УДК 33 **DOI: 10.34670/AR.2026.37.72.011**

Цифровые угрозы системе валютного регулирования: классификация и модели противодействия в контексте экономической безопасности

Чеботарев Станислав Стефанович

Доктор экономических наук, профессор,
Акционерное общество «Ордена Трудового Красного Знамени научно-исследовательский институт автоматической аппаратуры им. академика В.С. Семенихина»,
125319, Российская Федерация, Москва, ул. Свободы, 7;
e-mail: StSt57@yandex.ru

Чеботарев Владислав Стефанович

Доктор экономических наук, профессор,
Волжский государственный университет водного транспорта,
603950, Российская Федерация, Нижний Новгород, ул. Нестерова, 5;
e-mail: vschebotarev@rambler.ru

Хмыз Александр Александрович

Старший преподаватель,
Нижегородский институт путей сообщения - филиал Приволжский государственный университет путей сообщения,
603011, Российская Федерация, Нижний Новгород, ул. Народная, 4;
e-mail: g101@yandex.ru

Аннотация

Цифровизация формирует новую риск-среду для системы валютного регулирования как основы экономической безопасности. Существующие классификации угроз фрагментарны и не учитывают их комплексного воздействия. Цель исследования — разработка многокритериальной классификации по источникам, объектам, механизмам и целям угроз. Её ключевое преимущество — прямая связь типа угрозы с параметрами экономической безопасности, такой как стабильность курса валюты. На основе классификации предложены модели для идентификации и нейтрализации угроз, имеющие практическую значимость для органов регулирования.

Для цитирования в научных исследованиях

Чеботарев С.С., Чеботарев В.С., Хмыз А.А. Цифровые угрозы системе валютного регулирования: классификация и модели противодействия в контексте экономической безопасности // Экономика: вчера, сегодня, завтра. 2025. Том 15. № 11А. С. 119-131. DOI: 10.34670/AR.2026.37.72.011

Ключевые слова

Система валютного регулирования, экономическая безопасность, цифровые угрозы, классификация угроз, киберриски, отмывание доходов (ПОД/ФТ), вывод капитала, криптоактивы, финансовая стабильность, Росфинмониторинг.

Введение

Современная финансовая система претерпевает фундаментальные изменения, обусловленные процессами цифровизации. Система валютного регулирования, являясь институциональным и функциональным стержнем обеспечения экономической безопасности государства, не остается в стороне от этих процессов. Интеграция цифровых технологий в операции, связанные с движением капитала, проведением международных расчетов и валютным контролем, привела к формированию новой риск-среды. Традиционные угрозы, такие как уклонение от уплаты налогов, отмывание доходов, полученных преступным путем, и финансирование терроризма, приобрели цифровую форму, а также появились принципиально новые вызовы, связанные с киберпреступностью, целенаправленными атаками на финансовую инфраструктуру и использованием криптоактивов для обхода валютных ограничений.

Актуальность темы исследования обусловлена потребностью в систематизации и анализе цифровых угроз для разработки адекватных мер противодействия. Существующие классификации, как правило, фокусируются либо на технических аспектах кибербезопасности, либо на экономических рисках, без их комплексной увязки с целями и инструментами валютного регулирования. Данный пробел определяет цель исследования – разработать научно обоснованную классификацию цифровых угроз, ориентированную на систему валютного регулирования экономической безопасности.

Основная часть

Система валютного регулирования представляет собой совокупность правовых, административных и экономических мер, осуществляемых уполномоченными государственными органами с целью воздействия на порядок совершения валютных операций, движения капитала и обеспечения стабильности национальной валюты. С позиции экономической безопасности, ее ключевые функции включают: предотвращение незаконного оттока капитала, обеспечение устойчивости платежного баланса, противодействие легализации (отмыванию) преступных доходов и финансированию терроризма (ПОД/ФТ), а также защиту национального валютного суверенитета [Экономическая безопасность России, 2009].

В эпоху цифровых угроз данная система приобретает новые системные характеристики. К таковым относятся цифровая уязвимость инфраструктуры, размывание национальных юрисдикций, дематериализация и усложнение отслеживания операций интеллектуализация угроз.

Ключевые элементы системы – информационные базы данных органов контроля (например, Банка России, Росфинмониторинга), системы межбанковских расчетов (SWIFT, СПФС), платформы онлайн-банкинга – становятся первоочередными целями для кибератак. Успешная атака может парализовать валютные операции и подорвать доверие к финансовой системе. Использование децентрализованных технологий, таких как блокчейн, и криптоактивов позволяет субъектам осуществлять трансграничные переводы, минуя традиционные каналы

валютного контроля. Это создает серьезный вызов для реализации суверенной валютной политики [Глазьев, Фетисов, 2013]. Цифровые активы и финансовые технологии (FinTech) обеспечивают высокую скорость и анонимность транзакций, что затрудняет для регуляторов идентификацию бенефициарных владельцев и целей проводимых операций. Угрозы исходят не только от отдельных хакеров, но и от высокоорганизованных киберпреступных группировок и государственных структур, применяющих методы социальной инженерии, целенаправленное вредоносное программное обеспечение (targeted malware) и сложные схемы для атак на финансовые организации.

