DOI 10.22394/1726-1139-2022-2-123-138

Психологические аспекты информационной безопасности организации в контексте социоинженерных атак[1]

Тулупьева Т. В.

Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (Северо-Западный институт управления РАНХиГС), Санкт-Петербург, Российская Федерация; tulupeva-tv@ranepa.ru

РЕФЕРАТ

Целью данной обзорной статьи является определение подходов к решению имеющихся проблем в учете психологических аспектов информационной безопасности организации в контексте социоинженерных атак на основе анализа и систематизации источников по данной теме. **Методы.** Для достижения поставленной цели выбраны два взаимодополняющих направления. Первое направление включало в себя изучение выбранных специализированных журналов. В рамках второго направления была проанализирована представленность данной проблемы в базе данных Scopus за последние 20 лет. **Результаты.** Проведен анализ психологических аспектов ключевых элементов социоинженерной атаки: знания и умения злоумышленника, организационные условия, особенности сотрудника, который является частью автоматизированных информационных систем и направления обучения и профилактики. Предложена модель социоинженерной атаки с учетом психологических аспектов. **Выводы.** Проведенное исследование показало, что разработанных сейчас подходов достаточно для того, чтобы они легли в основу пересмотра кадровых процессов в организации. Без подключения кадровых служб в части изменения кадровых процессов с учетом политик информационной безопасности проблема социоинженерных атак не может быть решена. Результаты данного исследования будут интересны специалистам в области управления персоналом, подготовки кадров, информационной безопасности, информационных технологий, искусственного интеллекта; руководителям, владельцам бизнеса, руководителям государственных и муниципальных органов.

Ключевые слова: социальная инженерия, атакующее воздействие, уязвимость пользователя, обучение

Для цитирования: *Тулупьева Т. В.* Психологические аспекты информационной безопасности организации в контексте социоинженерных атак // Управленческое консультирование. 2022. № 2. С. 123–138.

Psychological Aspects of the Organization's Information Security in the Context of Socio-engineering Attacks

Tatyana V. Tulupieva

[1]Russian Presidential Academy of National Economy and Public Administration (North-West Institute of Management, Branch of RANEPA), Saint-Petersburg, Russian Federation; tulupeva-tv@ranepa.ru

ABSTRACT

The purpose of this review article is to determine approaches to solving existing problems in taking into account the psychological aspects of an organization's information security in the context of socio-engineering attacks based on the analysis and systematization of sources on this topic. **Methods.** To achieve this goal, two complementary directions were chosen. The first direction included the investigation of selected specialized journals. The second direction involved

[1] Исследование выполнено при финансовой поддержке Фонда развития научных исследований и прикладных разработок СЗИУ РАНХиГС.

the analysis of the representation of this problem in the Scopus database over the past 20 years. **Results.** The analysis of the psychological aspects of the key elements of a socio-engineering attack is carried out: the knowledge and skills of the attacker, organizational conditions, the characteristics of an employee who is part of information systems and the direction of training and prevention. A model of socio-engineering attack considering psychological aspects is proposed. **Conclusions.** The study showed that the approaches developed now are sufficient to form the basis for the revision of personnel processes in the organization. The problem of social engineering attacks cannot be solved without the involvement of HR services in terms of changing HR processes, taking into account information security policies. The results of this study will be of interest to specialists in the field of personnel management, personnel training, information security, information technology, artificial intelligence, executives, business owners, heads of state and municipal bodies.

Keywords: social engineering, attack impact, user vulnerability, training

For citing: Tulupieva T. V. Psychological Aspects of the Organization's Information Security in the Context of Socio-engineering Attacks // Administrative consulting. 2022. N 2. P. 123–138.

Введение

Кибербезопасность быстро превратилась в серьезную социальную проблему XXI в. [44]. Компания Verizon в своем отчете, выпущенном в 2021 г. [1], проанализировала 79 635 инцидентов атак в отношении организаций из 88 стран мира за 2020 г., из них 5258 случаев сопровождались нарушениями данных. В 2019 г. насчитывалось 3950 случаев утечки данных, то есть это значение возросло на треть за последний год. 85% случаев утечки данных связано с человеческим фактором. Было проанализировано 885 случаев нарушений в области государственного управления [40]. Из них на долю социальной инженерии приходится 69%, 80% украденных данных составляли учетные данные. При этом анализ динамики утечки данных в организациях за последние несколько лет показывает, что, хотя детали могут измениться, основная тенденция сохраняется.

В сфере информационной безопасности происходит непрерывный поток инцидентов и нарушений, о которых сообщают СМИ, государственные органы и регулирующие органы [15]. С ростом популярности интернета растет число угроз информационной безопасности, таких как социальная инженерия, взлом и вредоносное программное обеспечение. Несмотря на обычное использование методов безопасности для защиты информационных систем, таких как биометрия и антивирусное ПО, ландшафт угроз постоянно меняется. Например, в период с 2010 по 2017 г. в результате утечки данных было раскрыто более 7,1 млрд личных данных, что эквивалентно одному на каждого человека в мире. В 2016 г. было раскрыто более 1,1 млрд данных по сравнению с более чем 563 млн в 2015 г. (почти вдвое больше). В этих случаях утечки данных процент потерянной финансовой информации, такой как данные кредитной или дебетовой карты, составил 32,9% в 2015 г. и увеличился на 10% до 42,9% в 2016 г. [5]. Угрозы информационным системам организации продолжают приводить к значительным финансовым потерям и потерям интеллектуальной собственности [12].

В то время как различные контрмеры, в том числе аппаратные и программные средства и протоколы, были разработаны для смягчения проблемы, за рамками рассмотрения часто остается отдельный человек — сотрудник, пользователь [18]. Конечного пользователя часто называют самым слабым звеном в информационной системе [11; 17; 19; 30; 39]. Тенденцию последнего времени в сфере информационной безопасности хорошо иллюстрирует фраза: «Только любители атакуют машины, профессионалы нацелены на людей» [10, с. 802]. Однако, учитывая факт, что разные пользователи по-разному реагируют на одни и те же стимулы, опре-

деление причин различий в поведении в сфере безопасности и того, почему одни пользователи могут быть «подвержены риску» больше, чем другие, является серьезным фактором защиты пользователей и организаций от атак на систему безопасности [5].

Выявление таких характеристик, которые могут влиять на поведение пользователей в области безопасности и высокой степени уязвимости к угрозам, является важным шагом построения политик безопасности. Однако, поскольку, намерения пользователей могут отличаться от их фактического поведения, крайне важно понимать, в какой степени пользователи реализуют правильное поведение в области безопасности. Следовательно, знание того, как на это поведение влияют особенности пользователей и организационные условия, поможет в разработке решений, которые повышают информационную безопасность организации [5].

