**Вершицкий А.В., Мельниченко В.Х.**

**ПРИМЕНЕНИЯ BLOCKCHAIN В ГОСУДАРСТВЕННЫХ СТРУКТУРАХ И КИБЕРБЕЗОПАСНОСТЬ ГОСУДАРСТВА**

**Аннотация:** *в статье рассмотрены преимущества и недостатки современных Blockchain-технологий, которые угрожают кибербезопасности государственных данных. Актуальность работы заключается в оценке целесообразности применения технологии Blockchain в государственных структурах в условиях повышения активности киберпреступников.*

**Ключевые слова:** *кибертерроризм, кибербезопасность, Blockchain, государственные структуры, мошенничество, базы данных.*

В последние годы механизм работы кибербезопасности государства проходит значительное преображение. Это диктуется современными условиями, при которых кибертеррористы проводят все более изощренные атаки на все сферы государственного регулирования. Мошенничество в цифровой сфере уже не носит единичный характер как десятилетие назад, где случаи хакерских атак были прецедентами. Сейчас это сформированные преступные группировки, имеющие достаточное количество ресурсов, чтобы представлять угрозу не только отдельным организациям и компаниям, но и государству в целом. Атаки стали носить не массовый характер, все чаще они становятся целенаправленными. Существуют списки вакансий среди террористических организаций, среди которых IT-специалисты занимают не последнее место. Председатель комиссии Общественной палаты по развитию общественной дипломатии и поддержке соотечественников за рубежом Елена Сутормина привела на примере «Исламского государства» (запрещенной в РФ террористической организации) неутешительные цифры — продвижение таких «рабочих» предложений активно ведется на 24 языках мира, среди которых русский язык на 3 месте [1]. Еще одна черта современного кибертерроризма — быстрая адаптация к применяемым новым технологиям в цифровой среде.

Как такового конкретного понятие «кибертерроризм» не существует, пока исследователи сходятся лишь во мнении, что обязательным условием кибертерроризма является целенаправленная атака на компьютерные сети, в результате которой наносится вред населению, государству, социальной сфере. Впервые попытку дать определение новой угрозе со стороны технологий предпринял Барри Коллин в 1990-х г., но он отнес это явление к новой форме терроризма [2]. Не дает такого определения и законодательство РФ. Понятие не закреплено ни в одном официальном документе, а именно Уголовном Кодексе РФ, Федеральном законе от 06.03.2006 № 35-Ф3 «О противодействии терроризму», постановлении Пленума Верховного Суда РФ от 09.02.2012 № 1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности», постановлении Пленума ВС РФ от 09.02.2012 № 1 «О некоторых вопросах судебной практики по уголовным делам и о преступлениях компьютерной направленности». Кибертерроризм причислен к виду террористических актов. Подобное упущение в законодательстве приводит к тому, что отсутствует состав преступления и уголовная ответственность. Не указаны в законе и формы проявления кибертерроризма, что делает работы правоохранительных органов сложнее, а деятельность киберпреступников проще, поскольку им доступны на законных основаниях любые «цифровые инструменты».

Рост киберпреступлений неуклонно растет. МВД России официально заявило о росте преступлений с использованием IT-технологий с 8,8% в 2018 г. до 14,5% в 2019 г. [3]. Однако МВД предоставляют сводки лишь по зарегистрированным преступлениям. Реальные цифры могут отличаться, так как большинство организаций, компаний, предприятий предпочитают решать возникшую угрозу своими силами, чтобы не портить репутацию, что также усложняет работу по предупреждению атак. В ходе Всемирного экономического форума в Давосе в 2020 г. зампред правления Сбербанка Станислав Кузнецов представил данные о потерях экономики РФ от кибератак в размере 2,5 трлн. рублей за 2019г. В 2020 г. предполагаются потери в размере 3,5–3,6 трлн. руб [4].. В 2020 году компания Positive Technologies опубликовала отчет, в котором также указывался рост кибератак за 2019 год на 19% в сравнении с 2018 г. (рис.1).

