ОРГАНИЗАЦИЯ ИНФОРМАЦИОННОЙ РАБОТЫ

УДК 005.32:331.101.3

Л.В. Астахова

Модель нулевого доверия как фактор влияния на информационное поведение сотрудников организации*

Охарактеризована устойчивая тенденция к использованию концепции и модели нулевого доверия (zero trust) в мировой практике обеспечения информационной безопасности, выявлены проблемы ее реализации пользователями информационных систем. Обосновано негативное влияние этого подхода на информационное поведение сотрудников организации. Показана необходимость совершенствования модели нулевого доверия для устранения и предупреждения инцидентов угрозы информационной безопасности по вине пользователей и возможность использования в этих целях эвристического потенциала теории культуры информационной безопасности, теории доверия и теории самодетерминации.

Ключевые слова: *нулевое доверие, «zero trust», информационная безопасность, повышение осведомленности, культура информационной безопасности, теория самодетерминации, культура доверия, сотрудник, организация*

DOI: 10.36535/0548-0019-2022-03-2

ВВЕДЕНИЕ

Количество* инцидентов угрозы информационной безопасности (ИБ) в мире продолжает расти. В 2020 г. специалисты Экспертно-аналитического центра компании InfoWatch зафиксировали 2395 утечек данных из коммерческих и некоммерческих (государственных, муниципальных) организаций в различных странах мира (что на 5,8% превышает показатели 2018 г.), а также рост количества умышленных утечек [1]. Инсайдеры – самые частые виновники инцидентов. По оценкам компании SearthInform, в первом полугодии 2020 г. как минимум 60% утечек данных в России произошло по причине намеренных действий сотрудников организаций, которые имели к ним доступ [2]; ежемесячно каждая организация выявляла не менее 25 инцидентов по вине сотрудников и столкнулась с попытками слива информации [3]. Стабильно не снижающиеся цифры подобных инцидентов заставляют теоретиков и практиков в области ИБ искать новые концепции, подходы и модели их устранения.

Все большее внимание привлекает модель «нулевого доверия» (*zero trust*), призванная удовлетворять новые сложные требования сетевой безопасности организаций. Эта модель, разработанная в 2010 г. Дж. Киндервагом [4], стала наиболее популярной в сфере кибербезопасности как в России, так и за рубежом. Ее суть заключается в полном отсутствии доверия кому-либо – даже пользователям информационных систем организации. Подразумевается, что любой пользователь или устройство должны подтверждать свои данные каждый раз, когда они запрашивают доступ к какому-либо ресурсу внутри или за пределами сети. К основным принципам нулевого доверия авторы [5] относят: причисление всех источников данных и вычислительных услуг к организационным ресурсам; запрет на автоматическое предоставление доверия по умолчанию; доступ к ресурсам только на один сеанс; определение доступа исходя из характеристик устройства, поведенческих атрибутов; применение наименьших привилегий; постоянное обновление и оценку доступа; сбор и использование информации об активах, сетевой инфраструктуре и сообщений для улучшения безопасности. Несмотря на актуальность и широкое распространение этой модели и учитывая статистику роста инцидентов угрозы ИБ по вине внутренних пользователей, можно выразить сомнение в ее результативности. Этим обусловлена актуальность и цель настоящей статьи –

* Статья подготовлена при поддержке Правительства РФ (Постановление № 211 от 16.03.2013 г.), соглашение № 02. А03.21.0011.

выявить проблемные векторы влияния нулевого доверия на информационное поведение сотрудников организации и обосновать пути их коррекции.

