УДК 61, 57.016.3, 355.343.18 DOI 10.37468/2307-1400-2023-3-19-56

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ 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] Государственный институт экономики, финансов, права и технологий, Санкт-Петербург, Россия

АННОТАЦИЯ

Проанализировано внедрение цифровых технологий в систему здравоохранения Российской Федерации. Вместе с этим рассмотрено появление нового рентного товара – информации, цена которой с каждым годом возрастает. В связи с этим с каждым годом растет объем утечки информации из учреждений здравоохранения и наносимый им ущерб. Проведен статистический анализ утечки информации по характеру инцидентов, по типу похищаемой информации, по каналам утечки. Установлено содержание информации, относящееся к персональным данным и приведены многочисленные примеры утечки персональных дынных в России и за рубежом из медицинских учреждений. Дан сравнительный анализ утечки данных по отраслям. Установлены объекты защиты информации в медицинских учреждениях. Проанализирован репутационный ущерб от утечки информации в системе здравоохранения. Рассмотрены проблемы безопасности в сфере фармацевтики. Предложены некоторые рекомендации по повышению уровня информационной безопасности в системе здравоохранения.

Ключевые слова: цифровизация здравоохранения, безопасность, рента, экономический ущерб, репутация, здравоохранение, утечка информации, персональные данные, коммерческая тайна.

ENSURING INFORMATION 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] State Institute of Economics, Finance, Law and Technology, St. Petersburg, Russia

ABSTRACT

The introduction of digital technologies into the healthcare system of the Russian Federation is analyzed. At the same time, the emergence of a new rental product is considered - information, the price of which increases every year. In this regard, the volume of information leakage from healthcare institutions and the damage caused to them is growing every year. A statistical analysis of information leakage was carried out by the nature of the incidents, by the type of information stolen, and by leakage channels. The content of information related to personal data has been established and numerous examples of leakage of personal data in Russia and abroad from medical institutions have been given. A comparative analysis of data leakage by industry is given. Objects for protecting information in medical institutions have been established. Reputational damage from information leakage in the healthcare system is analyzed. Security problems in the pharmaceutical field are considered. Some recommendations are proposed to improve the level of information security in the healthcare system.

Keywords: digitalization of healthcare, security, rent, economic damage, reputation, healthcare, information leakage, personal data, trade secret.

1. Введение. Цифровизация в системе здравоохранения

В «Стратегии национальной безопасности РФ» (далее – Стратегия) указаны основные факторы, определяющие положение и роль Российской Федерации в мире в долгосрочной перспективе, в том числе, «*…состояние… здравоохранения…, как ключевой индикатор конкурентоспособности России*» [1].

«*Дальнейшее развитие человеческого потенциала должны обеспечить меры, направленные на… безусловную реализацию на всей территории страны конституционных прав и гарантий в сферах здравоохранения, санитарно-эпидемиологического благополучия населения, социального обеспечения, образования и культуры*», – говорится в Стратегии.

Для достижения данной цели в рамках развития национального проекта «Цифровая экономика» [2] в стране создана Единая государственная информационная система здравоохранения (ЕГИСЗ), представляющая собой экосистему и включающая в себя большое количество медицинских учреждений, государственных и частных клиник, медицинских лабораторий и т.д.

В национальном проекте «Цифровая экономика» определены его восемь направлений, в том числе пять базовых:

– нормативное регулирование;
– кадры и образование;
– формирование исследовательских компетенций и технических заделов;
– информационная инфраструктура;
– **информационная безопасность**;

а также три прикладных:

– умный город;
– государственное управление;
– **здравоохранение**.

Перед здравоохранением цифровая экономика ставит три задачи:

– создание новых способов ведения документации, баз данных о пациентах, доступа к этим данным;

– внедрение телемедицины и применение информационных систем для лечения пациентов, что и подразумевает Закон о телемедицине (т.е. будут действовать телемедицинские консультации, консилиумы и дистанционное наблюдение за состоянием здоровья пациентов);

– применение математических методов и методов искусственного интеллекта при обработке медицинских данных (автоматизация операционных процессов, алгоритмов и протоколов лечения).

С 1 января 2018 года вступил в силу ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационных технологий в сфере охраны здоровья» [3]. Этот закон известен как Закон о телемедицине. Таким образом, законодательно закреплены понятия «телемедицинские технологии» и «правовые основы» для их внедрения, позволяющие обеспечить дистанционное общение врачей и пациентов. Закон регулирует участие медицинских, фармакологических, технологических и других структур в функционировании и развитии этой сферы.

Закон охватывает следующие основные направления информационных технологий в сфере охраны здоровья:

1. Электронные рецепты (самая радикальная часть закона).
2. Телемедицина.
3. Электронный документооборот (в том числе с пациентами).
4. Единая государственная система в здравоохранении (ЕГИСЗ) (рис.1).

Для формирования и функционирования ЕГИСЗ введены понятия «иная информационная система в сфере здравоохранения» и «оператор иной информационной системы, который является участником информационного обмена». Это позволяет всем организациям, обеспечивающим запись к врачу, коммуникации между врачом и пациентом, управлять потоками пациентов – подключаться к единой системе идентификации аутоидентификации и взаимодействовать с ЕГИАСЗ, иметь доступ к регистрам медицинских организаций, застрахованных пациентов. Все учреждения, предоставляющие сервисы по организации медицинских консультаций, и дей-

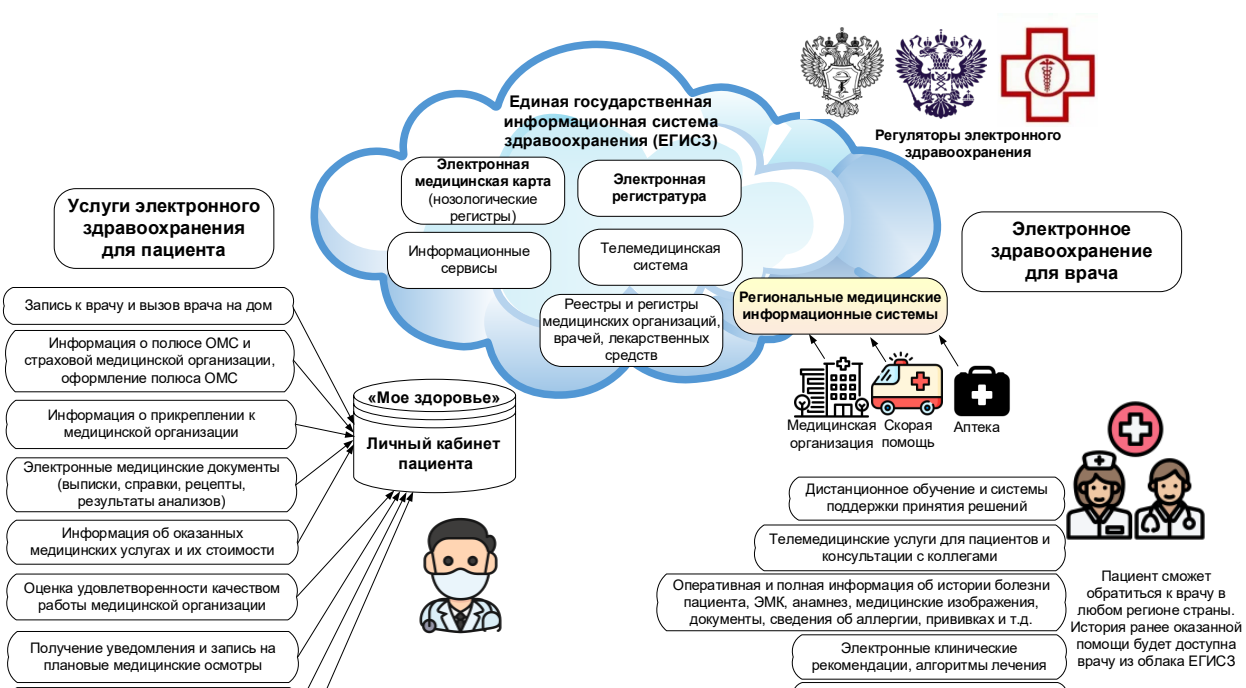


Рисунок 1 – Единая государственная информационная система здравоохранения (ЕГИСЗ)

ствующие информационные системы становятся законными и могут использоваться в ЕГИАСЗ.

