УДК 338.054.23
DOI: 10.34020/1993-4386-2024-1-98-107

НИВЕЛИРОВАНИЕ ЦИФРОВЫХ УГРОЗ КАК СРЕДСТВО ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННОМ МИРЕ

К. Е. Следнева
Омский государственный университет путей сообщения (ОмГУПС),
Омск, Россия
Т. Б. Кувалдина
Омский государственный университет путей сообщения (ОмГУПС),
Омск, Россия

В эпоху цифровизации, где развитие технологий тесно связано с экономическим процветанием, важно осознать угрозы, которые несет современный мир. Действительно, цифровая трансформация открывает новые горизонты для общественных сфер жизни, переплетая инновационные технологии с повседневными задачами, активно стимулируя социальный прогресс. Однако, по мере увеличения зависимости от новых технологий, усиливается влияние цифровых угроз на экономическую стабильность и безопасность. В основе привлекательности таких инцидентов лежат относительная дешевизна и доступность, что делает их более предпочтительными для злоумышленников по сравнению с другими видами преступлений. Различного рода атаки и вредоносные действия, такие как вирусы, фишинг, вредоносные программы, кибератаки, могут нарушить не только работу компаний, но и подорвать их финансовое положение в целом. На этом этапе проблема цифровых угроз превращается в глобальное явление, затрагивающее каждого – от обычных граждан до крупных компаний и государственных органов. Важно осознавать данную проблему, ведь без должного противодействия этим вызовам экономические потери от киберпреступлений будут только увеличиваться. Предотвращение подобных атак и сокращение их последствий требуют поиска комплексного подхода. Именно поэтому в статье рассматривается не только вопрос о том, какие негативные последствия несут цифровые угрозы, но и предлагаются необходимые, по мнению авторов, методы и стратегические решения, направленные на снижение экономических потерь в процессе постоянно меняющихся условий.

Ключевые слова: цифровые угрозы, нивелирование, экономические потери, инциденты, стратегии, экономическая безопасность.

Переориентация с традиционных методов и подходов в управлении, производстве, общении на цифровую технологическую парадигму обусловлена стремлением общества адаптироваться к быстро изменяющемуся внешнему окружению. Раскрытие новых перспектив для инноваций вместе со стремлением к увеличению эффективности и развитию предоставляют значительные возможности для изменения социальных структур, совершенствования форм межличностного взаимодействия.

В условиях перехода к цифровой экономике особое значение приобретают свойства адаптации, надежности функционирования и устойчивости секторов экономики[1], они не только испытывают на себе влияние цифровизации, но, оказывая значительное воздействие на разнообразные сферы деятельности, определяют направление, скорость цифровой трансформации, открывая новые горизонты для рыночных возможностей, инновационных идей, реализации уникальных проектов. Цифровизация ведет к значительным изме-

[1] *Сектор экономики* представляет собой совокупность отдельных институциональных единиц, имеющих некоторые сходства, основанные на единстве экономических целей и функций, которые призваны способствовать наиболее эффективному и успешному функционированию национальной экономики. Согласно Руководству по статистике государственных финансов 2014 г., экономика страны делится на пять взаимоисключающих институциональных секторов (ИнсС). Этими пятью ИнсС (секторами национальной экономики) являются: сектор нефинансовых корпораций (организаций); сектор финансовых корпораций (организаций); сектор государственного управления; сектор домашних хозяйств; сектор некоммерческих организаций, обслуживающих домашние хозяйства. Определения и описания институциональных секторов полностью согласованы с соответствующими определениями и описаниями в главе 4 Системы национальных счетов (СНС) 2008 г. [1, с. 19-20].

нениям в спросе на рабочую силу, увеличивая потребность в квалифицированных IT-специалистах в ключевых областях цифровой экономики.

В ходе процессов цифровой трансформации бизнеса крупные организации, как и индивидуальные предприниматели, сталкиваются с необходимостью кардинального пересмотра своих бизнес-моделей, процедур, способов взаимодействия с покупателями, обществом в целом. Те, кто гибко, успешно адаптируются к новым условиям, получают значительные конкурентные преимущества, выделяясь на рынке высокой лояльностью клиентов и способностью быстро реагировать на изменения в потребностях и предпочтениях потребителей. При этом экономическое развитие, опирающееся на внедрение последних цифровых инноваций, создание новаторских материалов, анализ огромных объемов данных и внедрение передовых управленческих систем, приводит к коренному изменению принципов конкуренции.

С точки зрения И. С. Крикунова, в таком контексте цифровая экономика переформатирует представления об экономической безопасности на различных уровнях – от государственного до индивидуального, из-за новых методов ведения бизнеса, обмена информацией, взаимодействия с рынком, способствуя появлению новых типов рисков для всех участников экономических отношений [2, с. 18]. Поэтому приходится решать не только задачу интеграции современных технологий с целью улучшения своего позиционирования на рынке, но и задачу создания надежных механизмов защиты в условиях повышения уровня цифровой угрозы, делая акцент на предотвращение, минимизацию потенциального ущерба.

Влияние такого рода инцидентов способно иметь широкий размах, начиная от нарушений в работе критически важной инфраструктуры и заканчивая парализующим эффектом на дестабилизацию финансовых рынков. Поэтому А. В. Бойкова справедливо отмечает, что в условиях современности более чем когда-либо государственный и частный сектор нуждаются в эффективных инструментах, способных обеспечить высокий уровень защищенности финансовых транзакций, бизнес-процессов, финансовых данных, информационных активов и т.д. [3]. О необходимости изменения условий защищенности экономики России в рамках национальной безопасности также высказываются Л. С. Есенжулова и Н. Б. Дроковский [4].

