Азиатско-Тихоокеанский регион: экономика, политика, право. 2023. Т. 25, № 4. С. 167–177.
Pacific Rim: Economics, Politics, Law. 2023, vol. 25, no. 4, pp. 167–177.

Научная статья
УДК 342:[004.056:004.8](595+594)
https://doi.org/10.24866/1813-3274/2023-4/167-177

ПРАВОВЫЕ ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В МАЛАЙЗИИ И ИНДОНЕЗИИ[1]

Наталья Анатольевна Князева[1], Екатерина Анатольевна Князева[2]
[1,2] Дальневосточный федеральный университет, г. Владивосток, Россия
[1]knyazeva.na@dvfu.ru, https://orcid.org/0000-0003-1584-1104
[2] kniazeva.ea@dvfu.ru, https://orcid.org/0000-0003-4444-0545

Аннотация. В статье проводится сравнительно-правовой анализ подходов к регулированию и использованию искусственного интеллекта в области кибербезопасности на примере стран Азиатско-Тихоокеанского региона – Малайзии и Индонезии. Рассмотрены основные правовые акты в области защиты персональных данных, авторского права, банковской и финансовой сферы, безопасности телекоммуникационных сетей, информационной инфраструктуры и предупреждения киберпреступлений, а также вопросы привлечения к административной и уголовной ответственности за киберпреступления. Перечисляются государственные органы, координирующие и реализующие вопросы кибербезопасности. Особое внимание уделено характеристикам основных понятий, раскрываемых в исследуемых актах. Отмечено, что правовое поле Индонезии содержит более четкие трактовки определений целого ряда понятий в области киберзащиты по сравнению с Малайзией. Однако законодательство Малайзии затрагивает больший спектр регулирования общественной жизни при реализации вопросов кибербезопасности – от медицины до транспорта. В Индонезии не все сферы так хорошо регламентированы для решения подобных вопросов. Арсенал средств защиты от кибератак или иных противоправных действий, посягающих на информационную и цифровую среду, в Малайзии и Индонезии примерно одинаков и различается лишь по способам и качеству (эффективности) реализации. Подчеркивается серьезный и разноплановый

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16129

подход обеих стран к дальнейшему развитию, изменению и совершенствованию законодательства в вопросах применения искусственного интеллекта по противодействию киберпреступлениям. Несмотря на имеющиеся противоречия по отдельным вопросам, каждая из стран стремится усилить свои инструменты борьбы с киберугрозами путем разработки отдельных национальных стратегий безопасности.

Ключевые слова: искусственный интеллект, кибербезопасность, киберпреступления, право Малайзии, право Индонезии, правовое регулирование ИИ, Закон о защите персональных данных, Закон о компьютерных преступлениях, Закон об авторском праве, Закон о связи и мультимедиа, Закон о стратегической торговле, Закон о защите персональных данных, стратегия кибербезопасности Малайзии и Индонезии

Для цитирования: Князева Н. А., Князева Е. А. Правовые особенности использования искусственного интеллекта для обеспечения кибербезопасности в Малайзии и Индонезии // Азиатско-Тихоокеанский регион: экономика, политика, право. 2023. Т. 25, № 4. С. 167–177.

Original article

LEGAL FEATURES OF THE USE OF ARTIFICIAL INTELLIGENCE FOR ENSURING CYBER SECURITY IN MALAYSIA AND INDONESIA

Natalia A. Knyazeva[1], Ekaterina A. Knyazeva[2]

