УДК 343.3/.7
DOI: 10.18384/2949-513X-2024-3-79-88

ПРЕСТУПЛЕНИЯ ПРОТИВ ЦИФРОВОЙ БЕЗОПАСНОСТИ СИСТЕМЫ ЗДРАВООХРАНЕНИЯ: ПОНЯТИЕ, ПРИЗНАКИ И СИСТЕМА

Шутова А. А.
Казанский инновационный университет имени В. Г. Тимирясова
420111, г. Казань, ул. Московская, д. 42, Российская Федерация

Аннотация
Цель. Обосновать необходимость введения термина «преступления против цифровой безопасности системы здравоохранения» в уголовно-правовую доктрину, сформулировать определение понятия, обозначить, какими признаками обладают подобные деяния, и представить их систему.
Процедура и методы. В качестве научного материала были использованы отечественные и зарубежные публикации, отражающие исследования по рассматриваемой проблеме. В статье предпринята попытка систематизировать имеющиеся теоретические воззрения как отечественных, так и зарубежных авторов, обобщить полученный материал в контексте развития цифровизации, цифровых технологий и влияния этого процесса на преступность. Полученные материалы были критически оценены автором, что позволило с учётом сущности цифровых технологий сформулировать собственную концепцию преступлений против цифровой безопасности системы здравоохранения, их систему и признаки.
Результаты. Неизбежным результатом цифровизации всех сфер общественной жизни, в т. ч. сферы здравоохранения, стало использование цифровых технологий в преступных целях, что должно послужить закономерным толчком к формированию теоретико-прикладных основ противодействия преступности. По итогам исследования сделан вывод о необходимости введения в научный оборот термина «преступления против цифровой безопасности системы здравоохранения», сформулированы признаки, характеризующие их и выработаны их системы, проведены отличия от цифровых преступлений.
Теоретическая и/или практическая значимость. В научный оборот введены термины «преступления против цифровой безопасности системы здравоохранения», «цифровые преступления», даны их определения, приведены критерии отличия, раскрыты признаки и представлена система уголовно наказуемых деяний, которые в целом расширяют имеющиеся знания в уголовно-правовой доктрине.

Ключевые слова: здравоохранение, искусственный интеллект, медицинские изделия, преступление, робототехника, уголовное право, уголовное законодательство, цифровые технологии, цифровая безопасность

CRIMES AGAINST DIGITAL SECURITY OF THE HEALTH SYSTEM: CONCEPT, SIGNS AND SYSTEM

A. Shutova
Kazan Innovative University named after V. G. Timiryasov,
ul. Moskovskaya 42, Kazan 420111, Russian Federation

Abstract
Aim. To justify the need to introduce the term “crimes against the digital security of the healthcare system” into the criminal law doctrine, to formulate a definition of the concept, to identify what characteristics such acts have and to present their system.

Methodology. Domestic and foreign publications reflecting research on the problem under consideration were used as scientific material. The article makes an attempt to systematize the existing theoretical views of both domestic and foreign authors, to summarize the obtained material in the context of the development of digitalization, digital technologies and the impact of this process on crime. The received materials were critically assessed by the author, which made it possible, taking into account the essence of digital technologies, to formulate his own concept of crimes against the digital security of the healthcare system, their system and characteristics.

Results. An inevitable result of the digitalization of all spheres of public life, including the healthcare sector, has been the use of digital technologies for criminal purposes, which should serve as a natural impetus for the formation of theoretical and applied foundations for combating crime. Based on the results of the study, it was concluded that it is necessary to introduce the term "crimes against the digital security of the healthcare system" into scientific circulation, the characteristics that characterize them were formulated and their systems were developed, and differences from digital crimes were drawn.

Research implications. The theoretical and practical significance lies in the fact that the terms "crimes against the digital security of the healthcare system", "digital crimes" have been introduced into scientific circulation, their definitions have been given, criteria for distinction are given, signs are revealed and a system of criminal offenses is presented, which in general expand existing knowledge in criminal law doctrine.

Keywords: healthcare, artificial intelligence, medical products, crime, robotics, criminal law, criminal law, digital technologies, digital security

Введение

Концепт «цифровой безопасности» в уголовном законодательстве является не новым и активно разрабатывается специалистами в уголовно-правовой доктрине (И. Р. Бегишевым [2], С. Я. Лебедевым [8], Н. А. Крайновой [7] и др.), что свидетельствует о его устойчивости и научной обоснованности.

