УДК 338.054.23: 338.242.2: 343.851.3 **DOI: 10.14451/1.189.104**

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДАННЫХ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ

© 2020 **Чернов Сергей Борисович**
кандидат экономических наук, доцент кафедры мировой экономики
и международных экономических отношений
Государственный университет управления, Россия, Москва
Email: chernov_s_b@mail.ru

© 2020 **Новикова Ольга Сергеевна**
аспирант кафедры управления инновациями
Государственный университет управления, Россия, Москва
Email: de.trevier.wife@gmail.com

Дано обоснование необходимости обеспечения безопасности конфиденциальных данных в условиях цифровой экономики. Рассмотрены вопросы трансформации системы управления. Установлена связь между угрозами несанкционированного доступа к данным и коррупционными деяниями со стороны сотрудников организации. Доказано, что при увеличении закрытости системы управления ресурсом возрастает потенциальная возможность коррупционных деяний со стороны сотрудников организации. Выявлены причины незаконного разглашения персональных данных. Выделены объекты защиты, к которым отнесены не только данные, но и информационно-коммуникационное оборудование. Информационная безопасность является немаловажным фактором обеспечения государственной безопасности. Обсуждены функции государства в области обеспечения информационной безопасности в условиях цифровой экономики. Указана необходимость проведения комплексной государственной политики, а также стимулирования разработки и внедрения российской программно-аппаратной продукции и подготовки квалифицированных кадров в области цифровой экономики.

Ключевые слова: цифровая экономика, конфиденциальные данные, информационная и экономическая безопасность, управление.

Текущий этап развития общества можно охарактеризовать интенсивным применением цифровых технологий. Все чаще мы говорим о цифровом обществе, цифровой трансформации, цифровой экономике. Под последней понимается хозяйственная деятельность, в которой в качестве ключевого фактора производства используются цифровые данные.

Выраженной характеристикой развития современного информационного общества является быстрое увеличение значимости данных и информационно-телекоммуникационного оборудования для обеспечения функционирования бизнеса и жизни людей. Роботизация, информатизация, искусственный интеллект и цифровая среда — это звенья научно-технического прогресса современного общества и составные элементы цифровой экономики. Следует отметить, что эффективное развитие последней невозможно без оперативности обработки данных, обеспечения их конфиденциальности и доступности для использования экономическими субъектами [1]. Цифровая экономика основывается на обмене данными в режиме реального времени, а взаимодействие осуществляется с использованием информационно-коммуникационных технологий (ИКТ).

Развитие цифровой экономики сопровождается ростом количества и видов преступлений в IT-сфере. Только за последние пять лет число киберпреступлений возросло в 25 раз с 11 тыс. до 295 тыс., при этом их раскрываемость чрезвычайно низка и не превышает 9% [2]. Поэтому актуальной задачей является обеспечение устойчивости и безопасности цифровизации российской экономики, а это невозможно без существенного трансформирования деятельности российских организаций.

Необходимость трансформации компаний в том числе вызвана тем, что современные потребители товаров и услуг ожидают более быстрое обслуживание, при этом стоимость товара

и услуг должна оставаться конкурентоспособной на рынке. Современные инновационные технологии, дают бизнесу компаний недоступные до этого возможности. Поэтому для сохранения результативности на рынке сегодня и для обеспечения себе будущего, бизнесу необходимо трансформироваться и быть готовым к запуску новых направлений своей деятельности, а также адаптироваться к новым условиям конкурентной среды и применения рядом иностранных государств антироссийских санкций.

На ускорение темпов цифровизации повлияли и новые реалии пандемии, которые более ярко отразили проблемы различных сфер производственной и финансовой деятельности. Подверглась критике система управления компаний, системы обеспечения информационной и экономической безопасности. Новая ситуация заставила пересмотреть ряд аспектов цифровизации. Это связано с угрозами, которые вызваны недостаточным освоением робототехники и искусственного интеллекта для выполнения производственных функции.

