12.00.08

Уголовное право и криминология; уголовно-исполнительное право

Criminal Law and Criminology; Criminal Enforcement Law

DOI: 10.33693/2223-0092-2021-11-3-67-73

УДК 343.3

Цифровые преступления, совершаемые в отношении роботов

И.Р. Бегишев ©

Казанский инновационный университет имени В.Г. Тимирясова, г. Казань, Российская Федерация

E-mail: begishev@mail.ru

Аннотация. *Цель исследования.* Стремительное развитие сквозных цифровых технологий, внедрение и применение робототехники предопределяет необходимость поиска путей решения проблем охраны общественных отношений, связанных с цифровой безопасностью роботов. Робот по своей сути является программно-аппаратным средством, функционирование которого невозможно в отсутствие цифрового кода компьютерной программы. Указанные программы не характеризуются существенными отличиями от программного обеспечения иных цифровых устройств, ввиду чего весь спектр посягательств, включая неправомерный доступ и внедрение вредоносных компьютерных программ, которые в настоящее время совершаются в отношении обычных средств вычислительной техники, могут быть распространены и на их компьютерные программы. ***Выводы.*** Проведенное теоретическое исследование позволило прийти к следующим основным выводам: 1) неправомерный доступ может осуществляться не только к информации, хранимой, обрабатываемой и передаваемой средствами компьютерной и иной микропроцессорной техники, но и робототехническими устройствами; 2) в случае если вредоносная компьютерная программа содержит элементы цифрового кода, образующие ее пригодность к захвату управления роботом, она приобретает повышенную общественную опасность; 3) в случае если робот, в отношении которого осуществлялось посягательство, является составной частью автоматизированной системы управления или информационной системой субъекта критической информационной инфраструктуры, ответственность должна наступать по ст. 274.1 УК РФ, поскольку робот подпадает под признаки предмета данного состава преступления. Исходя из соображений обеспечения цифровой безопасности роботов и противодействия неправомерному их использованию, находим возможным предложить законодателю дополнить УК РФ нормами об ответственности за неправомерный доступ к охраняемой законом компьютерной информации, содержащейся в роботе, если это деяние повлекло захват управления роботом, и за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для захвата управления роботом.

Ключевые слова: робот, робототехника, неправомерный доступ, вредоносная компьютерная программа, цифровая информация; захват управления, уголовная ответственность, общественная опасность, цифровые технологии

ДЛЯ ЦИТИРОВАНИЯ: Бегишев И.Р. Цифровые преступления, совершаемые в отношении роботов // Социально-политические науки. 2021. Т. 11. № 3. С. 67–73. DOI: 10.33693/2223-0092-2021-11-3-67-73

DOI: 10.33693/2223-0092-2021-11-3-67-73

Digital Crimes, Committed Against Robots

I.R. Begishev ©

Kazan Innovative University named after V.G. Timiryasov,
Kazan, Russian Federation

E-mail: begishev@mail.ru

Abstract. *The purpose of the research.* The rapid development of end-to-end digital technologies, the introduction and application of robotics determines the need to find solutions to the problems of protecting public relations related to the digital security of robots. A robot is essentially a software and hardware tool, the functioning of which is impossible in the absence of a digital code of a computer program. These programs are not characterized by significant differences from the software of other digital devices, which is why the entire range of attacks, including unauthorized access and the introduction of malicious computer programs that are currently committed against conventional computer equipment can be extended to their computer programs. ***Results.*** The conducted theoretical research allowed us to come to the following main conclusions: 1) unauthorized access can be carried out not only to information stored, processed and transmitted by means of computer and other microprocessor technology, but also by robotic devices; 2) if a malicious computer program contains elements of digital code that make it suitable for capturing robot control, it becomes an increased public danger; 3) if the robot against which the attack was carried out is an integral part of an automated control system or an information system of a subject of a critical information infrastructure, the responsibility must come under article 274.1 of the Criminal Code of the Russian Federation, since the robot falls under the characteristics of the subject of this crime. Based on the considerations of ensuring the digital security of robots and countering their illegal use, we find it possible to propose to the legislator to supplement the Criminal Code of the Russian Federation with rules on liability for unlawful access to legally protected computer information contained in the robot, if this act entailed the seizure of control of the robot and for the creation, distribution or use of computer programs or other computer information, deliberately intended to capture control of the robot.

