Оригинальная статья / Original article

УДК 343.34:004.056.5(470)

Использование блокчейн-технологий для противодействия неправомерному воздействию на критическую информационную инфраструктуру Российской Федерации

А. А. Гребеньков[1] ✉

[1] Юго-Западный государственный университет
ул. 50 лет Октября 94, г. Курск 305040, Российская Федерация

✉ e-mail: grebenkov@gmail.com

Резюме

Актуальность. *Статья рассматривает вопросы противодействия атакам на критическую информационную инфраструктуру РФ, которая является желанной целью для спецслужб иностранных государств, осуществляющих враждебные действия против нашей страны. Вероятность реализации таких угроз с учётом обострившейся геополитической обстановки в настоящее время как никогда велика. В таких условиях приобретает особую важность поиск новых путей противодействия угрозам, в том числе задействующих блокчейн-технологии.*

Цель *– разработка научно обоснованных предложений по применению блокчейн-технологий для защиты критической информационной инфраструктуры РФ от кибератак.*

Задачи: *выявить особенности блокчейн-технологий, обусловливающие возможность их использования в системе обеспечения информационной безопасности; на основе изучения мировой практики использования блокчейн-технологий в данной сфере определить наиболее перспективные сферы их применения и рассмотреть ограничивающие использование блокчейн-технологий факторы.*

Методология. *В процессе работы над исследованием использовались логический, формально-юридический, системно-структурный методы, кейс-стади.*

Результаты. *В ходе исследования выявлено, что использование блокчейн-технологий может защитить от уязвимостей, которые были использованы в Stuxnet-подобных атаках, и в мировой практике имеются примеры внедрения блокчейн-технологий для защиты критической информационной инфраструктуры.*

Вывод. *Наиболее перспективно использование блокчейна для обеспечения безопасности систем устройств Internet of Things. Это связано с такими свойствами блокчейн-систем, как децентрализованное хранение данных, программируемые смарт-контракты и авторизация. Препятствиями на пути полномасштабного внедрения технологии выступают избыточность информации, масштабируемость производительности и интеграция блокчейн-технологий в существующую инфраструктуру. Требуется правовая регламентация использования блокчейн-технологий.*

Ключевые слова*: кибервойна; кибердиверсия; информационная безопасность; киберпреступность; киберфизические системы.*

Конфликт интересов: *Автор декларирует отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.*

Для цитирования: Гребеньков А. А. Использование блокчейн-технологий для противодействия неправомерному воздействию на критическую информационную инфраструктуру Российской Федерации // Известия Юго-Западного государственного университета. Серия: История и право. 2021. Т. 11, № 3. С. 109–119.

Поступила в редакцию 02.04.2021 Принята к публикации 29.04.2021 Опубликована 25.06.2021

© Гребеньков А. А., 2021

The use of Blockchain Technologies to Counter Illegal Influence on the Critical Information Infrastructure of the Russian Federation

Alexander A. Grebenkov[1] ✉

[1] Southwest State University
50 Let Oktyabrya str. 94, Kursk 305040, Russian Federation

✉ e-mail: grebenkov@gmail.com

Abstract

Relevance. *The article examines the issues of countering attacks on the critical information infrastructure of the Russian Federation, which is a desirable target for the intelligence services of foreign states carrying out hostile actions against our country. Given the aggravated geopolitical situation, the likelihood of such threats being realized is now greater than ever. In such conditions, it becomes especially important to search for new ways to counter threats, including those involving blockchain technologies.*

The purpose *– development of scientifically substantiated proposals for the use of blockchain technologies to protect the critical information infrastructure of the Russian Federation from cyber-attacks.*

Objectives. *Identify the features of blockchain technologies that determine the possibility of their use in the information security system, based on the study of the world practice of using blockchain technologies in this area, determine the most promising areas of their application and consider the factors limiting the use of blockchain technologies.*

Methodology. *In the framework of the conducted research, we used logical, formal-legal, systemic-structural methods, case studies.*

Results. *The study revealed that the use of blockchain technologies can protect against vulnerabilities that were used in Stuxnet-like attacks, and in world practice there are examples of the implementation of blockchain technologies to protect critical information infrastructure.*

