ОРГАНИЗАЦИЯ ИНФОРМАЦИОННОЙ РАБОТЫ

УДК 004.056:316.776

Л.В. Астахова

Сотрудник организации как субъект управления её информационной безопасностью*

Выявлено противоречие между ростом количества инцидентов информационной безопасности организации по вине ее сотрудников и стабильной неэффективностью мер, предпринимаемых работодателем по их снижению. Сделан вывод о недостаточном внимании науки к современным тенденциям менеджмента организации (управления качеством, персоналом, знаниями, рисками), связанным с активизацией участия персонала в процессах управления. На примере обнаружения социоинженерных атак обоснована необходимость усиления роли пользователя информационной системы организации как субъекта управления её информационной безопасностью. Приведены организационные и программно-технические средства вовлечения пользователя в этот процесс.

Ключевые слова: *информационная безопасность, управление, организация, сотрудник, вовлеченность, социоинженерная атака, риски, человек как сенсор*

DOI: 10.36535/0548-0019-2020-05-2

Знание и интеллект все более становятся средством производства, и человек стремительно усиливает свои позиции в информационном пространстве общества. Однако он по-прежнему является «самым слабым звеном» любой системы информационной безопасности [1]. Эта проблема изучается много лет, но становится все более актуальной. Согласно аналитическим отчетам, в мире объем данных, скомпрометированных по вине внутреннего нарушителя в 2017 г., показал 10-кратный рост по сравнению с 2016 г. При этом на утечки, случившиеся в результате умышленных или непредумышленных действий внутренних нарушителей, приходилось 58% от их общего числа [2], а в России в 2018 г. эта цифра составила 77,9% [3]. Впервые с 2004 г. внутренние утечки показали более высокую «мощность», чем внешние: в результате одной внутренней утечки оказался скомпрометированным гораздо больший объем данных, чем в результате одной внешней [4].

Организации пытаются предотвращать угрозы со стороны человека. Сегодня мы постепенно преодолеваем стереотип об информационной безопасности (ИБ) как сугубо технической области деятельности. Стало очевидно, наконец, что даже самые новые, сильные технические средства защиты не могут гарантировать полной ИБ организации.

В международных и национальных стандартах серии ИСО/МЭК 27000 по управлению ИБ уделено определенное внимание безопасности, связанной с персоналом [5]. Для предотвращения деструктивных действий сотрудников в этих документах приводятся некоторые организационные меры на этапах их трудоустройства, занятости и увольнения, в том числе – требование повышения осведомленности сотрудников об информационной безопасности. Однако следует признать, что далеко не все организации выстраивают свои системы защиты информации согласно названным стандартам, поскольку последние носят рекомендательный характер. Организации, системы информационной безопасности которых проходят дорогостоящие процедуры сертификации на соответствие стандартам, все же не могут похвастаться снижением числа инцидентов по вине сотрудников. Логично полагать, что причиной тому выступает недостаточность, уязвимость декларируемых способов, методов и средств работы с персоналом, и требуется усиление его позиций в обеспечении ИБ, как и в других отраслях информационной экономики. Целый

* Статья выполнена при поддержке Правительства РФ (постановление от 16.03.2013 № 211, соглашение № 02. A03.21.0011).

ряд факторов требует пересмотра роли сотрудника организации в управлении её информационной безопасностью.

Во-первых, человек во все времена – это сложная система, объединяющая не только знания, но и личностные качества, исследование которых лежит в психологической плоскости. Поэтому одни лишь знания сотрудника, полученные в процессе повышения его осведомленности об ИБ, – это далеко не единственный фактор, способный предотвратить его деструктивное поведение в информационной среде организации.