Рис.1 Количество кибератак на государственные учреждения в 2019г.. Источник: [5]

По итогам отчета, в пятерку самых атакуемых отраслей вошли: госучреждение, финансовые отрасли, промышленность, медицина, образование и наука. К таким же выводам пришли эксперты McAfee, анализируя ситуацию в мире [6]. По мнению компаний, вектор интересов преступников сместился с получения финансовой выгоды на кражу персональных данных физических и юридических лиц. Конфиденциальные данные стали центральной мишенью преступников, поэтому особенно отмечается рост атак именно на госсектор (рис.2).

Рис.2 Цель кибератак на госструктуры. Источник: [5].

С чем же связана такая преступная активность? В первую очередь, в современном мире происходит постоянное накопление и увеличение данных, которую хранят на электронных носителях. Аналитическая компания Gartner прогнозирует что, объем цифрового контента в мире увеличится с 4 млрд. терабайт (4 зетабайта) в 2016 г. до 96 зетабайт в 2020 г. [7]. Увеличение персональных данных приведет и к росту киберпреступности.

Во-вторых, государства используют традиционные централизованные базы данных, доступ к которым можно получить через ведомственные запросы. С появлением «электронных правительств» крупнейшими базами данных стали государственные. Как уже отмечалось выше, именно персональные данные становятся интересом киберпреступников. Центральные базы данных имеют доверенного администратора, который хранит данные с фактического соглашения их владельцев. В «электронном правительстве» гарантом выступает само государство. Удачные атаки на государственные хранилища и последующие утечки информации могут носить как локальный, так и трансграничный характер, приводят к ухудшению отношений между государствами, нарушению экономических и дипломатических связей, затруднению работы межгосударственных организаций. Однако главной целью становится непоправимая репутация государства как внутри него, так и на международной арене.

До 2008 года как таковых альтернатив центральному хранилищу не существовало. В 2008 г. Сатоши Накамото впервые в своей работе описал способ работы технологии Blockchain, призванной обеспечить прозрачность транзакций в сфере криптовалют [8]. С 2016 г. технология набирала невероятную популярность, поскольку её применение вышло далеко за границы не только криптовалют, но и финансового сектора в целом. Молодую технологию внедряют во многих странах (США, Китай, ОАЭ, Великобритания), причем не только в коммерческих сферах, но даже в государственных структурах [9].

Создатель технологии определяет Blockchain как цифровой реестр, не имеющий центральных органов управления. Технология Blockchain представляет собой ряд различных блоков выстроенных по определённым правилам, которые содержат информацию пользователей и участников сети. Связь между такими блоками обеспечивается, как правило, наличием в каждом блоке одинаковой информации, которая вносится пользователями всей сети. Это позволяет каждому владельцу блока данных смотреть данные других пользователей, при этом, не имея права их редактировать. Такой подход к организации данных не позволяет внести несанкционированных изменений как при двустороннем участии лиц, так и при наличии третьих лиц. Так как в последовательности криптографически связанных блоков постоянно добавляются новые блоки, модифицировать старые становится значительно сложнее. Новые блоки дублируются во всех копиях реестров в сети, а конфликты разрешаются автоматически с использованием установленных правил. Blockchain имеет множество достоинств в сравнении с централизованными хранилищем данных: внесение новой информации легко отслеживается, неизменность данных, трудность взлома системы, поскольку факт взлома хотя бы в одном блоке будет проявляться в остальных, отсутствие доверенных лиц — прямое взаимодействие между участниками. Велика вероятность, что в будущем эта технология заменит традиционные централизованные системы баз данных, которые в современных реалиях уже устаревают. Однако технология появилась недавно и все еще не до конца исследована, чтобы с уверенностью утверждать о её безопасном использовании, особенно в государственных структурах. Скорее существуют такие факторы, при которых достоинства Blockchain могут стать его самыми большими недостатками, и в итоге технология может стать новым инструментом в руках кибертеррористов.