[1,2] Far Eastern Federal University, Vladivostok, Russia

[1] knyazeva.na@dvfu.ru, https://orcid.org/0000-0003-1584-1104

[2] kniazeva.na@dvfu.ru, https://orcid.org/0000-0003-4444-0545

Abstract. The article provides a comparative legal analysis of approaches to the regulation and use of artificial intelligence in the field of cybersecurity using the example of the countries of the Asia-Pacific region – Malaysia and Indonesia. The main legal acts in the field of personal data protection, copyright, banking and financial sector, security of telecommunication networks, information infrastructure, cybercrimes, as well as issues of bringing to administrative and criminal liability for cybercrimes are considered. State bodies coordinating and implementing cybersecurity issues are listed. Particular attention was paid to the characteristics of the basic concepts disclosed in the acts under study. It is noted that the legal framework of Indonesia contains clearer interpretations of the definitions of a number of concepts in the field of cyber defense compared to Malaysia. However, Malaysian legislation covers a wider range of regulation of public life in the implementation of cybersecurity issues – from medicine to transport. In Indonesia, not all areas are so well regulated to deal with such issues. At the same time, the arsenal of means of

protection against cyber-attacks or other illegal actions that encroach on the information and digital environment in Malaysia and Indonesia is approximately the same and differs only in the methods and quality (efficiency) of implementation. The serious and diverse approach of these countries for the further development, changes and improvement of legislation in matters of the use of artificial intelligence in activities to combat cybercrime is emphasized. Despite the contradictions on certain issues, each country seeks to strengthen its tools to combat cyber threats by developing separate national security strategies.

Keywords: artificial intelligence, cybersecurity, cybercrime, Malaysian law, Indonesian law, legal regulation of AI, personal data protection law, Computer Crime Law, Copyright Law, Communications and Multimedia Law, Strategic Trade Law, Personal Data Protection Law, cybersecurity strategy for Malaysia and Indonesia

For citation: Knyazeva N. A., Knyazeva E. A. Legal features of the use of artificial intelligence for ensuring cyber security in Malaysia and Indonesia. *PACIFIC RIM: Economics, Politics, Law*. 2023, vol. 25, no. 4, pp. 167–177. (In Russ.).

Стремительное развитие технологий, в частности искусственного интеллекта (ИИ), привело к активной разработке и внедрению ИИ в различные сферы общественной жизни – от медицины и транспорта до применения в области государственного управления и военном секторе.

Необходимость современного и эффективного нормативного регулирования в этой области вызвано решением ряда вопросов, таких как: использование ИИ в транспортной сфере; защита персональных данных, коммерческой, банковской тайны; ответственность при совершении ряда преступлений с использованием ИИ; возмещение вреда, причиненного искусственным интеллектом, и др.

Учитывая опыт других стран – лидеров в вопросах цифровизации, разработки, внедрения и использования искусственного интеллекта, мы можем определить свой путь в построении эффективной системы регулирования кибербезопасности.

Среди стран, которые уже утвердили механизмы нормативного регулирования разработки и использования ИИ, особое место занимают страны Юго-Восточной Азии. Многие развивающиеся страны этого региона являются перспективными и инвестиционно привлекательными, Малайзия и Индонезия не стали исключением. Выбор именно этих стран для исследования был обусловлен схожестью с Россией уровня цифровизации и регулирования в сфере цифрового права, что позволяет странам заимствовать опыт друг друга, а также осваивать новые рынки и налаживать сотрудничество, которое становится особенно актуальным в связи с поворотом российской политики на Восток.

Индонезия и Малайзия схожи по уровню общего регулирования в вопросах ИИ: единый закон, который содержал бы нормы, регламентирующие отношения в

сфере разработки, внедрения и применения ИИ, в обеих странах отсутствует. Также нет унифицированного правового акта по вопросам кибербезопасности. Все законодательство Малайзии и Индонезии по данному вопросу находит свое отражение в разнообразных правовых документах.

Еще в июне 2017 г. было объявлено, что правительство Малайзии примет новый закон, направленный на защиту малайзийцев от угроз кибербезопасности, однако по настоящее время единого законодательства в отношении кибербезопасности не существует.