Таким образом, современная система валютного регулирования существует в условиях гибридной риск-среды, где традиционные экономические риски неразрывно переплетены с технологическими угрозами, что требует адаптации как правовой базы, так и методологического аппарата.

Анализ научной литературы позволяет выделить несколько ключевых подходов к классификации цифровых угроз, каждый из которых акцентирует внимание на различных аспектах проблемы.

Технократический подход (А.И. Петренко, С.В. Симонов). Данный подход фокусируется на технических каналах и способах реализации атак. Угрозы подразделяются по типам используемых вредоносных программ (вирусы, черви, трояны, ransomware), видам атак (DDoS-атаки, фишинг, SQL-инъекции) и уязвимостям программного обеспечения [Петренко, Симонов, 2004]. В контексте валютного регулирования это позволяет оценить риски нарушения работоспособности информационных систем уполномоченных банков и государственных органов.

Экономико-правовой подход (С.В. Одинцов). Классификация строится на основе целей противоправной деятельности и видов экономического ущерба. Авторы выделяют угрозы, направленные на: незаконный вывод капитала за рубеж с использованием цифровых каналов; мошенничество на финансовых рынках с применением алгоритмического трейдинга; отмывание денег через онлайн-платежные системы и криптобиржи [Одинцов, Кошелюк, 2023]. Этот подход полезен для увязки цифровых инцидентов с нарушениями валютного законодательства, например, Закона «О валютном регулировании и валютном контроле» № 173-ФЗ.

Институциональный подход (А.Г. Коломиец). Угрозы классифицируются по объектам атаки, то есть по ключевым институтам финансовой системы. Выделяются угрозы для: центральных банков, коммерческих банков, осуществляющих валютный контроль, платежных систем и инфраструктурных организаций [Коломиец, 2018]. Такой подход помогает распределить зоны ответственности за противодействие угрозам между различными участниками системы.

Таксономический подход на основе рисков ПОД/ФТ («Группа разработки финансовых мер борьбы с отмыванием денег», ФАТВ (Financial Action Task Force, FATF)). Хотя ФАТФ не является отдельным автором, ее рекомендации и отчеты формируют международный стандарт классификации. Угрозы идентифицируются по методам отмывания денег: использование анонимных карт предоплаты, торговое финансирование с использованием фиктивных компаний, злоупотребление услугами виртуальных активов [FATF, 2021]. Этот подход напрямую интегрирован в национальное законодательство, включая Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» № 115-ФЗ.

Поведенческий подход (А.П. Бондарь). Акцент делается на человеческом факторе. Угрозы делятся на внешние (действия киберпреступников, использующих социальную инженерию для получения доступа к системам валютного контроля) и внутренние (недобросовестные действия или ошибки сотрудников банков и регуляторных органов) [Бондарь, 2020].

Комплексный подход (О.Б. Дигилин, А.М. Черняев). Авторы пытаеются объединить несколько критериев, выделяя угрозы по уровню воздействия (макро-, мезо-, микро-) и по природе возникновения (техногенные, преднамеренные, конкурентные) [Дигилина, Черняев, 2023]. Однако, как будет показано ниже, данный подход не лишен недостатков.

Критический анализ рассмотренных классификаций через призму современных экономических теорий выявляет их системные ограничения.

Применение инструментов институциональной экономики, в частности, теории трансакционных издержек, позволяет выявить системные ограничения рассмотренных подходов. Так, технократический подход, фокусируясь на технических уязвимостях, не учитывает, что несовершенство контрактов и институтов контроля создает для участников рынка стимулы к экономии на мерах безопасности, перекладывая риски на систему в целом. Поведенческий подход, выделяя человеческий фактор, не исследует институциональные причины, обуславливающие низкий уровень культуры соблюдения установленных требований в отдельных организациях, такие как слабость внутренних контрольных процедур (как неформальных институтов). Таким образом, игнорирование институционального контекста не позволяет данным подходам предложить решения по изменению системы стимулов для всех участников системы валютного регулирования. Институциональный подход А.Г. Коломиец, напротив, делает шаг в этом направлении, но не раскрывает механизмы взаимодействия между институтами в условиях кибератаки [Коломиец, 2018].

В рамках теории информационной асимметрии, являющейся краеугольным камнем современной финансовой теории, ни один из подходов в полной мере не рассматривает цифровые угрозы как следствие и инструмент усугубления информационной асимметрии между регулятором и участниками рынка. Мошеннические схемы с использованием цифровых технологий (например, фишинг) позволяют злоумышленникам получать приватную информацию, усиливая их преимущество. Экономико-правовой подход С.В. Одинцова частично затрагивает эту проблему, но не формализует ее [Одинцов, Кошелюк, 2023].

