МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ВСЕРОССИЙСКИЙ ИНСТИТУТ НАУЧНОЙ И ТЕХНИЧЕСКОЙ ИНФОРМАЦИИ
РОССИЙСКОЙ АКАДЕМИИ НАУК
(ВИНИТИ РАН)

НАУЧНО • ТЕХНИЧЕСКАЯ ИНФОРМАЦИЯ

Серия 1. ОРГАНИЗАЦИЯ И МЕТОДИКА ИНФОРМАЦИОННОЙ РАБОТЫ

ЕЖЕМЕСЯЧНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ СБОРНИК

Издается с 1961 г. **№ 4** **Москва 2021**

ОБЩИЙ РАЗДЕЛ

УДК 001.89:002–047.44

Л.В. Астахова

Трансформация стратегических моделей управления человеческими угрозами информационной безопасности предприятия как императив цифровой индустрии*

Обоснованы императивы трансформации модели управления человеческими угрозами информационной безопасности (ИБ) на предприятии цифровой индустрии, с использованием теорий стратегического менеджмента, психологической собственности (причастности) и культурных параметров человеческой деятельности. Обоснованы типы стратегий и стратегические модели культуры информационной безопасности; с помощью социологического исследования выявлены доминирование в организациях защитной стратегии культуры ИБ и закономерность перехода от защитной к развивающей стратегической модели, а затем – к интегративной стратегии управления культурой ИБ, сочетающей в себе обе стратегические модели. Представлена концепция проекта национального стандарта «Культура информационной безопасности», который может быть основой для проектирования и внедрения одноименного стандарта любого предприятия.

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

Ключевые слова: *культура информационной безопасности, осведомленность, управление, стратегии, организация, человеческие риски, доверие, вовлеченность, работодатель, работник*

DOI: 10.36535/0548-0019-2021-04-1

ВВЕДЕНИЕ

Факт доминирования человека в составе источников инцидентов информационной безопасности (ИБ) в организациях всех типов и видов всех отраслей деятельности остается неизменным. Как бы стремительно ни развивались технологии и средства защиты информации, информационная система становится уязвимой, если остается без внимания ее пользователь. По результатам аналитического исследования компании *Infowatch* [1], уже четыре года подряд доля внутренних утечек от общего числа утечек остается в диапазоне 53-61%, т. е. более половины всех утечек информации, зафиксированных в мире, происходит не по причине воздействия внешних хакеров, а из-за ошибок или умышленных действий сотрудников (включая руководство), владельцев и операторов информации: «Совокупный объем данных, скомпрометированных в результате внутренних утечек, в 2019 году составил 9,87 млрд записей. Впервые за все время наблюдений объем записей, скомпрометированных в результате внутренних утечек, превысил аналогичный показатель утечек внешних – 4,7 млрд записей». В условиях пандемии коронавируса COVID-19 угрозы воздействия информации на сотрудников организаций, работающих удаленно, усилились: резко возросло число фишинговых сайтов и рассылок на тему вируса и связанных с ними вредоносных кодов; увеличились масштабы мошенничества и дезинформации, направленных на эксплуатацию страха или неполноту информации о пандемии и др. [2]. Усиление антропогенных угроз информационной безопасности предприятия в условиях стремительно развивающейся цифровой индустрии не может не порождать глобальные стратегические изменения в процессах управления ИБ. Этим обусловлена цель статьи – обосновать направление и сущность трансформации стратегической модели управления человеческими угрозами информационной безопасности предприятия.

СТРАТЕГИИ КУЛЬТУРЫ ИБ И СРЕДСТВА ИХ РЕАЛИЗАЦИИ

Мировая наука и практика интенсивно изучают проблему управления угрозами в контексте культуры информационной безопасности. В России, к сожалению, безуспешной оказалась попытка принятия документа «Основы государственной политики по формированию культуры информационной безопасности в Российской Федерации», задачей которого должна была стать стратегия по созданию у российских граждан культуры безопасного поведения при использовании информационных технологий, интернет-серфинга, электронных платежей и т.п., начиная с детей и заканчивая пожилыми людьми [3]. Поэтому вся тяжесть ответственности за формирование и развитие культуры ИБ лежит сегодня на руководителях организаций.