ПОЛЬЗОВАТЕЛЬ ИНФОРМАЦИОННОЙ СИСТЕМЫ В МОДЕЛИ НУЛЕВОГО ДОВЕРИЯ КАК ОБЪЕКТ ИЗУЧЕНИЯ

Результаты исследований показывают, что в академической литературе основное внимание уделяется архитектуре ИБ и повышению её производительности при нулевом доверии, а в практической литературе – организационным преимуществам модели нулевого доверия и потенциальным стратегиям её развития. Однако и научные круги, и практики до сих пор игнорируют исследования пользователей в контексте *zero trust* [6]. При этом встречаются публикации, в которых декларируется роль пользователей как одного из наиболее слабых звеньев концепции угрозы безопасности и необходимость ограничить и контролировать их доступ к ресурсам внутри и вне компании [7]. Эксперты констатируют факт невнимания к пользователям в ходе внедрения модели «нулевого доверия», указывают, что возможные проблемы могут привести к их недовольству [8], и рекомендуют проводить предварительную загрузку и автоматическое обновление настроек, предоставлять краткие объяснения причин отказа в доступе. А для того, чтобы минимизировать разочарование пользователей с самого начала, призывают предвидеть потенциальные конфликты и проблемы и принимать меры реагирования [9]. На вопросы влияния нулевого доверия на взаимодействие человека и компьютера, человека и внешнего мира эксперты ответов не находят. Неясными остаются и возможности атак изнутри сети с нулевым доверием [10]. Как ни парадоксально, в процессе разработки этой новой модели специалисты-практики не обращаются к пользователям как к ее ключевому элементу, чтобы максимально учесть их потребности. В результате спустя десять лет по-прежнему существуют человеческие риски, которые несет построение в компании такой системы безопасности [11]. И в первую очередь к ним относят уклонение персонала от норм ограниченного доступа к данным и возникновение организационно-коммуникационных трудностей, связанных с ограничением доступа пользователей к информации.

Если иметь в виду человека, то мы не можем не рассматривать эту проблему в гуманитарной плоскости. Очевидно, что названные риски возникают не только по причине низкой осведомленности об ИБ сотрудников организации, но и из-за негативного влияния нулевого доверия на психологическую сферу личности сотрудника, на его информационное поведение.

Мы выделяем два вектора влияния нулевого доверия на пользователя информационной системы организации – позитивный и негативный.

Позитивное влияние модели нулевого доверия выражается в активном развитии практики повышения осведомленности сотрудников организации в области ИБ, необходимость которой ещё в начале XXI в. приходилось доказывать как проявление гуманитарной сущности деятельности по обеспечению ИБ [12]. Сегодня эта практика закреплена в международных и национальных стандартах по управлению информационной безопасностью, в нормативных правовых документах по защите персональных данных, критической информационной инфраструктуры и др. И это, безусловно, позитивный факт. Куда более сложен негативный вектор влияния нулевого доверия на информационное поведение сотрудников. Он связан со снижением доверия пользователей к руководству и внутренней мотивации к выполнению правил ИБ организации.

Снижение доверия пользователей к работодателю. Контроль со стороны руководства (нулевое доверие) часто воспринимается пользователями информационной системы как недоверие. Гипертрофированный контроль и надзор, поведенческий мониторинг с помощью систем видеонаблюдения и DLP-систем (Data Leakage Prevention – предотвращение утечки данных) на рабочих местах могут порождать ответное недоверие (нулевое доверие), злобу и цинизм сотрудников, дегармонизировать взаимодействие в организации, приводить как к утечке инсайдерской информации, так и к активизации текучести кадров. При внедрении модели нулевого доверия авторы обращают внимание на проблему, которая заключается в том, что сотрудники могут чувствовать себя проверяемыми и контролируемыми [13]. Беспокойство экспертов вызывают постоянный мониторинг и проверка трафика, проблемы с конфиденциальностью данных сотрудников [14], связанные с правовыми нормами.

В своих публикациях мы уже уделяли внимание проблеме доверия в информационной безопасности [15, 16]. Анализ этой проблемы дает ключ и к решению негативного восприятия модели нулевого доверия в организации. Доверие – это информационно-измерительный механизм управления (планирования, реализации, контроля и мотивации) безопасным взаимодействием субъектов информационных отношений, направленным на их устойчивое функционирование и развитие. Поэтому контроль и мотивация пользователя – это важнейшие элементы, от сбалансированности которых зависит результативность любой модели информационной безопасности, в том числе – нулевого доверия.