Цифровизация в сфере здравоохранения повышает эффективность оказания медицинских услуг [4]. Электронный документооборот в медучреждениях облегчает ведение учета, выводит качество обработки и хранения данных на новый уровень, повышает эффективность контроля за оказанными медицинскими услугами, распределением финансовых ресурсов и т. д. Но такая цифровизация имеет и обратную сторону – повышаются риски нарушения информационной безопасности, когда информация из электронных баз данных больниц и клиник используется в корыстных целях.

Безопасность в медицинской и фармакологической сферах имеет особую значимость, так как является составляющей социальной подсистемы государства [5].

В условиях рыночной экономики система здравоохранения стала одной из отраслей бизнеса. Бизнес-процессы медицинских и фармацевтических компаний связаны, в том числе, с обработкой большого объема критически важной информации: персональных данных, больничных листов, историй болезни, результатов диагностики, назначений и многого другого. А сама информация стала рентным товаром.

2. Информация – элемент рентной экономики

Рента – это регулярно получаемый доход с капитала.

Под капиталом следует понимать «*овеществлённый труд, возникающий в результате коммуникационных отношений (часто агрессивных), направленный на выстраивание цепочек заведомо неэквивалентных обменов себя на живой труд, слабые капиталы, криминальную ренту и пр. с целью реализовать себя в качестве самовозрастающей стоимости*» [6].

Рента может иметь различную природу: товарная; административная; военная. Товарная рента, в свою очередь, может превращаться в эксклюзивную ренту. А возникающий на основе ренты капитал становится основой власти, в том числе и глобальной.

Базовой является товарная рента – это прибыль, которую капиталист зарабатывает при производстве товаров. Её извлечение является

процессом фундаментальным для расширенного воспроизводства капитала, лежащего в основании всех остальных экономических процессов. Товарная рента:

во-первых, привела к рождению капитала, а тот, в свою очередь, породил ту социальную среду, в которой он мог бы эволюционировать;

во-вторых, процесс извлечения капиталом товарной ренты наполнил Мир морем товаров, в бурных «водах» которого возникла эксклюзивная рента.

Товарная рента возникает в процессе вращения обычных товарных циклов.

Катализатором, оживляющим товарные циклы, является прибыль, а если быть точнее, то жажда наживы. В итоге именно она заставляет крутить товарные циклы, обеспечивая капиталу расширенное воспроизводство.

До появления денег функцию эквивалента ресурсов, прибыли и свободного капитала исполняли пользовавшиеся устойчивым спросом товары длительного хранения.

На фундаменте товарной ренты возникла административная рента – рента структур, защищающих капитал глобальных структур управления. Это рента в обмен на услуги по созданию и содержанию социальной инфраструктуры, необходимой для расширенного воспроизводства капитала, предполагающего обеспечение прав собственности на капитал, создание как можно большей по размеру консолидированной зоны разделения труда, способствующей его углублению, и, как следствие, интенсификации товарного обмена. Данному процессу непременно сопутствуют войны и сопутствующая ей военная рента.

Товарные циклы непрерывно съедают платёжеспособный спрос, перерабатывая его в накопления. Регулярная военная добыча и дань, расширение инвестиционного контура на производство вооружения и военной техники, а затем восстановление разрушенной инфраструктуры, позволяют восстановить товарно-денежный обмен и затем поддерживать его, регулярно восполняя изъятие капиталами денег из обращения. Перманентная череда военных конфликтов в последнее время: Ирак, Ливия, Афганистан, Сирия, Украина, Палестина, в конце концов, имеют один и тот же замысел – восстановление нарушенных товарно-денежных отношений в результате изъятия капитала (обогащения глобального олигархата) и падения платежеспособного спроса (нарушение товарно-денежного баланса).

Быстро накапливаясь, свободный капитал постоянно решает задачу поиска новых инвестиционных ниш для собственного расширенного воспроизводства (рис. 2). Ввиду их дефицита он проявляет тенденцию к конкуренции за часть товарной, военной и административной ренты.

Издавна известны такие виды ренты, как:

– рента от международной морской торговли;
– колониальная рента;
– континентальная сетевая рента;
– ссудная рента;
– криминальная рента и др.

Современная глобальная цифровизация породила новый рентный товар – информацию (правильнее – данные). Использование информации о жизни и здоровье людей становится возможностью неявно и безраздельно подчинять себе всех людей, так или иначе обращающихся за медицинской помощью.

Глобальный финансово-экономический кризис 2007-2009 гг. не только подвел некоторую условную черту под современным этапом глобализации, но и де-факто ознаменовал собой переход мировой экономики в качественно новое состояние, а может быть, и на новый этап развития. Ожидания того, что после кризиса экономика снова вернется к предыдущей модели роста, не оправдались. После так называемого посткризисного отскока в 2010 г. темпы роста мировой экономики в 2011-2016 гг., по данным МВФ, устойчиво снижались (с 4,2% в 2011 г. до 3,1% в 2016 г.) (World Economic Outlook, 2017). А в 2023 г. ожидается снижение до 2,8% [7].

Эти процессы происходят на фоне исчерпания потенциала дальнейшего роста производительности труда в условиях существующего технологического уклада. Кризис стал лишь