Главная роль руководителя организации как субъекта развития культуры ИБ обусловлена и динамикой культурных параметров человеческой деятельности. Дело в том, что «культура – это не отрасль деятельности, производящая свой специфический продукт, а универсальная модальность, пронизывающая все отрасли деятельности и привносящая в них возможность коллективного осуществления этой деятельности или потребления ее результатов, определенную упорядоченность, а также символику, связанную с системой ценностных ориентации. Культура – это система взаимоотношений между людьми, способствующая их взаимопониманию и осуществлению совместной деятельности или потреблению ее продуктов» [4]. Культурными параметрами деятельности человека в современную постиндустриальную эпоху являются: доминирующая форма социальной организации субъектов деятельности (объединение вокруг общей работы, профессиональная самореализация как наиболее эффективный способ управления сознанием и поведением человека), порядок ее осуществления (новации) и профиль символизации результатов (дихотомия современное/архаичное). Именно с помощью этих средств культура регулирует сознание и поведение людей, удерживая их в рамках исторически сложившихся в постиндустриальном сообществе ценностных ориентаций [4, с. 302]. В отличие от социализации, которая ориентирует человека в условиях жизнедеятельности, определяемых преимущественно утилитарными, прагматическими задачами, инкультурация (процесс освоения человеком норм общественной жизни и культуры) ориентирует человека в условиях, детерминированных ценностными установками, характерными для данной социальной среды, историческими традициями, ментальными особенностями и пр. [5, с. 1].

Приведенные факторы легли в основу определения культуры информационной безопасности организации, представленного в наших публикациях. В результате анализа большого массива зарубежных статей мы сформулировали определение культуры информационной безопасности организации, понимая под ней способ целенаправленной созидательной совместной деятельности руководителей и сотрудников по обеспечению и повышению уровня ИБ организации, который выражен в их ценностях, потребностях, знаниях и поведении: а) в формировании ценностных моделей их информационного взаимодействия как отправителей и получателей информации; б) в гармонизации потребностей работодателя (в обеспечении ИБ организации) и сотрудников (в самореализации и саморазвитии); в) в непрерывном повышении их знаний, в том числе – осведомленности об ИБ; г) в способности работодателя и сотрудников реализовывать и развивать их культурные ресурсы в информационном поведении в процессе совместной профессиональной деятельности [6, 7]. Очевидно, что такая интерпретация культуры ИБ

применима для наиболее развитых, высших форм ее проявления, которые связаны не только с защитой информационных ресурсов организации и интересами работодателя, но и с интересами сотрудников, чем существенно отличается от существующих социально-профессиональных стереотипов. Именно этот подход к понятию культуры ИБ коррелирует с ценностями современной постиндустриальной культуры и будет использоваться в настоящей статье.

Поскольку любая организация всегда имеет особенности внутренней и внешней среды, проблемы самостоятельного выбора на местах определенной стратегии развития культуры информационной безопасности весьма актуальны. Однако в теории информационной безопасности эта проблема не изучена и до сих пор не становилась предметом специального исследования.

Согласно классической теории стратегического менеджмента, стратегия – это совокупность всех действий – управляющих, способствующих достижению целей организации [8, с. 44]. Следовательно, стратегия культуры ИБ – это обобщающая модель действий, необходимых для достижения поставленных целей. Она является функциональной стратегией, так как относится к одному из функциональных направлений деятельности организации – обеспечению ее информационной безопасности, связанной с персоналом.

Важнейшее требование к стратегии – её способность адаптироваться к изменяющимся обстоятельствам [8, с. 44]. Поэтому для изучения стратегий культуры ИБ считаем обязательным ситуационный подход. Известно, что теория ситуаций исследует понятие стратегии в двух измерениях: в статике (как единство субъективных и объективных факторов) и в динамике (как кондициально (условно)-смысловое взаимодействие) [9, с. 1003-1010]. Логично утверждать, что и стратегию культуры ИБ организации формируют объективные и субъективные (внешние и внутренние), а также ситуационно-коммуникационные, поведенческие факторы внутри организации и ее взаимодействие с внешней средой в каждый текущий момент времени.