Повсеместная оцифровка информации и возможность удаленного подключения рабочих систем неизбежно способствовали промышленному шпионажу с использованием киберпространства. Сбои в системе безопасности объясняют большинство инцидентов, связанных с киберпромышленным шпионажем, а инсайдеры могут непреднамеренно или намеренно создавать серьезные угрозы для организаций, облегчая доступ к конфиденциальным данным, являющимся собственностью, или злоупотребляя ими. Технические решения по обеспечению безопасности имеют довольно ограниченные возможности для решения этой проблемы, а социотехнический или социоинженерный подход может предоставить больше перспектив для решения проблемы. Такой подход мог бы преодолеть разрыв между разработкой и реализацией решений безопасности и созданием организационной культуры, ориентированной на безопасность.

Социоинженерная атака (СИА) — это нетехнический тип атаки, основанный на взаимодействии человека и дополняющий технические атаки. С. Абрахам и И. Ченгалур-Смит [2] предложили следующее определение: Использование социальной маскировки, культурных уловок и психологических уловок, чтобы заставить пользователей компьютеров (то есть целей) помочь хакерам (то есть преступникам) в их незаконном вторжении или использовании компьютерных систем и сетей. Одна из опасностей атак социальной инженерии — это их безобидный и якобы законный вид, так что пользователи не подозревают о том, что они стали жертвами при помощи обмана и манипуляции [10]. В контексте кибербезопасности социальная инженерия описывает тип атаки, в которой злоумышленник использует уязвимости человека (с помощью таких средств, как убеждение, обман, манипулирование и побуждение) для нарушения целей безопасности (таких как конфиденциальность, целостность, доступность). Обобщая, можно сказать, что социальная инженерия — это тип атаки, при которой злоумышленник использует уязвимость человека посредством социального взаимодействия для нарушения информационной безопасности [9; 28].

Многие отличительные особенности делают социальную инженерию довольно популярной и серьезной, универсальной и постоянной угрозой кибербезопасности [16; 33; 53].

1. По сравнению с классическими атаками социальная инженерия использует человеческие уязвимости для обхода или преодоления барьеров безопасности без необходимости бороться с брандмауэром или антивирусным программным обеспечением.

2. Для некоторых сценариев атак социальная инженерия может быть такой простой, как телефонный звонок или выдача себя за другого для получения секретной информации.

3. По мере развития технологий безопасности классические атаки становятся все сложнее, и все больше и больше злоумышленников обращаются к социальной инженерии.

4. Не существует информационных систем, которые не полагались бы на людей и не включали бы человеческий фактор, и этот человеческий фактор явно уязвим и может быть в значительной степени превращен в уязвимости безопасности организации квалифицированными злоумышленниками.

5. Сейчас социальная инженерия получает не только большие объемы конфиденциальной информации о людях, сети и устройствах, но и больше каналов атаки с помощью различных приложений, таких как сайты социальных сетей, Интернет вещей, мобильная связь [36].

6. Социальная инженерия становится более эффективной и автоматизированной благодаря таким технологиям, как машинное обучение и искусственный интеллект. В результате может быть достигнута большая группа целей, а конкретные жертвы могут быть тщательно отобраны для создания более надежной атаки. Становятся возможными целевые, крупномасштабные, роботизированные, автоматизированные и продвинутые атаки социальной инженерии [47].

С пандемией коронавируса (COVID-19) увеличилось использование онлайн-сервисов, а значит, и возможности для социоинженерных атак [7].

Цель данной статьи: сформулировать подходы к решению имеющихся проблем в учете психологических аспектов информационной безопасности организации в контексте социоинженерных атак на основе анализа и систематизации релевантной информации.

Перед написанием статьи была выдвинута гипотеза: даже при превалирующем технократическом подходе к данной проблеме накопленная информация создала основу для пересмотра имеющихся кадровых практик с учетом психологического аспекта информационной безопасности организации.

Материалы и методы

Метаанализ был использован для ответа на вопросы исследования. Было выбрано два взаимодополняющих направления. Первое направление включало в себя изучение выбранных специализированных журналов. В рамках второго направления была проанализирована представленность данной проблемы в базе данных Scopus.

Информационные ресурсы

В выбранный список вошли следующие издания: ACM Transactions on Information Systems, ACM Transactions on Management Information Systems, Information and Computer Security, Journal of Management Information Systems, Journal of Managerial Psychology, Journal of Organizational and End User Computing, Security Journal. Издания выбирались таким образом, чтобы рассмотреть аспект информационной безопасности, аспект управления в организации и очень важный юридический аспект. Кроме того, данное исследование относится к междисциплинарным, поскольку соединяет в себе проблемы и задачи, лежащие как в области психологии, управления, так и в области информационной безопасности, искусственного интеллекта и информационных технологий. Выбранные периодические издания в той или иной мере отражают указанную междисциплинарность.

После изучения выбранных источников проводился анализ представленной темы в базе данных Scopus. Было сделано три последовательных запроса:

- TITLE-ABS-KEY (Social engineering);
- TITLE-ABS-KEY (Social engineering attac);
- (TITLE-ABS-KEY (Social engineering attack)) AND (human OR psychological).

Результаты

В выбранных журналах было изучено 987 статей, из которых 43 статьи (4,4%) были посвящены социоинженерным атакам. Распределение представленности выбранной темы по годам изучения представлено в табл.

Обращает на себя внимание тот факт, что теме социоинженерных атак в контексте информационной безопасности не было уделено внимания в журналах, посвященных управленческой психологии и информационным системам для менеджмента. Журнал «Information and Computer security» в 2018 г. теме человеческого фактора, аспектов, связанных с человеком в системе безопасности, посвятил отдельный специальный выпуск. То есть важность социоинженерных атак и психологических факторов отражена в журналах, посвященных информационной безопасности, информационным системам (преимущественно технические журналы) и журнале, посвященном юридическим аспектам безопасности, но не в журналах, предназначенных для руководителей. А ведь именно руководители принимают решение и о создании организационной системы, обеспечивающей информационную безопасность, и о создании системы профилактических мер. Специалисты в сфере информационной безопасности уже стали задаваться вопросом, как наглядно объяснить руководителям важность учета возможных социоинженерных атак в системе информационной защиты организации. В частности, B. von Solms and R. von Solms — авторы статьи «Кибербезопасность и информационная безопасность — как соотносятся друг с другом?» (Cybersecurity and information security — what goes where?) — в 2018 г. видели своей целью дать упрощенное определение кибербезопасности и управлению кибербезопасностью и объяснить советам директоров и исполнительному руководству их обязанности и ответственность в этом вопросе [51]. Ряд других авторов явно указывают на то, какие последствия для организации может иметь невнимательное отношение к этой теме [5; 12]. Сейчас явно намечается запрос на изменение кадровых практик, инициированный именно специалистами в области информационной безопасности, социальной инженерии. Ими же разрабатываются рекомендации для руководства и кадровых служб организаций по повышению устойчивости сотрудников к социоинженерным атакам, но статистические данные (например, ежегодные отчеты о расследовании утечки данных «Data Breach Investigations Report», публикуемые компанией Verizon, демонстрирующие рост успешных социоинженерных атак, говорят о том, что превентивные меры не стали нормальной, регулярной практикой в организациях [1]. Изучение информационной безопасности,

