
ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ОТДЕЛЬНЫМ ВИДАМ ПРЕСТУПЛЕНИЙ

PROBLEMS OF COUNTERACTING SPECIFIC TYPES OF CRIME

УДК 343.346

DOI 10.17150/2500-4255.2021.15(1).55-67

ПОСЯГАТЕЛЬСТВА НА ИНФОРМАЦИОННУЮ СИСТЕМУ БЕСПИЛОТНИКА В ЭТИОЛОГИИ ДОРОЖНО-ТРАНСПОРТНЫХ ПРОИСШЕСТВИЙ

А.И. Чучаев, Ю.В. Грачева, С.В. Маликов

*Московский государственный юридический университет им. О.Е. Кутафина (МГЮА), г. Москва,
Российская Федерация*

Информация о статье

Дата поступления

2 июля 2020 г.

Дата принятия в печать

19 февраля 2021 г.

Дата онлайн-размещения

9 марта 2021 г.

Ключевые слова

Информация; информационная система; беспилотное транспортное средство; уязвимости информационной системы; угрозы безопасности; компьютерные преступления; транспортные преступления

Финансирование

Статья подготовлена при финансовой поддержке РФФИ в рамках научных проектов № 18-29-16162 и № 18-29-16158

Аннотация. В высокоавтономные транспортные средства (ВАТС) интегрируется множество технологий, позволяющих производить безопасную и эффективную транспортировку без участия водителя. Механизмы соединения осуществляют связь между транспортными средствами и инфраструктурой, обмен данными, такими как положение транспортного средства, скорость его движения и т.д. Каждая из этих функций предназначена для поддержки последующей автоматизации, которая переводит водителя из участника дорожного движения в наблюдателя-контролера, делегируя функции, ранее выполнявшиеся людьми, технологиям. Автоматизация управления достигается за счет непрерывного анализа окружающей среды сенсорами и использования заранее определенной информации, например карт, сведений о покрытии, для планирования деятельности транспортного средства. В ВАТС применяются многофункциональные программно-аппаратные комплексы, включающие датчики: лидары, радары, камеры, GPS, одометры, гиросистемы и пр.; системы обмена данными с дорожной инфраструктурой, работающие по GPRS, 5G, Wi-Fi и другим стандартам; программное обеспечение, управляющее системами транспорта, в числе которых системы машинного зрения, нейросети анализа ситуации на дороге. В статье приводится классификация угроз безопасности ВАТС, рассматриваются риски реализации угроз в отношении компрометации датчиков, механизмов управления и подключения, а также уязвимости в используемых технологиях. Авторами предлагается формулировка ряда новых статей в гл. 27 УК РФ, посвященных ВАТС, на основе учета: лиц, участвующих в разработке соответствующего программного обеспечения и правил эксплуатации, эксплуатантов; деяний, которые способны причинить вред; комплекса общественно опасных последствий. Развернуто характеризуются четыре группы субъектов (нарушителей) посягательств на информационную систему ВАТС: лица, использующие уязвимость информационной системы; авторы вредоносных программ; субъекты создания информационных систем; субъекты эксплуатации информационных систем. Выделение таких групп должно быть учтено при выработке соответствующих норм в рамках гл. 27 УК РФ, конструировании квалифицированных составов преступлений и индивидуализации наказания.

ATTACKS ON THE INFORMATION SYSTEM OF UNMANNED VEHICLES IN THE ETIOLOGY OF ROAD ACCIDENTS

Alexandr I. Chuchaev, Yulia V. Gracheva, Sergey V. Malikov

Kutafin Moscow State Law University (MSAL), Moscow, the Russian Federation

Article info

Received

2020 July 2

Accepted

2021 February 19

Available online

2021 March 9

Abstract. Highly automated vehicles (HAVs) integrate numerous technologies that provide safe and efficient transportation without a driver. Connecting mechanisms ensure communication between vehicles and their infrastructure, and the exchange of data, such as the positioning of the vehicle, its speed, etc. The purpose of each of these functions is to support further automation, which turns a driver from a road user into an observer-controller by transferring to technologies those functions that were earlier performed by people. The automation of control

Keywords

Information; information system; driverless vehicle; information system's vulnerabilities; security threats; computer crimes; transport crimes

Acknowledgements

The reported study was funded by the RFBR within research projects № 18-29-16162 and № 18-29-16158

is achieved through a constant analysis of the environment by sensors and the use of previously obtained information, such as maps or data on the road covering, for planning the performance of the vehicle. HAVs use multi-functional hardware and software units that include sensors: lidars, radars, cameras, GPS, odometers, hydro-systems, etc.; systems of data exchange with the road infrastructure using GPRS, 5G, Wi-Fi and other standards; software that controls transport systems, including the systems of machine vision, and neural networks for controlling the road situation. The authors present a classification of threats to HAVs' security and analyze risks connected with the threats of compromising sensors, control and connection mechanisms, as well as the vulnerabilities of the used technologies. They suggest the wording of a number of new articles in Chapter 27 of the Criminal Code of the Russian Federation devoted to HAVs, which incorporate the following: persons who participated in the development of the corresponding software and guidelines for using the vehicle, operators; actions that could inflict damage, a complex of publicly dangerous consequences. A detailed description of four groups of subjects (violators) of infringements on the information system of HAVs is presented: persons using the vulnerability of an information system; malware creators; creators of information systems; operators of information systems. These groups should be taken into account when developing the corresponding norms within Chapter 27 of the Criminal Code of the Russian Federation, the features of aggravating circumstances and the individualization of punishment.

Постановка проблемы

Будущее автономных автомобилей в России зависит от ряда факторов, среди которых соответствующее состояние дорожной сети, ее адаптация к умным автомобилям. Если для таких транспортных средств не подготовить дороги, то спроса на них не будет [1]. В Стратегии развития автомобильной промышленности Российской Федерации на период до 2025 года, утвержденной распоряжением Правительства РФ от 28 апреля 2018 г. № 831-р¹, подчеркивается, что «особую значимость для успешного развития беспилотного (автономного) транспорта приобретет усовершенствование существующей и создание новой дорожной и информационно-телекоммуникационной инфраструктуры, обеспечивающих беспилотные (автономные, самоуправляемые) транспортные средства необходимыми сервисами и информацией».

Для описания различных форм автоматизации наземного транспорта в настоящее время применяются разнообразные термины². В Российской Федерации употребляется понятие «высокоавтоматизированное транспортное

средство», под которым понимается транспортное средство, в конструкцию которого внесены изменения, связанные с его оснащением автоматизированной системой вождения. В свою очередь, автоматизированная система вождения рассматривается как программно-аппаратные средства, осуществляющие управление транспортным средством без физического воздействия со стороны водителя, с возможностью автоматического отключения при воздействии водителя на органы управления для перехода в режим ручного управления при необходимости, в том числе для предотвращения дорожно-транспортного происшествия³.

В высокоавтоматизированные транспортные средства (BATC) интегрируется множество технологий, позволяющих производить безопасную и эффективную транспортировку без участия водителя [2–7]. Механизмы соединения осуществляют связь между транспортными средствами и инфраструктурой, обмен данными, такими как положение транспортного средства, скорость его движения и т.д. Каждая из этих функций предназначена для поддержки

¹ Собрание законодательства РФ. 2018. № 19. Ст. 2804.