Углубление в цифровую эпоху неизбежно ведет к тому, что экономическая активность становится уязвимой перед использованием информационных технологий для осуществления вредоносных действий, включающих в себя: фишинг, распространение вирусов и вредоносного программного обеспечения, атаки распределенного отказа в обслуживании и вмешательство в цепочку поставок, кражу и манипулирование персональными данными, кибершпионаж и др. По мнению Д. В. Удалова, все это лишь некоторые проявления цифровых угроз, способных принести серьезный ущерб, классифицирующихся по различным критериям – в зависимости от источника, методов проникновения, цели и последствий [5, с. 16]. Кроме того, как считают Т. А. Саадулаева и М. М. Белановский, развитие цифровой экономики и платформ ведет к монополизации, рискам в сфере конфиденциальности и прав человека [6].

Сетевое пространство допускает две основные формы цифровых экономических преступлений, в основе которых лежат объект или метод осуществления. В зависимости от подхода, эти нарушения подразделяются на те, что основаны на манипуляции человеческими психологическими характеристиками (обман, угрозы, убеждение), и на те, что осуществляются через прямое использование технологического оборудования (компьютеры, смартфоны, маршрутизаторы и др.). Разделение обусловлено тем, что в первую группу преступлений входят виды деятельности, потенциально опасные для общества, при которых ущерб наносится в основном только объекту – экономическим отношениям. Атаки, ориентированные на получение денежных средств от жертв, быстро становятся одним из наиболее распространенных и серьезных видов цифровых угроз. Данная тенденция объясняется несколькими факторами. Во-первых, главной мотивацией для киберпреступников выступает финансовый аспект. Для них деньги представляют высокую ценность и легкость в реализации. Во-вторых, по мере того, как экономика и повседневная жизнь людей становятся более зависимыми от современных технологий, число пользователей, систем или устройств, которые могут стать объектом кибератак, возрастает. Это происходит из-за того, что больше данных и финансовых операций перемещается в онлайн-пространство, где их можно перехватить, украсть или иным образом скомпрометировать. В-третьих, цифровые атаки позволяют киберпреступникам действовать удаленно, избегая прямых физических рисков, возможной опасности для себя, обходя физические барьеры, оперируя лишь компьютером и Интернетом. Д. А. Галстян делает вывод, что анонимность действий, способность осуществлять операции из различных стран делают преступников трудно отслеживаемыми, при этом снижает необходимые затраты в сравнении с остальными преступлениями, что, в свою очередь, приводит к росту подобных неправомерных действий и позволяет достигать поставленных целей [7, с. 433]. Все эти факторы в совокупности делают цифровые атаки, направленные на получение денег, крайне привлекательными для мошенников.

Состояние информационной безопасности, затрагивающей экономику страны, в первую очередь, принято рассматривать как стратегическую проблему государства из-за непрерывного увеличения количества и серьезности киберугроз. В Отчете, подготовленном Всемирным Экономическим Форумом по глобальным рискам (The Global Risks Report 2023), киберпреступности и кибербезопасности в течение 2-летнего и 10-летнего периодов было определено восьмое место в списке глобальных рисков по степени важности вероятного воздействия, что говорит о значимости рассмотрения данной проблемы уже на мировом уровне (рис. 1) [8, с. 6].