Обосновав онтологический статус доверия в ИБ, требование баланса недоверия (контроля) и доверия, мы пришли к необходимости развития культуры доверия в информационной безопасности. Это - «способ организации человеческой деятельности, при котором субъекты информационных отношений способны управлять своими информационными взаимодействиями, направленными на их устойчивое функционирование и развитие в условиях информационных рисков, *посредством взаимного субъективного авансирования веры в ценности культуры и объективных действий по их передаче*» [15]. Взаимность авансирования веры в ценности культуры не требует исключительного доверия или недоверия друг к другу. Работодатель и сотрудник как субъекты информационных отношений должны стремиться к культуре доверия, основанной на балансе взаимного доверия и недоверия (выраженного в контроле в разумных пределах).

Культура доверия как феномен, определяющий потребность сотрудника в адекватном информационном поведении в организации, не может формироваться в рамках повышения осведомленности об ИБ. Нормативные документы и практика отличаются сугубо прагматической направленностью, отсутствием мотивационно-рефлексивных, мировоззренческих аспектов, на что мы не раз обращали внимание [17]. В последние годы в развитых странах мира осознается ограниченность столь прагматичного подхода, поэтому резко увеличился поток публикаций по культуре информационной безопасности, развивается её социальная практика в самых разных отраслях деятельности. Культура доверия является органичной частью развития культуры информационной безопасности – следующего этапа после повышения осведомленности об ИБ. Это следует учитывать при разработке моделей нулевого доверия в организациях.

Снижение внутренней мотивации работников к информационно-безопасному поведению в организации. В процессе внедрения модели нулевого доверия с ее жестким инструктивным характером снижается и мотивация пользователей. Это можно объяснить с позиции теории самодетерминации (ТСД), авторами которой являются американские психологи Эдвард Л. Деси и Ричард М. Райан [18]. Теория самодетерминации (*self-determination theory* – SDT) – психологический подход к пониманию человеческой мотивации, личности и психологического благополучия человека. В последние два десятилетия наблюдается всплеск активности в исследовании и применении этой теории в различных областях деятельности, функционирует специальная организация для ее продвижения [19]. Теория подчеркивает важность трех основных психологических потребностей человека – автономии, взаимосвязи и компетентности.

Уникальность теории самодетерминации заключается в её акценте на автономии. Способность индивида к автономии рассматривается как самодетерминация. Многие ошибочно путают автономию с независимостью, самостоятельностью и индивидуализмом, но в ТСД автономия – это чувство воли по отношению к своим действиям [20]. Согласно концепциям жизненных целей и причинных ориентаций, автономия способствуют развитию внутренней мотивации, и именно автономная (а не контролируемая) ориентация позитивно соотносится с психологическим здоровьем и эффективным поведением человека. Преобладание внутренней мотивации над внешними целями приводит к большей результативности деятельности человека [21]. Авторы ТСД [22] подчеркивают, что автономные люди могут рефлексивно оценивать свои действия, одобрять те из них, которые соответствуют их ценностям и потребностям, и при этом активно развивать действительность, достойную того, чтобы в ней жить и работать.

Это имеет прямое отношение к информационному поведению сотрудников организации в контексте обеспечения информационной безопасности. Инструктивно-исполнительский характер информационной деятельности сотрудника, чрезмерный контроль со стороны руководства формируют и развивают контролируемую (или безличную) причинную ориентацию сотрудника, что существенно снижает его мотивацию к выполнению правил ИБ и результативность работы.

Автономная ориентация пользователя информационной системы – это фактор влияния на культуру информационной безопасности. Мы обосновали много таких факторов [23], но результат эмпирического исследования с позиций теории самодетерминации показывает, что реципиенты воспринимают автономию как первостепенный фактор [24]. Многочисленные инструкции и правила ИБ, жесткий контроль и наказания за их невыполнение, демонстрирующие недоверие к сотруднику, – все это внешняя мотивация для работника. Культура же связана с внутренними потребностями. Именно с преобладанием внешней контролирующей причинной мотивации, а значит – с низким уровнем культуры ИБ, мы связываем большое число инцидентов угрозы информационной безопасности в организациях по вине сотрудников. В связи с этим работодателям следует стремиться к автономизации сотрудников.

