ОСОБЕННОСТИ ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ ПРЕДПРИЯТИЯ ЦИФРОВОГО ОБЩЕСТВА

И.Р. Чеканов, С.И. Неизвестный
Российский государственный социальный университет, г. Москва

Введение.

Переход к цифровому обществу, прежде всего, подразумевает максимальный перевод информационных потоков, средств получения информации, ее обработки, анализа, передачи, хранения в цифровой формат. Если при этом используется системный подход, в том числе подразумевающий 100% охват информации предприятия, включая и конфиденциальную всех уровней, то становится очевидным значимость обеспечения информационной безопасности. Естественно процесс погружения в цифровую среду затрагивает не только непосредственно защиту информации (ЗИ), но и соответствующую защиту всего ее окружения: физические носители, каналы передач, аппаратно-программные средства; всех объектов, субъектов, процессов, имеющих прямое или косвенное отношение к этой информации. В отличие от типичных технологий ЗИ, методов, способов, средств и инструментов, применяемых в обычных условиях отсутствия цифровизации (или частичного ее наличия), защита информации в цифровом обществе имеет свои особенности. Таким образом, проблема изучения этих особенностей защиты информации предприятия цифрового общества, несомненно, является актуальной.

Организация защиты информации предприятия цифрового общества сталкивается и с социальными аспектами. При всех положительных сторонах цифровизация имеет и ряд отрицательных, существенной из которых является проблема утилизации высвобождающихся трудовых ресурсов. На государственном уровне при декларировании перехода к цифровой экономике появляется содержательно-юридическая казуистика: массовое высвобождение трудовых ресурсов противоречит стратегии обеспечения социальной стабильности, системному гарантированию занятости трудоспособного населения. По оценкам специалистов при экстенсивном переходе на цифровую экономику миллионы трудоспособных людей РФ будут уволены [1,2]. Учет этой особенности ЗИ становится особенно актуальным при полномасштабном переходе страны к цифровой экономике.

Технические, технологические, социальные аспекты перехода к цифровой экономике формируют особые требования не только к объектам и процессам цифровизации, но и к субъектам. Цифровизация требует от специалистов, обеспечивающих ЗИ предприятия, и новых компетенций, и обладание достаточно высоким уровнем компетентности в них. Актуальность подготовки специалистов в области информационной безопасности (ИБ) цифровой экономики обоснована на разных уровнях управления, вплоть до высшего государственного [3].

Особенности организации защиты информации при переходе к цифровым технологиям в управлении делопроизводством предприятия

Любой переход на новые инструменты и технологии требует, по крайней мере, на время инсталляций и отладок, значительных дополнительных материальных, интеллектуальных, организационных ресурсов, включая и ресурсы по обеспечению информационной безопасности. При системном переводе процессов делопроизводства возникает ряд специфических угроз для ЗИ предприятия.

Во-первых, переход на новые технологические процессы сопряжен с доработками, связанными со спецификой условий инсталляций, отладкой аппаратно-программной и организационной частями внедряемого процесса.

Во-вторых, объективная организационно-методическая часть перехода от старого к новому процессу всегда подразумевает наличие работающего предыдущего варианта, запускаемого в производство нового (частично не полностью

апробированного) варианта, а между этими процедурами, как правило, возникают элементы «ручных» технологий, формирующих так называемые потенциальные «дырки», лазейки для несанкционированных действий. Хотя это состояние довольно краткосрочное, оно несет в себе большие информационные риски.

В-третьих, сотрудники, осуществляющие данный процесс, как правило, имеют недостаточную компетентность (а иногда и мотивированность), обеспечивающую 100% системную защиту информации при внедрении новых технологий, систем, инструментов. Привлечение же высококомпетентных сотрудников сторонних организаций (подрядчиков) всегда сопряжено с риском нарушения ЗИ, включая особенности конфликтов интересов сторон, при контактах с конфиденциальной информаций, доступ к которой формально разрешается только штатным сотрудникам. Эта процессно-юридическая коллизия, приводит к функциональному формированию рисков с последующей трансформацией их в инциденты нарушения ЗИ.

В-четвертых, внедрение новых инструментов, технологий всегда связано с настороженным принятием сотрудниками, пользователями этих новшеств. Это приводит к росту так называемых внутренних трансакционных издержек, вплоть до откровенного неприятия и саботажа [4]. Особенно велик риск нарушения ЗИ при неявных, скрытых формах саботажа.

В-пятых, не стоит недооценивать роль традиций и особенностей юридического сопровождения делопроизводства. Так в современной России юристы традиционно в большей степени доверяют бумажным документам по сравнению с электронным вариантом, заверенным ЭЦП (электронно-цифровыми подписями), в результате отдают предпочтение, а иногда и требуют сохранение бумажного делопроизводства.