Key words: robot, robotics, unauthorized access, malicious computer program; digital information; control takeover, criminal liability, public danger, digital technologies

FOR CITATION: Begishev I.R. Digital Crimes, Committed Against Robots. *Sociopolitical Sciences*. 2021. Vol. 11. No. 3. Pp. 67–73. (In Russ.) DOI: 10.33693/2223-0092-2021-11-3-67-73

ВВЕДЕНИЕ

Предотвращение несанкционированного воздействия на цифровой код компьютерных программ во многом предопределяет как безопасность функционирования информационно-телекоммуникационных устройств, так и сохранение конфиденциальности обращающейся в них цифровой информации. Предупреждение, прогнозирование и устранение рисков неправомерного доступа к цифровой информации, внедрения вредоносных компьютерных программ в современных условиях широко распространяющейся цифровизации общественных отношений становится приоритетным направлением деятельности, концентрирующим усилия специалистов различных областей знаний. Приведем представляющийся нам справедливым тезис А.В. Габова и И.А. Хавановой о том, что «технологии и их развитие – давно уже не просто цель регулирования, они – самостоятельный фактор, провоцирующий новые формы и расширяющий возможности регуляции, обогащающий юридический инструментарий» [Габов, Хаванова, 2018: 226].

Преступления, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, традиционно характеризуются наличием тенденции к возрастанию: так, только за первые два месяца 2021 г. было зарегистрировано 81 496 преступлений в данной сфере, что на 29,4% больше, чем за аналогичный период прошлого года[1]. В общей структуре данной разновидности преступности выделяются деяния, связанные с неправомерным доступом к компьютерной информации, число которых увеличилось на 80%[2].

Вышеуказанные статистические показатели свидетельствуют о том, что режим правомерного использования, получения, передачи, распространения информации, циркулирующей в цифровых устройствах, подвергается серьезным рискам, доля реализации которых с каждым годом возрастает.

Подобные тенденции видятся совершенно закономерными. Цифровая информация в настоящее время становится не только средством реализации тех или иных прав и законных интересов, во многих случаях она непосредственно является социальной ценностью,

[1] Состояние преступности в Российской Федерации за январь–февраль 2021 года // Официальный сайт Министерства внутренних дел Российской Федерации. URL: https://media.mvd.ru/files/application/2088236

[2] Там же.

то есть тем, по поводу чего складываются общественные отношения. К примеру, сведения, составляющие охраняемую законом тайну, содержание телефонных и иных переговоров, передаваемых по сетям связи сообщений, во многих случаях представлены в форме цифровой последовательности сигналов, хранимых, обрабатываемых и передающихся средствами компьютерной и иной микропроцессорной техники, ввиду чего их справедливо можно относить к цифровой информации [Бегишев, Бикеев, 2020: 34].

Актуальные направления развития цифровых технологий все больше демонстрируют вектор роботизации. Уже сейчас крупные хозяйствующие субъекты широко применяют автоматизацию производства, задействуя промышленных роботов на различных этапах изготовления продукции. Несмотря на то, что полностью обеспечить роботами производственные процессы пока не представляется возможным, думается, что такое положение образуется в результате недостаточного доверия потенциальных эксплуатантов роботов к данной сквозной цифровой технологии. Такое обстоятельство имеет субъективную природу. Объективных препятствий к расширению сфер и характера роботизации, как представляется, не наличествует: качество производимой роботом продукции прогнозируемо превосходит результаты человеческого труда, а обученные по заданным алгоритмам роботы лишены всего перечня субъективных факторов, закономерно присущих человеку. В то же время производственной сферой не исчерпываются области, в которых внедрение робототехники видится высокоперспективным: вопросы оказания услуг, высокоавтоматизированный транспорт, военная и правоохранительная сфера, беспилотные летательные аппараты, робототехнические устройства, способные выполнять работу, связанную с риском для жизни и здоровья человека, – все изложенные обстоятельства позволяют обоснованно предположить, что экспоненциальное внедрение робототехники есть высоковероятное явление.

