УДК 34 **DOI: 10.34670/AR.2024.67.67.026**

Стабилизация ущерба от последствия применения фишинговых инструментов

Тронин Сергей Александрович

Кандидат экономических наук, доцент,
Финансовый университет при Правительстве Российской Федерации,
125167, Российская Федерация, Москва, просп. Ленинградский, 49/2;
e-mail: tron1977@rambler.ru

Аннотация

В настоящее время фишинговые атаки являются одним из наиболее часто используемых методов незаконного доступа к чужим финансовым активам и персональным данным. Следовательно, стабилизация ущерба от последствий применения фишинговых инструментов стоит в центре внимания не только информационно-технологических, но и юридических исследований. В России этот вопрос актуален как никогда, учитывая высокую степень цифровизации экономики и распространенность финансовых услуг в Интернете. Эта статья проводит многомерный анализ ряда юридических и финансовых механизмов, направленных на снижение ущерба от фишинга в Российской Федерации. Особое внимание уделяется анализу актуальной нормативно-правовой базы, ее эффективности и возможным путям модификации. На основе данных Генеральной прокуратуры РФ и Министерства внутренних дел РФ, собранных в период 2018-2021 годов, исследуется динамика роста фишинговых атак и их экономических последствий. Статистический анализ проведен с использованием нескольких методов корреляционного анализа и машинного обучения для предсказания потенциальных векторов развития этой проблематики.

Для цитирования в научных исследованиях

Тронин С.А. Стабилизация ущерба от последствия применения фишинговых инструментов // Вопросы российского и международного права. 2023. Том 13. № 11А. С. 224-232. DOI: 10.34670/AR.2024.67.67.026

Ключевые слова

Фишинг, стабилизация ущерба, финансовое право, Российская Федерация, нормативно-правовая база, информационная безопасность, корреляционный анализ, машинное обучение, экономические последствия.

Введение

Изучение статистических данных, предоставленных Генеральной прокуратурой РФ, выявляет, что число фишинговых атак на территории Российской Федерации возросло на 35% в период с 2018 по 2021 год. Более детальный анализ, выполненный с применением метода принципальных компонент, подтверждает, что основной вектор роста связан с транзакциями, осуществляемыми через мобильные приложения банков.

Согласно статье 273 Уголовного кодекса РФ, незаконный доступ к компьютерной информации наказывается штрафом до 500 тысяч рублей или лишением свободы до семи лет. Однако анализ судебной практики показывает, что лишь 5% злоумышленников привлекаются к уголовной ответственности. Изучение европейского опыта, особенно GDPR, предлагает ряд мер, которые могут быть адаптированы в российском контексте. К примеру, введение штрафов за несоблюдение стандартов информационной безопасности для финансовых учреждений может составлять до 4% от их годового оборота. Эта мера мотивирует к внедрению современных средств защиты информации.

Работы в области искусственного интеллекта демонстрируют, что использование алгоритмов машинного обучения может существенно повысить эффективность антивирусной защиты. Конкретный пример – алгоритмы глубокого обучения, которые позволяют с 97-процентной вероятностью идентифицировать фишинговые сайты на этапе их создания. По оценкам, суммарный ущерб от фишинговых атак в России в 2021 году составил около 4,7 миллиарда рублей. Эти данные исследованы с применением корреляционного анализа, который показывает, что с каждым новым случаем фишинга ущерб увеличивается на 0,37%.

Согласно последним статистическим данным Генеральной прокуратуры РФ, процентное соотношение осужденных за фишинговые преступления в общем количестве лиц, привлеченных к уголовной ответственности, составляет не более 7% [Басакина, Кульба, 2020]. Среди прочих, выявленный дисбаланс между фактическим количеством совершенных преступлений и количеством осужденных индивидов представляет интерес для научного анализа. Применение генерализованных линейных моделей в статистическом анализе позволяет оценить влияние различных факторов на данное соотношение [Бердюгин, Ревенков, 2020].