В теории стратегического менеджмента выделяют оборонительные и наступательные стратегии организации [8, с. 249.], отличающиеся своими целями и средствами реализации. Логично утверждать, что такая же классификация применима и для стратегий культуры ИБ. На выбор оборонительной (назовем ее защитной) или наступательной (назовем ее развивающей) стратегии, безусловно, влияют объективные, внешние факторы: национально-культурные, политические и правовые, экономические, социально-культурные и технико-технологические. Так, отсутствие концептуальных и нормативных документов по культуре ИБ, кризисное состояние экономики в России, бюджетный дефицит обусловливают интуитивный выбор защитной стратегии.

Оборонительная (защитная) стратегия культуры ИБ – цель этой стратегии – снижение угроз быть атакованной по вине внутренних пользователей, возможность перенести их преднамеренные и непреднамеренные атаки на информационные системы с минимальными потерями для организации. При этом минимизация человеческих угроз ИБ – это начальная ступень развития культуры ИБ организации. Достижение ее более высокого уровня возможно исключительно в результате реализации наступательной стратегии.

Наступательная (развивающая) стратегия культуры ИБ – цель этой стратегии – получение и развитие конкурентных преимуществ организации за счет формирования человеческого, интеллектуального и культурного капиталов каждого сотрудника в отдельности и организации в целом, что является профилактикой реализации человеческих угроз ИБ.

В криминологии профилактика – это самый ранний, начальным этап предупредительной деятельности, направленной на недопущение правонарушения. По мнению экспертов, под профилактикой следует понимать процесс *выявления, устранения причин и условий*, способствующих совершению правонарушений, а под предупреждением - недопущение уже замышляемых и подготавливаемых противоправных деяний [10, с. 45]. Поэтому предупреждение может быть квалифицировано как защитная мера, а профилактика – как развивающая.

Впервые термин «профилактика» был нормативно закреплен в ст. 2 Федерального закона «Об основах системы профилактики правонарушений в Российской Федерации»[1], согласно которому «профилактика правонарушений – это совокупность мер социального, правового, организационного, информационного и иного характера, направленных на выявление и устранение причин и условий, способствующих совершению правонарушений, а также на оказание воспитательного воздействия на лиц в целях недопущения совершения правонарушений или антиобщественного поведения». Самостоятельную разновидность профилактики правонарушений образует виктимологическая профилактика, под которой понимают «целенаправленное специализированное воздействие на лиц с неправомерным или аморальным поведением, *а также на факторы, обусловливающие виктимность*, связанную с подобным поведением. В равной мере ее объектом являются факторы и лица, положительное поведение которых, тем не менее, виктимоопасно для них» [11, с. 241]. Основная задача виктимологической профилактики состоит в *создании системы эффективной защиты человека от потенциальной виктимизации* [12, с. 103]. Именно в этом заключена суть развивающей стратегии культуры ИБ: создание системы эффективной защиты сотрудников организации от потенциальной виктимизации, которая может стать угрозой для защищаемой информации.

Приняв во внимание классификацию профилактики по объектам воздействий [12, с. 104], можно утверждать, что объектами воздействий в рамках защитной стратегии культуры ИБ являются причины и условия совершения правонарушений, а также поведение лиц, потенциально способных совершить или уже совершивших правонарушение; в рамках развивающей стратегии – факторы, влияющие на формирование и развитие личности. Поэтому недостаток

[1] Федеральный закон от 23.06.2016 N 182-ФЗ "Об основах системы профилактики правонарушений в Российской Федерации". – URL: http://www.consultant.ru/document/cons_doc_LAW_199976/ (дата обращения 19.12.2020).

защитной стратегии заключается в том, что каждый сотрудник организации рассматривается потенциальным нарушителем безотносительно к его личностным качествам. Достоинство развивающей стратегии культуры ИБ – в определении возможностей личностной самореализации каждого сотрудника с целью его защиты от попадания в число нарушителей.

