УДК 004.056.5 DOI 10.37468/2307-1400-2024-4-60-76

ВЗАИМОСВЯЗЬ ИНФОРМАЦИОННОЙ, ЭКОНОМИЧЕСКОЙ И СОЦИАЛЬНОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ЗДРАВООХРАНЕНИЯ

Варзин Сергей Александрович [1,2]
Матвеев Владимир Владимирович [3]

[1] Санкт-Петербургский государственный университет, Санкт-Петербург, Россия

[2] Санкт-Петербургский медико-социальный институт, Санкт-Петербург, Россия

[3] Финансовый университет при Правительстве РФ (Санкт-Петербургский филиал), Санкт-Петербург, Россия

АННОТАЦИЯ

Актуальность настоящего исследования обусловлена значительным ростом киберугроз в сфере здравоохранения, усилившимся после пандемии COVID-19, и высокой уязвимостью медицинских учреждений перед атаками, как со стороны внешних злоумышленников, так и внутренних нарушителей. Утечки конфиденциальной информации в здравоохранении несут не только экономический и имиджевый ущерб, но и прямую угрозу здоровью и жизни пациентов.

В статье представлен всесторонний анализ состояния информационной безопасности в системе здравоохранения на основе статистики инцидентов за 2023–2024 годы. Авторы выделяют основные источники угроз – хакерские атаки, небрежность и злонамеренные действия персонала, а также недостаточную цифровую зрелость учреждений, проявляющуюся в устаревшем программном обеспечении и нехватке специалистов по информационной безопасности. Особое внимание уделено экономическим последствиям инцидентов информационной безопасности и международной практике регулирования, включая сравнительный анализ санкционных механизмов в России и за рубежом.

Научная новизна исследования заключается в комплексном подходе к оценке взаимосвязи информационной, экономической и социальной безопасности в контексте цифровизации системы здравоохранения.

Практическая значимость работы заключается в формировании основ для разработки эффективных стратегий управления рисками в области информационной безопасности медицинских организаций, включая обучение персонала, внедрение мониторинга действий сотрудников и повышение штрафных санкций за нарушения.

Ключевые слова: информационная безопасность, здравоохранение, кибератаки, утечки данных, персональные данные, экономический ущерб.

THE RELATIONSHIP BETWEEN INFORMATION, ECONOMIC AND SOCIAL SECURITY IN THE HEALTHCARE SYSTEM

Varzin Sergey A. [1,2]
Matveev Vladimir V. [3]

[1] St. Petersburg State University, St. Petersburg, Russia

[2] St. Petersburg Medical and Social Institute, St. Petersburg, Russia

[3] Financial University under the Government of the Russian Federation (St. Petersburg branch), St. Petersburg, Russia

ABSTRACT

The relevance of this study is due to the significant increase in cyber threats in the healthcare sector, which has intensified after the COVID-19 pandemic, and the high vulnerability of medical institutions to attacks from both external and internal attackers. Leaks of confidential information in healthcare not only cause economic and image damage, but also pose a direct threat to the health and lives of patients.

The article presents a comprehensive analysis of the state of information security in the healthcare system based on incident statistics for 2023-2024. The authors highlight the main sources of threats - hacker attacks, negligence and malicious actions of personnel, as well as insufficient digital maturity of institutions, manifested in outdated software and a shortage of information security specialists. Particular attention is paid to the economic consequences of information security incidents and international regulatory practices, including a comparative analysis of sanctions mechanisms in Russia and abroad.

The scientific novelty of the study lies in the integrated approach to assessing the relationship between information, economic and social security in the context of the digitalization of the healthcare system. The practical significance of the work lies in the formation of the basis for the development of effective risk management strategies in the field of information security of medical organizations, including staff training, the introduction of monitoring of employee actions and increasing penalties for violations.

Keywords: information security, healthcare, cyber attacks, data leaks, personal data, economic damage.

Введение

С началом пандемии COVID-19 сфера здравоохранения стала одной из самых привлекательных киберпреступников. Это относится как к учреждениям здравоохранения, так и предприятиям фармакологической промышленности.

Последствия утечки конфиденциальных данных могут носить различный характер: материальный, имидживый, снижение эффективности экономической деятельности вплоть до банкротства, а в здравоохранении – потерю здоровья пациентов и в некоторых случаях даже приводить к летальным исходам [1, 2].

Утечки конфиденциальной информации неслучайны. В модели рентной экономики образовался рынок, в том числе информационных данных, где данные стали товаром и одним из факторов ренты [3, 4].

Влияние кибератак на здоровье и жизнь пациентов можно продемонстрировать на примере отчета компании Proofpoint (штат Калифорния, США) [5]. Совместно с Ponemon Institute было проведено исследование влияния угроз кибербезопасности на оказание медицинской помощи, в ходе которого был опрошен 641 специалист из сферы здравоохранения. 89% респондентов заявили, что их организации подверглись кибератакам за 2022 г. Количество атак составило в среднем 43 инцидента за год на каждое учреждение здравоохранения.

Материальный ущерб от кибератак в среднем оценили в $4,4 млн, включая прямые и косвенные затраты на каждый инцидент информационной безопасности (ИБ). Наибольшей статьей затрат респонденты назвали простой в работе и перебой в оказании услуг пациентам. Учреждения здравоохранения оценили эти потери в среднем в $1,1 млн.

Помимо материального ущерба самый негативный сценарий – это влияние кибератак на реальный мир, когда последствия ИБ-инцидента становятся непосредственной угрозой здоровью и жизни людей. 70% опрошенных признали, что кибератаки повлияли на уход за больными: в результате пациентам не делали необходимые процедуры или анализы, что в половине случаев привело к ухудшению течения заболевания, появлению осложнений, а также увеличению срока госпитализации.

Кибератаки повлияли на количество летальных исходов: парализация систем в результате различных типов атак привела к росту смертности пациентов. Наиболее разрушительны в этом отношении оказались атаки с помощью программ-вымогателей – их влияние на уровень смертности отметили 24% опрошенных.

При этом исследование показало, что медицинские учреждения слабо готовы к отражению кибератак: основное финансирование медицинских организаций направлено на уход за пациентами, что в итоге ограничивает бюджет на обеспечение безопасности.

Наиболее уязвимы для кибератак медицинские устройства, поскольку работают на устаревшем программном обеспечении и не имеют актуальных функций, обеспечивающих их безопасность. Проблема по обеспечению кибербезопасности медицинских учреждений – это отсутствие ИБ-специалистов и неосведомленность собственных сотрудников.

По сути, сегодня киберпреступники имеют власть над жизнью людей, и кибератаки на медицинские организации могут привести к губительным последствиям для пациентов. Поэтому, как минимум, необходимо обучение сотрудников медицинских учреждений основам обеспечения ИБ, а также мониторинг их действий для снижения уровня внутренних нарушений и, как следствие, снижения ИБ-рисков для организаций в целом.

Таким образом, целью данного исследования является оценка безопасности в системе здравоохранения на основе комплексного анализа состояния информационной безопасности, угроз и последствий утечек конфиденциальной информации в системе здравоохранения.

Анализ состояния безопасности в системе здравоохранения

В соответствие со статистическими данными, общее количество утечек информации ограниченного доступа в мире за январь-сентябрь

2024 г. выросло более чем вдвое, а в России более чем на 80% по сравнению с аналогичным периодом 2023 г. На первый взгляд ситуация с защитой данных в медицинских учреждениях выглядит значительно лучше, чем в ряде других отраслей (рисунок 1). Но это обманчивое впечатление.

За девять месяцев 2024 г. (январь-сентябрь) в мире зарегистрировано 256 утечек конфиденциальной информации из сферы здравоохранения. Это на 5,9% меньше, чем за аналогичный период 2023 г. Количество утечек конфиденциальной информации из сферы здравоохранения в России за девять месяцев 2024 г. составило 8, что на треть меньше, чем в январе-сентябре 2023 г. [6].

Анализ показывает, что сохраняется достаточно высокий уровень хакерской активности после разгара пандемии COVID-19 (2020-2021 годы), когда многие злоумышленники не стали присоединяться к некоему этическому кодексу отдельных группировок [6], а вместо этого принялись атаковать медучреждения, до предела загруженные спасением жизней больных с опасной инфекцией. Естественно, в такой ситуации клиники не могли уделять должного внимания кибербезопасности.

В то же время, складывается мнение, что несмотря на определенные успехи в цифровизации медицины как в мире, так и в России, соответствующие учреждения и сейчас не уделяют должного внимания вопросам ИБ. Зачастую это направление финансируется по остаточному принципу, и даже крупные клиники часто не имеют выделенных специалистов по ИБ. Из этого можно предположить, что в больницах, поликлиниках и медицинских лабораториях существенно вырос уровень латентности инцидентов.

