УДК 343.45

К вопросу об уголовной ответственности за незаконное получение и распространение сведений о пациенте, представленных в электронной форме

Ефремова М.А.
Доктор юридических наук, доцент,
заведующий кафедрой уголовно-правовых дисциплин
Казанского филиала Российского государственного
университета правосудия

Каюмова А.А.
Преподаватель кафедры уголовно правовых дисциплин
Казанского филиала Российского государственного
университета правосудия

Статья посвящена проблеме защиты конфиденциальной информации о пациенте, хранящейся в электронной форме. Применение современных технологий для обработки и хранения данных о пациенте неизбежно ставит под угрозу их сохранность и конфиденциальность. Актуальность данного исследования заключается в стремительном росте процента преступлений с использованием информационных и цифровых технологий и отсутствия значительной положительной динамики в их раскрываемости. В статье рассматриваются показатели основанные, как на отечественной статистике, так и на данных иностранных государств. Приводятся существующие проблемы в сложности расследования такого рода преступлений и возможные пути их решения.

Ключевые слова: киберпреступления, частная жизнь, компьютерная информация, медицинские учреждения, пациент, информационные технологии

Информационные технологии с каждым днем все больше становятся неотъемлемой частью жизни граждан, а также интенсивно вовлекаются в деятельность государства. Стремительный темп их развития способствует тому, что преступники все чаще используют их потенциал в своей противоправной деятельности.

Современные информационные технологии используются не только для незаконного публичного распространения конфиденциальной информации, но и в других областях, таких как распространение наркотических веществ, продажа оружия, незаконное изъятие и продажа органов, мошенничество и многое другое.

Ввиду того, что информационные технологии активно внедрены и в сферу здравоохранения, в частности для обработки данных в цифровом виде, большинство современных частных медицинских организаций давно отказалась от традиционной бумажной медицинской карты пациента. Ожидается, что в 2024 г. государственные учреждения здравоохранения перейдут на электронные медицинские карты. Вызывает опасения возможность их утечки и распространения, что может привести к неблагоприятным последствиям.

Обращаясь за медицинской помощью, пациент неизбежно предоставляет данные о себе медицинской организации, заключающие в себе сведения не только о личности, такие как фамилия, имя отчество, дата рождения, место проживания, но и информацию о состоянии здоровья пациента и оказываемой ему медицинской помощи, в том числе данные о на-

личии заболевания, его диагнозе, прогнозе, способах диагностики, лечения и профилактики, риски, связанном с медицинским вмешательством.

Федеральный закон от 21 ноября 2011 г. № 323–ФЗ «Об основах охраны здоровья граждан в Российской Федерации» [1] в ст. 13 содержит положения о необходимости соблюдения врачебной тайны. В частности, закон прямо указывает, что сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении, составляют врачебную тайну.

Не допускается разглашение сведений, составляющих врачебную тайну, в том числе после смерти человека, лицами, которым они стали известны при обучении, исполнении трудовых, должностных, служебных и иных обязанностей.

Если подобная информация о пациенте станет достоянием третьих лиц, то она может быть использована для вмешательства в частную жизнь и совершения иных противоправных действий.

Опасность такого рода преступлений связана и с осложнением лечения, особенно тяжелобольных пациентов. Так, например, осенью 2020 г. была взломана база данных, где хранились результаты анализов пациентов онкологического диспансера в Екатеринбурге. В результате информационной атаки на екатеринбургский диспансер несколько сотен пациентов остались без результатов биопсии, что привело к осложнению их лечения и даже к нескольким смертельным исходам.

Приведенный пример показывает, что помимо утечки информации о заболеваниях и личных данных, подобного рода деяния ставят под угрозу не только тайну частной жизни гражданина, но непосредственно и их жизнь, и здоровье.

Весной 2022 г. стало известно о масштабной утечке более 300 Гб персональных данных клиентов лаборатории «Гемотест», включающих результаты анализов на ВИЧ. По итогу разбирательства лаборатория была привлечена к ответственности по ч. 1 ст. 13.11 КоАП РФ с назначением штрафа в размере 60 тысяч рублей [2]. Виновных же установить не удалось.

Согласно статистике, в 2022 г. наблюдался рост «утечек» данных: доля умышленно украденных баз, содержащих информацию о российских пациентах, увеличилась с 58,3 до 87,5 %. В два с лишним раза по сравнению с 2021 г. выросла и доля инцидентов в сфере здравоохранения с участием киберпреступников.

Схожую картину мы можем наблюдать во всем мире. Так, например, в США в 2019 г. было официально выявлено более 500 случаев утечки медицинских данных пациентов. В целом с 2017 г. по 2021 г. в США было потрачено более 65 млрд долл. для устранения и предупреждения преступлений, связанных с хищением личных данных пациентов и результатами их обследования.