Конечно, наилучшим методом противодействия киберпреступности и недопущения несанкционированного раскрытия данных является выработка и соблюдение политики безопасности. Но никакие информационные материалы и производственные совещания не будут иметь большого значения, если не будет выработана внутренняя мотивация персонала организации к обеспечению сохранности данных и активному выявлению ошибок в сфере информационной и экономической безопасности.

Административная власть какого-либо должностного лица над вверенным ему в управление ресурсом при неразвитости внутреннего аудита и других форм внутреннего контроля может порождать условия, способствующие возникновению в организациях случаев коммерческого подкупа персонала, направленного на получение несанкционированного доступа третьих лиц к информационным и другим коммерческим данным. Поэтому при увеличении закрытости системы управления ресурсом возрастает потенциальная возможность коррупционных деяний со стороны сотрудников организации [3, 4].

Цифровизация системы управления компании — это сложный процесс, требующий не только изменения в программно-аппаратном слое, но и корректировку процессов компании, реализации организационно-штатных изменений. Цифровая трансформация превращается в основное конкурентное преимущество современных организаций. Применение цифровых технологий требует переосмысления бизнес-модели компании, умения корректно работать с информацией в цифровом виде, извлекать из нее новые аналитические ценности — новые идеи и знания. При этом безусловно необходимо обеспечивать сохранность и конфиденциальность самих данных. Это связано с тем, что, основываясь на данных, компании имеют возможность развивать традиционные конкурентные преимущества и ставить перед собой следующие задачи:

- приобретать новых клиентов;
- захватывать новые рынки;
- выводить оперативно на рынок новые продукты;
- продвигать персонализированные, кросс-продуктовые и партнерские продукты;
- монетизировать данные;
- активно развивать цифровые каналы;
- обеспечить омниканальность обслуживания клиентов;
- повышать свою экономическую безопасность.

Для реализации данных задач необходимо выполнять углубленную аналитику, основанную на анализе структурированных транзакционных данных компании, а также анализировать изображения, видео, геоинформационные данные, применять технологии машинного обучения [5]. Будет полезен и анализ лингвистических данных. Но также важно обеспечить защиту данных компании от внешних и внутренних угроз, поскольку потеря данных может привести к значительным регуляторным и репутационным рискам.

Применение комплексных мер по использованию и защите данных позволит значительно расширить возможности компании, поменять подходы в работе с клиентами, поскольку для качественного решения данных поставленных задач необходимо:

- иметь в своем активе все возможные данные о клиенте;
- постоянно мониторить и повышать качество данных;
- обогащать информацию из внешних источников;
- постоянно анализировать имеющиеся

клиентские и другие данные;

- внедрять передовые технологии;
- работать с партнерами в одном информационном пространстве.

Работа с данными клиентов относится к работе с одним из наиболее охраняемых государством доменов данных — персональными данными. Под внешними и внутренними угрозами информационной безопасности персональных данных понимаются факторы и условия, которые могут повлечь несанкционированый доступ при их обработке, хранении и использованиив информационно-коммуникационном слое компании. Результатом реализации данных рисков может стать несанкционированное копирование, изменение, блокирование, распространение или уничтожение персональных данных [6].

Очень часто персональные данные разглашаются самими их носителями, которые становятся жертвами мошеннических действий киберпреступников, применяющих средства социальной инженерии. Среди других причин незаконного разглашения персональных данных могут быть технические сбои, компьютерная неграмотность сотрудников, простая небрежность персонала, отсутствие в организациях внутреннего контроля за сохранностью персональных данных, корыстные цели нечестных работников, а также хакерские атаки злоумышленников. Например, в 2017 г. бюро кредитных историй Equifax (США) заявило о хакерском взломе приложения на веб-сайте компании, в результате чего были похищены номера социального страхования, даты рождения, адреса, номера водительских удостоверений 143 млн. человек. Киберпреступники также завладели данными кредитных карт 209 тыс. человек [7].