Действующее законодательство, которое регулирует защиту критически важных систем и сетей от цифровых атак, состоит из следующих нормативных актов:

1. Закон о компьютерных преступлениях 1997 г. – Computer Crimes Act 1997 («CCA») [1]. Согласно положениям Закона, как преступления рассматриваются деяния, связанные с неправомерным использованием компьютеров. Закон может применяться, если компьютер, программа или данные находились в Малайзии или могли быть подключены, отправлены или использованы в Малайзии во время совершения преступного деяния. Также признаются преступными действия, связанные с получением несанкционированного доступа к компьютерам или сетям, несанкционированной модификацией содержимого любого компьютера и/или неправомерным доступом.

2. Закон о связи и мультимедиа 1998 г. – Communications and Multimedia Act 1998 г. (CMA) [2]. Закон, принятый для обеспечения и регулирования конвергентных коммуникационных и мультимедийных отраслей, регулирует сетевые средства, сетевые услуги, услуги приложений, услуги приложений контента и включает предписание для лицензирования деятельности и услуг. Раздел 263(1) CMA предписывает, что «лицензиат должен приложить все усилия, чтобы предотвратить использование сетевых средств, которыми он владеет или которые он предоставляет, или сетевых услуг, услуг приложений или услуг приложений контента, которые он предоставляет, в связи с совершением любого преступления в соответствии с любым законом Малайзии». CMA также запрещает мошенническое или ненадлежащее использование сетевых средств или сетевых услуг; использование и хранение поддельных устройств доступа; использование оборудования или устройств для получения несанкционированного доступа к любым сетевым услугам; перехват любых сообщений, кроме полученных на законных основаниях.

3. Закон об авторском праве 1987 г. – Copyright Act 1987 («CA») [3]. Согласно данному закону обход любой технологической меры защиты, которая применяется к копии произведения, защищенного авторским правом, является правонарушением в соответствии с Разделом 36A CA. Закон прямо запрещает кому бы то ни было: (a) разрабатывать, производить, адаптировать или выполнять действия с целью обеспечения или облегчения обхода мер технической защиты; (b) производить, им-

портировать или продавать любые технологии или устройства с целью обхода любых технических мер защиты.

4. Уголовный кодекс – Penal Code («PC») [4]. Если конкретные правонарушения, связанные с кибербезопасностью, не подпадают под действие иных норм законодательства, то применяются нормы УК, который предусматривает большинство преступлений и процедур в Малайзии.

5. Закон о защите персональных данных 2010 г. – The Personal Data Protection Act 2010 (PDPA) [5] применяется к любому лицу, кто обрабатывает и контролирует или разрешает обработку любых «персональных данных» в отношении коммерческих транзакций. Установлено 7 принципов защиты данных, которые составляют основу защиты в соответствии с PDPA, одним из них является принцип безопасности. В соответствии с разделом 9(1) PDPA пользователь должен при обработке персональных данных предпринимать практические шаги для защиты личных данных от любой потери, неправильного использования, модификации, несанкционированного или случайного доступа к раскрытию, изменению или уничтожению.

6. Закон о стратегической торговле 2010 г. – Strategic Trade Act 2010 («STA») [6]. В рамках международных обязательств Малайзии в отношении национальной безопасности STA контролирует экспорт, транзит и посредничество в отношении стратегических предметов и технологий, включая оружие и связанные с ним материалы, а также виды деятельности, которые будут или могут способствовать проектированию, разработке, производству и доставке оружия массового уничтожения. Раздел 7 STA предусматривает, что министр международной торговли и промышленности может приказом, опубликованным в Бюллетене, называть любые предметы в качестве стратегических предметов для целей STA.

7. Другие применяемые руководящие принципы или правила. В Малайзии действуют отраслевые руководящие принципы, касающиеся кибербезопасности. К ним относятся Структура системы управления данными и управленческой информацией – Data Management and Management Information System (MIS) и Руководящие принципы по интернет-страхованию, выпущенные Центральным банком Малайзии.