Самой острой проблемой для развития Blockchain в России является отсутствие законодательной базы. Существующие законы для криптовалюты не регулируют применения Blockchain даже в финансовом секторе. В России уже есть опыт применения даже в государственных структурах, однако контролируется Blockchain на основе законодательства, которое применяется для регулирования деятельности «электронного правительства», что является не совсем верным. «Электронное правительство» представляет собой центральную базу данных, доступ к которой пользователь может получить через посредника — государственный орган. В Blockchain такая работа госструктур недействительна, так как технология обеспечивает пользователя необходимыми данными. Законодатель не регулирует полномочия, права и обязанности органов при использовании Blockchain. По сути их роль сводится к контролю процессов в системе и совершенствовании алгоритмов Blockchain для повышения эффективности его работы, однако никаких регламентов и постановлений не существует. Законодательное регулирование порождает проблемы как со стороны государственных органов, так и со стороны пользователей.

Blockchain позволяет просматривать данные всех участников системы, отслеживая любые действия, тем самым обеспечивая прозрачность деятельности государственных органов. Отсутствие центральной базы не позволяет злоумышленникам выкрасть данные, однако появляется новый способ — утечка данных с персонального устройства.

Дискуссионный вопрос: лучше ли использовать для государственных структур централизованную систему хранения или децентрализованную? Поскольку в большинстве случаев именно кража персональных данных становится целью атак кибепреступников, то логично, что для государства важна их серьезная защита. Государство может сконцентрировать ресурсы на охране нескольких крупных баз данных, пресекая утечку информации и вовремя реагируя на сигналы атаки. Технология Blockchain не нуждается в каком-либо хранилище, поэтому цель атаки отсутствует. Атаковать систему бессмысленно, поскольку требуется одновременно изменять информацию во всех блоках информации, что практически нереально. Однако абсолютная прозрачность и доступ к данным не мешает злоумышленникам воспользоваться такой открытостью. В отличие от государственных баз данных, где созданы условия для максимальной защиты информации, пользовательские устройства не обладают в большинстве случаев достаточным уровнем защиты. Кража данных с персонального устройства намного успешнее, чем атаки на защищенную базу данных (рис.3). Еще более уязвимыми представляются мобильные носители. Поэтому встает еще один важный вопрос о необходимом количестве персональной информации в Blockchain. Это также проблема отсутствующего законодательства, поскольку регламентация количества информации — ответственность государства. В Blockchain активно используются электронные подписи, однако это тоже несовершенная мера защиты, к тому же подпись также можно выкрасть: основная часть атак приходится именно на логины и пароли пользователей, которые чаще всего хранятся на ПК. Поэтому любой злоумышленник имеет свободный доступ к Blockchain.

Рис.3 Объекты кибератак в государственных структурах. Источник: [5].

Проблемой для государственных структур может оказаться и сама система Blockchain. Технология, как и любая компьютерная программа, напрямую зависит от написания алгоритмов. От уровня квалификации программистов, разрабатывающих алгоритмы, зависит работа целой системы. В мире отмечается острая нехватка специалистов по Blockchain, так как он появился недавно, и профессионалов с опытом написания алгоритмов мало. В самом Blockchain формируются большое количество кодов, которые позволяют системе автоматизировано исполнять транзакции согласно установленным в системе правилам. Ошибки в алгоритмах, кодах могут использоваться преступниками. Сама система не распознает какого-либо вмешательства, так как действие будет выполняться в рамках заданного Blockchain ошибочного алгоритмома. Скандал в 2016 г. о выводе денег из Blockchain Ethereum является ярким примером кражи из-за ошибки в коде. Хакер вывел из системы 43,9 млн. долларов, воспользовавшись уязвимостью [10]. При этом он опубликовал письмо, где указал, что действовал легально, в рамках алгоритмов Ethereum. Скандал привел к рекордному падению курсу криптовалюты и падению репутации Ethereum. Таким образом, можно утверждать, что Blockchain не лишен недостатков из-за человеческого фактора.