Получив незаконный доступ к персональным данным, мошенники могут нанести потерпевшим как материальный ущерб, так и моральный вред. Например, они могут:

- оформить кредит в банке и похитить его;
- совершить незаконные действия с чужой недвижимостью;
- похитить денежные средства с банковских карт;
- открыть электронный кошелек для осуществления незаконных операций;
- зарегистрироваться на сайтах знакомств для последующего обмана людей;
- навязывать другим лицам услуги, в том числе незаконные.

Вирус COVID-19 вызвал всплеск киберпреступности и затронул многие страны. С начала пандемии мошенниками зарегистрировано более 4000 сайтов только со словами «коронавирус», covid. При этом возросло на 30% и количество фишинговых рассылок [8].

Использование компаниями технологии «интернет вещей» (IoT) позволяет получать большой объем данных, анализируя который можно выявлять новые знания о закономерностях, получая дополнительные конкурентные преимущества, финансовые и репутационные выгоды. Имея огромное количество данных, необходимо научиться безопасно работать с ними и для этого требуется не только оптимизировать существующий ландшафт программно-аппаратного комплекса, но и менять процессы внутри компании. Должны появиться новые процессы управления данными, в том числе процессы связанные с обеспечением их безопасности.

Имея огромные массивы данных, при их технической доступности и технологической прозрачности, компании сталкиваются и с проблемами недостаточности знаний об окружающей действительности, конъюнктуре рынка. Это связано с тем, что в ходе развития бизнеса компании интенсивно накапливали гигантские объемы данных, не рассматривая вопросы систематизации и управления ими. Интенсивный рост компаний в совокупности с недостаточным пониманием как управлять данными привели к многочисленным утечкам информации. В данной ситуации крайне проблематично извлекать ценные для бизнеса знания из имеющегося массива данных, увеличиваются риски компрометации данных, регуляторные и репутационные риски.

В предыдущие периоды цифровизации функции управления данными, функции информационной безопасности и технический ландшафт компании подстраивались под бизнес-процессы, то теперь бизнес вынужден подстраиваться под требования экономической и информационной безопасности, требования системы управления данными. Адаптация функций управления под новые реалии выполняется и с точки зрения дополнительной автоматизации ручных операций для минимизации рисков несанкционированной передачи данных третьим лицам. В целях минимизации и исключения негативного влияния человеческого фактора, функции контроля все больше стали переносить на автоматизи-

рованные системы управления деятельностью организации. Применяются дополнительные формы и методы контроля за деятельностью персонала. Выполняется пересмотр архитектуры информационно-коммуникационных комплексов для обеспечения минимального количества точек доступа к информационным сервисам компании. Активно создаются сервисы доступа сотрудников к данным, что тоже позволяет минимизировать риски несанкционированного доступа и утечки информации.

Для реализации данных изменений компании уже сейчас начали внедрять комплексные технологические решения в сфере хранения больших объемов структурированных и не структурированных данных, одновременно с техническими решениями по защите данных (например, статическое и динамическое маскирование данных). Технологические решения для работы с большими данными (BigData) обладают мощной аналитической платформой, позволяющей осуществлять поиск или автоматическую обработку данных. Это позволяет создавать новые ниши в исследовании товарных рынков, потребностей текущих и потенциальных клиентов, оптимизации производства.

Крайне важно, предоставляя пользователям информацию, сохранить ее конфиденциальность. Это несомненно большой шаг, который делают компании по пути цифровой трансформации. Однако большой проблемой, с которой сталкиваются компании, является отсутствие отработанных и общепринятых подходов, методик по анализу и защите данных, дефицит квалифицированных кадров, которые могли бы это сделать.

На данный момент имеет место разрыв между технологическим программно-аппаратным слоем, который призван обрабатывать большие данные (BigData) и выполнять их защиту, и потребностями бизнеса в извлечении новых знаний. Этот разрыв должен заполнить методический слой, отсутствующий во многих компаниях. Методика работы с большими данными, покрывающая не только бизнес-задачи, но и вопросы безопасности, должна стать бизнес-инструментом, помогающим трансформировать текущие виды деятельности компании [9].