В 2017 г. было создано Национальное агентство кибербезопасности (National Cyber Security Agency, NACSA) – национальное ведомство по вопросам кибербезопасности в целях повышения эффективности защиты Малайзии против кибератак путем объединения усилий лучших специалистов в области ИИ и киберзащиты как на национальном уровне, так и с привлечением международных экспертов.

Агентство разрабатывает и внедряет стратегию кибербезопасности на национальном уровне, организует защиту критически важных национальных объектов информационной инфраструктуры (Critical National Information Infrastructures, CNII), принимает меры по противодействию киберугрозам и киберпреступлениям, координирует программы просвещения населения и бизнеса о способах защиты

персональных данных, вырабатывает и продвигает подходы к дальнейшему развитию борьбы с кибератаками с учетом современных угроз и вызовов [7].

В 2020 г. была утверждена Стратегия кибербезопасности Малайзии (MCSS) [8]. MCSS создана Сайфуддином Абдуллой, министром связи и мультимедиа, представляющим премьер-министра ЯБ Тан Шри Дато Хаджи Мухиддин бин Хаджи Мохд Ясин. В MCSS приняли участие компании: MDEC, BAE Systems Applied Intelligence, Crowdfense, FireEye, Lenovo, System Consultancy Services и PERNEC. Основная цель Стратегии – киберзащита, кибербезопасность и развитие новых технологий для мирового сообщества.

Политика, связанная с кибербезопасностью, была инициирована в Индонезии еще в 2006 г., когда Министерство связи и информационных технологий опубликовало Постановление № 27 от 2006 г. Затем это Положение было отменено Постановлением № 26 от 2007 г., которое было впоследствии продлено и дополнено Постановлением № 5 от 2017 г. Постановлением 2007 г. была создана Индонезийская группа реагирования на инциденты безопасности в интернет-инфраструктуре (ID-SIRTII) в целях обеспечения контроля за безопасностью телекоммуникационных сетей на основе интернет-протоколов [9].

Кибербезопасность также регулируется Законом № 11 от 2008 г. «Об электронной информации и транзакциях» с дополнениями и изменениями, внесенными Законом № 19 от 2016 г. «О поправках к Закону № 11 от 2008 г. «Об электронной информации и транзакциях» («Закон об электронной информации») [10].

«Закон об электронной информации» был дополнен постановлением Правительства № 71 от 2019 г. «О внедрении электронных систем и транзакций» (GR № 71/2019) [11]. Кроме того, в конце 2020 г. Министерство связи и информационных технологий издало Постановление № 5 от 2020 г. «О поставщиках электронных систем в частном секторе» [12]. Перечисленные нормативные акты являются основой законодательства о кибербезопасности в Индонезии.

Правительство Индонезии в 2022 г. приняло Закон № 27 «О защите персональных данных» (PDPL) [13], который считается основным документом по защите персональных данных, иными словами – «объемными положениями» для защиты персональных данных, которые также затрагивают вопросы кибербезопасности в Индонезии. Положения PDPL охватывают все уровни защиты персональных данных в электронной и неэлектронной средах.

В дополнение положения PDPL для защиты персональных данных вводят новые меры, в которых:

- перечислены и раскрыты права носителей персональных данных (пользователей). Например, согласно ст. 1 персональные данные – это данные о физических лицах, идентифицированные или идентифицируемые сами по себе или в сочетании с другой информацией, прямо или косвенно через электронные или неэлектронные

системы. При этом персональные данные делятся на две категории: конкретные персональные данные, такие как информация о здоровье, биометрические данные, генетические данные, и общие персональные данные (полное имя, сексуальная ориентация, гражданство и семейное положение) (ст. 4 PDPL);

- раскрываются обязанностях контролера персональных данных и обработчика персональных данных. В частности, контролер персональных данных обязан контролировать представителей всех сторон, которые участвуют в обработке персональных данных (ст. 4 PDPL);
- дано определение положения о должностном лице, которое выполняет функции по работе с персональными данными клиентов и пользователей (контролера). Контроллером персональных данных является любое лицо, государственный орган и международные организации, которые действуют индивидуально или коллективно при определении целей и осуществлении обработки персональных данных (ст. 1 № (4) PDPL).