Для получения доступа к базам данных преступники используют *DDoS* атаки, которые могут быть совершены трансгранично, то есть с территории другой страны.

Еще одним весьма распространенным способом получения данных из медицинских учреждений является фишинг. Злоумышленники отправляют письмо, содержащее вредоносную ссылку, переход по которой позволяет получить доступ к базе данных о пациентах.

Ввиду того, что не все медицинские организации уделяют достаточное внимание вопросам кибербезопасности, преступники активно используют вредоносное программное обеспечение, так называемые «компьютерные вирусы» и программы-шпионы, которые также позволяют собирать и накапливать конфиденциальные данные.

Подобного рода обстоятельства порождают сложности раскрытия таких преступлений, так как зачастую злоумышленники скрывают свое местонахождение, путем неоднократного изменения IP-адресов. Это затрудняет работу правоохранительных органов, замедляет процесс расследования данной категории деяний.

Нельзя не отметить, что зачастую сами медицинские учреждения опасаются за свою репутацию, особенно если речь идет о частных клиниках, ввиду утечки данных о пациентах.

Цифровизация здравоохранения еще будет набирать обороты. В частности, все более широкое распространение в указанной сфере получили технологии искусственного интеллекта. Они применяются для проведения операций, для анализа клинических данных и назначения лечения. Следовательно, все больше данных о пациентах будет представлено в электронной форме, что, в свою очередь, требует обеспечения надлежащего уровня их защиты.

Обращаясь к вопросу о проблемах квалификации анализируемых деяний, следует отметить, что сведения о пациенте, хотя и представленные в электронной форме, составляют тайну частной жизни. Тайна личной и семейной жизни человека является своеобразным «фундаментом», на котором воздвигнуто право на неприкосновенность частной жизни. Уголовная ответственность за незаконное собирание или распространение сведений о частной жизни предусмотрена ст. 137 УК РФ.

В соответствии с п. 16 Постановления Пленума Верховного Суда РФ от 15.12.2022 г. № 37, «если действия, предусмотренные ст.ст. 272–274.1 УК РФ, выступали способом совершения иных преступлений (например, модификация охраняемой законом компьютерной информации производилась с целью нарушения авторских или смежных прав, наруше-

ния неприкосновенности частной жизни, тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений либо неправомерный доступ к ней осуществлялся с целью совершения кражи или мошенничества), они подлежат квалификации по совокупности с преступлениями, предусмотренными соответствующими статьями Уголовного кодекса Российской Федерации». Таким образом, незаконное собирание или распространение сведений о пациенте в электронной форме должно быть квалифицировано по совокупности ст. 137 УК РФ и ст.ст. 272–274.1 УК РФ, в зависимости от способа получения сведений.

Подводя итог вышеизложенному, следует отметить, что незаконное завладение данными о пациентах представляет серьезную угрозу как для самих пациентов, так и для медицинских организаций. Поэтому представляется необходимым не только реагировать на факты утечек, но на предотвращение и профилактику подобных инцидентов.

Литература:

1. Федеральный закон от 21.11.2011 г. № 323–ФЗ «Об основах охраны здоровья граждан в Российской Федерации» // Российской газета. – 2011. – № 263.
2. Постановление мирового судьи судебного участка № 281 района Вешняки города Москвы по ч. 1 ст.13.11 КоАП РФ № 12-2741/2022. – URL: https://mos-gorsud.ru/rs/perovskij/services/cases/appeal-admin/details/acc111a1-08cf-11ed-9eae-af1c53b4b591?ysclid=lt1y0y4j7q312791109 (дата обращения: 26.02.2024).
3. Постановление Пленума Верховного Суда РФ от 15.12.2022 г. №37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» // Бюллетень Верховного Суда РФ. – 2023. – № 3.

On the Issue of Criminal Liability for the Illegal Receipt and Dissemination of Information About a Patient Submitted in Electronic Form

Efremova M.A., Kayumova A.A.
Kazan branch The Russian State University of Justice

The article is devoted to the problem of protecting confidential patient information stored in electronic form. The use of modern technologies for processing and storing patient data inevitably jeopardizes their safety and confidentiality. The relevance of this study lies in the rapid increase in the percentage of crimes using information and digital technologies and the lack of significant positive dynamics in their detection rate. The article discusses indicators based on both domestic statistics and data from foreign countries. The existing problems in the complexity of investigating this type of crime and possible ways to solve them are presented.

Key words: cybercrimes, private life, computer information, medical institutions, patient, information technology