Решение приведенных проблем зависит сегодня не только от работодателя. Цифровизация в глобальном масштабе вызвала серьезные социально-культурные трансформации, которые не могли не оказать влияния на человека как на субъекта информационных отношений. Потребность людей в справедливости, независимости и самостоятельности обострилась и ее реализация принимает все более угрожающие формы, так как ведет к исчезновению традиций законопослушания. Мы разделяем озабоченность А. Лукацкого – ведущего российского эксперта в области информационной безопасности – в том, что свобода как вседозволенность, транслируемая средствами массовой информации последние два десятилетия, негативно сказалась не только на молодежи, но и на всех поколениях. Люди становятся все более непослушными и дерзкими, запреты их раззадоривают, а не пугают или загоняют в рамки. Они не желают соблюдать любые нормы – в жизни, в работе, в том числе правила и инструкции, что приводит к реализации угроз информационной безопасности [25]. Разрушенная система воспитания молодежи, недоверие людей к субъектам власти, невнимание государства к вопросам культуры информационной безопасности, неработающие статьи Уголовного Кодекса – все это обеспечивает перманентный рост числа киберпреступлений и инцидентов угроз информационной безопасности в организациях по вине сотрудников и пока складывается в удручающую картину. Её вряд ли может улучшить внедрение концепции нулевого доверия в информационной безопасности в тех границах, в которых она сейчас разработана техническими специалистами.

Понимание причин осложнившихся проблем – это шаг на пути к их решению. Государству следует, наконец, обратиться к человеку как к пользователю информационных систем, как носителю цифровой культуры, разработать и принять комплексную национальную программу развития культуры информационной (цифровой) безопасности (или кибербезопасности) всех членов общества. К сожалению, разработанный в начале XXI в. проект документа «Основные направления государственной политики в области функцио-

нирования и развития культуры информационной безопасности» так и не был утвержден.

Что касается субъектов экономики, то они могут и должны стать моделью таких информационных отношений, которые основаны на стремлении работодателя к удовлетворению базовых человеческих потребностей работников в автономии в ее лучших традициях, исключающих недоверие, эгоизм и вседозволенность. И модель информационной безопасности, названная 10 лет назад «нулевым доверием», при условии ее совершенствования в обозначенных в настоящей статье направлениях, может стать рычагом изменений в информационно-коммуникационной сфере организации.

Мы разделяем оптимистичные надежды ученых на то, что в будущем будут проведены исследования путей более широкого использования теории социальной детерминации в повседневной практике, стратегическом развитии и социальной политике [26] и в том числе – в сфере информационной безопасности. Это требует междисциплинарных исследований механизмов реализации этой теории в совершенствовании модели нулевого доверия. В технологии ее реализации должны быть изначально заложены принципы гармоничной автономизации пользователей, развития их внутренней ценностной мотивации, расширения вовлеченности в процессы управления ИБ, достижения баланса доверия в информационных коммуникациях работодателя и работника. Полагаем, что не только содержание, но и само название концепции – модель нулевого доверия – нуждается в обновлении. С точки зрения психологии восприятия, сейчас ее название обладает негативной семантической окраской для сотрудников организации, хотя для работодателя – является символом надежности системы ИБ организации. Для гармонизации информационных отношений в организации целесообразно именовать её моделью «сбалансированного доверия».

Субъект реализации этой модели – специалист по защите информации – также нуждается в совершенствовании своих компетенций. Высшее образование способно решить эту задачу. Модель нулевого доверия как объект освоения студентами вуза нуждается в коррекции с точки зрения содержания и форм. Выпускники должны быть способны внедрить эту модель в практику не только на технологическом, но и на пользовательском уровне в любой организации, независимо от формы собственности и отраслевой принадлежности. В процессе обучения требуется и развитие личностной культуры информационной безопасности самих студентов, включая их культуру доверия, автономность и мотивацию к организационной вовлеченности. Только при этом условии они смогут организовать этот процесс на профессиональном уровне.

