Вестник Евразийской науки / The Eurasian Scientific Journal https://esj.today

2025, Том 17, № s1 / 2025, Vol. 17, Iss. s1 https://esj.today/issue-s1-2025.html

URL статьи: https://esj.today/PDF/53FAVN125.pdf

5.2.3. Региональная и отраслевая экономика (экономические науки)

Ссылка для цитирования этой статьи:
Трушанина, А. Д. Трансформация риск-ориентированного подхода для борьбы с кибер-преступностью в условиях цифровизации / А. Д. Трушанина // Вестник евразийской науки. — 2025. — Т. 17. — № s1. — URL: https://esj.today/PDF/53FAVN125.pdf.

For citation:
Trushanina A.D. Transformation of a risk-based approach to combating cybercrime in the context of digitalization. *The Eurasian Scientific Journal*. 2025;17(s1): 53FAVN125. Available at: https://esj.today/PDF/53FAVN125.pdf. (In Russ., abstract in Eng.).

УДК 338

Трушанина Анна Дмитриевна
ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия
Аспирант кафедры «Экономической безопасности и управления рисками»
E-mail: luksemburganna@gmail.com
ORCID: https://orcid.org/0009-0002-7575-3982
РИНЦ: https://elibrary.ru/author_profile.asp?id=1077257

Трансформация риск-ориентированного подхода для борьбы с кибер-преступностью в условиях цифровизации

Аннотация. Настоящее исследование посвящено анализу трансформации риск-ориентированного подхода в целях борьбы с киберпреступностью в рамках противодействия отмыванию доходов, полученных преступным путем, в контексте стремительной цифровизации общества и экономики. Экспоненциальный рост масштабов и изощренности киберпреступлений, связанный с повсеместным проникновением цифровых технологий во все сферы жизни, ставит под сомнение эффективность традиционных реактивных стратегий уголовного преследования. Смещение акцентов на превентивную идентификацию, оценку и митигацию киберрисков рассматривается как необходимое условие для адаптации деятельности надзорных и правоохранительных органов к современным условиям.

В статье систематизируются современные концепции управления киберрисками, прослеживается эволюция подходов к оценке рисков в условиях неопределенности цифровой среды. Особое внимание уделяется проблематике интеграции технологических решений, основанных на больших данных и машинном обучении, в процесс выявления криминальных угроз и аномалий. Обосновывается переход от дискретных методов анализа post factum к динамическому мониторингу рискового ландшафта, превентивному выявлению уязвимостей и угроз. Проведен сравнительный анализ методик оценки киберрисков, моделей организации аналитической работы, механизмов взаимодействия с частным сектором. Особый акцент сделан на выявлении барьеров и драйверов успешного применения риск-ориентированного подхода в сфере ПОД/ФТ в контексте ограниченности ресурсов.

В ходе исследования были разработаны методические рекомендации по трансформации риск-ориентированного подхода в российской правоохранительной системе. Предложена концептуальная модель проактивной идентификации киберугроз на основе комплексного учета технических, социально-экономических и поведенческих факторов риска. Сформулированы предложения по модернизации нормативно-правовой базы, формированию цифровых компетенций сотрудников в целях эффективного превентивного воздействия на

киберпреступность. Результаты исследования имеют высокую практическую ценность для оптимизации правоохранительной и надзорной деятельности в условиях цифровизации. Внедрение динамических методов оценки рисков, алгоритмизация процессов выявления аномалий и прогнозирования угроз на основе продвинутой аналитики данных позволит существенно повысить обоснованность и адресность мер противодействия киберпреступности в рамках противодействия ОД/ФТ. Предлагаемые рекомендации носят универсальный характер и могут быть адаптированы с учетом специфики национальных юрисдикций.

Ключевые слова: киберпреступность; цифровизация; риск-ориентированный подход; управление рисками; большие данные; машинное обучение; ПОД/ФТ; трансформация

Введение

Стремительное развитие и повсеместное проникновение цифровых технологий в жизнь общества формирует качественно новый ландшафт криминальных угроз, затрагивающих легализацию доходов, полученных преступным путем. По данным глобального исследования PwC, в 2020 году потери организаций от киберпреступлений достигли беспрецедентной отметки в 42 млрд долл., продемонстрировав двукратный рост всего за 2 года.[1] В России, согласно статистике Генпрокуратуры, количество преступлений, совершенных с использованием ИКТ, в период пандемии возросло на 73,4 %, составив 25 % от всех зарегистрированных противоправных деяний.[2] В период экономической и политической изоляции в России продолжается сокращение объема сомнительных операций — в 2023 году общий объем сомнительных операций составил около 90,5 млрд рублей.[3] Тенденция к ежегодному сокращению этих объемов связана с деятельностью Росфинмониторинга, Центрального Банка Российской Федерации и правоохранительных органов по борьбе с преступлениями ОД/ФТ. Изменения в экономике, международная обстановка, активное внедрение новых цифровых технологий влияют на изменение структуры сомнительных операций. Преступники в целях легализации преступных доходов задействуют не только новые технологии, но и сектора экономики, которые могли ранее обладать низким уровнем риска ОД/ФТ и не использовались в распространенных схемах отмывания доходов в увеличенных масштабах. Высокая латентность, трансграничный характер, постоянная мутация схем и инструментов кибератак ставят под сомнение эффективность традиционного реактивного подхода к противодействию, основанного на расследовании уже свершившихся инцидентов.

В этих условиях на первый план выходит задача проактивной идентификации, оценки и митигации киберрисков, позволяющая опережающе выявлять и устранять предпосылки преступлений в цифровой среде. Смещение акцентов с наказания на профилактику становится ключевым императивом трансформации моделей работы правоохранительных органов в эпоху тотальной цифровизации. Риск-ориентированный подход, уже доказавший свою состоятельность в корпоративной практике обеспечения кибербезопасности, а также в обеспечении экономической безопасности государства, рассматривается в качестве перспективной основы для модернизации государственной политики борьбы с киберугрозами.

---

[1] Fighting fraud: A never-ending battle. PwC's Global Economic Crime and Fraud Survey — 2020– Режим доступа — https://www.pwc.at/de/publikationen/studien/global-economic-crime-and-fraud-survey-2020.pdf (дата обращения: 11.03.2025).

[2] МВД России. Краткая характеристика состояния преступности в Российской Федерации за январь — декабрь 2020 года — Режим доступа — https://xn--b1aew.xn--p1ai/reports/item/22678184/ (дата обращения: 11.03.2025).

[3] Банк России. Структура подозрительных операций и отрасли экономики, формировавшие спрос на теневые финансовые услуги за 2023 год — Режим доступа — https://www.cbr.ru/analytics/podft/resist_sub/2023/ (дата обращения: 12.03.2025).