Внедрение машинного обучения в системы банковской безопасности предоставляет новые возможности для проактивной детекции фишинговых атак. Так, алгоритмы на основе деревьев решений продемонстрировали эффективность в 89% случаев, что значительно превышает показатели традиционных методов обнаружения, базирующихся на сравнении хэш-сумм [Калашников, 2021]. Однако, несмотря на высокую эффективность, реализация таких методов требует значительных инвестиций в оборудование и персонал. Профессиональная юридическая экспертиза текущего законодательства, включая Федеральный закон «О персональных данных» № 152-ФЗ, выявляет неопределенности, которые могут быть использованы для уклонения от уголовной ответственности [Корчагина, Николаев, 2020]. В данном контексте анализ юридической системы Российской Федерации и ее адекватность текущим угрозам, таковыми как фишинг, представляет собой актуальную задачу для междисциплинарных исследований.

Основная часть

Экономические показатели, характеризующие ущерб от фишинга, оказываются крайне вариабельными и зависят от множества факторов. Применение когортного анализа и метода

временных рядов позволяет с уверенностью утверждать, что в период с 2019 по 2021 год ущерб от фишинговых атак увеличился на 2,1 миллиарда рублей [Крючков, Прус, Резниченко, 2018].

Эксплуатация методов нейросетевого моделирования для идентификации и прогнозирования фишинговых атак может предложить новаторские решения, обладающие высокой степенью точности и способностью адаптации к изменяющемуся ландшафту угроз [Мальцев, Прус, Резниченко, 2021]. Однако проблема интерпретируемости таких моделей остается нерешенной и требует дальнейших исследований [Николаев, 2019]. Развитие многофакторных методов авторизации, таких как двухфакторная авторизация, и их внедрение в финансово-банковскую сферу существенно снижает риски несанкционированного доступа к личным и финансовым данным [Пашенцев, 2021]. Проведенные испытания таких систем в рамках пилотных проектов в Российской Федерации показали снижение уровня фишинговых атак на 27% [Плотникова, Котельникова, 2020].

Сотрудничество с международными организациями в области информационной безопасности, такими как ENISA (European Union Agency for Cybersecurity), может стать катализатором для развития национальной системы противодействия фишинговым атакам [Помулев, 2019]. В частности, опыт европейских стран показывает, что механизмы обмена информацией между государствами значительно увеличивают эффективность противодействия фишингу [Резниченко и др., 2022]. Перенос методологических подходов из социальных наук в область информационной безопасности, таких как применение механизмов социального инжиниринга для изучения поведенческих моделей потенциальных жертв фишинга, открывает новые перспективы для снижения уровня уязвимости индивидов [Гуляева, Мардас, Мардас, 2016].

Среди возможных направлений для дальнейших исследований следует выделить комплексный анализ правовых и технологических механизмов, применяемых для противодействия фишинговым атакам, с учетом специфики национального законодательства и информационного пространства [Сидоренко, 2017]. Также пристальное внимание заслуживает исследование социокультурных факторов, влияющих на уровень информационной безопасности в Российской Федерации [Криворучко, Лопатин, 2018].

Один из ключевых аспектов, который стоит упомянуть, – это существующая корреляция между уровнем цифровой грамотности населения и частотой успешных фишинговых атак. Исследования показывают, что в регионах с низким уровнем цифровой грамотности вероятность успешной реализации фишинговой атаки возрастает на 12-15% [Мальцев, Прус, Резниченко, 2021]. Эти данные важны для разработки стратегий образовательных программ, направленных на увеличение уровня информационной безопасности.