Разные цели стратегий культуры ИБ и объекты воздействия определяют специфичность средств их реализации.

В ходе функционально-стратегического планирования в организации, выбравшей защитную стратегию, учитываются субъективные, внутриорганизационные факторы влияния на уровень развития культуры ИБ: внутреннее состояние, стадия жизненного цикла организации, уровень общей организационной культуры, наличие действующей системы защиты конфиденциальной информации в организации. От этого зависит стратегический план культуры ИБ, т. е. какие управленческие мероприятия будут проводиться: разработка и реализация политик управления рисками, инцидентами ИБ, изменениями, персоналом, осведомленностью, обучением и др. Полагаем, что именно на защитную стратегию профилактики правонарушений нацелен Федеральный закон «Об основах системы профилактики правонарушений в Российской Федерации», согласно которому реализация профилактики правонарушений осуществляется посредством: выявления, оценки и прогнозирования криминогенных факторов социального характера; правового регулирования профилактики правонарушений; разработки специальных программ в сфере профилактики правонарушений; выявления и устранения причин и условий, способствующих антиобщественному поведению и совершению правонарушений; выявления лиц, склонных к совершению правонарушений; проведения мониторинга в сфере профилактики правонарушений и др. (ст.6).

Кроме этих управленческих процедур, предусмотренных защитной стратегией, в стратегический план реализации развивающей стратегии включаются мероприятия, связанные с развитием организации и её сотрудников: изучение их личностных качеств и ценностей, потребностей и установок, эмоционального состояния; развитие их знаний об информационной безопасности; контроль за соблюдением правил ИБ-поведения. Огромное значение имеет степень взаимного доверия, лояльности (приверженности) сотрудников к организации, их вовлеченности в реализацию ИБ-стратегии предприятия, степень гармонизации потребностей работодателя (в обеспечении ИБ организации) и сотрудников (в самореализации и саморазвитии). Это существенно повышает шансы на успех обеспечения информационной безопасности и развития культуры ИБ. Высокий уровень лояльности сотрудника к организации предполагает, что он идентифицирует себя с ней, представляет себя и организацию как единое целое, отождествляет себя с ее культурой и способен реализовать все свои личностные характеристики в информационном поведении в процессе профессиональной деятельности. В результате развиваются и сотрудник, и организация, что является главным профилактическим средством обеспечения ИБ.

Очевидно, что связь развивающей стратегии культуры ИБ с развитием знаний, интеллектуального и культурного капиталов человека требует обращения к стратегиям управления знаниями в организации. Эксперты рассматривают управление знаниями в контексте устойчивости [13], а на основе эмпирических исследований признают, что управление угрозами знаниям – это значительный механизм повышения организационной эффективности [14]. Это в полной мере относится и к управлению культурой ИБ.

Хорошо известны 10 стратегий передачи информации от работников во внешнюю, внутреннюю среду и для развития индивидуальных компетенций сотрудников Э. Свейби [15]. Российские ученые обосновывают классификацию стратегий управления знаниями, в основе которой лежат 7 комбинаций из базовых стратегий, которые направлены либо на обмен знаниями в рамках одного вида интеллектуального капитала с целью его увеличения, либо на эффективный перенос знаний из одного вида интеллектуального капитала в другой. В своей основе они имеют движение знаний между: отдельными работниками (в рамках индивидуальной компетенции); отдельными элементами внутренней структуры; отдельными элементами внешней структуры; элементами внешней структуры и работниками организации; элементами внутренней структуры и работниками организации; элементами внутренней и внешней структуры; одновременно между всеми видами интеллектуального капитала [16, 17]. Другие авторы выделяют четыре стратегии управления знаниями по критерию их происхождения: внешняя и внутренняя кодификация, внешняя и внутренняя персонализация [18]; разрабатывают модель управления, основанную на знании-управлении-измерении-действии, стремясь объединить три области, обычно рассматриваемые отдельно: управление знаниями, измерение интеллектуального капитала и стратегические действия [19] и др.