Теория экономической безопасности (В.К. Сенчагов, С.Ю. Глазьев, Г.Г. Фетисов) требует оценки угроз через призму их воздействия на ключевые параметры безопасности: золотовалютные резервы, стабильность курса национальной валюты, устойчивость финансовой системы [Экономическая безопасность России, 2020; Глазьев, Фетисов, 2013].

Большинство проанализированных классификаций не содержат прямого соотнесения конкретного типа цифровой угрозы с тем, какой именно параметр экономической безопасности подвергается риску.

Таким образом, существующие классификации являются либо слишком узкоспециализированными, либо эклектичными, но не предлагают целостной модели, пригодной для комплексного анализа угроз системе валютного регулирования с позиций экономической безопасности.

На основе критического анализа существующих подходов предлагается авторская многокритериальная классификация, интегрирующая четыре ключевых критерия: источник угрозы, целевой объект атаки, механизм реализации и конечная цель воздействия на экономическую безопасность (табл. 1).

Таблица 1 – Авторская классификация цифровых угроз системе валютного регулирования

Критерий / Категория	Характеристика	Примеры	Связь с нормативно-правовой базой
1. По источнику угрозы:			
1.1. Внешние	Исходят из-за пределов национальной юрисдикции или от иностранных субъектов	Кибератаки иностранных государств, международные киберпреступные группировки	Закон № 173-ФЗ (ст. 23), Указ Президента РФ № 647 «О Стратегии национальной безопасности»
1.2. Внутренние	Исходят от резидентов, включая сотрудников организаций	Недобросовестные сотрудники банка, компании-резиденты, использующие фиктивные контракты	Закон № 115-ФЗ, Трудовой кодекс РФ
2. По целевому объекту атаки:			
2.1. Инфраструктурные	Направлены на критическую информационную инфраструктуру финансового сектора	Атаки на SWIFT, системы ЦБ, платежные системы (НСПК)	Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры»
2.2. Операционные	Направлены на искажение данных или нарушение процедур валютного контроля	Взлом клиент-банка для проведения несанкционированной валютной операции, фальсификация паспортов сделок	Закон № 173-ФЗ (ст. 15, 23), Инструкция Банка России № 181-И
2.3. Информационные	Направлены на хищение конфиденциальной информации	Кража баз данных о валютных операторах, перехват конфиденциальной переписки	Федеральный закон № 152-ФЗ «О персональных данных»
3. По механизму реализации:			
3.1. Кибернетические	Использование вредоносного ПО, хакерских атак, уязвимостей в коде	Ransomware для блокировки систем валютного контроля, DDoS-атака на сайт Росфинмониторинга	-
3.2. Технологические	Использование инновационных финансовых технологий для обхода регулирования	Использование криптоактивов, p2p-платформ, децентрализованных финансов (DeFi)	Закон № 259-ФЗ «О цифровых финансовых активах»
3.3. Психологические	Манипулирование поведением человека (социальная инженерия)	Фишинг для получения паролей к системам валютного контроля у сотрудников банка	-
4. По конечной цели (воздействие на экономическую безопасность):			
4.1. Подрыв валютной стабильности	Нацелены на дестабилизацию курса национальной валюты	Скоординированные кибератаки на крупные банки для создания паники и спекулятивного давления на рубль	Основные направления единой государственной денежно-кредитной политики
4.2. Нелегальный вывод капитала	Нацелены на незаконный перевод активов за рубеж.	Создание фиктивных цифровых контрактов, использование анонимных онлайн-кошельков.	Закон № 173-ФЗ, Закон № 115-ФЗ
4.3. Дискредитация институтов	Нацелены на подрыв доверия к системе валютного регулирования.	Публикация украденных данных ЦБ или Росфинмониторинга, демонстрация уязвимостей.	-

Предлагаемая авторская классификация базируется на интеграции четырёх взаимосвязанных критериальных блоков, формирующих системную матрицу для анализа. Первый критерий – источник угрозы – подразделяет их на внешние и внутренние, что позволяет определить принадлежность нарушителя и выбрать адекватные инструменты ответа, от международно-правовых до внутренних административных.

Второй критерий – целевой объект атаки – дифференцирует угрозы на инфраструктурные, операционные и информационные. Данный подход смещает фокус с абстрактной «кибератаки» на конкретный элемент системы, подвергающийся атаке, будь то платёжные системы, процедуры валютного контроля или базы данных, что позволяет точечно укреплять наиболее уязвимые звенья.

Третий критерий оценивает механизм реализации угрозы, выделяя кибернетические, технологические и психологические каналы. Его принципиальная новизна заключается в отделении технологического инструментария от конечной цели, поскольку одна и та же технология, например, криптоактивы, может использоваться для решения различных деструктивных задач.