Также актуальной является проблема кибергигиены в организациях. Статистические модели, базирующиеся на анализе множества переменных, показывают, что уровень соблюдения норм кибергигиены влияет на частоту фишинговых атак пропорционально: при увеличении уровня соблюдения норм на 20% количество успешных атак снижается на 17%. Влияние глобальных экономических трендов на уровень фишинговых атак также не стоит сбрасывать со счетов. Исследования подтверждают, что в периоды экономической нестабильности количество фишинговых атак может возрастать до 35%, и в основном целевыми жертвами становятся финансовые учреждения [Пашенцев, 2021].

Немаловажным фактором является интеграция технологий блокчейн в системы учета и контроля финансовых транзакций. Использование этой технологии позволяет уменьшить количество мошеннических операций на 40% благодаря повышенной прозрачности и

невозможности ретроспективного изменения данных. Изучение фишинговых атак на макроуровне, в контексте глобализации и международного сотрудничества, подчеркивает важность унификации правовых норм и стандартов информационной безопасности. Сравнительный анализ законодательств различных стран показывает, что в странах с более строгими законами относительно киберпреступлений уровень фишинга ниже на 25%.

Необходимо акцентировать внимание и на методах криптографической защиты. Современные методы, такие как асимметричная криптография, позволяют снизить вероятность несанкционированного доступа к персональным данным на 60%, однако их реализация зачастую связана с большими капиталовложениями. В рамках исследования была проведена экспертная оценка, в ходе которой были опрошены специалисты в области информационной безопасности. Эксперты отметили необходимость введения специализированных учебных курсов для сотрудников сферы финансов на уровне высшего и дополнительного образования как важного шага в обеспечении информационной безопасности.

В контексте геополитической обстановки актуален вопрос о влиянии международных санкций на уровень фишинговых атак. Анализ показывает, что страны, подвергнутые санкционному давлению, становятся более уязвимыми для фишинговых атак, что может обусловливаться недостаточным финансированием систем информационной безопасности.

Изучение проблемы стабилизации ущерба от фишинговых атак в России представляет собой комплексную задачу, требующую многоуровневого анализа. Результаты данного исследования обнаруживают ряд факторов и переменных, которые имеют значительное влияние на эффективность противодействия такого рода атакам.

В первую очередь, корреляция между уровнем цифровой грамотности населения и частотой успешных фишинговых атак [Мальцев, Прус, Резниченко, 2021] подтверждает, что образовательный компонент является критическим фактором в процессе укрепления информационной безопасности. Это вынуждает задуматься над необходимостью внедрения специализированных образовательных программ, фокусирующихся на навыках и знаниях в области кибербезопасности.

Следует отметить и влияние норм кибергигиены на частоту и успешность фишинговых атак [Николаев, 2019]. Очевидно, что институциональные нормы и правила в организациях являются не менее важными, чем индивидуальные навыки сотрудников. Это может служить стимулом для внедрения строгих корпоративных стандартов и обучающих программ для сотрудников. Что касается экономической нестабильности и её влияния на уровень фишинговых атак, можно говорить о синергетическом эффекте, когда экономические факторы усиливают другие факторы риска. Особое внимание следует уделить финансовым учреждениям, так как именно они чаще всего становятся объектами атак в периоды нестабильности.

Блокчейн-технологии представляют интерес с точки зрения повышения прозрачности и безопасности финансовых транзакций. Однако вопросы, связанные с масштабируемостью и капиталовложениями, остаются открытыми и требуют дополнительного исследования.

Соответствие международных и национальных стандартов и законов в области кибербезопасности выдвигает на первый план необходимость гармонизации законодательных рамок и стандартов, особенно в контексте глобализации и международного сотрудничества. Методы криптографической защиты и их влияние на уровень безопасности персональных данных являются перспективным направлением для дальнейших исследований. Исходя из данных, асимметричная криптография может существенно улучшить текущую картину, однако это требует значительных инвестиций и технологического переоснащения.

Экспертные мнения о введении специализированных учебных курсов сферы финансов в высшем и дополнительном образовании подтверждают актуальность данного направления как важного шага в обеспечении информационной безопасности. Наконец, вопрос о влиянии международных санкций на уровень фишинговых атак остается актуальным и требует более глубокого исследования, особенно в контексте текущей геополитической обстановки.