Движение знаний между внешними и внутренними структурами требует управления знаниями не только сотрудников, но и клиентов – *Customer Knowledge Managemen*t (*CKM*), ориентированного на данные подхода к управлению взаимоотношениями с клиентами (*Customer Relation-ship Management – CRM*) и человекоориентированного подхода к управлению знаниями. *CKM* характеризуется как инновационная практика извлечения и эксплуатации трех типов знаний: о клиентах, от клиентов и для клиентов. Этот интегрированный подход предполагает признание знаний клиентов как части компании. Управление этим интеллектуальным активом – источник для разработки продуктов, управления проектами и успеха бизнеса в целом [20, с. 92].

Особое внимание уделяется системам управления знаниями на малых и средних предприятиях, которые разделены на две категории: *KM-Practices* (определяемые как набор методов и приемов для поддержки организационных процессов управления знаниями) и *KM-Tools* (а именно – конкретные системы на базе *IT*, поддерживающие *KM-Practices*). Малые и средние предприятия принимают и используют более традиционные инструменты (*KM-Tools*), а не новые и более обновленные, которые обычно дешевле и проще в использовании. Они внедряют и более интенсивно

используют практики (*KM-Practices*), которые не сосредоточены исключительно на процессе управления знаниями, но стремятся адаптировать уже известные им практики к требованиям управления знаниями.

Некоторые авторы предлагают таксономию, которая объединяет стратегии использования *KM-Practices* и *KM-Tools* и определяют четыре стратегии: «ориентир», «эксплуататор», «исследователь» и «опоздавший». В основании этой классификации лежит набор инструментов и методов, используемых для управления знаниями [21].

Все эти подходы к сущности и видам управления знаниями, в результате реализации которых может быть достигнута профессиональная и личностная самореализация сотрудников организации, легко адаптируются и к управлению культурой информационной безопасности.

В рамках развивающей стратегии рассмотрим ключевой фактор влияния на культуру ИБ сотрудника как создателя, вовлеченного и погруженного в производственно-управленческие процессы организации.

Зарубежные эксперты изучили роль психологического состояния полного погружения сотрудника в деятельность и его психологической собственности – причастности в обеспечении ИБ организации. В результате они пришли к выводу, что и погружение, и психологическая собственность значительно увеличивают стремление и готовность сотрудников участвовать в соблюдении требований информационной безопасности, приводят к повышению производительности труда, а также инициируют этическое и ответственное поведение [22]. Вовлеченность в работу организации позволяет человеку увидеть свое отражение в цели и почувствовать свои усилия в её осуществлении. Согласно исследованиям, когда люди погружаются в определенную деятельность, они по своей природе мотивированы активно участвовать в этой деятельности и одновременно испытывают сильное чувство контроля над окружающей средой [23]. Сотрудники с сильной психологической причастностью не склонны демонстрировать такое поведение, как кража, повреждение имущества организации, преднамеренные ошибки в работе или кибербездействие [24].

Всё это имеет большое значение для управления информационной безопасностью. В процессе реализации защитной стратегии культуры ИБ организации вкладывают значительные средства в программы повышения осведомленности сотрудников. Для этой цели проводятся онлайн-тренинги, групповые встречи, общения по электронной почте и семинары и др. Однако это не дает ожидаемых результатов. Многие сотрудники считают посещение таких мероприятий дополнительной нагрузкой, рассматривают их как препятствия для обычной работы [25]. Использование внутренней мотивации, присущее развивающей стратегии, как правило, более эффективно, чем строгое принуждение сотрудников к обучению. Поэтому переход предприятия от защитной к развивающей стратегической модели культуры ИБ, позволяющей активировать мотивацию сотрудников, запустить механизм их самореализации и развития в управлении информационной безопасностью, – это закономерность управления человеческими угрозами ИБ предприятия. Постепенная трансформация защитной стратегической модели культуры ИБ в наступательную – это неизбежная траектория деятельности предприятия в цифровой индустрии, которая немыслима без человека и его вовлеченности в инновационное развитие экономики.