Четвёртый, ключевой критерий, определяет конечную цель воздействия на параметры экономической безопасности, а именно: подрыв валютной стабильности, нелегальный вывод капитала и дискредитацию институтов. Именно этот критерий составляет главное отличие авторской модели, так как он напрямую, а не опосредованно, связывает конкретную цифровую угрозу с макроэкономическими показателями, закреплёнными в качестве стратегических национальных приоритетов. В соответствии с пунктами 66 и 67 подраздела «Экономическая безопасность» Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента России от 2 июля 2021 г. № 400, к таким приоритетам отнесены, в том числе, укрепление финансовой стабильности, защита национального рынка и экономики от внешних и внутренних вызовов и угроз, а также повышение устойчивости национальной валюты [Указ Президента РФ № 400, 2021]. Таким образом, предлагаемый критерий позволяет оперативно оценить, насколько та или иная цифровая угроза создает риски для достижения конкретных целей государственной политики в сфере экономической безопасности.

Сравнительный анализ демонстрирует ряд преимуществ предложенной классификации. В отличие от существующих, она обладает свойством комплексности, интегрируя технические, экономические и институциональные аспекты в единую многомерную характеристику угрозы. Это напрямую повышает её практическую применимость для органов регуляции и контроля. Модель позволяет не только идентифицировать угрозу, но и категоризировать её для выбора адресного инструментария противодействия. Так, угроза, классифицируемая как «внешняя-инфраструктурная-кибернетическая-на подрыв стабильности», требует мобилизации мер киберзащиты со стороны Центрального банка и силовых структур, в то время как угроза по схеме «внутренняя-операционная-технологическая-на нелегальный вывод капитала» диктует необходимость усиления аналитического потенциала Росфинмониторинга. Немаловажным преимуществом является нормативная увязка каждой категории классификации с нормами федерального законодательства о валютном регулировании, противодействии отмыванию доходов и безопасности критической информационной инфраструктуры, что существенно облегчает правоприменительную практику. Модульная структура модели обеспечивает её адаптивность, позволяя легко интегрировать новые механизмы реализации и цели по мере эволюции цифрового ландшафта.

Таким образом, отличительной чертой предложенной классификации является ее системно-

целевой характер. Она функционирует как аналитический конструктор, обеспечивающий последовательную декомпозицию угрозы от технической реализации до макроэкономических последствий. Этот подход трансформирует разрозненные данные о киберинцидентах в структурированную информацию, пригодную для выработки упреждающих и адекватных управленческих решений, что и составляет её основное научное и прикладное значение для укрепления экономической безопасности государства.

Сравнительный анализ позволяет выделить следующие особенности предлагаемого подхода:

1. Системность и комплексность: интегрирует технические, экономические и институциональные аспекты, отсутствующие в узкоспециализированных подходах.

2. Ориентация на цель экономической безопасности: критерий «конечной цели» напрямую связывает угрозу с макроэкономическими параметрами, чего нет в подходах Петренко, Долгих или Щербакова.

3. Практическая применимость: позволяет не просто идентифицировать угрозу, но и определить, какой орган власти (ЦБ, Росфинмониторинг, ФСБ) и какими методами должен на нее реагировать, в зависимости от объекта атаки и механизма реализации.

4. Нормативная увязка: каждая категория угроз может быть соотнесена с конкретными нормами российского законодательства, что облегчает правоприменительную практику.

Для верификации практической применимости предложенной классификации целесообразно провести ее апробацию на примере реальных инцидентов. Такой анализ позволяет перейти от теоретического осмысления к инструменту для посредственного анализа.

Пример 1. Кибератака на систему SWIFT Банка Бангладеш (2016 г.). Данный инцидент может быть систематизирован в рамках авторской классификации следующим образом:

Источник: внешний (международная киберпреступная группировка).

Объект атаки: инфраструктурный (система межбанковских расчетов SWIFT).

Механизм реализации: кибернетический (использование вредоносного ПО для получения доступа к терминалам SWIFT и фальсификации платежных поручений).

Конечная цель: нелегальный вывод капитала (хищение средств со счета Банка Бангладеш в ФРС Нью-Йорка).

Комплексная категоризация инцидента как (Внешняя / Инфраструктурная / Кибернетическая / Нелегальный вывод капитала) не только систематизирует его понимание, но и детерминирует комплекс мер реагирования: усиление киберзащиты периметра (ответ на кибернетический механизм), ужесточение процедур подтверждения транзакций в критической инфраструктуре (ответ на инфраструктурный объект) и международное правовое сотрудничество для розыска виновных и возврата средств (ответ на внешний источник).

Пример 2. Использование криптоактивов для обхода валютных ограничений. В данном случае речь идет не об единичном инциденте, а о классе угроз:

Источник: внутренний/внешний (резиденты, стремящиеся вывести капитал, часто во взаимодействии с нерезидентами).