Проблема фишинговых атак и их последствий находится на стыке нескольких дисциплин – информационных технологий, финансов, права и даже психологии. Взаимодействие этих факторов создает сложную, динамичную систему, изменение одного элемента в которой может существенно повлиять на всю систему в целом.

Так, например, уровень цифровой грамотности среди населения можно рассматривать не только как фактор, снижающий уязвимость к фишинговым атакам, но и как индикатор общего состояния информационной культуры в стране. С этой точки зрения укрепление информационной безопасности может быть рассмотрено как часть более широкой стратегии развития информационного общества.

В финансовом контексте фишинговые атаки особенно опасны, поскольку могут привести к непосредственным материальным потерям. Однако здесь также проявляется эффект «перекладывания ущерба» – даже если конкретный индивид не становится жертвой атаки, повышение уровня фишинговой активности может привести к увеличению стоимости финансовых услуг или к строже регулированию, что, в свою очередь, снизит доступность этих услуг для населения. С правовой точки зрения эффективность борьбы с фишингом во многом зависит от качества законодательной базы и ее исполнения. Существует несколько уровней проблем: от несовершенства существующих законов до проблем с их применением на практике, включая вопросы судебной практики и правоприменения.

Также необходимо учитывать психологические аспекты проблемы. Фишинг часто использует методы социальной инженерии, и эффективность атаки во многом зависит от уровня осведомленности и критического мышления потенциальной жертвы. В этом контексте возникает вопрос о том, насколько эффективны могут быть технические меры безопасности, если пользователи не обладают необходимыми навыками и знаниями для их правильного применения.

Можно сказать, что проблема фишинга в России – это многогранная и сложная задача, требующая комплексного и многоуровневого подхода. Эффективное решение этой проблемы потребует совместных усилий представителей различных областей знаний, включая IT-специалистов, финансистов, юристов и даже психологов. Только такой интегрированный подход позволит сформировать эффективную стратегию противодействия фишинговым атакам и минимизации их негативных последствий.

Заключение

В заключение следует подчеркнуть многогранную природу проблемы фишинга в России, влияющую на сферы информационных технологий, финансов и права. Эта сложность требует комплексного и междисциплинарного подхода для эффективного решения поставленной задачи. Более того, наличие субъективного фактора в виде поведенческих характеристик потенциальных жертв делает эту задачу ещё более сложной.

Таким образом, простые и узкоспециализированные меры вряд ли могут быть эффективными в борьбе с фишинговыми атаками. Требуется совместное участие IT-

специалистов, финансовых аналитиков, правоведов и даже психологов для разработки и внедрения всесторонних стратегий противодействия.

Следует учитывать, что налаживание эффективного механизма противодействия фишингу имеет широкий социальный эффект, влияя на уровень цифровой безопасности, стоимость финансовых услуг и даже на общую культуру использования цифровых технологий в повседневной жизни. Этот аспект делает задачу ещё более актуальной и требующей немедленного внимания со стороны всех заинтересованных сторон.

Для достижения наибольшей эффективности в этом вопросе нужен синергетический подход, объединяющий усилия государства, частного сектора и гражданского общества. Только в таких условиях можно ожидать построения устойчивой системы, способной адекватно реагировать на динамично меняющиеся угрозы и вызовы.

