Вестник РУДН. Серия: Юридические науки 2020 Т. 24. № 3. 717–734
RUDN JOURNAL OF LAW http://journals.rudn.ru/law

УГОЛОВНОЕ ПРАВО И КРИМИНОЛОГИЯ

CRIMINAL LAW AND CRIMINOLOGY

DOI: 10.22363/2313-2337-2020-24-3-717-734

Научная статья

КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ В СОВЕРШЕНИИ ПРЕСТУПЛЕНИЙ ДИВЕРСИОННОЙ И ТЕРРОРИСТИЧЕСКОЙ НАПРАВЛЕННОСТИ

Л.Р. Клебанов[1], С.В. Полубинская[2]

[1] Российский университет дружбы народов
117198, г. Москва, Российская Федерация, ул. Миклухо-Маклая, д. 6

[2] Институт государства и права РАН (ИГП РАН)
119019, г. Москва, Российская Федерация, ул. Знаменка, д. 10

В статье рассматриваются проблемы, возникающие в связи с совершением преступлений против государственной и общественной безопасности с использованием компьютерных и сетевых технологий. Эта тема приобретает актуальность в условиях, когда некоторые государства уже испытали на себя действие «боевых» компьютерных вирусов, что может расцениваться как ведение войны с использованием кибероружия. Наиболее известный пример — атака компьютерного вируса Stuxnet на иранский завод, осуществляющий обогащение урана. Вирус был создан специально для выведения из строя промышленных систем управления. Особую опасность представляет использование средств беспилотного наземного и воздушного транспорта для совершения террористических актов. С атаками террористов постоянно сталкиваются российские военные в Сирии: база Воздушно-космических сил в Хмеймим регулярно подвергается нападениям с использованием беспилотных летательных аппаратов — дронов. Не меньшие угрозы несет и совершение террористических актов с помощью компьютерных и сетевых технологий. Разрушительный потенциал кибертерроризма обусловливается повсеместной компьютеризацией государственной и общественной жизни, реализацией проектов по созданию «умных» городов, включая технологии «умного» транспорта, а также интенсивным развитием Интернета вещей. Целью статьи является анализ новых криминальных угроз государственной и обществен-

ной безопасности, а также изучение приобретающих актуальность высокотехнологичных способов совершения таких преступлений, как диверсии, террористические акты, иные преступления террористической направленности. Цена их последствий для общества очень высока, причем преступникам не всегда надо атаковать социально значимые объекты непосредственно — достаточно посеять панику среди населения, используя интернет-медиа, социальные сети и интернет-сайты органов власти различных уровней, предварительно получив к ним незаконный доступ. В статье описываются некоторые уже использованные способы совершения преступлений диверсионной и террористической направленности. Авторы обращают внимание на приоритет кибербезопасности как для разработчиков технических устройств с элементами искусственного интеллекта, так и для законодателей, которым следует обратить внимание на методы технического прогнозирования при разработке правовых норм, направленных на предупреждение новых способов совершения подобных преступлений. При написании статьи авторы использовали широкий круг российских и зарубежных источников научно-правовой, статистической, социологической и иной информации. Авторы применяли такие методы исследования, как анализ, синтез, дедукция, индукция, логико-юридический и сравнительно-правовой.

Ключевые слова: киберпреступность, кибератака, компьютерный вирус, кибертерроризм, кибербезопасность, диверсия, беспилотный транспорт, дроны

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Дата поступления в редакцию: 19 марта 2020 г.
Дата принятия к печати: 30 июня 2020 г.

Для цитирования:

Клебанов Л.Р., Полубинская С.В. Компьютерные технологии в совершении преступлений диверсионной и террористической направленности // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2020. Т. 24. № 3. С. 717–734. DOI: 10.22363/2313-2337-2020-24-3-717-734.

DOI: 10.22363/2313-2337-2020-24-3-717-734

Research Article

COMPUTER TECHNOLOGIES FOR COMMITTING SABOTAGE AND TERRORISM

Lev R. Klebanov[1], Svetlana V. Polubinskaya[2]

[1] Peoples' Friendship University of Russia (RUDN University)
6 Miklukho-Maklaya str., 117198, Moscow, Russian Federation

[2] Institute of State and Law of Russian Academy of Sciences
10 Znamenka str., 119019, Moscow, Russian Federation

Abstract. The article discusses the problems that arise in connection with the crimes against state and public security committed by use of computer and network technologies. This topic is becoming relevant because some states have already experienced the effects of “combat” computer viruses, which can be regarded as waging war using cyber weapons. The most famous example is the attack by

the Stuxnet computer virus on an Iranian uranium enrichment plant. The virus was created specifically to disable industrial control systems. The use of unmanned ground and air vehicles to carry out terrorist acts is of particular danger. The Russian military in Syria is constantly confronted with terrorist attacks: the Khmeimim aerospace forces base is regularly attacked with unmanned air vehicles — drones. Terrorist acts with the use of computer and network technologies are no less dangerous. The destructive potential of cyberterrorism is determined by the widespread computerization of state and public life, the implementation of projects to create smart cities, including smart transportation, as well as the intensive development of the Internet of things. The purpose of the article is to analyze new criminal threats to state and public security, as well as to study high-tech ways of committing crimes such as sabotage, terrorist acts, and other crimes of a terrorist nature. The cost of their consequences for society is very high, and criminals do not always need to attack social objects directly — it is enough to spread panic among the population using online media, social networks and websites of authorities of various levels, after obtaining illegal access to them. The article describes some of the techniques already used to commit crimes of sabotage and terrorism. The authors draw attention to the priority of cybersecurity both for engineers of devices with elements of artificial intelligence, and for lawmakers who should pay attention to methods of technical forecasting when developing legal norms aimed at prevention of new ways of committing such crimes. When writing the article, the authors used a wide range of Russian and foreign sources of legal, statistical, sociological and other information. The authors used such research methods as analysis, synthesis, deduction, induction, formal legal method as well as comparative legal method.

Key words: Cybercrimes, cyberattack, computer virus, cyberterrorism, cybersecurity, sabotage, unmanned transport, drones

Conflicts of interest. The authors declared no conflicts of interest.

Article received March 19, 2020
Article accepted June 30, 2020

For citation:

Klebanov, L.R., Polubinskaya, S.V. (2020) Computer technologies for committing sabotage and terrorism. *RUDN Journal of Law.* 24 (3), pp. 717–734. DOI: 10.22363/2313-2337-2020-24-3-717-734.