Conclusion. *The most promising use of blockchain is to ensure the security of Internet of Things device systems. This is due to such properties of blockchain systems as decentralized data storage, programmable smart contracts, and authorization. The obstacles to the full-scale implementation of the technology are information redundancy, scalability of performance and the integration of blockchain technologies into the existing infrastructure. Legal regulation of the use of blockchain technologies is required.*

Keywords: *cyber war; cyber sabotage; Internet of Things; cybercrime; cyber-physical systems.*

Conflict of interest: *The Author declare the absence of obvious and potential conflicts of interest related to the publication of this article.*

For citation: Grebenkov A. A. The use of Blockchain Technologies to Counter Illegal Influence on the Critical Information Infrastructure of the Russian Federation. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Istoriya i pravo = Proceedings of the Southwest State University. Series: History and Law*. 2021; 11(3): 109–119. (In Russ.)

Received 02.04.2021 Accepted 29.04.2021 Published 25.06.2021

***

Введение

Основной особенностью современной характеристики преступлений, связанных с неправомерным доступом к компьютерной информации, использованием и распространением вредоносных компьютерных программ («традиционной» компьютерной преступности) является её организованный и профессиональный характер. Если в исследованиях компьютерной преступности конца 1990-х – начала 2000-х гг. типичным было изображение лица, совершающего компьютерные преступления, как «хакера-одиночки», использующего свои обширные знания в области информационных технологий в исследовательских или хулиганских целях [1], то в настоящее

время такая характеристика во многом утратила свою актуальность. И хотя среди привлечённых к ответственности за компьютерные преступления в основном преобладают молодые мужчины-одиночки с невысокими профессиональными навыками [2], следует иметь в виду, что киберпреступность является гиперлатентной, и наиболее опасные её проявления зачастую не получают должной правовой оценки. Наибольшая угроза в настоящее время исходит от законспирированных организованных групп и преступных сообществ, совершающих компьютерные преступления как для извлечения выгоды, так и для достижения иных целей, в том числе посягательств на безопасность государства [3]. Многие из таких групп и сообществ контролируются спецслужбами различных государств и используются в собственных целях.

«Компьютерные преступления» могут преследовать такую цель, как кибершпионаж, кибердиверсии, а также получение доступа к электронной переписке должностных лиц государства и её публикации с целью дискредитации их лично и политики государства в целом (примером может служить взлом электронного почтового ящика заместителя председателя Правительства РФ А. В. Дворковича в июле 2014 г.[1]).

Одной из желанных целей атаки киберпреступников являются системы автоматизированного управления технологическими процессами (АСУ ТП) и иные компьютерные системы, используемые для управления индустриальными машинами и механизмами, в последнее время также называемые «киберфизическими системами» [4]. По данным «Лаборатории Касперского», в 2017 г. минимум один инцидент информационной безопасности, связанный с такими системами, затронул 50% промышленных предприятий [5]. В современных условиях никакое производство не обходится без таких систем. Более того, электронные системы управления распространяются повсеместно и используются, например, в автомобилях и бытовой технике. Нетрудно представить, насколько опасной может быть утрата водителем контроля над автомобилем, движущимся на большой скорости, вследствие атаки на его компьютерную систему, однако возможный вред от этого меркнет по сравнению с возможными последствиями атаки на АСУ ТП, контролирующую атомную электростанцию, трубопроводную систему, горнодобывающее оборудование, медицинское оборудование или даже военные системы. Естественно, что подобные системы являются желанными целями для атаки кибертеррористов и прочих враждебных субъектов, включая спецслужбы иностранных государств.

Подобные системы получили название «критической информационной инфраструктуры». В настоящее время Российской Федерацией принимаются достаточно серьёзные усилия по предотвращению атак на критическую информационную инфраструктуру [6]. Например, если говорить о правовых мерах, то в 2017 г. был принят Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. № 187-ФЗ, а также включена в Уголовный кодекс РФ ст. 274[1], предусматривающая существенно повышенную по сравнению с другими компьютерными преступлениями ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

Разумеется, случайное попадание вредоносного программного обеспечения или несанкционированный доступ в такие системы вряд ли возможны, т. к. они достаточно хорошо защищены, прежде всего тем, что не подключены к глобальным сетям, используют специализированное программное обеспечение для

[1] Карпюк И. Взлом Дворковича // Полит.Ру. 2014. 22 июля. URL: http://polit.ru/article/2014/07/22/dvorkovich (дата обращения: 30.03.2021).