Таблица

Представленность статей по социоинженерным атакам
Table. Representation of articles on socio-engineering attacks

Журнал / Год	ACM Transactions on Information Systems	ACM Transactions on Management Information Systems	Information and Computer Security	Journal of Organizational and End User Computing	Security Journal
	%				
2018	2	6	47	0	0
2019	0	12	14	5	4
2020	2	15	6	4	6
2021	0	9	4	1	0

социоинженерных атак в рамках менеджмента должно сейчас попасть в число первоочередных вопросов повестки дня.

Запрос в базе данных Scopus подтвердил высокий интерес к этой теме. Всего по запросу «Social engineering» было обнаружено 2637 статей[1]. Первая статья, в которой встречается словосочетание «социальная инженерия», датируется 1926 г., конечно этот термин тогда рассматривался в несколько другом контексте. Из выявленных публикаций подавляющее большинство (2237) было издано за последние 20 лет, что показывает, как резко возросло внимание к этой теме в XXI в. Динамика публикаций по годам по социальной инженерии вообще и по социоинженерным атакам, в частности, представлена на рис. 1.

Социоинженерные атаки тесно связаны с человеческим фактором и психологическими особенностями, что подтверждается диаграммой на рис. 2.

Интересным является подъем числа публикаций в сфере социальной инженерии и социоинженерных атак в 2016 г. Данный всплеск интереса мог явиться следствием ставшей тогда достоянием общественности истории со взломом электронной почты Джона Бреннана, директора ЦРУ, осенью 2015 г. при помощи многоходовой социоинженерной атаки [31].

Первая публикация, содержащая описание именно социоинженерной атаки, датируется 1995 г. [55]. Это была статья в трудах симпозиума по безопасности и следом за ней (в 1996 г.) вышла статья с тем же авторством в журнале «Вычислительные системы» (Computing systems) [56]. Примечательным является начало аннотации к статье: «Многие компании тратят сотни тысяч долларов на обеспечение корпоративной компьютерной безопасности. Система безопасности защищает секреты компании, <...> и обеспечивает конфиденциальность клиентов компании. К сожалению, с помощью социальной инженерии можно обойти даже лучшие механизмы безопасности.» [56, с. 3] Примерно с таких же слов начинаются статьи, посвященные социоинженерным атакам и в наше время, только они усиливаются еще конкретными значениями потерь организации от социоинженерных атак. 25 лет назад была поставлена проблема, которая

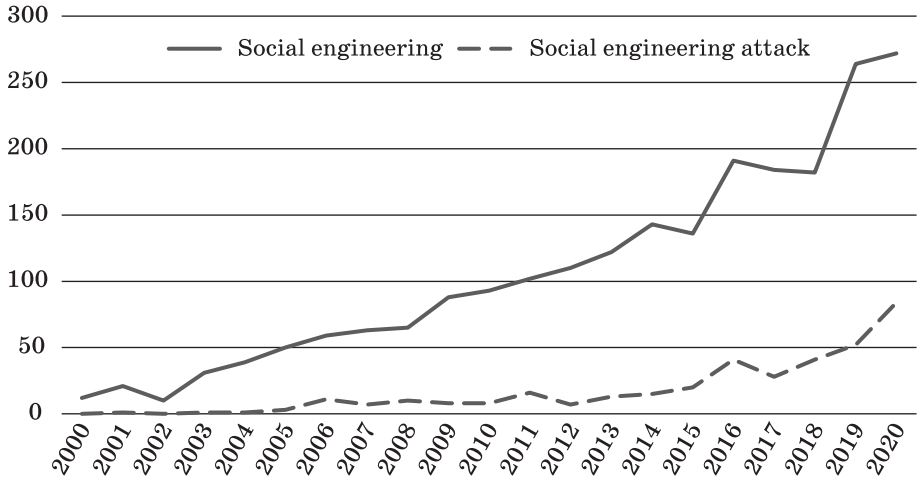

Рис. 1. Динамика публикаций по социальной инженерии социоинженерным атакам
Fig. 1. Dynamics of publications on social engineering and socio-engineering attacks

[1] Дата запроса —30 октября 2021 г.

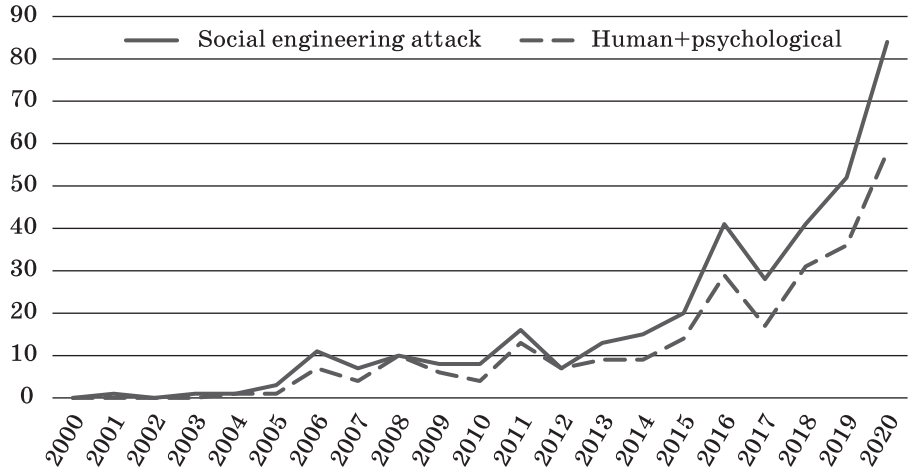

Рис. 2. Динамика публикаций по социоинженерным атакам и учету психологического фактора в них
Fig. 2. Dynamics of publications on socio-engineering attacks and consideration of psychological factor in them

