«КонсультантПлюс». URL: https://login.consultant.ru/link/?req=doc&demo=2&base=LAW&n=422054& (дата обращения: 18.09.2022).

5. О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 14.07.2022) // СПС «КонсультантПлюс». URL: https://login.consultant.ru/link/?req=doc&demo=2&base=LAW&n=422241 (дата обращения: 18.09.2022).

6. Концепция информационной политики судебной системы на 2020–2030 годы (одобрена Советом судей РФ 05.12.2019) // СПС «КонсультантПлюс». URL: https://login.consultant.ru/link/?req=doc&demo=2&base=LAW&n=339776 (дата обращения: 18.09.2022).

Ю. Ю. Малышева,
кандидат юридических наук, доцент,
заведующий кафедрой
уголовного права и криминологии,
Казанский институт (филиал) Всероссийского государственного
университета юстиции

УГОЛОВНО-ПРАВОВЫЕ РИСКИ ЦИФРОВИЗАЦИИ ЗДРАВООХРАНЕНИЯ

Аннотация. В статье освещаются основные риски цифровизации здравоохранения, указываются уголовно-правовые риски причинения вреда при передаче персональных данных, требующих обеспечения высокого уровня безопасности. Проблема в настоящее время заключается в отсутствии системы уголовно-правовой защиты персональных данных в России, что логически приводит к уголовно-правовым рискам цифровизации здравоохранения. Цифровизация является основным вектором развития современного российского общества, выступая в роли неотъемлемой российской действительности. Развитие информационных технологий в современной России неминуемо приводит к тому, что они стали использоваться при совершении преступлений. Закономерной реакцией на данные обстоятельства выступают уголовно-правовые меры, способные успешно противостоять данному явлению. Цифровизация здравоохранения включает развитие искусственного интеллекта в здравоохранении, нуждающемся в правильном уголовно-правовом регулировании текущих отношений. Цифровые технологии в здравоохранении необходимо развивать в целях устойчивого прогресса отрасли медицинского права, поскольку цифровизация здравоохранения позволяет решить ряд существенных проблем в условиях пандемии COVID-19.

Ключевые слова*:* цифровизация здравоохранения в уголовном праве, уголовно-правовые риски цифровизации здравоохранения, информационные технологии в уголовном праве, искусственный интеллект в уголовном праве, цифровизация здравоохранения в условиях пандемии COVID-19, уголовно-правовая защита персональных данных в РФ

CRIMINAL AND LEGAL RISKS OF DIGITALIZATION OF HEALTH CARE

Abstract. The article highlights the main risks of digitalization of healthcare, indicates the criminal-legal risks of harm in the transfer of personal data that require a high level of security. The problem currently lies in the lack of a system of criminal law protection of personal data in Russia, which logically leads to criminal law risks of digitalization of healthcare. Digitalization is the main vector of development of modern Russian society, acting as an integral Russian reality. The development of information technologies in modern Russia inevitably leads to the fact that they began to be used in the commission of crimes. A natural reaction to these circumstances is criminal law measures that can successfully counter this phenomenon. The digitalization of healthcare includes the development of artificial intelligence in healthcare, which needs the correct criminal law regulation of current relations. Digital technologies in healthcare need to be developed for the sustainable progress of the medical law industry, since the digitalization of healthcare allows solving a number of significant problems in the context of the COVID-19 pandemic.

Keywords: Gitalization of healthcare in criminal law, Criminal law risks of digitalization of health care, Information technologies in criminal law, Artificial intelligence in criminal law, Digitalization of healthcare in the context of the COVID-19 pandemic, Criminal law protection of personal data in the Russian Federation

Главной гарантией продолжительности и качества жизни человека является его здоровье, поэтому развитие медицины безусловно является ключевым вопросом национальной безопасности. В изменившихся в последнее время условиях жизни человека, при неизбежных обстоятельствах цифровизации нашего общества, вопрос безопасности личности приобрел глобальный масштаб. События, происходящие в мире, наглядно демонстрируют, какое значение имеет здравоохранение для обеспечения национальной безопасности. Инструментом, обеспечивающим предупреждение преступности, правопорядок, безопасность личности и национальную безопасность, является уголовная политика [1. С. 34].

Обеспечение безопасности личности в сфере оказания медицинской помощи предполагает дуалистическую направленность политики противодействия преступности в сфере оказания медицинской помощи.

