УДК 330.34 **DOI: 10.14451/1.196.191**

ЗНАЧЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ В ИННОВАЦИОННОМ РАЗВИТИИ РЕГИОНА

© 2021 **Сураева Мария Олеговна**
Самарский государственный экономический университет, Россия, Самара
E-mail: marusyasuraeva@mail.ru

© 2021 **Попова Екатерина Сергеевна**
Самарский государственный экономический университет, Россия, Самара
E-mail: popovaks07@yandex.ru

В статье рассматриваются важность системы экономической безопасности в развитии регионов и страны в целом. Описаны шесть ключевых критериев экономической безопасности, которые позволяют оставаться конкурентоспособными на международной арене, повышать уровень жизни населения. Было доказано, в цепочке решения задач задействованы отдельные предприятия и организации, которые на уровне регионов создают конкурентоспособный продукт или услугу, обеспечивают ими национальную экономику, повышая уровень инновационного развития государства. Дана характеристика кибер–устойчивого бизнеса, определены основные его принципы. Предметом исследования является система экономической безопасности. Объектом исследования выступает экономическая безопасность в «Сбере». Степень разработки находится на уровне теоретического и практического применения. Были рассмотрены работы ведущих специалистов в области экономической безопасности и диджитализации, развития и разработок, такие как: Диогенес, Чио К., Фриман Д., Годунова Г. Н. и другие.

Было выявлено, что кибер–устойчивый бизнес ориентируется на непрерывность своего бизнеса, устойчивость к проактивному предпринимательству и обеспечивает стабильность экономики. Он применяет различные стратегии эконмической безопасности, чтобы быстро реагировать на возможные угрозы, зачастую он может минимизировать ущерб и продолжать работу под атакой. инновационные возможности у компании создаются за счет других следующих составляющих: внешние и внутренние условия, которые оказывают особое влияние на инфраструктуру инновационного потенциала, потому что их существенное развитие прямо сказывается на эффективности функционирования всей компании. Было выявлено, что организации должны смотреть за «пределы своих четырех стен» (принцип «think outside the box»), чтобы защитить свои бизнес экосистемы и цепочки поставок.

Было доказано, создание киберпространства принимает командную работу, поскольку объединяет сотрудников, поставщиков, альянс партнеров, правоохранительные органы и даже конкурентов, так как каждый преследует свою цель и имеет свою роль в процессе. Было проанализировано, кибератаки составляют 40% нарушений безопасности, поскольку включают в себя еще и косвенный характер. Они нацелены на слабые связи в цепочке поставок или на всю бизнес-экосистему. Поэтому нередко происходит размытие истинных масштабов киберугроз.

Ключевые слова: экономическая безопасность, инновации, развитие региона, кибербезопасность, кибер–устойчивый бизнес, искусственный интеллект, цифровизация, конкурентоспособность.

Развитие системы кибербезопасности, на первый взгляд, сегодня усиливается, а киберустойчивость только растет. Большинство организаций становится более защищённее, поскольку обеспечивают предотвращение прямых кибератак. Но форма кибербезопасности со стороны злоумышленников уже переходит на иные косвенные цели, когда сотрудничество идет с новыми поставщиками и другими третьими лицами в создании цепочки поставок. Это та ситуация, когда необходимо создавать новые способы борьбы еще до того, как будет планироваться кибератака. В то же время с каждым годом происходит увеличение стоимости системы кибербезопасности, что влияет на инвестиции в данную сферу. В результате многие организации сталкиваются с точкой невозврата: приходится делать выбору в пользу переливания денежных

средств в пользу экономической безопасности и подгонять ее под инновационный путь развития в эпоху цифровизации.

Создается кластер двух основных групп: первая составляет 17% (те компании, которые достигают более высоких уровней производительности по сравнению с остальными, они устанавливают свой курс на инноватику), вторая группа включает в себя подавляющее большинство — 74% (компании, которые в среднем занимаются кибербезопасностью, но не ставят ее приоритетной задачей). В итоге, на рынке появляются два игрока: лидеры, задающие тренд на инновационную систему экономической безопасности, и средние исполнители, которые наблюдают и некоторые модели внедряют в свой рабочий процесс. Лидеры постоянно масштабируют усилия и привлекают новые ресурсы для сотрудничества. Но важно помнить, что быть инновационным в экономической безопасности сильно отличается от любого другого аспекта бизнеса. В данном случае необходимо придерживаться осторожной тактике, поскольку эта сфера является наиболее уязвимой.