Объект атаки: операционный (процедуры валютного контроля и идентификации участников операций).

Механизм реализации: технологический (использование децентрализованных криптобирж и p2p-платформ, анонимных кошельков).

Конечная цель: нелегальный вывод капитала и подрыв валютной стабильности (создание неконтролируемого канала оттока капитала).

Категоризация [Внутренне-внешняя/ Операционная/ Технологическая/ Нелегальный вывод капитала] указывает на необходимость адаптации именно операционных процедур контроля (например, разработка методов отслеживания цепочек транзакций в блокчейне) и совершенствования нормативной базы, регулирующей обращение виртуальных активов (Закон № 259-ФЗ), что является ответом на технологический механизм угрозы.

Проведенная апробация подтверждает, что предложенная классификация функционирует как аналитический инструмент, позволяющий не только структурировать информацию об угрозе, но и выстраивать адресную систему мер противодействия, замыкая логическую цепь от идентификации инцидента к выбору релевантных инструментов регулирования.

На основе предложенной классификации разработана концептуальная модель, иллюстрирующая, как различные типы угроз воздействуют на ключевые элементы системы валютного регулирования (рис. 1).

Предлагаемая концептуальная модель представляет собой теоретический конструкт, визуализирующий системные взаимосвязи между деструктивными воздействиями и элементами системы валютного регулирования. Ее принципиальное новшество заключается в отказе от линейного представления об угрозах в пользу сетевой многомерной модели, где каждый тип угрозы получает точку приложения в конкретном элементе системы и одновременно коррелирует с определенным параметром экономической безопасности. В отличие от существующих моделей, которые либо фокусируются на технических аспектах (например, модель «угроза-уязвимость"), либо на экономических последствиях, данная концепция интегрирует оба аспекта в единый причинно-следственный контур.

Рисунок 1 - Концептуальная модель воздействия угроз на ключевые элементы системы валютного регулирования

Модель строится на четырех взаимосвязанных блоках. Первый блок — классифицированные цифровые угрозы — выступает в качестве исходного импульса дестабилизации. Второй блок — ключевые элементы системы валютного регулирования — представляет собой мишени для воздействия. Третий блок — конечная цель воздействия

угрозы. Четвертый блок — параметры экономической безопасности — фиксирует конечные макроэкономические последствия. Принципиальное отличие от других подходов заключается в наличии не прямолинейных, а перекрестных связей между этими блоками, что позволяет моделировать каскадный эффект от единичного инцидента.

Так, кибернетическая атака (механизм), нацеленная на платежную инфраструктуру (объект), инициируемая из-за рубежа (источник) с целью подрыва стабильности национальной валюты (цель), в модели рассматривается не как изолированное событие. Она запускает цепную реакцию: нарушение работы инфраструктуры → сбой в процедурах валютного контроля → искажение данных о движении капитала → падение доверия к национальной валюте → реализация конечной цели по дестабилизации курса. Ни одна из существующих моделей не демонстрирует столь полный трафик трансформации технического инцидента в макроэкономическую угрозу.

Основные преимущества концептуальной модели проявляются в ее прикладном применении. Во-первых, она служит инструментом для стратегического планирования, позволяя органам валютного регулирования выявлять критические узлы системы, наиболее уязвимые для комплексных атак. Например, модель наглядно показывает, что атака на операционные процедуры (например, путем внедрения в программное обеспечение для оформления паспортов сделок) способна не только обеспечить нелегальный вывод капитала, но и дискредитировать сам институт валютного контроля, подрывая доверие к государству как к гаранту экономической стабильности.

Во-вторых, модель обладает прогностическим потенциалом. Анализируя формирующиеся угрозы, такие как развитие квантовых вычислений или децентрализованных финансов (DeFi), можно спрогнозировать их потенциальные точки приложения в системе и заблаговременно разработать превентивные меры. Если новая технология позволяет обойти традиционные механизмы идентификации, модель сразу указывает на риски для операционного блока и связанные с этим последствия для параметров контроля за движением капитала.

В-третьих, модель обеспечивает системность в управлении рисками. Она наглядно демонстрирует, что защита должна выстраиваться не по отдельным элементам (только инфраструктура или только данные), а по всей цепочке взаимосвязанных элементов, блокируя возможность трансформации и эскалации угрозы. Таким образом, предложенная концептуальная модель выступает не только как аналитический инструмент, но и как основа для формирования целостной, адаптивной стратегии укрепления экономической безопасности через совершенствование системы валютного регулирования в цифровую эпоху.

Для противодействия угрозам предлагается следующая логическая модель:

1. Идентификация: обнаружение инцидента (например, попытка несанкционированной валютной операции через взломанный клиент-банк).

2. Классификация: отнесение инцидента к категориям по авторской классификации (источник: внешний/внутренний; объект: операционный; механизм: кибернетический; цель: нелегальный вывод капитала).