Причины и обстоятельства дестабилизирующих информационных воздействий со стороны людей связаны с характером воздействий − преднамеренным или непреднамеренным. К причинам, вызывающим умышленное (преднамеренное) дестабилизирующее воздействие, относят: стремление получить материальную выгоду; отомстить руководству или коллеге по работе, а иногда и государству; оказать бескорыстную услугу приятелю из конкурирующей фирмы; продвинуться по службе; показать свою значимость. Обстоятельствами (предпосылками), способствующими появлению этих причин, могут быть: тяжелое материальное положение, финансовые затруднения; корыстолюбие, алчность; склонность к развлечениям, пьянству, наркотикам; зависть, обида; недовольство государственным строем, политическое или научное инакомыслие; личные связи с представителями конкурента; недовольство служебным положением, карьеризм; трусость, страх; тщеславие, самомнение, завышенная самооценка, хвастовство. Причинами непредумышленного (непреднамеренного) дестабилизирующего воздействия на информацию со стороны людей могут быть: неквалифицированное выполнение операций; халатность, безответственность, недисциплинированность, недобросовестное отношение к выполняемой работе; небрежность, неосторожность, неаккуратность; физическое недомогание. К обстоятельствам (предпосылкам) появления этих причин можно отнести: низкий уровень профессиональной подготовки; излишнюю болтливость, привычку делиться опытом, давать советы; незаинтересованность в работе, отсутствие стимулов для ее совершенствования; разочарованность в своих возможностях и способностях; перезагруженность работой, срочность ее выполнения, нарушение режима работы; плохое отношение со стороны администрации [6]. Зарубежные исследования показывают, что процесс принятия управленческих решений в области ИБ зависит от различных организационных и психологических факторов [7]. Поэтому все изложенные причины и обстоятельства деструктивных воздействий работников на информационную сферу организации должны быть в фокусе внимания руководителя по ИБ.

Во-вторых, человек сегодня, в обществе знания – это специфический объект управления. Особенности культуры этого общества заключены в расширении возможностей самореализации и саморазвития человека, в углублении интеллектуализации его профессиональной деятельности, в усилении его роли в управленческих процессах. В XXI веке долгосрочными трендами менеджмента и управления персоналом называют следующие: готовность сотрудников привносить свою инициативу, изобретательность, увлечённость; открытость, гибкость, сотрудничество, ориентация управления на заслуги сотрудника, а не на звания [8]; принятие научно-обоснованных решений на основе анализа полной и доброкачественной информации, собранной и обработанной с помощью современных методов; отказ от авторитарного стиля руководства и переход к лидерству (способности руководить не силой административного права, а авторитетом знаний, умений и человечности – вместо управления по целям или по результатам систем аттестации и ранжирования персонала, количественных норм и заданий, массового контроля качества продукции); как можно более глубокое и полное делегирование полномочий на всех уровнях управления, сопровождаемое соответствующим наделением ответственностью; постоянное обучение всех, везде и всегда; работа компании по принципу “мы все вместе делаем одно дело”; признание почти полной ответственности менеджеров за работу системы [9]; ориентация на человека, персонализация (от стандартизации – к индивидуальным потребностям, желаниям и возможностям кандидатов и сотрудников организации); повышение уровня доброты и доверия на рабочем месте к подчиненным, руководителям, коллегам; выявление и развитие талантливых сотрудников; обратная связь с сотрудниками; переход от аналитики людей (контроля) к аналитике для людей; микрообучение в процессе работы; использование блокчейна в работе с персоналом и др. [10]; переход от классической модели компании к модели «освобожденной» компании (она предполагает, что все работники могут предлагать решения и проекты для всей компании, свободны и ответственны за все действия, которые, по их мнению, будут необходимыми и лучшими для развития их организации) [11]; Agile-подход, который «возвращает ценность человеческого и профессионального общения, дает ощущение того, что человек влияет на то, что происходит с ним и вокруг него, повышает ощущение определенности и последовательности происходящего и помогает поддерживать баланс во взаимодействии людей и организаций»[12].

Особо пристальное внимание уделяется вовлечению сотрудников в работу организации – их готовности целиком вкладывать когнитивную, эмоциональную и физическую энергию [13–15].

В-третьих, усиление позиций сотрудников в системе ИБ организации диктуется принципами менеджмента качества. В разделе 3. «Взаимодействие работников» ГОСТ Р ИСО 9000-2015 Системы менеджмента качества. Основные положения и словарь [16], идентичного международному стандарту ISO 9000:2015 "Quality management systems – Fundamentals and vocabulary", указывается: «Для организации крайне важно, чтобы все работники были компетентными, наделены полномочиями и вовлечены в создание ценности. Компетентные, наделенные полномочиями и взаимодействующие работники на всех уровнях организации повышают ее способность создавать ценность. Поэтому для того чтобы эффективно и результативно управлять организацией, очень важно уважать

и вовлекать всех работников на всех уровнях организации». Следовательно, управленческая деятельность в области информационной безопасности, если она нацелена на снижение деструктивных инцидентов, должна развиваться в русле названных общих тенденций управления персоналом. Для этого необходимо обеспечивать более тесное взаимодействие работников и руководства организации. Как и в сфере менеджмента качества, для практической реализации этого принципа в сфере информационной безопасности требуется: углубление понимания работниками целей организации в области информационной безопасности; усиление мотивации по достижению этих целей; повышение вовлеченности работников в обеспечение информационной безопасности; усиление личностного развития, проявления инициативы и креативности; повышение удовлетворенности работников; развитие доверия и сотрудничества во всей организации; повышение внимания к общим ценностям и культуре во всей организации.