Развитие цифровых технологий, а вслед за ними систем обеспечения защиты информации определило высокую частоту использования термина «цифровая безопасность».

При этом бурное развитие цифровых технологий и необходимость обеспечения защиты цифровой информации вынуждают продумать комплекс мер, направленных на обеспечение состояния защищённости.

Цифровизация оказывает колоссальное влияние на систему здравоохранения, последняя также подвержена значительным рискам и угрозам в виду того, что:

– применяемые цифровые технологии являются новыми и не до конца изученными;

– ещё только можно делать прогнозы относительно возможных последствий применения цифровых технологий (в т. ч. негативных) и как они отобразятся в будущем на качестве оказываемой медицинской помощи;

– цифровизация ставит под угрозу все данные в цифровом формате, начиная от персональных данных пациента, заканчивая их анамнезом в связи с тем, что медицинские организации обрабатывают значительный массив данных, что может привести к их утечкам;

– посягательства на медицинские организации могут привести к негативным последствиям как самих учреждений, так и для людей;

– возможности цифровых технологий безграничны, они позволяют злоумышленникам взломать инсулиновую помпу, получив доступ к цифровому устройству на значительном расстоянии, а в последствии ввести в организм пациента смертельную дозу препарата, используемого при лечении сахарного диабета[1]. Возможны и другие атаки шифровальщиков на различные системы поддержания жизнедеятельно-

[1] Хакер, нашедший дыру в кардиостимуляторах // C.News: [сайт]. URL: https://www.cnews.ru/news/top/hakernashedshij_dyru_v_kardiostimulyatorah (дата обращения: 06.08.2024).

сти: аппараты искусственной вентиляции лёгких и искусственного кровообращения, оборудование для анализа.

Именно по данным причинам вопросам цифровой безопасности системы здравоохранения должно отдаваться первостепенное значение, особенно в свете революции, меняющей традиционное здравоохранение на новое цифровое, а также значительного роста преступлений, совершаемых в цифровом пространстве.

Последствия от криминальных посягательств в сфере здравоохранения могут быть самыми разнообразными, начиная от хищения персональных данных пациентов, заканчивая цепями многоуровневых негативных последствий, тянущихся один за одним (компьютерный вирус передаётся от одной больницы к другой, нанося вред её системам, системам безопасности программного обеспечения, ставя под угрозу жизнь и здоровье пациентов, которым не может быть оперативно оказана медицинская помощь, что в совокупности создаёт риски национальной безопасности страны).

Кроме того, после совершения преступлений против цифровой безопасности медицинских учреждений пациенты должны продолжать получать медицинскую помощь, в т. ч. проведение в отношении них операций, поскольку от этого может зависеть их жизнь и здоровье.

Исследование вопросов цифровой безопасности системы здравоохранения невозможно без формирования надлежащего понятийно-категориального аппарата, должно быть дано определение понятия «преступления против цифровой безопасности системы здравоохранения», сформулированы признаки, характеризующие подобные деяния, выявлены особенности их квалификации, что в целом позволит говорить о формировании теоретических основ в области уголовно-правового противодействия преступлениям против цифровой безопасности системы здравоохранения и создаст теоретико-прикладные основы их квалификации.

Криминальные риски и текущее состояние

В настоящее время готовые программные инструменты не справляются с обнаружением новых угроз и защитой медицинских учреждений, что приводит к техническому пробелу. За последнее время злоумышленники активно «атаковали» сектор здравоохранения и использовали программы-вымогатели для предотвращения доступа к критически важным системам и данным[1]. Подобная ситуация складывается во многих странах вместе с ростом зависимости от цифровых систем.

В результате подобных криминальных посягательств больницы, оказывающие медицинскую помощь населению, были вынуждены останавливать машины скорой медицинской помощи, отменять и откладывать приёмы, не могли перевозить пациентов в другие больницы. Многие нападения привели к сбоям в работе на несколько месяцев, а некоторые из них – к полному закрытию медицинских учреждений[2]. Сосредоточив внимание на протоколах безопасности, обнаружении уязвимостей и автоматических исправлениях, усилия должны быть направлены на уменьшение возможностей злоумышленников атаковать программное обеспечение цифрового здравоохранения, что в целом позволит предотвратить крупномасштабные противоправные посягательства.