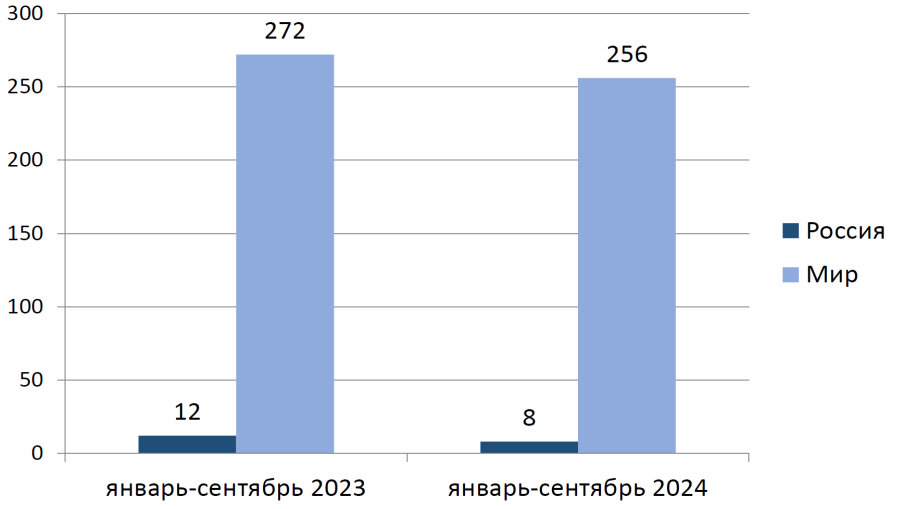

Рисунок 1 – Число утечек в сфере здравоохранения (Мир - Россия, январь-сентябрь 2024 г. - январь-сентябрь 2024) г.

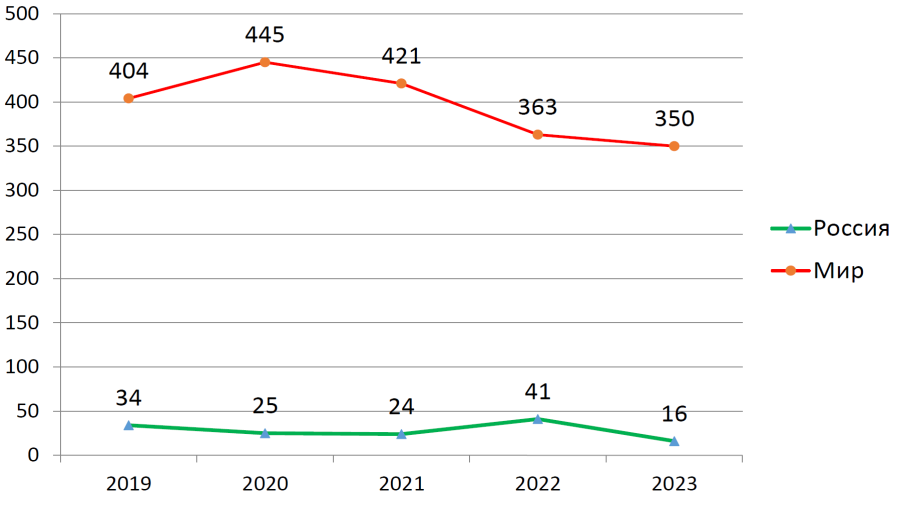

Рисунок 2 – Число утечек данных в здравоохранении

Существенное снижение количества зафиксированных в публичном пространстве утечек данных из сферы здравоохранения начало снижаться вскоре после острой фазы пандемии. В мире это произошло даже раньше, чем в России (см. рисунок 2).

Персональные данные пациентов, истории болезней и другая конфиденциальная информация представляют немалый интерес, как для хакеров, так и для внутренних нарушителей. Данные на бумажных носителях в медицинских учреждениях нередко компрометируются по небрежности персонала или являются источником преднамеренной утечки данных внутренними нарушителями.

О серьезных проблемах с защитой информации в национальных системах здравоохранения косвенно говорит резкий рост количества утекших записей – за девять месяцев 2024 г. в мире утекло без малого 150 млн записей персональных данных, то есть в три с лишним раза больше, чем за январь-сентябрь предыдущего года (рисунок 3).

Из них в России из медицинских учреждений зафиксирована утечка более 31 млн записей. Однако, почти весь этот объем записей за исследованный период пришелся на инцидент в сети лабораторий «Гемотест» [7]. Позднее эта компания была оштрафована на 60 тыс. рублей (менее $1 тыс.). Следует отметить, что в России размер штрафов за утечки информации пока скорее символический и вряд ли мотивирует компании к полному соблюдению мер ИБ и укреплению систем защиты информации.

На продаже в подпольном сегменте сети появилась база данных клиентов «Гемотеста», в которой 31 млн строк. В ней содержатся ФИО, дата рождения, адрес, телефон, электронная почта, серия и номер паспорта, номера страховки и СНИЛС пациентов. Предположительно данные были получены в результате хакерской атаки на ИТ-систему компании.

Опыт США указывает, что в медицинском страховании и учреждениях здравоохранения применяются исключительно цифровые технологии. Там уже много лет действует законодательство о защите персональных данных пациентов HIPAA [8], HITECH [9]. Штрафы за нарушения требований этих законов зачастую исчисляются сотнями тысяч, а то и миллионами долларов.

Так, например, компания EyeMed, предоставляющая услуги диагностики и лечения глазных заболеваний, выплатит $600 тыс. в результате потери конфиденциальной информации более 2 млн. пациентов [10]. Хакерам удалось взломать учетную запись электронной почты EyeMed и похитить такие персональные данные, как имена, почтовые адреса, номера социального страхования, а также сведения о лечении пациентов.

Таким образом, EyeMed заплатила примерно в 600 раз больше за потерю данных 2 млн пациентов, чем «Гемотест» за утечку информации более 30 млн клиентов лабораторий.

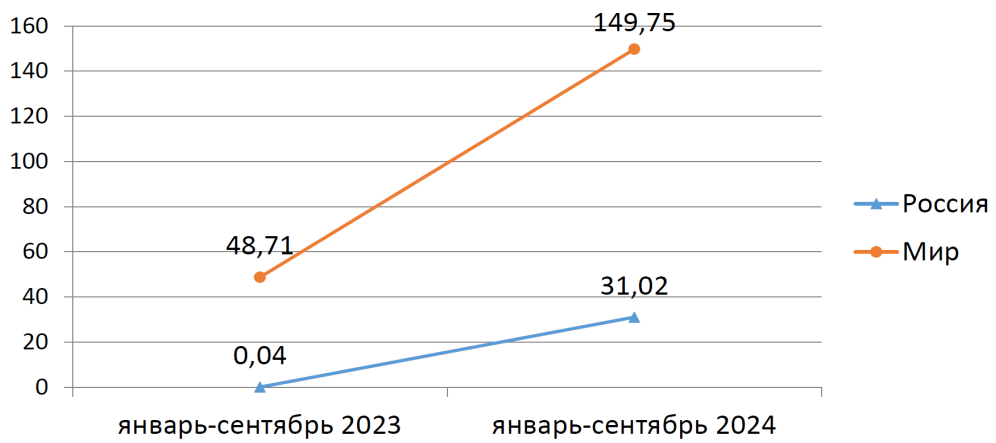

Рисунок 3 – Число утекших записей в здравоохранении, млн (Мир - Россия, Январь-сентябрь 2023 г. - январь-сентябрь 2024 г.)

Исходя из анализа активности теневого рынка данных, даже с учётом повторений и поддельных баз, можно предположить, что количество утечек персональных данных из медучреждений значительно выше, чем дает изучение публичных инцидентов.

В 2024 г. в мире существенно выросла доля утечек информации в результате действий внешних нарушителей. Здравоохранение здесь не исключение. На рисунке 4 показано, что в январе-сентябре 2024 г. в мировом здравоохранении 94% случаев компрометации данных пришлись именно на внешних нарушителей, в то время как в российском – 75% случаев.

Таким образом, несмотря на некоторое снижение количества утечек данных за изученный период, можно говорить о высокой активности хакеров. В то же время, вероятно, большой пласт утечек внутреннего характера оказался в серой зоне, то есть не был зафиксирован из-за слабости систем защиты во многих медицинских учреждениях.

Резкое снижение доли утечек внутреннего характера, то есть совершенных сотрудниками, – это сигнал по росту латентности инцидентов. В январе-сентябре 2022 г. из-за действий персонала произошло 44% утечек в мировом здравоохранении и почти 90% в российском. Но уже третий год эта доля падает, и дело здесь явно не в опережающих темпах роста количества утечек по вине внешних злоумышленников. Внутренние нарушения стали реже выявляться, а на многие случаи небрежного обращения персонала с данными пациентов (выброшенные карты из архива, неконтролируемый доступ к электронной истории болезни и т.д.), вероятно, уже перестали обращать на себя внимание. Как следствие, стало меньше подобных сообщений в СМИ.

Так, например, неизвестный хакер выставил на продажу в Даркнете персональные данные почти 39 млн пациентов. Предположительно, данные пациентов были похищены в результате взлома сети одного из крупнейших в Таиланде медицинских учреждений – больницы Сирирадж [11]. Покупатель может получить такую конфиденциальную информацию, как имена, адреса, номера удостоверений личности, номера телефонов, половая принадлежность, даты рождения и т.д.