В-четвертых, вовлечение сотрудников в управление ИБ обусловлено современным трендом управления знаниями в организации. В основе трансформационной модели SECI (SECI model of knowledge dimensions) И. Нонака и Х. Такеучи лежат различные способы трансформации знаний (спирали знаний): социализация, экстернализация, комбинирование, интернализация. В частности, экстернализация (*externalization*) предполагает преобразование неявных знаний в явные, извлечение смыслов и их передачу другим субъектам [17]. Проблема, обсуждаемая в настоящей статье, находится в русле этого процесса: пользователь корпоративной информационной системы должен быть способен трансформировать неявное знание об угрозах информационной безопасности в явное и передавать его лицам, принимающим управленческие решения.

В-пятых, усиление субъектных позиций сотрудников организации в системе защиты информации соответствует концепциям духовного развития человека в обществе знания. Самореализация и личностное развитие человека невозможны сегодня без интеграции информационно-потребительской (чувственное восприятие, рациональное познание и оценка потребляемых текстов и других носителей информации), информационно-репродуктивной (воспроизведение, передача информации) и информационно-созидательной (создание нового знания) составляющих [18]. Поэтому требование участия человека во всех видах информационной деятельности является аргументом в пользу сотрудника как субъекта управленческой деятельности организации по ИБ.

В шестых, участие человека в управлении информационной безопасностью необходимо и с позиций теории управления рисками. Один из лучших способов решения проблем информационной безопасности в корпоративном мире основан на оценке риска [19]. При этом еще в 1950-х гг. теоретики заявили, что риск не может быть определен за пределами человеческого восприятия [20]. К сожалению, сегодня наиболее распространенным методом оценки рисков ИБ является их экспертная оценка исключительно директором или специалистом по защите информации, пользователи информационной системы организации к этой работе не допускаются.

На практике директор по информационной безопасности (в западных странах – Chief Information Security Officer – CISO) традиционно рассматривает сотрудников как угрозу, поэтому занимает авторитарную позицию, пытаясь реализовать свои должностные функции. Поэтому он, как правило, использует одностороннюю модель связи с конечным пользователем информации без обратной связи с ним [21]. Однако сегодня становится ясно, что этот подход может хорошо работать только в жестких организационных иерархиях (особенно в вооруженных силах и полиции), и ему противоречит рост более открытых организационных структур. Автократизм препятствует эффективной информационной безопасности.

Возможности сотрудника в управлении ИБ организации проиллюстрируем на примере защиты от социоинженерных атак. К ним относятся атаки разной направленности воздействий: прямые (осуществляемые через физический, зрительный, аудиальный контакт, присутствие злоумышленника в рабочей зоне жертвы для выполнения атаки) и косвенные (запущенные удаленно с помощью вредоносного программного обеспечения, передаваемого через вложения электронной почты или СМС сообщения). Примеры прямых атак: физический доступ, «серфинг на плечах», дайвинг, телефон и др.; примеры косвенных атак: фишинг, фальшивое программное обеспечение, всплывающие окна, вымогатели, *SMSishing*, онлайн социальная инженерия и обратная социальная инженерия [22].

В последние годы конечные пользователи признаны самым слабым звеном в цепи безопасности, и теперь защита информации в значительной степени зависит от убеждения сотрудников в необходимости вести себя безопасно. Уже начинает складываться стереотип, что работник будет поступать правильно и заботиться о защите информации, если он осведомлен о проблемах организации. Однако этого не всегда достаточно. Так, в Нидерландах в результате эмпирического исследования была показана неэффективность двух методов, направленных на защиту пользователей от атак социальной инженерии: повышение осведомленности об опасностях социальных и кибератак и предостережение от раскрытия личной информации. У участников эксперимента запрашивался адрес электронной почты, 9 цифр из их 18-значного номера банковского счета, а также перечень покупок в интернет-магазине. В результате были получены относительно высокие показатели раскрытия информации: 79,1% участников заполнили свой адрес электронной почты, а 43,5% предоставили информацию о банковском счете. Среди онлайн-покупателей 89,8% респондентов указали тип продукта, который они приобрели, а 91,4% – название интернет-магазина, в котором они совершили эти покупки [23].