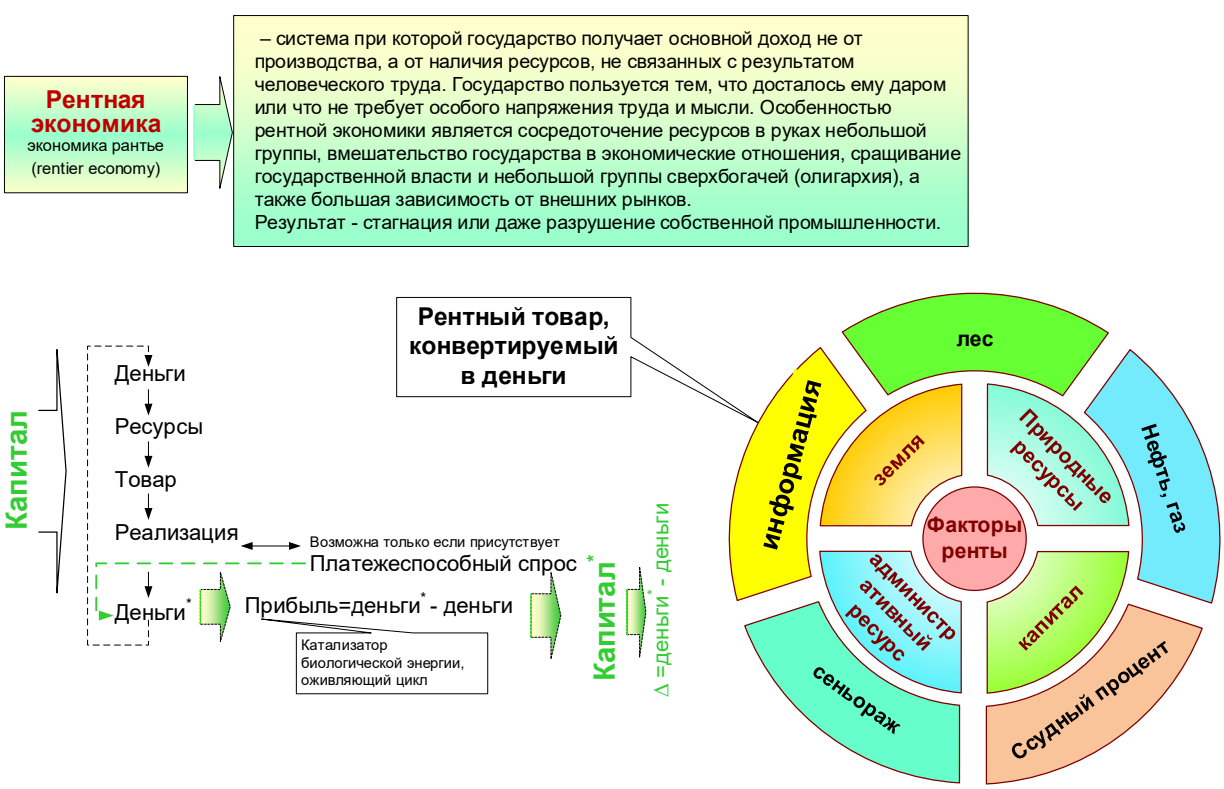


Рисунок 2 – Рентная экономика

одним из этапов формирования новой конфигурации и разрушения старых финансовых, экономических и технологических структур. Поскольку с 1970-х гг., после развала Бреттон-Вудских соглашений, решающую роль в мировом развитии приобрели финансы, хотя при этом именно сложившаяся финансовая система подошла к исчерпанию механизмов своего развития (это обозначил кризис 2007-2009 гг.), то вполне закономерно, что формирование новой конфигурации подразумевает прежде всего поиск механизмов сохранения и дальнейшего расширенного воспроизводства мировых финансов. Кризис и длительная фактическая стагнация (официально – крайне низкие темпы роста) мировой экономики подтолкнули мировых лидеров к поиску и разработке новых глобальных проектов с целью трансформации сложившейся финансовой системы и создания новых механизмов обеспечения экономического роста и повышения производительности труда.

В конечном счете таковым стал проект развития цифровой экономики (ЦЭ), к которому к 2017 г. подключилось большое число стран мира, включая Россию. ЦЭ стала темой номер один на всех крупнейших международных площадках и саммитах, включая Экономический форум в Давосе (Deep Shift…, 2014), G20, G7, ШОС, БРИКС. Так, развитие ЦЭ в качестве одного из приоритетных направлений консолидированных международных усилий нашло отражение в итоговых документах всех последних саммитов G20 (2015, 2016 и 2017 гг.). В 2018 г. эта тема стала ключевым пунктом повестки G20 [8]. Такие международные организации и институты, как МВФ, Всемирный банк и ОЭСР, стали разрабатывать различные индексы измерения ЦЭ, а также своды рекомендаций ее развития (Measuring the Digital…, 2014), а национальные правительства, в свою очередь, почти повсеместно приняли соответствующие программы развития ЦЭ в своих странах [9]. Несмотря на революционность, ЦЭ в действительности основывается на множестве технологий, которые развиваются уже более десятилетия, однако некоторые из них пока до сих пор не смогли создать новые массовые производства и рынки (например, робототехника, искусственный интеллект и т.п.).

Распространение ЦЭ в качестве глобального проекта началось с 2010-х гг., при этом в основе проекта оказались «кардинальные технологические изменения», которые могли бы стать главным драйвером преодоления «Великой рецессии» (ICT for Economic Growth…, 2009). Здесь также следует отметить, что смена технологического уклада, или новая технологическая революция, была выбрана в качестве средства перезапуска экономического роста неслучайно. На протяжении XX в. технологические новации демонстрировали способность продуцировать быстрый экономический рост. Однако гораздо важнее то, что сложившаяся на Западе в XIX в. модель научно-технологического прогресса (НТП) принципиально предполагает, что очередной технологический виток непременно сопровождается дальнейшим углублением процессов разделения труда, а это закономерно приводит к необходимости увеличения объемов рынков сбыта продукции (с целью окупить следующий технологический рывок) и установлению контроля над ними. При этом дальнейшее поддержание контроля возможно, как правило, за счет формирования локальной монополии на рынке, что обеспечивается непрерывным созданием новых инновационных продуктов. Как следствие, развитие экономики в рамках данной модели НТП неминуемо ведет к сокращению числа стран (и компаний-производителей), которые выпускают массовую высокотехнологичную продукцию, а также разделению всех стран на технологически независимые и зависимые [10].

Широкое внедрение цифровых технологий, в том числе, в здравоохранении породило, с одной стороны, новую рентную нишу получения капитала, а с другой стороны, высокую конкуренцию среди организаций и учреждений здравоохранения и фармакологической промышленности не за здоровье и жизнь людей, а за получение дополнительной прибыли.

3. Кибербезопасность в системе здравоохранения

Угрозы кибербезопасности медицинских учреждений чрезвычайно актуальны, поскольку сопряжены с угрозой жизни пациентов. Компания Proofpoit (США) и Ponemon Institute выпустили исследование о состоянии кибербезопасности в здравоохранении [11]. Их исследования стали основой для установления трендов в сфере обеспечения кибербезопасности в здравоохранении.

Для исследования было опрошено 653 ИТ (специалистов в области информационных технологий) и ИБ-специалистов (специалистов в области информационной безопасности), работающих в медицинских организациях. Основные выводы выглядят следующим образом [12].

По сравнению с 2021 г. тенденции в 2022 г. сохранились: 88% организаций подвергались минимум одной, а, в среднем, 40 кибератакам за истекший год.

Средняя стоимость кибератаки составила почти $5 млн, что на 13% выше, чем в предыдущем году ($4,4 млн). Стоимость складывалась из прямых и косвенных затрат на ликвидацию инцидента информационной безопасности, а также упущенной выгоды.

Потери от простоя из-за киберинцидента в среднем составили $1,3 млн – на 30% выше, чем в прошлом году.

Все опрошенные медицинские организации сталкивались с утечками данных за последний год, среднее количество инцидентов информационной безопасности такого характера – 19.

Инсайдеров назвали основной причиной утечек данных, на втором месте – халатность сотрудников.

В отчете исследователи кибербезопасности рассмотрели влияние различного типа атак на оказание медицинской помощи: компрометация облачных сервисов и корпоративной электронной почты, кибератаки на цепочки поставок и программы-вымогатели. В отличие от прошлого года, программы-вымогатели отошли на второй план: чаще всего атаковали облачные сервисы (74%). Отмечен рост количества кибератак через электронную почту (64%).

При всех вышеуказанных типах кибератак от 68% до 77% случаев в конечном итоге негативно

влияли на уход за пациентами и мешали оказанию медицинской помощи (задержка в оказании процедур, анализов и др.), что сопровождалось осложнениями, в 21% – 29% отмечено, что кибератаки повлияли на рост смертности.

Основными проблемами при обеспечении кибербезопасности организации специалисты назвали:

– недостаток собственного профессионального опыта (58% против 53% в 2022 году);

– нехватка специалистов в сфере кибербезопасности (50% против 46%);

– нехватка бюджета (47% против 41%).

Количество зарегистрированных в мире утечек персональных данных из медицинских учреждений, в том числе, номеров социального страхования, реквизитов платежных карт, специфических медицинских записей о состоянии здоровья, историй болезни пациентов, неуклонно растет из года к году. В России за последние 2-3 года отмечен был резкий рост количества «медицинских» утечек, который измеряется не процентами, а уже кратно [13].

Развитие новых технологий, в том числе телемедицины, а также способов использования медицинских данных в электронном виде, увеличивает ценность медицинской информации. Поэтому в ближайшей перспективе число утечек такой информации и объем скомпрометированных данных как в мире, так и в России неизбежно будут расти [14].

4. Классификация каналов и похищаемой медицинской информации

Рост спроса на медицинские услуги с одновременным повышением требований к их качеству и защищенности приводит к неизбежному увеличению стоимости медицинских услуг. Это ставит перед государством очень серьезную проблему – как обеспечить доступность всех видов медицинской помощи, гарантированной законодательством и при этом гарантировать медицинскую тайну.

Простым увеличением затрат на здравоохранение, как свидетельствует и отечественный, и мировой опыт, эту проблему не преодолеть. Решение может быть найдено только в интеграции всех имеющихся в системе здравоохранения ресурсов, а также в их оптимизации и эффективном планировании.