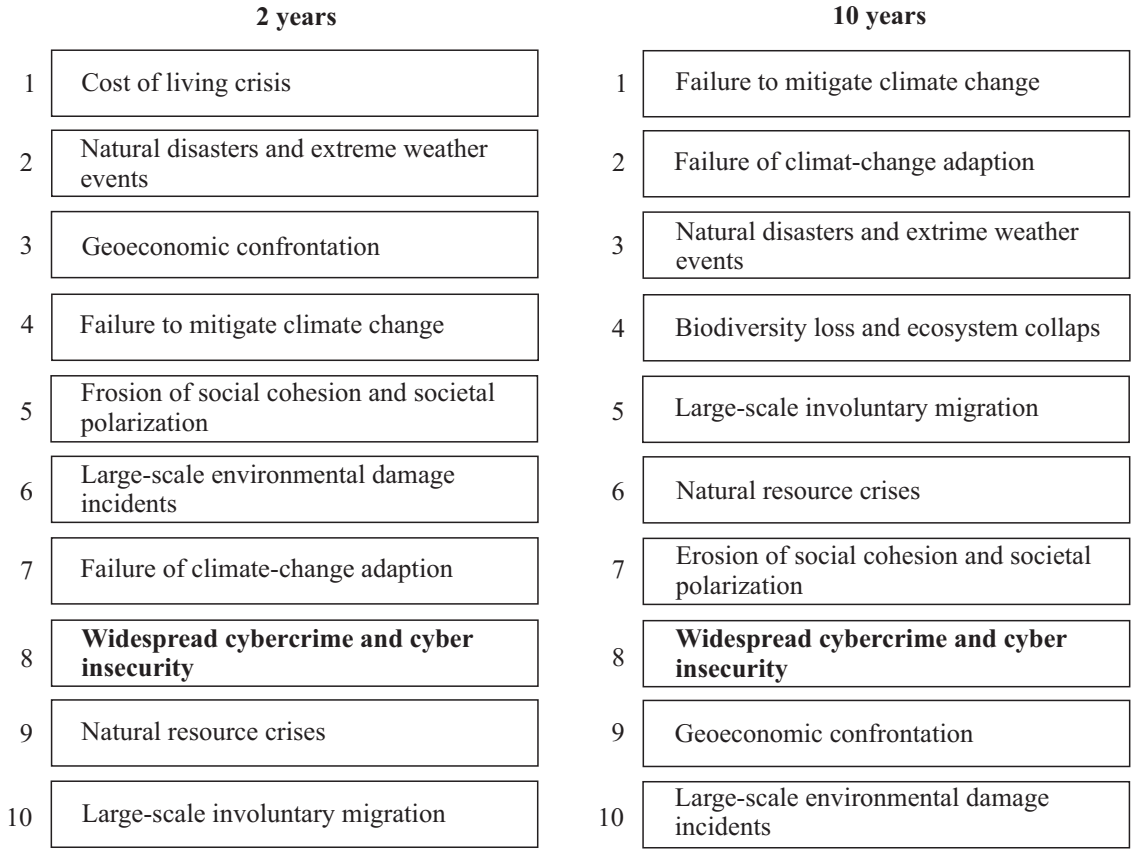

Рис. 1. Глобальные риски по степени важности

Проблемы, связанные с развитием цифровизации, активно отражаются в стратегиях развития многих стран, стремящихся улучшить социально-экономическую обстановку и уменьшить опасность кибератак путем создания и внедрения защитных механизмов. Безопасность в области цифровых технологий представляет собой актуальную задачу и требует решительных действий от всех участников цифровой среды. Инциденты, происходящие в малом бизнесе, могут оказывать значительное влияние на крупные компании и всех участников цепочки, в то время как системные сбои на уровне ключевых цифровых инфраструктур страны имеют потенциал угрожать деятельности разных организаций, банков, государственных органов. По мнению В. Б. Криштаносова и Н. А. Бровко, эти явления подчеркивают, насколько взаимосвязаны и взаимозависимы участники современного экономического процесса [9, с. 225].

Однако не стоит упускать из виду, что экономическое благополучие и устойчивое развитие также в значительной мере зависят от самих граждан, представляющих различные социальные слои. Ведь в случае неверного, рискованного поведения граждан, будь то представители работающего населения, бизнесмены, студенты, пенсионеры или домохозяйки, может исходить существенное отрицательное воздействие на состояние экономики по следующим причинам:

– утрата финансовых средств индивидуальными жертвами (любая группа общества подвержена стать жертвой кибермошенничества, приводящей к утрате личных средств; потери, умноженные на множество индивидуумов, существенно сокращают общедоступный для расходов денежный поток, тем самым, уменьшая общий спрос на товары, услуги, и замедляя экономический рост);

– снижение потребительского доверия (постоянная угроза цифровых преступлений подрывает доверие к онлайн-транзакциям и цифровым сервисам, что крайне значимо в контексте современной экономики; снижение уровня потребления в сфере электронной коммерции, онлайн-банкинга, других подобных онлайн-услуг негативно сказываются на экономической активности);

– накладные расходы на обеспечение цифровой безопасности (государственные учреждения, унитарные предприятия и иные организации сталкиваются с необходимостью повышать затраты на кибербезопасность для защиты индивидуальных пользователей, сокращая доступные финансовые ресурсы для остальных ключевых сфер, включая образование, здравоохранение, защита сбережений, разработка и реализация инвестиционных проектов);

– возможность использования украденных данных для дальнейших преступлений (злоумышленники часто используют украденную личную информацию для совершения дополнительных мошеннических действий, что усугубляет денежные потери и расширяет сферу воздействия преступления, включая создание поддельных учетных записей, кражу идентичности,

подачу фальшивых заявлений на получение государственных выплат);

– экономические потери из-за замедления инноваций (страх перед цифровыми угрозами тормозит прогресс и освоение новейших технологий среди конечных пользователей; это, в свою очередь, приводит к упущению ключевых возможностей для ускорения экономического развития, улучшения результативности труда, создания новых мест работы);

– влияние на трудоустройство и профессиональное развитие (студенты и молодые специалисты, подвергшиеся действиям цифрового мошенничества, могут испытывать значительные трудности при трудоустройстве или продвижении по службе из-за компрометации их личной информации через кражу или обман).

Из последних исследований становится ясно, как важно понимать демографический состав наиболее восприимчивых к киберугрозам групп населения. В этом контексте, по результатам опроса, проведенного Банком России[2], выявлен конкретный профиль людей, чаще всего становящихся жертвами экономических потерь. Исследование показало, что в 2023 г. доля пострадавших женщин относительно доли мужчин возросла и стала больше на 11 %, в то время как в 2022 г. разрыв составлял 8 %. На основании полученных данных, жертвами кибермошенничества стали: женщины – 55,5 %, а мужчины – 44,5 %. Большинство пострадавших находятся в возрасте от 25 до 44 лет (рис. 2)[3].

Среди опрошенных 25,9 % имеют высшее образование, 41,3 % – среднее, 32,8 % – общее, что говорит о том, что цифровые угрозы затрагивают людей вне зависимости от уровня образования (рис. 3)[4].

Исходя из анализа частоты использования различных каналов совершения цифровых преступлений, можно утверждать, что случаи мошенничеств посредством телефонных звонков и СМС-сообщений преобладают – 54,0 % (рис. 4)[5]. Далее в порядке убывания частоты использования следуют такие каналы мошенничества, как атака через мессенджеры – 22,5 %, сообщения в социальных сетях – 9,8 %, письма на электронную почту – 7,2 %, поддельный сайт (фишинг) – 4,8 %, поддельное приложение – 1,7 %.