В последнее время появились инструментальные средства защиты от социоинженерных атак. Самые популярные сегодня – это автоматические сканеры уязвимостей социальной инженерии, которые могут быть использованы для тестирования устойчивости организации к потенциальным атакам социальной

инженерии, возникающим в результате использования открытых источников [24, 25]. Многие зарубежные компании проводят симулированные фишинговые атаки, имея четко определенные цели снижения имитируемых фишинговых кликов ниже 5–10% [26]. Аналитические задачи решаются в процессе разработки и внедрения программных комплексов анализа защищённости пользователей компьютерных сетей от социоинженерных атак [27], а также программных продуктов, моделирующих злоумышленника и профиль его компетенций для оценки защищенности информационной системы от социоинженерных атак, выявления ее наиболее уязвимых звеньев [28] и др. Однако во всех этих продуктах сотрудник попрежнему остается пассивным объектом, что не меняет сути его взаимоотношений с руководством в процессе управления ИБ организации.

Кроме того, на фоне динамики технологических достижений, следует указать на негативные психологические последствия излишнего контроля за сотрудниками организации (в том числе в форме пентестирования): стрессы, озлобленность, утрата доверия к руководству и другие причины и обстоятельства, которые могут привести не к ожидаемому снижению, а, напротив, – к повышению их уязвимости в системе защиты информации [29]. Особенно это относится к лояльным сотрудникам, которые могут стать источниками угроз ИБ не умышленно, а из-за неосведомленности или невнимательности. Тестирование таких сотрудников на устойчивость к социоинженерным атакам может вызвать у них обратную реакцию [30].

Таким образом, становится очевидным, что для достижения эффективности управленческих усилий по обеспечению ИБ требуются альтернативные методы, основанные на более активных, доверительных (а потому – позитивных) двусторонних связях руководителя с сотрудниками. Упор должен делаться на делегирование и расширение прав и возможностей последних. Мы согласны с экспертами [31] в том, что сотрудники могут быть уполномочены брать на себя ответственность за информационную безопасность организации. Люди часто способны выявлять проблемы и решать их так, как не могут даже самые передовые технологии. Когда брандмауэры, системы предотвращения вторжений и другие средства защиты выходят из строя, люди становятся последней линией защиты. Но это работает только в том случае, если обеспечить им необходимую подготовку и поддержку, а также управление со стороны высших руководителей [26].

Если раньше приходилось нанимать лучших математиков, взломщиков кодов и секретных агентов для отчета о безопасности организации, то сегодня обработка, анализ и более доступная информация стали значительно более эффективными. Вскоре машинное обучение, программная робототехника, автоматизация процессов и центры слияния станут средствами, способными революционизировать сбор информации для отделов безопасности организаций. Прогресс, который мы наблюдали предыдущие 30 лет, теперь будет происходить шагом в 5 лет [32].

Полагаем, что в ближайшее время одним из таких новых источников информации и технологий ее обработки станет сотрудник организации. Одним из перспективных методов реализации человеческого потенциала в сфере управления ИБ, по нашему мнению, может быть вовлечение сотрудника в обнаружение кибератак на основе развиваемой сегодня в зарубежной науке и практике концепции, что человек есть датчик (сенсор) безопасности (The Human-as-a-Security-Sensor paradigm). За последние несколько лет эта концепция находит все большее применение для выявления угроз и неблагоприятных условий в физическом пространстве: аварийных ситуаций [33], шума и загрязнения окружающей среды [34], мониторинга наличия воды [35]. Успехи в физическом пространстве послужили мотивацией для применения и оценки концепции обнаружения угроз в киберпространстве. Особенно это актуально для раскрытия семантических социально-инженерных атак, где технические механизмы безопасности изначально ограничены в объеме и точности. Так, авторы [36] разработали приложение, предназначенное для того, чтобы пользователи могли активно обнаруживать такие атаки и сообщать о них.