Речь идет о повышении качества управления, оптимизации потоков пациентов, устранении излишних бюрократических звеньев, организации безбарьерного взаимодействия между всеми звеньями системы здравоохранения, активизации процессов широкого и быстрого внедрения в медицинскую практику новейших технологий диагностики, лечения и обеспечения информационной безопасности.

Медицинские организации обрабатывают большой объем сведений ограниченного распространения. Если систематизировать эти данные, то можно выделить следующие виды утечек информации в медицинских учреждениях:

1. Персональные данные пациентов, ответственность за утечку которых регламентирована законодательством и другими нормативными актами. Утечка персональной информации в медицинских учреждениях – наиболее «популярный» вид внутренних угроз практически во всех отраслях. Масштабы утечек персональной информации в 2022 году растут большими темпами во всех отраслях, и медицинская сфера не стала исключением.

2. Медицинская тайна, в том числе врачебная. Согласно закону, врачебная тайна – это данные о состоянии здоровья и диагнозе человека, результаты медицинского обследования и лечения (№323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»). Сам факт обращения за медицинской помощью также относится к врачебной тайне. Разглашение сведений, составляющих врачебную тайну, не допускается.

3. Данные автоматизированных информационных систем, выгрузки из которых могут стать объектом утечки и доступны внутренним инсайдерам. Медицинские организации, например, используют единую государственную информационную систему в сфере здравоохранения (ЕГИЗ). В таких системах хранятся данные электронной медицинской карты, журналов учета, сведения

о распределении бюджетных средств, данные о зарплатах, премиях сотрудников медицинских учреждений и т. д.

4. Коммерческая тайна (особенно актуально для медицинских организаций коммерческого сектора). К коммерческой тайне относят базы данных клиентов (пациентов), бизнес-планы, стратегические планы развития, обучающие методики, методологию контроля качества и т. д.

5. Сведения, содержащиеся в материалах служебных проверок и проверок исполнения обязанностей, соблюдения ограничений, запретов и требований к служебному поведению, установленных с целью противодействия коррупции и мошенничества [15].

Утечки информации могут быть в результате внешнего воздействия на базы данных медицинских учреждений, локальные сети, использования вредоносных программ, программ-вымогателей и т.д., а также в результате вредоносной деятельности источников – сотрудников (рис. 3).

Возможные сценарии утечки информации в медицинских учреждениях можно разделить на два блока: утечки, которые произошли случайно (по неосторожности), и злонамеренные утечки (умышленные).

Случайные утечки информации в медицинских учреждениях происходят по причине нехватки квалифицированных кадров и слабой киберграмотности персонала медицинских учреждений. В заголовки СМИ регулярно попадают новости о выброшенных на улицу и в мусорные баки медицинских картах, историях болезни. Чаще всего такие утечки происходят из-за низкой осведомленности сотрудников о возможных рисках и последствиях. Причины случайных утечек в медицинских учреждениях могут состоять и в ошибочных действиях персонала – так называемый человеческий фактор (отправка документов по ошибке, отправка сведений ограниченного доступа на свою личную электронную почту и т. д.).

Наиболее интересны умышленные сценарии утечки информации. Они происходят, когда у сотрудника медицинского учреждения есть намерение получить личную выгоду. Например, сотрудница службы муниципальной скорой помощи передавала данные об умерших и тяжелобольных пациентах представителям заинтересованных организаций за вознаграждение. Мошеннические действия сотрудников медицинских учреждений чаще всего связаны с передачей

Рисунок 3 – Классификация угроз информационной безопасности медицинского учреждения

(продажей) персональных данных пациентов, сведений об их заболеваниях третьим лицам.

Если в глобальной картине «медицинских» утечек около 30% инцидентов были связаны с внешними атаками злоумышленников, то в России все зафиксированные случаи носили исключительно внутренний характер (рис 4). Классический для России пример внутренней утечки из медицинских учреждений – это «слив» сотрудниками больниц и клиник данных о тяжелобольных и умерших пациентах ритуальным агентам.

Культура обращения с информацией ограниченного доступа у медицинских работников в России находится на довольно низком уровне. Кроме того, внутренние злоумышленники в различных медучреждениях осознали, что персональные данные пациентов и коллег остаются без должного контроля, а из кражи такой информации можно извлечь выгоду (рис 5).

В то же время, доля умышленных утечек информации, совершенных сотрудниками медучреждений, в России существенно выше, чем в мире – 39% против 30%.

В России и в мире примерно четверть «медицинских» утечек была сопряжена с квалифицированными действиями злоумышленников – мошенничеством или превышением прав доступа к информационным системам. При этом в России доля таких «квалифицированных» утечек возрастает значительно.

Информатизация российской медицины пока происходит недостаточно высокими темпами по сравнению с мировыми. Развитие медицинских систем сегодня носит скорее хаотичный характер, клиники все еще работают с большими массивами информации в бумажном виде – эти факторы делают отечественную сферу здравоохранения менее привлекательной мишенью для внешних злоумышленников – хакеров, организованной киберпреступности.

Компрометации в российских медучреждениях подвергались практически только персональные данные клиентов и персонала, в то время как медучреждения во всем мире также теряли и платежную информацию (12,2%), и данные, которые относятся к категории коммерческой тайны и ноу-хау (0,8%) (рис. 6).

4.1. Источники утечки информации

Распределение инцидентов по каналам утечек в системе здравоохранения в Российской Федерации существенно отличается от мирового (рис. 7). Так, для России характерна более высокая доля утечек через бумажные носители – 24% про-

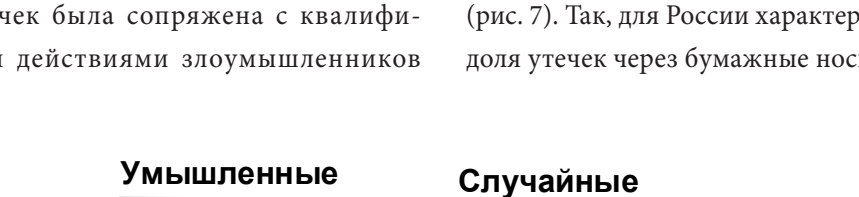


Рисунок 4 – Внутренние утечки данных из медицинских учреждений по типу умысла

Рисунок 5 – Доли инцидентов из медицинских учреждений по характеру

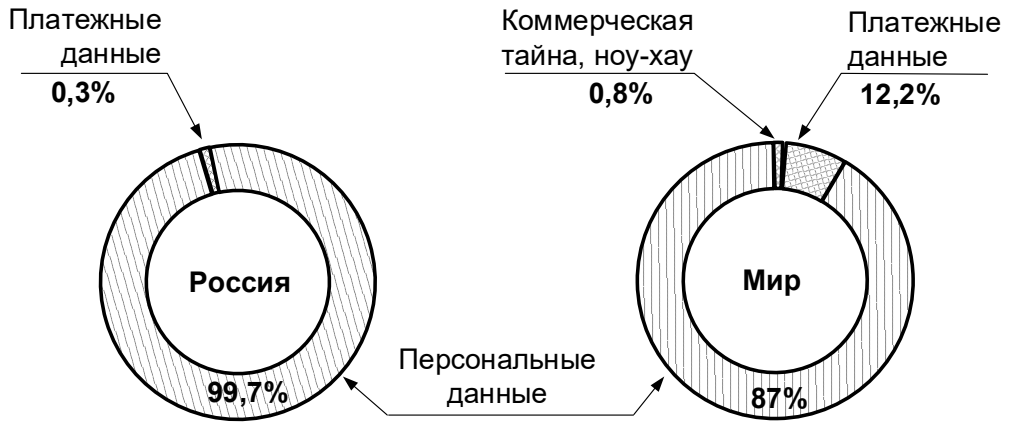


Рисунок 6 – Распределение долей утечек данных в медицинских учреждениях по типу информации