Таким образом, из-за высокой хакерской активности и, предположительно, повышенной латентности утечек по вине внутренних нарушителей в общем распределении утечек публичного характера их доля снизилась в несколько раз буквально в течение года.

Одновременно с резким ростом нарушений внешнего характера в здравоохранении выросла доля умышленных утечек как внешних, так и внутренних (рисунок 5).

Здесь можно выдвинуть две гипотезы:

– во-первых, информация из клиник стано-

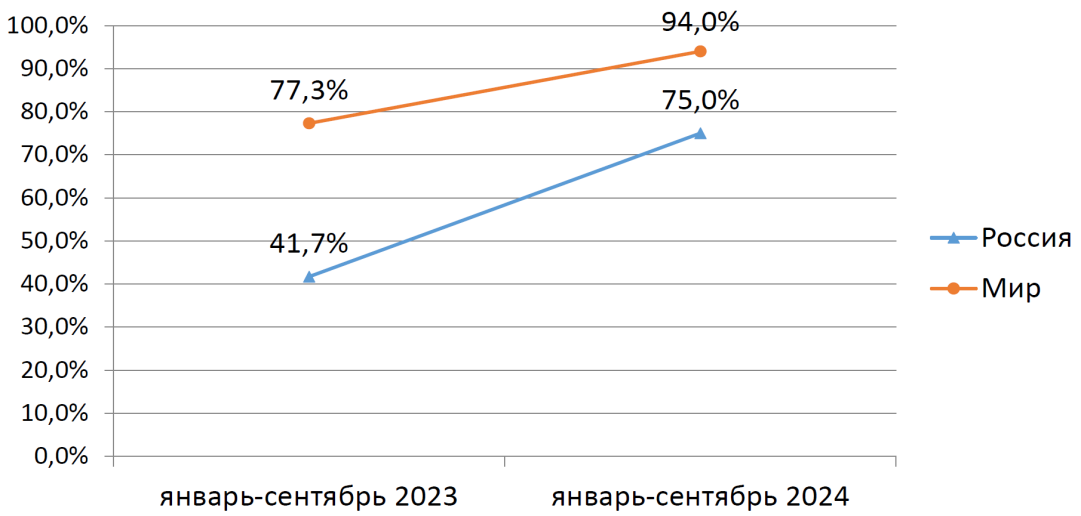

Рисунок 4 – Динамика доли утечек в здравоохранении вследствие внешнего воздействия (Мир - Россия, январь-сентябрь 2023 г. - январь-сентябрь 2024 г.)

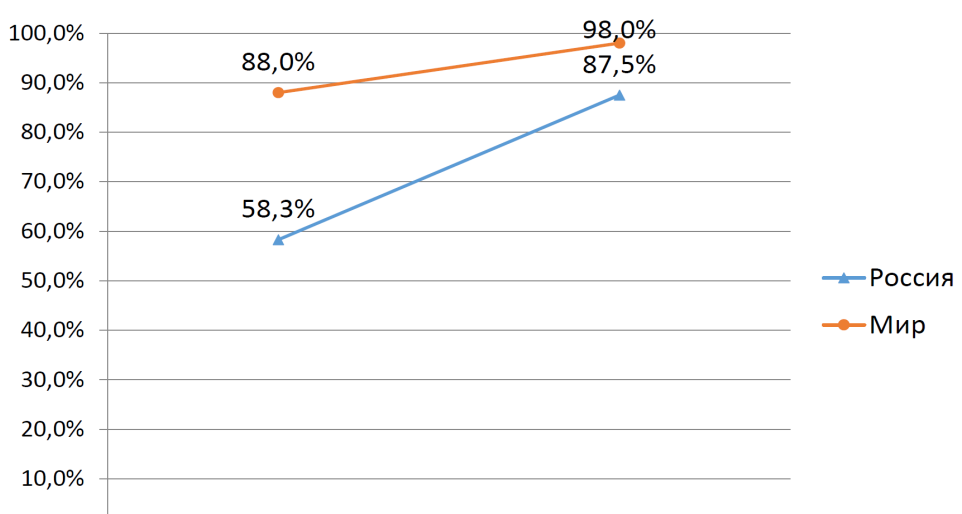

Рисунок 5 – Доля умышленных нарушений в здравоохранении (Мир - Россия, январь-сентябрь 2023 г. - январь-сентябрь 2024 г.)

вится все более ликвидным товаром на черном рынке данных и удобной основой для мошеннических действий;

– во-вторых, вследствие роста кибератак и обращения основного внимания на них, можно сделать предположение, что резко выросла латентность нарушений, прежде всего внутренних.

Вероятно, системы контроля за персоналом если и присутствуют в медучреждениях (в основном в крупных), то отстают по уровню реализации политик ИБ от широкого спектра актуальных угроз, в том числе новых. В период пандемии, когда вопросам ИБ в здравоохранении объективно уделялось недостаточно внимания, возможности предупреждения и обнаружения нарушений стали еще более ограниченными.

Пример. Поставщик медицинских услуг Shields Health Care Group из штата Массачусетс сообщил, что в результате кибератаки могли быть затронуты персональные данные примерно 2 млн пациентов. Злоумышленники похитили такую конфиденциальную информацию, как полные имена пациентов, номера социального страхования (SSN), данные о диагнозах, а также платежную информацию, номера медицинских карт, ID пациентов, даты рождения, адреса и сведения о лечении [12].

Посмотрим на распределение внутренних нарушений по характеру умысла. Среди утечек информации внутреннего характера, сведения о которых попали в открытые источники, в мире доминируют умышленные нарушения (см. рисунок 6), то есть сотрудники умышленно разглашают или распространяют персональные данные пациентов. Существенный рост их доли может свидетельствовать о давно назревшей проблеме контроля за персоналом медучреждений, имеющих доступ к персональным данным пациентов и другой конфиденциальной информации. Это видно даже по той «верхушке айсберга», которая доступна взгляду общественности.

Пример. 8 лет лишения свободы могут получить работники скорой помощи в Оренбурге, которые «сливали» информацию ритуальным агентствам. Об этом рассказали в региональном УФСБ. По данным ведомства, речь идет о двух жителях областного центра. Один из них является сотрудником ГБУЗ «ООКССМП», который работал специалистом по защите информации. По версии следствия мужчина установил вредоносную программу, которая была подключена к базе данных о вызовах в скорую. Полученные таким образом данные пересылались в чат в Telegram, в котором состояли агенты ритуальных услуг [13].

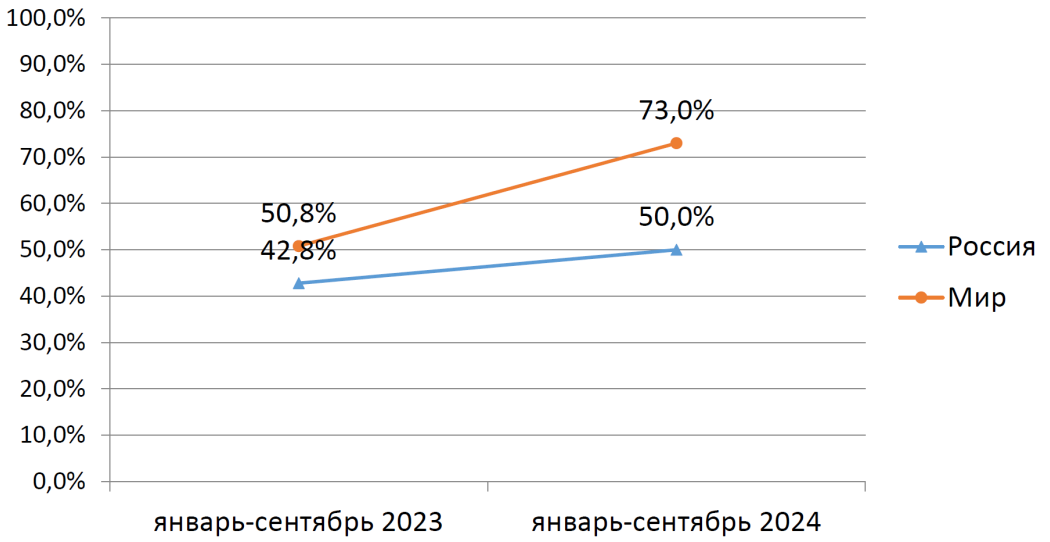

Рисунок 6 – Доля умышленных нарушений внутреннего характера в здравоохранении: Мир - Россия, январь-сентябрь 2023 г. - январь-сентябрь 2024 г.

Анализ источников утечек конфиденциальной информации

Распределение утечек конфиденциальной информации в медучреждениях по типу виновников подкрепляет гипотезу о большой активности хакеров и серьезных проблемах с выявлением инцидентов по вине персонала (см. рисунок 7, 8). Доля хакеров в 2024 году резко выросла, тогда как случаев утечек информации из-за действий (или бездействия) персонала клиник фиксируется намного меньше, что расходится с ранее зафиксированными тенденциями, например, в период пандемии.