Концептуальное осмысление возможностей и ограничений применения рискового подхода в контексте противодействия цифровой преступности приобретает высокую актуальность как в научно-исследовательском, так и в практическом аспектах. Систематизация накопленного опыта оценки и управления рисками ИКТ, поиск эффективных механизмов имплементации в деятельность правоохранительных структур позволят существенно продвинуться в решении стратегической задачи адаптации институтов безопасности и правопорядка к вызовам новой технологической реальности.

Формирование динамической картины угроз цифрового пространства, основанной на превентивном выявлении факторов риска и уязвимостей, даст возможность оптимизировать ресурсную базу, обеспечить высокую адресность оперативно-розыскных мероприятий. Важнейшим условием практической реализации потенциала риск-ориентированного подхода является налаживание эффективного взаимодействия с частным сектором — провайдерами цифровых услуг, разработчиками средств защиты, научно-исследовательскими центрами.

Целью работы является развитие научных представлений о сущности, возможностях и ограничениях риск-ориентированного подхода как концептуальной основы модернизации правоохранительной деятельности по противодействию преступности в цифровой среде, а также разработка прикладного инструментария его внедрения в практику российских органов внутренних дел с учетом передового зарубежного опыта.

Для реализации поставленной цели в исследовании решаются следующие **задачи**:

- Проследить эволюцию научных подходов к идентификации и оценке киберрисков, выявить ключевые детерминанты трансформации рискового ландшафта в условиях цифровой конвергенции технологий, бизнес-процессов, поведенческих паттернов и определить связь со сферой ПОД/ФТ.
- Систематизировать лучшие практики имплементации риск-ориентированного подхода, специализирующихся на борьбе с киберпреступностью, и выявить их концептуальные основы.
- Провести сравнительный анализ применяемых методологий оценки цифровых угроз, организационных моделей управления рисками, механизмов государственно-частного партнерства.
- Разработать концептуальную модель проактивной идентификации факторов риска киберпреступности на основе комплексного учета технических, социально-экономических, поведенческих детерминант противоправной активности в цифровом пространстве.

1. Материалы и методы

При написании автором использовались следующие методы: анализ и синтез, сравнительный, статистический и исторический анализы, обобщение научных исследований и статей, визуализация данных.

Теоретико-методологический фундамент исследования формируют концепции цифровой криминологии, превентивного воздействия на преступность и противодействия отмыванию доходов в современных условиях. Основополагающее значение имеют труды Д. Уолла [1], М. Йар [2], Д. Страттона [3], заложившие основы анализа генезиса и динамики криминальных феноменов под воздействием цифровизации. Развитию представлений о факторах становления жертвой преступного посягательства в киберпространстве, особенностях механизма преступного поведения посвящены работы Т. Хольта [4].

53FAVN125
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

Концептуальные подходы к оценке и управлению киберрисками на основе проактивной идентификации угроз и уязвимостей представлены в трудах Р. Фон Сольмса [5], А. Шостака [6]. Научные работы П. Гербрандса [7] затрагивают анализ последствий имплементации регулятивных мер в сфере ПОД/ФТ и поведение преступников, связанных с отмыванием доходов, полученных преступным путем.

Важную роль в понимании организационных аспектов имплементации риск-ориентированного подхода в правоохранительной деятельности сыграли исследования Б. Дюпона [8], раскрывающие институциональные, кадровые, технологические барьеры и драйверы внедрения инноваций в полицейскую практику.

Особое внимание уделено отечественной научной литературе, в частности трудам следующих авторов: Е.К. Волчинская, Г.А. Грицай, Л. Дембоски [9], И.Б. Горелик [10], А.Л. Осипенко [11], М.В. Губич [12], П.И. Иванов [13], Д.В. Будко [14], Д.П. Алейников [15], А.С. Александров, И.А. Александрова [16] и другие.

Информационной базой исследования также послужили аналитические материалы Росфинмониторинга, Банка России, официальные сайты и Интернет-ресурсы по тематике научного поиска.

2. Результаты и обсуждение

Проведенный анализ научного дискурса позволяет констатировать кардинальную трансформацию природы и механизмов преступности в условиях тотальной цифровизации общества. Повсеместное проникновение ИКТ во все сферы жизнедеятельности, сращивание физической и виртуальной реальности порождает качественно новые криминальные феномены и практики. Как подчеркивает Д. Уолл, преступность обретает сетевой, децентрализованный характер, оперируя глобальными потоками данных вне привязки к территориальным юрисдикциям [1]. Цифровая анонимность и экстерриториальность позволяют злоумышленникам атаковать множественные цели из любой точки мира, оставаясь недосягаемыми для правоохранительных органов конкретного государства. Предикатное (первичное) преступление в сочетании с легализацией преступных доходов представляет собой противоправное деяние, при совершении которого был получен доход [17]. Меры по противодействию отмыванию преступных доходов, в том числе и связанные с предикатными преступлениями, усложняют условия среды для отмывания доходов, но в то же время это заставляет преступников искать новые способы отмывания, специализироваться на каком-либо секторе или инструментарии, а также сотрудничать между собой [7].

Экспоненциальный рост объемов генерируемой пользователями информации расширяет масштабы потенциального становления жертвой киберпреступности. По оценке IBM, сейчас каждый день производится более 2,5 квинтиллионов байт личных сведений, которые хранятся в слабо защищенных облачных хранилищах и становятся объектом кражи и злоупотреблений.[4] Цифровые следы человеческой активности — история поисковых запросов, связей в социальных сетях, финансовых транзакций, геолокации — несут в себе широкий спектр криминальных рисков, включая манипуляции, шантаж, вымогательство. В опубликованном Отчете о глобальных рисках 2025 года Всемирного экономического форума (ВЭФ) отмечается рост уровня неопределенности, как в рамках долгосрочного, так и

[4] IBM Security. Cost of a Data Breach Report 2020 — Режим доступа — https://www.content.shi.com/SHIcom/ContentAttachmentImages/SharedResources/Solutions/Security/ibm-121321-Cost-of-a-Data-Breach-Report-2020.pdf (дата обращения: 11.03.2025).

53FAVN125
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

краткосрочного прогнозирования.[5] В двухлетней перспективе главным риском является ложная и вводящая в заблуждение информация — она является ведущим механизмом влияния на выбор и мнение людей о политической обстановке, продуктах и услугах. Распространение такой информации существенно усложняет текущую геополитическую и геоэкономическую обстановку. Риски, связанные с неблагоприятными последствиями использования искусственного интеллекта, учитывая стремительный характер развития информационных технологий, в наибольшей степени могут проявить себя через десять лет. Однако уже сейчас искусственный интеллект активно используется для генерирования ложной и вводящей в заблуждение информации, использующейся в преступных интересах.