Злоумышленники используют различные способы для взлома больничных систем:

1) фишинговые атаки;

2) поиск уязвимостей в программном обеспечении.

В действительности, исходя из складывающейся криминальной ситуации, можно констатировать, что *противоправные посягательства возникают по поводу:*

[1] Зона заражения: киберпреступники стали чаще атаковывать больницы // Известия: [сайт]. URL: https://iz.ru/1734712/dmitrii-bulgakov/zona-zarazheniia-kiberprestupniki-stali-chashche-atakovat-bolnitcy (дата обращения: 06.08.2024).

[2] Не успели спасти: пациентка умерла из-за хакерской атаки // Газета: [сайт]. URL: https://www.gazeta.ru/tech/2020/09/18/13255255/ransomware_death.shtml (дата обращения: 06.08.2024).

1) цифровой информации, т. к. в настоящее время в здравоохранении обычно собираются огромные объёмы данных – не только описательная информация (имя, профессия, физическое и психическое состояние, генетический профиль), но также данные, полученные с помощью датчиков окружающей среды, изображений (полученных с помощью эндоскопии, радиологических методов и т. д.) [14]. Данные о здоровье и генетические данные являются наиболее важной личной информацией; они могут быть использованы в преступных целях. Криминальную угрозу безопасности информации, обращающейся в учреждениях системы здравоохранения, представляют действия, направленные на незаконное собирание подобных сведений, их распространение, неправомерный доступ к ним [13, с. 136].

2) злоумышленников могут заинтересовать медицинские изделия и иные устройства, созданные на основе цифровых технологий, которые собирают цифровые данные и используются в целях оказания медицинской помощи. В силу наличия программной части у медицинского изделия, созданного и работающего с технологией искусственного интеллекта, оно, даже выраженное в материальной форме, может и не быть интересным для злоумышленника в качестве предмета внешнего (окружающего) мира; для него интерес представляет именно его программная составляющая, позволяющая реализовать функционал изделия в преступных целях или использовать, к примеру, возможности медицинского робота. Несмотря на высокую эффективность цифровых технологий в сфере здравоохранения, имеется ряд серьёзных рисков и угроз по поводу их использования, например, безопасности и сохранности истории болезни пациента, угрозу неприкосновенности частной жизни пациента, неправомерного доступа в медицинское роботизированное изделие с целью захвата управления им, хищение биопринтера, биочернил, незаконная торговля биопринтерами, биочернилами. Кроме того, цифровые технологии активно используются злоумышленниками как механизм в своей преступной деятельности. По мнению Р. В. Шишкина, криминальная ситуация, складывающаяся в сфере цифровых технологий, позволяет констатировать отсутствие специальных форм и средств противодействия преступным проявлениям [12];

3) посягательства на объекты критической информационной инфраструктуры причиняют ущерб как гражданам, так и обществу, и государству. В модели функционирования государства и общества огромную роль занимают объекты информационной инфраструктуры, т. к. они обеспечивают устойчивое развитие цифровизации [4, с. 133]. Имеется случай смерти пациента, которому вследствие поражения информационной инфраструктуры больницы не смогли оказать медицинскую помощь[1].

Следовательно, стоит констатировать, что противоправные посягательства в сфере цифрового здравоохранения возникают по поводу безопасности цифровой информации, безопасности критической информационной инфраструктуры и безопасности цифровых технологий.

Преступления против цифровой безопасности системы здравоохранения: признаки и понятие

Преступления против цифровой безопасности системы здравоохранения характеризуются специфическими признаками, которые их отличают от других уголовно наказуемых деяний (цифровых преступлений, преступлений в сфере компьютерной информации, компьютерных преступлений и т. д.):

1) наличием специфического объекта преступного посягательства – общественными отношениями, обеспечивающими цифровую безопасность (для уголовно наказуемых деяний, предусмотренных гл. 28 Уголовного кодекса Российской

[1] В Дюссельдорфе пациентка умерла после хакерской атаки на клинику // ТАСС: [сайт]. URL: https://tass.ru/obschestvo/9482283 [сайт] (дата обращения: 06.08.2024).