Введение

Большинство киберпреступлений «представляют собой не что иное, как совершение традиционного преступления нетрадиционным способом» (Brenner, 2007:383). Однако есть среди них и новые, ранее неизвестные уголовному праву общественно опасные деяния, которые могут совершаться лишь благодаря использованию компьютерных и сетевых технологий. К таким преступлениям относятся кибер- или компьютерные атаки (cyberattacks).

В российском законодательстве определение компьютерной атаки дается применительно к объектам критической информационной инфраструктуры. Такие действия определяются как целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функ-

ционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации (ст. 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры»)[3]. На практике кибератаки посягают на значительно более широкий круг объектов (Hathaway, Crootof, Levitz, Nix, Nowlan, Perdue, Spiegel, 2012:822–832).

В Ежегодном отчете о глобальных рисках Всемирный экономический форум, состоявшийся в 2018 г. в Давосе, риски кибератак выделил особо. Как отмечается в отчете, риски кибербезопасности в настоящее время возрастают как по частоте, так и по разрушительному потенциалу.

В этой статье мы рассматриваем некоторые hi-tech способы совершения преступлений, посягающих на государственную и общественную безопасность. В условиях, когда кибервойны становятся реальностью (Antonovich, 2011; Glebov, 2018; Shinkaretskaya, 2018), а кибератаки — главным орудием таких войн, эта проблема заслуживает повышенного внимания.

Использование «боевых» компьютерных вирусов как способ совершения диверсий

Эксперты по информационной безопасности предупреждают о новых киберугрозах и возрастающем риске уже известных, которые в скором времени могут стать реалиями нашей жизни. Среди них, в частности, — технологии Deepfake, способные создавать сфабрикованные фотоснимки, видео- и аудиозаписи, имеющие разительное сходство с оригиналом, аутсорсинг высокотехнологичных продуктов, рост числа онлайн-операций, производимых государственными и коммерческими организациями[4]. Добавим сюда и появление новых объектов для кибератак — автономных устройств с элементами искусственного интеллекта как мирного, так и военного назначения, активная разработка которых ведется во многих странах (Glebov, 2018:104–116; Ovcharov, Kozlov, 2019:179–187; Sheremet, Rudianov, Ryabov, Khruschev, 2016:35–39). Опасения, что террористы смогут получить контроль над автономным оружием, к которому относятся дроны, танки и т.п. устройства, «а хакеры смогут взламывать его для использования в недопустимых целях», стали одной из причин обращения группы из 116 специалистов, включая основателя *Tesla* и *SpaceX* Илона Маска, в ООН с призывом запретить разработку такого оружия[5].

Современный мир все больше убеждается в том, что т.н. «кибервойна» между суверенными государствами — уже не плод фантазий футурологов и пи-

[3] СЗ РФ. 2017. № 31 (ч. I). Ст. 4736.

[4] См.: Герасюкова М. Украсть лицо: 7 технологий, которых стоит бояться // Газета.ru. 6.10.2019, available at: https://www.gazeta.ru/tech/2019/10/05/12736819/tech_future.shtml?updated (Accessed 06 October 2019).

[5] См.: Более 100 специалистов требуют от ООН запретить разработку автономного оружия // Коммерсант, 21 августа 2017 г, available at: https://www.kommersant.ru/doc/3389860 (Accessed 25 February 2020).

сателей-фантастов, а обыденная реальность наших дней. Одним из первых актов диверсионной кибератаки одного государства против другого, ставшим достоянием общественности, считается атака компьютерного вируса Stuxnet (The Stuxnet Worm), разработанного американскими и израильскими специалистами и использованного против иранских предприятий, включенных в ядерную программу этой страны (Giraldi, 2019).

The Stuxnet Worm был разработан в первом десятилетии XXI в. и представляет собой вредоносное программное обеспечение, «изначально созданное для промышленных систем управления или группы аналогичных систем», используемых, к примеру, в газопроводах и электростанциях. Конечная цель вируса — «перепрограммирование промышленных систем управления с помощью изменения кода на программируемых логических контроллерах (ПЛК), чтобы заставить их работать так, как задумал злоумышленник, и скрыть эти изменения от оператора оборудования» (Falliere, Murchu, Chien, 2011). Stuxnet стал первым известным компьютерным вирусом, способным целенаправленно выводить из строя промышленные системы.

В Иране в 2010 г. (а возможно и раньше) вирус был применен в атаке на операционной системы компьютеров путем доступа к программному логическому контроллеру, который управляет механизмом для включения центрифуг, предназначенных для выделения и обогащения урана. Доступ к системе был получен через операционную систему Microsoft Windows и внутренние компьютерные сети, которые, в свою очередь, обеспечили доступ к программному обеспечению концерна Siemens, использовавшемуся в иранском ядерном научном центре в Натанзе (Langner, 2013). Центрифуги под воздействием вируса развили очень большую скорость вращения, что привело к их разрушению. В результате этой кибердиверсии было уничтожено около 20 процентов всех центрифуг на заводе общим числом не менее 1000.

Западные специалисты проследили путь действия Stuxnet в Натазне и определили последовательность действий, которые проделал вирус, разрушивший центрифуги[6] (Falliere, Murchu, Chien, 2011, Kushner, 2013).

Первый этап — проникновение вируса в компьютерную сеть завода. Специалисты по кибербезопасности определили, что вирус попал в сеть через инфицированный флэш-накопитель, что позволило ему автоматически загрузиться в компьютерную систему. Они также выдвинули версию, что кто-то вставил зараженную флэшку неумышленно или случайно, но, как мы покажем чуть позже, эта версия была ошибочной. Далее, вирус начал быстро распространяться через местную компьютерную сеть и приступил к поиску тех компьютеров (программного обеспечения, на них установленного), которые управляли центрифугами для

[6] Gershwin, A. (2019) Stuxnet, or How to Destroy a Centrifuge with a Small Piece of Code. Hackermoon. July 31, available at: https://hackernoon.com/stuxnet-or-how-to-destroy-a-centrifuge-with-a-small-piece-of-code-66se283f (Accessed 11 November 2019).