Киберпространство становится средой воспроизводства принципиально новых бизнес-моделей криминального предпринимательства. Коммерциализация хакерских услуг по модели «преступность-как-сервис», формирование экосистемы торговли цифровыми уязвимостями и вредоносным ПО на теневых рынках дает возможность рядовым правонарушителям без технических навыков организовывать масштабные кибератаки. За счет платформенных решений происходит размытие традиционных иерархических структур организованной преступности, тем самым затрудняется идентификация лидеров и рядовых исполнителей.

Цифровизация существенно расширяет радиус поражения и тяжесть последствий преступных посягательств. Уязвимости программного кода, ошибки конфигурации облачной инфраструктуры могут использоваться злоумышленниками для компрометации информационных систем критически значимых для общества секторов — здравоохранения, энергетики, транспорта, финансовой сферы. По оценкам Cybersecurity Ventures, к 2025 году глобальные убытки от кибератак могут достичь 10,5 трлн долл., что составляет 11 % мирового ВВП.[6] При этом непрямой ущерб от нарушения конфиденциальности данных, подрыва доверия к цифровым сервисам, социальной и политической дестабилизации в разы превосходит прямые финансовые потери. По всему миру общая стоимость потерь от взломов и мошенничества только на рынке криптовалют составила более 3 млрд долларов в 2024 году, что превысило значение предыдущего года на 15 %.[7] В Годовом отчете Росфинмониторинга за 2023 год отмечается рост рисков ОД/ФТ по следующим 5 основным направлениям: схемы обналичивания с участием физических лиц и «дропов», финансовое мошенничество с применением методов социальной инженерии, деятельность финансовых пирамид в сети Интернет, использование драгоценных металлов и камней в схемах по отмыванию преступных доходов и незаконному вывозу капитала из страны, использование криптовалют в целях ОД/ФТ.[8] Все эти риски связаны между собой из-за повсеместного использования цифровых технологий, киберпреступность задействована в том или ином виде во всех отмеченных направлениях.

---

[5] World Economic Forum. Global Risks Report 2025 — Режим доступа — https://www.weforum.org/publications/global-risks-report-2025/ (дата обращения: 12.03.2025).

[6] Cybercrime Magazine. Cybercrime To Cost The World $10.5 Trillion Annually By 2025 — Режим доступа — https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/ (дата обращения: 11.03.2025).

[7] РБК. ЦБ оценил объем операций россиян в криптовалютах. Главное из отчета. — Режим доступа — https://www.rbc.ru/crypto/news/665066579a794764c51aa31f?from=copy (дата обращения: 11.03.2025).

[8] Федеральная служба по финансовому мониторингу. Годовой отчет о работе Федеральной службы по финансовому мониторингу за 2023 год. — Режим доступа — https://www.fedsfm.ru/content/files/documents/%D0%BF%D1%83%D0%B1%D0%BB%D0%B8%D1%87%D0%BD%D1%8B%D0%B9%20%D0%BE%D1%82%D1%87%D0%B5%D1%82%20%D1%80%D1%84%D0%BC%202023.pdf (дата обращения: 11.03.2025).

53FAVN125
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

Изменение структуры сомнительных операций в соответствии с влиянием цифровых технологий на сферу ПОД/ФТ можно отразить через изменение структуры транзитных операций повышенного риска вне банковского сектора. Эти операции показывают изменение инструментов, которые могут использоваться хозяйствующими субъектами для отмывания доходов. Статистику предоставляет ЦБ РФ с 2015 года, по структуре транзитных операций она доступна только в процентном выражении. В денежном выражении общий объем операций повышенного риска вне банковского сектора Транзитные операции предшествуют обналичиванию и выводу средств за рубеж, часто могут сопровождаться сменой оснований платежей, «ломкой» НДС. Например, в 2018 году доля таких операций с использованием сектора закупки и обращения драгоценных металлов и драгоценных камней составляла 6 % в числе транзитных операций повышенного риска[9], а в 2023 году доля выросла до 24 %.[10] При учете, что в 2023 году объем операций без согласия клиентов увеличился по сравнению с 2022 годом на 11,48 %, и растет доля мошенничества с использованием цифровых технологий, можно говорить о том, что преступники от традиционных схем отмывания стали переходить к более специализированным способам и секторам, которые ранее не затрагивались так часто. Правоохранительным и надзорным органам необходимо учитывать, что структура рисков отмывания по секторам не постоянная, и применять это в своей деятельности по борьбе с ОД/ФТ.

Таким образом, цифровая преступность представляет собой результат сложного сопряжения социотехнических факторов, продуцирующих принципиально новые виды криминальных угроз. Эти угрозы носят неочевидный, труднопредсказуемый характер, плохо поддаются раннему выявлению традиционными методами оперативно-розыскной деятельности. Как отмечает М. Лунд, современные тренды цифровизации — Интернет вещей, искусственный интеллект, робототехника — порождают экспоненциальную динамику развития рисков, требующую качественной перестройки моделей управления безопасностью. Традиционный подход, сфокусированный только на расследовании уже произошедших преступлений, больше не соответствует современным реалиям быстро меняющихся киберугроз. Такая реактивная стратегия неэффективна в условиях постоянной трансформации и усложнения цифровых угроз, требуя перехода к более гибким и упреждающим методам обеспечения кибербезопасности (рис. 1).

[9] Банк России. Структура сомнительных операций в банковском секторе в 2018 году. — Режим доступа — https://www.cbr.ru/Content/Document/File/83370/2018.pdf (дата обращения: 11.03.2025).

[10] Банк России. Структура подозрительных операций и отрасли экономики, формировавшие спрос на теневые финансовые услуги. — Режим доступа — https://www.cbr.ru/analytics/podft/resist_sub/2023/ (дата обращения: 11.03.2025).