активно изучается в сфере информационной безопасности, но, если кадровые службы и руководители компаний не будут серьезно работать над изменением кадровых технологий, ситуация будет сохранять свою негативную тенденцию. В этой же статье дается определение социальной инженерии в контексте компьютерной безопасности: «Социальная инженерия — это термин, которым хакеры называют получение информации о компьютерных системах нетехническими средствами» [56, с. 5]. В статье анализируются факторы, обеспечивающие успешность социоинженерной атаки: низкий уровень осознания сотрудниками политик безопасности, человеческие слабости, непроверенные практикой организационные планы и процедуры в области безопасности. В статье подробно описывается атака социальной инженерии, проведенная против компании с ее разрешения, в результате которой была получена конфиденциальная информация компании и многочисленные пароли пользователей из многих подразделений компании. Документ завершается рекомендациями по минимизации угрозы социальной инженерии. Мы так подробно остановились именно на этой статье, потому что она задала вектор исследований на следующую четверть века и создает хорошую структурную основу для анализа последующих публикаций по этой теме: знания и умения злоумышленника, организационные условия, особенности сотрудника, который является частью автоматизированных информационных систем и направления обучения и профилактики.

Именно по этим направлениям и будет проводиться обзор публикаций.

Знания и умения злоумышленника

Злоумышленник для разработки и осуществления СИА должен обладать рядом знаний и умений. Он сначала изучает целевую жертву, чтобы собрать исходную информацию для кибератаки, затем пытается завоевать доверие жертвы и убедить ее предпринять дальнейшие действия, которые в итоге приведут к нарушению безопасности, такие как раскрытие конфиденциальной личной информации или предоставление доступа к личным профилям [7]. Существует огромное количество атак социальной инженерии для получения информации или доступа к системам

с помощью эксплуатации ничего не подозревающих сотрудников [19]. Несмотря на различные виды атак, можно выделить типичные этапы СИА [4]:
1) сбор информации об организации и жертве;
2) развитие отношений с жертвой;
3) эксплуатация отношений;
4) исполнение, направленное на достижение цели.

F. Mouton, L. Leenen, H. Venter [34] добавляют еще одну фазу — выход, не оставляя следов.

Для успешной реализации СИА злоумышленники используют разнообразные принципы и методы социального влияния. Р. Чалдини [13] определяет шесть психологических принципов влияния (или оружия влияния) как взаимность, приверженность и последовательность, социальное доказательство, симпатию, авторитет и дефицит. Принцип взаимности гласит, что люди склонны реагировать тем же, если им оказали услугу. Им также нравится быть последовательными, оставаться приверженными делу и действовать так, как действуют другие. Их тянет к другим, подобным им самим, и они уважают авторитетных фигур и отзываются на них. Наконец, люди обращают внимание на дефицитные вещи. Это оружие можно использовать для создания более убедительного (Санкт-Петербург, Российская Федерация) сообщения. Например, ссылка, встроенная в сообщение, с большей вероятностью будет нажата, если будет обещано что-то хорошее (например, подарочная карта) [21]. Авторитет, социальное доказательство и отвлечение были наиболее широко используемыми принципами влияния в атаках, за которыми следуют симпатия, сходство и обман. Эти принципы убеждения присутствовали в большинстве атак, в то время как приверженность, взаимность и последовательность — нет. Кроме того, злоумышленники комбинируют эти принципы, а конкретные способы реализации отдельных принципов влияния были довольно редкими [22]. Злоумышленнику нужно понимать механизмы воздействия, которые описывают, как методы атаки используют уязвимости человека, и объясняют, почему человеческие уязвимости приводят именно к таким последствиям атаки, а также, как методы атаки помогают достигать целей атаки. Таким образом, механизм воздействия, уязвимость человека и метод атаки могут служить тремя основными сущностями, позволяющими понять, как работают и действуют атаки социальной инженерии [52].

Организационные условия

Сначала стоит обратить внимание не на организационные условия, а на социально-экономический уровень страны в целом. Более высокий доход, более высокий уровень образования, более низкий уровень бедности повышают охват использования Интернета, что создает благоприятные условия для социоинженерных атак [38]. Уровень внедрения Интернета в нашу жизнь будет увеличиваться, следовательно, нужно обращать больше внимания на создание специальных организационных условий и политик безопасности, препятствующих успешности СИА.

Рост угроз кибербезопасности и проблемы, с которыми сталкиваются организации по защите своих информационных технологий, сделали соблюдение организационных процессов и процедур контроля безопасности важной проблемой, требующей адекватного решения. Знания о кибербезопасности и убеждения сотрудников существенно влияют на намерения сотрудников соблюдать механизмы контроля организационной кибербезопасности [37]. Лидерство, согласно исследованиям, играет критическую роль в содействии соблюдению организацией предписанных механизмов контроля безопасности [37]. Поэтому для эффективного соблюдения требований кибербезопасности именно руководители и лица, определяющие политику, должны продвигать инициативы по обеспечению безопасности организации, которые обеспечивают включение принципов и практик кибер-

безопасности в должностные инструкции, процедуры и процессы. Здесь уже сама организация начинает использовать принцип авторитета, выдвинутый Р. Чалдини. То есть непременным условием, снижающим успешность СИА, является поддержка руководством политики информационной безопасности и — что очень важно — следование разработанным правилам информационной безопасности. Более того, выявлено, что в поведении в области информационной безопасности присутствует «эффект леммингов» (эффект массовой поддержки небезопасного поведения) и может привести к парадоксальным проявлениям [46]. Анализ «эффекта леммингов» можно использовать, чтобы помочь компании понять, как сотрудники влияют друг на друга с точки зрения безопасности. И здесь роль руководителей и лидеров снова является определяющей.

Привлечение сотрудников к разработке правил информационной безопасности и внедрению мер защиты информации, разъяснение им необходимости таких правил является следующим условием. Это снизит количество нарушений со стороны сотрудников. Сотрудники, считающие, что организацией движет необходимость оптимизировать использование информации, считали, что меры безопасности оправданы [8]. Кроме того, если дать сотрудникам уверенность в том, что ко всем будут применяться одинаковые меры, когда дело доходит до применения санкций, количество нарушений также уменьшится [6]. И с точки зрения создания действующей стратегии информационной безопасности важны не суровость санкций, а немедленность обратной связи, то есть, не строгость наказания, а время реакции, дополненная организационной поддержкой [20]. И здесь уже речь идет о создании специальной корпоративной культуры, в которой согласованы процессы и ценности, связанные с рабочей ситуацией и чувствительностью к защите информации [24], когда сотруднику не приходится выбирать выполнить задачу в срок, любой ценой, используя незащищенные каналы передачи информации, или задуматься о возможной утечке чувствительной информации. На намерение соблюдать требования информационной безопасности влияют личные установки и нормы [54]. Результаты показывают, что, когда сотрудники попадают в затруднительное положение, они с большей вероятностью будут проявлять несоблюдение требований. Сотрудники также склонны отказываться от безопасного поведения, если такое поведение воспринимается как неудобное [3]. Следовательно, организации должны найти способы уменьшить воспринимаемое неудобство, используя различные методы автоматизации безопасности и специализированное обучение безопасности. Изучая, как препятствия приводят к таким ситуациям, специалисты по безопасности могут определить новые механизмы, чтобы противодействовать переходу сотрудников от соблюдения требований к несоблюдению [23]. Согласование стратегических ценностей и процессов возможно на основе модели анализа критических факторов успеха, которые способствуют эффективности управления информационной безопасностью [49]. При согласовании ценностей бизнеса, поддержке высшего руководства и осведомленности организации о рисках и средствах контроля безопасности можно разработать эффективные средства контроля информационной безопасности, что приведет к успешному управлению информационной безопасностью.