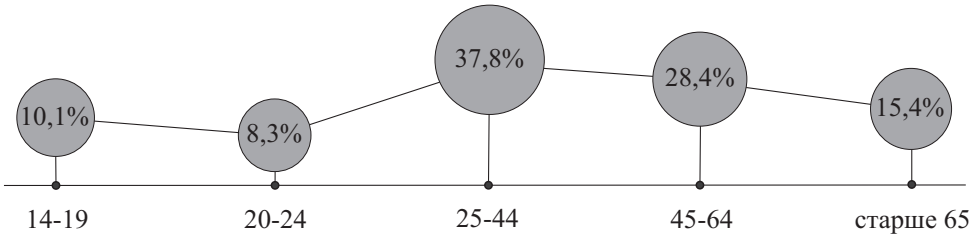

Рис. 2. Распределение граждан, пострадавших от мошенничества, по возрасту, %

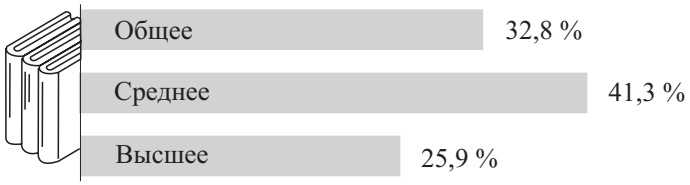

Рис. 3. Распределение граждан, подвергшихся экономическим потерям,по уровню образования, %

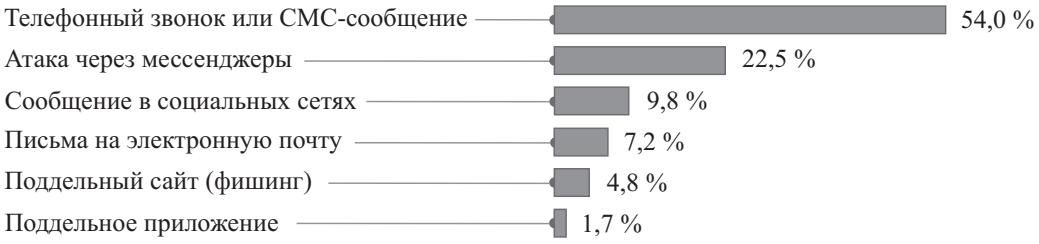

Рис. 4. Распределение технических средств по частоте их использования в целях мошенничества, %

[2] Кибермошенничество: портрет пострадавшего // Банк России: официальный сайт. URL: https://cbr.ru/statistics/information_security/cyber_portrait/ (дата обращения: 16.02.24).

[3] Там же.

[4] Кибермошенничество: портрет пострадавшего // Банк России [сайт]. URL: https://cbr.ru/statistics/information_security/cyber_portrait/ (дата обращения 16.02.24).

[5] Там же.

Данные показывают, что злоумышленники предпочитают использовать наиболее универсальные и доступные средства для достижения своих целей, выбирая при этом такие каналы, где у них больше шансов остаться незамеченными или вызвать доверие у жертв.

Банк России указывает, что 87,6 % опрошенных не поддавались уловкам мошенников и не предпринимали никаких действий. Однако из оставшегося количества респондентов столкнулись с финансовыми потерями в размере до 20 тыс. руб. в результате мошеннических действий – 64,1 %, утратили средства в размере от 20 до 100 тыс. руб. – 17,9 %, потеряли до 500 тыс. руб. – 9,9 %, и 4,3 % лишились суммы свыше одного миллиона рублей.

Как считает О. П. Чечин, кумулятивный эффект этих последствий указывает на сложность проблемы кибербезопасности и ее многоаспектное влияние (как на индивидуальном уровне, так и на уровне всей экономики), подчеркивая необходимость комплексного подхода к решению данных вопросов [10, с. 95].

Осознавая обширность и серьезность последствий, связанных с цифровыми угрозами, акцент смещается на разработку стратегий, направленных на уменьшение уязвимости для кибератак. По мнению А. М. Люевой и З. М. Казовой, реализация комплекса мероприятий по уменьшению шанса происшествий в киберпространстве и ограничение последствий инцидентов становится центральной задачей [11, с. 145]. Стоить учесть, что это не однократный процесс, а непрерывное действие, которое должно быть интегрировано в культуру организации и повседневную жизнь индивидуумов для обеспечения максимально эффективной защиты.

Одним из подходов борьбы с киберугрозами является нивелирование. В контексте теории экономической безопасности, процесс нивелирования не просто сводится к уменьшению воздействия угроз, способных нарушить стабильность финансовой системы, через их нейтрализацию или ослабление, а предполагает комплексный метод, который включает: идентификацию ключевых секторов экономики, ответственных за экономическую безопасность, выявление характера угроз для этих секторов, создание проектов, программ (планов действий, дорожных карт) развития секторов экономики с учетом вызовов для обеспечения экономической устойчивости, что включает в себя выбор стратегии, направление действий. Ввиду того, что практически все секторы экономики (их отрасли, сегменты) оказывают воздействие на уровень экономической безопасности, разновидностей процессов их балансировки может быть множество.

Нивелирование цифровых угроз в целях снижения экономических потерь в современном мире В. В. Смагина и М. И. Бородина подразделяют на четыре основных этапа, каждый из которых играет критически важную роль в обеспечении общей устойчивости национальной экономики к цифровым угрозам (рис. 5) [12, с. 79].

1-й этап. Определение сектора экономики (сегмента сектора). На этом этапе анализируются различные отрасли (сегменты секторов экономики) на предмет их уязвимости в условиях цифровых угроз. Основное внимание уделяется критически важной инфраструктуре, включающей финансовые организации, энергетические сети, системы здравоохранения и прочие секторы (сегменты), функционирование которых непосредственно влияет на экономическую стабильность. Важно в каждом секторе экономики (его сегменте, сферы) правильно идентифицировать и классифицировать активы, которые могут стать целями для кибератак.