Изложенное позволяет утверждать, что для эффективного управления ИБ организации необходимо учреждение правового статуса сотрудника как субъекта обнаружения социоинженерных атак. В организации должна быть создана стабильная система взаимодействия сотрудников и руководителей, основанного на формализованных, документированных правилах, нормах, статусах и ролях, которые способны обеспечить снижение человеческих угроз ИБ. При этом новая информационно-функциональная роль сотрудника должна быть подкреплена системой морального или материального вознаграждения. Это будет способствовать укреплению доверия между руководством и работником, усилению мотивации работника по достижению целей ИБ, личностному развитию, повышению его инициативности и креативности. В итоге максимально вероятно достижение целей не только работодателя (обеспечение ИБ), но и работников (удовлетворенность работой, самореализация и саморазвитие).

Обоснованная трансформация ролей пользователей информационных систем организации способна привести к активизации факторов повышения уровня культуры информационной безопасности организации и ее работников: их осведомленности, формированию ценностей, ответственности и лояльности; взаимного доверия и гармонизации потребностей работодателя и работников и др. Так, в процессе правового учреждения управленческой функции сотрудника он получает знания об опасности различных типов и видов кибератак, о технологиях реализации и защиты от их деструктивного воздействия. Самостоятельная обработка фишинговых писем, пришедших на персональный ящик электронной почты сотрудника, усиливает осознание им опасности рисков ИБ и повышает его ответственность в этой области. Это подтверждают постулаты психологии рисков, согласно которым персонифицированные риски считаются более опасными, чем анонимные [37]. Как правило, человек больше боится опасности, которая затрагивает его лично и поэтому более внимательно

относится к ней и предпринимает больше усилий для её устранения, чем опасности, которая угрожает другим [38]. Уверенности в информационной безопасности придаёт сотруднику реальная возможность управления рисками (контроля над ними, реализации технологий их обработки), ведь большинство людей меньше опасаются рисков, над которыми они чувствуют некоторый контроль, и больше опасаются рисков, которые они не контролируют [37].

Усиление роли сотрудника в управлении информационной безопасностью особенно актуально для небольших организаций, не имеющих достаточных ресурсов на приобретение дорогостоящих средств защиты информации. Для такого типа организаций мы разработали специальное программное приложение HUMAN FIREWALL, которое нацелено на техническое обеспечение процесса обнаружения человеком социоинженерной атаки, её классифицирование (отнесение к определенному типу атак), цифровую передачу информации о ней в отдел информационной безопасности, получение и обработку обратной связи.

* * *

На фоне возрастания роли человека в обществе информации и знания слишком много организаций все еще верят в технологические решения проблем обеспечения информационной безопасности. И это несмотря на то, что отчет за отчетом, нарушение за нарушением показывают, что злоумышленники больше внимания уделяют конечным пользователям. Поэтому актуальная задача работодателей сегодня – оценить важность сотрудника в управлении ИБ. Именно человек может быть последней линией защиты и предохранить организацию от атак в случае отказа всех других технологий.

Потребность наделения сотрудника организации полномочиями обнаружения кибератак и оперативного оповещения о них руководства обусловлена достижениями таких разных отраслей науки и практики, как управление информационной безопасностью, менеджмент качества, управление персоналом, управление знаниями, психология рисков, информационно-психологическая теория информационной деятельности. Сотрудник должен быть не только объектом управления, но и его активным субъектом, вовлеченным в процесс управления ИБ и организационного сотрудничества, не только потреблять знание об ИБ и репродуцировать его на практике, но и создавать новое знание об угрозах ИБ организации, уметь трансформировать неявное знание об угрозах ИБ в явное, выступать в роли первичного преобразователя и отправителя информации для принятия управленческих решений в области ИБ.

В управлении информационной безопасностью сотрудник организации имеет широкие возможности как датчик социоинженерных атак. Существующие инструментальные средства часто способствуют предотвращению угроз ИБ, связанных с социоинженерными атаками. Однако на практике требуется разработка программных продуктов, которые могли бы реализовать человеческий потенциал для обнаружения этих атак, информирования о них руководства и обработки рисков ИБ на основе обратной связи.

