Научная статья
УДК 343.3/7

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УЧРЕЖДЕНИЙ СИСТЕМЫ ЗДРАВООХРАНЕНИЯ: УГОЛОВНО-ПРАВОВОЙ АСПЕКТ

Альбина Александровна Шутова
Казанский инновационный университет имени В.Г. Тимирясова, Казань, Россия,
shutova1993@inbox.ru, ORCID 0000-0003-3015-3684

Аннотация. В представленной публикации поднимаются вопросы информационной безопасности учреждений системы здравоохранения, на основе материалов судебной практики определяются существующие угрозы в данной сфере, предлагаются некоторые меры по повышению эффективности уголовно-правовых средств противодействия подобным рискам. В целом делается вывод о том, что посягательства на информационную безопасность системы здравоохранения может поставить под угрозу самые ценные объекты уголовно-правовой охраны – жизнь и здоровье граждан, собственность и другие. Автором уделяется внимание участившимся случаям посягательств в информационном пространстве на учреждения системы здравоохранения в связи с тем, что некоторые из них являются значимыми объектами критической информационной инфраструктуры Российской Федерации.

Ключевые слова: уголовное право, уголовно-правовая политика, информационная безопасность, критическая информационная инфраструктура, преступления в сфере здравоохранения, компьютерная информация.

Для цитирования: Шутова А. А. Угрозы информационной безопасности учреждений системы здравоохранения: уголовно-правовой аспект // Вестник Уфимского юридического института МВД России. 2023. № 3 (101). С. 131–137.

Original article

THREATS TO THE INFORMATION SECURITY OF HEALTHCARE INSTITUTIONS: CRIMINAL-LEGAL ASPECT

Albina A. Shutova
Kazan Innovative University named after V.G. Timiryasov, Kazan, Russia,
shutova1993@inbox.ru, ORCID 0000-0003-3015-3684

Abstract. The presented publication raises issues to information security of healthcare institutions, identifies existing threats in this area on the basis of judicial practice materials, and suggests some measures to improve the effectiveness of criminal legal means of countering such risks. In general, it is concluded that encroachments on the information security of the healthcare system can endanger the most valuable objects of criminal law protection – the life and health of citizens, property and others. The author pays attention to the frequent cases of encroachments in the information space on healthcare institutions due to the fact that some of them are significant objects of the critical information infrastructure of the Russian Federation.

Keywords: criminal law, criminal law policy, information security, critical information infrastructure, crimes in the field of healthcare, computer information

For citation: Shutova A. A. Threats to the information security of healthcare institutions: criminal-legal aspect // Bulletin of Ufa Law Institute of the Ministry of Internal Affairs of Russia. 2023. No 3 (101). P. 131–137. (In Russ.)

Введение. Жизнь и здоровье каждого человека являются наивысшей ценностью с точки зрения Конституции Российской Федерации и иных правовых актов между-

народного характера. Несомненно, государство стремится соблюдать провозглашенные права, что нашло свое отражение в действующем Уголовном кодексе Российской Федерации 1996 г., именно поэтому значительное внимание в данном направлении следует уделять своевременной и качественно оказываемой медицинской помощи населению, особенно в свете последних событий – активного и массового (в мировом масштабе) характера распространения новой коронавирусной инфекции, оспы обезьян и иных массовых заболеваний.

Однако в связи с массовой информатизацией общества значительным ростом внедрения цифровых технологий увеличились преступные посягательства на информационную безопасность учреждений, оказывающих медицинскую помощь населению. Подобные криминальные действия могут причинить колоссальный ущерб как всей системе здравоохранения в целом, так и отдельному пациенту, жизнь и здоровье которого всецело зависят от времени и качества проведения операционного вмешательства.

В последние годы рост количества посягательств на информационную инфраструктуру учреждений системы здравоохранения отмечается во всем мире. Медицинские учреждения являются особенно уязвимыми в связи с содержащимся в них массивом сведений о пациентах – персональных данных. Однако в отличие от большинства отраслей, неправомерные посягательства на организации системы здравоохранения могут напрямую угрожать жизни или здоровью людей. Кроме того, растет количество цифровых медицинских услуг, в том числе оказываемых с использованием сервисов телемедицины, что неизбежно ставит перед собой необходимость охраны информационной безопасности указанных учреждений. Подобные противоправные случаи уже не являются редкостью в современной действительности. Некоторые авторы уже оценивают последствия от биохакерства и возможного противоправного воздействия на информационную составляющую больниц [1, с. 201].