3. Оценка воздействия: анализ потенциального ущерба для параметров экономической безопасности (например, сокращение золотовалютных резервов).

4. Выбор инструмента реагирования: применение мер в зависимости от категории:

- правовые: например, возбуждение дела по ст. 193.1 УК РФ (Совершение валютных операций по переводу денежных средств в иностранной валюте или валюте Российской Федерации на счета нерезидентов с использованием подложных документов);

- технические: например, внедрение систем поведенческого анализа транзакций (Anti-Fraud);

- институциональные: например, взаимодействие ЦБ РФ и Росфинмониторинга для блокировки подозрительных операций.

5. Обратная связь и адаптация: такие как, корректировка классификации и процедур на основе нового опыта.

В контексте усиления цифровых вызовов традиционные реактивные модели реагирования, основанные на устранении последствий уже произошедших инцидентов, демонстрируют свою недостаточную эффективность. В отличие от них, предлагаемая авторская логическая модель представляет собой итеративный алгоритм проактивного управления рисками, ядром которого является не разрозненное устранение симптомов, а системный анализ и блокировка угроз на основе их предварительной классификации. Её принципиальное новшество заключается в органичном внедрении разработанной многокритериальной классификации в качестве ключевого аналитического инструмента на этапе идентификации, что кардинально меняет всю последующую логику принятия решений.

Отличие данной модели от существующих, например, стандартных циклов реагирования на киберинциденты (таких как NIST Computer Security Incident Handling Guide), состоит в её чёткой ориентации на обеспечение именно экономической безопасности, а не только IT-безопасности. Если стандартные циклы завершаются этапом «восстановления работоспособности» системы, то предлагаемый алгоритм выходит на уровень «адаптации системы валютного регулирования», предполагающий корректировку нормативно-правовых и процедурных механизмов. Это трансформирует её из технического регламента в стратегический инструмент управления.

Преимущества модели реализуются через последовательность её этапов. Первоначальная идентификация инцидента, например, попытки проведения сомнительной валютной операции через цифровой канал, сменяется этапом его глубинной классификации. На этом этапе, в отличие от общепринятой практики, инцидент не просто фиксируется как «кибератака» или «мошенническая операция», а получает комплексную характеристику по четырём критериям авторской системы. Так, попытка несанкционированного перевода с использованием компрометированных данных может быть классифицирована как [Внутренняя/Операционная/Кибернетическая/Нелегальный вывод капитала]. Эта точная категоризация, в свою очередь, напрямую детерминирует выбор адекватных инструментов реагирования на следующем этапе.

Именно здесь раскрывается ключевое преимущество модели — её способность генерировать адресные, а не универсальные ответные меры. Для приведённого примера это будет означать не просто блокировку конкретной операции, а комплекс действий: применение норм Уголовного кодекса РФ о невозвращении средств из-за границы (ст. 193 УК РФ), усиление процедур двухфакторной аутентификации в банковских системах (технический ответ) и проведение внеплановой проверки кредитной организации регулятором (институциональный ответ). Оценка воздействия на этапе анализа ущерба фокусируется не на стоимости утраченных данных, а на потенциальном сокращении золотовалютных резервов или давлении на валютный курс, что соответствует критерию конечной цели.

Завершающий этап обратной связи и адаптации обеспечивает эволюционное развитие всей системы. Накопленный опыт по конкретным категориям угроз позволяет вносить точечные изменения в регламенты валютного контроля, методики надзора и нормативную базу. Таким образом, предложенная логическая модель замыкает цикл управления, преобразуя единичный

инцидент в системное знание, и формирует самосовершенствующуюся среду для обеспечения устойчивости системы валютного регулирования в условиях цифровизации.

Заключение

Как итог отметим, что проведенное исследование подтвердило гипотезу о том, что существующие подходы к классификации цифровых угроз для системы валютного регулирования являются фрагментарными и не в полной мере учитывают их комплексное воздействие на экономическую безопасность государства. Предложенная авторская многокритериальная классификация, интегрирующая источник, объект, механизм и конечную цель угрозы, позволяет преодолеть этот методологический разрыв.

Ее ключевые преимущества – системность, практическая ориентированность и прямая увязка с параметрами экономической безопасности и нормативной правовой базой. Разработанные на ее основе концептуальная и логическая модели предоставляют органам валютного регулирования и контроля структурированный инструментарий для идентификации, анализа и нейтрализации цифровых вызовов. Дальнейшие исследования могут быть направлены на количественную оценку рисков по каждой категории классификации и разработку на ее основе автоматизированной системы поддержки принятия решений.

