**Глеб Эдуардович Егунов**
*студент специальности «Экономическая безопасность»*
*Тюменского государственного университета, г. Тюмень,* egunov.gleb69@gmail.com
**Алена Вадимовна Кулакова**
*студентка специальности «Экономическая безопасность»*
*Тюменского государственного университета, г. Тюмень,* alenakul3529@gmail.ru
**Юлия Сергеевна Сахно**
*кандидат экономических наук, доцент, доцент кафедры экономической безопасности, системного анализа и контроля Тюменского государственного университета, г. Тюмень,* y.s.sakhno@utmn.ru

# ВЛИЯНИЕ ЦИФРОВОЙ ТРАНСФОРМАЦИИ НА ОБЕСПЕЧЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

**Аннотация.** В статье рассмотрено влияние цифровой трансформации на обеспечение экономической безопасности. Цифровая трансформация ускоряет и упрощает экономические процессы, но при этом несет в себе риски. Специалисту экономической безопасность важно для предупреждения и предотвращения экономических преступлений иметь в своем арсенале современные системы по противодействию экономическим правонарушениям.
**Ключевые слова:** экономическая безопасность, цифровая трансформация, экономическая правонарушения, DLP-системы.

**Gleb Eduardovich Egunov**
*Student of the specialty "Economic Security" at the Tyumen State University, Tyumen,* egunov.gleb69@gmail.com
**Alena Vadimovna Kulakova**
*Student of the specialty "Economic Security" at the Tyumen State University, Tyumen,* alenakul3529@gmail.ru
**Yulia Sergeevna Sakhno**
*Candidate of Economic Sciences, Associate Professor of the Department of Economic Security, System Analysis and Control at the Tyumen State University, Tyumen,* y.s.sakhno@utmn.ru

# IMPACT OF DIGITAL TRANSFORMATION ON ENSURING ECONOMIC SECURITY

**Abstract.** The article considers the impact of digital transformation on ensuring economic security. Digital information speeds up and simplifies economic processes, but at the same time carries risk. It is important foe a specialist in economic security to have modern systems for combating economic offenses in their arsenal to prevent economic crimes.
**Keywords:** economic security, digital transformation, economic offense, DLP systems.

В современном мире многие процессы во всех сферах подвергаются автоматизации и цифровизации. Эти элементы мирового развития также учитываются и в стратегиях стран. Например, в Стратегии национальной безопасности Российской Федерации данные тенденции затрагиваются в социальной, политической, экономической и других сферах. Разберем влияние цифровых изменений на основе экономической безопасности. Российский экономист, доктор экономических наук, профессор, академик РАН Л. Абалкин определяет экономическую безопасность как «совокупность условий и факторов, обеспечивающих независимость национальной экономики, ее стабильность и устойчивость, способность к постоянному обновлению и самосовершенствованию» [1].

Можно сделать вывод, что экономическая безопасность представляет собой систему, в которую включены множество элементов такие, как экономическую независимость, ее устойчивость и стабильность, способность к росту и развитию, поэтому будет логичным выделить ее субъекты и объекты. К субъектам экономической безопасности относятся государственные и местные органы законодательной и исполнительной власти, министерства, организации и граждане страны. К объектам — экономическая система страны в целом и ее отдельные сферы деятельности, например, политическая, военная, правовая, социальная и другие.

Для определения тенденций развития экономической безопасности необходимо выделить следующие задачи, прописанные в Указе Президента РФ от 02.07.2021 № 400 «О стратегии национальной безопасности Российской Федерации» [2]:

1. Обеспечение институциональной и структурной перестройки национальной экономики на современной технологической основе, ее диверсификации и развития на основе использования низкоуглеродных технологий.

2. Сохранение макроэкономической устойчивости, поддержание инфляции на стабильно низком уровне, обеспечение устойчивости рубля и сбалансированности бюджетной системы.

3. Обеспечение устойчивого развития реального сектора экономики, создание высокотехнологичных производств, новых отраслей экономики, рынков товаров и услуг на основе перспективных высоких технологий.