Один из отличительных аспектов действия Закона PDPL – обязанность контролера персональных данных предоставить субъекту персональных данных определенное правовое основание для обработки персональных данных, в соответствии с которым контролер персональных данных также обязан указать (среди прочего) тип и соотношение персональных данных, данные, срок хранения и права субъекта персональных данных (ст. 21).

Наконец, PDPL также предусматривает санкции за любые нарушения и/или несоблюдения PDPL, то есть возможность привлечения лиц (в том числе и должностных) к административной и/или уголовной ответственности.

Постановление президента № 82 от 2022 г. «О защите жизненно важной информационной инфраструктуры» (PR № 82/2022) [14] содержит определение понятия «кибербезопасность». В соответствии со статьей 1(4) ПР № 82/2022 кибербезопасность представляет собой адаптивную и инновационную попытку защитить все уровни киберпространства, включая содержащиеся в нем информационные активы, от киберугроз и атак, как технических, так и социальных. Кибербезопасность является частью жизненно важной информационной инфраструктуры (IIV), системы, которая поддерживает стратегические секторы для предотвращения вмешательства в электронную инфраструктуру.

Кибербезопасность также регулируется постановлением Министерства связи и информационных технологий Индонезии № 4 от 2016 г. «О системах управления информационной безопасностью» («Правило № 4/2016») [15], которое обязывает применять стандарт SNI ISO/IEC 27001 в качестве международного стандарта для систем управления информационной безопасностью. Однако постановление Министерства связи и информационных технологий Индонезии № 4/2016 предназна-

чено только для тех, кто предоставляет электронные системы для государственных услуг.

23 ноября 2020 г. специализированный орган по надзору за кибербезопасностью в Индонезии – Национальное агентство по кибербезопасности и шифрованию (BSSN) – обнародовал собственное постановление «Правило BSSN № 8 от 2020 г.» («Правило BSSN № 8»). В соответствии с этим постановлением применение стандарта SNI ISO/IEC 27001 является обязательным для поставщиков электронных систем в частном секторе (ст. 4 Положения BSSN № 8).

Другим актом, который можно рассматривать как один из основных ориентиров в области кибербезопасности, является Совместный указ Коминфо и Министерства юстиции и прав человека № 14 от 2015 г. и № 26 от 2015 г. «О реализации запрета на контент и/или Право доступа пользователя в отношении нарушения авторских прав и/или смежных прав в электронной системе» («Совместный указ 2015 г.»). Данный указ определяет технические процедуры и механизмы в отношении любого нарушения авторских прав начиная с подачи отчета и заканчивая закрытием контента и/или права доступа.

Помимо вышеупомянутых правил, существуют также положения о кибербезопасности, содержащиеся в отраслевом законодательстве, например в банковских секторах и других финансовых услугах, которые предоставляют возможность потребителям финансового сектора подавать жалобы через электронные средства, предоставляемые финансовыми учреждениями (ст. 7 постановления Управления финансовых услуг № 18 от 2018 г. (OJK). Также были приняты два дополнительных постановления, которые предусматривают несколько ключевых моментов, касающихся кибербезопасности. Во-первых, это Положение OJK № 38/POJK.03/2016 с последующими поправками, внесенными Положением OJK № 13/POJK.03/2021 (Рег. OJK № 38/2016), которое устанавливает определенный перечень обязанностей для коммерческих банков:

- иметь собственный план аварийного восстановления;
- внедрить систему внутреннего контроля в отношении использования информационных технологий;
- разместить свой центр обработки данных и/или центр аварийного восстановления на территории Индонезии.