² Автономный (autonomous) автомобиль; высокоавтоматизированное транспортное средство (highly automated vehicle); беспилотный автомобиль (driverless car); беспилотное транспортное средство (unmanned vehicle); полностью автоматизированное транспортное средство (fully automated vehicle); роботизированный автомобиль (robotic car); самоуправляемое транспортное средство (self-driving vehicle).

³ О проведении эксперимента по опытной эксплуатации на автомобильных дорогах общего пользования высокоавтоматизированных транспортных средств (вместе с «Положением о проведении эксперимента по опытной эксплуатации на автомобильных дорогах общего пользования высокоавтоматизированных транспортных средств») : постановление Правительства РФ от 26 нояб. 2018 г. № 1415 : (в ред. от 22 февр. 2020 г.) // Собрание законодательства РФ. 2018. № 49, ч. 2. Ст. 7619 ; 2020. № 9. Ст. 1200.

последующей автоматизации, которая переводит водителя из участника дорожного движения в наблюдателя-контролера, делегируя функции, ранее выполнявшиеся людьми, технологиям. Автоматизация управления достигается за счет непрерывного анализа окружающей среды сенсорами и использования заранее определенной информации, например карт, сведений о покрытии и т.д. В ВАТС применяются многофункциональные программно-аппаратные комплексы, включающие датчики: лидары, радары, камеры, GPS, одометры, гиросистемы и пр.; системы обмена данными с дорожной инфраструктурой, работающие по GPRS, 5G, Wi-Fi и другим стандартам; программное обеспечение, управляющее системами транспорта, в числе которых системы машинного зрения, нейросети анализа ситуации на дороге. Глубокая автоматизация создает и усиливает риски безопасности дорожного движения в силу появления новых векторов атак на транспортные системы и инфраструктуры, связанные с наличием уязвимостей программного обеспечения и каналов связи.

Классификация угроз информационной системе «высокоавтоматизированное транспортное средство — дорожная инфраструктура» (ИС «ВАТС — ДИ»)

В информационной отрасли под информационной безопасностью предлагается понимать стабильное состояние защищенности информации, ее носителей и инфраструктуры (компьютеры, сети, телекоммуникационное оборудование, помещения, системы жизнеобеспечения, персонал). Другое базовое понятие информационной безопасности — угроза безопасности — определяется как воздействие, которое прямо или косвенно может нанести ей ущерб. Ущербом безопасности, или реализацией угрозы безопасности, называют нарушение состояния защищенности информации, содержащейся и обрабатываемой в системе⁴.

Угрозы информационной безопасности, в частности, классифицируются:

- по видам возможных источников угроз;
- типу подсистем, на которые направлена атака;
- используемой уязвимости;
- объекту воздействия;

- способу реализации угрозы безопасности;
- видам несанкционированного доступа.

По *видам возможных источников угроз* выделяются:

– угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к ИС «ВАТС — ДИ», включая пользователей, реализующих угрозы непосредственно в контуре ВАТС (так называемый внутренний нарушитель);

– угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к ИС «ВАТС — ДИ», реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена (так называемый внешний нарушитель).

Кроме того, угрозы могут возникать в результате внедрения аппаратных закладок и вредоносных программ.

По *типу подсистем ИС «ВАТС — ДИ»*, на которые направлены угрозы безопасности, выделяются:

– угрозы безопасности информации, обрабатываемой в локальном контуре ВАТС;

– угрозы безопасности информации, обрабатываемой в контуре ВАТС — управляющие устройства без использования сети связи общего пользования;

– угрозы безопасности информации, обрабатываемой в контуре ВАТС — управляющие устройства с подключением к сети общего пользования (к сетям международного информационного обмена);

– угрозы безопасности информации, обрабатываемой в контуре ИС «ВАТС — ДИ» без подключения к сетям международного информационного обмена;

– угрозы безопасности информации, обрабатываемой в ДИ на базе распределенных информационных систем без подключения к сети общего пользования (к сетям международного информационного обмена);

– угрозы безопасности информации, обрабатываемой в ДИ на базе распределенных информационных систем с подключением к сети общего пользования (к сетям международного информационного обмена).

По *используемой уязвимости* выделяются угрозы, реализуемые исходя из уязвимостей системного ПО, прикладного ПО, протоколов сетевого взаимодействия и каналов передачи данных, технических каналов компрометации

⁴ Методика моделирования угроз безопасности информации : проект 2020 г. URL: <https://fstec.ru/component/attachments/download/2727>.

информации⁵, средств защиты информации, а также уязвимостей, вызванных наличием в аппаратных устройствах аппаратной закладки и недостатками организации технической защиты информации.

По объекту воздействия выделяются угрозы:

- безопасности информации, обрабатываемой в управляющей системе ВАТС;
- безопасности информации, обрабатываемой в выделенных средствах сбора (датчики) и обработки информации (лидары, радары и пр.);
- безопасности информации, передаваемой по сетям связи, в том числе беспроводным;
- прикладным программам, с помощью которых обрабатываются данные;
- системному ПО, обеспечивающему функционирование ВАТС;
- безопасности информации, обрабатываемой в ДИ;
- прикладным программам, с помощью которых обрабатываются данные в ДИ;
- системному ПО, обеспечивающему функционирование ДИ.

По способам реализации выделяются угрозы:

- связанные с компрометацией информации (в том числе угрозы внедрения вредоносных программ);

– утечки данных по техническим каналам.

Несанкционированный доступ можно разделить на три подвиды:

- проникновение в операционную систему субъекта информационной системы «ВАТС — ДИ»;
- создание нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренного изменения служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п.;
- внедрение вредоносных программ (программно-математического воздействия).

Обобщенно источники угроз безопасности ВАТС приведены на рисунке.

⁵ В системах информационной защиты под компрометацией понимается событие, связанное с получением кем-либо несанкционированного доступа к защищенным данным, утерей носителя закрытого ключа шифрования, несанкционированным копированием и др.

Посагательства на уязвимости транспортных средств высокой автономности⁶

Как указывалось, транспортные средства с высокой степенью автоматизации отличаются от неавтоматизированных как с точки зрения программного обеспечения, так и с технической стороны. Для того чтобы движение такого типа транспортных средств было возможно в автоматизированном режиме, разработчики и производители устанавливают на них дополнительное оборудование, как правило включающее в себя камеры, радары⁷, лидары⁸, инерциальный блок⁹, систему высокоточной навигации¹⁰.