предотвращения атак и обслуживаются квалифицированным персоналом. В то же время ещё в конце 2000-х гг. в ряде экспериментов было показано, что многие системы, в частности в области электроэнергетики, являются уязвимыми, и проведение кибератак может привести к таким серьёзным последствиям, как самоуничтожение генератора или даже аварийная остановка реактора на атомной электростанции [7].

Однако угроза направленных атак на такие системы является вполне реальной и давно перестала быть лишь теоретической. Так, в 2010 г. программное обеспечение Stuxnet было использовано для нанесения вреда ядерной программе Ирана [8; 9]. В 2013 г. компьютерной атакой была нарушена работа финансовых учреждений Южной Кореи [10]. В декабре 2015 г. программа BlackEnergy3 была использована для атаки на энергогенерирующую систему Ивано-Франковска (Украина) [11]. В первом квартале 2019 г. более половины кибератак затрагивали инфраструктурные объекты [12]. В апреле 2020 г. атака «Dark Nexus», использующая устройства Internet of Things, затронула объекты критической инфраструктуры Китая, Таиланда, Бразилии, Южной Кореи и России [13].

Следует отметить, что общее мнение специалистов сходится в том, что данные атаки не были действиями преступников-одиночек или даже каких-то относительно маломасштабных преступных групп. Сложность данных программ говорит о том, что они были созданы большими коллективами хорошо подготовленных и финансируемых разработчиков. Так, в отношении Stuxnet считается, что заказчиками его разработки выступили спецслужбы США и Израиля [14].

В настоящее время крайне высока угроза организованных атак на критическую информационную инфраструктуру Российской Федерации со стороны враждебно настроенных государств. В частности, в New York Times в марте 2021 г. была опубликована информация о том, что серия таких атак готовится США, якобы в ответ на вмешательство «российских хакеров» в выборный процесс в этом государстве[1].

Как отмечают Р. В. Мещеряков, А. Ю. Исхаков и О. О. Евсютин, имеется насущная «потребность в новых методах и механизмах обеспечения безопасности» киберфизических систем, в том числе использующих блокчейн-технологии [13]. Ввиду этого необходимы изучение и анализ особенностей данных технологий, позволяющих противостоять угрозам, связанным с атаками на критическую информационную инфраструктуру.

Методология

В процессе работы над исследованием использовались традиционные для теоретико-прикладных правовых исследований общенаучные, частнонаучные и специальные методы – логический, формально-юридический, системно-структурный, кейс-стади.

Применение формальной логики требовалось для осуществления анализа особенностей применяющихся в настоящее время блокчейн-технологий, выявления их недостатков, которые могут помешать внедрению их для защиты критической информационной инфраструктуры, а также для формулирования авторских выводов.

Формально-юридический метод был необходим для установления содержания правовых норм, сформулированных в законодательных актах Российской Федерации, выявления недостаточности имеющихся предписаний закона для полноценного внедрения блокчейн-технологий в систему защиты критической информационной инфраструктуры.

[1] Sanger D. E., Barnes J. E., Perlroth N. Preparing for Retaliation Against Russia, U. S. Confronts Hacking by China // New YorkTimes. 2021. March 07. URL: https://www.nytimes.com/2021/03/07/us/politics/microsoft-solarwinds-hack-russia-china.html (accessed 20.03.2021).

Системно-структурный метод позволил выделить в структуре системы защиты критической информационной инфраструктуры наиболее уязвимые составляющие и предложить меры их защиты с учётом их функциональной роли и связей с другими подсистемами.

Метод кейс-стади использовался для рассмотрения и авторской оценки конкретных примеров атак на критическую информационную инфраструктуру и историй успешного внедрения блокчейн-технологий для организации её защиты.