Несколько лет назад доминирующим типом нарушителя выступали сотрудники. Еще пять лет назад среди утечек данных в мире доля хакеров составляла чуть больше 30% [14], а в медучреждениях России и вовсе не было зафиксировано ни одного нарушения по вине внешних злоумышленников. В ходе исследования, посвященного утечкам информации из медучреждений в период пандемии COVID-19, была выявлена схожая картина [15].

Пример. О том, что ошибки сотрудников системы здравоохранения при работе с информацией могут приводить к самым серьезным последствиям для пациентов, свидетельствует случай в медицинском центре университета Вирджинии.

Virginia Commonwealth University Health System (VCU Health) допустил утечку конфиден-

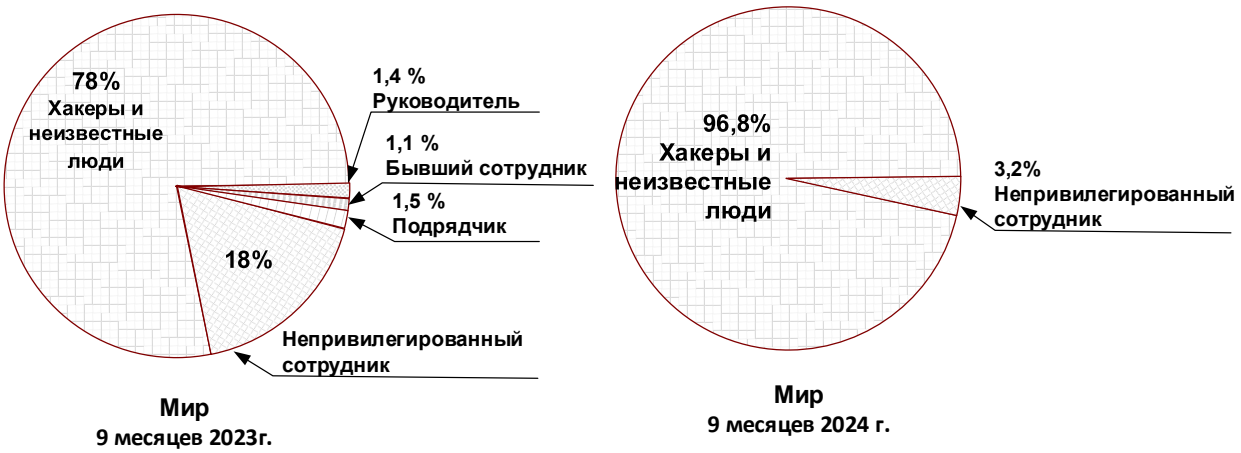

Рисунок 7 – Распределение утечек в здравоохранении по виновникам (Мир, январь-сентябрь 2023 г. - январь-сентябрь 2024 г.)

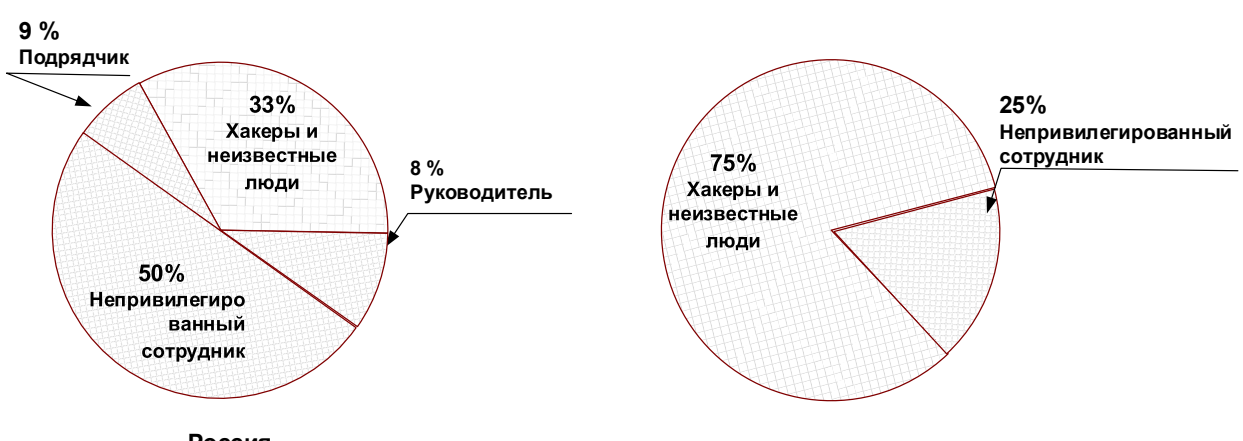

Рисунок 8 – Распределение утечек в здравоохранении по виновникам (Россия, январь-сентябрь 2023 г. - январь-сентябрь 2024 г.)

циальной информации тысяч людей, которым делали операции по пересадке органов и которые при этом выступали донорами. Компрометация конфиденциальной информации произошла из-за ошибки на портале VCU Health. Согласно заявлению VCU Health могли быть скомпрометированы такие данные, как номера социального страхования, номера медицинских карт, результаты лабораторных исследований и другая информация. Эти данные могли быть доступны донорам органов, реципиентам и их представителям при заходе на портал для пациентов. В VCU Health считают, что утечка информации могла затронуть персональные данные около 4500 человек [16, 17].

Распределение утечек по типам каналов

Доминирующим каналом остается интернет. В России снижается доля бумажных документов, что связано с тенденцией цифровизации медицины в целом (см. рисунок 9, 10).

Экономический ущерб от утечек конфиденциальной информации

Анализ ущерба от утечек конфиденциальной информации предложено провести на конкретных примерах.

1. *ИТ-вендор заплатил партнеру за нарушение*

Производитель игрового оборудования Razer выиграл судебный процесс по делу об утечке информации у поставщика Capgemini. В резуль-

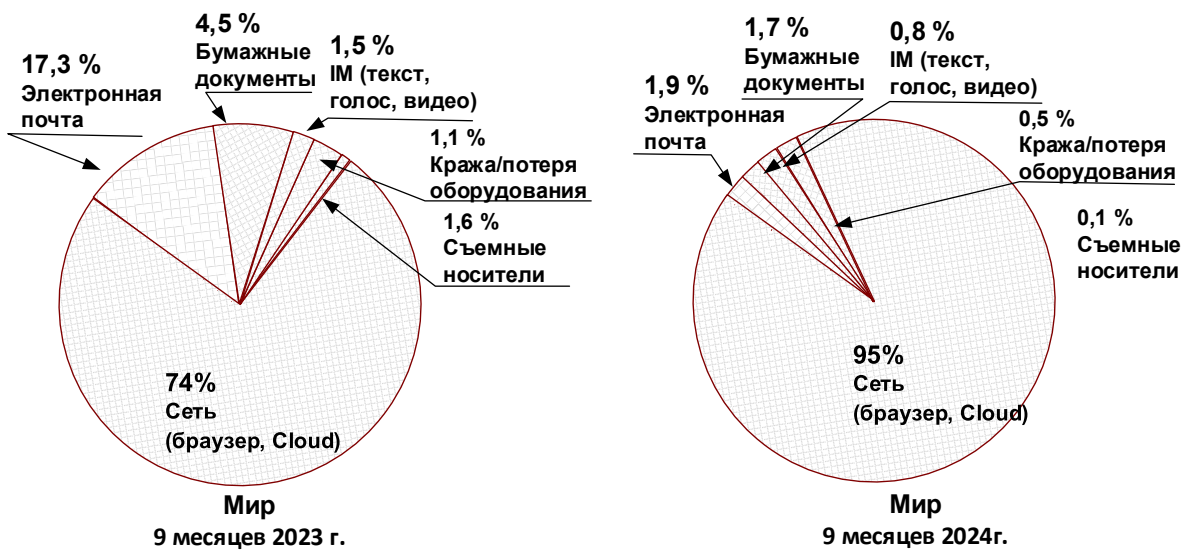

Рисунок 9 – Здравоохранение: распределение утечек по каналам (Мир, январь-сентябрь 2023 г. - январь-сентябрь 2024 г.

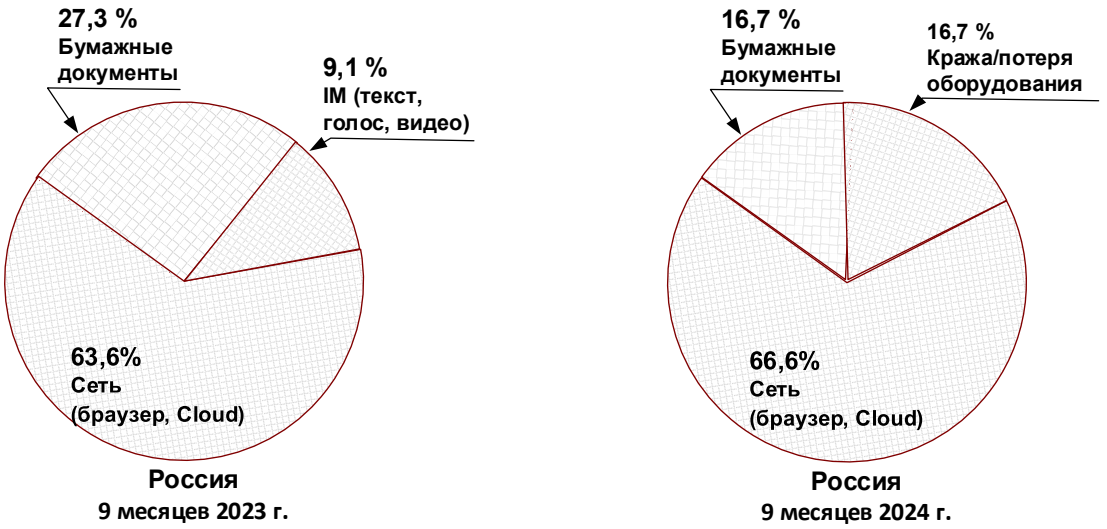

Рисунок 10 – Здравоохранение: распределение утечек по каналам (Россия, январь-сентябрь 2023 г. - январь-сентябрь 2024 г.