Уязвимости ВАТС главным образом группируются по типу атакуемых устройств [8; 9]. Так, многие современные камеры, в том числе при-

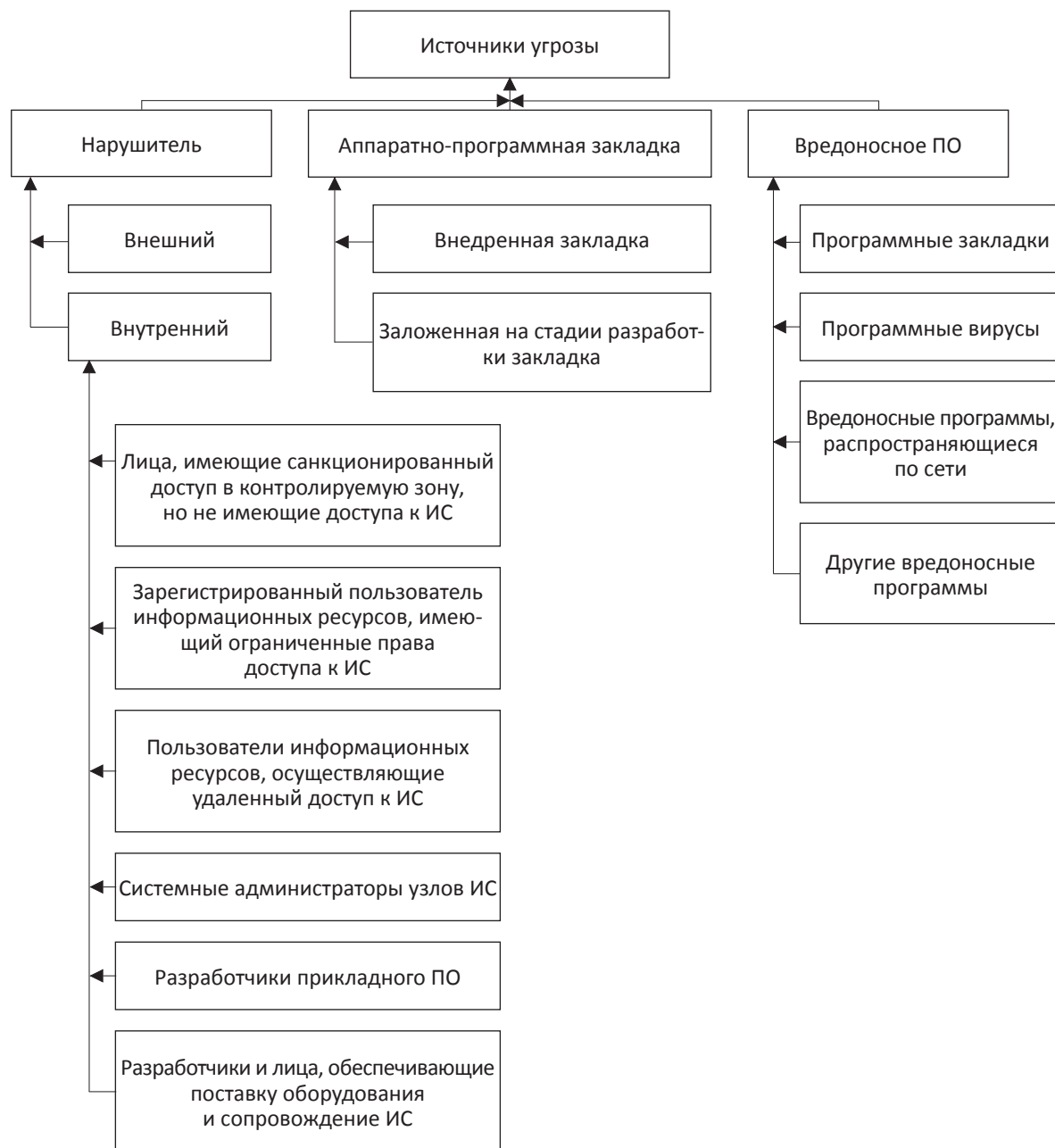
⁶ Данные об уязвимостях ВАТС получены на основе контент-анализа открытых источников: Cyber threat intelligence. URL: <https://www.surfwatchlabs.com/threat-categories>; Tesla Model S и Model 3 уязвимы к GPS-спуфингу. URL: https://www.securitylab.ru/news/499537.php?fbclid=IwAR2s0QSDdKxbuVrYrCPWDQKS_2SP0NoH6bVzO9Tb2WS_9vAd8a-eLQJJK6Q; McKinsey: переосмыслим софт и архитектуру электроники в automotive. URL: https://m.habr.com/ru/company/itelma/blog/476824/?_ga=2.111013836.858919990.1588694261-883227591.1584961570; Взлом беспилотного транспорта: кто понесет ответственность (исследование RAND Corporation). URL: <https://m.habr.com/ru/company/itelma/blog/496776>; Police may have used Tesla's Autopilot feature to stop driver asleep at the wheel. URL: <https://www.theverge.com/2018/12/3/18124017/chp-tesla-autopilot-police-redwood-city-drunk-driver>; Tencent Keen Security Lab: Experimental Security Research of Tesla Autopilot. URL: <https://keenlab.tencent.com/en/2019/03/29/Tencent-Keen-Security-Lab-Experimental-Security-Research-of-Tesla-Autopilot>.

⁷ Радар (с англ. Radio Detection and Ranging) — устройство, предназначенное для радиообнаружения предметов и измерения дальности.

⁸ Лидар (с англ. Light Identification, Detection and Ranging) — технология получения и обработки информации дистанционного зондирования с помощью активных оптических систем (лазеров, светодиодов), использующих в том числе явления отражения света от поверхности Земли для проведения высокоточных измерений координат транспортного средства. Она активно применяется в качестве датчика положения в автономных транспортных средствах.

⁹ Инерциальная единица измерения (IMU) — электронное устройство, которое измеряет и сообщает определенную силу, угловую скорость, а иногда ориентацию тела на основе комбинации акселерометров, гироскопов и магнитометров.

¹⁰ Высокоточная навигация (GNSS) — глобальные навигационные спутниковые системы (Global Navigation Satellite System), применяемые для создания координатно-временного поля на поверхности Земли и в околоземном пространстве.



Классификация источников угроз информации в ИС «ВАТС — ДИ»

меняемые в ВАТС, содержат датчик, который может быть частично отключен с расстояния 3 м с помощью маломощного лазера, извлекаемого из обычного CD-плеера.

Другой вектор воздействия — атака на функцию автоматической коррекции экспозиции камеры, что может привести к ее неспособности распознать дорожный знак или пешехода. Так, беспилотный автомобиль производства Google оказался уязвим в ситуации, когда яркий солнечный свет ослепил камеры автомобиля. Те же проблемы у ВАТС производства компании Tesla:

на испытаниях ни автомобиль, ни водитель не опознали белый коммерческий трейлер на фоне ярко освещенного неба. Используя такие уязвимости, злоумышленники могут довольно легко совершить атаку, направив яркий свет на транспортное средство; источником такого света могут быть компактные мощные фонари. Стоит отметить, что даже интенсивный свет собственной системы освещения может отразиться в сторону транспортного средства. Не исключены вмешательства в ВАТС злоумышленника, использующего любую зеркальную поверхность.