Создание культуры, способствующей информационной безопасности, поможет положительно повлиять на восприятие сотрудниками конфиденциальности и ответственности, что в свою очередь влияет на нарушения информационной безопасности [6; 25].

Особенности сотрудника

Поскольку сотрудник-пользователь является частью информационной системы, то те или иные его личностные особенности оказывают влияние на то, как он будет реагировать на социоинженерную атаку и ассоциированы с профилем уязвимости

пользователя. Зная психологические особенности сотрудников, можно предположить выраженность уязвимостей у каждого конкретного сотрудника и возможные вредоносные (даже невольные, случайные) действия, на которые он способен. Тогда возникает задача сопоставления личностных особенностей сотрудников с теми профилями, которые могут быть критичными для организации с точки зрения сохранности информации. Если организация большая, то такой процесс сопоставления нужно проводить не в ручном режиме, а автоматизировано. Есть ряд исследований, в которых разработали технологии сопоставления личностных особенностей и определенных требований рабочего места. В частности, определение личностных особенностей при приеме на работу и автоматическое (при помощи нейронных сетей) определение соответствия личностных качеств человека требованиям вакансии [41]. Благодаря дизайну иерархической структуры представления, нейронная сеть, определяющая соответствие «кандидат — вакансия», может не только оценить, подходит ли кандидат для работы, но также определить, какие конкретные элементы требований в объявлении о вакансии удовлетворены кандидатом, путем измерения расстояний между соответствующими представлениями [58]. То есть решение задачи «оптимального найма», в которой цель состоит в том, чтобы выбрать минимальное количество новых сотрудников из набора кандидатов для заполнения вакантных должностей, созданных уходящими сотрудниками, обеспечивая при этом удовлетворительность указанным условиям безопасности [42], достаточно легко адаптируется под условия оценки уязвимости персонала, основываясь на личных особенностях.

При изучении связи личностных особенностей и поведения в сфере информационной безопасности был выявлен ряд свойств. Четыре фактора из так называемой Большой пятерки (пятифакторный опросник личности) — добросовестность, сотрудничество, открытость новому и нейротизм — связаны с безопасностью поведения [5]. Добросовестность отрицательно коррелирует с риском большинства действий, связанных с безопасностью пользователей. Аналогичная тенденция наблюдается и в отношении личностных факторов сотрудничества и открытости; оба отрицательно коррелируют с уровнем риска в области безопасности. Люди с высоким уровнем нейротизма могут быть эмоциональными и более нестабильными; в результате их поведение в сфере безопасности может быть более рискованным, чем у других. Стрессоустойчивость и отсутствие стрессов на работе вносят свой вклад в безопасное поведение: сотрудники с большей стрессоустойчивостью также имели более высокий уровень осведомленности о информационной безопасности [29].

При исследовании демографических факторов возраст статистически достоверно отрицательно связан с уровнем риска, что позволяет предположить, что, чем моложе пользователь, тем выше риск [5]. Одна из причин этого может заключаться в том, что, чем взрослее человек, тем он ответственнее. Так, наиболее уязвимы к фишинговым атакам оказались женщины и молодые люди в возрасте от 18 до 25 лет [21].

Чем выше уровень ИТ-навыков пользователей и их знакомство с ИТ-услугами, тем ниже уровень риска, связанный с их поведением, они, как правило, более серьезно относятся к ИТ-безопасности. Однако пользователи с очень высоким уровнем навыков в сфере ИТ могут быть более самоуверенны и, как следствие, недооценивать определенные риски [5].

Профилактика и обучение

Для того чтобы разрабатывать превентивные меры в организации, нужно хорошо понимать, какие типы СИА бывают и анализировать их. Поскольку атак может быть очень много, для анализа нужно применять достижения в области искусственного

интеллекта [44]. Также важно применять более проактивный подход к выявлению возникающих угроз и успешных моделей кибербезопасности, которые в итоге улучшат состояние информационной безопасности организации. Данный подход может состоять в регулярном мониторинге новостных статей в авторитетных СМИ и публикации в релевантных академических периодических изданиях [27].

Следующим этапом является оценка вероятности компрометации информации (раскрытие или повреждение) в результате атаки социальной инженерии и потенциальных потерь, чтобы эффективно дополнять существующие инструменты оценки безопасности. Оценка защищенности информации может осуществляться на основе профилирования пользователей (сотрудников) и дальнейшей группировки пользователей для разработки мер профилактического воздействия [57]. Дополнительным инструментом может быть метод измерения индекса культуры конфиденциальности информации [14].

На основе имеющейся информации следует строить процесс управления информационной безопасностью с помощью цикла Деминга «планирование — выполнение — проверка — действие(корректировка)» (PDCA) [35] и постоянно его эмпирически проверять и вносить корректировки. Для проверки рекомендуется использовать мониторинг информационной безопасности. Мониторинг делает упор на ожидаемое поведение и помогает укрепить организационные нормы, мониторинг (в том числе, самомониторинг) также может ускорить обучение, когда сотрудники начинают внимательно следить за своим поведением. Тем не менее при таком общении необходимо соблюдать осторожность, чтобы избежать недовольства и ощущения подозрения в недоверии среди сотрудников [3].

При разработке мероприятий профилактик и программ обучения следует учитывать, что сотрудникам с разным уровнем осведомленности и навыков в сфере информационной безопасности, с разными личностными особенностями следует предлагать разные мероприятия. Рекомендации, основанные на подходе «один размер для всех», не являются очень эффективными, поэтому сотрудников для обучения нужно делить по уровням и группам [48]. Это подтверждает и то, что наиболее эффективны высокоинтенсивные вмешательства с узкой направленностью [10], то есть, важно точечное, специализированное обучение. Иными словами, предлагается снижение уязвимости человека путем измерения текущего статуса и предоставления подходящего решения для устранения разрыва между осведомленностью и поведением текущего пользователя и целевым уровнем для повышения безопасности организации [7]. Также нужно учитывать, что меры по профилактике и обучению могут иметь ограничения из-за подверженности человека эмоциональному влиянию [34].