выделения обогащенного урана. Затем вирус устанавливает контроль над сотнями центрифуг, перепрограммирует их, и они начинают работать на очень высокой скорости, выходя из-под контроля. Как отмечают исследователи, вирус осуществил две атаки. Во время первой он «приказал» центрифугам работать на опасно высокой скорости в течение 15 минут, после чего «вернул» им обычную скорость. Во время второй атаки, месяц спустя, он замедлил вращение центрифуг приблизительно на 50 минут. Так повторялось на протяжении нескольких месяцев. И, наконец, спустя время, в результате работы на чрезмерно высокой скорости, зараженные механизмы вышли из строя, причинив ядерному научному центру в Натанзе тот вред, о котором говорилось выше.

Однако этим дело не закончилось — вирус, судя по всему, распространился дальше и инфицировал сотни тысяч компьютеров, использующих систему Microsoft и программное обеспечение Siemens, и, в конечном итоге, повредил большое число устройств за пределами Ирана. Несмотря на то, что Stuxnet был разработан с таким расчетом, чтобы исключить его дальнейшее распространение, он заразил другие компьютеры и распространился по всему миру (Giraldi, 2019).

В связи с этой кибератакой до недавнего времени оставался невыясненным одни вопрос: каким же образом вирусу удалось заразить компьютеры на заводе в Натанзе, если этот научный центр был на «строгом карантине» и не имел доступ к Интернету, так что попасть извне вирус не мог. Теперь ответ на этот вопрос известен. В 2004 году США и Израиль обратились к голландской службе внутренней безопасности (AIVD) с просьбой оказать помощь и найти подходящего иранца для проведения операции. На тот момент в Голландии проживало много граждан Ирана, и найти того, кто поедет в Иран, было относительно легко. В итоге подходящая кандидатура (иранский инженер, который в свое время сотрудничал с научным центром в Натанзе) была найдена. Инженер был завербован и проинструктирован, как инфицировать вирусом компьютеры с тем, чтобы вывести из строя центрифуги, обогащающие уран. Завербованный иранец, которому в обмен предложили солидную сумму денег и устройство на Западе, прибыл в Иран, основал компанию по установке компьютерных систем и ремонту компьютеров и смог получить контракт на работу с ядерным научным центром. Инженер несколько раз посетил центр, в процессе чего и смог внедрить вирус (Giraldi, 2019).

По сути, Stuxnet является кибероружием, и как пишет один из ведущих экспертов по кибербезопасности Ральф Лангнер, «только будущее может показать, как кибероружие повлияет на международные конфликты и, возможно, даже на преступность и терроризм». Он отмечает, что Stuxnet был использован как инструмент противодействия распространению ядерного оружия, но «в конечном счете открыл дверь к распространению, которое гораздо сложнее контролировать: к распространению технологии кибероружия» (Langner, 2013:17).

В подтверждение верности оценок Ральфа Лангнера в октябре 2018 г. в израильской прессе появились сообщения о том, что важные объекты иранской инфраструктуры и стратегические компьютерные сети вновь подверглись атаке компьютерного вируса, который был еще более агрессивным, разрушительным и сложным, нежели Stuxnet, однако израильские официальные лица отказались как-либо обсуждать роль Израиля в этом происшествии. Шеф иранского министерства гражданской обороны Голам Реза Джалали заявил, что Иран обезвредил новую версию вируса Stuxnet: «Недавно мы обнаружили новую версию Stuxnet, который состоял из нескольких частей… и пытался внедриться в наши системы»[7].

Более того, угроза кибердиверсий актуальна не только для стран Ближнего Востока. Так, по информации газеты The Washington Post, бывший президент США Барак Обама отдавал распоряжения провести секретную операцию по внедрению в российскую инфраструктуру «кибербомб» в ответ на якобы имевшее место вмешательство России в президентскую предвыборную кампанию 2016 г. Планировалось привести эти «кибербомбы» в действие в случае эскалации напряженности с Москвой. Кибероружие, вероятно, должно было вывести из строя или нарушить функционирование определенных важных объектов инфраструктуры страны[8].

Кибертерроризм — одна из самых разрушительных угроз XXI века

Террористы из группировок исламских фундаменталистов все большее внимание уделяют теме «электронного джихада», призывая своих сторонников, обладающих навыками хакеров, использовать их как можно шире (Ovchinskii, 2017:271).

Рабочее определение кибертерроризму дал в 1997 г. специальный агент ФБР Марк Поллит: «Преднамеренные политически мотивированные атаки на информацию, компьютерные системы, компьютерные программы и данные, выраженные в применении насилия по отношению к гражданским целям со стороны субнациональных групп или нелегальных агентов»[9].

Однако в этом определении речь идет преимущественно о направленности посягательств террористического характера, а для определения понятия тер-

[7] См.: TV report: Israel silent as Iran hit by computer virus more violent than Stuxnet. The Times of Israel. October 31, 2018, available at: https://www.timesofisrael.com/tv-report-israel-silent-as-iran-hit-by-computer-virus-more-violent-than-stuxnet/ (Accessed 14 November 2019).

[8] См.: Дунаевский И. WP: Обама приказал внедрить «цифровые бомбы» в инфраструктуру России // Российская газета. 23.06.2017, available at: https://rg.ru/2017/06/23/smi-obama-prikazal-vnedrit-cifrovye-bomby-v-infrastrukturu-rossii.html (Accessed 15 July 2017); Зубов Н. Барак Обама приготовил «кибербомбы» для России // Коммерсант. 23.06.2017, available at: https://www.kommersant.ru/doc/3335422 (Accessed 28 August 2017).

[9] См.: Krasavin S. What is Cyber-terrorism? available at: http://www.crime-research.org/analytics/Krasavin (Accessed 09 March 2018).

роризма требуется обращение к уголовному законодательству, поскольку терроризм практически во всех государствах рассматривается как преступление.

Так, УК РФ определяет террористический акт как совершение взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях дестабилизации деятельности органов власти или международных организаций либо воздействия на принятие ими решений, а также угроза совершения указанных действий в тех же целях (ст. 205). В американском законодательстве терроризм определяется как деятельность, связанная с насильственными действиями или действиями, опасными для жизни человека, направленными на запугивание или принуждение гражданского населения, оказание влияния на политику правительства путем запугивания или принуждения или воздействие на деятельность правительства с помощью массового уничтожения, убийства или похищения людей[10].