Похожие проблемы свойственны *радарам* и *лидарам*. Специалистами по безопасности при тестировании уязвимостей выявлялась возможность наведения помех на лидары путем прямого излучения света на блок сканера, который имеет ту же частоту, что и используемый для сканирования лазер. Уровень помех был доведен до такого уровня, что ВАТС фактически было ослеплено. Кроме наведения помех и подавления работы датчика, специалистам с помощью недорогого оборудования — микрокомпьютера Raspberry Pi и маломощного лазера — удалось заставить блок управления автомобилем сделать вывод, что перед ним находится большой объект и заставить его остановиться. Атака подобного рода может ставить целью вызвать аварию в местах с повышенной транспортной активностью посредством инициирования резкой остановки автомобиля.

Значительное количество уязвимостей сосредоточено в *инерциальном блоке* ВАТС. Показания датчиков проверяются блоком управления для определения нахождения их в пределах допустимых значений. Компрометация любого датчика с целью имитации ложных, но реалистичных данных о характере движения транспортного средства может приводить к тому, что системы управления будут реагировать неадекватно фактической дорожной обстановке, становясь причиной причинения вреда. Такие атаки требуют доступа к датчику, чтобы изменить его показания или перехватить связь между датчиком и блоком управления, который может быть осуществлен по кабелю или с помощью беспроводного соединения. Знание диапазонов допустимых значений датчиков может быть использовано для их искажения. Это приведет к тому, что система не распознает нарушение и не переведет ВАТС в безопасный режим.

При тестировании уязвимостей одной из моделей ВАТС был проведен детальный анализ сетевых пакетов¹¹ и их модификация, т.е. реализована атака man-in-the-middle на коммуникационную сеть автомобиля (Controller Area Network, CAN). Это обеспечило возможность фальсифицировать показания спидометра при движении на большой скорости и исказило у водителя и механизмов управления представление о дорожной ситуации. В настоящее время фиксируются факты нарушения функцио-

нирования двигателя посредством удаленного проникновения в сеть CAN и атаки на двигатель с помощью эксплойтов¹², реализующих подмену пакетов.

Критическая значимость каждого датчика ВАТС может быть продемонстрирована на примере датчика контроля давления в шинах. Несмотря на то что он мал и выполняемая им функция примитивна по сравнению со сложностью всего транспортного средства, передаваемая им информация имеет существенное значение для безопасности движения. В связи с этим в США их наличие стало обязательным требованием для всех транспортных средств с 2007 г., а с 2012 г. — и в Европе. В частности, специалистами установлено, что сигналы таких датчиков могут быть перехвачены и модифицированы с помощью методов пакетного анализа с расстояния до 40 м. Разработка специального оборудования и программного обеспечения для выполнения этой атаки не составила затруднений. Атака на датчики давления в шинах приводит к тому, что водителю будет представлена неверная информация: имитация ложного изменения давления в шинах (резкое падение, имитирующее прокол), недостоверная информация о нормальном состоянии. Ложная информация о резком падении давления может вызывать у водителей или управляющей системы опасную для дорожного движения реакцию — совершить аномальный маневр или резкую остановку. Соккрытие действительного предупреждающего сообщения о давлении в шинах может привести к тому, что водитель упустит возможность довести транспортное средство до безопасной и контролируемой остановки, создаст аварийную ситуацию.

В ВАТС имеется целый ряд и *других ключевых компонентов*, штатное функционирование которых обеспечивает его безопасность: модуль управления навигацией (NCM); модуль управления двигателем (ECM); электронный модуль управления тормозом (EBCM); модуль управления трансмиссией (TCM); телематический модуль с дистанционным командованием; модуль управления телом (BCM); надувной

¹¹ В компьютерных сетях пакет — это определенным образом оформленный блок данных, передаваемый по сети в пакетном режиме.

¹² Компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему. Целью атаки может быть как захват контроля над системой (повышение привилегий), так и нарушение ее функционирования.

удерживающий модуль (IRM); система видения автомобиля (VVS); дистанционный приемник замка двери; отопление, вентиляция и кондиционирование воздуха (ОВКВ); модуль приборной панели; радиоразвлекательный центр.

Например, модуль управления навигацией (NCM) — один из важнейших в BATC, поскольку он получает информацию от датчиков, которые анализируют окружающую среду (GPS, камеры, инфракрасное излучение и т.д.), и затем выбирает подходящий навигационный план. Этот модуль имеет контроль над тем, как автомобиль будет перемещаться, и если он будет скомпрометирован, то транспортному средству может быть приказано двигаться в место, указанное злоумышленником.

Компрометация электронной системы контроля устойчивости (ESC) может повлиять на электронный модуль управления тормозом. Так, модификация пакетов данных от ЕСМ к ЕВСМ, содержащих информацию о скорости вращения колеса, заставила ЕВСМ применить тормоза, что привело к выполнению транспортным средством непредусмотренного опасного торможения.

Наличие *программного обеспечения* также становится серьезной уязвимостью BATC, заключающейся, с одной стороны, в возможности его перезаписи, с другой — в необходимости его постоянного обновления. Несмотря на то что последняя процедура относительно проста, проблема состоит в том, что для устранения всех недостатков (функциональных и безопасности BATC) требуется регулярное обновление программного обеспечения. Имеющиеся механизмы их выполнения посредством физического подключения к блоку управления неприменимы из-за необходимости обновлять огромное количество BATC. Проведение таких операций человеком требует внешнего контроля, а альтернативное использование удаленного, в том числе беспроводного, обновления создает риски компрометации посредством замены обновлений микропрограммного обеспечения в исходном коде вредоносным кодом.

Как и любая информационная система, BATC подвержено заражению вредоносными программами, например из-за несовершенства безопасности диагностических механизмов — незащищенные порты, а также встроенные в экосистему BATC веб-браузеры, медиаплееры. При этом после заражения очень трудно идентифицировать наличие вредоносного про-

граммного кода в большом объеме корректного кода модуля управления двигателем.

Одной из серьезных уязвимостей BATC является *использование широкого спектра коммуникационных технологий*. Соединение BATC с множеством различных коммуникационных механизмов (транспортного средства с транспортным средством (V2V), транспортного средства с инфраструктурой (V2I) и облачной коммуникацией) приведет к тому, что они будут доступны через общедоступную инфраструктуру, например Интернет, либо будут транслировать свои данные в публичное пространство. Как и прочие ИТ-инфраструктуры, BATC становится подверженным крупномасштабным автоматизированным вредоносным атакам.

Уголовно-правовое парирование угроз ИС «BATC — ДИ»

На сегодняшний день ни в одном государстве мира уголовная ответственность (равно как и административная) за дорожно-транспортные происшествия с участием беспилотных (полностью автономных) автотранспортных средств, как нам известно, не установлена.

В зарубежной доктрине сложилось множество теорий, основные положения которых по аналогии можно применить при рассмотрении ответственности за вред, причиненный при эксплуатации беспилотного автомобиля. Речь идет о теориях, раскрывающих особенности ответственности за вред, причиненный: при эксплуатации лифта; автопилотом корабля, самолета или поезда; водителем-человеком. Существуют идеи о применении аналогии с промышленными роботами либо о создании совершенно нового концепта правового регулирования, не принимающего во внимание сложившуюся доктрину и судебную практику [10–16].