Помимо традиционных (инструкции и классическое обучение по информационной безопасности) предлагается ряд интерактивных обучающих методов.

1. Игровой метод. Игровое обучение оказалось эффективным методом во множестве областей [26]. Правильно разработанные игры могут побуждать пользователей к изменению своего поведения в области безопасности [45]. Так, игровой метод в обучении распознаванию фишинга снижает вероятность успешности фишинга на 40% [21]. Задачи, выполняемые через игровой процесс, могут постепенно становиться более сложными, что, в свою очередь, вынуждает игрока повышать навыки и способности для продолжения успеха [32]. Игры предлагают множество преимуществ, включая положительные когнитивные, мотивационные и социальные эффекты. Игры также требуют навыков и знаний, которые часто приобретаются со временем. Серия испытаний дает игроку возможность улучшить и отточить свою способность добиваться успеха с помощью повторения. Сочетание факторов стимулирует мотивацию, энтузиазм и стремление учиться. Хотя влияние игр на обучение в целом положительное, его величина широко варьируется в зависимости

от множества факторов, включая тип игры, атрибуты игры и то, как она используется в процессе обучения [21].

2. Оценка и обучение через практические задачи. Важность навыков и практической оценки высока и в сфере информационной безопасности. С использованием проверенного экспертами набора задач, основанных на сценариях атак, можно измерить навыки кибербезопасности неспециалистов в области информационных технологий. Этот инструмент применим и в развитии навыков кибербезопасности [12].

3. Двухэтапный подход: предвиктимизационная интервенция в сочетании с обучением. Обучение является эффективным по отношению к тем, кто в нем нуждается и кто осознал, что у него есть зоны развития. Для того чтобы выявить тех, кто демонстрирует небезопасное поведение, используется предварительная виктимизация в имитационной атаке. Это служит для мотивации пользователя: если он попался на атаку социальной инженерии, это побудит его узнать, как этого избежать в будущем. Поэтому часто используют двухэтапный подход:

1) все сотрудники получают, например, фиктивное фишинговое письмо;
2) те, кто выполнили желаемое поведение (например, не щелкнули ссылку), «оставлены в покое», тогда как те, кто стали жертвой (например, щелкнули по ссылке), перенаправляются или приглашаются для участия в тренинге по социальной инженерии [10].

Обсуждение

На основе проведенного исследования, обобщив изученные материалы и взяв за основу интегральную модель социального влияния [50], можно предложить модель социоинженерной атаки с учетом психологических аспектов (рис. 3).

Злоумышленник, обладая определенными знаниями в области социальной инженерии и навыками, располагая знаниями о жертве и ее уязвимостях, собранных предварительно, выбирает тип атаки и планирует ее. Но на выбор атаки влияет не только сам злоумышленник, но и организационные условия (политики безопасности, корпоративная культура, установки руководства, технические условия) и осо-

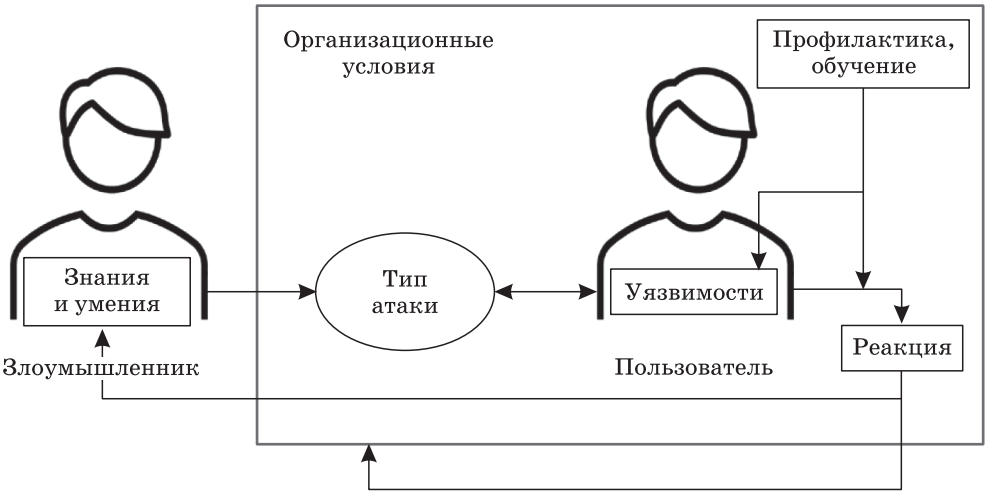

Рис. 3. Модель социоинженерной атаки с учетом психологических аспектов
Fig. 3. Model of socioengineering attack taking into account psychological aspects

бенности жертвы — самого сотрудника организации, пользователя информационной системы. Тип атаки должен соответствовать профилю уязвимости пользователя, а значит, тип атаки зависит и от пользователя. То есть социоинженерная атака выбирается на основе сочетания трех компонентов модели: злоумышленник, пользователь и организационные условия.

Вследствие осуществленной социоинженерной атаки пользователь демонстрирует реакцию. Это может быть: вредоносное действие (тогда СИА считается успешной), информирование службы безопасности об осуществленной попытке получить доступ к информации или просто игнорирование действий злоумышленника. То, какую реакцию продемонстрирует пользователь, зависит от его особенностей, его уязвимостей, его психического состояния на настоящий момент. Организационные условия создают фон для демонстрации той или иной реакции пользователя. Например, правильно выстроенная и объясненная сотрудникам политика безопасности снижает вероятность совершения вредоносных действий. Меры профилактики и программы обучения, разработанные в определенных организационных условиях, могут влиять как на уязвимости пользователя, так и на реакции пользователя. Продемонстрированная реакция пользователя влияет на организационные условия и на знания и умения злоумышленника. Так, игнорирование действий злоумышленника может привести к тому, что ему придется совершенствовать свои знания и навыки для следующей социоинженерной атаки, чтобы получить желаемое. Наоборот, совершение вредоносных действий пользователем может привести к пересмотру политик безопасности, установки руководства по отношению к информационной безопасности или к пересмотру корпоративной культуры.

Заключение

Большинство организаций зависят от конфиденциальности и целостности своих информационных активов, информационная безопасность играет решающую роль в благополучии такой организации. В настоящее время множество организаций использует киберпространство для критически важных бизнес-процессов, и интернет стал неотъемлемой частью в современных информационных системах.