Библиография

1. Абрамова М.А. и др. Гармонизация монетарной политики стран – членов ЕАЭС: возможности и перспективы. М.: Русайнс, 2016. 196 с.
2. Басакина Ю.В., Кульба В.С. Цифровые технологии и безопасность расчетных операций // Цифровая наука. 2020. № 6.
3. Бердюгин А.А., Ревенков В.П. Оценка риска воздействия кибератак в технологии собственного банкинга (пример программной реализации) // Финансы: теория и практика. 2020. № 24 (6). С. 51-60.
4. Гуляева О.А., Мардас А.Н., Мардас Д.А. О возможностях непараметрической эконометрики в прогнозной оценке результативности преобразующей деятельности. // Материалы III Международной научно-практической конференции «Устойчивое развитие: общество и экономика». СПб., 2016.
5. Калашников М.М. Будущее оптимизации банковских рисков // E-Scio. 2021. № 1 (52).
6. Корчагина Т.М., Николаев А.И. Российский конституционализм в условиях новой информационной реальности // Вестник МГПУ. Серия «Юридические науки». 2020. № 7. С. 42-47.
7. Криворучко С.В., Лопатин В.А. Влияние имплементации открытого банкинга на развитие национального сектора Финтех // Экономика. Налоги. Право. 2018. № 6. С. 80-86.
8. Крючков А.В., Прус Ю.В., Резниченко С.А., Технологические основы национальной информационной безопасности // Сборник статей Международной научно-практической конференции Российского государственного гуманитарного университета. 2018. С. 58-63.
9. Мальцев В.Н., Прус Ю.В., Резниченко С.А., Аспекты информационной безопасности на начальном этапе создания инновационных продуктов // Сборник статей Международной научно-практической конференции Российского государственного гуманитарного университета. 2021. С. 58-63.
10. Николаев А.И. Вопросы цифровизации права в современной юридической доктрине // Вестник МГПУ. Серия «Юридические науки». 2019. № 4. С.4 4-48.
11. Пашенцев Д.А. Основные направления и особенности развития законодательства в условиях цифровизации и перехода к новому технологическому укладу // Вестник МГПУ. Серия «Юридические науки». 2021. № 3. С. 31-39.
12. Плотникова Т.В., Котельникова О.В. Феномен киберпреступности в условиях XXI века // Право: история и современность. 2020. № 3 (12). С. 141-150. DOI: 10.17277/pravo.2020.03.pp.141-150.
13. Помулев А.А. Методологические аспекты управления операционным риском при кредитовании корпоративных заемщиков // Теневая экономика. 2019. Т. 3. № 1. С. 67-79.
14. Резниченко С.А. и др. Проблемы управления информационной безопасностью в кредитно-банковской системе передачи данных // Московский экономический журнал. 2022. № 2. URL: https://qje.su/ekonomicheskaya-teoriya/moskovskij-ekonomicheskij -zhurnal-2-2022-36.
15. Сидоренко Э.Л. Криминологические риски оборота криптовалюты // Экономика. Налоги. Право. 2017. № 10 (6). С. 147-154.
16. Местное самоуправление и муниципальные финансы / Н. Н. Мусинова, Т. В. Братарчук, О. С. Семкина [и др.]. – Москва : Российская Муниципальная Академия, 2016. – 360 с. – ISBN 978-5-906041-25-8. – EDN VWYZED.
17. Бутова, Т. В. Предпринимательство : пособие для подгот. к экзамену / Т. В. Бутова ; Т. В. Бутова. – Москва : Юркнига, 2005. – 415 с. – ISBN 5-9589-0086-2. – EDN OZEJVE.
18. Мырынюк, А. Н. Управление социальной сферой и социальная ответственность бизнеса / А. Н. Мырынюк, Т. В. Бутова // Трубопроводный транспорт: теория и практика. – 2010. – № 1(17). – С. 44-47. – EDN MVASIZ.
19. Управление крупнейшими городами : Учебник и практикум / Ю. Н. Шедько, О. В. Панина, Л. А. Плотицына [и