Классификация стратегий культуры ИБ, как и любая классификация, условна. Здесь следует использовать интегративную, защитно-развивающую стратегию управления культурой ИБ, сочетающую в себе обе обоснованные стратегии. Интегративная стратегия должна быть по своей сути ситуационной, основанной на мониторинге уровня культуры ИБ сотрудников в процессе как внутренних, так и внешних коммуникаций организации.

В ходе исследования мы провели опрос сотрудников организаций разных типов с целью выяснения восприятия ими стратегических аспектов управления культурой ИБ. В опросе принял участие 51 человек, из них: 64,7% – рядовые сотрудники, а 66,7% участников опроса составляли сотрудники от 18 до 25 лет. Организации относились к разным сферам: технологий и программного обеспечения (19,6%); услуг (17,7%); образования (13,7%); государственных услуг (11,8%), торговли (9,8%), финансовых услуг (7,8%), промышленности (5,9 %), здравоохранения, связи и энергетики (по 2%) и др. 56,9% из них – частные предприятия, 33,3% – государственные, 9,8% – некоммерческие организации. Частные предприятия представлены малым (41%), средним (33,3%) и крупным (25,6%) бизнесом. 84,3% всех организаций – российские, 7,8% – имеют представительство в странах Ближнего Зарубежья, 5,9% – в Европе, 2% – в Северной Америке.

Подавляющее большинство респондентов ответили, что в их организации действует политика информационной безопасности (82,4%); есть сотрудник по информационной безопасности (76,5%); проводится повышение осведомленности среди сотрудников об информационной безопасности (76,5%). Однако лишь в 39,2% организаций сотрудники вовлечены в процесс обнаружения о нарушениях / инцидентах в области информационной безопасности, у них есть средство сообщения / адрес электронной почты. Дисциплинарные взыскания за несоблюдение политики информационной безопасности действуют в 66,7% организаций, но лишь в 19,6% работает система поощрений сотрудников (признание, оценка производительности, вознаграждения и т.д.) для обеспечения соответствия политике информационной безопасности. Из этого можно заключить, что большинство организаций используют защитную стратегию культуры ИБ, а значит находятся на начальном этапе ее развития.

Для стимулирования развития культуры ИБ в науке и практике требуется стандартизация этого процесса. Так, для отрасли безопасности жизнедеятельности – это давно пройденный этап: в ней разработан, принят и применяется ГОСТ Р 22.3.07-2014 «Безопасность в чрезвычайных ситуациях. Культура безопасности жизнедеятельности. Общие положения» [26]. ГОСТ Р МЭК 62508-2014 «Менеджмент риска. Анализ влияния на надежность человеческого фактора. Идентичен международному стандарту МЭК 62508:2010* «Анализ влияния на надежность

человеческого фактора" (IEC 62508:2010 Guidance on human aspects of dependability)» [27] используется и в других отраслях. Эти стандарты дали импульс развитию научных исследований и практической деятельности в нашей стране. Так, изучение показателей и критериев оценки человеческого фактора с целью снижения его влияния весьма распространены в сфере транспорта [28] и др.

Логично предположить, что снижение человеческих угроз в ИБ и развитие культуры ИБ также должны стать объектами отражения в подобных стандартах. Разработанный нами проект стандарта «Культура информационной безопасности» содержит 7 разделов, в которых: сформулированы определения понятий человеческого фактора, человеческих рисков, культуры, стратегий развития; факторов влияния на культуру ИБ на индивидуальном и организационном уровнях; цели, направления, средства и методы ее формирования и развития; организационные принципы и организационно-методические требования (требования к организации и методике ее планирования, оценки, контроля и совершенствования); требования к документированию этих процессов (к политике развития культуры ИБ и другим локальным документам организации этой тематики) в рамках реализации как защитной, так и развивающей стратегий культуры ИБ. Целесообразно также дополнить этим контентом стандарты серии ИСО/МЭК 27000 по управлению информационной безопасностью, их разделы по ИБ, связанной с персоналом.