Оценивая материалы правоприменения в рассматриваемой сфере и деятельность правоохранительных органов в области обеспечения информационной безопасности на мировом уровне, выделим основные криминальные способы совершения противоправных деяний и уязвимости, с которыми сталкиваются организации системы здравоохранения.

1. Хакерские атаки на серверы медицинских учреждений, которые влекут отключение или блокировку аппаратов приборов (к примеру, кардиостимуляторов) во время операций, срыв самой операции.

Так, в 2019 г. произошла атака на сервер Федерального центра нейрохирургии в г. Тюмени во время экстренной операции головного мозга 11-летней девочки. В результате часть приборов внезапно отключилась во время операции, некоторые аппараты, сопровождающие операцию, оказались заблокированы. За восстановление доступа злоумышленники требовали от руководства биткойны. Врачам пришлось завершать манипуляции в ручном режиме, без поддержки современной аппаратуры. Жизнь девочки была спасена[1].

Рассмотрим следующий случай. Несколько больниц и больничных сетей, входящих в систему Национальной службы здравоохранения Великобритании, подверглись атаке злоумышленников, в результате данные, в том числе медицинские записи, были зашифрованы вредоносным программным обеспечением, запущенным в ИТ-систему. Подобные действия привели к отмене плановых операций и приемов в больнице[2].

[1] В Тюмени хакеры атаковали центр нейрохирургии во время операции // Российская газета. URL: https://rg.ru/2018/07/06/reg-urfo/centr-nejrohirurgii-v-tiumeni-podvergsia-hakerskoj-atake.html (дата обращения: 12.07.2022).

[2] Sky: в Великобритании кибератаке подверглись объекты здравоохранения // Международная панорама – ТАСС. URL: https://tass.ru/mezhdunarodnaya-panorama/4248397 (дата обращения: 12.07.2022).

Осенью 2020 г. в одной из больниц Дюссельдорфа (Германия) женщину, нуждающуюся в срочной госпитализации, не приняли в больницу по причине взлома компьютерных систем и отправили в соседний г. Вупперталь, находящийся в 32 км от Дюссельдорфа. В связи с тем,что время для оказания помощи было упущено, пациентка скончалась. В течение недели компьютерные системы выходили из строя, из-за чего пациентов направляли в другие госпитали, плановые операции были отменены[1].

Достаточно часто в процессе противоправных действий умысел злоумышленников направлен на получение имущественных благ, руководствуются они при этом корыстными мотивами. Подобные криминальные посягательства приводят к тому, что ряд медицинских учреждений может прекратить оказывать прием гражданам, что в свою очередь может стать причиной тяжких негативных последствий, как в последнем приведенном случае. Несомненно, стоит предполагать возможность неправомерного доступа и к сложному медицинскому оборудованию, например, кардиостимулятору, который может привести к электрошоку пациента, опасному для жизни.

2. Неправомерный доступ к компьютерной информации, повлекший хищение персональных данных пациентов (сведений, составляющих медицинскую тайну) или ограничение доступа к ним («блокировка»).

Приведем пример, наглядным образом иллюстрирующий угрозу информационной безопасности персональных данных пациентов в сфере здравоохранения. Так, в 2020 г. злоумышленники получили доступ к данным патологоанатомического отделения Свердловского областного онкологического диспансера, из-за чего пациенты остались без результатов биопсии. Указанные сведения были необходимы врачам, так как без них было невозможно назначить лечение. Злоумышленники требовали 80 тыс. рублей за разблокировку данных[2].

Область здравоохранения привлекает злоумышленников в связи с тем, что в последние годы данная отрасль переходит на хранение всего массива информации (истории болезней, результаты анализов, адреса, телефоны, номера полисов обязательного медицинского страхования пациентов и иные сведения) в цифровом виде, что, несомненно, удобно для граждан-пациентов и больниц. Однако подобное обстоятельство одновременно породило серьезную проблему информационной безопасности рассматриваемой сферы. Неправомерный доступ к указанным данным может служить основой совершения иных уголовно наказуемых деяний: мошенничества, вымогательства. Наличие подобных сведений позволяет лицам обмануть родственников пациентов. Лица с антисоциальными наклонностями, получая доступ к медицинским картам пациента, могут вносить в них ложные данные, а после шантажировать пациентов распространением сведений, к примеру, о их заболеваниях и т. д. Кроме того, интерес для подобной категории граждан представляет информация о счетах за оказанные медицинские услуги, которую они могут использовать, к примеру, для оценки объема денежных средств, имеющихся у пациентов клиник. Особенно ценными являются сведения о различных научных исследованиях, ведущихся в медицинском центре (к примеру, сведения о разработанной вакцине от новой коронавирусной инфекции (COVID-2019).

3. Неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, – учреждении системы здравоохранения.

---

[1] Хакерская атака на больницу в Германии привела к смерти пациентки // Газета.ру. URL: http://mt.gazeta.ru/blog/43173373428/Hakerskaya-ataka-na-bolnitsu-v-Germanii-privela-k-smerti-patsien (дата обращения: 12.07.2022).

[2] Вирус лишил свердловский онкоцентр доступа к анализам больных. Хакерскую атаку посчитали случайной // 360ТВ. URL: https://360tv.ru/news/tekst/virus-lishil-sverdlovskij-onkotsentr/ (дата обращения: 12.07.2022).

К примеру, медицинская сестра одной из больниц вносила сведения о гражданах, привитых против новой коронавирусной инфекции (COVID-19) в Федеральной регистр. По просьбе гражданки она внесла в систему недостоверные сведения о прохождении ею вакцинации двухкомпонентным препаратом. Однако внесение заведомо ложных сведений создает угрозу жизни и здоровью других людей. В отношении медицинской сестры было возбуждено уголовное дело по признакам состава преступления, предусмотренного ч. 4 ст. 274[1] Уголовного кодекса Российской Федерации (далее – УК РФ)[1].

Изучение опубликованных материалов свидетельствует о том, что противоправные посягательства осуществляются в основном с целью получения денежных средств или криптовалюты за расшифровку данных или предоставление доступа к заблокированной информации.

Подобные факты уже не будоражат общественность, а наоборот свидетельствуют о необходимости изучения состояния системы информационной безопасности учреждений здравоохранения. Кибератаки могут повлечь причинение колоссального ущерба: начиная от блокирования доступа к цифровым картам пациентов, заканчивая – смертью пациентов, так как медицинское оборудование (кардиостимуляторы, рентгены и т. д.) подключено к информационно-телекоммуникационной сети. Оставшись без сведений, содержащихся в медицинских картах пациентов, работники системы здравоохранения лишены возможности полноценно наблюдать за здоровьем граждан.

Стоит отметить, что согласно Федеральному закону от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[2] многие учреждения системы здравоохранения (как государственные, так и юридические лица и индивидуальные предприниматели) являются субъектами критически важной информационной инфраструктуры Российской Федерации, которым принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления (далее – объекты КИИ), именно поэтому с учетом общественной важности системы здравоохранения, от которой зависит жизнь и здоровье граждан, особое значение в этом ключе отдается мерам уголовно-правовой охраны общественных отношений от преступных посягательств. Федеральным законом от 26 июля 2017 г. № 194-ФЗ 28 глава «Преступления в сфере компьютерной информации» УК РФ была дополнена ст. 274[1] УК РФ, направленной на охрану особой разновидности, с точки зрения законодателя, компьютерной информации – критической информационной инфраструктуры Российской Федерации (далее – КИИ). В соответствии с положениями действующей правовой системы России объект КИИ подлежит категорированию и ему присваивается соответствующая категория значимости (первая, вторая или третья) либо не присваивается категория, в случае если он не соответствует категориям значимости.

Однако интересно заметить тот факт, что УК РФ не полностью учитывает положения законодательства, регулирующего эту сферу, так как не устанавливает дифференциацию уголовной ответственности, исходя из значимости категории объекта КИИ. Получается, что уголовный закон охраняет все объекты КИИ, включая те, которые не имеют категории, несмотря на то, что они не соответствуют показателям значений,

[1] Три уголовных дела возбуждено в Дагестане по факту незаконной реализации документов о прохождении вакцинации // Зори Табасарана. URL: https://zoritabasarana.ru/rubriki/news/vakcina/item/19016-tri-ugolovnykh-dela-vozbuzhdeno-v-dagestane-po-faktu-nezakonnoj-realizatsii-dokumentov-o-prokhozhdenii-vaktsinatsii (дата обращения: 12.07.2022).

[2] О безопасности критической информационной инфраструктуры Российской Федерации: федеральный закон от 26 июля 2017 г. № 187-ФЗ // Собрание законодательства Российской Федерации. 2017. №. 31 (ч. I). Ст. 4736.