Результаты и их обсуждение

Блокчейн является перспективной технологией, решающей важные проблемы, связанные с тем, что отдельные компоненты критических инфраструктур часто в значительной мере полагаются на устройства Internet of Things (IoT — например, различные датчики и прочие устройства сбора информации, а также контроллеры, управляющие различными устройствами, от дверных замков до медицинского оборудования и промышленных агрегатов), которые обмениваются данными и осуществляют их обработку, в том числе автоматически, без вмешательства в этот процесс человека и без его контроля. Поэтому узлы IoT должны иметь возможность распознавать и аутентифицировать друг друга, а также гарантировать целостность данных, которыми они обмениваются. Кроме того, важно убедиться, что программное обеспечение, работающее на устройствах IoT, не было изменено путём внешнего (или внутреннего, но несанкционированного) воздействия. Состояние и целостность программного обеспечения таких устройств должны постоянно отслеживаться на предмет несанкционированных модификаций [15].

Блокчейн предоставляет децентрализованную и распределенную среду обработки, которая может использоваться для организации взаимодействия внутри инфраструктуры IoT [16]. Можно выделить следующие присущие блокчейн-технологиям особенности, которые могут оказаться важными для обеспечения безопасности систем устройств IoT и обеспечения их взаимодействия в условиях угрозы внешнего несанкционированного вмешательства.

1. Децентрализованное хранение данных. Блокчейн основан на цепочечных структурах данных и механизме консенсуса. Блокчейн-система хранит копии данных на узлах сети, синхронизируя их между собой. Цепочечная структура, использующая средства криптографии, гарантирует, что сохранённые данные не могут быть изменены; механизм консенсуса обеспечивает целостность и синхронизацию данных. Во взаимодействии эти особенности блокчейн-системы создают безопасную среду для хранения данных в инфраструктуре IoT, которая может использоваться приложениями более высокого уровня. Хранение нескольких копий данных в блокчейне позволяет также создавать системы, в которых отсутствует единая точка отказа, которой может выступать централизованное хранилище данных.

2. Программируемые смарт-контракты. Под смарт-контрактом в блокчейне понимается определённый программный код, который определяет обязанности каждого участника контракта и условия признания их выполненными. Смарт-контракты хранятся в блокчейне, что позволяет обеспечить их целостность, синхронизацию и неизменность. Фиксация механизмов взаимодействия отдельных составляющих критической информационной инфраструктуры в смарт-

контрактах позволяет надёжно выявить аномалии в их поведении. Блокчейн-система является удобной платформой для реализации смарт-контрактов, являющихся основой логики взаимодействия инфраструктуры IoT.

3. Авторизация. Для информации, хранящейся в блокчейне, можно отследить источник происхождения. Кроме того, она защищена криптографическими средствами от несанкционированных изменений. На практике это означает, что блокчейн-система содержит в себе надежный механизм, позволяющий надёжно идентифицировать происхождение и целостность любых цифровых объектов: управляющих команд, программ, входных и выходных данных и т. д.

Использование блокчейн-технологий в контексте критической информационной инфраструктуры может защитить от уязвимостей, подобных тем, которые были использованы в Stuxnet. В частности, хранение ключевых параметров работы оборудования в блокчейне позволяет обнаруживать несанкционированные изменения в конфигурациях программного обеспечения путем анализа полной цепочки истории внесения изменений в эти данные, а также обеспечить целостность хранения входных и выходных данных, обрабатываемых элементами системы [17].

Блокчейн-системы можно использовать для фиксации любых важных операций, сетевого взаимодействия и даже программного кода в распределённом реестре. В результате любая попытка осуществления атаки путём изменения любых важных данных, копия которых хранится в реестре блокчейна, может быть легко обнаружена, а целостность и защита самого реестра от несанкционированного вмешательства обеспечивается криптографическими средствами, безопасность которых может быть подтверждена и базируется на том, что их обход требует чрезвычайно высоких вычислительных ресурсов, которыми не могут обладать потенциальные атакующие. Кроме того, программный код вычислительных устройств, являющихся составляющими критической информационной инфраструктуры, и все проверенные его исправления и обновления могут храниться в реестре, и при этом фактически выполняемый код может непрерывно сопоставляться с эталонным, хранящимся в блокчейне. Обнаружение любого несоответствия фактически выполняемого и эталонного кода сразу же говорит о том, что информационная система подверглась несанкционированному воздействию, что позволяет оперативно принять меры реагирования.