Федерации (далее – УК РФ) – непосредственным объектом, для иных – дополнительным объектом);

2) совершая цифровые преступления, злоумышленник чаще всего посягает сразу на несколько объектов уголовно-правовой охраны: на цифровую безопасность и на иные общественные отношения, интересы и блага (жизнь, здоровье, собственность и т. д.).

При этом первоначально противоправное воздействие злоумышленников осуществляется на цифровую составляющую правоотношений, поскольку через посягательство именно на неё происходит воздействие на иные охраняемые законом общественные отношения, блага и интересы (жизнь и здоровье человека, национальную безопасность, персональные данные, собственность, интеллектуальные права и т. д.). Указанные общественные отношения, интересы и блага страдают в результате воздействия на них в цифровом пространстве. Так, в 2020 г. злоумышленники получили доступ к данным патолого-анатомического отделения Свердловского областного онкологического диспансера, из-за чего пациенты остались без результатов биопсии. Указанные сведения были необходимы врачам, т. к. без них невозможно было назначить лечение. Злоумышленники требовали 80 тыс. руб. за разблокировку данных[1].

Система здравоохранения подвержена цифровизации, что характеризуется переходом хранения всей информации (данные о пациентах, анамнез, персональные данные, иная медицинская документация) в цифровой формат. Подобное обстоятельство одновременно породило серьёзную проблему цифровой безопасности. Неправомерное получение подобных данных может быть использовано в преступных целях, в т. ч. для мошенничества, вымогательства и других противоправных деяний. Цифровая информация, выступающая обязательным признаком составов преступлений против цифровой безопасности системы здравоохранения, непосредственно влияет на содержание непосредственного объекта преступного посягательства и в некоторых составах определяет его (характерно для гл. 28 УК РФ);

3) «цифровая» составляющая преступлений находит свою реализацию в элементах состава преступления: предмете, средстве и способе совершения преступлений;

4) субъектами преступлений могут быть как медицинские работники, выполняющие должностные (профессиональные) обязанности, соответствующие требованиям (уровень образования, стаж и т. д.), занимающие определённую должность и обладающие определёнными правомочиями, а также иные лица, непосредственно не относящиеся к сфере здравоохранения.

Цифровая безопасность системы здравоохранения может быть объектом преступных посягательств со стороны как медицинских работников, так и обычных граждан, которые не имеют медицинского образования, однако их противоправные намерения непосредственно причиняют вред организации системы здравоохранения. Несомненно, в некоторых случаях действия виновных могут быть направлены на достижение корыстных целей, однако осуществляют их посредством воздействия на учреждения системы здравоохранения;

5) потерпевшими в результате совершения уголовно наказуемых деяний являются как юридические (учреждения и организации системы здравоохранения в независимости от формы собственности), так и физические лица (медицинские работники, пациенты и т. д.);

6) специфические негативные общественно опасные последствия (как юридически значимые, так и не влияющие на квалификацию, но оказывающие негативное воздействие) от совершения преступлений против цифровой безопасности системы здравоохранения (блокировка доступа к электронным программам больниц, в результате чего медицинские учреждения не могут оказывать помощь, не зная анамнеза

[1] Вирус лишил свердловский онкоцентр доступа к анализам больных. Хакерскую атаку посчитали случайной // 360.RU: [сайт]. URL: https://360.ru/tekst/obschestvo/virus-lishil-sverdlovskij-onkotsentr. (дата обращения: 06.08.2024).

и истории болезни пациента, рост нагрузки на соседние медицинские учреждения из-за атак на больницы, которые вынуждены принимать пациентов от организаций, пострадавших в результате хакерской атаки, причинение вреда жизни или здоровью пациентов, приостановление работы медицинской организации, отсутствие возможности оперативно оказывать помощь, потеря доступа к медицинским картам пациентов, отключение больниц от цифрового оборудования и т. д.). Так, в 2023 г. в Приморье были атакованы информационные системы склада льготных лекарств, в результате чего отпуск жизненно важных препаратов был временно приостановлен[1].

Итак, выявленные в процессе исследования основные признаки, которые характеризуют преступления против цифровой безопасности системы здравоохранения, позволят сформулировать их определение.

Так, под преступлениями против цифровой безопасности системы здравоохранения следует понимать *противоправные общественно опасное деяния, посягающие на состояние защищённости цифровой информации, цифровой инфраструктуры и цифровых технологий в системе здравоохранения от внутренних и внешних цифровых угроз*.