Бурное развитие сквозных цифровых технологий, внедрение и применение робототехники и технологий искусственного интеллекта предопределяет необходимость поиска путей решения проблем охраны общественных отношений [Бегишев, Хисамова, 2021: 126].

Цель исследования – выявить особенности неправомерного использования роботов, рассмотреть способы цифровых преступлений, совершаемых в отношении роботов, а также обосновать и предложить нормы об ответственности за неправомерный доступ к охраняемой законом компьютерной информации, содержащейся в роботе, если это деяние повлекло захват управления роботом, и за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для захвата управления роботом.

МЕТОДИКА ПРОВЕДЕНИЯ ИССЛЕДОВАНИЯ

Материалами для работы послужили положения российского уголовного законодательства об ответственности за совершение преступлений в сфере компьютерной информации, а также результаты теоретических исследований в сфере применения робототехнических технологий. Методологическую основу исследования составили общенаучные и частнонаучные методы научного познания. Их применение позволило обеспечить обоснованность проведенного исследования, теоретических и практических выводов и разработанных предложений.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

В затронутом контексте обозначим, что робот по своей сути является программно-аппаратным средством, функционирование которого невозможно в отсутствие цифрового кода компьютерной программы. Именно данный код содержит в себе алгоритмы действий, реализуя которые робот совершает конкретные механические манипуляции (перемещение в пространстве, перенос предметов, изменение своего состояния и т.д.). Содержание и количество алгоритмов действий, внедренных разработчиками в цифровой код компьютерной программы робота, напрямую детерминирует характер, пределы совершаемых роботом манипуляций, их длительность, взаимосвязь и, как итог, конечный результат деятельности робота. Нарушение функционирования вышеуказанного цифрового кода, инициирование сбоев в его работе закономерно может повлечь негативные, в том числе общественно опасные девиации в его механических манипуляциях.

Отметим, робот не является типичным средством вычислительной техники. Помимо возможностей по хранению, обработке, передаче цифровой информации, робот, и это его отличительная особенность, может совершать вышеупомянутые механические манипуляции, что повышает общественную опасность цифровых противоправных посягательств, совершаемых в отношении него. Как справедливо отмечается Е.С. Михалевой, Е.А. Шубиной, «для юридической науки важным аспектом выступает не столько конкретная инженерно-техническая архитектура робота, сколько возможности и функции, которые могут быть воплощены с помощью данной архитектуры» [Михалева, Шубина, 2019: 27].

В то же время программная часть робота не характеризуется существенными отличиями от программного обеспечения иных цифровых устройств, ввиду чего весь спектр посягательств, включая перехват и внедрение вредоносных программ, которые в настоящее время совершаются в отношении обычных средств вычислительной техники, при придании роботам большей распространенности могут быть распространены и на их компьютерные программы. Таким образом, противоправные вмешательства в работу цифрового кода компьютерной программы робота охватываются действующими составами УК РФ.

Так, робот, равно как и иное цифровое устройство, может хранить, обрабатывать и передавать посредством цифровых каналов информацию, которая может быть перехвачена и видоизменена. При этом такая информация может быть обычным сообщением либо сигналом управления, получив который робот совершает определенные механические манипуляции. Представляется, что несанкционированное воздействие на сигналы управления роботом является в достаточной степени общественно опасным, поскольку

влечет нарушение его функционирования и затруднение управления им. При этом средства, способы, методы и инструменты цифрового перехвата, совершаемого в отношении роботов, по существу, не отличаются от аналогичных деяний, оказывающих неправомерное воздействие на компьютеры, серверы, информационные системы и т.д.

Аналогичным образом представляется возможным высказаться и в отношении внедрения в программные компоненты робота вредоносных компьютерных программ. Будучи способными оказывать, в том числе скрытое, несанкционированное воздействие на информацию, вредоносные программы выступают серьезной угрозой функционированию роботов.

Заметим, что действующие в настоящее время редакции составов преступлений, описывающие такие деяния как неправомерный доступ к компьютерной информации и использование вредоносных программ, предусматривают либо обязательное последствие в виде уничтожения, блокирования, модификации либо копирования информации, либо использование программ, заведомо предназначенных для таких последствий.