С точки зрения отечественного уголовного законодательства, на первый взгляд может показаться, что ответственность за причинение вреда высокоавтоматизированным транспортным средством полностью охватывается нормами гл. 28 УК РФ, поскольку связана главным образом с воздействием на информационную систему BATC. Однако даже в данной главе имеются пробелы, которые не позволяют парировать угрозы, возникающие в связи с введением в эксплуатацию BATC.

Так, в отечественном уголовном законодательстве в части защиты компьютерной информации (гл. 28 УК РФ) не учитывается следующая

специфика информационной сферы, в том числе применимая к информационной системе ВАТС:

- информация об уязвимостях таких систем и программного обеспечения, которые дают возможность совершения преступления, распространяется свободно, в том числе самими их авторами;

- уязвимости создаются и выявляются непрерывно, запросы на обеспечение безопасности в информационной сфере, в том числе относительно юридических мер обеспечения такой безопасности, возникают постоянно, что требует перманентной актуализации законодательства;

- средства реализации преступления (специализированное программное обеспечение) может создавать человек, имеющий определенные навыки, в любой точке мира;

- не существует средств, которые заведомо предназначены для совершения преступного деяния, практически любое средство атаки может использоваться лишь как инструмент контроля защищенности;

- подключение к сетям общего пользования расширяет географию вовлеченных в преступную деятельность, а возможность удаленных атак усложняет установление субъекта, совершающего преступные деяния;

- распределение сфер ответственности осуществляется лишь в рамках одной информационной системы, нет общего подхода к распределению ответственности за создание условий для преступления.

Применительно к конкретным составам преступлений эта специфика проявляется в следующем:

1. По ст. 272 УК РФ: деяния по уничтожению, блокированию информации, влекущие причинение ущерба, могут осуществляться не только посредством неправомерного доступа к охраняемой законом компьютерной информации, но и посредством атак на отказ в обслуживании, не требующем доступа; деяние может привести к снижению скорости доступа к информации, т.е. информация не блокируется, не уничтожается, не модифицируется, что может привести к причинению ущерба (в ИС «ВАТС — ДИ» скорость обработки информации имеет существенное значение); само деяние может привести к снижению доверия к информационной системе и данным, при этом уничтожение, блокирование, модификация либо копирование не осуществлялись.

2. По ст. 273 УК РФ: любое средство выявления уязвимостей может быть использовано как

для атак, так и для контроля защищенности, т.е. фактически любое тестирующее систему безопасности программное обеспечение можно рассматривать как вредоносное, а его создание и распространение всегда можно трактовать как преступные.

3. По ст. 274 УК РФ: не закреплена ответственность автора правил эксплуатации, т.е. возникает вопрос о том, какую ответственность должен нести разработчик правил в случае, если они не нарушались, но недостаточность правил привела к причинению ущерба.

4. По ст. 274.1 УК РФ: информацию об уязвимостях, которую авторы программного обеспечения публикуют для уведомления пользователей, можно трактовать как заведомо предназначенную для неправомерного воздействия, так же как описание методики атаки, реализующей уязвимость, можно рассматривать в качестве инструмента выявления уязвимостей. Иными словами, термин «заведомо предназначенный» малоприменим в цифровой среде. Также следует отметить, что в критической информационной инфраструктуре может обрабатываться информация, ценность которой невысока, и вред, причиненный в результате нарушения правил эксплуатации, не будет существенным, т.е. нет градации вреда в зависимости от категории информации, что дает почву для неоднозначного трактования и назначения несоразмерного деянию наказания [17–28].

Следует учесть, что ИС «ВАТС — ДИ» не сводится лишь к информационной системе, она включает собственно транспортное средство и дорожную инфраструктуру. Размывание ответственности за причинение вреда беспилотником по нормам глав о компьютерных преступлениях, преступлениях против личности и собственности не позволяет установить специфику новых складывающихся общественных отношений — безопасности движения и эксплуатации ВАТС, не отражает его социальной сущности и направленности.

Важной задачей правового регулирования является четкое и последовательное установление зон ответственности лиц, действующих в системе «ВАТС — ДИ». Изложенное позволяет утверждать, что необходимо формулирование ряда новых статей в гл. 27 УК РФ [29; 30], посвященных ВАТС, на основе учета:

- лиц, участвующих в разработке соответствующего программного обеспечения и правил эксплуатации, а также их эксплуатантов;

- деяний, которые способны причинить вред;
- комплекса общественно опасных последствий [31].

В рамках информационной безопасности принято вести речь о типе нарушителей и модели угроз безопасности, что также должно быть положено в основу конструирования соответствующих составов преступлений. Применительно к «ВАТС — ДИ» можно говорить о четырех группах субъектов (нарушителей): лица, использующие уязвимость информационной системы; авторы вредоносных программ; субъекты процесса создания информационных систем; субъекты эксплуатации информационных систем. В конечном счете выделение таких групп должно быть учтено при выработке соответствующих норм в рамках гл. 27 УК РФ, конструировании квалифицированных составов преступлений и индивидуализации наказания.

Группа 1. Лица, непосредственно совершающие деяния, приводящие к нарушению безопасности систем и причинению ущерба. Обобщенно их криминологический портрет может быть представлен следующим образом:

- имеют корыстную заинтересованность (профессиональные преступники, работающие по заказу третьих лиц; субъекты, преследующие собственные интересы);
- действуют из хулиганских побуждений (цифровой вандализм — действия, ставящие разрушение информационных систем как цель; вредоносные действия, не ставящие целью нанесение вреда, но нарушающие права владельца системы).

Предметами их воздействия может выступать информация (ее хищение, блокирование, модификация, копирование); имущество (транспортное средство); вычислительные мощности информационной системы.

Общественная опасность деяний таких лиц, которую необходимо отразить в самостоятельной норме, состоит в доступе к информационной системе «ВАТС — ДИ», нарушившем конфиденциальность, целостность и доступность информации, а также приведшем к падению скорости ее обработки и снижению общего уровня доверия к системе, причинившим ущерб.

Группа 2. Авторы и распространители вредоносных программ. Разработчики таких программ играют значимую роль практически в каждом киберпреступлении: организация преступления без использования вредоносного программного обеспечения является сложной и трудоемкой задачей, а круг лиц, способных совершить деяние

без него, ограничен. Собственно, бесконтрольное распространение инструментов расширяет круг потенциальных преступников.

Общественная опасность деяний таких лиц, которую также необходимо отразить в самостоятельной норме, заключается в создании вредоносного программного обеспечения, нарушившего конфиденциальность, целостность и доступность информации, что привело к падению скорости ее обработки и к снижению общего уровня доверия к системе, причинивших ущерб ИС «ВАТС — ДИ».

Группа 3. Субъекты создания информационных систем. Деятельность именно этих лиц, их подход к организации процесса производства, к определению функции программного обеспечения (служит ли он целям обеспечения безопасности или нет), выделение ресурсов на выявление и ликвидацию уязвимостей информационных систем во многом определяют преступную среду киберпространства. При определении ответственности создателей ПО за ущерб, нанесенный в результате киберпреступления, следует учитывать их классы и характеристики:

- по принятию рекомендованных и обязательных стандартов в обеспечении безопасности приложений и систем;
- по наличию процессов аудита безопасности, интегрированных в производственный процесс;
- по эффективности мер, реализованных в продукции;
- по организации процесса выявления уязвимостей;
- по организации процесса ликвидации уязвимостей и донесения до пользователей продукции результатов (обновлений программного обеспечения);
- по реакции на выявление уязвимостей: отреагировал ли производитель на информацию о недостатках, приводящих к нарушению безопасности;
- по поддержанию уровня информированности пользователей о выявленных уязвимостях и регулярности процесса донесения этой информации.