ВЫВОДЫ

Как бы стремительно ни развивались технологии и средства защиты информации, информационная система становится уязвимой, если остается без внимания ее пользователь. По результатам аналитических исследований, уже четыре года подряд доля внутренних утечек информации от общего их числа составляет более половины всех утечек, зафиксированных в мире, которые происходят из-за ошибок или умышленных действий сотрудников (включая руководство) и владельцев информации. На основе культурных параметров деятельности человека в современную постиндустриальную цифровую эпоху, а также теорий стратегического менеджмента и психологической собственности (причастности) нами представлены две стратегии управления человеческими угрозами информационной безопасности организации: оборонительная (защитная) и наступательная (развивающая).

Поскольку человеческие угрозы информационной безопасности нельзя рассматривать вне сферы культуры, эти стратегии являются стратегиями культуры информационной безопасности организации, имеющими специфику целей, объектов и средств реализации.

Защитная стратегия нацелена на минимизацию угроз информационной безопасности, направлена на сотрудников как на потенциальных нарушителей и реализуется преимущественно посредством мер принуждения. Развивающая стратегия имеет целью создание системы снижения угроз потенциальной виктимизации сотрудников, направлена на развитие факторов их личностного развития и реализуется с помощью сотрудничества работодателя и сотрудников, усиления вовлеченности в производственно-управленческие процессы и развития психологической собственности работников.

Выявлен современный императив цифровой индустрии и закономерность перехода от защитной к наступательной стратегии культуры информационной безопасности.

Представлены результаты социологического опроса работников организаций различных отраслей и форм собственности по вопросам управления информационной безопасностью, проведенного нами с помощью инструментов *Google Forms*.

Сделан вывод о доминировании в организациях защитной стратегии с использованием повышения осведомленности и дисциплинарных взысканий за нарушение политик информационной безопасности.

Доказана необходимость использования технологий управления знаниями, а также интегративной, ситуационной стратегии управления культурой информационной безопасности, сочетающей в себе обе обоснованные стратегии на уровнях внутренних и внешних коммуникаций организации.

Обоснована потребность в стандартизации культуры информационной безопасности с использованием опыта стандартизации культуры в родственной области – безопасности жизнедеятельности. Представлена концепция проекта национального стандарта «Культура информационной безопасности».