Таким образом, террористические акты от внешне сходных преступных деяний отличаются мотивами и целями лиц, их совершающих. По верному замечанию Сьюзан Бреннер, «деятельность та же самая, что осуществляется [обычными] преступниками — отличается только мотивация» (Brenner, 2007:399).

Поскольку компьютерные и сетевые технологии выступают орудиями и средствами совершения террористических актов, то в контексте нашего исследования нас будут интересовать *способы террористических кибератак (Terrorist Cyberattack),* что, по сути, представляет собой способы совершения террористических актов с использованием киберпространства. К этому добавим и иные способы совершения террористических актов, когда преступники прибегают к использованию высоких технологий. Использование современными террористами Интернета, информационных и телекоммуникационных систем для пропаганды своих идей, вербовки новых сторонников, получения информации и финансирования террористической деятельности также составляет существенный сегмент преступлений террористической направленности и требует специального анализа, выходящего за рамки настоящей статьи.

Использование киберпространства для совершения террористических актов возможно в разных вариациях. Одним из таких способов называют *web-defacement*. Суть этого способа в искажении информации, размещаемой на сайтах официальных органов с тем, чтобы посеять панику среди населения. Например, один из вероятных сценариев этой атаки, описанный в литературе, выглядит так: террористы размещают на веб-сайте Министерства национальной безопасности информацию, обращенную к жителям больших городов. Жители должны покинуть город из-за утечки химикатов. Если этот призыв подхватит пресса или

[10] 18 U.S. Code § 2331.

большое количество людей, то такое фальшивое послание может выглядеть «легитимным» и посеять панику с неописуемыми последствиями при массовом желании покинуть город и ясными финансовыми последствиями. Несмотря на то, что успех такого сценария маловероятен, поскольку иные формы предупреждения не продублируют эту фальшивку, но если его растиражирует интернет-телевидение, то последствия будут разрушительными. Увеличение популярности «New Media» позволяет увеличить действенность такого способа, поскольку их ответственность за проверку достоверности источников информации не такая, как у традиционных средств массовой информации (Charvat, 2018).

Другой сценарий распространения в компьютерных сетях заведомо ложной информации описывает Сьюзан Бреннер. Представим, что местное Управление экстренных служб и национальной безопасности в г. Сан-Франциско (США) через безопасную правительственную компьютерную систему получает сообщение о заложенном в системе скоростных электропоездов, обслуживающих город и окрестности (Bay Area Rapid Transit), «чемодане с ядерным устройством». В сообщении говорится, что устройство находится в руках террористов, обещающих взорвать его через два часа. Власти объявляют немедленную эвакуацию, что приводит к панике и хаосу в городе. На самом деле террористы, взломав правительственную компьютерную систему, отправили ложное сообщение о заложенном ядерном устройстве, а местные власти вполне объяснимо в эту информацию поверили. В результате в городе возникают паника и давка, дезорганизуется работа транспорта и дорожное движение, причиняется огромный материальный ущерб и — как следствие — снижается доверие населения к властям, не способным обеспечить безопасность людей (Brenner, 2007:392). Этот способ кибертерроризма, где компьютерные технологии используются для психологического манипулирования гражданским населением, автор называет *mass distraction* (Brenner, 2007:391–393).

Еще одним способом осуществления актов кибертерроризма является выведение *из строя объектов инфраструктуры, сопровождаемое человеческими жертвами, при помощи вирусного (вредоносного) программного обеспечения (malware)*. Возможности этого способа уже описаны на примере вируса Stuxnet.

Недавние атаки вирусов-шифровальщиков дают представление о другом сценарии развития событий. Такие программы могут либо просто блокировать доступ к компьютеру, либо зашифровывают все имеющиеся на нем файлы, а впоследствии за разблокировку и расшифровку требуют с потерпевших выкуп. Наиболее известной стала атака вируса-шифровальщика *Wanna Cry*, которой 12 мая 2017 г. только за один день подверглось в общей сложности 200 тысяч компьютеров в 74 странах мира, включая Украину, Тайвань, Индию, а самое большое количество атак было зафиксировано именно в нашей стране. Для расшифровки преступники требовали с каждой жертвы отправить сумму в 300–600 долларов США в криптовалюте биткоин на кошелек преступников. Конеч-

но, никаких гарантий расшифровки файлов после уплаты выкупа не было[11]. Помимо *WannaCry* существуют и другие программы-вымогатели (например, *CryptoLocker* и *CTB-Locker*). Вредоносные программы-вымогатели можно приобрести на специальных хакерских форумах и сайтах. В странах Восточной Европы, к примеру, некоторые из них продаются по цене от 35 до 3500 евро. Программы-вымогатели являются многофункциональными и, помимо блокировки устройства или шифрования файлов на нем, они могут похищать данные с этих устройств, причиняя тем самым вред не только клиентам банков, но и финансовой системе государства в целом (Ovchinskii, 2017:93, 94).

Использование беспилотного транспорта для совершения террористических актов и иных преступлений

Современные автотранспортные средства — от автомобилей до грузовиков — являются технически сложными устройствами, оснащенными большим количеством компьютеров, что делает их весьма уязвимыми для компьютерных атак[12]. Террористы могут получить доступ к запуску двигателя, рулевому управлению, тормозной системе автомобиля, наконец, заблокировать людей в машине. В 2015 г. два американских программиста экспериментально продемонстрировали, как можно перехватить управление автомобилем, за рулем которого находится водитель, и заставить машину двигаться по их желанию, причем Интернет позволяет совершать подобные действия из любой точки мира[13]. В этой связи специалист по компьютерной безопасности из Университета Нью-Йорка Джастин Каппос предупреждает: «Любая нация с возможностью запуска кибердрона может убить миллионы гражданских лиц путем взлома автомобилей»[14].

Самодвижущиеся беспилотные автомобили (self-driving cars), разработка которых активно ведется во многих странах, существенно увеличивают разрушительный потенциал автотерроризма. Чем более зависимым от компьютерных и сетевых технологий является транспортное средство, тем более уязвимым оно становится для кибератак.

---

[11] См.: Матвеев П. Как вирусы-вымогатели принимают платежи и почему они требуют «выкуп» в биткоинах? Forbes. 19.05.2017, available at: http://www.forbes.ru/technologii/344607-kak-virusy0vimogateli-prinimayut-platezhi-i-pochemu-oni-trebuyt-vykupv-bitkoynach (Accessed 11 August 2018).