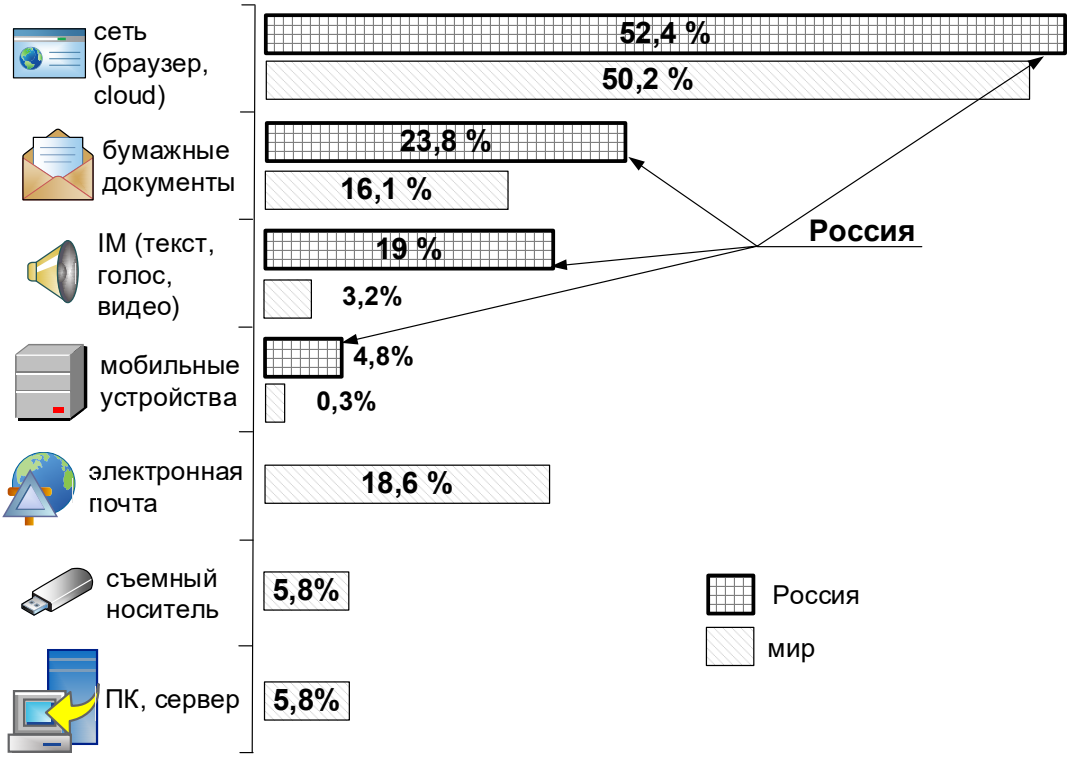


Рисунок 7 – Каналы утечек из медицинских учреждений

тив 16% в мире, а также посредством мгновенных сообщений – 19% против 3% в мире.

4.2. Доля утечек по отраслям

В целом организации сферы здравоохранения занимают одно из первых мест среди всех отраслей хозяйства по такому показателю, как воздействие на информационные активы со стороны внутренних злоумышленников (рис. 8). Именно по вине сотрудников, топ-менеджеров и системных администраторов медучреждений происходит подавляющее большинство инцидентов, утекает основной объем записей в данной сфере [16].

Цена, которую медицинская отрасль вынуждена платить, ликвидируя последствия утечек информации, постоянно возрастает. По оценкам профильных аналитических агентств, средний ущерб компаний различных отраслей от каждой утечки данных, которая произошла в результате действий внутреннего злоумышленника, составляет $8,5 млн. По мере роста ценности информации медицинских организаций, продолжит расти и число злоумышленников, которые стремятся ею завладеть.

С учетом того, что в медицинских учреждениях России в подавляющем большинстве объектом утечки информации являются персональные

Рисунок 8 – Доля внутренних утечек в различных отраслях

данные, то далее следует рассмотреть статистику, риски и угрозы, экономический и репутационный ущерб в связи утечкой персональных данных.

5. Объекты защиты информации медицинских учреждений

5.1. Персональные данные

Утечка персональных данных может привести к негативным последствиям как для медицинской организации с точки зрения необходимости уплаты штрафов, уголовной ответственности, потери репутации (особенно когда речь идет о частной клинике), но также для медицинского персонала и самого пациента. Например, утечка сведений о том, что пациент болеет ВИЧ, может стать поводом для преследования, буллинга , увольнения и т.д. Обеспечение безопасности медицинской тайны, персональных данных и других конфиденциальных сведений является важным шагом для минимизации репутационных и финансовых рисков [17].

Персональная информация относится к категории сведений, защищаемых законом. В связи с этим любой оператор, который имеет отношение к хранению и обработке данных, обязан придерживаться определенных правил в своей деятельности и принимать дополнительные меры для обеспечения защиты информации от ее нецелевого использования. Рекомендации и указания по этому вопросу определены в 152-ФЗ о защите персональных данных от 27.07.2006 г. [18]. Данный нормативный акт является основополагающим документом, регулирующим отношения между владельцем личных данных и оператором.

Данный нормативный акт устанавливает перечень базовых понятий, вокруг которых распространяется действие закона. Ключевыми понятиями являются следующие.

Персональные данные – сведения произвольного характера, которые косвенно или прямо способны идентифицировать конкретного человека.

Персональные данные с правом свободного распространения – сведения, к которым открыт неограниченный доступ со стороны владельца путем заключения согласия на обработку.

Оператор – любой орган, физическое или юридическое лицо, которые используют персональную информацию: обрабатывают, хранят, передают согласно установленным целям.

Обработка персональных данных – процедура, в ходе которой происходит исполнение таких процессов как сбор, запись, систематизация информации вручную или посредством автоматизированных инструментов.

Любая организация, независимо от ее размера и специфики деятельности, так или иначе ведет

обработку персональной информации, касающейся собственных сотрудников, пациентов.

При расследовании инцидентов, связанных с утечками, кражей персональных сведений, к виновным лицам могут быть применены следующие меры наказания:

– дисциплинарная ответственность. Выносится на основании статей 81, 90, 192 ТК РФ за мелкие нарушения, не повлекшие за собой значимого ущерба и последствий. Обычно выражается в форме замечания, выговора, в крайних случаях заканчивается увольнением сотрудника;

– гражданско-правовая ответственность. Выносится на основании статьи 15 ГК РФ в виде соразмерного возмещения причиненных убытков или в меньшем объеме, исходя из законодательных и трудовых нормативов;

– административная ответственность. Выносится на основании статей 13.11, 19.7 КоАП РФ. В качестве меры наказания виновному лицу назначается штраф в размере 1.000-50.000 рублей, исходя из тяжести последствий преступления;

– уголовная ответственность. Выносится на основании статей 137, 140, 272 УК РФ за нарушения, повлекшие тяжелые последствия. В качестве наказания могут быть назначены крупный штраф, либо принудительные или обязательные работы, либо тюремное заключение.

Любая организация и физическое лицо при работе с персональной информацией должны в обязательном порядке придерживаться требований и рекомендаций 152-ФЗ о защите персональных данных. В противном случае придется отвечать по всей строгости закона. Защита персональных данных людей входит в приоритетную задачу национальной безопасности РФ.

Приведем несколько примеров утечки персональных данных из баз данных медицинских учреждений.

Пример 1. *Утечка базы данных клиентов.*

В конце октября 2023 года стало известно об утечке данных одной из клиник сети «РЖД-Медицина». Речь идет о лечебном учреждении во Владивостоке. Хакерская группировка UHG получила три текстовых файла со следующими записями клиентов медицинского центра:

- *ФИО;*
- *номер телефона (23,1 тыс. уникальных номеров);*
- *адрес электронной почты (11 тыс. уникальных адресов);*
- *хешированный пароль;*
- *адрес;*
- *серия/номер паспорта;*
- *СНИЛС;*
- *номер полиса ОМС;*
- *пол;*
- *дата рождения;*
- *дата регистрации и последнего входа в личный кабинет (с 20.06.2017 по 23.10.2023).*

В Vk был размещен дамп[1], имеющий отношение к клинике «РЖД-Медицина», находящейся во Владивостоке. Дамп включает папку с результатами анализов пациентов, файлы Patients, Registration и Users.