СПИСОК ЛИТЕРАТУРЫ

1. Утечки данных организаций по вине или неосторожности внутреннего нарушителя. Сравнительное исследование. 2013-2019 гг.: Аналитический отчет. – URL: https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_Analytical_Report.pdf (дата обращения 19.12.2020).
2. Лукацкий А. Эксплуатация темы коронавируса в угрозах ИБ. – URL: https://habr.com/ru/company/cisco/blog/494726/ (дата обращения 19.12.2020).
3. Лукацкий А. Кибербезопасность "утопающих" дело рук самих "утопающих». – URL: https://lukatsky.blogspot.com/2019/12/blog-post_23.html (дата обращения 19.12.2020).
4. Флиер А.Я. Человеческая деятельность и ее культурные параметры // II Моисеевские чтения: культура как фактор национальной безопасности России. Доклады и материалы Общероссийской (национальной) научной конференции / под редакцией А.В. Костиной, В.А. Лукова. – Москва, 2019. – С. 299-305.
5. Флиер А.Я. Локальная культурная система: факторы устойчивости // Культура культуры. – 2020. – № 1. – С. 1.
6. Adéle da Veiga, Liudmila V. Astakhova, Adéle Botha, Marlien Herselman. Defining organisational information security culture – Perspectives from academia and industry // Computers & Security. – 2020. – Vol. 92. – P. 101713.
7. 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.
8. Томпсон А.А., Стрикленд А.Дж. Стратегический менеджмент. Искусство разработки и реализации стратегии. – М.: Банки и биржи, ЮНИТИ, 1998. – 576 с.
9. Veklenko P.V. Situational approach in the social-human cognition: objectives, principles and categories // Journal of Siberian Federal University. Humanities & Social Sciences. – 2015. – Vol. 8, № 5. – P. 1003-1010.
10. Лекарь А.Г. Профилактика преступлений. – М.: Юрид. лит., 1972. – 104 с.
11. Ривман Д.В. Криминальная виктимология. – СПб: Питер, 2002. – 304 с.
12. Гербеков И.И. "Понятие и виды профилактики правонарушений // Юридическая наука и правоохранительная практика. – 2017. – № 4(42). – P. 99-105
13. Martins V.W.B., Rampasso I.S., Anholon R., Quelhas O.L.G., W. Leal Filho. Knowledge management in the context of sustainability: Literature review and opportunities for future research // Journal of Cleaner Production. – 2019. – Vol. 229. – P. 489-500.
14. Susanne Durst, Christoph Hinteregger, Malgorzata Zieba. The linkage between knowledge risk management and organizational performance // Journal of Business Research. – 2019. – Vol. 105(December). – P. 1-10.
15. Sveiby K.-E. A Knowledge-based Theory of the Firm. To guide Strategy Formulation // Journal of Intellectual Capital. – 2001. – Vol. 2, №4. – URL: file:///C:/Users/1D1D~1/AppData/Local/Temp/knowledgetheoryoffirmfin-draft-1.pdf
16. Гапоненко А., Орлова Т. Управление знаниями. – Москва: Эксмо, 2008. – 400 с.
17. Паникарова С.В., Власов М.В. Управление знаниями и интеллектуальным капиталом / М-во образования и науки РФ, Урал. федер. ун-т. – Екатеринбург: Изд-во Урал. ун-та, 2015. – 140 с.
18. Tae Hun Kim, Jae-Nam Lee, Jae Uk Chun, Izak Benbasat. Understanding the effect of knowledge management strategies on knowledge management performance: A contingency perspective // Information & Management. – 2014. – Vol. 51, Issue 4, June. – P. 398-416.
19. Córdova F.M., Durán C.A., Pincheira M., Palominos F., Galindo R. Knowledge Management of Intangible Actives // Service Companies Procedia Computer Science. – 2019. – Vol. 162. – P. 596-603.
20. Гербина Т.В. Стратегии управления: управление знаниями клиента // Социально-ориентированное управление в условиях глобализации. Материалы VI Всероссийской заочной научно-практической конференции / Российский университет дружбы народов. – Москва, 2017. – С. 91-96.
21. Roberto Cerchione, Emilio Esposito. Using knowledge management systems: A taxonomy of SME strategies // International Journal of Information Management. – 2017. – Vol. 37, Issue 1(Part B, February). – P. 1551-1562.
22. Yoo C., Sanders G., Cerveny R. Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance // Decision Support Systems. – 2018. – Vol. 108. – P. 107-118.
23. Ho L.-A., Kuo T.-H. How can one amplify the effect of e-learning? An examination of high-tech employees' computer attitude and flow experience // Computers in Human Behavior. – 2010. – № 26(1). – P. 23-31.
24. Shantz A., Alfes K., Truss C., Soane E. The role of employee engagement in the relationship between job design and task performance, citizenship and deviant behaviours // International Journal of Human Resource Management. – 2013. – №24(13). – P. 2608-2627.
25. Bulgurcu B., Cavusoglu H., Benbasat I. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness // MIS Quarterly: Management Information Systems. – 2010. – № 34 (SPEC. ISSUE 3). – P. 523-548.
26. ГОСТ Р 22.3.07-2014 «Безопасность в чрезвычайных ситуациях. Культура безопасности жизнедеятельности. Общие положения». – Москва: Стандартинформ, 2019. – URL: http://docs.cntd.ru/document/1200109440 (дата обращения 19.12.2020).
27. ГОСТ Р МЭК 62508-2014 «Менеджмент риска. Анализ влияния на надежность человеческого фактора. Идентичен международному стандарту МЭК 62508:2010* "Анализ влияния на надежность человеческого фактора" (IEC 62508:2010 Guidance on human aspects of dependability)». – URL: http://docs.cntd.ru/document/1200113803 (дата обращения 19.12.2020).
28. Яньшина И.В., Репина И.Б. Состояние, показатели и критерии оценки человеческого фактора в структуре отказов технических средств путевого комплекса железной дороги // Вестник Сибирского государственного университета путей сообщения. 2019. – № 3(50). – С. 53-58.

Материал поступил в редакцию 19.12.20.

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