organizations, including telecommunications networks, can only be ensured by the complex application of methods and means of protection. The most vulnerable link in this case, according to experts, is the man.*

The paper presents and analyzes data characterizing the share of the impact of social engineering methods on individuals and legal entities. In Russia, social engineering methods have become quite widespread, and their share during the pandemic shows steady growth.

Information nowadays turns out to be a key resource of almost any organization or community, company and even the state as a whole. As a result, the issues of protecting an information resource around the world come to key positions and require careful analysis, assessment and prompt response to modern challenges.

Within the framework of this study, the analysis and evaluation of the importance of the human factor in ensuring the information security of the organization are carried out.

The conducted research has confirmed that the most effective way to counteract social engineering is to train employees. It is advisable to organize the process periodically, which can be carried out both in person and remotely, adapting the program to the position held by the employee. The training, in addition to theoretical classes on the study of methods and methods of protection, should contain active methods, discussions on the analysis of current information security incidents and the solution of case tasks.

Keywords: *distance learning, personnel training, information security, counteraction methods, social engineering, security threat, information, personnel training, fraud, attack*

For citation: Ostanin O. V., Ostanina E. A. Training of the organization's personnel on information security issues. *Business. Education. Law*, 2022, no. 2, pp. 340—344. DOI: 10.25683/VOLBI.2022.59.258.

Введение

Актуальность темы исследования обусловлена необходимостью защиты информации в условиях постоянного совершенствования технических средств передачи и обработки информации и постоянного роста ценности информации, сопровождающегося появлением новых способов неправомерного доступа.

Изучению проблемы противодействия информационным угрозам, а также обучению персонала по информационной безопасности посвящено множество научных трудов. Так, информационные угрозы подробно описаны в работах Ю. Родичева, А. Бабаша, Е. Баранова, вопросы противодействия этим угрозам — в работах С. Нестерова, В. Гафнера, Ю. Громова, а необходимости обучения по обеспечению информационной безопасности уделено внимание в трудах С. Петрова, Т. Партыка. Вместе с тем ряд проблем, имеющих принципиальное значение для предотвращения потенциальных возможностей утечки информации, порой упускается из вида и не получает достаточного внимания со стороны научного сообщества. Представляется целесообразным на основании существующих исследований продолжить разработку указанной темы.

Научная новизна заключается в том, что впервые предлагается использовать комплексный анализ влияния социальной инженерии в совокупности с техническими средствами на состояние информационной безопасности организации.

Целью данного исследования является обоснование необходимости противодействия информационным атакам. Для достижения указанной цели решается ряд задач, к которым отнесены анализ способов воздействия на персонал, обоснование способа противодействия атакам, направленным на получение неправомерного доступа к информации организаций.

Теоретическая значимость работы обусловлена актуализацией проблемы влияния использования методов социальной инженерии на состояние информационной

безопасности организации и сокращение инцидентов с помощью обучения персонала.

Практическая значимость работы заключается в том, что впервые на основе проведенных исследований для защиты информации (при наличии защищаемой информации) предлагается систематическое обучение всего персонала с дальнейшей оценкой уровня его подготовки.

Основная часть

Социальная инженерия — метод получения доступа к информации, основанный на особенностях психологии человека. Основной целью социальной инженерии является получение доступа к конфиденциальной информации, другим защищенным системам.

К методам и средствам защиты информации в первую очередь относят программно-технические, законодательные и организационно-административные методы [1].

Непредвиденное или нежелательное событие, которое может нарушить деятельность организации в части информационного внутриорганизационного или внешнего взаимодействия или ее информационную безопасность в целом, принято называть инцидентом информационной безопасности [2].

При атаке используемые злоумышленником методы направлены на формирование такой поведенческой модели работника, которая ему выгодна и носит ложное представление о добровольности и самостоятельности ее принятия объектом воздействия [3].

Как правило, все техники социальной инженерии основаны на личностных особенностях человека и их учете при принятии решений человеком. Важно отметить, что такие методы достаточно эффективны, просты и дешевы в реализации, а также имеют невысокую степень риска [4].

Мошенники, взламывая психологию объектов атаки, полагаются на общедоступные данные для создания профилей жертв.

Эксперты Fortinet выделяют следующие варианты атак с использованием социальной инженерии [5].

Spearphishing — атаки на базе электронной почты, направленные на конкретного человека или всю организацию в целом. Цель — побуждение к переходу по вредоносным ссылкам или сбор учетных данных. Отмечается, что локальный фишинг нацелен на конкретного человека через социальные сети и мессенджеры [6].

Обман в социальных сетях через создание поддельных профилей. Цель — завоевание доверия жертвы, ее обман.