Медицинские данные по данным «Лаборатории Касперского» на черном рынке стоят больше банковских [19]. Данные размещаются в Дарнете, за которые просят значительную плату. И таких объявлений с каждым годом становится всё больше. Продаваемая информация содержит медицинские данные, в том числе, из медицинских карт и страховых полисов, поскольку она считается ценным ресурсом для злоумышленников. Такие медицинские данные могут использоваться для того, чтобы входить в доверие к пользователям, обманывать их самих или их родственников.

Доступ к данным электронных медицинских карт может быть интересен не только для того, чтобы красть их. Хакеры могут вносить в них изменения, чтобы совершать целевые атаки и намеренно затруднять постановку диагнозов.

Рост интереса хакеров к медицинским компаниям, которые все чаще становятся жертвами про-

1 Дамп (англ. dump – сбрасывать) – файл, включающий в себя содержимое памяти компьютера или базы данных.

грамм-шифровальщиков, определяется тем, что:

– в настоящее время существует недостаточно серьёзное восприятие рисков, связанных с цифровизацией, в индустрии здравоохранения;

– отсутствует должное внимание к вопросам обучения сотрудников базовым навыкам кибербезопасности.

За 2022 г. в медицинских организациях по всему миру было атаковано каждое пятое цифровое устройство. Число подобных атак по прогнозам специалистов в сфере кибербезопасности будет расти, особенно в развивающихся странах, где только начинается процесс цифровизации таких услуг. В частности, будет все больше целевых атак с помощью программ-шифровальщиков, которые приводят к потере доступа к внутренним данным или ресурсам. Это чревато нарушениями в процессе постановки диагноза и даже лишением пациентов помощи, которая требуется немедленно.

Также в исследовании говорится о росте количества атак на научно-исследовательские медицинские институты и фармацевтические компании. Так, в 2019 году были атакованы 49% устройств в фармкомпаниях [20].

Российские медицинские компании, как правило, стараются не предавать публичной огласке факты нарушения кибербезопасности, чаще оплачивая запросы программ-вымогателей. Поэтому установить точную статистику по утечкам информации из российских медицинских учреждений достаточно сложно. Но для хакеров не существует государственных границ.

С учетом того, что в Российской Федерации, как правило, не фиксируются атаки на медицинские учреждения, а это не значит, что их вовсе нет, то в качестве примеров проиллюстрируем нарушение кибербезопасности на примере нескольких иностранных медицинских учреждений.

Пример 2. *Персональные данные около 9 млн человек были украдены в результате кибератаки на службу медицинской транскрипции Perry Johnson & Associates (PJ&A) из американского штата Невада.*

Компания PJ&A предоставляет медицинским организациям услуги расшифровки записей исследований пациентов. В уведомлении, которое было подано в министерство здравоохранения и социальных служб США, PJ&A сообщила, что более 8,95 млн человек пострадали в результате утечки данных в 2023 г.

PJ&A заявляет, что начала уведомлять пациентов о нарушении их конфиденциальности. Согласно сообщению компании, украденные данные включали имена и даты рождения пациентов, а также их адреса, медицинские записи и номера аккаунтов, установленные при госпитализации диагнозы, а также даты предоставления услуг. В результате инцидента также утекло некоторое количество номеров социального страхования и клинические данные из файлов медицинской транскрипции, включая результаты лабораторных и диагностических исследований, названия лекарств, наименования лечебных учреждений и поставщиков медицинских услуг.

Инцидент в компании Perry Johnson & Associates затронул как минимум двоих ее корпоративных клиентов, включая Northwell Health, крупнейшую сеть клиник в штате Нью-Йорк. В результате атаки на службу медицинской транскрипции в его организации были скомпрометированы данные 3,89 млн пациентов. Ранее Northwell Health пострадала в результате атаки на компанию Nuance Communications, которая предоставляет ИТ-решения для медицины.

Cook County Health, система здравоохранения из штата Иллинойс, в публичном уведомлении сообщила, что в ходе атаки на PJ&A утекли данные 1,2 млн ее пациентов. В частности, скомпрометированы 2600 номеров социального страхования.

По данным министерства здравоохранения и социальных служб США, утечка из PJ&A является одной из крупнейших в 2023 году среди медицинских организаций. По масштабу она уступает только нарушению в компании HCA Healthcare, которая потеряла записи около 11 млн пациентов [21].

Пример 3. *Американская сеть клиник McLaren Health Care уведомила, что более 2 млн человек в 2023 г. пострадали из-за того, что были скомпрометированы их персональные данные. Согласно заявлению организации, персональные данные множества пациентов утекли в результате хакерского вторжения.*

McLaren Health Care – некоммерческая сеть здравоохранения, включающая 14 больниц в штате Мичиган. Служба расследований США подтвердила, что в результате несанкционированного доступа в информационные системы McLaren были скомпрометированы следующие типы данных: полные имена, номера социального страхования (SSN), даты рождения, информация о выставлении счетов или претензий, диагностическая информация, сведения о врачах, номера медицинских карт, информация о программах Medicare/Medicaid, данные о рецептах и назначенных лекарствах, информация о лечении. Набор скомпрометированных данных у тех или иных пациентов может различаться в зависимости от того, какую информацию люди предоставляли клинике и какие услуги они получали.

McLaren уже уведомила об утечке информации власти США и сообщила о ней по электронной почте всем пострадавшим, отправив им инструкцию по использованию бесплатных услуг по защите персональных данных сроком на 12 месяцев.

Представители McLaren Health Care советуют всем пострадавшим лицам осторожно воспринимать любые сообщения и внимательно отслеживать операции по своим банковским счетам.

Ответственность за инцидент взяла на себя хакерская группировка ALPHV, также известная как BlackCat. Хакеры опубликовали фрагмент данных, которые были якобы украдены у McLaren, и пригрозили продать на аукционе весь набор информации, который, по словам злоумышленников, затрагивает 2,5 млн человек [22].

Пример 4. *Атака с использованием вируса-вымогателя привела к тому, что медики из Канады потеряли персональные данные сотен тысяч пациентов. В руки хакеров также попали персональные данные сотрудников ряда клиник.*

Хакерская группировка Daixin взяла на себя ответственность за атаки на пять больниц, расположенных на юго-западе провинции Онтарио. Несколько наборов украденных данных злоумышленники выложили в сеть.

Инцидент привел к сбою в работе ряда систем, включая программы для записи пациентов и электронную почту. Пострадали пять клиник: Windsor Regional Hospital, Erie Shores HealthCare, Hôtel-Dieu Grace Healthcare, Bluewater Health, а также Chatham-Kent Health Alliance. Все они отмечали задержки в приеме пациентов.

Атака также затронула компанию TransForm, которая занимается внедрением ИТ и расчетом заработной платы по договорам с канадскими медучреждениями. В Transform заявляют, что не стали выплачивать выкуп за возврат данных, но пообещали связаться со всеми людьми, у которых утекли данные.

Хакерам удалось украсть данные с общего файлового сервера. Эта информация включала сведения «разного объема и уровня конфиденциальности» о пациентах. Украденные данные содержали сведения о 5,6 млн приемов 267 тыс. уникальных пациентов. Утечка информации затронула идентификационные номера сотрудников (SIN) и банковские сведения.

Представители другой клиники – Chatham-Kent Health Alliance заявляют, что хакеры похитили данные о 1446 сотрудниках, которые работали в клинике. Эта информация включает имена, SIN, адреса и размеры окладов. Данные электронных медицинских карт не были затронуты, но злоумышленники могли получить доступ к некоторым сведениям о пациентах.