[12] См.: Krisher, T. Hackers find ways to hijack car computers and take control. CTV News. September 3, 2013, available at: https://www.ctvnews.ca/sci-tech/hackers-find-ways-to-hijack-car-computers-and-take-control-1.1438138 (Accessed 13 January 2020).

[13] См.: Алексеева Е. Программисты перехватили управление автомобилем Jeep Cherokee через Интернет // За рулем. 22 июля 2015, available at: https://www.zr.ru/content/news/800391-programmisty-smogli-perexvatit-upravlenie-sovremennym-avtomobilem-video/ (Accessed 13 January 2020).

[14] См.: Хакеры могут убить миллионы людей путем удаленного взлома автомобилей, предупредили ученые // NEWSru.com. 21 ноября 2017 г., available at: https://auto.newsru.com.article/21nov2017/hack (Accessed 24 December 2017).

Пока даже без вмешательства хакеров этот вид транспорта нельзя считать в достаточной степени безопасным, и ряд несчастных случаев на дорогах с его участием уже зафиксирован в разных странах. Так, беспилотный автомобиль компании Uber в американском штате Аризона насмерть сбил женщину-велосипедиста. Этот автомобиль был создан на базе Volvo XC90 и управлялся в беспилотном режиме системой компьютерного контроля. В автомобиле, скорость движения которого составляла 45 миль в час, не было пассажиров, и управлялся он одним оператором[15]. Другой инцидент, обошедшийся без человеческих жертв, произошел в Вене, когда беспилотный автобус-шаттл компании Navya столкнулся с пешеходом, причинив ему незначительные травмы. Правда, оставалась неясность, по чьей вине произошло столкновение. Возможно, что причиной тому стало неосторожное поведение самого пешехода — 30-летней женщины, которая, одев наушники и глядя в экран мобильного телефона, переходила через дорогу[16].

Для кибертеррористов существует много возможностей применения для террористических атак беспилотного наземного транспорта, например, путем установления контроля над транспортными средствами и их использования для наезда на пешеходов, причинения вреда имуществу, дезорганизации дорожного движения и т.п[17]. Поэтому вопросы кибербезопасности таких автомобилей, среди прочих, должны стать приоритетными для их разработчиков и законодателей (Wing, 2016:707–742, Lee, 2017:25–52, Spencer, 2018:647–671).

Мировая практика уже дает немало примеров, когда для террористических атак используются и беспилотные летальные аппараты (дроны). Например, российская военная база (Хмеймим) в Сирии неоднократно уже подвергалась атакам беспилотников, запускаемых боевиками. Во время одного из таких «авианалетов» силы противовоздушной обороны базы уничтожили шесть беспилотников террористов, когда те только подлетали к базе[18]. В сентябре 2019 г. российские военные вновь отразили атаку десятков дронов и ракет, запущенных боевиками по базе Хмеймим. По словам официального представителя Минобороны России И. Конашенкова, к настоящему времени (сентябрь 2019 года) российские военные уничтожили 58 дронов и 27 ракет, выпущенных по базе. Он

[15] См.: Preliminary Report Highway HWY18MH010. National Transportation Safety Board. May 24, 2018, available at: https://www.ntsb.gov/investigations/AccidentReports/Pages/HWY18MH010-prelim.aspx (Accessed 24 November 2019).

[16] См.: Porter, J. (2019). Pedestrian collision puts Vienna's driverless bus trial on hold. The Verge. July 19, available at: https://www.theverge.com/2019/7/19/20700482/navya-self-driving-driverless-bus-vienna-collision-pedestrian (Accessed 22 July 2019).

[17] См.: Куликов Н. Безопасность беспилотников на дорогах: от соблюдения ПДД до киберугроз и терроризма // Forbes. 06.07.2017, available at: https://www.forbes.ru/tehnologii/346083-bezopasnost-bespilotnikov-na-dorogah-ot-soblyudeniya-pdd-do-kiberugroz-i (Accessed 15 September 2019).

[18] См.: Rockets Attack Hits Russian Base in Syria, Injuring Civilians. The Moscow Times. August 6, 2019, available at: https://www.themoscowtimes.com/2019/08/12/russia-repels-3rd-drone-attack-on-syrian-base-a66807 (Accessed 12 August 2019).

также добавил, что, несмотря на внешнюю примитивность сбитых дронов, они эффективны и их очень трудно обнаружить, и выразил беспокойство тем фактом, «что террористы использовали технологии навигации и управления, которыми обладают всего несколько стран»[19].

Западные специалисты обращают внимание на то, что угроза террористических атак на города, в которых будут использоваться дроны, снабженные программным обеспечением, позволяющим навести их на цели и выполнить запрограммированные действия, в настоящее время возрастает, и власти должны принимать соответствующие меры, чтобы отразить атаки террористов с использованием беспилотных летательных аппаратов против зданий и иных важных объектов. Как отмечает Николас Гроссман, террористы ИГИЛ (запрещенная в России террористическая организация) уже использовали в Сирии дроны, начиненные взрывчаткой, и ни одна террористическая группировка еще не использовала высокие технологии с таким размахом: «Поскольку дроны стали привычным делом в городах, их появление будет менее подозрительным, облегчая террористам атаку цели»[20]. К таким целям можно отнести, в числе прочих, атомные электростанции и посольства зарубежных государств[21].

Террористы ИГИЛ (запрещенная в России террористическая организация) также снабжают дроны GPS-навигаторами или видеокамерами, а управлять ими могут даже слабо обученные боевики. В начале 2018 г. в США возникла настоящая паника из-за падения на лужайку перед Белым домом в Вашингтоне двух небольших дронов, которых было очень трудно «засечь». Это происшествие вызвало целый ряд вопросов: как это могло случиться перед домом Президента США, каковы были цели этих дронов, что делала служба охраны, пока они кружили вокруг? И хотя дроны, как оказалась, использовались лишь в целях орошения, непринятие соответствующих мер безопасности в будущем может очень дорого обойтись[22].