В целом криминологически можно выделить три группы разработчиков программного обеспечения:

- профессиональные преступники, разрабатывающие программы, изначально предназначенные для совершения преступлений;
- исследователи-разработчики, ставящие целью выявление уязвимостей информацион-

ных систем для передачи информации производителям и владельцам уязвимых инфраструктур;
– распространители вредоносных программ.

Общественная опасность деяний таких лиц состоит в разработке программного обеспечения и (или) правил эксплуатации информационной системы «ВАТС — ДИ», т.е. в создании условий для противоправного посягательства на нее, повлекшего причинение ущерба. Данная угроза не охватывается уголовным законодательством, в связи с чем УК РФ требуется дополнить соответствующей уголовно-правовой нормой.

Группа 4. Субъекты процесса эксплуатации информационных систем. При разработке средств и методов защиты от киберугроз обеспечение безопасности — это непрерывный процесс выявления и анализа уязвимостей. Одной из важнейших проблем становится применение средств их ликвидации владельцами систем, эксплуатирующими службами. Производитель программного обеспечения передает права на его использование владельцу, поэтому он не всегда в состоянии применить изменения к разработанному ПО, его зона влияния ограничена. Пренебрежение по отношению к наличию выявленных уязвимостей и бездействие эксплуатирующих служб актуализируют уязвимость, способствуют реализации атаки на информационную систему и наносят ущерб.

Ответственность должна определяться исходя из роли субъекта в процессе эксплуатации и зоны его ответственности:

– *формирование архитектурного решения*, т.е. оценка безопасности архитектуры ИС, проведение анализа угроз, выработка мер, соответствующих актуальным угрозам безопасности;

– *формирование регламентов*. В законодательстве предусмотрена ответственность за нарушение регламентов и инструкций, однако за разработку требований, описывающих недостаточные меры безопасности, ответственность не закреплена. В частности, не регламентирована ответственность служб и организаций, дающих предписание о необходимости принятия

неэффективных мер безопасности, приводящих к тому, что будут задействованы неадекватные средства защиты информации;

– *ликвидация уязвимостей* на уровне операционной системы и программного обеспечения, т.е. осуществление доступных обновлений, мониторинг источников, сообщающих об уязвимостях системы;

– *кадровое обеспечение* процессов безопасности. Если владелец информационной системы принимает решение не включать в коллектив специалистов в сфере информационной безопасности, то он должен нести всю полноту ответственности;

– *обучение персонала*. Должна быть установлена ответственность за причинение вреда, наступившего от действий лиц, не прошедших соответствующую подготовку (инструктаж);

– *материальное обеспечение*, т.е. внедрение средств защиты информации как необходимого компонента каждой информационной системы. Сознательный отказ от применения средств защиты информации порождает риски и влечет причинение ущерба;

– *исполнение регламентов*, т.е. добросовестное исполнение регламентов и недопущение нарушения правил эксплуатации некоторых типов информационных систем должны быть отражены в действующем законодательстве.

Отметим также, что для создания эффективной системы уголовно-правовой охраны эксплуатации беспилотных транспортных средств необходима дифференциация ответственности в зависимости от причиненного ущерба (вреда). При этом в рамках крупного ущерба следует оценивать: стоимость восстановления инфраструктуры; стоимость похищенных данных как актива на основе его рыночной стоимости; упущенную выгоду (простой транспортных средств); стоимость утраченного свойства инфраструктуры на основе рыночной стоимости услуг по обеспечению доступности, конфиденциальности ИС; стоимость вычислительных мощностей на основе их рыночной стоимости и размера полученной выгоды.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Шадрин Т. Без руля, но с головой / Т. Шадрин // Российская газета. — 2018. — 22 мая.
2. Hamida E. Security of Cooperative Intelligent Transport Systems: Standards, Threats Analysis and Cryptographic Countermeasures / E. Hamida, H. Noura, W. Znaidi // Electronics. — 2015. — № 4. — P. 380–423.
3. Communication Architecture for Cooperative Systems in Europe / I. Kosch, M. Kulp, M. Bechler [et al.] // IEEE Communications Magazine. — 2009. — Vol. 47, № 5. — P. 116–125.
4. Телематика на автомобильном транспорте / В.М. Власов, С.В. Жанказиев, А.Б. Николаев, В.М. Приходько. — Москва : Изд-во Моск. гос. автомобил.-дорож. ин-та, 2003. — 173 с.