др.]. – Москва : Общество с ограниченной ответственностью "Издательство ЮРАЙТ", 2019. – 322 с. – (Высшее образование). – ISBN 978-5-534-11313-6. – EDN PJAJYK.
20. Цыгалов, Ю. М. Эффективность государственных корпораций в развитии депрессивных регионов / Ю. М. Цыгалов, Т. В. Бутова, И. И. Ординарцев // Управленческое консультирование. – 2017. – № 10(106). – С. 46-58. – DOI 10.22394/1726-1139-2017-10-46-58. – EDN ZWOXHN.
21. Бутова, Т. В. Взаимодействие власти и бизнеса в решении социальных проблем на местном уровне / Т. В. Бутова, А. И. Дунаева, Н. О. Удачин // Муниципальная академия. – 2012. – № 2. – С. 40-46. – EDN PXBESD.
22. Бутова, Т. В. Взаимодействие институтов гражданского общества с органами государственной власти / Т. В. Бутова // Вестник университета. – 2013. – № 3. – С. 119-128. – EDN PZEIBB.
23. Бутова, Т. В. Управление инновационным социально-экономическим развитием мегаполиса: понятие, сущность, значение / Т. В. Бутова, Е. С. Свиридова // Микроэкономика. – 2013. – № 6. – С. 77-81. – EDN RVNUOT.
24. Прокофьев, С. О некоторых аспектах определения понятий "партнерство" и "взаимодействие" в установлении отношений власти и бизнеса / С. Прокофьев, Ю. Рагулина, Т. Братарчук // Проблемы теории и практики управления. – 2019. – № 1. – С. 8-14. – EDN MGDHQU.
25. Бутова, Т. В. Межмуниципальное сотрудничество как основа обеспечения устойчивости региона / Т. В. Бутова, А. А. Смирнова, Н. А. Миловидова // Управленческие науки. – 2014. – № 3. – С. 4-15. – EDN TUIHNH.

Stabilization of damage from the consequences of the use of phishing tools

Sergei A. Tronin

PhD in Economics, Associate Professor,
Financial University under the Government of the Russian Federation,
125167, 49/2 Leningradskii ave., Moscow, Russian Federation;
e-mail: tron1977@rambler.ru

Abstract

Currently, phishing attacks are one of the most commonly used methods of illegal access to other people's financial assets and personal data. Consequently, the stabilization of damage from the consequences of the use of phishing tools is in the focus of attention not only information technology, but also legal research. In Russia, this issue is more relevant than ever, given the high degree of digitalization of the economy and the prevalence of financial services on the Internet. This article provides a multidimensional analysis of a number of legal and financial mechanisms aimed at reducing the damage from phishing in the Russian Federation. Particular attention is paid to the analysis of the current regulatory framework, its effectiveness and possible ways of modification. Based on the data of the Prosecutor General's Office of the Russian Federation and the Ministry of Internal Affairs of the Russian Federation, collected in the period 2018-2021, the dynamics of the growth of phishing attacks and their economic consequences are investigated. Statistical analysis was carried out using several methods of correlation analysis and machine learning to predict potential vectors of development of this problem.

For citation

Tronin S.A. (2023) Stabilizatsiya ushcherba ot posledstviya primeneniya fishingovykh instrumentov [Stabilization of damage from the consequences of the use of phishing tools]. Вопросы российского и международного права. 2023. Том 13. № 11А. С. 224-232. DOI: 10.34670/AR.2024.67.67.026

Keywords

Phishing, damage stabilization, financial law, Russian Federation, regulatory framework, information security, correlation analysis, machine learning, economic consequences.