Экономическая безопасность рассматривается с точки зрения шести основных критериев [2]:

1. Пространственный (производится оценка мирового уровня воздействия на формирование международной экономической безопасности, государственного уровня экономической безопасности страны, регионального уровня раскрытия экономической безопасности региона, локального уровня экономической безопасности организации);

2. Социально–направленный (рассматривается экономическая безопасность личности и всего общества на степень защищенности от внутренних и внешних угроз);

3. Информационный (неотъемлемая часть экономической безопасности, опирается на большой объем информации, которая является гарантом лидерства в экономической сфере);

4. Инновационный (опирается на уникальные инновационные решения и разработки, которые позволяют достигать лидирующие позиции в ведущих отраслях экономики, повышая конкурентоспособность страны);

5. Экологический (оценивает степень предотвращения противоречий между обществом и средой обитания);

6. Критерий обеспеченности определенным ресурсом (оценивает обеспеченность государства сырьем и продовольствием, которые реализуют эффективное функционирование национальной экономики).

Поэтому выделяют кибер–устойчивый бизнес, который объединяет все возможности системы кибербезопасности в рабочую среду, ориентируется на непрерывность своего бизнеса, устойчивость к проактивному предпринимательству и обеспечивает стабильность экономики. Он применяет различные стратегии эконмической безопасности, чтобы быстро реагировать на возможные угрозы, зачастую он может минимизировать ущерб и продолжать работу под атакой [3]. В результате кибер-устойчивый бизнес может надежно внедрить инновационные предложения и бизнес-модели, укреплять доверие клиентов и расти с уверенностью, усиливая значение экономической безопасности в развитии региона и страны в целом.

Огромное значение для развития регионов имеет уровень развития экономической безопасности [1]. Хорошая новость заключается в том, что большинство организаций тратят 10,9% своего бюджета на разработку и внедрение программ кибербезопасности. Так делает вторая группа компаний. Лидеры же отправляют 11,2% бюджета, что является недостаточным для достижения более высоких уровней производительности. Их инвестиции в передовые технологии, такие как искусственный интеллект, машинное обучение или роботизированная автоматизации бизнес-процессов, существенно растут [11]. Какая же сегодня наблюдается тенденция: 84% организаций переводят более 20% бюджета на систему кибербезопасности в сторону тех инструментов, которые включают в себя все технологии в качестве фундаментальных компонентов. При чем лидеры с каждым годом увеличивают процентное соотношение распределение денежных средств в сторону экономической безопасности. Три года назад только 41% лидеров отправляли более 20 процентов своих бюджетов в систему кибербезопасности.

То есть тренд на развитие экономической безопасности за счет трансформации системы кибербезопасности актуален и прогрессивно растет [4]. Фактически, более чем четыре из пяти компаний утверждают, что инструменты кибербезопасности значительно продвинулись в течение последних нескольких лет и заметно улучшают киберустойчивость своей организации.

Возможность точно оценить количество кибератак против организации зависит от способности каждой организации обнаруживать их. С другой стороны, нарушения безопасности являются реальными событиями и могут быть более точно зафиксированы. Например, общее количество кибератак упало на 11%, от 232 до 206 целевых атак. В то же время около 27% атак серьезно подрывают экономическую безопасности.

Если провести более глубинный анализ, то кибератаки составляют 40% нарушений безопасности, поскольку включают в себя еще и косвенный характер. Они нацелены на слабые связи в цепочке поставок или на всю бизнес-экосистему. Поэтому нередко происходит размытие истинных масштабов киберугроз. А сложность глобальных цепочек поставок, включая регуляторные требования различных регионов и стран, добавляют свои сложности.

Это приводит к тому, что организации должны смотреть за «пределы своих четырех стен» (принцип «think outside the box»), чтобы защитить свои бизнес экосистемы и цепочки поставок. В среднем компании защищают только 60% своего бизнеса и экосистемы организации. Но целых 40% нарушений проходят через этот маршрут. Средняя стоимость за атаку составляет 380 000 долларов за инцидент в крупных фирмах. В такой среде сложнее оставаться на конкурентоспособной волне. 83% топ — менеджмента считает, что их организации должны думать за пределами своих предприятий и предпринять шаги для обеспечения эффективности своих экосистем [5].

Практика показывает, что 81% членов советов директоров хранят на своих телефонах закрытую и дорогостоящую информацию. К тому же 29% топ-менеджмента предпочитают общаться с другими членами советов директоров с помощью личной электронной почты. Учащаются случаи копирования SIM-карт, как это было в Москве в 2020 году, когда у бизнесмена были сняты 26 млн. рублей с его личного счета и со счета организации, который был привязан к тому же мобильному номеру. Был тотальный контроль над банковскими приложениями, поэтому не стоит недооценивать возможности киберпреступников.