тате ошибки сотрудника технологической компании произошла утечка информации порядка 100 тыс. человек. Суд постановил, что компания Capgemini должна будет выплатить компании Razer компенсацию в размере $6,5 млн.

Сведения о заказах многих тысяч клиентов попали в Сеть в результате серьезного нарушения информационной безопасности, случившегося в 2022 г. В том же году игровая фирма Razer, имеющая штаб-квартиры в США и Сингапуре, подала в суд на Capgemini, по вине которой произошла утечка данных.

Согласно решению суда, компания Razer должна будет получить от своего ИТ-поставщика $6,1 млн в качестве выплаты за упущенную выгоду. Сумма компенсации также включает расходы на услуги эксперта-криминалиста ($60 тыс.), выплаты юристам (около $320 тыс.) и вознаграждение исследователю безопасности Бобу Дьяченко ($2 тыс.), который обнаружил некорректно сконфигурированный облачный кластер Elasticsearch с данными Razer.

Представители Razer заявили, что утечка информации произошла в 16-минутный промежуток 18 июня 2020 г. По их данным, в тот день сотрудник Capgemini Аргель Кабалаг (Argel Cabalag), которому было поручено устранить неполадки в системе, после того как специалисты Razer не смогли получить доступ к данным, оказался единственным, кто обратился к облачному хранилищу в течение 16-минутного интервала времени. Аргель Кабалаг признал, что именно его ошибка вызвала некорректную настройку файлового хранилища [18].

2. *Персональные данные: Meta получила мега-штраф*

Компания Meta (Организация признана экстремистской и запрещена на территории России), управляющая социальными сервисами Facebook, Instagram и WhatsApp, оштрафована европейским регулятором на 265 млн евро (примерно $275 млн) за то, что злоумышленникам удалось собрать персональные данные 500 млн пользователей. В результате персональные данные попали в сеть.

Управляющая компания соцсети Facebook получила штраф от комиссии по защите данных (DPC) в Ирландии, где расположена европейская штаб-квартира этого ИТ-гиганта. Ирландский надзорный орган начал расследование после того, как на хакерском форуме были размещены данные более чем 500 млн пользователей. Значительная часть из них – это жители Европы.

DPC заявила, что Meta нарушила две статьи законодательства ЕС о защите данных после того, как в 2018 и 2019 годах неизвестные собрали из открытых профилей Fac5ebook информацию о подписчиках соцсети.

Помимо назначения штрафа в размере 265 млн евро европейский регулятор потребовал от Meta

привести процесс обработки данных в соответствие требованиям ЕС.

В общей сложности, начиная с сентября 2023 г. Ирландская комиссия по защите данных оштрафовала компанию Meta за различные нарушения примерно на 1 млрд евро. Так, в сентябре 2023 г. компании назначен штраф в размере 405 млн евро за то, что она допустила создание пользователями-подростками аккаунтов в Instagram, в которых номера телефонов и электронные адреса находились в общем доступе. В то же самое время за нарушения на 225 млн евро оштрафован сервис WhatsApp. Еще один штраф (в размере 17 млн евро) за несоблюдение европейского регламента по защите данных Meta получила в марте 2022 г. [19, 20].

3. *Пять сотрудников больницы годами сливали персональные данные*

Федеральный суд США в штате Теннесси предъявил обвинение пяти бывшим сотрудникам клиники Methodist, которые передавали персональные данные за пределы медучреждения. Слитые персональные данные продавались заинтересованным лицам. Согласно обвинению, пять бывших сотрудников Methodist Hospital вступили в сговор с 40-летним Родериком Харви (Roderick Harvey) с целью незаконного разглашения конфиденциальной информации пациентов в нарушение Закона о переносимости и подотчетности медицинского страхования (HIPAA). Этот закон был принят Конгрессом США в 1996 г. для создания национальных стандартов о защите конфиденциальной информации пациентов от разглашения без ведома и согласия пациентов. Раскрытие данных о пациенте или их получение с целью продажи, передачи или использования в личных целях классифицируется как преступление.

Согласно обвинительному заключению, в период с ноября 2017 г. по декабрь 2020 г. Харви платил пяти сотрудникам клиники Methodist за передачу ему имен и номеров телефонов пациентов, которые были доставлены в медучреждение после дорожно-транспортных происшествий. Получив эту информацию, Харви далее отправляя ее юристам и мануальным терапевтам.

Харви предъявлены обвинения по семи пунктам. По каждому из них ему грозило до десяти лет тюремного заключения, штраф до $250 тыс., а также три года надзора после освобождения.

Каждый из бывших сотрудников, которые обвинялись в отдельных нарушениях HIPAA, могли получить до одного года тюрьмы, штраф до $50 тыс. и один год надзора [21, 22].

4. *AstraZeneca раскрывала персональные данные пациентов*

Фармацевтический гигант AstraZeneca больше года держал в открытом доступе данные для внутренних ресурсов, в результате чего могли быть скомпрометированы персональные данные различных пациентов. Интересно, что персональные данные хранились в тестовой среде.

Моссаб Хуссейн (Mossab Hussein), директор по безопасности стартапа SpiderSilk, сообщил журналистам, что еще в 2021 г. разработчики компании AstraZeneca оставили учетные данные для внутреннего сервера на одном из репозиториев ресурса для обмена кодом GitHub. По словам Хуссейна, эти учетные данные позволяли получить доступ к тестовой среде на облачном сервисе Salesforce. Несмотря на тестовый характер хранилища, в нем находилась конфиденциальная информация пациентов, которые покупали лекарства от AstraZeneca. По словам Хуссейна, некоторая конфиденциальная информация относилась к приложению ZX&ME, которое предлагает скидки на лекарственные препараты.

Репортеры TechCrunch уведомили AstraZeneca об утечке данных, и через несколько часов репозиторий GitHub, содержащий учетные данные, оказался недоступен. «Из-за ошибки пользователя некоторые записи данных временно оказались на платформе разработчиков. Мы закрыли доступ к этим данным сразу после того, как нас проинформировали об этом. Мы расследуем причину инцидента, а также оцениваем наши нормативные обязательства», – заявил представитель AstraZeneca Патрик Барт (Patrick Barth). Барт отказался сообщить, почему данные пациентов хранились в открытой тестовой среде и есть ли у AstraZeneca журналы событий, которые

помогут выяснить, получил ли кто-нибудь доступ к данным и какие данные могли быть скомпрометированы [23].

5. *Персональные данные пациентов утекли из-за веб-трекеров*

Сеть клиник Advocate Aurora Health (AAH) уведомила министерство здравоохранения и социальных служб США о потенциальном инциденте, в ходе которого могли быть скомпрометированы персональные данные порядка 3 млн пациентов. Медицинская организация выяснила, что персональные данные утекали через инструменты отслеживания аудитории на ее веб-сайте.

AAH – крупная медицинская организация, работающая в штатах Висконсин и Иллинойс. Она насчитывает 27 клиник, 32 тыс. врачей и медсестер, а в зоне ее обслуживания находятся миллионы пациентов.

Руководители AAH опасаются, что размещенные на ее веб-сайтах трекеры для отслеживания аудитории передают конфиденциальную информацию в Meta, Google и другим компаниям. Речь идет об инструментах типа «пиксель», например, Meta Pixels, который принадлежит компании Meta, управляющей социальной сетью Facebook.

Представители AAH говорят, что разместили коды аналитических инструментов на своих онлайн-порталов с целью получить информацию о поведении пациентов: сколько людей посещают те или иные страницы и входят в свои учетные записи, что они используют и т.д. Однако, постепенно выяснилось, что установленные на веб-страницы «пиксели» могут передавать конфиденциальную информацию разработчикам, то есть таким платформам, как Facebook и Google. По данным AAH эти инструменты передают не только ID посетителя сайта, его IP-адрес или детали просмотра страниц, но и такую конфиденциальную информацию, как имена лечащих врачей, болезни, от которых страдает тот или иной пациент, рецептурные назначения, данные о медицинских страховках и т.д. [24, 25].