Библиография

1. Экономическая безопасность России : общий курс: учебник / А. А. Арбатов, А. А. Ведев, М. И. Гельвановский [и др.] ; Российская академия наук, Институт экономики РАН, Центр финансово-банковских исследований; Российская академия естественных наук, Секция "Проблем макроэкономики и социального рыночного хозяйства", Московское региональное отделение "Макроэкономические и финансовые исследования". – 3-е издание, дополненное и переработанное. – Москва : ООО "Издательство "БИНОМ. Лаборатория знаний", 2009. – 815 с. – ISBN 978-5-9963-0166-9. – EDN QUNUTL.
2. Глазьев, С. Ю. О стратегии устойчивого развития экономики России / С. Ю. Глазьев, Г. Г. Фетисов // Экономические и социальные перемены: факты, тенденции, прогноз. – 2013. – № 1(25). – С. 23-35. – EDN PVQCEL.
3. Петренко, С. А. Управление информационными рисками : Экон. оправд. безопасность : Информ. технологии для инженеров / С. А. Петренко, С. В. Симонов ; Петренко С. А., Симонов С. В.. – Москва : Акад. АйТи, 2004. – 383 с. – (Информационные технологии для инженеров). – ISBN 5-98453-001-5. – EDN QQESJB.
4. Одинцов, С. В. Проблемы квалификации преступлений, сопряженных с использованием криптовалют / С. В. Одинцов, Б. Е. Кошелюк // Вестник Томского государственного университета. – 2023. – № 487. – С. 220-229. – DOI 10.17223/15617793/487/25. – EDN KEHEWG.
5. Коломиец, А. Г. Существенность угроз безопасности финансово-банковской системы / А. Г. Коломиец // Вестник Института экономики Российской академии наук. – 2018. – № 1. – С. 103-117. – DOI 10.24411/2073-6487-2018-00021. – EDN YPNCJT.
6. FATF (2021). Guidance on Digital Identity [Электронный ресурс]. – FATF, Paris. – URL: https://www.fatf-gafi.org/en/publications/Methodsandtrends/Digital-identity-guidance.html (дата обращения: 25.10.2023).
7. Бондарь, А. П. Факторы и угрозы обеспечения финансовой безопасности кредитных организаций / А. П. Бондарь // Финансово-экономическая безопасность Российской Федерации и ее регионов : Сборник материалов V Международной научно-практической конференции, Симферополь, 30 сентября 2020 года. – Симферополь: ФГАОУ ВО «Крымский федеральный университет имени В.И. Вернадского», 2020. – С. 67-69. – EDN TLXIBN.
8. Дигилина, О. Б. Угрозы экономической безопасности в условиях цифровизации / О. Б. Дигилина, А. М. Черняев // Горизонты экономики. – 2023. – № 6(79). – С. 67-75. – EDN QNLCTF.
9. Экономическая безопасность России. Обший курс : учебник / под ред. В. К. Сенчагова. — 6-е изд. - Москва : Лаборатория знаний, 2020. - 818 с. - ISBN 978-5-00101-840-7. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1209184 (дата обращения: 26.04.2025). – Режим доступа: по подписке.
10. Глазьев, С. Ю., Фетисов, Г. Г. О стратегии устойчивого развития экономики России // Экономические и социальные перемены: факты, тенденции, прогноз. 2013. №1 (25). URL: https://cyberleninka.ru/article/n/o-strategii-ustoychivogo-razvitiya-ekonomiki-rossii (дата обращения: 14.06.2025).

11. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации». URL: http://publication.pravo.gov.ru/Document/View/0001202107020016 (дата обращения: 15.10.2025).

Digital Threats to the Currency Regulation System: Classification and Counteraction Models in the Context of Economic Security

Stanislav S. Chebotarev

Doctor of Economic Sciences, Professor,
JSC "Order of the Red Banner of Labor Research Institute of Automatic Equipment named after Academician V.S. Semenikhin",
125319, 7, Svobody str., Moscow, Russian Federation;
e-mail: StSt57@yandex.ru

Vladislav S. Chebotarev

Doctor of Economic Sciences, Professor,
Volga State University of Water Transport,
603950, 5, Nesterova str., Nizhny Novgorod, Russian Federation;
e-mail: vschebotarev@rambler.ru

Aleksandr A. Khmyz

Senior Lecturer,
Nizhny Novgorod Institute of Transport Engineering - branch of Volga State University of Water Transport,
603011, 4, Narodnaya str., Nizhny Novgorod, Russian Federation;
e-mail: g101@yandex.ru

Abstract

Digitalization creates a new risk environment for the currency regulation system as a foundation of economic security. Existing threat classifications are fragmented and do not account for their complex impact. The goal of the research is to develop a multi-criteria classification based on sources, objects, mechanisms, and goals of threats. Its key advantage is the direct connection between the type of threat and economic security parameters, such as currency exchange rate stability. Based on the classification, models for identifying and neutralizing threats are proposed, having practical significance for regulatory authorities.