Отличие преступлений против цифровой безопасности системы здравоохранения от цифровых преступлений

Концепция «преступления против цифровой безопасности системы здравоохранения» шире концепции «цифровых преступлений», в связи с этим полагаем, что их можно рассматривать как часть (цифровые преступления) и целое (цифровая безопасность). Стоит отметить, что если в доктрине уже активно употребляется термин «цифровые преступления»[2] [5; 9], то вопросам цифровой безопасности уделяется меньше внимания.

Мы придерживаемся позиции, согласно которой цифровые преступления – это общественно опасные деяния, совершенные с использованием цифровых технологий и (или) в отношении них. В данном определении мы акцентируем внимание на том, что данные уголовно наказуемые деяния характеризуются влиянием на цифровые технологии, а не на информационные, несмотря на то, что некоторые авторы рассматривают их как тождественные [10, с. 39].

При этом безопасность – это ключевое и комплексное понятие, в нормативных правовых актах Российской Федерации под которым понимается состояние защищённости жизненно важных интересов личности, общества и государства[3], национальных интересов[4], участников дорожного движения[5] от каких-либо угроз. В свою очередь, любой вид безопасности представляет собой определённый набор инструментов и методов, которые следует использовать для защиты. Так, защита информации от незаконного доступа, использования, раскрытия или изменения является основной целью информационной безопасности. В свою очередь, защита цифровой информации, цифровой инфраструктуры и цифровых технологий субъектов, осуществляющих деятельность в системе здравоохранения, является целью цифровой безопасности системы здравоохранения.

Система преступлений против цифровой безопасности системы здравоохранения

Исходя из складывающейся криминальной ситуации (приведённой выше), а также с учётом того, что основными элементами

[1] В Приморье приостановили выдачу лекарств льготникам из-за хакерской атаки // RGRU: [сайт]. URL: https://rg.ru/2023/07/14/v-primore-iz-za-hakerskoj-ataki-priostanovlena-vydacha-lekarstv-lgotnikam.html (дата обращения: 06.08.2024).

[2] Цифровое право: учебник / под ред. Э. Л. Сидоренко. М.: Юрлитинформ, 2024. 720 с.

[3] Закон Российской Федерации от 05.03.1992 № 2446-I «О безопасности» // Российская газета. 1992. № 103.

[4] Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // СПС Консультант Плюс.

[5] Федеральный закон от 10.12.1995 № 196-ФЗ «О безопасности дорожного движения» // СПС Консультант Плюс.

цифровой безопасности системы здравоохранения являются: цифровая информация, цифровые технологии и цифровая инфраструктура, – полагаем возможным выработать систему преступлений, посягающих на цифровую безопасность системы здравоохранения. Данная система позволит выявить общие признаки, характеризующие подобные противоправные посягательства в русле процессов цифровизации, определить влияние цифровых технологий, цифровой информации на преступность, сформулировать предложения по квалификации подобных деяний и меры по совершенствованию уголовного законодательства.

Систему преступлений против цифровой безопасности системы здравоохранения составляют:

1) уголовно наказуемые деяния против безопасности цифровой информации, обращающейся в учреждениях системы здравоохранения (ст.ст. 137, 138, 138[1], 159[6], 272, 273, 274, 274[1] УК РФ). В данном случае цифровая информация является предметом преступного посягательства;

2) преступления против безопасности цифровой инфраструктуры учреждений системы здравоохранения (274[1] УК РФ). В данном случае цифровая инфраструктура (информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления) и информация, содержащаяся в ней, являются предметами преступного посягательства;

3) преступления против безопасности цифровых технологий, применяемых в системе здравоохранения (нейротехнологии, технологии искусственного интеллекта и робототехники; интернет вещей и технологии больших данных и др.). При этом цифровые технологии находят свою материальную форму выражения, реализуясь как медицинские изделие. Технологии искусственного интеллекта, применяемые в сфере здравоохранения, находят своё воплощение в программном обеспечении, не имеющем своей материальной формы выражения.

Примечательно, что авторы уже проводят исследования влияния цифровых технологий – дипфейков – на преступность, правовое регулирование которых ещё не сложилось [6, с. 55].