4. Повышение производительности труда путем модернизации промышленных предприятий и инфраструктуры, цифровизации, использования технологий искусственного интеллекта, создания высокотехнологичных рабочий мест.

5. Интенсивное технологическое обновление базовых секторов экономики (промышленность, строительство, связь, энергетика, сельское хозяйство, добыча полезных ископаемых), форсированное развитие российского машиностроения, в том числе приборо- и станкостроения, приоритетное использование отечественной продукции при решении задач модернизации экономики.

Исходя из данных задач можно сделать вывод, что на сегодняшний день важную роль в развитии страны играют информационные технологии и цифровая трансформация, так как они позволяют повысить производительность труда в разных отраслях экономики и предоставляют множество возможностей для роста, улучшить работу с покупателями, сокращают расходы, обеспечивают устойчивое функционирование субъектов экономики, позволяют соответствовать быстро меняющимся условиям окружающего мира.

Впервые информационные технологии были использованы в 1964 г. компанией IBM, которая произвела оцифровку данных. Суть оцифровки состоит в переносе информации с бумажных носителей в электронный формат. В процессе оцифровки содержание и качество информации никак не изменялось, она лишь переходила в электронную форму. На данном этапе информационных технологий была внедрены обработка текстов и электронные таблицы.

Следующим этапом развития стала автоматизация, смысл которой состоял в быстром обмене данными между сотрудниками предприятия, удобным хра-

нением и поиском информации. Это, в свою очередь, ускорило и упростило рабочий процесс, что привело к повышению производительности труда. Крайним этапом является цифровая трансформация экономических систем.

Цифровая трансформация — более сложное понятие, в отличие от оцифровки данных и автоматизации. Она представляет собой не только установку программного обеспечения или современного оборудования, но и полное переосмысление процесса управления, корпоративного учета, а также внешних коммуникаций. На сегодняшний день существует великое множество определений цифровой трансформации. Это связано с тем, что она касается практически всех секторов и постоянно изменяется.

Для дальнейшего исследования представляет интерес определение, данное сайтом РБК: «Цифровая трансформация — это не только инвестиции в новые технологии (искусственный интеллект, блокчейн, анализ данных и интернет вещей), но и глубокое преобразование продуктов и услуг, структуры организации, стратегии развития, работы с клиентами и корпоративной культуры. Иными словами, это революционная трансформация модели организации» [3].

Исходя из национальных целей развития страны, цифровая трансформация является одной из главных на период до 2030 г. Для отслеживания ее развития существует мониторинг, показатели которого представлены в таблице 1.

*Таблица 1*

**Показатели мониторинга развития цифровой трансформации**

| *Показатели* | *Ожидания на 2030 г.* |
|---|---|
| Ключевые сферы экономики | Достижение «Цифровой зрелости» |
| Социальная область | Увеличение доли массовых услуг, доступных в электронном виде до 95% |
| Домашнее хозяйство | Рост доли домохозяйств, которым обеспечен доступ к интернету до 97% |
| Область информационных технологий | Увеличение вложений в отечественные решения в четыре раза по сравнению с 2019 г. |

Источник: составлено авторами на основе данных [4].

В ракурсе популярного доказательного подхода к принятию решений запрос на количественные оценки процесса цифровой трансформации обычно формируются с точки зрения следующих критериев:

1. Операционные, управленческие и организационные процессы.
2. Управления информацией и данными.
3. Разработка и внедрение новых цифровых технологий, управление информационными технологиями.
4. Качества услуг и товаров.
5. Окружения или среды (ресурса предприятия, регулирование).
6. Защищенности данных и инфраструктуры.
7. Финансирования (затраты, возвраты на инвестиции).
8. Отношение к новым цифровым технологиям.

Каждый отдельный показатель может иметь собственные показатели.