За время действия Уголовного кодекса РФ, уже более четверти века, существенно изменилось общество, цифровые технологии уверенно вошли в жизнь большинства людей, в особенности в связи с пандемией коронавируса COVID-19, и роль цифровых технологий заметно укрепилась и стала гораздо важнее. Все то, что казалось в XX в. фантастикой, в XXI в. является элементом нормальной повседневной жизни людей.

Таким образом, цифровизация – это актуализация информации, обращающейся в определенной социальной области, в формат, обеспечивающий возможность машинной (компьютерной) обработки данных.

В качестве одной из национальных идей развития цифровых технологий в России на период до 2024 г. указано обеспечение ускоренного внедрения цифровых

технологий в сфере оказания медицинской помощи. Поэтому приведение в соответствие положений уголовного права с глобальной информатизацией преступности является перспективной задачей, которая, безусловно, должна быть решена в ближайшее время. Сформировавшееся в последние годы новые формы преступной деятельности с использованием современных информационно-телекоммуникационных технологий должны получить достойный «ответ» в виде уголовно-правовых императивных методов.

В 1999 году Институтом медицины Национальной академии наук США (NAS) был опубликован отчет «Человеку свойственно ошибаться», в котором отмечено, что врачебные ошибки являются причиной смерти от 44 000 до 98 000 больных ежегодно, что в несколько раз превышает смертность от автомобильных аварий (43 458) и ряда серьезных заболеваний.

В сложившихся условиях важно обеспечить защиту здравоохранения с обеих сторон. По традиции центральным вопросом противодействия преступности в сфере здравоохранения являлось обеспечение безопасности пациента, и, безусловно, значимость этой проблемы нельзя преуменьшать. Вместе с тем, важно обеспечить безопасность и защиту не только пациента, но и медицинского работника. По нашему мнению, защита прав и свобод человека и гражданина не должна носить однобокий характер, обращенный в сторону лишь одного участника правоотношений – пациента. Законодатель должен помнить и о другой стороне этих правоотношений – медицинском работнике. Здесь важно соблюсти такой баланс, чтобы, защищая интересы одной из сторон, не ущемить интересы другой, поскольку, по мнению выдающихся философов, любая дисгармония в отношениях негативно влияет на интересы обеих сторон, и это бесспорно.

В конце XX – начале XXI в. особо остро встала проблема цифровизации здравоохранения.

Цифровизация уголовного права целиком и полностью зависит от аналогичного процесса, происходящего в экономике, поскольку уголовное право современности неизбежно и своевременно старается реагировать на процессы, происходящие в обществе [2. С. 388].

Камнем преткновения в настоящее время является полное отсутствие в России системы защиты персональных данных, по справедливому замечанию Э. Л. Сидоренко, что безусловно отражается на процессе цифровизации здравоохранения.

В октябре 2019 г. Министерством здравоохранения Российской Федерации был утвержден Федеральный проект «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ «Цифровой контур здравоохранения») на период 2019–2024 годов» (далее – ЕГИСЗ). Настоящий проект призван решать задачи по трансформации процессов организации системы здравоохранения.

Примечательным является то, что в России в 2020 г. в цифровое здравоохранение было вложено 47,3 млн долл., в 2021 г. уже 50,2 млн долл. Самыми популярными направлениями у инвесторов этой сферы в России стали– телемедицина, мобильные приложения, сервисы для пациентов, медицинское страхование, а также особое место занимают решения с использованием искусственного интеллекта.

С активным развитием искусственного интеллекта в сфере здравоохранения возникают вопросы, касающиеся правовой оценки действия систем и тех, кто будет нести ответственность в случае причинения вреда. С одной стороны системы искусственного интеллекта способны к самообучению (система способна сама принять решение о совершение действия, которое может квалифицироваться как преступление) с другой стороны указанные системы функционирует посредством деятельности конкретного физического лица. Необходимо учитывать, что в основе функционирования искусственного интеллекта находится производитель продукта и разработчик, которые могут нести ответственность за выполнение работ и оказание услуг, не отвечающих требованиям безопасности жизни или здоровья потребителя. Не исключено, что в деятельность системы может вмешаться иное лицо со стороны и заразить вирусом, изменить исходный код, перепрограммировать систему. В этом случае имеет место совокупность преступлений в сфере компьютерной безопасности и преступлений против личности. В сфере применения искусственного интеллекта отсутствует объективная статистика, поэтому чтобы лица, использующие информационные системы для совершения преступления не могли избежать юридической ответственности необходимо совершенствование всего российского законодательства, в том числе и уголовного.