Совсем недавно имело места атака дронов на два ключевых нефтяных завода в Саудовской Аравии. Саудиты заявили, что эту атаку осуществили йеменские хуситы, а Государственный секретарь США Майк Помпео обвинил Иран в том, что именно эта страна стояла за атаками йеменских боевиков. Атака вызвала мгновенную эскалацию напряженности в Персидском заливе между США и Ираном. Основной вопрос так и остался невыясненным: были ли эти

[19] См.: Russian military in Syria says it downed dozens of drones. Associated Press. September 27, 2019, available at: https://apnews.com/7bb8ba55ed504c2eb2c756135e22c54b (Accessed 12 October 2019).
[20] См.: Terrorist Drone Threat Against Western Cities is Increasing, available at: https://i-hls.com/archives/82445 (Accessed 12 April 2019).
[21] См.: In Depths: Drones and organized crime // EU-OCS — European Observatory of Crimes and Security. May 11, 2017, available at: //https://eu-ocs.com/depth-drones-organaized-crime (Accessed 27 July 2019).
[22] См.: Drone Surveillance: How criminals are using drones to commit crimes, available at: https://www.911security.com/blog/drone-surveillance-how-criminals-are-using-drones-to-commit-crimes (Accessed 25 August 2019).

беспилотники запущены с территории Ирана, и как хуситы смогли поразить цели в глубине Саудовской Аравии, находившиеся на расстоянии 500 миль от Йемена[23]. Заметим, что такие «бомбовые» атаки с помощью беспилотных летательных аппаратов использовали и мексиканские наркокартели, сбрасывая на цель взрывные устройства, приводимые в действие на расстоянии[24].

В практике борьбы с терроризмом уже известны случаи, когда террористы «взламывали» системы наблюдения, установленные на беспилотных летательных аппаратах сил государственной безопасности. К примеру, в 2017 г. суд израильского города Беер-Шева приговорил к девяти годам тюремного заключения компьютерного инженера Маджида Овейду — палестинского араба из сектора Газа. Как установило следствие, М. Овейда был завербован террористической организацией «Исламский джихад» (запрещенная в Российской Федерации террористическая организация) в 2011 г. В 2015 г. он согласился создать программное обеспечение, с помощью которого можно было «взломать» дроны-беспилотники Армии обороны Израиля. Будучи оснащенным персональным компьютером, декодером и спутниковой антенной, ему удалось с третьей попытки подключиться к передаче данных с израильских дронов. Это подключение в итоге позволило террористам получать ту же «картинку», которую наблюдали израильские военные, а такая информация относилась к категории секретной[25].

Беспилотные летательные аппараты могут использоваться также при совершении посягательств на жизнь глав государств и правительств, иных государственных и политических деятелей. Одна из таких попыток имела место в Венесуэле, когда, по информации властей этой страны, было совершено покушение на жизнь президента Венесуэлы Николаса Мадуро. Президент Мадуро произносил речь на мероприятии в Каракасе, посвященном 81-летию национальных вооруженных сил. По словам министра связи и коммуникаций Венесуэлы Хорхе Родригеса, вблизи того места, где выступал президент Мадуро, взорвались два дрона, начиненные взрывчаткой. Власти Венесуэлы обвинили в этом покушении руководство Колумбии и некоторые американские круги[26].

Помимо преступлений против государственной и общественной безопасности использование беспилотного транспорта встречается и при совершении уголовно наказуемых посягательств на иные охраняемые законом объекты.

---

[23] См.: Hubbard, B., Karasz, P., Reed, S. (2019) Two Major Saudi Oil Installations Hit by Drone Strike, and U.S. Blames Iran. The New York Times. September 14, 2019, available at: https://www.nytimes.com/2019/09/14/world/middleeast/saudi-arabia-refineries-drone-attack.html (Accessed 16 September 2019).

[24] См.: Tangermann, V. (2018) Criminals Are Now Using Swarms Of Small Drones To Befuddle Law Enforcement. Futurism. May 7, available at: https://futurism.com/royal-wedding-facial-recognition-ai (Accessed 19 July 2019).

[25] См.: Islamic Jihad terrorist convicted of hacking into drones. Arutz Sheva. February 3, 2017, available at: http://www.israelnationalnews.com/News/News.aspx/224344 (Accessed 13 October 2019).

[26] См.: Venezuela President Maduro survives 'drones assassination attempt'. BBC. August 5, 2018, available at: https://www.bbc.com.news/world-latin-america-45073385 (Accessed 13 October 2019).

Так, беспилотные летательные аппараты широко используются в целях контрабандного перемещения различных предметов, как находящихся в гражданском обороте, так и изъятых из него, например, для контрабанды наркотиков. Дроны-беспилотники применяются также для доставки в места лишения свободы различных запрещенных предметов — в США нередки новости о чрезвычайных ситуациях, которые возникают по причине «сбрасывания» с дронов наркотиков и оружия в тюремные внутренние дворы. Используются дроны и для дезориентации полиции во время проводимых ею операций. К примеру, агенты ФБР осуществляли наблюдение за организованной преступной группировкой, вовлеченной в захват и удержание в неизвестном месте заложников. Чтобы сорвать наблюдение, преступники использовали множество небольших дронов, которые на большой скорости летали на близком расстоянии от агентов, вынуждая их выдавать свое тайное местоположение. Более того, преступники стали выкладывать в YouTube сделанные с дронов снимки местоположения полицейских, чтобы помочь своим сообщникам избежать задержания[27].

Не так давно в британской прессе появилась информация о том, что дроны-беспилотники могут использоваться преступниками-педофилами. Полиция Соединенного Королевства уже получала заявления о подозрительных беспилотниках, которые кружили вокруг несовершеннолетних. К примеру, они были замечены вокруг несовершеннолетних девочек, загорающих на солнце. Эта информация дала основание полагать, что дроны используют педофилы, чтобы отслеживать передвижение детей или вести их съемку[28].

Широкое распространение беспилотных летательных аппаратов в разных странах ставит вопрос о правовом регулировании их оборота, выдаче разрешений на владение ими и их использование, официальной регистрации, юридической ответственности их владельцев и страховании такой ответственности, а также их кибербезопасности.