Аналитики высказывают мнение о том, что выявление и измерение цифровой трансформации является важным процессом для современного мира — в том числе в силу распространения социальных опасений относительно сохранности персональных данных и неприкосновенности частной жизни, а также неопределенности итогов цифровой трансформации [4].

Цифровая трансформация, как и любые новые технологии, помимо упрощения и улучшения различных процессов несет в себе риски. Основными рисками в социально-экономической сфере для данной отрасли являются [5]:

– угроза «цифровой безопасности» страны и пересмотр роли государства в международном мире «Цифровой» экономики;
– уменьшение уровня сохранности данных;
– снижение количества рабочих мест низкой и средней квалификации;
– прирост уровня сложности бизнес-моделей и схем их взаимодействия;
– быстрое повышение конкуренции во всех сферах экономики;
– трансформация моделей поведения производителей и потребителей.

Одним из основных рисков цифровой трансформации является утечка информации.

В 2020 г. Экспертно-аналитический центр InfoWatch зарегистрировал 404 случая утечки данных из коммерческих и некоммерческих (государственных, муниципальных) организаций в России. В 2019 г. было зарегистрировано 395 утечек, что на 2,2% меньше, чем в 2020 г. Также в 2020 г. было зарегистрировано более 100 миллионов утечек записей платежной информации и персональных данных. Около 20% всех утечек в России происходят через канал мгновенных сообщений, то есть мессенджеры, остальные 80% — в результате умышленных действий, из которых 21% утечек были спровоцированы внешними нарушителями, 79% — внутренними. Стоит отметить, что доля утечек умышленного характера по вине внутренних нарушителей увеличилась с 38,7% до 79,3% [6].

Одним из основных направлений работы службы экономической безопасности является защита активов организации и минимизация рисков их утраты и / или обесценивания. Признаки многих способов хищения информации могут быть обнаружены с помощью DLP-систем, которые анализируют информационные потоки предприятия по различным каналам: интернет, мобильная связь, мессенджеры, электронная почта, локальная вычислительная сеть, устройства печати. Для выполнения ранее озвученной задачи, в DLP-систему загружено множество данных баз контекстной фильтрации, то есть она оснащена средствами контекстного анализа и предиктивной аналитики. Также данную систему можно обучить специфическому языку конкретного предприятия. Именно поэтому на основе принципов выявления хищений в различных потоках данных с высокой точностью можно сигналы о подготовке или совершении экономических преступлений, например, таких как: отправка конкурентам данных конкретного предприятия, внутреннего хищения, преступного сговора с контрагентами и т. д.

К сожалению, сотрудники служб экономической безопасности во многих компаниях до сих пор лишены возможности использовать системы DLP в своей

работе, поэтому они вынуждены по старинке запрашивать у служб информационной безопасности детали переписки подозреваемых личностей, что существенно ограничивает их возможности.

Важность DLP-систем, как инструмента сотрудника экономической безопасности заключается в том, что с помощью данных систем возможно контролировать такие данные, как:

– каналы компьютерных коммуникаций и информацию, передаваемую по ним;

– объекты хранения информации (жесткие диски, съемные накопители, облачные ресурсы, корпоративные файловые хранилища и прочее);

– соответствие передачи, получения и хранения информации правилам организации;

– действия пользователей (вход в корпоративную систему, соответствие пользователей учетной записи, со служебными и личными мобильными и другими подключаемыми ресурсами, посещения интернет-ресурсов, геолокация, размещение постов в различных соцсетях и другие действия);

– соответствия действий пользователя правилам;

– сводную активность пользователя и различные аномалии активности.

Современная DLP-система имеет возможность получать и анализировать информацию из корпоративных систем путем интеграции с ними, что в разы расширяет базу анализа и позволяет контролировать гораздо больше действий сотрудников в сравнении с возможностями агентов экономической безопасности только в рабочих станциях.