Атака «Просьбы под предлогом» предполагает подготовку киберпреступником хорошего предлога или правдоподобной истории для убеждения жертвы в необходимости предоставления определенной информации.

WaterHolding предполагает сбор информации о посещениях веб-сайтов среди целевой группы злоумышленником.

Smashing — атака с использованием текстовых телефонных сообщений, якобы от надежного отправителя. Цель — загрузка вируса или другой вредоносной программы в устройство жертвы.

Spoofing — атака, которая заключается в подделке идентификатора вызывающего абонента.

Отдельно стоит выделить такое явление, как обратная социальная инженерия, которая предполагает самостоятельное обращение человека за «помощью» к злоумышленнику [7—9]. Это достигается проведением рекламных или диверсионных операций, например созданием обратимой неполадки на компьютере жертвы с последующей рекомендацией обратиться при таких проблемах к злоумышленнику по указанным координатам [10].

Это неполный перечень возможных жизненных ситуаций, и он предполагает постоянный мониторинг подобных инцидентов и включение разбора их в процесс обучения по вопросам информационной безопасности.

Отмечается, что 95 % всех нарушений безопасности в настоящее время обусловливаются человеческим фактором. Вот почему необходимо обучать сотрудников и постоянно углублять их знания в области кибербезопасности.

В ходе проведения эмпирического исследования проведена оценка процентного соотношения респондентов, в отношении которых были успешно применены методы социальной инженерии.

В России методы социальной инженерии получили достаточно широкое распространение в период пандемии и перехода сотрудников к удаленному формату работы. По сравнению с другими странами эта проблема «нарастает со взрывной скоростью» [1]. В докладах Центрального банка и в комментариях компаний в сфере информационной безопасности обозначаются при этом две причины такого роста: низкая киберграмотность граждан и практически регулярные утечки баз данных из госструктур и коммерческих организаций.

Приоритетной целью большинства кибератак является кража информации. При атаках на юридических и физических лиц ее доля составляет 58 % и 55 % соответственно. В результате этого часто реализуется угроза распространения компрометирующей информации о человеке с целью вымогательства [11].

Рассматривая социальные сети и многочисленные форумы как источник информации, установлено, что пользователи не всегда заботятся о безопасности аккаунтов, используя простые и идентичные пароли, не проверив надежность ресурса. Этим исследователи объясняют высокую долю украденных учетных данных (44 %) в атаках на частных лиц [11].

Приведем типизацию украденных данных при атаках на частные и юридические лица. Так, при атаке на юридическое лицо (компанию) учетные записи составляют 27 %, персональные данные — 29 %, данные платежных карт — 13 %, информация, относящаяся к категории коммерческой тайны, — 12 %, медицинская информация — 7 %, базы данных клиентов — 6 %, личная переписка — 2 %, другая информация — 4 %. В то же время при атаке на физическое лицо складывается следующая картина: 44 % составляют учетные данные, 7 % — персональные данные, данные платежных карт — 34 %, 9 % — личная переписка и 6 % — другая информация [11].

Отметим, что доля целенаправленных атак постоянно растет, причем наиболее активно реализуются атаки на государственные организации (порядка 20 %), промышленные компании (10 %), медицинские и банковские организации.

Доля операций, проведенных без согласия пользователей с использованием социальной инженерии, за 2019 и 2020 гг. [12] составляет для системы дистанционного банковского обслуживания юридических лиц в первом квартале 2019 г. 5 %, во втором квартале — 8 %; в 2020 г. первый квартал уже характеризуется долей операций с применением социальной инженерии 44 %, второй квартал — 29 %. По ряду позиций доля атак с использованием социальной инженерии достигает значений в 80…90 %.

По данным информационного портала по безопасности SecurityLab.ru, количество подобных атак в 2020 г. выросло на 147 % [13].

Третий квартал 2020 г., по данным специалистов Центрального банка РФ, также показал рост по всем видам атак, за исключением атак с использованием уязвимостей в программном обеспечении.

В 2020 г. появилось множество новых схем мошенничества [5]. К ним можно отнести схемы мошенничества в Telegram, через заражение посредством «презентаций» продукта, предполагаемого к демонстрации в оплачиваемой рекламе, и активное паразитирование на повышенной тревожности и неуверенности людей в период пандемии.

Как правило, компании тратят огромные финансовые средства на обеспечение информационной безопасности техническими методами, в то время как эти технические средства могут быть бесполезны, если сотрудники не будут знать меры по противодействию социальной инженерии либо просто пренебрегут ими [14]. Основным способом защиты от социальной инженерии, по многочисленным утверждениям ученых и работодателей, является обучение. В этой связи предлагается вариативная программа обучения, учитывающая должностной статус сотрудника.