Принципиальная возможность использования подобного использования блокчейна для защиты устройств IoT с использованием достаточно дешёвой технологической базы была показана коллективом учёных из Московского технического университета связи и информатики [18].

В настоящее время в мировой практике существуют примеры внедрения блокчейн-технологий в системы защиты критической информационной инфраструктуры. Так, компания Guardtime использует технологию блокчейна для защиты энергосистемы Великобритании, включая атомные электростанции, средства защиты от наводнений и прочие элементы критической инфраструктуры. Guardtime использует собственный вариант блокчейна для защиты критической инфраструктуры, основанный на технологии под названием Keyless Signature Infrastructure (KSI). Эта система основывается на использовании хеш-функции для обеспечения целостности данных, что позволяет эффективно обеспечивать

синхронизацию блокчейна, аутентификацию данных и связь их с конкретным источником.

Технология блокчейна Guardtime KSI уже используется для защиты критически важной инфраструктуры в Эстонии, где блокчейн-технологии внедрены в ряде крупных сфер оказания государственных услуг – от регистрации браков до хранения медицинской информации о пациентах в общегосударственной системе [19].

Ограниченное внедрение технологий блокчейн (в частности, системы децентрализованного хранения данных) планируется осуществить и в России, в частности для мониторинга достоверности сведений Единого государственного реестра недвижимости [20]. Однако по состоянию на апрель 2021 г. реализуются лишь отдельные пилотные проекты.

Хотя блокчейн-технологии имеют большой потенциал использования для защиты распределенных элементов критической информационной инфраструктуры, для их повсеместного внедрения необходимо решение определённых проблем, которые могут стать ограничивающим фактором для их использования. К таким факторам можно отнести следующее [21].

1. Избыточность информации. При использовании блокчейн-технологий создается несколько копий данных на разных сетевых узлах, что позволяет обеспечить безопасное хранение данных в реестре. Однако при таком решении требуется обеспечивать избыточное хранение и обработку информации. Отдельные узлы должны участвовать в процессе проверки каждой транзакции, что требует увеличения занимаемого хранимыми данными пространства, а также приводит к увеличению потребления энергии. Кроме того, будущие кибератаки могут учитывать эту особенность блокчейн-систем для того, чтобы, осуществляя воздействие на один узел сети и наблюдая за распространением копий информации, атакующие могли установить структуру всей сети. Следовательно, применение блокчейн-технологий для обеспечения безопасности критической информационной инфраструктуры требует внедрения более эффективных технологий дедупликации информации.

2. Масштабируемость производительности. В одноранговой системе блокчейн необходимы поиски компромисса между децентрализацией и производительностью системы. Типичные блокчейн-системы обрабатывают транзакции со скоростью на один или несколько порядков медленнее, чем их централизованные аналоги. В отличие от других распределенных систем, добавление большего количества вычислительных узлов в блокчейн-сеть может не привести к увеличению пропускной способности сети. В зависимости от используемого протокола добавление большего количества узлов может даже существенно замедлить работу системы. В настоящее время учёные и коммерческие компании, внедряющие блокчейн-системы, работают над созданием новых протоколов согласования для решения проблемы масштабируемости.

3. Интеграция блокчейн-технологий в существующую инфраструктуру. Внедрение блокчейна во вновь создаваемых объектах критической информационной инфраструктуры требует интеграции с уже существующими системами, в частности использующими облачные технологии взаимодействия устройств IoT. Облачные ресурсы и сети IoT обычно имеют ограниченную пропускную способность, а использование блокчейн-технологий зачастую приводит к значительному росту объёмов передаваемой в компьютер-

ных сетях информации. Кроме того, возникают проблемы совместимости блокчейн-системы и других информационных технологий. Важно также, что внедрение блокчейна требует сотрудничества различных операторов систем критической информационной инфраструктуры, что также является нетривиальной организационной задачей.