Западные специалисты уже поднимают вопрос о том, каким образом уголовное право сможет адаптироваться к быстрому развитию современных технологий и нужно ли вводить специальные нормы об ответственности за совершение преступлений с помощью дронов. В связи с частым использованием беспилотников для доставки запрещенных предметов в тюрьмы Соединенного Королевства обсуждается квалификация содеянного, поскольку действия лиц,

[27] См.: Crawford, J. (2018) 10 Crimes Committed Using a Drone. Listverse. July 26, available at: https://listverse.com/2018/07/26/10-crimes-committed-using-a-drone/ (Accessed 25 August 2019); Hicks, M. (2018) Criminal Intent: FBI details how drones are being used for crime. Techradar. May 4, available at: https://www.techradar.com/news/criminal-intent-fbi-details-how-drones-are-being-used-for-crime (Accessed 25 August 2019); Swales, V. (2019) Drones Used in Crime Fly Under the Law's Radar. The New York Times. November 3, available at: https://www.nytimes.com/2019/11/03/us/drones-crime.html (Accessed 14 November 2019).

[28] См.: In Depths: Drones and organized crime. EU-OCS — European Observatory of Crimes and Security. May 11, 2017, available at: https://eu-ocs.com/depth-drones-organaized-crime (Accessed 19 July 2019).

передающих в учреждения для отбывания наказания наркотики и оружие, укладываются лишь в рамки общих уголовно-правовых норм, не «отягощенных» таким квалифицирующим признаком, как использование дронов[29].

Речь идет, к примеру, о доставке или сговоре на доставку в тюрьмы запрещенных предметов, специально указанных в законе — в ст. ст. 40A, 40B, 40C Prison Act 1952. В ст. 40A приводятся три списка — A, B, C — запрещенных к доставке в тюрьму без соответствующего разрешения определенных предметов, как-то: мобильные телефоны, видеокамеры, алкоголь, наркотические средства, взрывные устройства, огнестрельное оружие и т.д[30]. Кроме того, в соответствии с Psychoactive Substances Act 2016 несет ответственность любое лицо, которое умышленно предлагает другому лицу психоактивное вещество, а значит, те, кто передают с помощью дронов на территорию тюрьмы такие вещества, совершают такое деяние[31].

С помощью удаленного доступа к компьютерным системам и сетям становятся возможным похищения людей и захват заложников. Так, в средствах массовой информации появились сообщения, что хакеры могут похитить миллиардеров — владельцев дорогих яхт и их гостей прямо в открытом море, получив через Интернет доступ к навигационным системам управления. Это наглядно продемонстрировал эксперт по кибербезопасности компании *BlackBerry* Кемпбелл Мюррей: через свой ноутбук он получил полный контроль над мегаяхтой, пришвартованной неподалеку. Контроль был установлен всего за 30 минут, после чего он мог спокойно управлять спутниковой связью, телефонной системой, навигацией и системой *Wi-Fi*. Сходным образом можно отключить систему видеонаблюдения на яхте, что позволит похитителям проникнуть на борт и захватить находящихся там людей. Уже есть случаи, когда некоторые владельцы яхт были вынуждены платить вымогателям выкуп за разблокирование навигационных систем своих судов[32].

Для захвата заложников может использоваться и ранее упомянутый беспилотный автомобильный транспорт. Например, американский город Денвер (штат Колорадо) недавно начал сотрудничество с корпорацией Panasonic с целью внедрения смарт-технологий для улучшения городской инфраструктуры и превращения Денвера в смарт-город (Smart City). Результатом сотрудничества стал проект развития транспорта (Transit-oriented Development Project), в част-

[29] См.: New Technology and Crime: Drones. The Open University. July 25, 2018, available at: https://www.open.edu/openlearn/society-politics-law/law/new-technology-and-crime-drones (Accessed 16 October 2019).
[30] См.: Prison Act 1952, available at: http://www.legislation.gov.uk/ukpga/Geo6and1Eliz2/15-16/52/crossheading/offences (Accessed 16 October 2019).
[31] См.: Psychoactive Substances Act 2016. Section 5, available at: http://www.legislation.gov.uk/ukpga/2016/2/section/5 (Accessed 16 October 2019).
[32] См.: Злобин А. Похищения и шантаж в открытом море: хакеры научились взламывать яхты миллиардеров // Forbes. 19.05.2017, available at: https://www.forbes.ru/milliardery/344611-pohishcheniya-i-shantazh-v-otkrytom-more-hakery-nauchilis-vzlamyvat-yahty (Accessed 24 August 2017).

ности, сообщения с аэропортом города с помощью беспилотного шаттла, который Panasonic создал совместно с французским производителем беспилотных автобусов Easy Mile[33].

Надо отметить, что в США федеральная программа по созданию, развитию и тестированию технологий «умного» транспорта реализуется в соответствии с Законом об эффективности наземных перевозок с взаимодействием различных видов транспорта 1991 г. (Intermodal Surface Transportation Efficiency Act или ISTEA). «Умные» транспортные системы (Intelligent Transportation System или ITS) используют три вида технологий: во-первых, связанные с дорожной инфраструктурой, во-вторых, связанные с транспортными средствами, и, наконец, обеспечивающие интеграцию транспортных средств и дорожной инфраструктуры. Подобные разработки осуществляются и в Японии, Южной Корее, Сингапуре и ряде других стран (Glancy, 2014:1623–1625). Транспортные средства и различные устройства дорожной инфраструктуры, контролирующие и регулирующие дорожное движение, соединяются между собой и обмениваются информацией с использованием компьютерных и сетевых технологий, к примеру, мобильных и беспроводных сетей (Glancy, 2014:1626–1640). Террористическая угроза таких технологий очевидна: установив контроль над «умными» транспортными системами и их элементами, террористы могут не только захватить в заложники пассажиров подключенных автобусов и автомобилей (connected vehicles), но и дезорганизовать работу самой системы.

Заключение

Подводя итог, отметим, что темпы появления новых способов совершения преступлений диверсионной и террористической направленности существенно опережают традиционные возможности выработки соответствующих норм уголовного закона. По-видимому, требуется применить методы технического прогнозирования, чтобы проектировать правовые нормы для предупреждения новых, еще не придуманных способов совершения преступлений и отрабатывать их на теоретических моделях, чтобы вводить их в действие сразу же после появления первых такого рода посягательств.

Библиографический список / References

Antonovich, P.I. (2011) O sovremennom ponimanii termina “kibervoina” [About modern concept of “cyberwar” term]. *Vestnik Akademii voennych nauk.* 2 (35), 89–96. (in Russian).
Антонович П.И. О современном понимании термина «кибервойна» // Вестник Академии военных наук. 2011. № 2(35). С. 89–96.