6. *Сколько стоит возврат данных*

Основной мотивацией хакеров остается получение денег. Используя в ходе атак вирусы-вымогатели, хакеры рассчитывают получить выкуп за возврат данных.

Персональные данные более 300 тыс. пациентов были скомпрометированы в ходе атаки на службу скорой помощи Empress EMS в Нью-Йорке. По данным журналистов, злоумышленники из группировки Hive похитили не только номера социального страхования и другие персональные данные людей, обращавшихся за помощью, но также сведения из договоров, документов по бюджетированию, инвестиционным контрактам и данные о состоянии счетов Empress EMS. Вероятно, Hive получила выкуп со стороны компании. Так, анонсировав эту утечку данных в июле, хакеры вскоре удалили информацию о ней со своего сайта, так и не опубликовав украденные данные [26].

На одном из хакерских форумов неизвестный пользователь под псевдонимом optusdata заявил, что ему удалось украсть данные абонентов австралийского оператора связи Optus. Всего телекоммуникационный гигант с зеленого континента потерял конфиденциальную информацию около 10 млн подписчиков. За возврат данных злоумышленник потребовал выкуп в размере $1 млн (эквивалент в криптовалюте) [27, 28]. В доказательство серьезности своих намерений хакер опубликовал фрагменты из 100, а потом из 10 тыс. записей. По данным некоторых источников, optusdata дал компании неделю на размышления, однако через некоторое время отказался от идеи выкупа и даже принес извинения пострадавшим клиентам Optus [29].

Большинство экспертов по кибербезопасности и представители правоохранительных органов советуют компаниям, ставшим жертвами атак с использованием вирусов-вымогателей, не идти на поводу у хакеров и не поощрять распространение преступности [30]. Однако, некоторые организации решают удовлетворить требования злоумышленников, чтобы вернуть ценную информацию. Так поступило управление образования округа Гленн в штате Калифорния (ClennCOE). В ходе атаки хакерам из группировки Quantum удалось отключить Интернет и электронную почту чиновников, а также частично вывести из строя

телефонию и систему финансового учета. Кроме того, киберпреступники заблокировали данные управления. Согласно утверждениям Quantum, они уничтожили все резервные копии. За получение ключа-дешифратора GlennCOE пришлось заплатить $400 тыс [31].

Один из самых громких инцидентов информационной безопасности в последнее время – нападение хакеров на крупную клинику Centre Hospitalier Sud Francilien в пригороде Парижа. Выяснилось, что к инциденту информационной безопасности причастна группировка, которая работает с программой-вымогателем LockBit. Отказ клиники заплатить хакерам выкуп в размере $1 млн (первоначальные требования были в десять раз больше) привел к публикации в Сети 12 Гб данных о пациентах и персонале. Открытыми стали номера социального страхования, лабораторные отчеты и другие сведения о здоровье пациентов. В своем заявлении представители больницы отметили, что зона атаки была ограничена виртуальными серверами, на которых хранилась примерно десятая часть данных медучреждения [32].

Специалисты компании Resecurity в этом году провели исследование тактики одного из крупнейших хакерских синдикатов BlackCat (также известен как ALPHV) [33]. По словам экспертов, злоумышленники обычно выдвигают сумму выкупа в размере $ 2,5 млн, но допускают возможность сделать скидку в размере до 50%, мотивируя компанию-жертву как можно скорее разрешить инцидент. Среднее время, которое отводится на выплату выкупа, составляет от пяти до семи дней. Это необходимо на то, чтобы компания успела приобрести криптовалюту.

По сравнению с 2022 г., в первой половине 2023 г. средний размер выкупа вырос на 82% и достиг $570 тыс., а к 2022 г. он еще удвоился. Согласно последним прогнозам 2024 г., общий объем рынка программ-вымогателей достигнет $ 265 млрд к 2031 г., а общий ущерб для предприятий по всему миру составит $ 10,5 трлн. Такие показатели могут сделать программы-вымогатели крупнейшим в мире сектором теневой экономики, ущерб от действий которых будет даже выше, чем от стихийных бедствий. Несмотря на рекомендации регуляторов не вносить выкуп, почти половина (более 48%) организаций, пострадавших от атак с использованием программ-вымогателей, предпочли выполнить требования хакеров, так как не нашли альтернативных вариантов оперативного восстановления своей деятельности, отмечают в Resecurity.

Заключение и выводы

Изучение утечек данных из сферы здравоохранения за последние 5 лет позволяет сделать о вывод, что некоторое снижение количества случаев компрометации информации за 9 месяцев 2024 года обусловлено значительно возросшим уровнем латентности нарушений, прежде всего, совершенных по вине персонала. Его рост начал проявляться еще в 2020 году после завершения первой фазы пандемии. Судя по всему, в публичное информационное пространство стало попадать намного меньше утечек, ставших следствием нарушений со стороны сотрудников медучреждений. Внимание всех привлечено к разгоревшемуся до уровня кибервойны противостоянию в киберпространстве.

В то же время рост объемов утекшей информации из сферы здравоохранения, в несколько раз больший по сравнению с предыдущим периодом, позволяет сделать вывод о том, что данные о пациентах и деятельности медицинских учреждений стали очень привлекательным объектом для преступников. Развитие цифровизации здравоохранения разных стран привело к появлению удобных форм хранения и передачи больших объемов информации, содержащей персональные данные и врачебную тайну [34]. Однако, в условиях недостаточного внимания к вопросам информационной безопасности такое удобство влечет массу рисков как для медицины, так и для граждан (в развитых странах практически каждый имеет страховку или хоть раз побывал в качестве пациента в медицинских учреждениях на коммерческой основе).

Медицинские учреждения в целом нельзя отнести к числу основных на отраслевой карте утечек конфиденциальной информации, то есть

обстановку с кибербезопасностью там нельзя назвать критичной, однако и позитивной тоже нельзя. Ряд актуальных исследований (например, отчет Ponemon Institute) показывают, что медицинские учреждения слабо готовы к отражению кибератак, так как направление ИБ финансируется явно недостаточно, значительное количество медицинского оборудования работает на устаревшем ПО и не поддерживает функции, обеспечивающие безопасность [35, 36]. Есть немало примеров, когда уровень безопасности в клиниках напрямую влияет на здоровье и жизни пациентов (атаки на оборудование для операционных и сервисное ПО для онкологических больных, попытки удаленного отключения кардиостимуляторов и т.д., в том числе повлекшие смерти пациентов).

И то, что на этом фоне известных случаев утечек данных из сферы здравоохранения за 9 месяцев 2024 г. стало меньше, в целом не должно успокаивать. Если в результате многочисленных атак и эксплуатации уязвимостей в сеть пока «просочился» лишь небольшой процент украденных данных, значит через некоторое время в Дарквебе можно ожидать намного больше объявлений о продаже информации из клиник и лабораторий (в разных вариантах и компоновках). Аналогично и с внутренними нарушителями – скомпрометированные в результате умышленных действий или небрежности данные рано или поздно станут удобным средством для мошенников.

Вероятно, в новой мировой реальности, когда происходит слом прежних устоев, а формирование многополярного мира провоцирует более жесткие столкновения в киберпространстве, сфера здравоохранения будет одной из возможных арен борьбы.

Список литературы

1. *Галлезе-Нобиле К.* Правовые аспекты использования искусственного интеллекта в телемедицине // Journal of Digital Technologies and Law. – 2023. – Т. 1, № 2. – С. 314-336. – DOI 10.21202/jdtl.2023.13. – EDN VSKCFB.
2. *Харченко Е.Б., Шейдаков Н.Е.* Об опасности кибератак на ис учреждений здравоохранения // Информационные системы, экономика и управление : Ученые записки. Том Выпуск 23. – Ростов-на-Дону: Ростовский государственный экономический университет «РИНХ», 2021. – С. 76-79. – EDN YNZFOW.
3. *Зайцев А.К., Матвеев В.В.* Экономические преступления с использованием цифровых технологий // Национальная безопасность и стратегическое планирование. – 2022. – № 1(37). – С. 63-81. – DOI 10.37468/2307-1400-2022-1-63-81. – EDN WFNIFZ.
4. *Антонов А.Е., Матвеев В.В.* Обеспечение экономической безопасности с использованием DLP системы (искусственного интеллекта) // Теоретические и прикладные вопросы комплексной безопасности: Материалы V Международной научно-практической конференции, Санкт-Петербург, 23 марта 2022 года. – СПб: Санкт-Петербургский институт природопользования, промышленной безопасности и охраны окружающей среды, 2022. – С. 251-257. – EDN DEOZZA.
5. *Shekokar N. M. et al. (ed.).* Cyber Security Threats and Challenges Facing Human Life. – CRC Press, 2022.
6. Аналитика в сфере утечки информации [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/analytics
7. *Трусов Ю.А., Антипов А.В.* Право на забвение: опыт практического анализа // Цифровые технологии и право: Сборник научных трудов I Международной научно-практической конференции. В 6-ти томах, Казань, 23 сентября 2022 года. – Казань: Издательство «Познание», 2022. – С. 362-366. – EDN HAUILR.
8. *Moore W., Frye S.* Review of HIPAA, part 1: history, protected health information, and privacy and security rules // Journal of nuclear medicine technology. – 2019. – V. 47. – No 4. – P. 269-272. – DOI: https://doi.org/10.2967/jnmt.119.227819
9. *Kiel J. M., Ciamacco F. A., Steines B. T.* Privacy and data security: HIPAA and HITECH // Healthcare information management systems: Cases, strategies, and solutions. – 2016. – P. 437-449. – DOI: https://doi.org/10.1007/978-3-319-20765-0_25
10. EyeMed agrees $600,000 settlement over