Выводы

Атаки на критическую информационную инфраструктуру крайне опасны, и следует использовать максимально широкий спектр защиты от них, в том числе блокчейн-технологии. Наиболее перспективно использование блокчейна для обеспечения безопасности систем устройств Internet of Things и обеспечения их взаимодействия в условиях угрозы внешнего несанкционированного вмешательства. Это связано с такими свойствами блокчейн-систем, как децентрализованное хранение данных, программируемые смарт-контракты и авторизация. Использование блокчейн-технологий в контексте критической информационной инфраструктуры может защитить от уязвимостей, подобных тем, которые были использованы в Stuxnet. В мировой практике уже имеются примеры внедрения блокчейна для защиты критической информационной инфраструктуры, однако для полномасштабного использования данной технологии необходимо решить такие проблемы, как избыточность информации, масштабируемость производительности и интеграция блокчейн-технологий в существующую инфраструктуру.

В качестве правового механизма реализации указанных мер можно предложить внесение поправок в Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», регламентирующих возможность использования блокчейн-технологий, а также принятие подзаконных актов Правительства РФ и отраслевых министерств, устанавливающих требования к блокчейн-технологиям, используемым при защите объектов критической информационной инфраструктуры Российской Федерации.

Список литературы

1. Головин А. Ю. Классификация и характеристика лиц, совершающих преступления в сфере компьютерной информации // Организованная преступность, миграция, политика. М.: Рос. криминолог. ассоц., 2002. С. 108-111.

2. Поляков В. В., Попов Л. А. Особенности личности компьютерных преступников // Известия Алтайского государственного университета. 2018. № 6. С. 256–259.

3. Алиев Н. Т., Борбат А. В. Транснациональная организованная преступная деятельность в эпоху глобализации // Всероссийский криминологический журнал. 2020. Т. 14, № 3. С. 431–440.

4. Киберфизические, кибербиологические и искусственные когнитивные системы: сущность и юридические свойства / Д. Л. Кутейников, О. А. Ижаев, С. С. Зенин, В. А. Лебедев // Российское право: образование, практика, наука. 2019. № 3. С. 75–81.

5. Сердюк В., Тарви И. Некоторые аспекты защиты АСУ ТП // Information Security. 2017. № 6. С. 12–13.

6. Begishev I. R., Khisamova Z. I., Mazitova G. I. Criminal legal ensuring of security of critical information infrastructure of the Russian Federation // Revista gênero e direito. 2019. Vol. 8, No. 6. P. 283–292.

7. Bibliographical review on cyberattacks from a control-oriented perspective / H. S. Sánchez, D. Rotondo, T. Escobet, V. Ruig // Annual Reviews in Control. 2019. Vol. 48. P. 103–128.

8. The cousins of stuxnet: duqu, flame, and gauss / B. Bencsáth, G. Pek, L. Buttyan, M. Fellgyhazi // Future Internet. 2012. Vol. 4, is. 4. P. 971–1003.

9. Langner R. Stuxnet: dissecting a cyberwarfare weapon // IEEE Security & Privacy. 2011. Vol. 9, no. 3. P. 49–51.

10. Решетников А. Ю., Русскевич Е. В. Об уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274[1] УК России) // Законы России: опыт, анализ, практика. 2018. № 2. С. 51–55.

11. Piggin R. Cyber security trends: What should keep CEOs awake at night // International Journal of Critical Infrastructure Protection. 2016. Vol. 13. P. 36–38.

12. Бегишев И. Компьютерные атаки на КИИ России: правовые меры защиты // Information Security. 2019. № 5. С. 8–10.

13. Мещеряков Р. В., Исхаков А. Ю., Евсютин О. О. Современные методы обеспечения целостности данных в протоколах управления киберфизических систем // Информатика и автоматизация. 2020. Т. 19, № 5. С. 1089–1122.

14. Chen T. M., Abu-Nimeh S. Lessons from Stuxnet // Computer. 2011. Vol. 44, is. 4. P. 91–93.

15. Kendzierskyj S., Jahankhani H. The role of Blockchain in supporting critical national infrastructure // 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3). IEEE, 2019. P. 208–212. https://doi.org/10.1109/icgs3.2019.8688026.