Защита информации в автоматизированных системах принятия решений и юридическая ответственность в киберменеджменте

Цифровизация это не только массовый перевод повторяющихся действий роботам, привлечение искусственного интеллекта (ИИ), но и создание комплексных он-лайн систем принятия управленческих решений с синергией автоматизированных управляющих систем со специалистами профессионалами высокого уровня компетентности, прежде всего в области управления интеграцией. Цифровизация позволяет работать с гигантскими объемами информации, с которыми человек не в состоянии справиться, особенно если речь идет о необходимости принятия он-лайн решений, где ключевую роль играет человеческий фактор. Цифровизация должна строиться на основе синергетического эффекта в создании компромиссного баланса между деятельностью человека и кибер-менеджера, в создании симбиотической команды проекта, в которой искусственный интеллект будет трудиться «рука об руку» с людьми.

Естественно, переход на цифровые технологии предъявляют высокие требования к надежности, бесперебойности, защищенности всех операций с информацией. Так, например, при полном переходе на безбумажный цифровой документооборот, малейший сбой может привести к остановке, параличу всего бизнеса, предприятия, отрасли, что повлечет за собой к большим материальным, финансовым репутационным потерям и дискредитации цифровых технологий в целом. Особенно важным становится обеспечение надежности цифровизации в медицине и транспорте [5].

Системы киберфизических устройств позволяют эффективно управлять инфраструктурой не только отдельных домов, но и жизнью целых кварталов, микрорайонов, городов и мегаполисов [6].

Цифровизация диктует новые требования и подходы к формированию компетентности специалистов ИБ. Актуальными становятся не только коррекция существующих обучающих дисциплин управления проектами, но востребованы и

принципиально иные компетенции, новые обучающие курсы, новые учебные материалы. Цифровизация требует принципиального изменения методологии ИБ, коррекции стандартов и законов, регламентирующих эту сферу деятельности.

Цифровизация актуализирует процесс определения надежности источников информации и надежности данных. В этой связи существенно диверсифицируется роль доверия в управлении проектами. С одной стороны изменяется /ограничивается/ круг доверительных связей, с другой – доверие на уровне творческих личностей должно быть глубоким, взаимный. Внешне это выглядит парадоксально: кажется, что превращение «в цифру» значительно снижает субъективный человеческий фактор, обезличивает многие бизнес-процессы и должно приводить к снижению роли доверия между участниками проектной деятельности. Однако качество, надежность и результаты цифровизации сильнейшим образом зависят от качества входной информации, качества ресурсов, процессов и методологии преобразования этой информации. Незначительные нарушения в любом из этих элементов приведут к недостоверным результатам цифровизации. Отсюда диктуется необходимость инжиниринга процессов, методологии, трансформации компетентности старых ролей ИБ и необходимость в новых ролях ИБ, в совершенно новых автоматизированных рабочих местах.

В области ответственности за последствия принятия решений автоматизированными информационными системами (АИС) непосредственно пока нет нормативно-правовых документов, регулирующих действия кибер-менеджеров. Последствия, связанные с управлением в автоматизированных системах поддержки принятия решений с административно-юридической точки зрения, лежат на авторах разработки и функционирования этих систем, на их руководстве [7].

Безопасность принятия решений в киберменеджменте принципиально улучшается, если в управленческий процесс вводится жесткая обратная связь, направленная на «сходимость» принимаемых устойчивых решений. В «умных» механизмах процесс управления переводится на обратные технологии принятия решений [7]. С течением времени основная часть стоимости систем управления предприятием и систем управления ИБ будет определяться их цифровой составляющий, их интеллектуальным ядром принятия управленческих решений.

Организационные особенности перехода к цифровизации, связанные с изменением требований к компетентности специалистов ИБ

Цифровизация может вернуть человеку приоритет творческой составляющей в его труде. Изначально, от рождения в любом человеке присутствуют творческие способности. Промышленные революции с одной стороны позволили повысить производительность труда, с другой – привели к резкой дифференциации на людей, занимающихся творчеством и на людей, выполняющих однотипно повторяющиеся действия, приводящих к атрофии креативную составляющую в работе. Осознание этого явления позволит системно перейти к цифровизации, решая проблему безработицы, путем активизации, заложенной в человеке от природы, творческого начала и развития созидательной деятельности. Вернувшись к этим истокам, можно активизировать отношение к человеку как к личности, но не как к бездуховному исполнительному механизму. Естественно это требует от управленцев реинжиниринга управленческой культуры, организационного потенциала и системы формирования компетенций ИБ. Игнорирование данного процесса в цифровизации бизнеса может дискредитировать саму сущность цифровизации и привести к значительным социальным проблемам. Чтобы упредить данные проблемы, необходимо принципиально изменить систему формирования компетентности специалистов ИБ, вовлекаемых в процесс цифровизации.

Цифровизация уже идет и будет расширяться, постепенно охватывая все новые и новые виды деятельности, увеличивая влияние на культуру ведения бизнеса, на

культуру работы и информацией ее защиты, перераспределяя людские ресурсы, приводя человеческий труд в более креативное русло и активизацию творческого потенциала. Цифровизация влечет за собой изменение соотношения между физическим и умственным трудом, перестройку структуры, содержания многих видов компетенций и уровней компетентности трудовых людских ресурсов, изменение в подготовке специалистов, в том числе и в области информационной безопасности.