2020 data breach [Электронный ресурс]. – Режим доступа: https://www.zdnet.com/article/eyemed-us-attorney-agree-600000-settlement-over-2020-data-breach/

11. *Swasey K.* Insufficient healthcare cybersecurity invites ransomware attacks and sale of phi on the dark web // Center for Anticipatory Intelligence Student Research Reports. – 2020. URL: https://www.usu.edu/cai/files/studentpaper-swasey.pdf

12. *Reeves K.* Cyberattacks: Not a Matter of If, but When // Applied Radiology. – 2024. – V. 53. – No 2. – P. 38-41. URL: https://cdn.agilitycms.com/applied-radiology/PDFs/Issues/AR_03-24_radmatters.pdf

13. Оренбургские хакеры передавали данные скорой помощи ритуальным агентствам [Электронный ресурс]. – Режим доступа: https://www.securitylab.ru/news/532648.php

14. Исследование утечек конфиденциальной информации из медицинских учреждений в 2017 году [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_med2017.pdf

15. COVID-19: утечки периода пандемии (1 полугодие 2020) [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/analytics/analitika/covid-19-utechki-perioda-pandemii-1-polugodie-2020

16. More than 4,000 individuals' medical data left exposed for 16 years. URL: https://portswigger.net/daily-swig/more-than-4-000-individuals-medical-data-left-exposed-for-16-years

17. *Rawat R. et al.* Organ trafficking on the dark web—The data security and privacy concern in healthcare systems // Internet of Healthcare Things: Machine Learning for Security and Privacy. – 2022. – P. 189-216. – DOI: https://doi.org/10.1002/9781119792468.ch9

18. Gaming firm Razer wins lawsuit against IT vendor over data leak, awarded $8.7m in damages. URL: https://www.straitstimes.com/singapore/courts-crime/gaming-firm-razer-wins-lawsuit-against-it-vendor-over-data-leak-awarded-87m-in-damages

19. *Mrežar F.* Analysis of fines under GDPR. – University of Zagreb. Faculty of Law. Information Technology Law and Informatics, 2023. URL: https://repozitorij.pravo.unizg.hr/en/islandora/object/pravo:5002

20. Meta fined €265m over data protection breach that hit more than 500m users. URL: https://www.theguardian.com/technology/2022/nov/28/meta-fined-265m-over-data-breach-affecting-more-than-500m-users

21. *Heath M., Porter T. H., Silvera G.* Hospital characteristics associated with HIPAA breaches // International Journal of Healthcare Management. – 2022. – V. 15. – No 2. – P. 171-180. – DOI: https://doi.org/10.1080/20479700.2020.1870349

22. Five former Methodist Hospital employees charged with HIPAA violations. URL: https://www.databreaches.net/five-former-methodist-hospital-employees-charged-with-hipaa-violations/

23. AstraZeneca password lapse exposed patient data. URL: https://techcrunch.com/2022/11/03/astrazeneca-passwords-exposed-patient-data/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZGF0YWJyZWFjaGVzLm5ldC8&guce_referrer_sig=AQAAAAE8Y-wn6fo1Qi-8AU_fm0vQeRXNT33dCZm9xadXJu-GZWz74n7EcPfHE32674LobeN4v1ZqAtZSv0juf8txbWO4h84jFb0rLKorSpG0Uv514Oa95_LvoJVpkDniwzWwBy_PjdW8N1rfJTEQdOr_XzjK0b69LDt9eP2nAzyO9o72

24. *Besenyő J.* Security Science Journal Healthcare Cybersecurity Threat Context and Mitigation Opportunities (Vol. 4 No. 1, 2023. Security Science Journal). – DOI: https://doi.org/10.37458/ssj.4.1.6

25. Oops, web trackers may have leaked 3 million patients' info. URL: https://www.theregister.com/2022/10/20/health_group_says_tracking_pixel/

26. 300K Patients' Data Compromised In Ransomware Attack On Yonkers-Based Empress EMS. URL: https://patch.com/new-york/newrochelle/300k-patients-compromised-ransomware-attack-empress-ems

27. *Kayes A. S. M. et al.* Safeguarding Individuals and Organisations from Privacy Breaches: A Comprehensive Review of Problem Domains, Solution Strategies, and Prospective Research Directions // IEEE Internet of Things Journal. – 2024. – DOI: https://doi.org/10.1109/JIOT.2024.3481316

28. How a massive data breach has exposed Australia. URL: https://www.saudigazette.com.sa/

article/625539/World/Asia/How-a-massive-data-breach-has-exposed-Australia

29. Alleged Optus hacker apologises for data breach and drops ransom threat. URL: https://www.theguardian.com/business/2022/sep/27/alleged-optus-hacker-apologises-for-data-breach-and-drops-ransom-threat

30. *Thomas J.* Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks // Thomas, JE (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. International Journal of Business Management. – 2018. – V. 12. – No 3. – P. 1-23. – DOI: 10.5539/ijbm.v13n6p1

31. SCOOP: Glenn County Office of Education Pays $400K Ransom After Ransomware Attack. URL: https://www.databreaches.net/scoop-glenn-county-office-of-education-paid-400k-ransom-after-ransomware-attack/

32. LockBit Publishes Stolen Data as Hospital Rejects Extortion. URL: https://www.bankinfosecurity.com/lockbit-publishes-stolen-data-as-hospital-rejects-extortion-a-20155

33. BlackCat (aka ALPHV) Ransomware is Increasing Stakes up to $2,5M in Demands. URL: https://resecurity.com/blog/article/blackcat-aka-alphv-ransomware-is-increasing-stakes-up-to-25m-in-demands

34. *Варзин С.А., Матвеев В.В.* Обеспечение информационной безопасности в системе здравоохранения // Национальная безопасность и стратегическое планирование. – 2023. – № 3(43). – С. 19-56. – DOI 10.37468/2307-1400-2024-2023-3-19-56. – EDN ONKEFE.

35. *Ige T. O., Frimpong A. A., Akinbobola B. A.* Mitigating Cybersecurity Threats in the Healthcare Sector: An Analysis of Challenges and Solutions in the USA // Journal of Energy Technologies and Policy. – 2024. – V. 14. – No 2. – P. 66-76. – DOI: 10.7176/JETP/14-2-05

36. *Campbell R. J.* Cybersecurity Vulnerabilities and Considerations in US Healthcare Facilities: A Scoping Review. – 2024. URL: https://digitalcommons.unmc.edu/coph_slce/352

References

1. *Gallese-Nobile K.* Legal aspects of using artificial intelligence in telemedicine // Journal of Digital Technologies and Law. – 2023. – Vol. 1, No. 2. – Pp. 314-336. – DOI 10.21202/jdtl.2023.13. – EDN VSKCFB.

2. *Kharchenko E.B., Sheydakov N.E.* On the danger of cyberattacks on the information systems of healthcare institutions // Information systems, economics and management: Scientific notes. Volume Issue 23. – Rostov-on-Don: Rostov State University of Economics "RINH", 2021. - Pp. 76-79. - EDN YNZFOW.

3. *Zaitsev A.K., Matveev V.V.* Economic crimes using digital technologies // National security and strategic planning. – 2022. – No. 1(37). – P. 63-81. – DOI 10.37468/2307-1400-2022-1-63-81. – EDN WFNIFZ.

4. *Antonov A.E., Matveev V.V.* Ensuring economic security using a DLP system (artificial intelligence) // Theoretical and applied issues of integrated security: Proceedings of the V International scientific and practical conference, St. Petersburg, March 23, 2022. – SPb: St. Petersburg Institute of Nature Management, Industrial Safety and Environmental Protection, 2022. – P. 251-257. – EDN DEOZZA.

5. *Shekokar N. M. et al. (ed.).* Cyber Security Threats and Challenges Facing Human Life. – CRC Press, 2022.

6. Analytics in the field of information leakage [Electronic resource]. – Access mode: https://www.infowatch.ru/analytics

7. *Trusov Yu.A., Antipov A.V.* The right to be forgotten: experience of practical analysis // Digital technologies and law: Collection of scientific papers of the I International scientific and practical conference. In 6 volumes, Kazan, September 23, 2022. – Kazan: Publishing house "Poznanie", 2022. – P. 362-366. – EDN HAUILR.