Требуется разработать методику, которая определила бы корпоративную политику, стандарты, бизнес-процессы и регламенты, направленные на максимальную эффективность и полезность использования данных и знаний компании. Управление ими, в том числе должно быть направлено на обеспечение качества, достоверности и доступности данных. Качество достоверных данных влияет на прибыль, получаемую компаниями. Неполные, неточные или устаревшие данные служат причиной увеличения операционных расходов.

Переход на работу с большими данными потребовал от компаний пересмотреть:

- функцию контроля информационной безопасности и усилить её;
- информационно-коммуникационный ландшафт для создания технической защиты безопасности данных;
- процессы управления с точки зрения их конкретизации и формализации, поскольку необходимо органично вплести функцию обеспечения информационной безопасности в наиболее рисковые места бизнеса;
- функцию контроля экономической безопасности и усилить её, поскольку в условиях централизации данных появляется больше возможностей как для внешнего, так и внутреннего мошенничества.

Таким образом, изменение внешней среды деятельности российских организаций заставляет их неукоснительно выполнять требования информационной и экономической безопасности в системе управления данными, автоматизировать контрольную функцию управления и минимизировать количество точек доступа к автоматизированным сервисам.

Основной целью внедрения системы управления данными является принятие своевременных и правильных управленческих решений, повышающих эффективность хозяйственных процессов организации. Для реализации поставленной цели необходимо выполнить следующие задачи:

- непрерывно улучшать качество данных;
- увеличивать уровень достоверности данных;
- повышать уровень доступности данных;
- создавать механизмы управления данными на корпоративном уровне.

В результате внедрения системы управления данными будет происходить:

- улучшение своевременности принятия управленческих решении за счет скорости получения, качества и достоверности данных;
- рост производительности и прозрачности

бизнес-процессов для осуществления внутреннего аудита;

• уменьшение операционных издержек за счет общей доступности данных и снижения количества дублирующих функций по вводу, анализу, очистке, обогащению данных;

• снижение стоимости владения информационными технологиями за счет максимизации эффекта от интеграции данных, снижения количества ненужных, избыточных или дублирующих данных.

Основой внедрения методики системы управления данными будет являться интеграция бизнеса, людей и технологий. На уровне бизнеса должна быть принята стратегия, направленная на развитие данных как актива компании. Данная стратегия должна поддерживаться первыми лицами организации. Внедряя методологию управления корпоративными данными, необходимо внести изменение в организационную структуру компании, провести организационные преобразования и внести изменения в должностные инструкции сотрудников.

Правильное и эффективное управление данными в сочетании с обеспечением информационной безопасности данных может открыть новые возможности по использованию имеющихся активов компании, для создания новой потребительской ценности, появлению новой бизнес-модели. Это требует изменения или создания новых организационных связей и новой операционной модели взаимодействия субъектов производственных отношений и в корне меняет парадигму функционирования компании, изменяя масштабы ее деятельности и жизненный цикл продукта. Как следствие будет возникать возможность осваивать новые рынки, предлагать новые продукты и услуги.

Для цифровой трансформации в первую очередь нужно по-новому посмотреть на собираемые организацией данные и на их безопасность, выстраивать вокруг данных свой бизнес и уделять им значительное внимание. Следуя парадигме цифровой экономике, становится понятным, что объектом защиты являются не только данные, но и информационно-коммуникационное оборудование. Поэтому на первый план выходят вопросы разделения доступа к ИКТ и накопленным данным, а также проблема маскирования данных.