Теперь создание киберпространства принимает командную работу, поскольку объединяет сотрудников, поставщиков, альянс партнеров, правоохранительные органы и даже конкурентов, так как каждый преследует свою цель и имеет свою роль в процессе. Около 15% лидеров рынка имеют более 500 000 записей клиентов, выставленные через «CyberAttacks» портал за последние 12 месяцев. Это говорит о том, что альянс лидеров способен быстро реагировать на нарушения и начинать оперативное их исправление, уменьшая общий ущерб компании [9]. безопасности раньше, чтобы уменьшить общий ущерб. Учитывая конечные ресурсы системы безопасности, существует высокая ценность в управлении данными, ориентированными на бизнес — процессы. Это может означать введение управляемых услуг или серверов, способных усилить систему безопасности и сохранности данных в организации, направленному на широкие объемы и массивы данных. Все это создает целостность экосистемы, но многим организациям трудно согласовать уровень их инвестиций в инновации с результатами киберпространства для своего бизнеса [10].

Каким образом борется кредитно–финансовые учреждения, например, с подобными атаками, ведь в данный сектор совершаются постоянные угрозы. «Сбер» активно использует, разрабатывает и внедряет ИИ-технологии, которые завоевали доверие со стороны специалистов и клиентов. На сегодняшний день ИИ уже зарекомендовал себя как зрелая промышленная технология, которая помогает решать сложные профессиональные задачи в самых разных сферах. В «Сбере» борьба с киберпреступностью ведется сразу по нескольким направлениям. Первое состоит в защите ключевых банковских систем, где хранятся все сведения о счетах и клиентах. Второе включает подходы к разработке продуктов и участию безопасности в этих процессах. Если раньше разрабатывались новые продукты, а только потом производился анализ их безопасности, то сегодня «Сбер» еще при обсуждении концепции создания продукта уже устанавливает для программистов некие безусловные принципы безопасности, которые реализуются в программном коде. Следующее направление работы — это клиентская защита.

Любому правонарушению противостоит фрод-мониторинг «Сбера», в основе которого лежит искусственный интеллект. Его показатель эффективности сегодня составляет около 97%. Операции, которые являются мошенническими, банк умеет хеджировать и не допускать совершения преступления. Так, благодаря системе

фрод-мониторинга банку удалось предотвратить хищение средств клиентов на 25 миллиардов рублей [6].

«Сбер» совместно с «Московским университетом Министерства внутренних дел РФ имени В. Я. Кикотя» будет вести работу в области киберпреступности. В рамках соглашения университет продолжит осуществлять подготовку специалистов по направлению информационной безопасности и противодействию преступлениям в сфере информационных технологий. Стороны планируют проводить практико-ориентированные занятия учащихся университета в банке, адаптировать образовательные программы, реализовывать совместные научно-исследовательские и прикладные проекты и разрабатывать предложения по совершенствованию законодательства в области противодействия киберпреступности.

Так как ведется активная цифровизация, банк сокращает количество банкоматов и переводит клиентское обслуживание в режим «онлайн», тем самым увеличивая риск атак. По итогу 2020 г. число ежемесячно активных пользователей «Сбербанка онлайн» в сравнении с 2019 г. возросло до 65 млн., это больше на 19%. Ежедневная аудитория показали еще больший, 31-процентный рост — до 32 млн. человек [6]. В таблице 1 представлены основные принципы этической составляющей системы ЭБ, которые способствуют борьбе с кибератаками и преступностью, а также повышают степень развития регионов, усиливая их шансы на международной арене.

Например, для реализации подобных принципов этических вопросов в области ИИ и экономической безопасности в «Сбере» создана специальная рабочая группа в рамках Комитета ESG [6]. Она стала первым в России специальным органом для спорных этических вопросов ИИ. И в целом, банк можно отнести к лидерам рынка и кибер–устойчивому бизнесу, поскольку «Сбер» расширил своё присутствие за пределами финансового рынка и вошёл практически во все цифровые индустрии, и теперь компании Группы могут покрыть все конечные потребности клиентов в цифровом мире.

При этом «Сбер» не просто цифровизирует отдельные продукты или сервисы, а трансформирует целые рынки и создаёт новые. Будет интегрирована цифровая платформа «Platform V», которая является ключевой технологической инвестицией и фундаментальной составляющей опорной стратегии банка, на которой базируются все планы развития финансового и нефинансового бизнеса [6]. Решается вопрос с