Поясним, что хранение, обработка и передача информации хотя и могут осуществляться программными средствами робота, однако не являются его основным предназначением. В этом, в том числе, и состоит отличие робота от иной компьютерной техники: обладая развитой аппаратной частью, робот используется для совершения механических манипуляций (либо коммуникации с человеком). В этой связи уничтожение, блокирование, модификация и копирование информации, хранящейся в роботе и выступающей средством его функционирования, не является наиболее общественно опасным последствием несанкционированного воздействия на него.

Заметим также, что объективными и субъективными признаками вышеуказанных составов преступлений в значительной степени охватываются как неправомерный доступ, так и внедрение вредоносных программ в робота. Выявленные различия касаются только признаков, характеризующих последствие (применительно к ст. 272 УК РФ, в ст. 273 УК РФ последствия не включены в структуру обязательных признаков основного состава).

Помимо этого, следует отметить, что предметом посягательства в данном случае будет не робот (представляющий собой единство программного или аппаратного компонентов), а цифровой код компьютерной программы робота. Именно цифровой код содержит поведенческие алгоритмы робота, реализуя которые последний способен на совершение конкретных механических действий. Целенаправленное воздействие программных, в том числе вредоносных, и (или) программно-аппаратных средств на иные составляющие робота не приведет к общественно опасному результату.

Нам представляется, что уничтожение, блокирование, модификация либо копирование цифровой информации, содержащейся в роботе, является только предпосылкой наиболее неблагоприятного варианта развития преступного события, в качестве которого выступает образование возможности совершения преступления с использованием робота. При этом лицо должно не просто осуществить неправомерный доступ, но и получить реальную возможность своими действиями определять действия робота, то есть осуществлять в отношении него управленческие функции.

В то же время в случае вовлечения в процесс совершения преступления управляемый робот выступает только и исключительно в качестве средства совершения преступления, ввиду чего возможно квалифицировать такие деяния по тем уголовно-правовым нормам, которые предусматривают ответственность за основные преступления (те, объективная сторона которых была выполнена с использованием робота). К примеру, в случае если в рамках приготовления к умышленному уничтожению имущества в крупном размере лицо осуществило несанкционированное воздействие на цифровой код компьютерной программы робота, в результате чего приобрело возможность управлять им и с его помощью уничтожило имущество, содеянное образует совокупность преступлений. В данном контексте выражаем солидарность с позициями авторов, указывающих, что не все составы преступлений в действующем УК РФ нуждаются в дополнении квалифицирующим признаком, характеризующим использование роботов при выполнении объективной стороны [Грачева, Арямов, 2020: 176].

В то же время действия, совершаемые с использованием робота после захвата его управления, могут не образовывать состава преступления, однако влечь причинение вреда законным интересам государства, общества и личности. В затронутом контексте возможны два варианта:

- деяние, совершаемое с использованием робота после несанкционированного воздействия и захвата управления, содержит признаки состава административного правонарушения;
- деяние, совершаемое с использованием робота после несанкционированного воздействия и захвата управления, не образует состава преступления или административного правонарушения, однако является противоправным, к примеру, порождает гражданско-правовые отношения ответственности в случае причинения ущерба в виде упущенной выгоды.

К примеру, в случаях, когда робот, входящий в систему осуществления производственных процессов, был выведен из строя (при этом полностью сохранил свой функционал, то есть не был ни поврежден, ни уничтожен), что повлекло приостановление производственного процесса организации – хозяйствующего субъекта и причинило ущерб в виде упущенной выгоды, которую данное юридическое лицо могло бы получить в нормальных производственно-технических условиях, если бы его право на осуществление коммерческой деятельности не было бы нарушено в результате захвата управления роботизированной производственной системой, а также ущерба в виде издержек, истраченных на возобновление производственного процесса.

Таким образом, представляется целесообразным утверждать, что в качестве общественно опасного последствия несанкционированного воздействия на цифровой код компьютерной программы робота выступает захват управления им.