53FAVN125
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

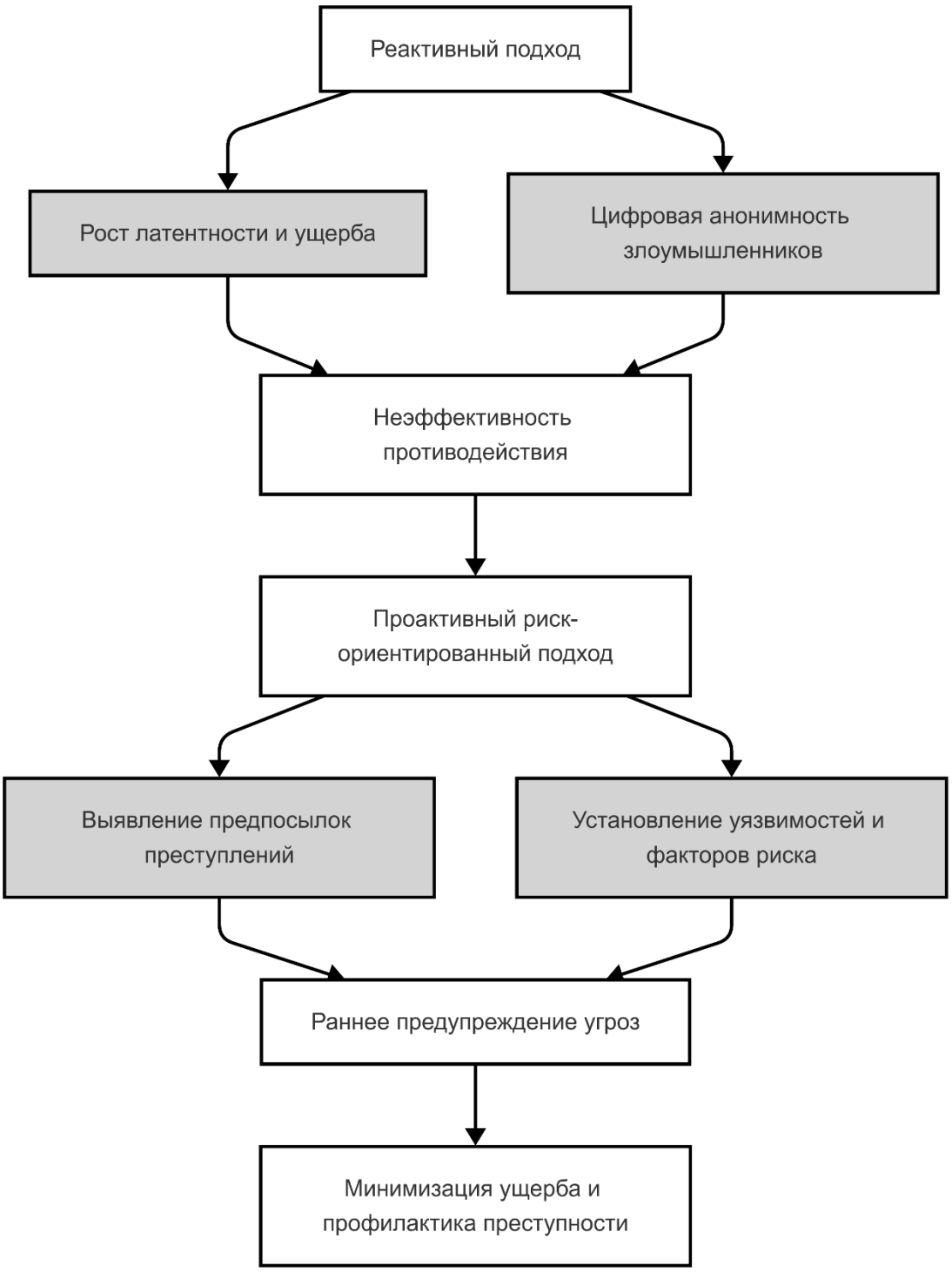

Рисунок 1. *Сравнение традиционного реактивного и проактивного риск-ориентированного подходов к борьбе с киберпреступностью (составлено автором)*

В этих условиях на первый план выходит задача превентивной идентификации и митигации криминальных рисков в цифровой среде. Как показано на рисунке 1, в отличие от реактивной парадигмы реагирования на уже случившиеся инциденты, риск-ориентированный подход фокусируется на заблаговременном выявлении факторов, являющихся причинами преступного поведения. Речь идет о проактивном сканировании цифрового пространства на предмет обнаружения уязвимостей, аномалий, индикаторов подготовки кибератак. Оценка рисков как вероятности реализации угроз и тяжести их последствий позволяет расставить

53FAVN125
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

приоритеты превентивных мер, оптимизировать ресурсы правоохранительных и надзорных органов.

Реализация потенциала риск-ориентированного подхода требует кардинального переосмысления методологии анализа киберугроз. Традиционные дискретные модели оценки на основе ретроспективных данных об уже состоявшихся инцидентах не позволяют отслеживать динамику зарождающихся угроз в условиях экспоненциального роста цифровых взаимодействий. По мнению А. Шостака, проблема киберрисков не может быть решена средствами классической теории вероятностей и актуарной математики [6]. Турбулентность цифровой среды, высокая гетерогенность атакующих технологий и мотивов требует перехода к парадигме динамического риск-менеджмента, ориентированного на проактивную идентификацию аномалий в больших потоках неструктурированных данных.

Систематизация практик оценки киберрисков в правоохранительной деятельности позволила выделить ряд общих тенденций перехода от реактивного к проактивному подходу. Традиционные модели ретроспективной оценки, основанные на статистике зафиксированных преступлений, все чаще уступают место превентивным инструментам анализа цифровых следов (диджитал-форензики) и предиктивной аналитики. Фокус смещается с прошлых инцидентов на раннее выявление сигналов о потенциальных угрозах, поиск закономерностей в массивах структурированных и неструктурированных данных, моделирование сценариев реализации рисков.

Таблица 1

Концептуальная основа
риск-ориентированного подхода к противодействию киберпреступности

Уровень управления	Категории рисков	Методы оценки	Инструменты митигации
Стратегический	— Геополитические — Макроэкономические — Социокультурные	— PESTEL-анализ — Сценарное планирование — Экспертные панели	— Международное сотрудничество — Совершенствование законодательства — Государственно-частное партнерство
Оперативный	— Отраслевые — Технологические — Кадровые	— Бенчмаркинг — Сетевой анализ — Профилирование субъектов	— Проактивный мониторинг — Обмен киберразведданными — Целевые профилактические меры
Тактический	— Уязвимости ПО/конфигураций — Инциденты ИБ — Следы ранее неизвестных угроз	— Сканирование на уязвимости — Расследование инцидентов — Охота на угрозы	— Устранение уязвимостей — Реагирование на инциденты — Охота на угрозы (Threat Hunting)

Составлено автором на основе [18; 19]

Как видно из таблицы 1, управление киберрисками в правоохранительной деятельности носит многоуровневый характер. На стратегическом уровне оценка фокусируется на понимании общего контекста угроз, определяемого геополитическими, макроэкономическими, социокультурными факторами. Ключевыми инструментами выступают методы PESTEL-анализа, сценарного планирования, форсайт-сессии с привлечением широкого круга экспертов. Митигация стратегических рисков предполагает развитие международного сотрудничества, гармонизацию уголовного законодательства, формирование доверенной среды государственно-частного партнерства в противодействии киберпреступности.

Оперативный уровень управления киберрисками связан с отраслевой и технологической спецификой криминальных угроз. Правоохранительные органы активно применяют методы

53FAVN125
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

сравнительного анализа (бенчмаркинга) для выявления лучших практик защиты в различных секторах экономики. Особое значение приобретают инструменты сетевой аналитики и профилирования субъектов теневой киберактивности на основе графов связей, выделения центральности и влиятельности узлов [20]. Для минимизации рисков используются проактивный мониторинг индикаторов угроз, межведомственный обмен киберразведданными, целевое воздействие на криминогенные факторы.