Проведенное исследование показало, что разработанных сейчас подходов достаточно для того, чтобы они легли в основу пересмотра кадровых процессов в организации. Без подключения кадровых служб в части отбора персонала с определенными личностными особенностями, разработки политик информационной безопасности, мотивирующих воздействий в отношении соблюдения разработанных политик, корпоративной культуры, провозглашающей ценность безопасного поведения, правильной системы информационного мониторинга и, главное, обучения, специализированного с учетом имеющихся знаний и навыков каждого сотрудника, проблема социоинженерных атак не может быть решена.

Результаты данного исследования будут интересны специалистам в области управления персоналом, подготовки кадров, информационной безопасности, информационных технологий, искусственного интеллекта; руководителям, владельцам бизнеса, руководителям государственных и муниципальных органов.

Литература/ References

1. 2021 Data Breach Investigations Report (DBIR) [Electronic resource]. URL: https://enterprise.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdfx/ (дата обращения: 20.12.2021).
2. Abraham S., Chengalur-Smith I. “An overview of social engineering malware: TRENDS, tactics, and implications” // Technology in Society. 2010. Vol. 32. N 3. P. 183–196.

3. Ahmad Z., Ong T.S., Liew T.H., Norhashim M. Security monitoring and information security assurance behaviour among employees: An empirical analysis // Information and Computer Security. 2019. Vol. 27. N 2. P. 165–188.
4. Algarni A., Xu Y., Chan T., Tian Y.-C. Social engineering in social networking sites: Affect-based model // Internet Technology and Secured Transactions (ICITST). 8th International Conference for. IEEE. 2013. P. 508–515.
5. Alohali M., Clarke N., Li F., Furnell S. Identifying and predicting the factors affecting end-users' risk-taking behavior // Information and Computer Security. 2018. Vol. 26. N 3. P. 306–326.
6. Alshare K.A., Lane P.L., Lane M.R. Information security policy compliance: a higher education case study // Information and Computer Security.2018. Vol. 26. N 1. P. 91–108.
7. Alsharif M., Mishra S., AlShehri M. Impact of Human Vulnerabilities on Cybersecurity // Computer Systems Science and Engineering. 2022. Vol. 40 (3). P. 1153–1166.
8. Ashenden D. In their own words: employee attitudes towards information security // Information and Computer Security. 2018. Vol. 26. N 3. P. 327–337.
9. Bezuidenhout M., Mouton F., Venter H. Social engineering attack detection model: Seadm // Information Security for South Africa (ISSA), 2010. IEEE. 2010. P. 1–8.
10. Bullee J.-W., Junger M. How effective are social engineering interventions? A meta-analysis // Information and Computer Security.2020. Vol. 28. N 5. P. 801–830.
11. Camp L.J., Grobler M., Jang-Jaccard J., Probst C. at al. Measuring human resilience in the face of the global epidemiology of cyber attacks // Proceedings of the 52nd Hawaii International Conference on System Sciences. 2019.
12. Carlton M., Levy Y., Ramim M. Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills // Information and Computer Security. 2019. Vol. 27. N 1. P. 101–121.
13. Cialdini R. B. Influence: Science and practice (5th ed.). Boston : Allyn & Bacon, 2009.
14. Da Veiga A. An information privacy culture instrument to measure consumer privacy expectations and confidence // Information and Computer Security.2018. Vol. 26. N 3. P. 338–364.
15. Evans M.G., He Y., Yevseyeva I., Janicke H. Published incidents and their proportions of human error // Information and Computer Security.2019. Vol. 27. N 3. P. 343–357.
16. Ghafir I., Prenosil V., Alhejailan A., Hammoudeh M. Social Engineering Attack Strategies and Defence Approaches // 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud). 2016. P. 145–149.
17. Glaspie H.W., Karwowski W. Human factors in information security culture: a literature review // Advances in Human Factors in Cybersecurity. 2018. Springer International Publishing. P. 269–280.
18. Hatzivasilis G., Ioannidis S., Smyrlis M., Spanoudakis G. at al. Modern aspects of cyber-security training and continuous adaptation of programmes to trainees // Applied Sciences. 2020. Vol. 10, N 16. P. 5702.
19. 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 and Security. 2018. Vol. 76. P. 101–127.
20. Hong Y., Xu M. Autonomous Motivation and Information Security Policy Compliance: Role of Job Satisfaction, Responsibility, and Deterrence // Journal of Organizational and End User Computing (JOEUC). 2021. Vol. 33 (6). P. 1–17.
21. Hwang M.I., Helser S. Cybersecurity educational games: a theoretical framework // Information and Computer Securityю 2021. Vol. ahead-of-print N ahead-of-print. DOI: 10.1108/ICS-10-2020-0173.
22. Jones K.S., Armstrong M.E., Tornblad M.K., Siami Namin A. How social engineers use persuasion principles during vishing attacks // Information and Computer Security. 2021. Vol. 29. N 2. P. 314–331.
23. Kajtazi M., Cavusoglu H., Benbasat I., Haftor D. Escalation of commitment as an antecedent to noncompliance with information security policy // Information and Computer Security. 2018. Vol. 26. N 2. P. 171–193.
24. Karlsson M., Denk T., Åström J. Perceptions of organizational culture and value conflicts in information security management // Information and Computer Security. 2018. Vol. 26. N 2. P. 213–229.
25. Kim H.L., Choi H.S., Han J. Leader power and employees' information security policy compliance // Secur J. 2019. Vol. 32. P. 391–409.
26. Komura R., Yajima K. Security education using gamification theory // International Conference on Engineering, Applied Sciences, and Technology (ICEAST). 2018. P. 1–4.