For citation

Chebotarev S.S., Chebotarev V.S., Khmyz A.A. (2025) Tsifrovyye ugrozy sisteme valyutnogo regulirovaniya: klassifikatsiya i modeli protivodeystviya v kontekste ekonomicheskoy bezopasnosti [Digital Threats to the Currency Regulation System: Classification and Counteraction Models in the Context of Economic Security]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 15 (11A), pp. 119-131. DOI: 10.34670/AR.2026.37.72.011

Keywords

Currency regulation system, economic security, digital threats, threat classification, cyber risks, money laundering (AML/CFT), capital outflow, crypto-assets, financial stability, Rosfinmonitoring.

References

1. *Ekonomicheskaia bezopasnost' Rossii : obshchii kurs: uchebnik* [Economic security of Russia: general course: textbook]. (2009). (3rd ed., enl. and rev.). Moscow: OOO "Izdatel'stvo "BINOM. Laboratoriia znanii". ISBN 978-5-9963-0166-9. EDN: QUNUTL.
2. Glaz'ev, S.Iu., & Fetisov, G.G. (2013). O strategii ustoychivogo razvitiia ekonomiki Rossii [On the strategy of sustainable development of the Russian economy]. *Ekonomicheskie i sotsial'nye peremeny: fakty, tendentsii, prognoz* [Economic and Social Changes: Facts, Trends, Forecast], (1(25)), 23–35. EDN: PVQCEL.
3. Petrenko, S.A., & Simonov, S.V. (2004). *Upravlenie informatsionnymi riskami : Ekon. opravd. bezopasnost' : Inform. tekhnologii dlia inzhenerov* [Information risk management: Economically justified security: Information technologies for engineers]. Moscow: Akademiia AiTi. ISBN 5-98453-001-5. EDN: QQESJB.
4. Odintsov, S.V., & Kosheliuk, B.E. (2023). Problemy kvalifikatsii prestuplenii, sopriazhennykh s ispol'zovaniem kriptovaliut [Problems of qualifying crimes related to the use of cryptocurrencies]. *Vestnik Tomskogo gosudarstvennogo universiteta* [Bulletin of Tomsk State University], (487), 220–229. https://doi.org/10.17223/15617793/487/25 EDN: KEHEWG.
5. Kolomiets, A.G. (2018). Sushchestvennost' ugroz bezopasnosti finansovo-bankovskoi sistemy [The materiality of threats to the security of the financial and banking system]. *Vestnik Instituta ekonomiki Rossiiskoi akademii nauk* [Bulletin of the Institute of Economics of the Russian Academy of Sciences], (1), 103–117. https://doi.org/10.24411/2073-6487-2018-00021 EDN: YPNCJT.
6. FATF. (2021). *Guidance on digital identity*. Retrieved October 25, 2023, from https://www.fatf-gafi.org/en/publications/Methodsandtrends/Digital-identity-guidance.html
7. Bondar', A.P. (2020). Faktory i ugrozy obespecheniia finansovoi bezopasnosti kreditnykh organizatsii [Factors and threats to ensuring the financial security of credit institutions]. In *Finansovo-ekonomicheskaia bezopasnost' Rossiiskoi Federatsii i ee regionov: Sbornik materialov V Mezhdunarodnoi nauchno-prakticheskoi konferentsii* [Financial and economic security of the Russian Federation and its regions: Proceedings of the V International Scientific-Practical Conference] (pp. 67–69). Simferopol: FGAOU VO "Krymskii federal'nyi universitet imeni V.I. Vernadskogo". EDN: TLXIBN.
8. Digilina, O.B., & Cherniaev, A.M. (2023). Ugrozy ekonomicheskoi bezopasnosti v usloviiakh tsifrovizatsii [Threats to economic security in the context of digitalization]. *Gorizonty ekonomiki* [Economic Horizons], 6(79), 67–75. EDN: QNLCTF.
9. Senchagov, V.K. (Ed.). (2020). *Ekonomicheskaia bezopasnost' Rossii. Obshii kurs : uchebnik* [Economic security of Russia. General course: textbook] (6th ed.). Moscow: Laboratoriia znanii. ISBN 978-5-00101-840-7. Retrieved April 26, 2025, from https://znanium.ru/catalog/product/1209184
10. Glaz'ev, S.Iu., & Fetisov, G.G. (2013). O strategii ustoychivogo razvitiia ekonomiki Rossii [On the strategy of sustainable development of the Russian economy]. *Ekonomicheskie i sotsial'nye peremeny: fakty, tendentsii, prognoz* [Economic and Social Changes: Facts, Trends, Forecast], 1(25). Retrieved June 14, 2025, from https://cyberleninka.ru/article/n/o-strategii-ustoychivogo-razvitiya-ekonomiki-rossii
11. *Ukaz Prezidenta RF ot 02.07.2021 № 400 «O Strategii natsional'noi bezopasnosti Rossiiskoi Federatsii»* [Decree of the President of the Russian Federation No. 400 of 02.07.2021 "On the National Security Strategy of the Russian Federation"]. Retrieved October 15, 2025, from http://publication.pravo.gov.ru/Document/View/0001202107020016