В процессе обучения следует обратить внимание на обязательность исполнения инструкций компаний. В них, как правило, прописываются вопросы, затрагивающие информационную безопасность компании, как идентифицировать человека и определить его принадлежность к сотрудникам компании, как сопровождать клиентов [15].

Отметим, что программа должна быть адаптирована для конкретной организации или группы компаний с учетом специфики их деятельности и опыта работы по предотвращению инцидентов.

Заключение

Результаты данной работы позволяют актуализировать процесс обучения с учетом сложившейся обстановки и переходом сотрудников к удаленному формату.

Таким образом, все возрастающая ценность информации, переход к повсеместному активному использованию при работе информационных технологий и сетевых ресурсов, а также совершенствование способов неправомерного получения информации потребуют периодического дополнительного обучения сотрудников в каждой организации. Организация такого обучения с использованием дистанционных технологий способна привнести дополнительный эффект за счет приближения условий обучения к реальной деятельности сотрудников в новых условиях.

СПИСОК ИСТОЧНИКОВ

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. М. : Стандартинформ, 2008.
2. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. М. : Стандартинформ, 2009.
3. Карпенко Л. А. Петровский А. В., Ярошевский М. Г. Краткий психологический словарь. Ростов н/Д. : Феникс, 1998.
4. Гридин А. Краткое введение в социальную инженерию. URL: https://habr.com/ru/post/83415.
5. Социальная инженерия. Обзор TAdviser. URL: https://www.tadviser.ru/a/521580.
6. Информационная безопасность в 2021 году. Угрозы, отраслевые тренды. ITGLOBAL.COM. URL: https://habr.com/ru/company/itglobalcom/blog/540748.
7. Mitnick K. D., Simon W. L. The Art of Deception: Managing the Human element of Security. URL: https://www.rulit.me/author/mitnik-kevin/the-art-of-deception-controlling-the-human-element-of-security-download-489913.html.
8. Ализар А. Социальная инженерия в России эффективнее, чем в других странах. URL: https://habr.com/ru/news/t/459278.
9. Хэднеги К. Искусство обмана: социальная инженерия в мошеннических схемах / Пер. с англ. М. : Альпина Паблишер, 2020.
10. Кузнецов М. В., Симдянов И. В. Социальная инженерия и социальные хакеры. СПб. : БХВ-Петербург, 2007.
11. Исследование Positive Technologies. Актуальные киберугрозы. II квартал 2019 года. URL: https://ptsecurity.com.
12. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств. I и II кварталы 2019—2020 годов. Банк России. URL: https://cbr.ru/analytics/ib/review_1q_2q_2020.
13. Количество атак с использованием социальной инженерии выросло на 147 % в 2020 году. URL: https://www.securitylab.ru/news/515178.php.
14. Останина Е. А. Информационная безопасность при реализации концепции BYOD // Человеческий капитал. 2019. № 12(132). С. 131—141.
15. Следите за своими SMS-сообщениями: смягчение социальной инженерии при аутентификации второго фактора / Х. Сиадати, Т. Нгуен, П. Гупта, М. Якобссон, Н. Мемо // Компьютеры и безопасность. 2017. № 65. С. 14—28.

REFERENSES

1. *GOST R 50922-2006. Information protection. Basic terms and definitions*. Moscow, Standartinform, 2008. (In Russ.)
2. *GOST R 53114-2008. Information security. Ensuring information security in the organization. Basic terms and definitions*. Moscow, Standartinform, 2009. (In Russ.)
3. Karpenko L. A., Petrovskii A. V., Yaroshevskii M. G. *A brief psychological dictionary*. Rostov-on-Don, Feniks, 1998. (In Russ.)
4. Gridin A. *Brief introduction to social engineering*. (In Russ.) URL: https://habr.com/ru/post/83415.
5. *Social engineering. Overview of TAdviser*. (In Russ.) URL: https://www.tadviser.ru/a/521580.
6. *Information security in 2021. Threats, industry trends*. ITGLOBAL.COM. (In Russ.) URL: https://habr.com/ru/company/itglobalcom/blog/540748.
7. Mitnick K. D., Simon W. L. *The Art of Deception: Managing the Human element of Security*. URL: https://www.rulit.me/author/mitnik-kevin/the-art-of-deception-controlling-the-human-element-of-security-download-489913.html.
8. Alizar A. *Social engineering in Russia is more effective than in other countries*. (In Russ.) URL: https://habr.com/ru/news/t/459278.