Согласно заявлению Erie Shores HealthCare, в руки хакеров попали 352 номера SIN, принадлежащих сотрудникам. По данным Windsor Regional Hospital, с ее сегмента на общем файловом диске

утекли некоторые данные пациентов: либо имена, либо краткое описание состояния здоровья. Также была скомпрометирована некоторая информация о сотрудниках, включая штатное расписание.

Hôtel-Dieu Grace Healthcare заявляет, что взломанный сервер содержал некоторые данные о ее пациентах, но какие конкретно сведения утекли, предстоит определить в ходе анализа. Также скомпрометированы отдельные данные сотрудников этой больницы, при этом SIN и банковская информация не были затронуты.

Все канадские больницы, которые пострадали от кибератаки, предлагают бесплатные услуги кредитного мониторинга своим пациентам и персоналу [23].

***Пример 5.** Топ-менеджер киберфирмы стал хакером и взломал две больницы.*

Один из бывших руководителей компании по кибербезопасности взломал две клиники, входящие в состав медицинского центра Гвинетт (GMC). Стать хакером топ-менеджер решил с целью стимулирования бизнеса своей фирмы.

Викас Сингла (Vikas Singla), работавший в компании Securolytics, которая предоставляла услуги сетевой безопасности в сфере здравоохранения, признал себя виновным во взломе информационных систем клиник GMC Northside Hospital в городах Дулут и Лоренсвилль. Обвинительное заключение прокуратуры было представлено в июне 2021 г.

По данным следствия, 27 сентября 2018 г. в ходе атаки Сингла нарушил работу телефонной связи и сетевого принтера медицинского учреждения, а также персональные данные более 200 пациентов из дигитайзера, подключенного к аппарату для маммографии в больнице Лоренсвилля.

В тот же день Сингла подключился к 200 принтерам больницы GMC в Дулуте для распечатки украденной информации о пациентах. Он также отправил на печать лозунг «Мы владеем вами!».

В заключении следствия отмечается, что обвиняемый публиковал информацию об атаке и разглашал сведения о пациентах с целью развития бизнеса компании Securolytics.

Известно, что Викас Сингла рассказал о взломе GMC в Твиттере, разместив там украденные данные 43 пациентов (имена, даты рождения, пол). После этого ряд потенциальных клиентов Securolytics получили сообщения, где акцент делался на инцидент в GMC.

Обвинения Сингле предъявлены по 17 пунктам умышленного нанесения ущерба защищенным компьютерам и одному пункту получения информации с защищенного компьютера. Прокуратура утверждает, что атака ответчика на телефонную систему ASCOM, принтеры и дигитайзер в клиниках GMC привела к финансовым потерям на сумму 817 тыс. долларов США.

В рамках сделки по признанию вины Викас Сингла готов полностью возместить причиненные убытки, а также выплатить проценты по ущербу клинике Northside Hospital Gwinnett в Лоренсвилле, а также американской страховой компании Ace.

Прокуратура рекомендует назначить обвиняемому наказание в виде 57 месяцев условно и поместить его под домашний арест. Столь мягкий вариант наказания мотивирован тем, что у Синглы диагностирована редкая и неизлечимая форма рака, также бывший топ-менеджер страдает серьезным сосудистым заболеванием.

Самое строгое наказание, которое грозит Викасу Сингле, – 10 лет тюремного заключения. Приговор будет оглашен 15 февраля 2024 г.

***Пример 6.** Утекли персональные данные миллионов пациентов в Филиппинах.*

В результате кибератаки с использованием вируса-вымогателя Medusa украдены данные по меньшей мере 13 млн клиентов Филиппинской корпорации медицинского страхования (PhilHealth). Также утекли персональные данные ряда сотрудников корпорации.

«Утекли действительно данные миллионов. Пока можно предположить, что он [инцидент] охватывает около 13 млн человек. Мы только завершаем разбор, чтобы получить полную информацию», – заявила на пресс-конференции старший вице-президент PhilHealth и специалист по конфиденциальности данных Нерисса Сантьяго (Nerissa Santiago).

По словам Сантьяго, помимо конфиденциальной информации миллионов застрахованных пациентов, также утекли данные от 600 до 800 сотрудников PhilHealth. Все пострадавшие работники уже проинформированы об инциденте, в ближайшее время корпорация начнет оповещение клиентов.

Поскольку количество жертв утечки информации велико, PhilHealth воспользовалась базой департамента информационных и коммуникационных технологий (DICT), чтобы тщательно проверить и проанализировать данные.

«Компания готова принять все меры для предотвращения подобных инцидентов в будущем и гарантирует бесперебойную работу своих сервисов», - заявил президент и главный исполнительный директор PhilHealth Эммануэль Ледесма-младший (Emmanuel Ledesma Jr.). При этом Ледесма выразил удивление по поводу решения Совета директоров компании о переназначении семи членов исполнительного комитета. При этом, по его словам, Совет директоров еще не издал директивы о том, куда будут переведены эти должностные лица.

***Пример 7.** В Сеть утекли персональные данные 2 млн пациентов из Египта.*

Власти Египта подтвердили, что недавно утекли персональные данные получателей медицинских услуг по президентской программе оплаты сложных операций. Украденные персональные данные пациентов хакеры продают на подпольном форуме.

Министр здравоохранения и демографии Египта Халед Абдель-Гаффар (Khaled Abdel-Ghaffar) подтвердил, что государственные органы разобрались с утечкой персональных данных 2 млн пациентов. В заявлении для местных СМИ министр сказал, что утечка произошла два месяца назад.

Впервые об утечке конфиденциальной информации египетских пациентов 23 июля сообщила фирма Falcon Feeds, которая анализирует объявления о продаже данных в дарквебе. Специалисты фирмы обнаружили, что конфиденциальная информация 2 млн египтян продавалась за 5 тыс. долларов.

На подпольном форуме Popürler неизвестный хакер представил образец украденных данных, включающий записи 1000 пациентов. Для связи с ним заинтересованных лиц неизвестный продавец попросил использовать Telegram.

Известно, что хакеры продают такие данные египетских пациентов, как имена, национальные ID, диагнозы, сведения о регионах проживания, данные о хирургическом вмешательстве, а также документы, связанные с президентской программой по закрытию листов ожидания на лечение в период с января 2019 г. по январь 2023 г. Запущенная в 2018 году, эта программа направлена на то, чтобы египтяне как можно скорее получали квоты на сложные и критичные операции. В мае 2023 г. минздрав Египта сообщил, что с начала запуска инициативы государство оплатило 1,7 млн операций.

***Пример 8.** Утекли персональные данные сотен тысяч канадских медиков.*

Персональные данные множества медработников были похищены в результате хакерской атаки на Ассоциацию сотрудников системы здравоохранения канадской провинции Британская Колумбия (HEABC). Хакеры украли персональные данные из серверов нескольких участников ассоциации.

К настоящему времени известно, что злоумышленники получили доступ к информационным системам HEABC в период с 9 мая по 10 июня 2023 г., но инцидент не был выявлен до 13 июля. Ассоциация подтвердила, что в июле была выявлена аномальная активность

в ее сети, но отказалась сообщать подробности инцидента.

Министр здравоохранения Британской Колумбии Адриан Дикс (Adrian Dix) признал факт утечки информации, но заявил, что инцидент не затронул работу департаментов министерства, а также то, что ни информация о пациентах, ни данные государственных информационных систем не были затронуты.

Президент HEABC Майкл Макмиллан (Michael McMillan) не смог назвать количество пострадавших медработников, но сказал, что утекли электронные адреса 240 тыс. адресов электронной почты, связанных с паспортными данными, номерами водительских удостоверений, датами рождения, номерами социального страхования. Но весь спектр утекшей информации представители медицинского сообщества пока затрудняются оценить.