Важным остается и уровень доверия к государственным кадрам, которые будут работать с базами Blockchain. Государственные служащие, работающие с Blockchain, несут особую ответственность за внесение данных, так как они остаются неизменными в системе. Отсутствие закона и здесь играет важную роль — не определена правовая ответственность лиц, работающих с Blockchain. Всем платформам Blockchain присуща одна проблема — так называемая «задача византийских генералов» или проблема 51%. Если предположить, что произойдет искажение информации в более чем 50% блоков с данными, то Blockchain расценит искажение как верную информацию [11]. Намеренное злоумышленное внесение недостоверной информации, с целью получения собственной выгоды, также является уязвимостью системы. Коррупционный фактор можно рассматривать как мошенничество и даже кибертерроризм, поскольку противоправные действия наносят вред населению. К тому же это может привести к падению репутации государственных структур, не зависимо от того, являлись ли злоумышленники частью государственных структур или же нет.

Сейчас Blockchain продолжает изучаться многими странами, которые готовы его внедрить и узаконить. Нельзя не признать достоинства Blockchain, определенно, при условии его совершенствования, он окажет существенное влияние на методы управления и регулирования в используемых сферах [12]. Однако на современном этапе бездумное внедрение во все отрасли государственного регулирования может привести к катастрофическим последствиям, особенно в области государственного управления. Кибертеррористы могут вычислить недостатки в такой несовершенной технологии и воспользоваться ими, причиняя вред физическим и юридическим лицам, а также государству. Развитие Blockchain как инструмента на службе государства зависит от двух факторов: наличие четкого законодательства, регулирующего применение технологии в различных отраслях, и масштабная, работа специалистов, программирующих Blockchain. В таком случае Blockchain не только принесет пользу, как эффективная и прозрачная система транзакции, но и станет гарантом кибербезопасности данных пользователей.

**Библиографический список**

1. Дипломированный терроризм: ИГ пытается вербовать в России переводчиков и программистов // Russia Today [Электронный ресурс] – Режим доступа: https://ru.rt.com/8aar

2. Collin B. The Future of Cyberterrorism // Crime & Justice International Journal. — 1997. — Vol. 13

3. В МВД сообщили о росте числа преступлений в сфере IT // ТАСС - [Электронный ресурс] – Режим доступа: https://tass.ru/obschestvo/7491421

4. Сбербанк оценил потери экономики РФ от кибератак в 2019 году // ТАСС - [Электронный ресурс] – Режим доступа: https://tass.ru/ekonomika/7567667

5. Актуальные киберугрозы: итоги 2019 года // Отчет компании Positive Technologies - [Электронный ресурс] – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019/#id22

6. Cashen L. Cybercrime set to cost the world $6 trillion annually by 2021, could Blockchain be the answer? – [Электронный ресурс] – Режим доступа: https://medium.com/natmin-pure-escrow/-656f334f7a09

7. Herjavec R. Official Annual Cybercrime Report. Cybersecurity Ventures – [Электронный ресурс] – Режим доступа: https://cybersecurityventures.com.

8. Nakamoto. S., «Bitcoin: A Peer-to-Peer Electronic Cash System» - 2008. – [Электронный ресурс] – Режим доступа: https://bitcoin.org/bitcoin.pdf

9. Генкин А.С., Михеев А.А. Блокчейн. Как это работает и что ждет нас завтра. - М.: Альпина Паблишер, - 2017 – 572 с.

10. Хакер вывел $43,9 млн виртуальной валюты, созданной на Blockchain // Ведомости – [Электронный ресурс] – Режим доступа: https://www.vedomosti.ru/technology/articles/2016/06/20/645932

11. The Byzantine Generals Problem (with Marshall Pease and Robert Shostak) // ACM Transactions on Programming Languages and Systems – 1982 - 382-401 c.