8. *Moore W., Frye S.* Review of HIPAA, part 1: history, protected health information, and privacy and security rules // Journal of nuclear medicine technology. – 2019. – V. 47. – No 4. – P. 269-272. – DOI: https://doi.org/10.2967/jnmt.119.227819

9. *Kiel J. M., Ciamacco F. A., Steines B. T.* Privacy and data security: HIPAA and HITECH // Healthcare information management systems: Cases, strategies, and solutions. – 2016. – P. 437-449. – DOI: https://doi.org/10.1007/978-3-319-20765-0_25

10. EyeMed agrees $600,000 settlement over 2020 data breach [Электронный ресурс]. – Режим доступа: https://www.zdnet.com/article/eyemed-us-attorney-agree-600000-settlement-over-2020-data-breach/

11. *Swasey K.* Insufficient healthcare cybersecurity invites ransomware attacks and sale of phi on the dark web // Center for Anticipatory Intelligence Student Research Reports. – 2020. URL: https://www.usu.edu/cai/files/studentpaper-swasey.pdf

12. *Reeves K.* Cyberattacks: Not a Matter of If, but When // Applied Radiology. – 2024. – V. 53. – No 2. – P. 38-41. URL: https://cdn.agilitycms.com/applied-radiology/PDFs/Issues/AR_03-24_radmatters.pdf

13. Orenburg hackers transferred ambulance data to funeral agencies URL: https://www.securitylab.ru/news/532648.php

14. Study of leaks of confidential information from medical institutions in 2017 URL: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_med2017.pdf

15. COVID-19: leaks during the pandemic (1st half of 2020) URL: https://www.infowatch.ru/analytics/analitika/covid-19-utechki-perioda-pandemii-1-polugodie-2020More than 4,000 individuals' medical data left exposed for 16 years. URL: https://portswigger.net/daily-swig/more-than-4-000-individuals-medical-data-left-exposed-for-16-years

16. More than 4,000 individuals' medical data left exposed for 16 years. URL: https://portswigger.net/daily-swig/more-than-4-000-individuals-medical-data-left-exposed-for-16-years

17. *Rawat R. et al.* Organ trafficking on the dark web—The data security and privacy concern in healthcare systems // Internet of Healthcare Things: Machine Learning for Security and Privacy. – 2022. – P. 189-216. – DOI: https://doi.org/10.1002/9781119792468.ch9

18. Gaming firm Razer wins lawsuit against IT vendor over data leak, awarded $8.7m in damages. URL: https://www.straitstimes.com/singapore/courts-crime/gaming-firm-razer-wins-lawsuit-against-it-vendor-over-data-leak-awarded-87m-in-damages

19. *Mrežar F.* Analysis of fines under GDPR. – University of Zagreb. Faculty of Law. Information Technology Law and Informatics, 2023. URL: https://repozitorij.pravo.unizg.hr/en/islandora/object/pravo:5002

20. Meta fined €265m over data protection breach that hit more than 500m users. URL: https://www.theguardian.com/technology/2022/nov/28/meta-fined-265m-over-data-breach-affecting-more-than-500m-users

21. *Heath M., Porter T. H., Silvera G.* Hospital characteristics associated with HIPAA breaches // International Journal of Healthcare Management. – 2022. – V. 15. – No 2. – P. 171-180. – DOI: https://doi.org/10.1080/20479700.2020.1870349

22. Five former Methodist Hospital employees charged with HIPAA violations. URL: https://www.databreaches.net/five-former-methodist-hospital-employees-charged-with-hipaa-violations/

23. AstraZeneca password lapse exposed patient data. URL: https://techcrunch.com/2022/11/03/astrazeneca-passwords-exposed-patient-data/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZGF0YWJyZWFjaGVzLm5ldC8&guce_referrer_sig=AQAAAAE8Y-wn6fo1Qi-8AU_fm0vQeRXNT33dCZm9xadXJu-GZWz74n7EcPfHE32674LobeN4v1ZqAtZSv0juf8txbWO4h84jFb0rLKorSpG0Uv514Oa95_LvoJVpkDniwzWwBy_PjdW8N1rfJTEQdOr_XzjK0b69LDt9eP2nAzyO9o72

24. *Besenyő J.* Security Science Journal Healthcare Cybersecurity Threat Context and Mitigation Opportunities (Vol. 4 No. 1, 2023. Security Science Journal). – DOI: https://doi.org/10.37458/ssj.4.1.6

25. Oops, web trackers may have leaked 3 million patients' info. URL: https://www.theregister.com/2022/10/20/health_group_says_tracking_pixel/

26. 300K Patients' Data Compromised In Ransomware Attack On Yonkers-Based Empress EMS. URL: https://patch.com/new-york/newrochelle/300k-patients-compromised-ransomware-attack-empress-ems

27. *Kayes A. S. M. et al.* Safeguarding Individuals and Organisations from Privacy Breaches: A Comprehensive Review of Problem Domains, Solution Strategies, and Prospective Research Directions // IEEE Internet of Things Journal. – 2024. – DOI: https://doi.org/10.1109/JIOT.2024.3481316

28. How a massive data breach has exposed Australia. URL: https://www.saudigazette.com.sa/article/625539/World/Asia/How-a-massive-data-breach-has-exposed-Australia

29. Alleged Optus hacker apologises for data breach and drops ransom threat. URL: https://www.theguardian.com/business/2022/sep/27/alleged-optus-hacker-apologises-for-data-breach-and-drops-ransom-threat

30. *Thomas J.* Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks // Thomas, JE (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. International Journal of Business Management. – 2018. – V. 12. – No 3. – P. 1-23. – DOI: 10.5539/ijbm.v13n6p1

31. SCOOP: Glenn County Office of Education Pays $400K Ransom After Ransomware Attack. URL: https://www.databreaches.net/scoop-glenn-county-office-of-education-paid-400k-ransom-after-ransomware-attack/

32. LockBit Publishes Stolen Data as Hospital Rejects Extortion. URL: https://www.bankinfosecurity.com/lockbit-publishes-stolen-data-as-hospital-rejects-extortion-a-20155

33. BlackCat (aka ALPHV) Ransomware is Increasing Stakes up to $2,5M in Demands. URL: https://resecurity.com/blog/article/blackcat-aka-alphv-ransomware-is-increasing-stakes-up-to-25m-in-demands

34. *Varzin S.A., Matveev V.V.* Ensuring information security in the healthcare system // National security and strategic planning. – 2023. – No. 3 (43). – P. 19-56. – DOI 10.37468/2307-1400-2024-2023-3-19-56. – EDN ONKEFE.

35. *Ige T. O., Frimpong A. A., Akinbobola B. A.* Mitigating Cybersecurity Threats in the Healthcare Sector: An Analysis of Challenges and Solutions in the USA // Journal of Energy Technologies and Policy. – 2024. – V. 14. – No 2. – P. 66-76. – DOI: 10.7176/JETP/14-2-05

36. *Campbell R. J.* Cybersecurity Vulnerabilities and Considerations in US Healthcare Facilities: A Scoping Review. – 2024. URL: https://digitalcommons.unmc.edu/coph_slce/352

Статья поступила в редакцию 16 ноября 2024 г.
Принята к публикации 21 декабря 2024 г.

Ссылка для цитирования: Варзин С.А., Матвеев В.В. Взаимосвязь информационной, экономической и социальной безопасности в системе здравоохранения // Национальная безопасность и стратегическое планирование. 2024. № 4(48). С. 60-76. DOI: https://doi.org/10.37468/2307-1400-2024-4-60-76

For citation: Varzin S.A., Matveev V.V. The relationship between information, economic and social security in the healthcare system // National security and strategic planning. 2024. № 4(48). pp. 60-76. DOI: https://doi.org/10.37468/2307-1400-2024-4-60-76

Сведения об авторах:

ВАРЗИН СЕРГЕЙ АЛЕКСАНДРОВИЧ – *доктор медицинских наук, доцент, профессор кафедры факультетской хирургии Санкт-Петербургского государственного университета, заведующий кафедрой хирургических болезней № 2, Санкт-Петербургского медико-социального института, г. Санкт-Петербург, Россия*
ORCID: https://orcid.org/0000-0003-4437-7603
SPIN-код: 2529-6768
e-mail: drvarzin@mail.ru
МАТВЕЕВ ВЛАДИМИР ВЛАДИМИРОВИЧ – *доктор технических наук, профессор, профессор кафедры экономики и финансов, Финансовый университет при Правительстве РФ (Санкт-Петербургский филиал), г. Санкт-Петербург, Россия*
SPIN-код: 6680-9575
e-mail: 070355mvv@gmail.com

Information about authors:

VARZIN SERGEY A. – *Doctor of Medical Sciences, Associate Professor, Professor of the Department of Faculty Surgery of St. Petersburg State University, Head of the Department of Surgical Diseases No. 2, St. Petersburg Medical and Social Institute, St. Petersburg, Russia*
ORCID: https://orcid.org/0000-0003-4437-7603
SPIN-код: 2529-6768
e-mail: drvarzin@mail.ru
MATVEEV VLADIMIR V. – *Doctor in Engineering, Professor, Professor of the Economics and Finance Department, Financial University under the Government of the Russian Federation (St. Petersburg branch), St. Petersburg, Russia*
SPIN: 6680-9575
e-mail: 070355mvv@gmail.com