Во-вторых, Положение OJK № 4/POJK.05/2021 (Рег. OJK № 4/05/2021) распространяется также на небанковские финансовые учреждения и требует:

- разработать собственный план аварийного восстановления;
- разместить центр обработки данных и/или центр аварийного восстановления на территории Индонезии;
- проводить обработку транзакций на основе информационных технологий в Индонезии.

Как видно из рассмотренного выше, законодательство Малайзии и Индонезии представляет собой довольно широкую базу для использования искусственного интеллекта при осуществлении кибербезопасности. При этом сфера правового регулирования меняется в зависимости от области применения ИИ – будь то общие вопросы защиты персональных данных или банковская сфера. Особенно это заметно в правовом поле Малайзии, поскольку ряд законов государства предусматривает свою зону ответственности при защите прав и интересов граждан, организаций и государства в целом от кибератак и киберпреступлений в цифровом поле. Законодательство Индонезии в этом вопросе оказалось более унифицированным, несмотря на отсутствие единого закона о кибербезопасности.

Список источников

1. Computer crimes act 1997 г. URL: https://ccid.rmp.gov.my/Laws/Computer_Crime_Act_1997.pdf.

2. Communications and multimedia act 1998 г. URL: https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/MCMC-ACT-1998.pdf.

3. Copyright act 1987. URL: https://www.swinburne.edu.my/docs/libra-ry/copyright_act_1987.pdf.

4. Criminal law of Maplaysia. URL: https://ccid.rmp.gov.my/Laws/Act_574_Panel_Code_Malaysia.pdf.

5. Personal Data Protection Act. URL: https://www.malaysia.gov.my/portal/content/-654.

6. Strategic Trade Act 2010 (STA) [Act 708]. URL: https://www.mcmc.gov.my/en/-legal/acts/strategic-trade-act-sta-act-708.

7. Гурков Р. А. Малайзия. Рынок цифровых технологий. URL: https://ved.today/wp-content/uploads/2022/08/IT_MALAYZIYA.pdf.

8. Malaisya ciber strategy 2020–2024. URL: https://asset.mkn.gov.my/web/wp-content/uploads/sites/3/2019/08/MalaysiaCyberSecurityStrategy2020-2024Compressed.pdf.

9. Peraturan menteri komunikasi dan informatika nomor 27/PER/M.KOMINFO/9-/2006 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet. URL: https://jdih.kominfo.go.id/produk_hu-kum/view/id/445/t/peratu-ran+menteri+komunikasi+dan+informatika+nomor+27permkominfo92006+tanggal+20+september+2006.

10. Personal data protection efforts through law number 27 of 2022 on personal data protection. URL: https://aco-law.com/articles/personal-data-protection-efforts-through-law-number-27-of-2022-on-personal-data-protection/.

11. General data protection regulation (Regulation (EU) 2016/679). URL: https://www.dataguidance.com/comparisons/general-data-protection-regulation.

12. Regulation No. 5 of 2020 on the electronic system providers in the private sector. URL: https://jdih.kominfo.go.id/pro-duk_hukum/view/id/759/t/peratu-ran+menteri+komunikasi+dan+informatika+nomor+5+tahun+2020.

13. Law No. 11 of 2008 on Electronic Information and Transactions. URL: https://platform.dataguidance.com/legal-research/law-republic-indonesia-no-11-2008-concerning-electronic-information-and-transactions.

14. President Regulation No. 82 of 2022 on the protection of vital information infrastructure. URL: https://www.dataguidance.com/opinion/indonesia-cybersecu-rity#:~:text=%20Regu-lation%20No.%2082%20of,at-tacks%2C%20both%20technical%20and%20social

15. Regulation No. 4 of 2016 on information security management systems. URL: https:// jdih.kominfo.go.id/produk_hukum/view/id/532/t/peraturan+men-teri+kom-unikasi+-dan+informatika+nomor+4+tahun+2016+tanggal+11+april+2016.