ISSN 2223-0092 (print)
ISSN 2310-7065 (online)

При этом суть опасности состоит в том, что приобретение возможности управления роботом детерминирует порождение обстоятельств, способствующих совершению иных преступлений и противоправных деяний, ликвидирует возможность собственника такого робота владеть, пользоваться или распоряжаться правомерно принадлежащим ему имуществом.

В то же время необходимо отличать захват управления от иных следствий уничтожения, блокирования либо модификации информации. К примеру, ликвидация возможности собственника робота по осуществлению требуемых действий может быть вызвана не только захватом управления, но и такой разновидностью модификации информации, как ее шифрование, в результате которой утрачивается возможность совершения каких-либо действий с зашифрованными сведениями.

Следует обозначить, что робот, как было обозначено ранее, в отличие от иных цифровых устройств, способен к совершению механических манипуляций, однако использование такой возможности в противоправных целях возможно только в случае, если был осуществлен захват управления. Иными словами, захват управления – это такое воздействие на цифровой код компьютерной программы робота, в результате которого виновное лицо получает возможность задействовать по своему усмотрению аппаратные возможности робота по совершению преступлений.

В случае если такого воздействия не было и описанное последствие не наступило, преступное событие как по характеру совершаемых действий, так и по наступающим последствиям полностью подпадает под признаки составов преступлений, предусмотренных ст. 272 и 273 УК РФ. В таком случае в отсутствие захвата управления отличительная особенность робота по совершению множества механических действий не вовлекается в орбиту преступления. Ввиду чего в ситуациях, когда несанкционированное воздействие программных и (или) программно-аппаратных средств робота не повлекло захват управления, робот выступает в качестве обычного цифрового устройства (средства вычислительной техники).

В то же время остановим внимание на том, что цифровые коды компьютерных программ современных роботов содержат различные по своей структуре, длине и сложности алгоритмы действий. Некоторые разновидности алгоритмов предполагают при их реализации возможность совершения роботом однократной, простой механической манипуляции (к примеру, перемещение в пространстве одной из частей робота), иные алгоритмы цифровых кодов предполагают возможность совершения роботом длительных, взаимосвязанных, объединенных единым назначением механических манипуляций, в результате которых робот совершает действия, сопоставимые с итогами человеческой деятельности. Подобные роботы предполагают различные характер и пределы человеческого участия: в первом случае человек полностью управляет и контролирует процесс совершения роботом механических манипуляций, поскольку каждая из них предопределена отдельным сигналом управления, направляемым человеком; во втором случае множества сигналов управления не требуется, для выполнения роботом конкретной задачи человеку достаточно подать исходный сигнал управления, который инициирует совершение роботом длинной цепочки взаимосвязанных действий.

Таким образом, представляется возможным сформулировать следующее определение захвата управления как признака, характеризующего последствие – приобретение в результате осознанного целенаправленного воздействия программных и (или) программно-аппаратных средств на цифровой код компьютерной программы робота возможности управления (координации) механическими манипуляциями робота либо возможности подавать роботу сигналы, инициирующие совершение им множества взаимосвязанных, не требующих человеческого вмешательства механических манипуляций.

В данном случае под несанкционированным воздействием возможно понимать как совершение действий, описанных в ст. 272 УК РФ, так и использование вредоносных компьютерных программ, предусмотренных ст. 273 УК РФ.

Обратим внимание на следующее обстоятельство: упомянутые составы преступлений являются неоднородными по структуре признаков, описывающих объективную сторону, – если неправомерный доступ для образования состава обязательно должен повлечь последствие, то в ст. 273 УК РФ законодатель указывает на «заведомую предназначенность» компьютерных программ для использования в целях достижения таких последствий. В то же время сами последствия не являются обязательным признаком основного состава преступления.

Полагаем, что подобное законодательное конструирование адекватно отражает характер и степень общественной опасности описанных в составах деяний и является удачным и конструктивным.

Думается, что в случае, если вредоносная компьютерная программа заведомо предназначена для захвата управления роботом, ее создание, использование и распространение само по себе общественно опасно и образует состав преступления вне зависимости от факта наступления последствий.