2-й этап. Определение угроз. После идентификации ключевых уязвимых сфер экономики следующим шагом является анализ и определение потенциальных цифровых угроз, которые могут нанести ущерб. Уделяется внимание как внешним, так и внутренним источникам цифровых рисков. Цель этапа – создать полный профиль угроз для каждой сферы, понимая специфику и возможный ущерб от каждого типа атак.

3-й этап. Разработка проекта. Следующий шаг предполагает разработку проекта (или программы, или плана действий, или дорожной карты), включающего стратегии и меры по защите от выявленных угроз: внедрение технологических решений, улучшение процедур и практик в области информационной безопасности, а также обучение и повышение осведомленности персонала. Ключевым элементом становится выбор оправданных технологических инструментов и методик, способных обеспечить надежную защиту от цифровых рисков. В ходе разработки проекта определяются ключевые области ответственности, устанавливаются четкие временные рамки реализации пунктов проекта (программы, плана действий), выделяются необходимые ресурсы.

4-й этап. Реализация проекта. Финальный этап включает в себя практическое внедрение разработанного плана мероприятий (дорожной карты).

[6] Даркнет – это часть интернета, в которой пользователи могут скрывать свою личность и местонахождение от других людей и правоохранительных органов. Его часто используют для торговли краденными персональными данными. URL: https://support.google.com/googleone/answer/12262331?hl=ru&ref_topic=13016717&sjid=13278492421415233260-EU (дата обращения: 12.02.2024).

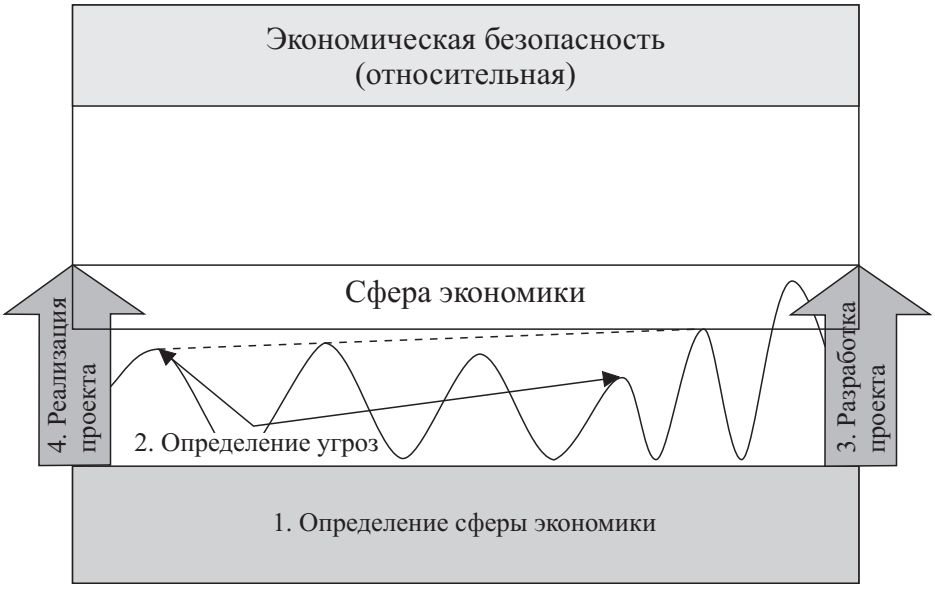

Рис. 5. Этапы нивелирования цифровых угроз в целях обеспечения экономической безопасности в современном мире

Важной составляющей является мониторинг и оценка продуктивности реализованных мер, что позволяет вносить коррективы в стратегию защиты и повышать ее действенность.

Практика показывает, что наибольшему риску подвержены те организации и подразделения, что управляют финансами, обладают критически значимой корпоративной информацией, поскольку утечки в этих сферах могут нанести организации большой урон, истощая клиентскую базу, уменьшая конкурентное преимущество. К примеру, не так давно ПАО Сбербанк столкнулся с серьезной проблемой утечки персональных данных, затронувшей множество пользователей. Как стало известно из сообщения в Telegram-канале сервиса DLBI, специализирующегося на обнаружении утечек данных и мониторинге даркнета[6], в интернет попала база данных, включающая сведения почти о 50 миллионах участников этого интернет-сегмента. В архиве информации основную часть составляют уникальные номера телефонов пользователей, без каких-либо повторений. Электронных адресов заметно меньше, но их количество также достаточно велико. Используя эти сведения, мошенники могут совершать звонки от официального лица, к примеру службы безопасности Сбербанка, предлагая перевести средства на «абсолютно безопасный» счет, якобы для защиты от финансовых афер или же отправлять фишинговые письма клиентам для получения банковских данных.

В силу того, что понимание вопросов цифровой безопасности среди граждан не достаточно велико, не каждый знает, как корректно обращаться со своей персональной информацией правильно и может повестись на такие уловки. Кроме того, архив содержит хешированные номера банковских карт, используемые потребителями для платежей, данные, которых зашифрованы с использованием устаревшего и, как показала практика, неэффективного в современных условиях алгоритма. Специалисты DLBI[7] отмечают, что, несмотря на хранение данных в закодированном виде, применение старой функции хеширования не представляет трудности для восстановления исходных номеров карт путем полного перебора. Зачастую применяемые способы обеспечения безопасности информации недостаточно хороши и влекут за собой опасность для финансовых данных пользователей. Это выявляет срочную потребность в применении более передовых решений, которые могут устойчиво сопротивляться современным методам кибератак.