В настоящее время информационная безопасность является немаловажным фактором обеспечение государственной безопасности [12]. Однако в России наблюдается отставание во многих сферах информационно-коммуникационных технологий, что может привести к потере контроля над информацией и она может перейти к потенциальному противнику, использующему промышленный шпионаж [10]. Поэтому необходимо проводить комплексную государственную политику, направленную:

• на стимулирование разработки и внедрения российской программно-аппаратной продукции;

• на подготовку квалифицированных кадров, способных достигать конкурентных преимуществ в условиях цифровизации экономики на мировых рынках;

• на наказание тех должностных лиц организаций, которые необоснованно требуют и используют без разрешения личную информацию клиентов;

• на усиление ответственности за разглашение персональных данных клиентов.

Отсутствие достаточного количества квалифицированных кадров является одной из главных проблем развития цифровой экономики в современной Российской Федерации. Например, доля ИТ-специалистов в общей структуре занятого населения в России составляет 2,44%, что в 2 раза меньше, чем в США [11].

Таким образом, увеличение подготовки квалифицированных специалистов, способных обеспечить безопасность данных в условиях цифровой экономики, позволит своевременно обрабатывать большие их объемы и использовать результаты анализа для существенного увеличения эффективности различных видов производств, технологий, оборудования, хранения, продажи, доставки товаров и услуг.

Библиографический список

1. *Захарова А.В., Чернов С.Б.* К проблеме национальной безопасности и государственного налогового контроля в условиях цифровизации экономики. // Шаг в будущее: искусственный интеллект и цифровая экономика: smartnations: экономика цифрового равенства. Сборник материалов III Международного научного форума, Москва, 09–10 декабря 2019 г.: Москва, ГУУ, 2020. С. 99–105.

2. Генпрокурора заявила о низкой раскрываемости киберпреступлений. — URL: https://iz.ru/987854/2020–03–17/genprokuror-krasnov-zaiavil-o-nizkoi-raskryvaemosti-kiberprestuplenii (дата обращения: 29.07.2020).
3. *Чернов, С. Б.* Противодействие коррупции в условиях цифровой экономики / С. Б. Чернов // Экономические науки. — 2020. — № 186. — С. 139–144.
4. *Чернов С. Б.* Механизм деловой коррупции и проблемы противодействия. // Государственное регулирование экономики: политико-экономические аспекты. Сборник научных трудов по материалам 5-й Международной научно-практической конференции: Москва, ГУУ, 2018. С. 51–55.
5. *Новикова О. С.* Система управления данными как основа использования искусственного интеллекта на предприятии // Шаг в будущее: искусственный интеллект и цифровая экономика. Революция в управлении: новая цифровая экономика или новый мир машин. Сборник материалов II Международного научного форума, Москва,06–07 декабря 2018 г.: Москва, ГУУ, 2018. С. 277–282.
6. Постановление Правительства Российской Федерации от 01.11.2012 N 1119»Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». — URL: www.consultant.ru/document/cons_doc_LAW_137356/(дата обращения: 08.08.2020).
7. Персональные данные: строго «не» конфиденциально. Как защитить личную информацию. — URL: https://ria.ru/20171205/1508949158.html(дата обращения: 10.08.2020).
8. *Кузнецов С.* Коронавирус породил новые схемы мошенничества. — URL: https://ria.ru/20200413/1569949717.html (дата обращения: 16.05.2020).
9. *Новикова О. С.* Использование современных технологий и систем для обеспечения экономической безопасности предприятия в условиях цифровизации // Анализ социально-экономического состояния и перспектив развития Российской Федерации.Сборник материалов6-й Международной студенческой научно-практической конференции, Москва,02 ноября 2018 г.: Москва, ГУУ, 2019.С. 12–15.
10. *Чернов, С. Б.* Политика противодействия финансированию терроризма: определение и угрозу в условиях развития ранка искусственного интеллекта/ С. Б. Чернов // Экономические науки. — 2019. — № 176. — С 85–91.
11. Кадры в эпоху цифровой экономики. — URL: https://ria.ru/20191230/1562653998.html(дата обращения: 09.08.2020).
12. *Klochkova E, Tyurina Y, Chernov S, Glembotskaya G.* Methods for evaluating economy information potential. Espacios 2019; 40(38):29.