5. Оптимизация организации движения на основе имитационного моделирования / В.А. Голенков, А.Н. Новиков, А.А. Катунин [и др.] // Наука и техника в дорожной отрасли. — 2015. — № 3 (73). — С. 5–7.
6. Жанказиев С.В. Интеллектуальные транспортные системы : учеб. пособие / С.В. Жанказиев. — Москва : Изд-во Моск. гос. автомобил.-дорож. ин-та, 2016. — 120 с.
7. Халилев Р.Ф. Проектирование интеллектуальных транспортных систем / Р.Ф. Халилев // Международный научно-исследовательский журнал. — 2013. — № 7-2 (14). — С. 98–100.
8. Jouini M. Threat Classification: State of art / M. Jouini, Latifa Ben Arfa Rabai. — URL: https://www.researchgate.net/publication/313241139_Threat_classification_State_of_art.
9. Kornwitz J. The Cybersecurity Risk of Self-Driving Cars / J. Kornwitz // Phys.org. — 2017. — 16 Febr. — URL: <https://phys.org/news/2017-02-cybersecurity-self-driving-cars.html>.
10. Чурилов А.Ю. Ответственность за вред, причиненный при эксплуатации автономного (беспилотного) автомобиля / А.Ю. Чурилов // Интеллектуальные права: вызовы 21-го века : материалы междунар. конф. (14–16 нояб. 2019 г.) / под ред. Э.П. Гаврилова, С.В. Бутенко. — Томск : Изд. дом ТГУ, 2019. — С. 127–132.
11. Незнамов А.В. Новые законы робототехники. Регуляторный ландшафт. Мировой опыт регулирования робототехники и технологий искусственного интеллекта / А.В. Незнамов, А.Д. Волюнец, В.В. Бакуменко. — Москва : Инфотропик, 2018. — 220 с.
12. Робот и человек: новое партнерство? / Ю.А. Тихомиров, Н.Б. Крысенкова, С.Б. Нанба, Ж.А. Маргушева // Журнал зарубежного законодательства и сравнительного правоведения. — 2018. — № 5 (72). — С. 5–10.
13. Vellinga N.E. From the Testing to the Deployment of Self-Driving Cars: Legal Challenges to Policymakers on the Road ahead / N.E. Vellinga // Computer Law and Security Review. — 2017. — № 33 (6). — P. 847–863.
14. Robot Ethics: The Ethical and Social Implications of Robotics / ed. P. Lin, K. Abney, G.A. Bekey. — Cambridge : MIT Press, 2012. — 108 p.
15. Lemann A.B. Autonomous Vehicles, Technological Progress, and the Scope Problem in Products Liability / A.B. Lemann // Journal of Tort Law. — 2019. — Vol. 12, № 2. — P. 157–212.
16. Ljungholm D.P. The Safety and Reliability of Networked Autonomous Vehicles: Ethical Dilemmas, Liability Litigation Concerns, and Regulatory Issues / D.P. Ljungholm // Contemporary Readings in Law and Social Justice. — 2019. — Vol. 11, № 2. — P. 9–14.
17. Русскевич Е.А. Уголовное право и «цифровая преступность»: проблемы и решения / Е.А. Русскевич. — Москва : Инфра-М, 2019. — 227 с.
18. Козаев Н.Ш. Противодействие злоупотреблениям современными технологиями: международно-правовые и уголовно-правовые аспекты / Н.Ш. Козаев. — Москва : Юрлитинформ, 2016. — 192 с.
19. Дремлюга Р.И. Компьютерная информация как предмет посягательства при неправомерном доступе: сравнительный анализ законодательства США и России / Р.И. Дремлюга // Журнал зарубежного законодательства и сравнительного правоведения. — 2018. — № 6 (73). — С. 129–133.
20. Юрченко И.А. Уголовно-правовой запрет Ddos-атак / И.А. Юрченко // Уголовное право: стратегия развития в XXI в. : материалы 12-й междунар. науч.-практ. конф., Москва, 29–30 янв. 2015 г. — Москва, 2015. — С. 413–416.
21. Талан М.В. Компьютерные преступления и преступления в сфере компьютерной информации / М.В. Талан // Уголовное право: стратегия развития в XXI в. : материалы 7-й междунар. науч.-практ. конф. — Москва, 2010. — С. 431–434.
22. Третьяк М.И. Модификация компьютерной информации и ее соотношение с другими способами компьютерного мошенничества / М.И. Третьяк // Уголовное право. — 2016. — № 2. — С. 95–101.
23. Омаров М.Д. Проблемы определения состава преступления за неправомерный доступ к информационным ресурсам информационных систем / М.Д. Омаров // Юридический вестник ДГУ. — 2011. — № 4. — С. 56–58.
24. Ефремова М.А. Ответственность за неправомерный доступ к компьютерной информации по действующему уголовному законодательству / М.А. Ефремова // Вестник Казанского юридического института МВД России. — 2012. — № 8. — С. 54–56.
25. Панфилова Е.И. Компьютерные преступления / Е.И. Панфилова, А.Н. Попов. — Санкт-Петербург : Изд-во С.-Петерб. юрид. ин-та Генер. прокуратуры РФ, 2003. — 48 с.
26. Stoddart K. UK Cyber Security and Critical National Infrastructure Protection / K. Stoddart // International Affairs. — 2016. — Vol. 92, iss. 5. — P. 1079–1105.
27. Carr M. Public-Private Partnerships in National Cyber-Security Strategies / M. Carr // International Affairs. — 2016. — Vol. 92, iss. 1. — P. 43–62.
28. Henriksen A. The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace / A. Henriksen // Journal of Cybersecurity. — 2019. — Vol. 5, iss. 1. — P. 1–9.
29. Коробеев А.И. Беспилотные транспортные средства: новые вызовы общественной безопасности / А.И. Коробеев, А.И. Чучаев // Lex Russica. — 2019. — № 2 (147). — С. 9–28.
30. Чучаев А.И. Ответственность за причинение ущерба высокоавтоматизированным транспортным средством: состояние и перспективы / А.И. Чучаев, С.В. Маликов // Актуальные проблемы российского права. — 2019. — № 6 (103). — С. 117–124.
31. A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding how they Propagate / I. Agrafiotis, J. Nurse, M. Goldsmith [et al.]. — DOI: 10.1093/cybsec/tyy006 // Journal of Cybersecurity. — 2018. — Vol. 4, iss. 1.

REFERENCES

1. Shadrina T. Without a wheel, but with brains. *Rossiiskaya Gazeta*, 2018, May 22.
2. Hamida E., Noura H., Znaidi W. Security of Cooperative Intelligent Transport Systems: Standards, Threats Analysis and Cryptographic Countermeasures. *Electronics*, 2015, no. 4, pp. 380–423.