Однако большинство нарушений происходит из-за активных действий или, наоборот, пассивной позиции работников организации (компании), способных привести к нарушениям, совершаемым как случайным образом, так и осознанно.

В работе П. С. Швыряева [13, с. 240] приведено описание множества инцидентов, спровоцированных работниками компании; это указывает на то, что внутренние факторы, а не внешние обстоятельства представляют большую опасность. Когда происходят утечки информации, особенно, если они крупные, в первую очередь появляется

[7] Речь идет о компании «Data Leakage & Breach Intelligence».

интерес со стороны контролирующих органов, занимающихся вопросами безопасности данных. В этом случае компания неизбежно столкнется с серьезными штрафами, касающимися защиты интересов потребителей, а если будет доказан тот факт, что данная ситуация возникла в связи с действиями работников компании, возможные последствия будут включать не только дисциплинарные меры, денежные взыскания, но уже и уголовную ответственность. Также может последовать подача исков от пострадавших лиц с требованиями компенсации нанесенного ущерба. В совокупности все события способны серьезно подпортить репутацию бизнеса, привести к сокращению числа клиентов, потере доверия, снижению конкурентоспособности на рынке. Следовательно, процесс восстановления операционной инфраструктуры бизнеса потребует значительных ресурсов, инвестиций.

Для успешного предотвращения неблагоприятных событий в сфере информационной безопасности и уменьшения риска встречи с непредвиденными ситуациями крайне важно прибегнуть к стратегиям нивелирования угроз. Следуя четко установленным правилам, компании смогут значительно снизить вероятность возникновения инцидентов, обеспечить надежную защиту своих информационных активов, что будет способствовать укреплению доверия со стороны клиентов и партнеров и минимизации потенциальных финансовых потерь от нарушений безопасности. В долгосрочной перспективе такой подход способствует повышению репутации, устойчивости компании на рынке.

Рассмотрим основные принципы реализации подхода к нивелированию угроз.

1. Укрепление знаний в области цифровых технологий и формирование культуры в сфере информационной безопасности предусматривает широкий спектр мероприятий, направленных на увеличение уровня осведомленности и умений пользователей работать с цифровыми инструментами путем организации учебных программ, тренингов. Несмотря на то, что термин «цифровая грамотность» широко известен благодаря новостным источникам, социальным сетям, подобным платформам, в реальной жизни часто отсутствуют необходимые практические навыки, знания о мерах предосторожности при столкновениях с угрозами цифровой среды. Стоит не только подчеркивать значимость цифровой грамотности[8], но и понимать возможные последствия неправильных действий, поскольку это касается не только профессиональной деятельности, но и личной жизни каждого.

2. Внедрение актуальных технологических решений и подходов к нивелированию угроз основывается на интеграции, использовании передовых достижений IT-технологий, направленных против различных видов несанкционированного доступа. Процедура означает переход от использования базовых технологий обеспечения безопасности к применению продвинутых решений. К ним относятся многофакторная аутентификация, блокчейн технологии, эндпоинт-защита, шифрование данных, облачные решения, средства с использованием искусственного интеллекта, другие средства, которые не просто оберегают важные сведения от угроз со стороны и изнутри, но также способствуют непрерывности процессов компании в быстро меняющемся технологическом ландшафте. Данный способ позволяет совместить разные слои защиты, увеличивая трудности для получения нежелательного доступа к информации. В то же время, принятие новейших технологий простирается далеко за рамки защиты информации, охватывая использование инновационных подходов. К техническим методам добавляется акцент на формирование законодательных рамок и инди-

[8] Считаем целесообразным напомнить о введении в действие двух документов:

– Указа Президента РФ от 17 мая 2023 г. № 358 «О Стратегии комплексной безопасности детей в Российской Федерации на период до 2030 года», где среди задач в сфере формирования безопасной информационной среды для детей являются: 1) выявление, предупреждение и пресечение угроз информационной безопасности (ИБ) детей, осуществляемые в том числе при участии организаций, деятельность которых ориентирована на достижение общественно значимых целей, и с использованием их современных аппаратно-программных комплексов; 2) создание информационной продукции для детей, способствующей их ценностному, моральному, духовному, нравственному и личностному развитию; 3) реализация мероприятий в сфере ИБ для детей и их родителей (законных представителей), педагогических работников организаций, осуществляющих образовательную деятельность; 4) формирование у детей навыков самостоятельного, осознанного и ответственного использования информационной продукции; а среди показателей, характеризующих уровень безопасности детей – число детей, освоивших образовательные программы в области информационной безопасности и (или) цифровой грамотности и (или) принявших участие в мероприятиях, посвященных этой тематике;

– профессионального стандарта «Консультант в области развития цифровой грамотности населения (цифровой куратор)». Он утвержден приказом Минтруда России от 31 октября 2018 г. № 682н. Среди основных трудовых функций стандарта: консультирование граждан в области развития цифровой грамотности; организация и проведение мероприятий по консультированию граждан в области развития цифровой грамотности.

видуальных этических норм, способствующих соблюдению нормативов охраны личных данных. Приверженность этим стандартам, правилам становится краеугольным камнем в формировании надежного цифрового пространства.