9. Hadnegi K. *The Art of Deception: Social Engineering in fraudulent schemes*. Transl. from English. Moscow, Al'pina Pablisher, 2020. (In Russ.)

10. Kuznetsov M. V., Simdyanov I. V. *Social engineering and social hackers*. Saint Petersburg, BKhV-Peterburg, 2007. (In Russ.)

11. *Positive Technologies research. Current cyber threats. Q2 of 2019*. (In Russ.) URL: https://ptsecurity.com.

12. *Review of reporting on information security incidents during the transfer of funds. Q1 and Q2 of 2019—2020. The Bank of Russia*. (In Russ.) URL: https://cbr.ru/analytics/ib/review_1q_2q_2020.

13. *The number of attacks using social engineering increased by 147 % in 2020*. (In Russ.) URL: https://www.securitylab.ru/news/515178.php.

14. Ostanina E. A. Information security in the implementation of the BYOD concept. *Human capital*, 2019, no. 12, pp. 131—141. (In Russ.)

15 Siadati H., Nguyen T., Gupta P., Jacobsson M., Memon N. Mind your SMSes: Mitigating social engineering in second factor authentication. *Computers and security*, 2017, no. 65, pp. 14—28. (In Russ.)

Статья поступила в редакцию 10.04.2022; одобрена после рецензирования 22.04.2022; принята к публикации 29.04.2022.
The article was submitted 10.04.2022; approved after reviewing 22.04.2022; accepted for publication 29.04.2022.

Обзорная статья
УДК 378.146
DOI: 10.25683/VOLBI.2022.59.259

Sharbanu Omirgaliyevna Uisenbayeva
Postgraduate of the Department of General and Social Pedagogy,
Altai State Pedagogical University
Barnaul, Russian Federation
sharbanu_usenbaeva-esilbaeva@mail.ru

Шарбану Омиргалиевна Уйсенбаева
аспирант кафедры общей и социальной педагогики,
Алтайский государственный педагогический университет
Барнаул, Российская Федерация
sharbanu_usenbaeva-esilbaeva@mail.ru

ОБЗОР ИНСТРУМЕНТОВ ОЦЕНКИ МЕЖКУЛЬТУРНОЙ КОМПЕТЕНЦИИ МЕДИЦИНСКИХ СПЕЦИАЛИСТОВ

13.00.08 — Теория и методика профессионального образования

Аннотация. *Этническое разнообразие, процессы миграции населения, усиливающиеся темпы глобализации и интернационализации делают вопросы межкультурной коммуникации особенно актуальными. В настоящее время существует множество инструментов оценки межкультурной (культурной) компетентности медицинских работников. Целью исследования был обзор научно обоснованных анкет самооценки межкультурной компетентности для медицинских работников, преподавателей и студентов. Для обзора было отобрано 15 научных публикаций. Критериями включения были период публикации (2000—2022) и наличие ключевых слов: культурная компетентность, показатели оценки межкультурной компетенции, культурная компетентность, межкультурная коммуникация медицинских специалистов (cultural competence, indicators of assessment of intercultural competence, cultural competence, intercultural communication, medical professionals). Анализ литературных источников позволил выделить 48 научно обоснованных методик оценки межкультурной компетентности, из которых в настоящей статье описаны шесть: CSES, CAS, IAPCC-R, IAPCC-SV, TSET, SAICS. Все перечисленные инструменты оценки были апробированы в научных исследованиях и имеют высокий уровень валидности. Авторы методик едины в подходах к оценке межкультурной компетентности, стараясь охватить все три домена: знания, навыки и отношение. Описанные в настоящей статье методики могут быть использованы учеными при исследовании уровня межкультурной компетентности медицинских работников, а также организациями медицинского образования для оценки эффективности академических программ или специализированных программ повышения квалификации. Поскольку оказание культурно компетентной медицинской помощи имеет важное значение для этнически разнообразного населения, измерение культурной компетентности и ее влияния на результаты лечения пациентов должно стать важным приоритетом для будущих исследований. Данный обзор освещает только часть существующих методик оценки межкультурной компетентности. В будущем планируется провести аналогичный обзор и по другим инструментам оценки.*

Ключевые слова: *межкультурная компетенция, инструменты оценки межкультурной компетенции, культурная компетентность, межкультурная коммуникация, CSES, CAS, IAPCC-R, IAPCC-SV, TSET, SAICS*

Для цитирования: Уйсенбаева Ш. О. Обзор инструментов оценки межкультурной компетенции медицинских специалистов // Бизнес. Образование. Право. 2022. № 2 (59). С. 344—349. DOI: 10.25683/VOLBI.2022.59.259.