27. Mahdi R. Alagheband, Atefeh Mashatan, Morteza Zihayat. Time-based Gap Analysis of Cybersecurity Trends in Academic and Digital Media // ACM Trans. Manage. Inf. Syst. 2020. Vol. 11. N 4. Art. 20 (December 2020). 20 p. DOI: 10.1145/3389684.
28. Mann M. I. Hacking the human: social engineering techniques and security countermeasures. Gower Publishing, Ltd., 2012.
29. McCormac A., Calic D., Parsons K., Butavicius M. at al. The effect of resilience and job stress on information security awareness // Information and Computer Security.2018. Vol. 26. N 3. P. 277–289.
30. Melzer A., Steffgen G. Trick with treat — reciprocity increases the willingness to communicate personal data // Computers in Human Behavior. 2016. Vol. 61. P. 372–377.
31. Messing Ph., Schram J., Golding B. Teen says he hacked CIA director's AOL account [Electronic resource]. URL: https://nypost.com/2015/10/18/stoner-high-school-student-says-he-hacked-the-cia/ (дата обращения: 20.12.2021).
32. Micallef N., Arachchilage N. A. G. Security questions education: exploring gamified features and functionalities // Information and Computer Securityю 2018. Vol. 26. N 3. P. 365–378.
33. Mitnick K. D., Simon W. L. The art of deception: Controlling the human element of security. John Wiley & Sons, 2011.
34. Mouton F., Leenen L., Venter H. Social engineering attack examples, templates and scenarios // Comput. Secur. 2016, 59, 186–209.
35. Nicho M. A process model for implementing information systems security governance // Information and Computer Securityю 2018. Vol. 26. N 1. P. 10–38.
36. Oliseenko V. D., Abramov M. V., Tulupyev A. L. Identification of user accounts by image comparison: The phash-based approach // Scientific and Technical Journal of Information Technologies, Mechanics and Optics. 2021. Vol. 21 (4). P. 562–570.
37. Onumo A., Ullah-Awan I., Cullen A. Assessing the Moderating Effect of Security Technologies on Employees Compliance with Cybersecurity Control Procedures // ACM Trans. Manage. Inf. Syst. June 2021. Vol. 12. N 2. Art. 11. 29 p. DOI: 10.1145/3424282
38. Park Jiyong, Cho Daegon, Lee Jae Kyu, Lee Byungtae. The Economics of Cybercrime: The Role of Broadband and Socioeconomic Status // ACM Trans. Manage. Inf. Syst. December 2019. Vol. 10. N 4. Art. 13. 23 p. DOI: 10.1145/3351159
39. Parsons K., Calic D., Pattinson M., Butavicius M. at al. The human aspects of information security questionnaire (hais-q): two further validation studies // Computers and Security. 2017. Vol. 66. P. 40–51.
40. Public Administration Data Breaches [Electronic resource]. URL: https://www.verizon.com/business/resources/reports/dbir/2021/data-breach-statistics-by-industry/public-administration-data-breaches/ (дата обращения: 20.12.2021).
41. Qin Chuan, Zhu Hengshu, Xu Tong, Zhu Chen at al. An Enhanced Neural Network Approach to Person-Job Fit in Talent Recruitment // ACM Trans. Inf. Syst. March 2020. Vol. 38. N 2. Art. 15. 33 p. DOI: 10.1145/3376927.
42. Roy Arindam, Sural Shamik, Majumdar Arun Kumar, Vaidya Jaideep at al. Optimal Employee Recruitment in Organizations under Attribute-Based Access Control // ACM Trans. Manage. Inf. Syst. March 2021. Vol. 12. N 1. Art. 6. 24 p. DOI: 10.1145/3403950
43. Salahdine F., Kaabouch N. Social Engineering Attacks: A Survey // Future Internet. 2019. Vol. 11. N 89. DOI: 10.3390/fi11040089.
44. Samtani S., Kantarcioglu M., Chen Hsinchun. Trailblazing the Artificial Intelligence for Cybersecurity Discipline: A Multi-Disciplinary Research Roadmap // ACM Trans. Manage. Inf. Syst. December 2020. Vol. 11. N 4. Art. 17. 19 p. DOI: 10.1145/3430360
45. Silic M., Lowry P. B. Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance // Journal of Management Information Systems. 2020. Vol. 37. N 1. P. 129–161.
46. Snyman D. P., Kruger H., Kearney W. D. I shall, we shall, and all others will: paradoxical information security behavior // Information and Computer Security. 2018. Vol. 26. N 3. P. 290–305.
47. Stoliarova V. F., Tulupyev A. L. Regression Model for the Problem of Parameter Estimation in the Gamma Poisson Model of Behavior: An Application to the Online Social Media Posting Data // Proceedings of 2021 24th International Conference on Soft Computing and Measurements. 2021. N 9507187. P. 24–27.
48. Tambe Ebot A. Using stage theorizing to make anti-phishing recommendations more effective // Information and Computer Security. 2018. Vol. 26. N 4. P. 401–419.

49. Tu C. Z., Yuan Y., Archer N., Connelly C. E. Strategic value alignment for information security management: a critical success factor analysis // Information and Computer Security. 2018. Vol. 26. N 2. P. 150–170.
50. Tulupieva T. V., Abramov M. V., Tulupiev A. L. Model of Social Influence in Analysis of Socio-engineering Attacks // Administrative Consulting. 2021. Vol. 8. P. 97–107. (In Russ.)
51. von Solms B., von Solms R. Cybersecurity and information security — what goes where? // Information and Computer Security. 2018. Vol. 26. N 1. P. 2–9.
52. Wang Z., Zhu H., Sun L. Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods // IEEE Access. 2021. Vol. 9. P. 11895–11910.
53. Wang Z., Zhu H., Liu P. et al. Social engineering in cybersecurity: a domain ontology and knowledge graph application examples // Cybersecur. 2021. Vol. 4. N 31.
54. Wiafe I., Koranteng F. N., Wiafe A., Obeng E. N. at al. The role of norms in information security policy compliance // Information and Computer Security. 2020. Vol. 28. N 5. P. 743–761.
55. Winkler I. S., Dealy B. Information security technology? Don't rely on it a case study in social engineering // 5th USENIX Security Symposium. 1995.
56. Winkler Ira S. Non-technical threat to computing systems // Computing systems. 1996. Vol. 9. N 1. P. 3–14.
57. Ye Z., Guo Y., Ju A., Wei F. at al. A Risk Analysis Framework for Social Engineering Attack Based on User Profiling // Journal of Organizational and End User Computing (JOEUC). 2020. Vol. 32. N 3. P. 37–49.
58. Zhu Chen, Zhu Hengshu, Xiong Hui, Ma Chao at al. Person-Job Fit: Adapting the Right Talent for the Right Job with Joint Representation Learning // ACM Trans. Manage. Inf. Syst. November 2018. Vol. 9. N 3. Art. 12. 17 p. DOI: 10.1145/3234465

Об авторе:

Тулупьева Татьяна Валентиновна, доцент факультета государственного и муниципального управления Северо-Западного института управления РАНХиГС (Санкт-Петербург, Российская Федерация), кандидат психологических наук, доцент; tulupeva-tv@ranepa.ru

About the author:

Tatyana V. Tulupieva, Associate Professor of the Faculty of State and Municipal Management of North-West Institute of Management, Branch of RANEPA (St. Petersburg, Russian Federation), PhD in Psychology, Associate Professor; tulupeva-tv@ranepa.ru