Цифровая экосистема здравоохранения должна обеспечивать беспрепятственный и безопасный обмен медицинскими данными между пользователями, поставщиками медицинских услуг, менеджерами систем здравоохранения и службами медицинских данных.

В цифровой стратегии особая роль отводится медицинским данным, которые классифицируются как конфиденциальные персональные данные или личная идентифицируемая информация, требующая высокого уровня безопасности.

Активность киберпреступников в отношении медицинских учреждений с каждым годом растет. В 2021 г. самой атакуемой отраслью года было здравоохранение, а к 2022 г. медицина входит в тройку лидеров по количеству разного рода кибератак. Уже в начале мая 2022 г. Президент России Владимир Путин подписал указ о создании отдельной кибербезопасности на объектах критической информационной инфраструктуры, включая учреждения здравоохранения. Поэтому в рамках уголовно-правовой политики совершенствование правового регулирования предупреждения преступности происходит за счет концентрации внимания на изменении норм уголовно-правового законодательства и практики его применения [3. С. 65].

Для того, чтобы не стать жертвой уголовных преступлений, совершенных с помощью информационных технологий, следует не только быть осведомленным в алгоритме действий при взаимодействии с правоохранительными органами, но и применять определенные превентивные меры. Несмотря на существование широкого пласта возможностей для противодействия преступлениям с использованием информационных технологий, большинство экспертов склоняются к мнению, что превентивные меры являются наиболее эффективным способом борьбы с киберпреступлениями.

Список литературы

1. Лопашенко Н. А. Уголовная политика. Москва: ВолтерсКлувер, 2009. С. 34.
2. Малышева Ю. Ю. К вопросу о цифровизации уголовного права в тандеме с цифровой экономикой // Вектор развития управленческих подходов в цифровой экономике: материалы III Всероссийской научно-практической конференции. Казань, 2021. С. 387–393.
3. Малышева Ю. Ю. Мнимая криминализация и уголовная политика: актуальные вопросы // Сборник материалов VIII Международной научно-практической конференции. Санкт-Петербург, 2020. С. 64–67.

Н. В. Машинская,
кандидат юридических наук, доцент,
Северный (Арктический) федеральный университет
имени М. В. Ломоносова

ПРОБЛЕМЫ ЗАКОНОДАТЕЛЬНОГО РЕГУЛИРОВАНИЯ ДОПРОСА, ОЧНОЙ СТАВКИ И ОПОЗНАНИЯ С ИСПОЛЬЗОВАНИЕМ СИСТЕМ ВИДЕОКОНФЕРЕНЦСВЯЗИ

Аннотация. Включение в Уголовно-процессуальный кодекс Российской Федерации ст. 189.1, предусматривающей проведение в ходе предварительного расследования допроса, очной ставки и опознания путем использования систем видеоконференцсвязи, вызвало дискуссии среди теоретиков и практикующих юристов относительно обеспечения доказательственного значения получаемого результата и обеспечения прав участников процесса. В настоящем исследовании на основе анализа законодательного регулирования и мнений различных авторов формулируется вывод о необходимости совершенствования рассматриваемой нормы.

Ключевые слова: участники уголовного судопроизводства, следственные действия, доказательства, принципы уголовного судопроизводства, видеоконференцсвязь, допрос, очная ставка

PROBLEMS OF LEGISLATIVE REGULATION OF INTERROGATION, CONFERENCE AND IDENTIFICATION USING VIDEO CONFERENCE COMMUNICATION SYSTEMS

Abstract. The inclusion in the Code of Criminal Procedure of the Russian Federation of Article 189.1, which provides for interrogation, confrontation and identification during the preliminary investigation through the use of videoconferencing systems, caused discussions among theorists and practicing lawyers regarding ensuring the probative value of the result obtained and ensuring the rights of participants in the process. In this study, based on the analysis of legislative regulation and the opinions of various authors, a conclusion is made about the need to improve the norm in question.

Keywords: Participants in criminal proceedings, Investigative actions, Evidence, Principles of criminal justice, Video conferencing, Interrogation, Rate