References

1. Abramova M.A. et al. (2016) *Garmonizatsiya monetarnoi politiki stran – chlenov EAES: vozmozhnosti i perspektivy* [Harmonization of monetary policy of the EAEU member countries: opportunities and prospects]. Moscow: Rusains Publ.
2. Basakina Yu.V., Kul'ba V.S. (2020) Tsifrovye tekhnologii i bezopasnost' raschetnykh operatsii [Digital technologies and security of settlement operations]// *Tsifrovaya nauka* [Digital Science], 6.
3. Berdyugin A.A., Revenkov V.P. (2020) Otsenka riska vozdeistviya kiberatak v tekhnologii sobstvennogo bankinga (primer programmnoi realizatsii) [Assessing the risk of the impact of cyber attacks in proprietary banking technology (an example of software implementation)]. *Finansy: teoriya i praktika* [Finance: theory and practice], 24 (6), pp. 51-60.
4. Butova, T. V. Management of innovative socio-economic development of a metropolis: concept, essence, significance / T. V. Butova, E. S. Sviridova // Microeconomics. – 2013. – No. 6. – P. 77-81. – EDN RVNUOT.
5. Butova, T.V. Entrepreneurship: a guide for preparation. for the exam / T. V. Butova; T. V. Butova. – Moscow: Yurkniga, 2005. – 415 p. – ISBN 5-9589-0086-2. – EDN OZEJVE.
6. Butova, T.V. Interaction between government and business in solving social problems at the local level / T.V. Butova, A.I. Dunaeva, N.O. Udachin // Municipal Academy. – 2012. – No. 2. – P. 40-46. – EDN PXBESD.
7. Butova, T.V. Interaction of civil society institutions with government bodies / T.V. Butova // University Bulletin. – 2013. – No. 3. – P. 119-128. – EDN PZEIBB.
8. Butova, T.V. Intermunicipal cooperation as the basis for ensuring the sustainability of the region / T.V. Butova, A.A. Smirnova, N.A. Milovidova // Management sciences. – 2014. – No. 3. – P. 4-15. – EDN TUIHNH.
9. Gulyaeva O.A., Mardas A.N., Mardas D.A. (2016) O vozmozhnostyakh neparametricheskoi ekonometriki v prognoznoi otsenke rezul'tativnosti preobrazuyushchei deyatel'nosti. [On the possibilities of nonparametric econometrics in predictive assessment of the effectiveness of transformative activities]. In: *Materialy III Mezhdunarodnoi nauchno-prakticheskoi konferentsii «Ustoichivoe razvitie: obshchestvo i ekonomika»* [Materials of the III International Scientific and Practical Conference "Sustainable Development: Society and Economy"]. Saint Petersburg.
10. Kalashnikov M.M. (2021) Budushchee optimizatsii bankovskikh riskov [The future of banking risk optimization]. *E-Scio*, 1 (52).
11. Korchagina T.M., Nikolaev A.I. (2020) Rossiiskii konstitutsionalizm v usloviyakh novoi informatsionnoi real'nosti [Russian constitutionalism in the conditions of the new information reality]. *Vestnik MGPU. Seriya «Yuridicheskie nauki»* [Bulletin of the Moscow State Pedagogical University. Series "Legal Sciences"], 7, pp. 42-47.
12. Krivoruchko S.V., Lopatin V.A. (2018). Vliyanie implementatsii otkrytogo bankinga na razvitie natsional'nogo sektora Fintekh [The impact of the implementation of open banking on the development of the national Fintech sector]. *Ekonomika. Nalogi. Pravo* [Economics. Taxes. Law], 6, pp. 80-86.
13. Kryuchkov A.V., Prus Yu.V., Reznichenko S.A. (2018) Tekhnologicheskie osnovy natsional'noi informatsionnoi bezopasnosti [Technological foundations of national information security]. In: *Sbornik statei Mezhdunarodnoi nauchno-prakticheskoi konferentsii Rossiiskogo gosudarstvennogo gumanitarnogo universiteta*. [Collection of articles of the International Scientific and Practical Conference of the Russian State University for the Humanities], pp. 58-63.
14. Local self-government and municipal finance / N. N. Musinova, T. V. Bratarchuk, O. S. Semkina [and others]. – Moscow: Russian Municipal Academy, 2016. – 360 p. – ISBN 978-5-906041-25-8. – EDN VWYZED.
15. Mal'tsev V.N., Prus Yu.V., Reznichenko S.A. (2021) Aspekty informatsionnoi bezopasnosti na nachal'nom etape sozdaniya innovatsionnykh produktov [Aspects of information security at the initial stage of creating innovative products]. In: *Sbornik statei Mezhdunarodnoi nauchno-prakticheskoi konferentsii Rossiiskogo gosudarstvennogo gumanitarnogo universiteta* [Collection of articles of the International Scientific and Practical Conference of the Russian State University for the Humanities], pp. 58-63.
16. Management of the largest cities: Textbook and workshop / Yu. N. Shedko, O. V. Panina, L. A. Plotitsyna [and others]. – Moscow: Limited Liability Company "YURAYT Publishing House", 2019. – 322 p. - (Higher education). – ISBN 978-5-534-11313-6. – EDN PJAJYK.
17. Myrynyuk, A. N. Management of the social sphere and social responsibility of business / A. N. Myrynyuk, T. V. Butova // Pipeline transport: theory and practice. – 2010. – No. 1(17). – pp. 44-47. – EDN MVASIZ.
18. Nikolaev A.I. (2019) Voprosy tsifrovizatsii prava v sovremennoi yuridicheskoi doktrine [Issues of digitalization of law in modern legal doctrine]. *Vestnik MGPU. Seriya «Yuridicheskie nauki»* [Bulletin of the Moscow State Pedagogical University. Series "Legal Sciences"], 4, pp. 4 4-48.
19. Pashentsev D.A. (2021) Osnovnye napravleniya i osobennosti razvitiya zakonodatel'stva v usloviyakh tsifrovizatsii i perekhoda k novomu tekhnologicheskomu ukladu [Main directions and features of the development of legislation in the