16. Арюков А., Бегишев И., Мальцев Н. Некоторые аспекты информационной безопасности технологии блокчейн // Information Security. 2018. № 6. С. 18–19.

17. Georgescu A., Cîrnu C. E. Blockchain and critical infrastructures-challenges and opportunities // Romanian Cyber Security Journal. 2019. Vol. 1, No. 1. P. 93–100.

18. Защита данных в устройствах интернета вещей посредством применения технологии блокчейна / М. Г. Городничев, С. С. Махров, Е. Н. Денисова, И. Д. Булдин // Фундаментальные проблемы радиоэлектронного приборостроения. 2018. Т. 18, № 4. С. 879–883.

19. Shackelford S. J., Myers S. Block-by-block: leveraging the power of blockchain technology to build trust and promote cyber peace // Yale Journal of Law & Technology. 2017. Vol. 19. P. 334-388.

20. Заворина Л. Д., Ерохина А. А., Макарова Д. Г. Построение юридически значимого защищенного документооборота на основе блокчейн в информационных системах // Интерэкспо ГЕО-Сибирь. 2019. Т. 9. С. 42–46.

21. Dong Z., Luo F., Liang G. Blockchain: a secure, decentralized, trusted cyber infrastructure solution for future energy systems // Journal of Modern Power Systems and Clean Energy. 2018. Vol. 6, No. 5. P. 958–967. https://doi.org/10.1007/s40565-018-0418-0.

References

1. Golovin A. Yu. Klassifikaciya i harakteristika lic, sovershayushchih prestupleniya v sfere komp'yuternoj informacii [Classification and characteristics of persons committing crimes in the field of computer information]. *Organizovannaya prestupnost', migraciya, politika = Organized crime, migration, politics*. Moscow, Ros. kriminolog. assoc. Publ., 2002, pp. 108–111.

2. Polyakov V. V., Popov L. A. Osobennosti lichnosti komp'yuternyh prestupnikov [Features of the personality of computer criminals]. *Izvestiya Altayskogo gosudarstvennogo universiteta = News of the Altai State University*, 2018, no. 6, pp. 256–259.

3. Aliev N. T., Borbat A. V. Transnacional'naya organizovannaya prestupnaya deyatel'nost' v epohu globalizacii [Transnational organized criminal activity in the era of globalization]. *Vserossijskij kriminologicheskij zhurnal = All-Russian Journal of Criminology*, 2020, vol. 14, no. 3, pp. 431–440.

4. Kutejnikov D. L., Izhaev O. A., Zenin S. S., Lebedev V. A. Kiberfizicheskie, kiberbiologicheskie i iskusstvennye kognitivnye sistemy: sushchnost' i yuridicheskie svojstva [Cyberphysical, cyberbiological, and artificial cognitive systems: Essence and legal properties]. *Rossijskoe pravo: obrazovanie, praktika, nauka = Russian Law: Education, Practice, Science*, 2019, no. 3, pp. 75–81.

5. Serdyuk V., Tarvi I. Nekotorye aspekty zashchity ASU TP [Some aspects of automated process control system protection]. *Information Security*, 2017, no. 6, pp. 12–13.

6. Begishev I. R., Khisamova Z. I., Mazitova G. I. Criminal legal ensuring of security of critical information infrastructure of the Russian Federation. *Revista gênero e direito*, 2019, vol. 8, no. 6, pp. 283–292.

7. Sánchez H. S., Rotondo D., Escobet T., Puig V. Bibliographical review on cyberattacks from a control-oriented perspective. *Annual Reviews in Control*, 2019, vol. 48, pp. 103–128.

8. Bencsáth B., Pek G., Buttyan L., Fellgyhaz M. The cousins of stuxnet: duqu, flame, and gauss. *Future Internet*, 2012, vol. 4, is. 4, pp. 971–1003.