установленных отраслевым законом. В связи с этим, полагаем, что на данный момент является существенным упущением с точки зрения законодателя привлечение к ответственности по ст. 274[1] УК РФ в случае неправомерного воздействия на объект КИИ без соответствующей категории. В данном случае лицо должно привлекаться к уголовной ответственности по ст. 274[1] УК РФ только при противоправном воздействии на значимый объект КИИ, то есть на объект которому присвоена одна из категорий значимости. В случае отсутствия у объекта КИИ категории значимости действия виновных следует квалифицировать по ст.ст. 272–274 УК РФ (в зависимости от элементов состава преступления, в том числе описания признаков объективной стороны). С целью недопущения проблем, которые могут возникнуть в процессе правоприменения, предлагаем конкретизировать, что посягательство должно быть совершено исключительно на значимые объекты критической информационной инфраструктуры Российской Федерации, тем самым внести соответствующие изменения в наименование ст. 274[1] УК РФ и в диспозицию уголовно-правовых норм, закрепленных ч.ч. 1–3 ст. 274[1] УК РФ.

Кроме того, хотелось бы обратить внимание также на то, что согласно ч. 5 ст. 274[1] УК РФ преступлением признается деяние, предусмотренное частями 1, 2 и 3, при наступлении общественно опасных последствий в виде наступления тяжких последствий. Помимо этого, категория «тяжкие последствия» как наступившее негативное последствие в результате совершения общественно опасного деяния не раскрывается. Законодатель не установил правила по определению размера тяжести подобного вреда, оставляя это правоохранительным и судебным органам. В связи с этим возникают закономерные вопросы о том, что следует понимать под тяжкими последствиями применительно к данной норме, какие деяния будут влечь привлечение лица к более строгому виду и размеру уголовного наказания.

Кроме того, исходя из законодательного построения уголовно-правовой нормы и того, что данный признак является особо квалифицированным составом преступления, считаем, что «тяжкие последствия» (ч. 5 ст. 274[1] УК РФ) являются более опасным, чем вред, причиняемый критической информационной инфраструктуре Российской Федерации (ч. 2 и 3 ст. 274[1] УК РФ). Следует обратить внимание на то, что в уголовном законодательстве говорится именно о причинении вреда КИИ, что сужает определение негативных последствий и не позволяет их трактовать также широко, как в ч. 5 рассматриваемой нами статьи.

Полагаем, что к тяжким последствиям следует относить непосредственный вред, причиняемый как объектам КИИ, так и деятельности субъектов КИИ. Стоит согласиться с мнением Ю. В. Трунцевского, согласно которому для определения последствий тяжкими нельзя ограничиваться только материальными последствиями [2, с. 104]. Для этого в разъяснении Верховному Суду Российской Федерации по квалификации указанных преступлений для единообразного применения законодательства следует указать, что под тяжкими последствиями следует понимать наступление смерти человека (в том числе двух и более лиц), причинение тяжкого вреда здоровью двум и более лицам, ухудшение состояния здоровья населения, в том числе массовое заболевание, заражение, облучение или отравление людей, причинение крупного или особо крупного ущерба, наступление техногенного или экологического бедствия, чрезвычайной экологической ситуации, ухудшение состояния окружающей среды, создание угрозы безопасности государства, катастрофы или аварии, срыв исполнения поставленных органами публичной власти задач или выполнения боевой задачи, длительное снижение уровня боевой готовности и боеспособности воинских частей и подразделений, вывод из строя боевой техники, а также иные последствия, свидетельствующие о тяжести причиненного вреда.

В связи с тем, что достаточно часто, как нам удалось выяснить, действия виновных направлены на воздействие на информаци-

онную безопасность учреждений здравоохранения с целью хищения имущества, возникла необходимость также рассмотреть вопрос юридической квалификации преступления, предусмотренного ст. 163 УК РФ.

С точки зрения конструкции уголовно-правовой нормы вымогательство характеризуется обязательными способами, отсутствие которых свидетельствует и об отсутствии состава преступления. Однако в условиях массовой цифровизации общества следует говорить об ограниченном описании указанных способов, не позволяющих даже на данный момент достаточно схожие деяния квалифицировать как преступления против собственности. В связи с этим следует уточнить то, что требование передачи имущества, права на имущество или совершение иных действий имущественного характера могут быть осуществлены и под угрозой совершения таких противоправных действий, как уничтожение, блокирование, модификация охраняемой компьютерной информации, в том числе шифрования данных, похищения документов или иных противоправных деяний. Однако все высказанные угрозы могут быть восприняты потерпевшим реально, он в действительности может опасаться и испытывать чувство страха, что повлечет передачу имущества или права на имущество злоумышленнику.