Участие конечных пользователей в обнаружении кибератак повышает общий уровень их культуры информационной безопасности. Если люди достаточно умны, чтобы защищать себя на работе, то они охраняют себя и дома, делятся знаниями с членами семьи и знакомыми, и тогда мы действительно добиваемся хорошего прогресса в развитии культуры ИБ. Персональное участие сотрудника организации в управлении ИБ повышает его ответственность, уверенность в причастности к решению серьезных корпоративных задач. Реализация сотрудником функции обнаружения социоинженерных атак способствует не только оперативному реагированию на угрозы ИБ организации, но и гармонизации взаимодействия работодателя и работника, усилению организационной мотивации и лояльности, самореализации и саморазвитию.

Активизация роли человека в управлении информационными процессами организации и реализация этой усиливающейся тенденции в сфере ИБ становятся возможными благодаря цифровой трансформации общества в глобальном масштабе, в том числе – развитию цифровых компетенций человека. Это – ключевая особенность современной, цифровой культуры. Поэтому проблемы, поставленные в настоящей статье, имеют широкие перспективы исследования. К ним мы относим изучение различных стратегий вовлечения сотрудников в управление ИБ и оценку уровня их вовлеченности в рамках каждой из стратегий. В настоящее время существуют разные стратегии вовлечения сотрудников и более десяти шкал, которые были разработаны для их измерения [13]. Однако в сфере информационной безопасности эти стратегии и метрики имеют специфические особенности, требующие специального изучения.

В ближайшем будущем предметом научного анализа должно стать использование блокчейн-технологий и технологий машинного обучения в процессе обработки пользовательской информации о кибератаках разных видов.

СПИСОК ЛИТЕРАТУРЫ

1. Caldwell T. Training – the weakest link // Computer Fraud & Security. – 2012. – Vol. 2012, Issue 9. – P. 8-14.
2. Исследование утечек конфиденциальных данных коммерческих компаний и государственных организаций, произошедшие по вине или неосторожности внутреннего нарушителя. Сравнительное исследование. 2013-2017 гг. – URL: https://www.infowatch.ru/resources/analytics/reports/15194 © InfoWatch (дата обращения – 17.12.2019).
3. Утечки данных. Россия. 2018 год – URL: https://www.infowatch.ru/resources/analytics/reports/russia2018 © InfoWatch (дата обращения: 17.12.2019).
4. PriceWaterhouseCoopers. The Global State of Information Security® Survey 2018. – URL: https://www.pwc.com/us/en/services/consulting/