Тактический срез рискового анализа сосредоточен на выявлении конкретных уязвимостей информационной инфраструктуры, технических артефактов кибератак, следов ранее неизвестных угроз (APT). Ключевую роль играют методы этичного хакинга и тестирования на проникновение, компьютерной криминалистики и реагирования на инциденты. Проактивное выявление индикаторов компрометации и «охота на угрозы» (threat hunting) дополняется оперативным устранением брешей в защите, минимизацией «окна уязвимости».

Практики реализации риск-ориентированного подхода существенно варьируются в зависимости от уровня развития цифровых компетенций и аналитических возможностей правоохранительных органов. Сравнительный анализ кейсов позволил идентифицировать 5 ключевых измерений зрелости оценки киберрисков (табл. 2):

- цели и задачи (от ретроспективной отчетности к проактивному предотвращению);
- методология (от экспертных оценок к предиктивному моделированию);
- данные (от структурированных выборок к обогащению из гетерогенных источников);
- аналитика (от описательной статистики к алгоритмам машинного обучения);
- организация (от разрозненных инициатив к интегрированным междисциплинарным командам).

Таблица 2

Уровни зрелости правоохранительных органов в оценке киберрисков

Уровень зрелости	Начальный	Развивающийся	Определенный	Продвинутый	Оптимизирующий
Цели и задачи	Соблюдение требований отчетности	Устранение последствий инцидентов	Проактивная идентификация угроз	Предупреждение криминальных рисков	Адаптивное управление безопасностью
Методология оценки рисков	Экспертные оценки post factum	Количественные метрики событий	Сценарный анализ и стресс-тестирование	Предиктивное моделирование и симуляции	Динамическая оптимизация контролей
Данные для анализа	Структурированные выборки прошлых периодов	Потоковая телеметрия и сетевые логи	Обогащение из внешних источников	Неструктурированный контент соцсетей и дарквеба	Интеграция данных кибервразведки и partner feeds
Аналитический инструментарий	Описательная статистика и визуализация	Правила корреляции событий SIEM	Поведенческая аналитика и профилирование	Алгоритмы машинного обучения и языковые модели	ИИ-ассистенты реального времени
Организация работы	Эпизодические проекты узких специалистов	Центр мониторинга SOC	Выделенная служба управления рисками	Кросс-функциональные группы реагирования	Интегрированные междисциплинарные киберкоманды

Составлено автором

Как показано в таблице 2, правоохранительные органы эволюционируют от базового уровня, характеризующегося реактивным соблюдением регуляторных требований post factum, к статусу проактивных центров превосходства, реализующих динамическую адаптацию к изменениям ландшафта угроз. Если на начальных стадиях оценка рисков носит спорадический

53FAVN125
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

характер, основываясь на экспертных мнениях в отношении уже состоявшихся инцидентов, то зрелые организации переходят к предиктивному моделированию будущих сценариев на базе обогащенных и разнородных массивов данных. Простая визуализация статистики преступлений уступает место продвинутой аналитике, выявляющей неочевидные закономерности с помощью алгоритмов машинного обучения и обработки естественного языка (NLP). Разрозненные процессы трансформируются в непрерывный инжиниринг безопасности, реализуемый междисциплинарными проектными командами.

Результаты исследования подтверждают определяющую роль технологий больших данных и искусственного интеллекта как драйверов трансформации управления киберрисками. Правоохранительные органы стран-лидеров активно экспериментируют с предиктивными инструментами выявления цифровых угроз на основе анализа неструктурированной информации из открытых источников (OSINT) и теневого интернета (DARKINT). Алгоритмы машинного обучения применяются для построения профилей рисков подозреваемых, обнаружения аномальных паттернов в сетевом трафике, идентификации индикаторов подготовки кибератак. Внедрение платформ обогащения данных из множественных источников (data fusion) позволяет формировать целостную картину киберкриминальной обстановки, визуализировать взаимосвязи между субъектами, объектами и контекстами преступлений.

Вместе с тем интеграция продвинутой аналитики в процессы оценки киберрисков сопряжена с рядом концептуальных и прикладных вызовов. Ключевыми барьерами, выделенными респондентами, являются:

- Дефицит репрезентативных данных для обучения прогностических моделей вследствие высокой латентности и волатильности цифровых следов преступлений.
- Непрозрачность и плохая интерпретируемость алгоритмов, порождающая проблемы доверия к результатам среди сотрудников и сложности в доказывании обоснованности профилактических мер.
- Усиление рисков дискриминации и нарушения презумпции невиновности в условиях опоры на вероятностные оценки, не всегда учитывающие индивидуальный социальный контекст.
- Недостаточность цифровых компетенций и навыков аналитической работы у значительной части оперативного состава, приверженность традиционным реактивным практикам.
- Узкие места ИТ-инфраструктуры, затрудняющие сбор, хранение и обработку больших массивов неструктурированной информации.
- Отсутствие четких стандартов оценки валидности предиктивных инструментов, правовых и этических принципов их применения.

По оценке экспертов, зрелая реализация риск-ориентированного подхода требует не просто технологических инноваций, но глубокой трансформации институциональной культуры, доминирующих установок и поведенческих паттернов сотрудников. Внедрение проактивной аналитики должно сопровождаться целенаправленными мерами по развитию междисциплинарных компетенций на стыке цифровой криминалистики, науки о данных, социальной психологии и правовой защиты. Необходима выработка твердых этических гарантий и регуляторных рамок, обеспечивающих справедливость и подотчетность алгоритмических решений в высокочувствительной сфере правопорядка.

53FAVN125
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

На основе анализа передового опыта разработана концептуальная модель риск-ориентированного управления для российской правоохранительной системы (рис. 2).