Применительно к данной категории злоумышленник стремится неправомерно завладеть доступом к тем или иным цифровым данным [11, с. 392] в цифровом устройстве (медицинском изделии) и получает их в процессе выполнения определённых манипуляций с программами и системами устройств. При этом конкретная цифровая технология относится к предмету совершения преступления, а непосредственным объектом являются общественные отношения, обеспечивающие их цифровую безопасность (в текущей редакции УК РФ – общественные отношения, обеспечивающие безопасность в сфере компьютерной информации и т. д.). Однако в том случае, если, к примеру, модификация охраняемой законом цифровой информации производилась с целью нарушения неприкосновенности частной жизни, то они подлежат квалификации по совокупности с преступлением, предусмотренными ст. 137 УК РФ и составом преступлений, предусмотренных гл. 28 УК РФ.

Если же противоправное посягательство производилось непосредственно на программный код искусственного интеллекта, то имеет место преступление в сфере компьютерной информации, которое может быть квалифицировано в рамках отечественного уголовного законодательства, к примеру, по ст.ст. 272 или 273 УК РФ. К предмету преступлений в сфере компьютерной информации следует относить компьютерную информацию, определение которой содержится в примечании к ст. 272 УК РФ. Самообучаемая система состоит из программного кода, т. е. является компьютерной информацией.

Однако считаем важным указать, что в данном случае целесообразно выделять уголовно наказуемые деяния, совершаемые:

– *непосредственно против цифровой технологии*. При этом следует сделать оговорку, что в рамках указанной группы преступлений подразумевается применение не интеллектуальных свойств медицин-

ских изделий, а именно «физическое» наполнение технологий;

– *против результата цифровой технологии*. В рамках указанной группы преступлений подразумевается применение «интеллектуальных» свойств медицинских изделий, оснащённых цифровыми технологиями.

В свою очередь, преступления, совершённые с использованием цифровых технологий в системе здравоохранения, это:

– цифровые технологии, используемые в качестве способа совершения преступления;

– цифровые технологии, используемые в качестве средства совершения преступления.

Программисты уже продемонстрировали, как они могут вмешиваться в работу кардиостимуляторов и инсулиновой помпы[1], являющихся медицинскими изделиями, для получения дистанционного контроля над ними, в результате чего могут причинить вред здоровью, а также вообще лишить человека жизни. Можно предполагать, что потенциальные злоумышленники смогут взять под контроль и иное медицинское оборудование, включая медицинских роботов для проведения удалённой хирургии. Во время телехирургической операции доктор удалённо управляет медицинским роботом с помощью специализированного программного и аппаратного обеспечения.

В случае, если в рамках приготовления к умышленному уничтожению движимого имущества (к примеру, автомобиля) в крупном размере лицо осуществило несанкционированное воздействие на цифровой код компьютерной программы робота, в результате чего приобрело возможность управлять им и с его помощью уничтожило имущество, то содеянное образует совокупность преступлений, предусмотренных ст.ст. 167 и 272 УК РФ [3, с. 71].

Заключение

В связи с построением цифрового государства и цифрового общества [1, с. 26] полагаем возможным использовать в уголовно-правовой доктрине дефиницию «преступления против цифровой безопасности системы здравоохранения», поскольку цифровизация затрагивает как большой комплекс правоотношений в рассматриваемой сфере, связанных с надлежащим осуществлением цифровой медицинской помощи пациентам, так и другие деяния прямо или косвенно связанные с ней.

Уголовно-правовая характеристика преступлений против цифровой безопасности системы здравоохранения требует анализа специфических признаков деяний, их системы. Для этих целей важное место занимает системный подход.

Под преступлениями против цифровой безопасности системы здравоохранения следует понимать противоправные общественно опасные деяния, посягающие на состояние защищённости цифровой информации, цифровой инфраструктуры и цифровых технологий в системе здравоохранения от внутренних и внешних цифровых угроз.

Система преступлений, посягающих на цифровую безопасность системы здравоохранения, строится из:

1) преступлений против безопасности цифровой информации, обращающейся в учреждениях системы здравоохранения (ст.ст. 137, 138, 138[1], 159[6], 272, 273, 274, 274[1] УК РФ).

2) преступлений против безопасности цифровой инфраструктуры учреждений системы здравоохранения (ст. 274[1] УК РФ).

3) преступлений против безопасности цифровых технологий в системе здравоохранения.

Статья поступила в редакцию 24.02.2024.