References

1. Computer Crimes Act 1997 («CCA»). URL: https://ccid.rmp.gov.my/Laws/Computer_Crime_Act_1997.pdf.

2. Communications and Multimedia Act 1998 («CMA»). URL: https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/MCMC-ACT-1998.pdf.

3. Copyright Act 1987 («CA»). URL: https://www.swinburne.edu.my/docs/library/copyright_act_1987.pdf.

4. Penal Code. URL: https://ccid.rmp.gov.my/Laws/Act_574_Panel_Co-de_Malaysia.pdf.

5. The Personal Data Protection Act 2010. URL: https://www.malaysia.gov.my/portal/content/654 (дата обращения: 18.09.2023)

6. Strategic Trade Act 2010 («STA»). URL: https://www.mcmc.gov.my/en/le-gal/acts/strategic-trade-act-sta-act-708.

7. Gurkov R. A. Malajzіna. Rynok cifrovyh tehnologіn [Malaysia. Digital technology market]. URL: https://ved.today/wp-content/uploads/2022/08/IT_MALAYZIYA.pdf. (In Russ.).

8. Malaysia Cyber Security Strategy 2020–2024. URL: https://asset.mkn.gov.my/-web/wp-content/uploads/sites/3/2019/08/MalaysiaCyberSecurityStrategy2020-2024Compressed.pdf.

9. Regulation No. 27 of 2006 of the Ministry of Communication and Information Technology. URL: https://jdih.kominfo.go.id/produk_hu-kum/view/id/445/t/peratu-ran+men-teri+komunikasi+dan+in-formatika+nomor+27permkominfo92006+tan-ggal+20+september+2006.

10. Law No. 27 of 2022 regarding Personal Data Protection. URL: https://acolaw.-com/articles/personal-data-protection-efforts-through-law-number-27-of-2022-on-per-sonal-data-protection/.

11. General Data Protection Regulation (Regulation (EU) 2016/679). URL: https://www.dataguidance.com/comparisons/general-data-protection-regulation

12. Regulation No. 5 of 2020 on the Electronic System Providers in the Private Sector. URL: https://jdih.kominfo.go.id/produk_hukum/view/id/759/t/pe-raturan+mente-ri+komunikasi+dan+informatika+nomor+5+tahun+2020.

13. Law No. 11 of 2008 on Electronic Information and Transactions. URL: https://platform.dataguidance.com/legal-research/law-republic-indonesia-no-11-2008-concer-ning-electronic-information-and-transactions.

14. President Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure. URL: https://www.dataguidance.com/opinion/indonesia-cybersecu-rity#:~: text=Pre-sident%20Regulation%20No.%2082%20of,attacks%2C%20both%20te-chnical%-20-and%20social.

15. Regulation No. 4 of 2016 on Information Security Management Systems. URL: https://jdih.kominfo.go.id/produk_hukum/view/id/532/t/peraturan+menteri+komunikasi+dan+informatika+nomor+4+tahun+2016+tanggal+11+april+2016.

Информация об авторах

Н. А. Князева – кандидат юридических наук, доцент, доцент кафедры уголовного права и криминологии, Юридическая школа, Дальневосточный федеральный университет, г. Владивосток, Россия.

Е. А. Князева – кандидат юридических наук, доцент кафедры уголовного права и криминологии, Юридическая школа, Дальневосточный федеральный университет, г. Владивосток, Россия.

Information about the authors

N. A. Knyazeva – Candidate of Law, Associate Professor of the Department of Criminal Law and Criminology, School of Law, Far Eastern Federal University, Vladivostok, Russia.

E. A. Knyazeva – Candidate of Law, Associate Professor of the Department of Criminal Law and Criminology, School of Law, Far Eastern Federal University, Vladivostok, Russia.

Статья поступила в редакцию 15.03.2023; одобрена после рецензирования 24.05.2023; принята к публикации 10.10.2023.

The article was submitted 15.03.2023; approved after reviewing 24.05.2023; accepted for publication 10.10.2023.