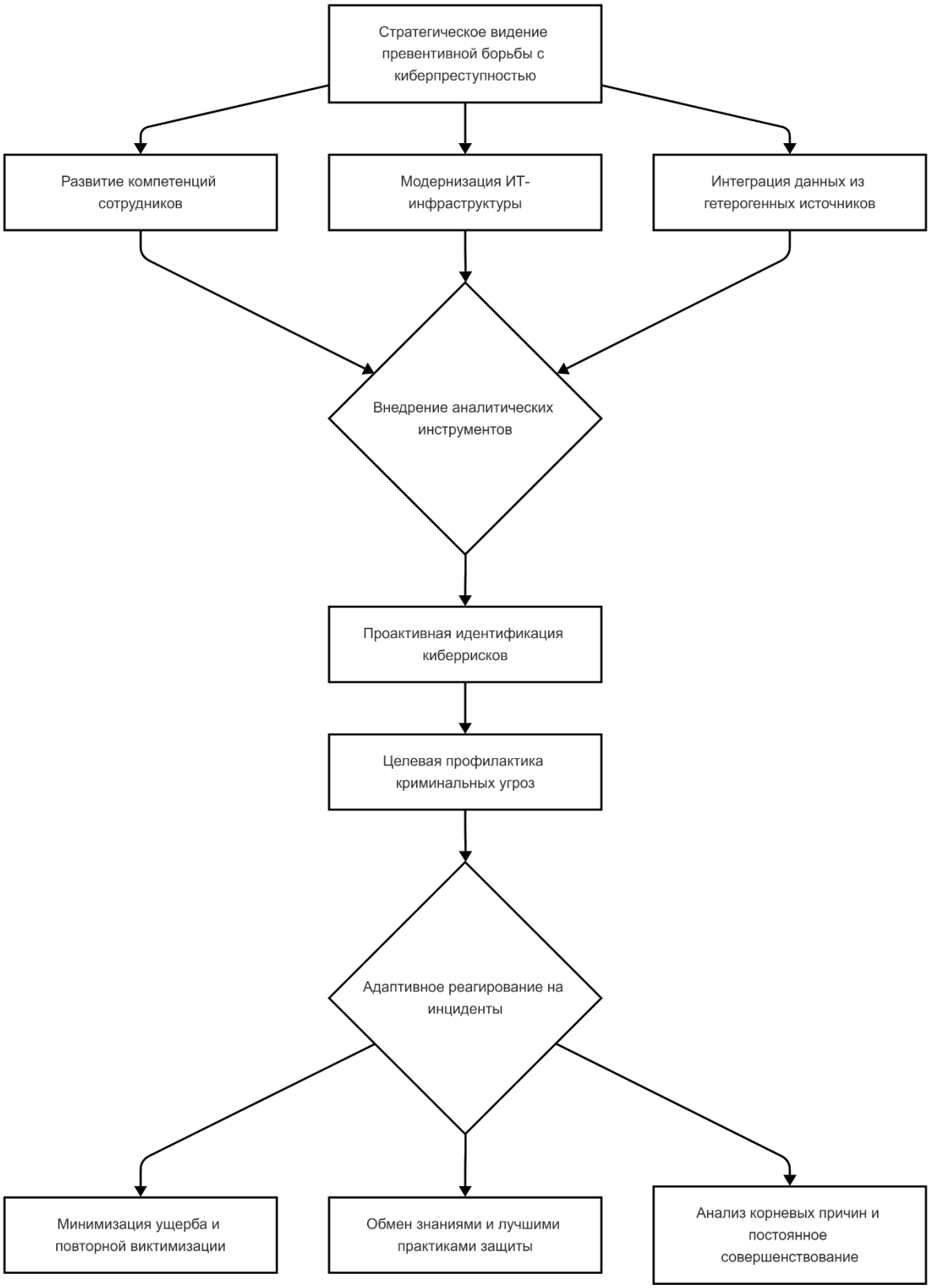

Рисунок 2. *Концептуальная модель риск-ориентированного подхода к управлению киберпреступностью (составлено автором на основе синтеза лучших практик и экспертных рекомендаций)*

53FAVN125
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

Фундаментом трансформации выступает стратегическое видение проактивного предотвращения киберугроз за счет упреждающего воздействия на их причины и условия. Ключевые компоненты потенциала реализации этого видения — развитие междисциплинарных цифровых компетенций сотрудников, модернизация ИТ-ландшафта ведомств, обеспечение механизмов доступа к множественным источникам данных. Ядром модели является внедрение продвинутого аналитического инструментария на базе алгоритмов машинного обучения, позволяющих динамически выявлять закономерности и взаимосвязи в больших потоках структурированной и неструктурированной информации.

Конечной целью риск-ориентированного управления должно стать устойчивое снижение уровня виктимизации граждан и ущерба от киберпреступлений за счет динамической адаптации оперативно-профилактических мер к изменениям криминальной обстановки. По мере наращивания потенциала правоохранительной системы в оценке и митигации цифровых рисков фокус смещается с рутинного реагирования на инциденты к стратегической аналитике причинно-следственных связей, формированию банка знаний об индикаторах угроз и эффективных практиках защиты. Превентивное устранение предпосылок и контекстов преступлений дополняется непрерывным организационным обучением, распространением проверенных кейсов в профессиональном сообществе.

Имплементация предлагаемой модели в деятельность органов внутренних дел предполагает поэтапную реализацию следующих мер:

1. Законодательное закрепление требований, обязанностей и процедур по оценке киберрисков, регламентация процедур сбора и обработки цифровых следов, введения унифицированной системы классификации и учета киберпреступлений.
2. Развитие механизмов информационного взаимодействия и координации с частным сектором: интеграция индикаторов угроз от вендоров средств защиты, провайдеров телекоммуникационных услуг, исследовательских организаций. Формирование единого реестра (базы знаний) типовых сценариев реализации криминальных рисков в цифровой среде.
3. Формирование междисциплинарных проектных команд на стыке подразделений киберкриминалистики, информационной безопасности, оперативно-розыскной деятельности и аналитики данных. Проведение регулярных учений и кросс-функциональных семинаров для развития навыков совместного реагирования на инциденты, унификации подходов к оценке киберрисков.
4. Модернизация системы профессиональной подготовки и повышения квалификации сотрудников. Разработка специализированных образовательных программ, сочетающих компетенции цифровой криминалистики, науки о данных, предиктивной аналитики, методов социальной инженерии. Организация стажировок в ведущих исследовательских центрах и ИТ-компаниях.
5. Внедрение гибкой и масштабируемой инфраструктуры сбора, обработки и хранения неструктурированных данных из множественных источников. Развитие инструментов интеллектуального анализа больших массивов информации на базе алгоритмов машинного обучения, предиктивного моделирования и обогащения данных.
6. Формирование организационной культуры, поощряющей проактивность, инновационность мышления, готовность к постоянному экспериментированию и адаптации. Учреждение системы нематериальной мотивации за инициативы по совершенствованию методов профилактики киберпреступности.

53FAVN125
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

7. Разработка единой методологии оценки эффективности риск-ориентированных практик на основе сочетания количественных показателей динамики преступности и качественных индикаторов превентивной активности. Проведение регулярного бенчмаркинга лучших региональных кейсов, тиражирование проверенных подходов.