Таким образом, представляется, что возможно ввести признак «заведомого предназначения» программы для целей захвата управления роботом, под которым возможно понимать совершение описанных в составе действий в отношении цифрового кода компьютерной программы, содержащей элементы, которые при их внедрении в компьютерную программу робота могут повлечь захват управления им. При этом виновное лицо во всех случаях должно осознавать наличие во вредоносной компьютерной программе таких элементов.

При этом совершенно закономерно, что захват управления робота может влечь иные общественно опасные последствия, в том числе и образующие самостоятельные составы преступлений, однако указанные последствия видится нецелесообразным включать в законодательную конструкцию (то есть состав преступления).

Следует обозначить, что робот как программно-аппаратное средство может использоваться на объектах критической информационной инфраструктуры, выполняя самостоятельные функции либо являясь частью иных обеспечительных систем.

Появление робота в составе критически важных и (или) потенциально опасных объектов представляется более вероятным, ввиду чего видится необходимым выработать достаточные уголовно-правовые средства, обеспечивающие их безопасное функционирование в составе объектов критической информационной инфраструктуры.

В затронутом контексте выскажем замечание, что состав преступления, предусматривающий ответственность за посягательства на такие объекты (ст. 274.1 УК РФ), в числе признаков, характеризующих деяние, предусматривает все вышеизложенные формы противоправного поведения, как касающиеся неправомерного доступа, так и связанные с вредоносными программами.

Отличительным признаком в данном случае выступает предмет посягательства – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления критически важных и (или) потенциально опасных объектов информационной инфраструктуры.

В данном случае образуется некоторое формальное противоречие между предметом данного состава и роботом, поскольку отсутствует определенное представление о том, чем из вышеперечисленного выступает робототехническое устройство. В наибольшей степени робот сходен с автоматизированной системой управления производственными процессами, однако ввиду присущих возможностей по осуществлению механических манипуляций робот вполне закономерно может выполнять и сами технологические процессы, равно как и осуществлять за ними контроль.

Помимо изложенного, сохраняя способность к хранению, обработке и передаче цифровой информации, робот вполне может выступать частью информационной системы (к примеру, сервисные роботы, выполняющие функции коммуникации с посетителями).

Робот как программно-аппаратное средство может, в зависимости от своих тактико-технических характеристик и целевого предназначения, выступать как часть автоматической системы управления производственными процессами (при этом не только контролируя и управляя, но и самостоятельно осуществляя такие процессы), так и элементом информационной системы. Таким образом, включение понятия «робот» в Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» не требуется.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ И ВЫВОДЫ

Комплексно анализируя изложенное, приходим к следующим выводам.

1. Неправомерный доступ может осуществляться не только к информации, хранимой, обрабатываемой и передаваемой средствами компьютерной и иной микропроцессорной техники, но к информации, обращающейся в робототехнических устройствах. При этом уничтожение, блокирование, модификация и копирование информации не являются наиболее общественно опасными последствиями такого несанкционированного воздействия в отношении роботов. Наиболее общественно опасным, а соответственно и релевантным с точки зрения уголовного права является захват управления роботом. В то же время, в случае если такой неправомерный доступ не повлек захват управления роботом, а единственными общественно опасными последствиями выступают те, которые перечислены в ч. 1 ст. 272 УК РФ, данное деяние полностью охватывается признаками состава вышеуказанного преступления, поскольку отличительные свойства робота (по совершению механических манипуляций) в процесс общественно опасного посягательства вовлечены не были.
2. В случае если вредоносная компьютерная программа содержит элементы цифрового кода, образующие ее пригодность к захвату управления роботом, она приобретает повышенную общественную опасность, и, соответственно, деяние, состоящее в создании, использовании и распространении таких программ, должно влечь более тяжкую ответственность по сравнению с общей нормой (ст. 273 УК РФ).
3. В случае если робот, в отношении которого осуществлялось посягательство, является составной частью автоматизированной системы управления или информационной системой субъекта критической информационной инфраструктуры, ответственность должна наступать по ст. 274.1 УК РФ, поскольку робот подпадает под признаки предмета данного состава преступления.

Итак, в целях обеспечения цифровой безопасности роботов и противодействия неправомерному их использованию представляется возможным высказать предложение о дополнении структуры УК РФ следующими положениями.