9. Langner R. Stuxnet: dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, 2011, vol. 9, no. 3, pp. 49–51.

10. Reshetnikov A. Yu., Russkevich E. V. Ob ugolovnoj otvetstvennosti za nepravomer-noe vozdejstvie na kriticheskuyu informacionnuyu infrastrukturu Rossijskoj Federacii (st. 274[1] UK Rossii) [On Criminal Liability for Unlawful Influence on the Critical Information Infrastructure of the Russian Federation (Article 2741 of the Criminal Code of Russia)]. *Zakony Rossii: opyt, analiz, praktika = Laws of Russia: experience, analysis, practice*, 2018, no. 2, pp. 51–55.

11. Piggin R. Cyber security trends: What should keep CEOs awake at night. *International Journal of Critical Infrastructure Protection*, 2016, vol. 13, pp. 36–38.

12. Begishev I. Komp'yuternye ataki na KII Rossii: pravovye mery zashchity [Computer attacks on Russian CII: Legal protection measures]. *Information Security*, 2019, no. 5, pp. 8–10.

13. Meshcheryakov R. V., Iskhakov A. Yu., Evsyutin O. O. Sovremennye metody obespecheniya celostnosti dannyh v protokolah upravleniya kiberfizicheskih sistem [Modern methods of ensuring data integrity in control protocols of cyberphysical systems]. *Informatika i avtomatizaciya = Informatics and Automation*, 2020, vol. 19, no. 5, pp. 1089–1122.

14. Chen T. M., Abu-Nimeh S. Lessons from Stuxnet. *Computer*, 2011, vol. 44, is. 4, pp. 91–93.

15. Kendzierskyj S., Jahankhani H. The role of Blockchain in supporting critical national. 2019 IEEE 12th International conference on global security, safety and sus-tainability (ICGS3). IEEE, 2019, pp. 208–212. https://doi.org/10.1109/icgs3.2019.8688026.

16. Aryukov A., Begishev I., Mal'cev N. Nekotorye aspekty informacionnoj bezopasnosti tekhnologii blokchejn [Some aspects of information security of blockchain technology]. *Information Security*, 2018, no. 6, pp. 18–19.

17. Georgescu A., Cîrnu C. E. Blockchain and critical infrastructures-challenges and opportunities. *Romanian Cyber Security Journal*, 2019, vol. 1, no. 1, pp. 93–100.

18. Gorodnichev M. G., Mahrov S. S., Denisova E. N., Buldin I. D. Zashchita dannyh v ustrojstvah interneta veshchej posredstvom primeneniya tekhnologii blokchejna [Data protection in Internet of Things devices through the use of blockchain technology]. *Fundamental'nye problemy radioelektronnogo priborostroeniya = Fundamental problems of radio-electronic instrumentation*, 2018, vol. 18, no. 4, pp. 879–883.

19. Shackelford S. J., Myers S. Block-by-block: leveraging the power of blockchain technology to build trust and promote cyber peace. *Yale Journal of Law & Technology*, 2017, vol. 19, pp. 334–388.

20. Zavorina L. D., Erohina A. A., Makarova D. G. Postroenie yuridicheski znachimogo zashchishchennogo dokumentooborota na osnove blokchejn v informacionnyh sistemah [Building a legally significant secure document flow based on blockchain in information systems]. *Interekspo GEO-Sibir' = Interexpo GEO-Siberia*, 2019, vol. 9, pp. 42–46.

21. Dong Z., Luo F., Liang G. Blockchain: a secure, decentralized, trusted cyber infrastructure solution for future energy systems. *Journal of Modern Power Systems and Clean Energy*, 2018, vol. 6, no. 5, pp. 958–967. https://doi.org/10.1007/s40565-018-0418-0.

Информация об авторе / Information about the Author

Гребеньков Александр Александрович, кандидат юридических наук, доцент, доцент кафедры уголовного права, Юго-Западный государственный университет, г. Курск, Российская Федерация,
e-mail: grebenkov@gmail.com
ORCID: 0000-0001-5028-090X

Alexander A. Grebenkov, Candidate of Juridical Sciences, Associate Professor, Associate Professor of the Department of Criminal Law, Southwest State University, Kursk, Russian Federation,
e-mail: grebenkov@gmail.com
ORCID: 0000-0001-5028-090X