Ключевой предпосылкой успешного перехода к новой модели является обеспечение вовлеченности и слаженного взаимодействия всех субъектов правоохранительной и надзорной деятельности — от руководителей ведомств до линейных сотрудников. Особое значение имеет синергия традиционных функций криминальной полиции, следствия, дознания и подразделений киберкриминалистики, информационной безопасности, аналитики данных. Формирование единого видения превентивной борьбы с цифровой преступностью, общей ментальной карты киберрисков позволит преодолеть ведомственные барьеры и высвободить творческую энергию для поиска нестандартных решений.

Таким образом, риск-ориентированный подход в современных реалиях подразумевает трансформацию фокуса правоохранительных и надзорных органов с узковедомственных практик борьбы с преступностью на стратегическое системное управление средой кибербезопасности через вовлечение всех значимых субъектов детерминации и превенции криминальной активности. Речь идет о формировании проактивной культуры бдительности к цифровым угрозам, совместном проектировании многоуровневой архитектуры защиты от постоянно эволюционирующих форм виртуального криминала. Такая система взглядов необходима и для эффективной борьбы с отмыванием доходов, полученных преступным путем. Достижение столь амбициозной цели требует пересмотра базовых принципов и инструментов работы в цифровом пространстве, развития компетенций социотехнического анализа и моделирования неопределенности. Способность правоохранительной и надзорной системы к динамической адаптации ценностей, структуры, процессов под сетевую логику взаимодействий в условиях тотальной цифровизации становится важнейшей предпосылкой обеспечения эффективного социального контроля над преступностью в высокотехнологичную эпоху.

Выводы

Резюмируя результаты проведенного исследования, можно сформулировать следующие ключевые выводы:

1. Цифровая трансформация общества и экономики порождает принципиально новые виды криминальных угроз, связанные с широким проникновением ИКТ во все сферы жизнедеятельности. Анонимность, трансграничность, гиперподключенность киберпространства затрудняют идентификацию и пресечение противоправных деяний традиционными реактивными методами правоохранительных органов. Экспоненциальный рост масштабов и ущерба от киберпреступлений актуализирует задачу смещения акцентов в сторону проактивной превенции, воздействия на причины и условия криминальной активности.

2. Систематизация научного дискурса позволила проследить эволюцию подходов к оценке киберрисков от статичных моделей, ориентированных на количественный анализ данных о свершившихся атаках, к динамической парадигме проактивного выявления уязвимостей и аномалий на основе предиктивной аналитики. Зрелая реализация риск-ориентированного управления требует перехода от изолированных суждений экспертов к построению вероятностных сценариев угроз, интегрирующих технические, социально-экономические, поведенческие факторы в единую объяснительную рамку.

53FAVN125
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

3. Анализ лучших практик правоохранительной деятельности позволил выделить 5 ключевых измерений потенциала имплементации рискового подхода: гибкость целеполагания, комплексность методологии оценки, объем и разнообразие используемых данных, продвинутость аналитического инструментария, адаптивность организационных процессов. Определяющую роль в трансформации играет внедрение технологий больших данных и искусственного интеллекта, обеспечивающих выявление неочевидных взаимосвязей и построение прогностических моделей поведения злоумышленников.

4. Разработана концептуальная модель риск-ориентированного управления киберпреступностью, синтезирующая технологические и человеческие факторы потенциала проактивной превенции цифровых угроз. Ключевыми компонентами выступают: стратегическое видение безопасного развития ИКТ, комплексные компетенции сотрудников, продвинутая аналитическая инфраструктура, гибкие организационные процессы. Конечным результатом является снижение ущерба от киберпреступлений за счет динамической адаптации защитных мер к изменениям среды, формирование экспертного сообщества и культуры кибербезопасного поведения.

Обобщая вышеизложенное, можно заключить, что риск-ориентированный подход выступает перспективной концептуальной основой трансформации правоохранительной деятельности в цифровую эпоху. Смещение фокуса с анализа ретроспективных данных к динамическому моделированию будущих угроз становится стратегическим приоритетом обеспечения безопасности и правопорядка в условиях нарастающей цифровизации всех сфер общественной жизни. Эффективное противостояние вызовам киберпреступности требует синергии потенциала государства, бизнеса, научного сообщества и граждан в заблаговременном выявлении факторов риска и воздействии на первопричины противоправной активности. Только так можно эффективно бороться со сложными, деструктивными и латентными экономическими процессами, такими как отмывание преступных доходов и киберпреступность.

Вместе с тем практическое внедрение рискового подхода не следует рассматривать как разовую кампанию или очередную институциональную реформу. Речь идет о запуске долгосрочного, многостороннего и нелинейного процесса изменений, затрагивающего фундаментальные аспекты функционирования надзорной и правоохранительной системы — от культуры управления до операционных процедур взаимодействия с внешней средой. Масштабы цифровой трансформации преступности предопределяют необходимость непрерывной итерации и совершенствования методик и инструментов оценки рисков, поддержания высокой готовности к адаптации под динамику развития экосистемы информационного противоборства.

В заключение следует отметить, что риск-ориентированный подход не является панацеей и не способен полностью устранить киберугрозы. Однако системные инвестиции в проактивную аналитику, алгоритмизацию процессов выявления аномалий, интеграцию гетерогенных данных, развитие прогностических компетенций значительно повышают устойчивость надзорной и правоохранительной системы к криминогенным вызовам цифровой реальности. Формируя опережающее видение ландшафта угроз, структурируя факторы и сценарии их реализации, располагая арсеналом превентивных защитных мер, государство получает принципиально новые возможности для стратегического управления безопасностью и поддержания режима законности в киберпространстве.