Заключение

Исследования аналитических центров показывают, что нарушение защиты информации на предприятиях перехода к цифровой экономике в большинстве случаев осуществляется сотрудниками самих предприятий [8]. Причем основными причинами подобных инцидентов являются конфликты между средним и верхним управленческими звеньями организаций, что является функциональной недоработкой, прежде всего, руководителей служб информационной безопасности и следствием неэффективной организационной политики.

Проанализировав подобные инциденты, связанные с хищением персональной и конфиденциальной информации, можно сделать вывод, что в центре причин оказываются конфликты между сотрудниками, проблемы, связанные с формированием здоровой корпоративной культуры [9].

Проблема безопасности принятия решений в киберменеджменте обостряется в связи с резкой глобализаций бизнеса и информационных систем, вызванных четвертой промышленной революцией [10]. Информационные ресурсы отдельного государства вынуждены взаимодействовать, обмениваться разного рода информационными потоками с глобальными мировыми системами, при это относится и к критическим инфраструктурам, обеспечивающим жизнедеятельность общества. Особенно значимым становится защита автоматизированных информационных систем центров принятия решений в военно-оборонной сфере [11]. Развитие оборонного потенциала мировых держав, повышение практического интереса к применению цифровых технологий в военной области, разработка стратегий ведения кибервойн, накопление боевых вирусных программ и утечка в сеть их исходных кодов резко обострили информационные риски и киберугрозы [12].

Один из эффективных путей повышения информационной защищенности киберсистем, интегрированных в глобальные системы, лежит в организационной области и относится к согласованию технологий, форматов обмена данными и их защиты на межгосударственном уровне. Примером здесь может служить подобный процесс, организованнный между РФ и КНР, между странами ШОС [13].

Перевод реальных процессов управления ИБ в гибридный вариант в результате цифровизации (основной объем принятия управленческих решений будет проходить в результате цифровых когнитивных технологий с привлечением комплексных АИС, ИИ, многопараметрического моделирования и фази-логики: т.е. в среде виртуальной реальности) принципиально выведет на ведущее место управление информационной безопасностью, роль которой в текущих широко используемых методах управления предприятием, пренебрежимо мало. Несравненно возрастет значимость функции ИБ *управление интеграцией*, культуры управления, междисциплинарного подхода, моделирования и формирования компетенций «завтрашнего дня». Подобные аспекты методологических трендов приведут к тому, что цифровизация как инструмент спровоцирует системный реинжиниринг методов организации и управления ИБ и вывод их из-под анестезии вчерашних методологий и стандартов.

Библиографический список

1. Атлас новых профессий. Агентство стратегических инициатив // Сколково, 2014. URL: http://asi.ru/upload/iblock/d69/Atlas.pdf.

2. Открытое правительство. Работники в возрасте от 45 до 55 лет будут уволены. // 20.11.2017. URL: http://econbez.ru/news/cat/22727.
3. Программа «Цифровая экономика Российской Федерации» // Распоряжение от 28 июля 2017 года №1632-р. - URL: http://government.ru/docs/28653/.
4. Неизвестный С.И. Социально-психологические проблемы перехода к цифровой экономике // Ученые записки РГСУ – 2018. - Т.17. - №.2(147). - С.5-13.
5. Kitaev A., Mironova I., Pogodaeva A., Sokolov D., Guseva E. Railway station 2.0: a new pattern for the development of the digital railway // International Journal of Open Information Technologies. – 2017. – Т.5. – №.2, - С.85-96.
6. Songdo – Smart City. International Business District. // 2017 URL:http://www.businessinsider.com/songdo-south-korea-design-2017-11/#fifteen-miles-of-bike-lanes-go-through-the-district-connecting-to-a-larger-90-mile-network-in-songdo-city-4.
7. Бурков В.Н., Буркова И.Н. Цифровая экономика и умные механизмы принятия решений // Управление проектами и программами – 2018. - №2.(54). - С.118-125.
8. Безопасность информации в корпоративных информационных системах. Внутренние угрозы. Аналитический Центр InfoWatch [Электронный ресурс] // 2018. – URL: www.infowatch.ru/analytics.
9. Гришин С.Е. Формирование культуры кибербезопасности в обществе актуальная задача современности // Вестник Саратовского государственного социально-экономического университета. – 2011. - №5. - С.170-173.
10. Schwab K. The fourth industrial revolution // World Economic Forum. Cologny, Switzerland. - 2016. 208 с.
11. Мазур М.Ю. Цифровая экономика - вызов для оборонно-промышленного комплекса // Государственное управление. Электронный вестник. – 2018. - №.71, С.226-238.
12. Исаев А.С. Российско-китайское взаимодействие по вопросам обеспечения информационной безопасности. Китай в мировой и региональной политике // История и современность. – 2018. – С.223-238.
13. Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности // Распоряжение Правительства РФ 30 апреля 2015 г. N 788-р. – URL: http://www.pravo.gov.ru.