[33] См.: Autonomous Shuttle Will Take Passengers to Airport. iHLS. January 18, 2018, available at: https://i-hls.com/archives/80857 (Accessed 13 October 2019).

Brenner, S. (2007) "At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare. *The Journal of Criminal Law and Criminology*. 97(2), 379–386.

Charvat, J. (2018) Cyber Terrorism: A New Dimension in Battlespace. 5th October, available at: https://ccdcoe.org/uploads/2018/10/05_CHARVAT_Cyber-Terrorism.pdf (Accessed 14 November 2019).

Falliere, N., Murchu, L. O., Chien, E. (2011) W32.Stuxnet Dossier. Version 1.4 (February), 1, available at: https://www.wired.com/images_blogs/threatlevel/2011/02/Symantec-Stuxnet-Update-Feb-2011.pdf (Accessed 11 November 2019).

Giraldi, P. (2019) Revisiting Stuxnet: The Israeli-American Computer Virus that Started Cyber-Warfare. *Global Research*. September 9, available at: https://www.globalresearch.ca/stuxnet-israeli-american-computer-virus-cyber-warfare/5688506 (Accessed 14 November 2019).

Glancy, D.J. (2014) Sharing the Road: Smart Transportation Infrastructure. *Fordham Urban Law Journal*. 41 (5), 1617–1664.

Glebov, I.N. (2018) Mezhdunarodnoe gumanitarnoe pravo i kibervoina [International humanitarian law and cyberwar]. *Rossiskoe gosudarstvovedenie*. 2, 137–153. (in Russian).
Глебов И.Н. Международное гуманитарное право и кибервойна // Российское государствоведение. 2018. № 2. С 137–153.

Glebov, I.N. (2018) Pravovoe regulirovanie avtonomnych robotizirovannych sredstv vedenia voiny [Legal regulation of autonomous robot war tools]. *Rossiskoe gosudarstvovedenie*. 3, 104–116. (in Russian).
Глебов И.Н. Правовое регулирование автономных роботизированных средств ведения войны // Российское государствоведение. 2018. № 3. С. 104–116.

Hathaway, O.A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., Spiegel, J. (2012) The Law of Cyber-Attack. *California Law Review*. 100 (4), 817–886.

Kushner, D. (2013) The Real Story of Stuxnet. *IEEE Spectrum*. February 26, available at: https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (Accessed 11 November 2019).

Langner, R. (2013) *To Kill a Centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achive*. The Langner Group. November, available at: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf (Accessed 11 November 2019).

Lee, C. (2017) Grabbing the Wheel Early: Moving Forward on Cybersecurity and Privacy Protections for Driverless Cars. *Federal Communications Law Journal*. 69(1), 25–52.

Ovcharov, A.V., Kozlov, A.V. (2019) The use of lethal Autonomous systems weapons require criminal law regulations. *Voennoe pravo [Military Law]*. 5(57), 179–187. (in Russian).
Овчаров А.В., Козлов А.В. Применение смертоносных автономных систем вооружения требует уголовно-правовой регламентации // Военное право. 2019. № 5(57). С. 179–187.

Ovchinskii, V.S. (2017) *Osnovy bor'by s kiberprestupnost'yu i kiberterrorizmom: khrestomatiya [Fundamentals of the fight against cybercrime and cyber terrorism: a reader]*. Compiled by. V.S. Ovchinsky. Moscow, Norma Publ. (in Russian).
Основы борьбы с киберпреступностью и кибертерроризмом: хрестоматия. Сост. В.С. Овчинский. М.: Норма, 2017. 528 с.

Sheremet, I.B., Rudianov, N.A., Ryabov, A.V., Khruschev, V.S., (2016) About need of the concepts development of construction and application of military autonomous robotic systems. *Extreme Robotics*. 1(1), 35–39. (in Russian).
Шеремет И.Б., Рудианов Н.А., Рябов А.В., Хрущев В.С. О необходимости разработки концепции построения и применения робототехнических комплексов военного назначения // Extreme Robotics. 2016. Т. 1. № 1. С. 35–39.

Shinkaretskaya, G.G. (2013) Mezhdunarodno-pravovye problemy vrazhdebnogo vozdeistvia na informacionnye sistemy [International law problems of enemy influence on information systems]. *Gosudarstvo i pravo [State and Law]*. 9, 82–88. (in Russian).
Шинкарецкая Г.Г. Международно-правовые проблемы враждебного воздействия на информационные системы // Государство и право. 2013. № 9. С. 82–88.
Spencer, D. (2018) The Road to the Future: A Regulatory Regime for the Rise of the Robot Cars. *William & Mary Environmental Law and Policy Review*. 42 (2), 647–671.
Wing, C. (2016) Better Keep Your Hands on the Wheel in That Autonomous Car: Examining Society's Need to Navigate the Cybersecurity Roadblocks for Intelligent Vehicles. *Hofstra Law Review*. 45 (2), 707–742.

Об авторах:

Клебанов Лев Романович — доктор юридических наук, доцент, профессор кафедры уголовного права, уголовного процесса и криминалистики, Юридический институт, Российский университет дружбы народов
ORCID ID: 0000-0002-1452-9568; SPIN-код: 8500-609
e-mail: solomon70@bk.ru

Полубинская Светлана Вениаминовна — кандидат юридических наук, доцент, ведущий научный сотрудник сектора уголовного права, уголовного процесса и криминологии, Институт государства и права Российской академии наук (ИГП РАН)
ORCID ID: 0000-0002-2469-2502; SPIN-код: 2485-5545
e-mail: svepol@yandex.ru

About the authors:

Lev R. Klebanov — Doctor of Legal Sciences, Associate Professor, Professor of the Department of Criminal Law, Criminal Procedure and Criminalistics, Law Institute, Peoples' Friendship University of Russia
ORCID ID: 0000-0002-1452-9568; SPIN-код: 8500-609
e-mail: solomon70@bk.ru

Svetlana V. Polubinskaya — Candidate of Legal Sciences, Associate Professor, Leading Researcher in the Criminal Law, Criminal Procedure and Criminology Sector, Institute of State and Law of Russian Academy of Sciences
ORCID ID: 0000-0002-2469-2502; SPIN-код: 2485-5545
e-mail: svepol@yandex.ru