1. Дополнить ст. 272 УК РФ новой частью в следующей редакции:
   «5. Неправомерный доступ к охраняемой законом компьютерной информации, содержащейся в роботе, если это деяние повлекло захват управления роботом.
   Неправомерный доступ к охраняемой законом компьютерной информации, содержащейся в роботе, если это деяние повлекло захват управления роботом, наказывается…»
2. Дополнить ст. 273 УК РФ новой частью в следующей редакции:
   «4. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для захвата управления роботом.
   Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для захвата управления роботом, наказывается…».

ISSN 2223-0092 (print)
ISSN 2310-7065 (online)

ЛИТЕРАТУРА

1. *Габов А.В.*, *Хаванова И.А.* Эволюция роботов и право XXI в. // Вестник Томского государственного университета. 2018. № 435. С. 215–233.
2. *Бегишев И.Р.*, *Бикеев И.И.* Преступления в сфере обращения цифровой информации. Казань: Казанский инновационный ун-т, 2020. 300 с.
3. *Бегишев И.Р.*, *Хисамова З.И.* Искусственный интеллект и уголовный закон. М.: Проспект, 2021. 192 с.
4. *Михалева Е.С.*, *Шубина Е.А.* Проблемы и перспективы правового регулирования робототехники // Актуальные проблемы российского права. 2019. № 12 (109). С. 26–35.
5. *Грачева Ю.В.*, *Арямов А.А.* Роботизация и искусственный интеллект: уголовно-правовые риски в сфере общественной безопасности // Актуальные проблемы российского права. 2020. Т. 15. № 6 (115). С. 169–178.

REFERENCES

1. *Gabov A.V.*, *Havanova I.A.* Evolution of robots and the 21st century law. *Vestnik Tomskogo Gosudarstvennogo Universiteta*. 2018. No. 435. Pp. 215–233.
2. *Begishev I.R.*, *Bikeev I.I.* Crimes in the sphere of digital information circulation. Kazan, 2020. 300 p.
3. *Begishev I.R.*, *Hisamova Z I.* Artificial intelligence and criminal law. Moscow, 2021. 192 p.
4. *Mikhaleva E.S.*, *Shubina E.A.* Challenges and prospects of the legal regulation of robotics. *Aktualnye Problemy Rossijskogo Prava*. 2019. No. 12 (109). Pp. 26–35.
5. *Gracheva Yu.V.*, *Aryamov A.A.* Robotization and artificial intelligence: Criminal law risks in the field of public security. *Aktualnye Problemy Rossijskogo Prava*. 2020. Vol. 15. No. 6 (115). Pp. 169–178.

Статья проверена программой Антиплагиат. Оригинальность – 81,08%

Р е ц е н з е н т: *Бикеев И.И.*., доктор юридических наук, профессор, заслуженный юрист Республики Татарстан; первый проректор, проректор по научной работе, профессор кафедры уголовного права и процесса Казанского инновационного университета имени В.Г. Тимирясова

Статья поступила в редакцию 14.04.2021, принята к публикации 25.05.2021
The article was received on 14.04.2021, accepted for publication 25.05.2021

СВЕДЕНИЯ ОБ АВТОРЕ

Бегишев Ильдар Рустамович, кандидат юридических наук, заслуженный юрист Республики Татарстан; старший научный сотрудник Казанского инновационного университета имени В.Г. Тимирясова. Казань, Российская Федерация. ORCID: https://orcid.org/0000-0001-5619-4025; Researcher ID: T-2409-2019; Scopus Author ID: 57205305394; eLIBRARY Author ID: 595003; E-mail: begishev@mail.ru

ABOUT THE AUTHOR

Ildar R. Begishev, Cand. Sci. (Law), Honored Lawyer of the Republic of Tatarstan; senior researcher at the Kazan Innovative University named after V.G. Timiryasov. Kazan, Russian Federation. ORCID: https://orcid.org/0000-0001-5619-4025; Researcher ID: T-2409-2019; Scopus Author ID: 57205305394; eLIBRARY Author ID: 595003; E-mail: begishev@mail.ru