Таблица 1. **ключевые принципы системы экономической безопасности**

Принцип	Область применения
Secure AI: Контролируемость и управляемость систем	Разработка и применение технологий ИИ должны быть безопасными, управляемыми и контролируемыми в максимально возможной степени. Компания должна учитывать возможные риски, связанные с безопасностью технологий ИИ, и не допускать их выхода из-под контроля или причинения системой ИИ вреда человеку. Внедрение ИИ никогда не является самоцелью, а применяемые технологии должны пользоваться доверием клиентов, сотрудников и общества.
Explainable AI: Прозрачность и предсказуемость функционирования	Компания несет ответственность за применение систем ИИ в своей деятельности и стремится обеспечивать максимальную прозрачность, внутренний контроль и предсказуемость процесса и результатов их работы. Технологии ИИ должны применяться с соблюдением законодательства, в том числе требований конфиденциальности, и с уважением к частной жизни человека, а также к коммерческой тайне. Системы ИИ никогда не используются для незаконной обработки персональной информации граждан или информации корпоративных клиентов.
Reliable AI: Стабильность и надежность систем	Организация должна обеспечивать стабильность и надежность функционирования систем ИИ и необходимый уровень технического оснащения, создает условия наибольшего благоприятствования для разработки и внедрения надежных систем ИИ. Компания реализует высочайший уровень гарантий всех прав и свобод человека при применении ИИ, поддерживая применение технологий ИИ исключительно на законных основаниях.
Responsible AI: Ответственное применение	При внедрении ИИ в центре внимания компании всегда находится потребность клиентов и сотрудников, а технологии ИИ должны использоваться для улучшения клиентского опыта. Организация принимает во внимание и ответственно относится ко всем опасениям, которые возникают в связи с применением технологий ИИ.
Fair AI: Непредвзятость	Технологии ИИ применяются компанией справедливо и объективно на равных для всех условиях. Она стремится к тому, чтобы технологии ИИ приносили пользу для развития человечества.

созданием единого (бесшовного) и максимально персонального пути клиента с помощью объединяющих элементов и предложений, а также развиваются продукты благосостояния населения, тем самым помогает развитию регионов в рамках всей страны. В этом также велика роль экономической безопасности, которая лежит в основе стратегического курса и развития всего бизнеса в эпоху цифровизации.

Таким образом, сегодня активно складывается целостная экосистема, которая базируется на ключевых принципах системы экономической безопасности, когда во главе стоит проактивный лидер и топ–менеджер, задающий курс компании. Экономическая безопасность тесно связана с политическими, экономическими задачи, которые опираются на национальные интересы государства. Она позволяет оставаться конкурентоспособными на международной арене, повышать уровень жизни населения. В цепочке решения задач задействованы отдельные предприятия и организации, которые на уровне регионов создают конкурентоспособный продукт или услугу, обеспечивают ими национальную экономику, повышая уровень инновационного развития государства. Но вопросы кибератак все больше ставятся на повестку дня, ведь с каждым днем появляются новые способы и методы хакерских угроз.

Библиографический список

1. *Ахмедуев А.Ш., Меджидов З. У.* Теоретические аспекты о сущности и роли территорий с особым экономическим статусом в обеспечении пространственного развития регионов России. Вопросы региональной экономики. 2019. № 40(3). С. 3–7.
2. *Годунова Г. Н.* Экономическая безопасность в системе национальной безопасности. Московский экономический журнал. 2019. № 11. С. 1–7.
3. *Диогенес Ю., Озкайа Э.* Кибербезопасность: стратегии атак и обороны. // ДМК Пресс. 2020. С.326.
4. *Запечников С. В.* Информационная безопасность открытых систем. / Средства защиты в сетях / С. В. Запечников, Н. Г. Милославская, А. И. Толстой, Д. В. Ушаков. // М.: ГЛТ. 2018. С. 558.
5. *Мезенина Е. В.* Инновационная стратегия развития организации // Инновационная Росссия; Модернизация, Инновации, Развитие. URL: http://econf.rae.ru/article/6533 (дата обращения: 29.03.2021).
6. *Самиев П.А., Закирова В. Р., Швандар Д. В.* ЭКОСИСТЕМЫ И МАРКЕТПЛЕЙСЫ: ОБЗОР РЫНКА ФИНАНСОВЫХ УСЛУГ. Финансовый журнал. // Цифровизация финансовых услуг. 2020. С. 1–13.
7. *Сураева М. О.* Развитие компенсационных систем в сфере регулирования трудовых отношений через инструменты менеджмента //Экономика и бизнес: управление экономическими системами. 2015. С. 1–13.
8. *Сураева М. О.* Инновационное развитие предприятий промышленного комплекса // Экономика и управление. № 1(11).2020. С. 66–69.
9. *Суржиков М. А.* Формирование инновационной стратегии на предприятии // Вестник Адыгейского государственного университета. Серия 5: Экономика. 2016. № 2 (180). URL: https://cyberleninka.ru/article/n/formirovanie-innovatsionnoy-strategii-na-predpriyatii. (дата обращения: 29.03.2021).
10. *Сысоева Е.А.* РАЗВИТИЕ ИНФОРМАЦИОННОГО ОБЩЕСТВА В РЕГИОНАХ РОССИЙСКОЙ ФЕДЕРАЦИИ. Вестник Волжского университета им. В. Н. Татищева. 2021. № 1(2). С. 1–16.
11. *Чио К., Фриман Д.* Машинное обучение и безопасность. // ДМК Пресс. 2020. С. 390.