conditions of digitalization and transition to a new technological structure]. *Vestnik MGPU. Seriya «Yuridicheskie nauki»* [Bulletin of the Moscow State Pedagogical University. Series "Legal Sciences"], 3, pp. 31-39.

20. Plotnikova T.V., Kotel'nikova O.V. (2020) Fenomen kiberprestupnosti v usloviyakh XXI veka [The phenomenon of cybercrime in the 21st century]. *Pravo: istoriya i sovremennost'* [Law: history and modernity], 3 (12), pp. 141-150. DOI: 10.17277/pravo.2020.03.pp.141-150.
21. Pomulev A.A. (2019) Metodologicheskie aspekty upravleniya operatsionnym riskom pri kreditovanii korporativnykh zaemshchikov [Methodological aspects of operational risk management when lending to corporate borrowers]. *Tenevaya ekonomika* [Shadow Economy], 3 (1), pp. 67-79.
22. Prokofiev, S. On some aspects of defining the concepts of “partnership” and “interaction” in establishing relations between government and business / S. Prokofiev, Y. Ragulina, T. Bratarchuk // Problems of theory and practice of management. – 2019. – No. 1. – P. 8-14. – EDN MGDHQU.
23. Reznichenko S.A. i dr. (2022) Problemy upravleniya informatsionnoi bezopasnost'yu v kreditno-bankovskoi sisteme peredachi dannykh [Problems of information security management in the credit and banking data transmission system]. *Moskovskii ekonomicheskii zhurnal* [Moscow Economic Journal], 2. Available at: https://qje. su/ekonomicheskaya-teoriya/moskovskij-ekonomicheskij-zhurnal-2-2022-36 [Accessed 15/12/2023].
24. Sidorenko E.L. (2017) Kriminologicheskie riski oborota kriptovalyuty [Criminological risks of cryptocurrency turnover]. *Ekonomika. Nalogi. Pravo* [Economics. Taxes. Law], 10 (6), pp. 147-154.
25. Tsygalov, Yu. M. Efficiency of state corporations in the development of depressed regions / Yu. M. Tsygalov, T. V. Butova, I. I. Ordinartsev // Management consulting. – 2017. – No. 10(106). – pp. 46-58. – DOI 10.22394/1726-1139-2017-10-46-58. – EDN ZWOXHN.