cybersecurity/library/information-security-survey.html (дата обращения – 17.12.2019).
5. Астахова Л.В. Проблемы культуры информационной безопасности в условиях цифровой экономики // Научно-техническая информация. Сер. 1. – 2020. – №2. – С. 28-37.
6. Алексенцев А.И. Понятие и структура угроз защищаемой информации // Безопасность информационных технологий. – 2000. – № 3. – С. 10–17.
7. Dor D., Elovici Y. A model of the information security investment decision-making process // Computers & Security. – 2016. – Vol.63. – P.1-13.
8. Хэмел Г. Менеджмент XXI века: Новые открытия. Перевод на русский язык: Наталья Коношенко // Электронная публикация: Центр гуманитарных технологий. – URL: https://gtmarket.ru/library/articles/4246 (дата обращения: 17.12.2019).
9. Менеджмент 21 века – краткий обзор основных тенденций. – URL: https://mirznanii.com/a/165547-4/menedzhment-21-veka-kratkiy-obzor-osnovnykh-tendentsiy-4 (дата обращения: 17.12.2019).
10. Haak T. 12 HR Trends for 2020. – URL: https://hrtrendinstitute.com/2019/11/26/12-hr-trends-for-2020/ (дата обращения: 17.12.2019).
11. Костенко Е.П. Современные тренды в управлении персоналом: отечественный и зарубежный опыт // Journal of Economic Regulation. – 2018. – Т. 9, № 4. – С. 107-123.
12. Чухно Ю. Управление изменениями в VUCA-мире: как вовлечь людей и помочь им стать лидерами новых решений. – URL: http://novaterra-coaching.su/change- management-in-vuca (дата обращения – 17.12.2019).
13. Saks A.M. Translating Employee Engagement Research into Practice // Organizational Dynamics. – 2017. – Vol.46, Iss. 2. – P.76-86.
14. Employee engagement and motivation. Understand the concept of employee engagement and learn how to build an engaged and motivated workforce / Chartered Institute of Personnel and Development. – 2018. – URL: https://www.cipd.co.uk/ (дата обращения – 17.12.2019).
15. Веретковская О.В. Вовлеченность персонала организации как актуальная задача современных компаний // Экономика и бизнес: теория и практика. – 2019. – № 4-2. – С. 40-43.
16. ГОСТ Р ИСО 9000-2015 Системы менеджмента качества. Основные положения и словарь (с Поправкой). Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 28 сентября 2015 г. № 1390-ст. – URL: http://docs.cntd.ru/document/1200124393 (дата обращения: 17.12.2019).
17. Нонака И., Такеучи Х. Компания – создатель знания. Зарождение и развитие инноваций в японских фирмах. – М.: Олимп-Бизнес, 2003. – 320 с.
18. Астахова Л.В. Информационно-психологическая теория духовного развития личности в эпоху цифровой культуры. К 95-летию со дня рождения Ю.С. Зубова // Научно-техническая информация. Сер. 1. – 2019. – № 5. – С. 1-7.
19. Shameli-Sendi A., Aghababaei-Barzegar R., Cheriet M. Taxonomy of information security risk assessment (ISRA) // Computers & Security. – 2016. – Vol. 57. – P.14-30.
20. Munteanu A.-B., Fotache D. Enablers of Information Security Culture // Procedia Economics and Finance. – 2015. – Vol.20. – P. 414-422.
21. Albrechtsen E. A qualitative study of users' view on information security // Computers & Security. – 2007. – Vol. 26, Iss. 4. – P.276-289.
22. 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: 17.12.2019).
23. 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.
24. 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.
25. Faircloth J. Chapter 8: Client-side attacks and social engineering // Penetration Tester's Open Source Toolkit (Fourth Edition). – 2017. – P.273-318.
26. Mansfield-Devine S. Raising awareness: people are your last line of defence // Computer Fraud & Security. – 2017. – Vol. 2017, Issue 11. – P. 10-14.
27. Абрамов М.В. Автоматизация анализа социальных сетей для оценивания защищённости от социоинженерных атак // Автоматизация процессов управления. – 2018. – № 1(51). – С. 34-40.
28. Абрамов М.В., Азаров А.А., Тулупьева Т.В., Тулупьев А.Л. Модель профиля компетенций злоумышленника в задаче анализа защищённости персонала информационных систем от социоинженерных атак // Информационно-управляющие системы. – 2016. – № 4(83). – С.77-84.
29. Астахова Л.В. Онтологический статус доверия в информационной безопасности // Научно-техническая информация. Сер. 1. – 2016. – № 3. – С. 1-9; Astakhova L.V. The ontological status of trust in information security // Scientific and Technical Information Processing. – 2016. – Vol. 43, № 1. – С. 58-65.
30. Hatfield J.M. Virtuous human hacking: The ethics of social engineering in penetration-testing // Computers & Security. – 2019. – Vol. 83. – P.354-366.
31. Ashenden D., Sasse A. CISOs and organisational culture: Their own worst enemy? // Computers & Security. – 2013. – Vol. 39, Part B. – P. 396-405.
32. Allen M. Chapter 1: Corporate security today // The Chief Security Officer's Handbook. – 2019. – P. 1-18.
33. Avvenuti M., Cimino M.G., Cresci S., Marchetti A., Tesconi M. A framework for detecting unfolding emergencies using humans as sensors // SpringerPlus. – 2016. – Vol. 5(1). – P.1-23.
34. Zheng Y., Liu T., Wang Y., Zhu Y., Liu Y. Chang E. Diagnosing new york city's noises with

ubiquitous data // ACM International Joint Conference on Pervasive and Ubiquitous Computing. – 2014. – P.715-725.
35. Jurrens E.H., Broring A., Jirkai S. A human sensor web for water availability monitoring // OneSpace 2009 - 2nd International Workshop on Blending Physical and Digital Spaces on the Internet, Berlin, Germany. – URL: https://www.researchgate.net/ publication/228886237 (дата обращения: 17.12.2019).
36. 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.
37. Schneier B. The Psychology of Security. – URL: https://www.schneier.com/academic/paperfiles/paper-psychology-of-security.pdf (дата обращения: 17.12.2019).
38. Ropeik D., Gray G. M. Risk: A Practical Guide for Deciding What's Really Safe and What's Really Dangerous in the World Around You. – Boston, New York: Houghton Mifflin Harcourt, 2002. – 485 p.

Материал поступил в редакцию 17.12.19.

Сведения об авторе

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