53FAVN125
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

ЛИТЕРАТУРА

1. Wall D.S. Policing cybercrime: networked and social media technologies and the challenges for policing / D.S. Wall, M.L. Williams — DOI: 10.1080/10439463.2013.780227 // Policing and Society. — 2013. — Т. 23, № 4. — С. 409–412.
2. Yar M. The Novelty of «Cybercrime»: An Assessment in Light of Routine Activity Theory // European Journal of Criminology. — 2005. — Т. 2, № 4. — С. 407–427.
3. Stratton G. Crime and justice in digital society: towards a «digital criminology»? / G. Stratton, A. Powell, R. Cameron — DOI: 10.5204/ijcjsd.v6i2.355 // International Journal for Crime, Justice and Social Democracy. — 2017. — Т. 6, № 2. — С. 17–33.
4. Holt T. Cybercrime and digital forensics: An introduction / T. Holt, A. Bossler, K. Seigfried-Spellar. — 2nd ed. — Routledge, 2022. — 500 с.
5. Von Solms R. From information security to cyber security / R. Von Solms, J. Van Niekerk — DOI: 10.1016/j.cose.2013.04.004 // Computers & Security. — 2013. — Т. 38. — С. 97–102.
6. Shostack A. Threat modeling: Designing for security. — Wiley, 2014. — 624 с.
7. Gerbrands P. The effect of anti-money laundering policies: an empirical network analysis / P. Gerbrands [et al.] — DOI: 10.1140/epjds/s13688-022-00326-w. // EPJ Data Science. — 2022. — Т. 11, № 1. — С. 15.
8. Dupont B. The cyber-resilience of financial institutions: significance and applicability // Journal of Cybersecurity. — 2019. — Т. 5, № 1. — С. 1–17.
9. Управление интернетом и борьба с киберпреступностью: глобальные угрозы и российские интересы / Е.К. Волчинская, Г.А. Грицай, Л. Дембоски [и др.] // Индекс безопасности. — 2013. — Т. 19, № 4(107). — С. 89–106. — EDN RRRNCX.
10. Горелик И.Б. Международно-правовое противодействие киберпреступности: процесс формирования и проблемы управления / И.Б. Горелик — DOI 10.54449/76585_2021_1_12_87. // Вестник Дипломатической академии МИД России. Международное право. — 2021. — № 1(12). — С. 87–104 — EDN PDTHCE.
11. Осипенко А.Л. Использование механизмов государственно-частного партнерства в сфере противодействия киберпреступности: преимущества, риски и ограничения / А.Л. Осипенко // Вестник Краснодарского университета МВД России. — 2019. — № 4(46). — С. 105–113. — EDN LTCWNB.
12. Губич М.В. Правовые предпосылки к развитию государственно-частного партнерства в сфере противодействия киберпреступности / М.В. Губич // Борьба с преступностью: теория и практика: Тезисы докладов VIII Международной научно-практической конференции, Могилев, 23 апреля 2020 года. — Могилев: Учреждение образования «Могилевский институт Министерства внутренних дел Республики Беларусь», 2020. — С. 463–466. — EDN XKGESF.
13. Иванов П.И. Внедрение метода риск-ориентированного подхода в деятельность по оперативно-розыскному противодействию экономическим и коррупционным преступлениям (в порядке постановки проблемы) / П.И. Иванов // Юристъ-Правоведъ. — 2023. — № 1(104). — С. 80–89. — EDN BHAOHS.

53FAVN125
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

14. Будко Д.В. Концепция риск-ориентированного подхода в условиях развития технологий искусственного интеллекта / Д.В. Будко — DOI 10.37973/VESTNIKKUI-2024-57-6. // Вестник Казанского юридического института МВД России. — 2024. — Т. 15, № 3(57). — С. 49–58 — EDN MXTPAQ.

15. Алейников Д.П. Основные проблемы противодействия киберпреступности в эпоху цифровой трансформации / Д.П. Алейников — DOI 10.24412/2076-1503-2022-6-229-231. // Образование и право. — 2022. — № 6. — С. 229–231 — EDN PGCNNS.

16. Александров А.С. Организационно-правовой механизм противодействия киберпреступности в эпоху цифровых технологий / А.С. Александров, И.А. Александрова // Юридическая наука и практика на рубеже эпох: уроки прошлого, взгляд в будущее (к 135-летию со дня рождения профессора Юрия Петровича Новицкого): сборник трудов XIV Всероссийских декабрьских юридических чтений в Костроме: Всероссийская научно-практическая конференция, Кострома, 14–16 декабря 2017 года. — Кострома: Костромской государственный университет, 2018. — С. 303–309. — EDN VKCUFQ.

17. Кондратьева Е.А. Процессы противодействия легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма (ПОД/ФТ): категориальные подходы / Е.А. Кондратьева — DOI 10.18334/tek.1.1.37716. // Теневая экономика. — 2017. — Т 1, № 1. — С. 31–46 — EDN YSFADE.

18. Бессонов А.А. Цифровая криминалистическая модель преступления как основа противодействия киберпреступности / А.А. Бессонов // Академическая мысль. — 2020. — № 4(13). — С. 58–61. — EDN CHQQAU.

19. Желудков М.А. Особенности противодействия киберпреступности в России и зарубежных странах / М.А. Желудков, А.М. Попов, М.М. Дубровина — DOI 10.25724/VAMVD.CVWX. // Вестник Волгоградской академии МВД России. — 2018. — № 3(46). — С. 97–102 — EDN MIBSMX.

20. Leukfeldt E.R. A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists / E.R. Leukfeldt, E.R. Kleemans, W.P. Stol — DOI: 10.1007/s10611-016-9660-4 // Crime, Law and Social Change. — 2017. — Т. 67. — С. 21–37.

53FAVN125
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

Trushanina Anna Dmitrievna
Financial University under the Government of the Russian Federation, Moscow, Russia
E-mail: luksemburganna@gmail.com
ORCID: https://orcid.org/0009-0002-7575-3982
RSCI: https://elibrary.ru/author_profile.asp?id=1077257

Transformation of a risk-based approach to combating cybercrime in the context of digitalization

Abstract. This study is devoted to the analysis of the transformation of a risk-based approach to countering cybercrime in the context of the rapid digitalization of society and the economy. The exponential growth in the scale and sophistication of cybercrime, associated with the widespread penetration of digital technologies into all spheres of life, calls into question the effectiveness of traditional reactive criminal prosecution strategies. The shift in emphasis to preventive identification, assessment, and mitigation of cyber risks is seen as a necessary condition for law enforcement agencies to adapt to the new criminal reality.

The article systematizes modern concepts of cyber risk management, traces the evolution of approaches to risk assessment in the conditions of uncertainty of the digital environment. Particular attention is paid to the problems of integrating technological solutions based on big data and machine learning into the process of identifying criminal threats and anomalies. The transition from discrete methods of post factum analysis to dynamic monitoring of the risk landscape, preventive identification of vulnerabilities and threats is substantiated. A comparative analysis of cyber risk assessment methods, models for organizing analytical work, and mechanisms for interaction with the private sector is carried out. Particular emphasis is placed on identifying barriers and drivers for the successful application of a risk-oriented approach in the field of AML/CFT in the context of limited resources.

The study developed methodological recommendations for transforming the risk-oriented approach in the Russian law enforcement system. A conceptual model of proactive identification of cyber threats based on a comprehensive accounting of technical, socio-economic and behavioral risk factors is proposed. Proposals are formulated for modernizing the regulatory framework, forming digital competencies of employees for the purpose of effective preventive impact on cybercrime. The results of the study are of high practical value for optimizing law enforcement and supervisory activities in the context of digitalization. The introduction of dynamic risk assessment methods, algorithmization of the processes of identifying anomalies and predicting threats based on advanced data analytics will significantly improve the validity and targeting of measures to combat cybercrime as part of countering ML/FT. The proposed recommendations are universal in nature and can be adapted to the specifics of national jurisdictions.

Keywords: cybercrime; digitalization; risk-based approach; risk management; big data; machine learning; digital competencies; AML/CFT; transformation

53FAVN125
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com