12. Вершицкий А.В. Регуляторные технологии (RegTech) как метод усовершенствования нормативно-правового регулирования / А.В. Вершицкий, Н.А. Вершицкая // Экономика и предпринимательство. – 2020. – No 6. – С. 946-949.

**Информация об авторах**

Мельниченко Валерия Хачатуровна (Российская Федерация, г. Севастополь) – студент, Институт экономики и управления Крымского федерального университета имени В.И. Вернадского (melnchenko-lera2000@yandex.ru).

Вершицкий Андрей Вячеславович (Российская Федерация, г. Симферополь) - кандидат экономических наук, доцент, Институт экономики и управления Крымского федерального университета имени В.И. Вернадского (vershitsky@gmail.com).

**Vershitsky A.V., Melnichenko V.H.**

**BLOCKCHAIN APPLICATIONS IN STATE STRUCTURES AND STATE CYBER SECURITY**

**Annotation**: *the paper considers shortcomings of modern blockchain technologies that threaten the cyber security of government data. The relevance of the paper is the appropriateness of applying Blockchain technologies in the public bodies in conditions of cybercriminals’ increasing activity.*

**Keywords**: *cyber terrorism, cyber security, Blockchain, government agencies, fraud, databases.*

**Information about the authors**

Melnichenko, Valeriya H. (Russian Federation, Sevastopol) – student, Institute of Economics and Management, V.I. Vernadsky Crimean Federal University (melnchenko-lera2000@yandex.ru)

Vershitsky, Andrey V. (Russian Federation, Simferopol) - Candidate of Economics, Associated Professor of State and Municipal Management Department, Institute of Economics and Management, V.I. Vernadsky Crimean Federal University ([vershitsky@gmail.com](mailto:vershitsky@gmail.com))

**References**

1. Certified terrorism: IS is trying to recruit translators and programmers in Russia // M. Tishenko // Russia Today. – 2017. – 6 May. – URL: https://ru.rt.com/8aar

2. Collin B. The Future of Cyberterrorism // Crime & Justice International Journal. — 1997. — Vol. 13

3. The Ministry of Internal Affairs reported an increase in the number of crimes in the field of IT // TASS. – 2020. – 10 Jun. – URL: : https://tass.ru/ekonomika/7567667

4. Sberbank estimates the loss of the Russian economy from cyber attacks in 2019 // Economic Forum in Davos // TASS. – 2020. – 21 Jun. – URL: https://tass.ru/ekonomika/7567667

5. Actual cyberthreats: 2019 results // Positive Technologies – 2020. – 18 March. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019/#id22

6. Cashen L. Cybercrime set to cost the world $6 trillion annually by 2021, could Blockchain be the answer? Available at: https://medium.com/natmin-pure-escrow/-656f334f7a09

7. Herjavec R. Official Annual Cybercrime Report. Cybersecurity Ventures. Available at: https://cybersecurityventures.com.

8. Nakamoto. S., «Bitcoin: A Peer-to-Peer Electronic Cash System». Available at: : https://bitcoin.org/bitcoin.pdf

9. Genkin A., Mikheev A. Blockchain How it works and what awaits us tomorrow. Moscow, Alpina Publisher, 2017, 572 p.

10. Hacker withdrew $ 43.9 million of virtual currency created on Blockchain // P. Kantyshev // Vedomosti. – 2016. – 19 June. – URL: https://www.vedomosti.ru/technology/articles/2016/06/20/645932

11. The Byzantine Generals Problem (with Marshall Pease and Robert Shostak) // ACM Transactions on Programming Languages and Systems, 1982, 382-401 p.

12. Vershitsky A.V. Regulyatornyye tekhnologii (RegTech) kak metod usovershenstvovaniya normativno-pravovogo regulirovaniya / A.V. Vershitsky, N.A. Vershitskaya // Ekonomika i predprinimatel'stvo. – 2020. – No 6. – S. 946-949.