3. Регулярный обзор возможных опасностей и непрерывное обновление информационно-технологической инфраструктуры исходит из осознания весомости инициативного обнаружения, изучения всех потенциальных угроз цифрового пространства, которое подразумевает не пассивное ожидание возникновения проблем, а предварительное, осознанное, целенаправленное действие для их выявления, понимания. Основой стратегии является систематическое проведение проверок, охватывающих детальное изучение всего функционального комплекса работы. Использование специализированных приложений, способных изучить всю систему в целом, играет не менее важную роль, позволяя автоматизировать процесс выявления проблемных областей, а внимательное изучение несостыковок и аномалий в данных или поведении системы может служить ранним указателем наличия угроз. Как только возможные уязвимости опознаны, необходимо приступить к их устранению. Во многих случаях это означает регулярное обновление программного и аппаратного обеспечения до последних версий. Разработчики обновлений часто реагируют на известные уязвимости, и установка этих обновлений является необходимым шагом в процессе закрытия «дверей» для злоумышленников. Стоит учесть, что обновления касаются не только операционных систем, применяемых программ, но и сетевого оборудования, баз данных, технологических компонентов.

4. Подготовка плана действий для случаев неавторизованного доступа обретает свою значимость в контексте постоянно усиливающейся угрозы кибератак. Основой результативного плана есть всестороннее понимание тех угроз, которые способны затронуть систему, предполагая уже известные сценарии, каналы возможных утечек информации, методы, которыми мошенники будут пытаться получить доступ. Потому необходимо четко обозначить шаги реагирования на инциденты: от изоляции затронутых областей до уведомления всех заинтересованных сторон о происшествии. План действий должен всегда находиться в зоне видимости (доступа) соответствующего персонала на каком-либо, удобном для персонала, носителе, где будут содержаться контактные данные службы поддержки, специалистов по безопасности, предварительно оговоренные меры восстановления действий после инцидентов, включая процедуры восстановления данных, системы в целом. Так, корректно составленный план реагирования призван уменьшить возможные убытки от утечек информации, сократить время простоя, способствовать быстрому восстановлению операционной деятельности, помочь обеспечить соблюдение законодательных, нормативных требований, а также обеспечить ответное действие, способствующее сокращению негативных последствий.

Влияние цифровых нарушений выходит за рамки определенных секторов или социальных групп, охватывая все больше областей. Эффект от таких преступлений оказывается крайне разрушительным, обширность возможного ущерба может затронуть всю экономику в целом. В свете постоянного роста объемов и важности данных усиление защиты от цифровых угроз становится непременно значимым аспектом в современном мире. Важно осознавать, что там, где технологии развиваются с невероятной скоростью, борьба с киберугрозами никогда не будет полностью завершена. Именно постоянное совершенствование методов защиты и правильный подход к решению проблемы позволят значительно снизить риски и уменьшить потери.

Литература

1. Руководство по статистике государственных финансов 2014 года. – США, Вашингтон: Международный валютный фонд, 2014. – 575 с. URL: https://www.imf.org/external/Pubs/FT/GFS/Manual/2014/GFSM_2014_rus.pdf (дата обращения 16.02.24).

2. *Крикунов И. С.* Цифровая экономика как фактор обеспечения экономической безопасности // Прогрессивная экономика. 2023. № 5. С. 18–31. DOI: 10.54861/2713 1211_2023_5_18.

3. *Бойкова А. В.* Цифровые угрозы экономической безопасности // Экономика и предпринимательство. 2022. № 12 (149). С. 26–29. DOI: 10.34925/EIP.2022.149.12.001.

4. *Есенжулова Л. С., Дроковский Н. Б.* Угрозы и риски экономической безопасности в условиях цифровизации экономики // Экономика и бизнес: теория и практика. 2023. № 5-1 (99). С. 219–222. DOI: 10.24412/2411-0450-2023-5-1-219-222.

5. *Удалов Д. В.* Угрозы и вызовы цифровой экономики // Экономическая безопасность и качество. 2018. № 1 (30). С. 12–18.

6. *Саадулаева Т. А., Белановский М. М.* Цифровая экономика государства: оценка угроз, рисков и проблем регулирования финансово-экономической безопасности // Международный журнал гуманитарных и естественных наук. 2022. № 9-2 (72). С. 231–234. DOI: 10.24412/2500-1000-2022-9-2-231-234.

7. *Галстян Д. А.* Экономические преступления в условиях цифровизации и проблемы их уголов-

но-правовой оценки // Вопросы российской юстиции. 2022. № 19. С. 432–439.

8. The Global Risks Report 2023. 18th Edition / World Economic Forum. – Geneva, Switzerland, 2023. – 98 p. URL: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf (дата обращения 16.02.24).

9. *Криштаносов В. Б., Бровко Н. А.* Концептуально-аналитические подходы к возникновению потенциальных угроз в цифровой экономике // ALTERECONOMICS. 2023. Т. 20, № 1. С. 216–245. DOI: 10.31063/AlterEconomics/2023.20-1.11.

10. *Чечин О. П.* Цифровая трансформация в концепции экономической безопасности // Экономические науки. 2019. № 7 (176). С. 92–97.

11. *Люева А. М., Казова З. М.* Цифровизация и ее влияние на российскую экономику // Известия Кабардино-Балкарского государственного аграрного университета им. В. М. Кокова. 2020. № 4 (30). С. 141–146.

12. *Смагина В. В., Бородина М. И.* Нивелирование угроз как процесс обеспечения экономической безопасности государства // Вестник Тамбовского университета. Серия: гуманитарные науки. 2014. № 12 (140). С. 77–81.

13. *Швыряев П. С.* Утечки конфиденциальных данных: главный враг внутри // Государственное управление. Электронный вестник. 2022. № 91. С. 226–241. DOI: 10.24412/ 2070-1381-2022-91-226-241.