[1] Уязвимости в медицинских приборах – реальность [Электронный ресурс]. URL: https://www.kaspersky.ru/blog/vzlamyvaya-lyudej/1530/ (дата обращения: 15.08.2024).

ЛИТЕРАТУРА

1. Арзамасов Ю. Г., Певцова Е. А. Роль цифровизации в систематизации юридической терминологии // Московский юридический журнал. 2022. № 4. С. 24–34. DOI: 10.18384/2310-6794-2022-4-24-34.
2. Бегишев И. Р. Семантический анализ термина «цифровая безопасность» // Юрислингвистика. 2021. № 20. С. 24–38. DOI: 0000-0001-5619-4025
3. Бегишев И. Р. Цифровые преступления, совершаемые в отношении роботов // Социально-политические науки. 2021. Т. 11. № 3. С. 67–73.
4. Дремлюга Р. И., Зотов С. С., Павлинская В. Ю. Критическая информационная инфраструктура как предмет преступного посягательства // Азиатско-Тихоокеанский регион: экономика, политика, право. 2019. Т. 21. № 2. С. 130–139.
5. Долгиева М. М. Цифровой объект преступления // Вестник Томского государственного университета. 2022. № 483. С. 253–260. DOI: 10.17223/15617793/483/27
6. Киселёв А. С. О необходимости правового регулирования в сфере искусственного интеллекта: дипфейк как угроза национальной безопасности // Московский юридический журнал. 2021. № 3. С. 54–64. DOI: 10.18384/2310-6794-2021-3-54-64
7. Крайнова Н. А. «Международная цифровая безопасность»: миф или реальность? // Криминология: вчера, сегодня, завтра. 2019. № 4. С. 42–46.
8. Лебедев С. Я. Цифровой безопасности – цифровой уголовно-правовой ресурс // Криминология: вчера, сегодня, завтра. 2019. № 4. С. 17–25.
9. Перина А. С. «Цифровые преступления»: понятие, типология, признаки // Юридический вестник Самарского университета. 2023. Т. 9. № 3. С. 106–115. DOI: 10.18287/2542-047X-2023-9-3-106-115.
10. Сидорова Е. З., Усов Е. Г. Основные меры предупреждения цифровой преступности // Вестник ВИПК МВД России. 2024. № 2. С. 38–43. DOI: 10.29039/2312-7937-2024-2- 38-43.
11. Фаллетти Э. Алгоритмическая дискриминация и защита неприкосновенности частной жизни // Journal of Digital Technologies and Law. 2023. Т. 1. № 2. С. 387–420. DOI: 10.21202/jdtl.2023.16
12. Шишкин Р. В. Преступления, совершаемые с использованием цифровых технологий: проблемы противодействия // Вестник Уральского юридического института МВД России. 2022. № 4. С. 148–153. DOI: 10.21869/2223-1501-2024-14-2-119-130
13. Шутова А. А. Влияние телемедицины на преступность: риски и тенденции, уголовно-правовое реагирование // Вестник Московского государственного областного университета. Серия: Юриспруденция. 2022. № 4. С. 133–142. DOI: 10.18384/2310-6794-2022-4-133-142.
14. Martian CO2 ice observation at high spectral resolution with ExoMars / F. Oliva, E. D'Aversa, G. Bellucci, F. G. Carrozzo, L. R. Lozano, F. Altieri, et al. // Journal of Geophysical Research. 2022. № 127. DOI: 10.1029/2021JE007083