Стоит поддержать мнение некоторых авторов, которые также высказывали точки зрения о необходимости внесения изменений в ст. 163 УК РФ в части уточнения и расширения способов совершения противоправного деяния. Так, М. А. Простосердов предлагает дополнить основной состав вымогательства (ст. 163 УК РФ) таким признаком, как совершение преступления «под угрозой удаления, блокирования либо модификации компьютерной информации, а равно под угрозой иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, которое может причинить существенный вред правам или законным интересам потерпевшего или его близких» [3, с. 143].

Выводы.

1. На сегодняшний момент существует значительное множество угроз безопасности учреждений здравоохранения, ключевыми из которых являются нарушения кибербезопасности. Изменение способов и технологий взаимодействия врачей и пациентов в цифровом пространстве открывает новые возможности совершения преступлений, в том числе умышленное искажение данных, нарушение режима доступа к медицинской тайне [4, с. 150]. В свою очередь, цифровые инновации в здравоохранении становятся неустойчивыми к кибератакам. По мере того, как здравоохранение ускорило процессы цифровой трансформации, особенно из-за пандемии COVID-19, также возросли угрозы кибербезопасности учреждений здравоохранения.

2. На данный момент является существенным упущением с точки зрения законодателя привлечение к ответственности по ст. 274^1 УК РФ в случае неправомерного воздействия на объект КИИ без соответствующей категории. В данном случае лицо должно привлекаться к уголовной ответственности по ст. 274^1 УК РФ только при противоправном воздействии на значимый объект КИИ, то есть на объект, которому присвоена одна из категорий значимости. В случае отсутствия у объекта КИИ категории значимости действия виновных следует квалифицировать по ст.ст. 272–274 УК РФ (в зависимости от элементов состава преступления, в том числе описания признаков объективной стороны).

3. К тяжким последствиям как к последствиям, которые указаны в ч. 5 ст. 274^1 УК РФ, следует относить непосредственный вред, причиняемый как объектам КИИ, так и деятельности субъектов КИИ. Для этого в разъяснении Верховному Суду Российской Федерации по квалификации указанных преступлений для единообразного применения законодательства следует указать, что следует понимать под тяжкими последствиями.

4. Следует внести изменения в диспозицию ч. 1 ст. 163 УК РФ путем расшире-

ния способов совершения преступления, а именно «под угрозой совершения иного преступления в отношении потерпевшего или его близких», что позволит учитывать иные противоправные деяния в качестве вымогательства и не избегать злоумышленникам привлечения к уголовной ответственности.

СПИСОК ИСТОЧНИКОВ

1. Ищенко Е. П., Кручинина Н. В. Высокие технологии и криминальные вызовы // Всероссийский криминологический журнал. № 2. 2022. С. 199–206.

2. Трунцевский Ю. В. Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев и эксплуатантов // Журнал российского права. № 5. 2019. С. 99–106.

3. Простосердов М. А. Экономические преступления, совершаемые в киберпространстве. М., 2017. 198 с.

4. Грачева Ю. В., Коробеев А. И., Маликов С. В., Чучаев А. И. Уголовно-правовые риски в сфере цифровых технологий: проблемы и предложения // Lex Russica. № 1 (158). 2020. С. 145–159.

REFERENCES

1. Ishchenko E. P., Kruchinina N. V. High technologies and criminal challenges // All-Russian Journal of Criminology. No. 2. 2022. P. 199–206. (In Russ.)

2. Truntsevsky Yu. V. Unlawful impact on critical information infrastructure: criminal liability of its owners and operators // Journal of the Russian Law. No. 5. 2019. P. 99–106. (In Russ.)

3. Prostoserdov M. A. Economic crimes committed in cyberspace. M., 2017. 198 p. (In Russ.)

4. Gracheva Yu. V., Korobeev A. I., Malikov S. V., Chuchaev A. I. Criminal law risks in the field of digital technologies: problems and suggestions // Lex Russica. № 1 (158) 2020. P. 145–159. (In Russ.)

Информация об авторе:
А. А. Шутова, кандидат юридических наук.

Information about the author:
A. A. Shutova, Candidate of Law.

Статья поступила в редакцию: 04.08.2022; одобрена после рецензирования: 23.10.2022; принята к публикации: 15.09.2023.

The article was submitted: 04.08.2022; approved after reviewing: 23.10.2022; accepted for publication: 15.09.2023.