Сведения об авторах

Следнева Кристина Евгеньевна – студент кафедры «Информационная безопасность», Омский государственный университет путей сообщения (ОмГУПС), Омск, Россия.
Email: ksledneva2003@gmail.ru

Кувалдина Татьяна Борисовна – доктор экономических наук, профессор кафедры «Экономическая безопасность и управление финансами», Омский государственный университет путей сообщения (ОмГУПС), Омск, Россия.
Email: kuvaldina2004@mail.ru

LEVELING DIGITAL THREATS AS A MEANS OF ENSURING ECONOMIC SECURITY IN THE MODERN WORLD

K. Sledneva
Omsk State Transport University (OSTU),
Omsk, Russia

T. Kuvaldina
Omsk State Transport University (OSTU),
Omsk, Russia

In the era of digitalization, where the development of technology is closely linked to economic prosperity, it is important to realize the threats posed by the modern world. Indeed, digital transformation opens up new horizons for public spheres of life, intertwining innovative technologies with everyday tasks, actively stimulating social progress. However, as dependence on new technologies increases, the impact of digital threats on economic stability and security increases. The attractiveness of such incidents is based on the relative cheapness and accessibility, which makes them more preferable for intruders compared to other types of crimes. Various kinds of attacks and malicious actions, such as viruses, phishing, malware, cyber attacks, can disrupt not only the work of companies, but also undermine their financial situation as a whole. At this stage, the problem of digital threats is turning into a global phenomenon affecting everyone – from ordinary citizens to large companies and government agencies. It is important to be aware of this problem, because without proper counteraction to these challenges, economic losses from cybercrimes will only increase. Preventing such attacks and reducing their consequences requires a comprehensive approach. That is why the article considers not only the question of what negative consequences digital threats have, but also suggests the necessary, according to the authors, methods and strategic solutions aimed at reducing economic losses in the process of constantly changing conditions.

Keywords: digital threats, leveling, economic losses, incidents, strategies, economic security.

References

1. Руководство по статистике государственных финансов 2014 года. – США, Вашингтон: Международный валютный фонд, 2014. – 575 с. URL: https://www.imf.org/external/Pubs/FT/GFS/Manual/2014/GFSM_2014_rus.pdf (дата обращения 16.02.24).

2. Krikunov I. S. The digital economy as a factor of ensuring economic security, *Progressivnaya ekonomika*, 2023, no. 5, pp. 18-31 (In Russ.). DOI: 10.54861/27131211_2023_5_18

3. Boikova A. V. Digital threats to economic security, *Ekonomika i predprinimatel'stvo*, 2022, no. 12 (149), pp. 26-29 (In Russ.). DOI: 10.34925/EIP.2022.149.12.001

4. Esenzhulova L. S., Drokovskii N. B. Threats and risks of economic security in the context of digitalization of the economy, *Ekonomika i biznes*, 2023, no. 5-1 (99), pp. 219-222 (In Russ.). DOI: 10.24412/2411-0450-2023-5-1-219-222

5. Udalov D. V. Threats and challenges of the digital economy, *Ekonomicheskaya bezopasnost' i kachestvo*, 2018, no. 1 (30), pp. 12-18 (In Russ.).

6. Saadulaeva T. A., Belanovskii M. M.Digital economy of the state: assessment of threats, risks and problems of regulation of financial and economic security, *Mezhdunarodnyj zhurnal gumanitarnyh i estestvennyh nauk*, 2022, no. 9-2 (72), pp. 231-234 (In Russ.). DOI: 10.24412/2500-1000-2022-9-2-231-234

7. Galstyan D. A. Economic crimes in the context of digitalization and the problems of their criminal legal assessment, *Voprosy rossiiskoi yustitsii*, 2022, no. 19, pp. 432-439 (In Russ.).

8. The Global Risks. Report 2023. 18th Edition. Insight Report. World Economic Forum. Geneva, Switzerland, 2023. 98 p. Available at: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf (Date of application: 02/15/2024).

9. Krishtanosov V. B., Brovko N. A. Conceptual and analytical approaches to the emergence of potential threats in the digital economy, *AlterEconomics*, 2023, Vol. 20, No. 1, pp. 216-245 (In Russ.). DOI: 10.31063/AlterEconomics/2023.20-1.11

10. Chechin O. P. Digital transformation in the concept of economic security, *Jekonomicheskie nauki – Economic sciences*, 2019, no. 7 (176), pp. 92-97 (In Russ.).

11. Lyueva A. M., Kazova Z. M. Digitalization and its impact on the Russian economy, *Izvestiya Kabardino-Balkarskogo gosudarstvennogo agrarnogo universiteta im. V. M. Kokova*, 2020, no. 4 (30), pp. 141-146 (In Russ.).

12. Smagina V. V., Borodina M. I. Leveling threats as a process of ensuring the economic security of the state, *Vestnik Tambovskogo universiteta. Seriya: gumanitarnye nauki*, 2014, no. 12 (140), pp. 77-81 (In Russ.).

13. Shvyryaev P. S. Confidential data leaks: the main enemy inside, *Gosudarstvennoe upravlenie. Elektronnyi vestnik*, 2022, no. 91, pp. 226-241 (In Russ.). DOI: 10.24412/2070-1381-2022-91-226-241

About the authors

Kristina E. Sledneva – student of the Department of Information Security, Omsk State Transport University (OSTU), Omsk, Russia.
Email: ksledneva2003@gmail.ru

Tatyana B. Kuvaldina – Professor of the Department of Economic Security and Financial Management, Omsk State Transport University (OSTU), Omsk, Russia