ВЫВОД

Модель нулевого доверия (*zero trust*), составной частью которой является жестко регламентированное управление доступом пользователей к информационным ресурсам, все шире внедряется в системы информационной безопасности организаций. Однако в настоящее время сложилась тенденция чрезмерного акцентирования внимания работодателя на контролирующей функции управления пользователями и недооценке другой важнейшей управленческой функции – мотивации. Усиленный контроль информационного поведения сотрудников организации, направленный на повышение доверия к безопасности информационных систем, все больше воспринимается ими как недоверие со стороны руководства и вызывает взаимный скептицизм и снижение внутренней мотивации не только к выполнению правил информационной безопасности организации, но и должностных обязанностей в целом.

Снижение доверия работников к работодателю и их мотивации к соблюдению норм информационно-безопасного поведения является следствием не только усиленного контроля, но и негативной глобальной трансформации, выражающейся в нежелании людей следовать установленным нормам и выполнять правила.

Концепция нулевого доверия, положенная в основу системы информационной безопасности организации и интерпретируемая как концепция сбалансированного доверия, способна повысить результативность усилий работодателя по достижению информационно-безопасного поведения сотрудников. Это возможно при условии повышения культуры доверия и автономизации пользователей информационных систем организации как составляющих культуры информационной безопасности. Большой потенциал в решении новых практических задач имеют вузы в процессе подготовки будущих специалистов по защите информации.

СПИСОК ЛИТЕРАТУРЫ

1. InfoWatch. Исследование утечек информации ограниченного доступа в 2020 году. – URL: https://www.infowatch.ru/analytics/analitika/issledovanie-utechek-informatsii-ogranichennogo-dostupa-v-2020-godu (дата обращения: 06.12.2021).
2. SearthInform. Утечки из организаций России. I полугодие. – URL: https://searchinform.ru/blog/2020/08/18/itogi-polugodiya-v-94-sluchaev-iz-organizacij-utekli-poleznye-dlya-moshennikov-dannye/?fbclid=IwAR1tAlLgOePEAY1_FunX219mSKoZdP6xMIur3ElVCAcr4xAr3dCYOuk1YPo (дата обращения: 06.12.2021).
3. SearthInform. Инциденты внутренней безопасности в Российских компаниях. Данные за первое полугодие 2020 года. – URL: https://searchinform.ru/practice-and-analytics (дата обращения: 06.12.2021).
4. Kindervag J. No More Chewy Centers: Introducing the Zero Trust Model of Information Security // Forrester Research. – 2010. – URL: https://www.forrester.com/report/No+More+Chewy+Centers+The+Zero+Trust+Model+Of+Information+Security/-/E-RES56682 (дата обращения: 26.11.2021).
5. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture // National Institute of Standards and Technology. – 2020. – URL: https://csrc.nist.gov/publications/detail/sp/800-207/final (дата обращения: 06.12.2021).
6. Buck C., Olenberger C., Schweizer A., Völter F., Eymann T. Never trust, always verify:

A multivocal literature review on current knowledge and research gaps of zero-trust // Computers & Security. – 2021. – Vol. 110, 102436. – URL: https://www.sciencedirect.com/science/article/ pii/S0167404821002601 https://doi.org/10.1016/j.cose.2021. 102436 (дата обращения: 06.12.2021).
7. Кузнецов С.А. Модель нулевого доверия применительно к корпоративным информационным системам / С.А. Кузнецов, И.А. Куликов, А.А. Фоминых // Актуальные научные исследования в современном мире. – 2021. – № 6-1(74). – С. 59-62.
8. Cittadini L., Spear B., Beyer B., Saltonstall M. BeyondCorp Part III: The Access Proxy. Google; 2016. – URL: https://research.google/pubs/pub45728 (дата обращения: 06.12.2021).
9. Escobedo V.M., Zyzniewski F., Beyer A.E., Saltonstall M. BeyondCorp: The User Experience. Google; 2017. – URL: https://research.google/pubs/pub46366/ (дата обращения: 06.12.2021).
10. Singh J., Refaey A., Shami A. Multilevel security framework for NFV based on software defined perimeter // IEEE Network. – 2020b. – № 34(5). – P. 114–19. DOI: 10.1109/MNET.011.1900563
11. Колпащикова Е.А. Переход от традиционной модели кибербезопасности к модели нулевого доверия / Е.А. Колпащикова, А.А. Юровская // Аллея науки. – 2018. – Т. 4, № 10(26). – С. 942-947.
12. Астахова Л.В. Информационная безопасность: герменевтический подход // Избранные труды Российской школы по проблемам науки и технологий. – Москва: Российская академия наук, 2010. – 186 с.
13. Gigamon. The IT and Security Landscape for 2020 and Beyond and the Role of Zero Trust. Gigamon. – 2020. – URL: https://www. gigamon.com/resources/resource-library/analyst-industry-reports/ar-zerotrust-surveyreport.html (дата обращения: 06.12.2021).
14. American Council for Technology. Zero Trust Cybersecurity: Current Trends. American Council for Technology; 2019. – URL: https://www.actiac.org/zero-trust-cybersecurity- current-trends (дата обращения: 20.11.2021).
15. 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. – P. 58-65. DOI: 10.3103/S0147688216010123.
16. Astakhova L.V. Developing students' culture of trust as a preventive means of combating cyber extremism // EDULEARN17 Proceedings. – 2017. – P. 4964-4971. – URL: https://library.iated.org/view/ASTAKHOVA2017DEV (дата обращения: 06.12.2021).
17. Астахова Л.В. Проблемы культуры информационной безопасности в условиях цифровой экономики // Научно-техническая информация. Сер. 1. – 2020. – № 2. – С. 28-37; Astakhova L.V. Issues of the Culture of Information Security under the Conditions of the Digital Economy // Scientific and Technical Information Processing. – 2020. – Vol. 47, № 1. – P. 56-64. DOI: 10.3103/S0147688220010062.
18. Deci E.L., Ryan R.M. Intrinsic motivation and self-determination in human behavior. – NY: Plenum Publishing Co, 1985. – 371 p. – URL: https://doi.org/10.1007/978-1-4899-2271-7 (дата обращения: 06.12.2021).
19. CSDT. Center for Self-Determination Theory. – URL: https://selfdeterminationtheory.org (дата обращения: 06.12.2021).
20. Koestner R., Holding A. A generative legacy: SDT's refined understanding of the central role of autonomy in human lives // Motivation Science. – 2021. – № 7(2). – P. 111–112. – URL: https://doi.org/10.1037/mot0000221 (дата обращения: 06.12.2021).
21. Лабзова И.Ю. Теория самоопределения и её применение в зарубежной образовательной практике // Человек и образование. – 2017. – № 3(52). – С. 152-156.
22. Ryan R.M., Deci E.L., Vansteenkiste M., Soenens B. Building a science of motivated persons: Self-determination theory's empirical approach to human experience and the regulation of behavior // Motivation Science. – 2021. – № 7(2). – P. 97-110. – URL: file:///C:/Users/1D1D~1/AppData/Local/ Temp/2021_RyanDeciVansteenkisteSoenens_BuildingAScience_Manuscript.pdf (дата обращения: 06.12.2021).
23. Da Veiga A. Defining organisational information security culture-Perspectives from academia and industry / A. Da Veiga, L. V. Astakhova, A. Botha, M. Herselman // Computers & Security. – 2020. – Vol. 92. – P. 101713. DOI: 10.1016/j.cose.2020.101713 (дата обращения: 06.12.2021).
24. Gangire Y., Da Veiga A., Herselman M. Assessing information security behaviour: a self-determination theory perspective // Information and Computer Security. – Mar 2021. – URL: https://www.emerald.com/insight/content/doi/10.1108/ICS-11-2020-0179/full/html (дата обращения: 06.12.2021).
25. Лукацкий А. Почему не работают политики ИБ, а также наказания за их нарушения?. – URL: https://www.securitylab.ru/blog/personal/Business_without_danger/20720.php (дата обращения: 26.11.2021).
26. Patall E.A. Self-determination theory: Eminent legacy with boundless possibilities for advancement // Motivation Science. – 2021. – №7(2). – P. 117–118. – URL: https://doi.org/10.1037/mot0000223 (дата обращения: 06.12.2021).

Материал поступил в редакцию 07.12.21.

Сведения об авторе

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