3. Kosch I., Kulp M., Bechler M., Strassberger B., Weyl R., Lasowski B. Communication Architecture for Cooperative Systems in Europe. *IEEE Communications Magazine*, 2009, vol. 47, no. 5, pp. 116–125.
4. Vlasov V.M., Zhankaziev S.V., Nikolaev A.B., Prikhodko V.M. *Telematika na avtomobil'nom transporte* [Telematics in Road Transport]. Moscow Automobile and Road Construction State Technical University Publ., 2003. 173 p.
5. Golenkov V.A., Novikov A.N., Katunin A.A., Baranov Yu.N., Matnazarov D.D. Optimization of Traffic Management in the City of Orel by Traffic Flow simulation. *Nauka i tekhnika v dorozhnoi otrasli = Science and Engineering for Highways*, 2015, no. 3 (73), pp. 5–7. (In Russian).
6. Zhankaziev S.V. *Intellektual'nye transportnye sistemy* [Intelligent Transport Systems]. Moscow Automobile and Road Construction State Technical University Publ., 2016. 120 p.
7. Khalilev R.F. Design Intelligent Transport Systems. *Mezhdunarodnyi nauchno-issledovatel'skii zhurnal = International Research Journal*, 2013, no. 7-2 (14), pp. 98–100. (In Russian).
8. Jouini M., Latifa Ben Arfa Rabai. *Threat Classification: State of art*. Available at: https://www.researchgate.net/publication/313241139_Threat_classification_State_of_art.
9. Kornwitz J. The Cybersecurity Risk of Self-Driving Cars. *Phys.org*, 2017, February 16. Available at: <https://phys.org/news/2017-02-cybersecurity-self-driving-cars.html>.
10. Churilov A.Yu. Liability for damage inflicted by an automated (unmanned) automobile. In Gavrilov E.P., Butenko S.V. (eds.). *Intellektual'nye prava: vyzovy 21-go veka. Materialy Mezhdunarodnoi konferentsii, Tomsk, 14–16 noyabrya 2019 g.* [Intellectual Rights: Challenges of the 21st Century. Materials of the International Conference, Tomsk, November 14–16, 2019]. Tomsk, 2019, pp. 127–132. (In Russian).
11. Neznamov A.V., Volynets A.D., Bakumenko V.V. *Novye zakony robototekhniki. Regulyatornyi landschaft. Mirovoi opyt regulirovaniya robototekhniki i tekhnologii iskusstvennogo intellekta* [New Laws of Robotics. The Regulatory Landscape. The International Experience of Regulation of Robotics and Artificial Intelligence Technologies]. Moscow, Infotropik Publ., 2018. 220 p.
12. Tikhomirov Yu.A., Krysenkova N.B., Nanba S.B., Margusheva Zh.A. Robot and Human: A New Partnership? *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya = Journal of Foreign Legislation and Comparative Law*, 2018, no. 5 (72), pp. 5–10. (In Russian).
13. Vellinga N.E. From the Testing to the Deployment of Self-Driving Cars: Legal Challenges to Policymakers on the Road ahead. *Computer Law and Security Review*, 2017, no. 33 (6), pp. 847–863.
14. Lin P., Abney K., Bekey G.A. (eds.). *Robot Ethics: The Ethical and Social Implications of Robotics*. Cambridge, MIT Press, 2012. 108 p.
15. Lemann A.B. Autonomous Vehicles, Technological Progress, and the Scope Problem in Products Liability. *Journal of Tort Law*, 2019, vol. 12, no. 2, pp. 157–212.
16. Ljungholm D.P. The Safety and Reliability of Networked Autonomous Vehicles: Ethical Dilemmas, Liability Litigation Concerns, and Regulatory Issues. *Contemporary Readings in Law and Social Justice*, 2019, vol. 11, no. 2, pp. 9–14.
17. Russkevich E.A. *Ugolovnoe pravo i «tsifrovaya prestupnost'»: problemy i resheniya* [Criminal Law and Digital Crime: Problems and Solutions]. Moscow, Infra-M Publ., 2019. 227 p.
18. Kozaev N.Sh. *Protivodeistvie zloupotrebleniyam sovremennymi tekhnologiyami: mezhdunarodno-pravovye i ugolovno-pravovye aspekty* [Counteracting the Abuse of Modern Technologies: International Legal and Criminal Aspects]. Moscow, Yurilitinform Publ., 2016. 192 p.
19. Dremlyuga R.I. Computer Information as an Target for Illegal Access: Comparative Analysis of the USA and Russian Legislation. *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya = Journal of Foreign Legislation and Comparative Law*, 2018, no. 6 (73), pp. 129–133. (In Russian).
20. Yurchenko I.A. Criminal Law Prohibition of Ddos Attacks. *Ugolovnoe pravo: strategiya razvitiya v XXI v. Materialy 12-i mezhdunarodnoi nauchno-prakticheskoi konferentsii, Moskva, 29–30 yanvarya 2015 g.* [Criminal Law: Development Strategy in the XXI Century. Materials of the 12th International Scientific and Practical Conference, Moscow, January 29–30, 2015]. Moscow, 2015, pp. 413–416. (In Russian).
21. Talan M.V. Computer Crimes and Crimes in the Field of Computer Information. *Ugolovnoe pravo: strategiya razvitiya v XXI v. Materialy 7-i mezhdunarodnoi nauchno-prakticheskoi konferentsii, Moskva, 2010 g.* [Criminal Law: Development Strategy in the XXI Century. Materials of the 7th International Scientific and Practical Conference, Moscow, 2010]. Moscow, 2010, pp. 431–434. (In Russian).
22. Tretyak M.I. Modification of Computer Information and its Correlation with Other Types of Computer Fraud. *Ugolovnoe pravo = Criminal Law*, 2016, no. 2, pp. 95–101. (In Russian).
23. Omarov M.D. Problems of Definition of Structure of a Crime for Wrongful Access to Information Resources of Information Systems. *Yuridicheskii vestnik Dagestanskogo gosudarstvennogo universiteta = Law Herald of Dagestan State University*, 2011, no. 4, pp. 56–58. (In Russian).
24. Efremova M.A. Responsibility for Wrongful Access to Computer Information under the Current Criminal Legislation. *Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii = Bulletin of the Kazan Law Institute of MIA Russia*, 2012, no. 8, pp. 54–56. (In Russian).
25. Panfilova E.I., Popov A.N. *Komp'yuternye prestupleniya* [Computer Crimes]. Saint Petersburg, Law Institute of the Office of the Prosecutor General of the Russian Federation Publ., 2003. 48 p.
26. Stoddart K. UK Cyber Security and Critical National Infrastructure Protection. *International Affairs*, 2016, vol. 92, iss. 5, pp. 1079–1105.
27. Carr M. Public-Private Partnerships in National Cyber-Security Strategies. *International Affairs*, 2016, vol. 92, iss. 1, pp. 43–62.
28. Henriksen A. The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace. *Journal of Cybersecurity*, 2019, vol. 5, iss. 1, pp. 1–9.
29. Korobeev A.I., Chuchaev A.I. Unmanned Vehicles: New Challenges to Public Security. *Lex Russica*, 2019, no. 2 (147), pp. 9–28. (In Russian).

30. Chuchaev A.I., Malikov S.V. Responsibility for Causing Harm by a Highly Automated Vehicle: State and Perspectives. *Aktual'nye problemy rossiiskogo prava = Topical Problems of Russian Law*, 2019, no. 6 (103), pp. 117–124. (In Russian).

31. Agrafiotis I., Nurse J., Goldsmith M., Creese S., Upton D. A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding how they Propagate. *Journal of Cybersecurity*, 2018, vol. 4, iss. 1. DOI: 10.1093/cybsec/tyy006.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Чучаев Александр Иванович — профессор кафедры уголовного права Московского государственного юридического университета им. О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, г. Москва, Российская Федерация; e-mail: moksha1@rambler.ru.

Грачева Юлия Викторовна — профессор кафедры уголовного права Московского государственного юридического университета им. О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, г. Москва, Российская Федерация; e-mail: uvgracheva@mail.ru.

Маликов Сергей Владимирович — профессор кафедры уголовного права Московского государственного юридического университета им. О.Е. Кутафина (МГЮА), доктор юридических наук, г. Москва, Российская Федерация; e-mail: s.v.malikov@yandex.ru.

ДЛЯ ЦИТИРОВАНИЯ

Чучаев А.И. Посягательства на информационную систему беспилотника в этиологии дорожно-транспортных происшествий / А.И. Чучаев, Ю.В. Грачева, С.В. Маликов. — DOI: 10.17150/2500-4255.2021.15(1).55-67 // Всероссийский криминологический журнал. — 2021. — Т. 15, № 1. — С. 55–67.

INFORMATION ABOUT THE AUTHORS

Chuchaev, Alexandr I. — Professor, Chair of Criminal Law, Kutafin Moscow State Law University (MSAL), Doctor of Law, Professor, Moscow, the Russian Federation; e-mail: moksha1@rambler.ru.

Gracheva, Yulia V. — Professor, Chair of Criminal Law, Kutafin Moscow State Law University (MSAL), Doctor of Law, Professor, Moscow, the Russian Federation; e-mail: uvgracheva@mail.ru.

Malikov, Sergey V. — Professor, Chair of Criminal Law, Kutafin Moscow State Law University (MSAL), Doctor of Law, Moscow, the Russian Federation; e-mail: s.v.malikov@yandex.ru.

FOR CITATION

Chuchaev A.I., Gracheva Yu.V., Malikov S.V. Attacks on the information system of unmanned vehicles in the etiology of road accidents. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2021, vol. 15, no. 1, pp. 55–67. DOI: 10.17150/2500-4255.2021.15(1).55-67. (In Russian).