Для выявления фактов корпоративного мошенничества недостаточно только функционала, который служит фундаментом аналитической работы и позволяет решать задачи технического характера, также необходимы методики анализа и алгоритмы выявления инцидентов. На сегодняшний день методики анализа разрабатываются с учетом применения технологий машинного оборудования, что при внедрении позволяет сотруднику безопасности фокусироваться только на существующих событиях, ко с другой стороны — существенно снижает требования к квалификации и опыту операторов, осуществляющих повседневную деятельность.

Актуальной проблемой на сегодняшний день остается отсутствие доступа специалистов в области экономической безопасности к использованию DLP-систем, так как данные системы распространены как инструмент служб информационной безопасности. В связи с тем, что возможности DLP-систем в большинстве случаев неизвестны руководителям служб экономической безопасности, они не рассматривают этот инструмент решения задач и не могут сформулировать обоснование закупки и требования к системе.

В свою очередь, с помощью системы DLP сотрудники сферы экономической безопасности могут решить ряд задач таких, как [7]:

1. Выявление и предотвращение корпоративного мошенничества (хищение из компании, хищение при закупках и продажах, использование ресурсов компании в личных целях).

2. Выявление групп риска, то есть работников, имеющих склонности, увлечения, которые использованы для ведения или привлечения к незаконной

деятельности, к деятельности в ущерб компании, ее руководству или работникам.

3. Получение и закрепление доказательств совершения противоправных действий.

4. Минимизация последствий от противоправных действий.

5. Совместно со службой информационной безопасности выявление и предотвращение неумышленных утечек или уничтожения, искажения информации, представляющей ценность для компании, включая получение сигналов о попытке и факте несанкционированных действий, в том числе при наличии легального доступа.

6. Выявление признаков конфликта интересов.

Цифровая трансформация вносит свои изменения во все экономические процессы. Данная тенденция несет в себе, помимо усовершенствования и упрощения процессов производства и экономического взаимодействия, большое количество рисков. Главной проблемой, по которой данные риски не могут быть предотвращены, является отсутствие у сотрудников служб экономической безопасности достаточной оснащенности инструментами, необходимых для предупреждения и выявления экономических правонарушений. При обеспечении сотрудников экономической безопасности необходимыми инструментами, значительно снизится количество совершаемых правонарушений, что, в свою очередь, приведет к более стабильному развитию экономических сфер. Глобально это может привести к укреплению положения экономической безопасности в разрезе национальной безопасности страны.

**БИБЛИОГРАФИЧЕСКИЙ СПИСОК**


1. Абалкин Л.И. Экономическая безопасность России: угрозы и их отражение. Вопросы экономики. 1994. С. 4-13.
2. О стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 02.07.2021 № 400 // Официальный интернет-портал правовой информации: [сайт]. 2005–2022. [дата публ. 03.07.2021]. URL: http://publication.pravo.gov.ru/Document/View/0001202107030001 (дата обращения: 31.03.2022).
3. Что такое цифровая трансформация? // РБК. [сайт]. 1995-2022. URL: https://trends.rbc.ru/trends/innovation/5d695a969a79476ed81148ef (дата обращения 01.04.2022).
4. Цифровая трансформация: изменения экономики и социальной сферы под влиянием технологий // Научно-образовательный портал IQ. [сайт]. 1993-2022. URL: https://iq.hse.ru/news/465484100.html (дата обращения 08.04.2022).
5. Кешелава А.В. Введение в «Цифровую» экономику // На пороге «цифрового» будущего. 2017. С. 14-15.
6. Россия: утечки информации ограниченного доступа // Экспертно-аналитический центр InfoWatch. [сайт]. 2021 С. 5-8. URL: https://www.infowatch.ru/sites/default/files/analytics/files/c_IW_Россия_2020_утечки_v%201%207%201пп%20(2).pdf (дата обращения 10.04.2022).
7. DLP и экономическая безопасность // Экспертно-аналитический центр InfoWatch. [сайт]. 2003-2022. URL: https://www.infowatch.ru/sites/default/files/analytics/files/dlp-i-ekonomicheskaya-bezopasnost-otchyot-po-rezultatam-issledovaniya.pdf (дата обращения 31.03.2022).