REFERENCES

1. Arzamasov Yu. G., Pevtsova E. A. [The Role of Digitalization in the Systematization of Legal Terminology]. In: *Moskovskiy yuridicheskiy zhurnal* [Moscow Law Journal], 2022, no. 4, pp. 24–34. DOI: 10.18384/2310-6794-2022-4-24-34
2. Begishev I. R. [Semantic Analysis of the Term "Digital Security"]. In: *Yurislingvistika* [Jurislinguistics], 2021, no. 20, pp. 24–38. DOI: 0000-0001-5619-4025
3. Begishev I. R. [Digital Crimes Committed against Robots]. In: *Sotsialno-politicheskaya nauka* [Social and Political Sciences], 2021, vol. 11, no. 3, pp. 67–73.
4. Dremlyuga R. I., Zotov S. S., Pavlinskaya V. Yu. [Critical information infrastructure as an object of criminal encroachment]. In: *Aziatsko-Tikhookeanskiy region: ekonomika, politika, pravo* [Asia-Pacific region: economics, politics, law], 2019, vol. 21, no. 2, pp. 130–139.
5. Dolgieva M. M. [Digital object of crime]. In: *Vestnik Tomskogo gosudarstvennogo universiteta* [Bulletin of Tomsk State University], 2022, no. 483, pp. 253–260. DOI: 10.17223/15617793/483/27
6. Kiselev A. S. [On the need for legal regulation in the field of artificial intelligence: deepfake as a threat to national security]. In: *Moskovskiy yuridicheskiy zhurnal* [Moscow Law Journal], 2021, no. 3, pp. 54–64. DOI: 10.18384/2310-6794-2021-3-54-64
7. Kraynova N. A. ["International Digital Security": Myth or Reality?]. In: *Kriminologiya: vchera, segodnya, zavtra* [Criminology: Yesterday, Today, Tomorrow], 2019, no. 4, pp. 42–46.
8. Lebedev S. Ya. [Digital Security – a Digital Criminal-Law Resource]. In: *Kriminologiya: vchera, segodnya,*

zavtra [Criminology: Yesterday, Today, Tomorrow], 2019, no. 4, pp. 17–25.
9. Perina A. S. ["Digital Crimes": Concept, Typology, Features]. In: *Yuridicheskiy vestnik Samarskogo universiteta* [Legal Bulletin of Samara University], 2023, vol. 9, no. 3, pp. 106–115. DOI: 10.18287/2542-047X-2023-9-3-106-115.
10. Sidorova E. Z., Usov E. G. [Basic measures to prevent digital crime]. In: *Vestnik VIPK MVD Rossii* [Bulletin of the All-Russian Institute of Advanced Training of the Ministry of Internal Affairs of Russia], 2024, no. 2, pp. 38–43. DOI: 10.29039/2312-7937-2024-2-38-43.
11. Falletti E. [Algorithmic discrimination and protection of privacy]. In: *Zhurnal Tsifrovyye tekhnologii i pravo* [Journal of Digital Technologies and Law], 2023, vol. 1, no. 2, pp. 387–420. DOI: 10.21202/jdtl.2023.16
12. Shishkin R. V. [Crimes committed using digital technologies: problems of counteraction]. In: *Vestnik Ural'skogo yuridicheskogo instituta MVD Rossii* [Bulletin of the Ural Law Institute of the Ministry of Internal Affairs of Russia], 2022, no. 4, pp. 148–153. DOI: 10.21869/2223-1501-2024-14-2-119-130
13. Shutova A. A. [The impact of telemedicine on crime: risks and trends, criminal-law response]. In: *Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta. Seriya: Yurisprudentsiya* [Bulletin of Moscow State Regional University. Series: Jurisprudence], 2022, no. 4, pp. 133–142. DOI 10.18384/2310-6794-2022-4-133-142.
14. Oliva F., D'Aversa E., Bellucci G., Carrozzo F. G., Lozano L. R., Altieri F., et al. Martian CO2 ice observation at high spectral resolution with ExoMars. In: *Journal of Geophysical Research,* 2022, no. 127. DOI: 10.1029/2021JE007083

ИНФОРМАЦИЯ ОБ АВТОРЕ

Шутова Альбина Александровна – кандидат юридических наук, старший научный сотрудник научно-исследовательского института цифровых технологий и права Казанского инновационного университета имени В. Г. Тимирясова;
e-mail: shutova1993@inbox.ru

INFORMATION ABOUT THE AUTHOR

Albina A. Shutova – Cand. Sci. (Law), Senior Researcher, Research Institute of Digital Technologies and Law, Kazan Innovative University named V. G. Timiryasov;
e-mail: shutova1993@inbox.ru

ПРАВИЛЬНАЯ ССЫЛКА НА СТАТЬЮ

Шутова А. А. Преступления против цифровой безопасности системы здравоохранения: понятие, признаки и система // Московский юридический журнал. 2024. № 3. С. 79–88.
DOI: 10.18384/2949-513X-2024-3-79-88

FOR CITATION

Shutova A. A. Crimes against Digital Security of the Health System: Concept, Signs and System. In: *Moscow Juridical Journal,* 2024, no. 3, pp. 79–88.
DOI: 10.18384/2949-513X-2024-3-79-88