По словам Макмиллана, ассоциация сотрудничает с экспертами по кибербезопасности, чтобы устранить последствия инцидента, оценить его масштабы и оповестить всех пострадавших. Глава HEABC заявил, что ассоциация не получала от хакеров требования о выкупе, но отказался сообщить о характере взлома. Позже Майкл Макмиллан лишь уточнил, что инцидент не связан с эксплуатацией уязвимости в ПО MOVEit.

Все канадские медработники, пострадавшие от утечки информации, получат бесплатные услуги кредитного мониторинга.

***Пример 9.** Больница потеряла персональные данные более миллиона пациентов.*

Американская клиника Tampa General Hospital (TGH) сообщила об утечке информации, которая могла затронуть персональные данные 1,2 млн человек. Хакерам удалось извлечь персональные данные в результате майской атаки.

В уведомлении на своем сайте TGH отмечает, что аномальная активность в сети клиники была обнаружена 31 мая. В больнице также пояснили, что попытки хакеров зашифровать данные были сорваны благодаря эффективным системам мониторинга угроз и бдительности специалистов по кибербезопасности, что помогло предотвратить серьезные сбои в лечении пациентов.

Однако, в ходе расследования выяснилось, что хакеры все-таки получили доступ к определенным файлам, в которых содержалась конфиденциальная информация пациентов. Извлечение части конфиденциальной информации произошло в период с 12 по 30 мая. При этом электронная медицинская система клиники не была затронута инцидентом, уверяют в TGH. Больница сообщила о взломе в ФБР, чтобы сотрудники этого ведомства помогли найти киберпреступников, стоящих за атакой.

Представители Tampa General Hospital заявляют, что набор похищенной информации различается от пациента к пациенту, но в целом были скомпрометированы такие данные, как имена, адреса, даты рождения, номера телефонов, номера социального страхования, сведения из программ медицинского страхования, номера медицинских карт, номера счетов пациентов, даты приема, а также ограниченная информация о лечении.

Эта утечка информации подвергает пациентов риску кражи персональных данных и риску финансового мошенничества, а также подрывает доверие людей к обеспечению безопасности данных со стороны клиники, отмечает Ани Чаудхури (Ani Chaudhuri), генеральный директор компании Dasera.

В связи со случившимся инцидентом пациенты TGH должны защитить себя. Людям очень важно внимательно следить за своими финансовыми счетами, регулярно отслеживать кредитные отчеты и не терять бдительность перед лицом любых подозрительных действий.

В начале июля Европейское агентство по сетевой и информационной безопасности (ENISA) обнародовало отчет, согласно которому программы-вымогатели составляют более половины всех киберугроз, направленных на сферу здравоохранения в ЕС.

5.2. Производственная тайна

Для злоумышленников представляет интерес следующая информация:

- формулы, способ производства и др.;
- химический состав фармакологической продукции;
- данные об исследованиях и испытаниях.

«Спутник V» – российская, первая в мире зарегистрированная вакцина на основе вектора аденовируса человека. Векторы являются носителями, которые могут доставить генетический материал в клетку. При этом генетический код аденовируса, который вызывает инфекцию, удаляется и на его место вставляется материал с кодом белка от другого вируса, в данном случае от шипа коронавируса.

Векторный вирус можно выращивать только в живых клеточных культурах, что требует при масштабировании высокотехнологичного производства. И с этим могут быть сложности в некоторых странах. Вакцина должна храниться при минус 18 градусах, что затрудняет логистику.

В середине марта 2023 года хакеры выложили в интернет «засекреченные» документы о вакцине. В открытый доступ в интернете попали сотни документов, связанных с разработкой и клиническими испытаниями вакцины «Спутник V» для профилактики коронавирусной инфекции COVID-19.

О раскрытии конфиденциальной информации заявила кибергруппировка, известная как KelvinSecurity. Утверждается, что данные получены в результате «проверки почтовых ящиков компании-разработчика» – Национального исследовательского центра эпидемиологии и микробиологии имени Н.Ф. Гамалеи. Речь идёт о взломе ИТ-систем этой организации.

Кибергруппа KelvinSecurity заявила, что ее целью было продемонстрировать неэффективность вакцины и что это всего лишь российская государственная пропаганда [24].

В выложенных документах в числе прочего содержались сведения о смерти участников клинических испытаний вакцины «Спутник V» (регистрационное наименование «Гам-КОВИД-Вак»), включая имена погибших. Летальные исходы якобы зафиксированы в таких странах, как Гана и Египет. Хакеры заявляют, что некоторые документы были засекречены: в них приводится информация об этапах разработки вакцины, финансировании и качестве. Некоторые файлы включают технические подробности, тогда как другие касаются переговоров с зарубежными компаниями, в том числе из Швейцарии. В общей сложности в интернет выложены более 300 файлов общим объёмом приблизительно 522 Мбайт. Другие документы содержат счета-фактуры и относятся к стоимости научных работ, одна из которых оценивается в семь миллионов рублей, или около 93.000 долларов. Также имеется информация о различных лабораториях, производивших вакцину, и уровне их производительности.

5.3. Коммерческая тайна

Спросом у злоумышленников пользуется следующая информация:

- результаты тендерной деятельности;
- данные договоров с партнерами и подрядчиками, условия работы;
- цены на поставляемые услуги;
- планы развития торговых сетей.

Пример 9. *В мае 2023 года стало известно об утечке данных клиентов сети клинико-диагностических лабораторий «Ситилаб». Клинико-диагностические лаборатории СИТИЛАБ – это федеральная сеть медицинских центров по всей стране и диагностические лабораторные комплексы в 7 крупнейших городах России: Москва, Санкт-Петербург, Новосибирск, Самара, Екатеринбург, Казань, Красноярск. Информацию предоставила исследовательская компания Data Leakage & Breach Intelligence (DLBI), специализирующаяся на утечках информации [25] . По словам экспертов, в слитый дамп вошли:*

- *логин;*
- *ФИО;*
- *адреса электронной почты (483 тыс. уникальных адресов);*
- *телефон (435 тыс. уникальных номеров);*
- *хешированный пароль;*

- *пол (не у всех);*
- *дата рождения (не у всех);*
- *дата регистрации (с 01.01.2007 по 18.05.2023).*

В DLBI выборочно проверили случайные адреса электронной почты из этой утечки через форму восстановления пароля на сайте my.citilab.ru/client/ и выяснили, что они все действительные. В открытом доступе находился архив объемом 1,7 Тбайт. В архиве, помимо пользовательских данных, содержатся PDF-документы с отсканированными анализами и исследованиями, а также договорами и чеками.

Пример 10. *В марте 2023 года стало известно, что хакеры-вымогатели из группировки Alphv взломали сеть больниц Lehigh Valley Health Network и начали публиковать в интернете фото больных раком американцев в надежде получить выкуп.*

Злоумышленники внедрили вредоносный код в систему медицинского портала, в результате чего украли данные электронных медицинских карт пациентов. Украденные персональные данные включали ФИО, адреса, даты рождения, номера банковских карт, даты окончания действия карт, а также конфиденциальную информацию по различным болезням пациентов.

По информации Минздрава США, электронную карту создает врач, когда пациент приходит к нему на прием. В нее попадает информация о заболеваниях пациента, визитах к врачу, назначенных лекарственных препаратах, больничных листах. А затем в карте появляются результаты клинических анализов и другие важные данные о пользователе.

Злоумышленники выложили в интернет клинические снимки, используемые Lehigh Valley Health Network, с описанием на сайте Alphv как «обнаженные фотографии». В действительности же в папке были файлы электронных карт со снимками радиотерапии для борьбы со злокачественными клетками и фотографиями больных раком.

Инцидент произошел с компьютерной системой, используемой для получения клинически значимых изображений пациентов для лечения радиационной онкологии и другой конфиденциальной информации [26]. Мотивацией злоумышленников было получение выкупа за разглашение коммерческой тайны.

Пример 11. *В феврале 2023 года стало известно об утечке данных пользователей интернет-аптеки «Здравсити». Выставленная на продажу информация на теневом форуме содержала более 8,9 млн уникальных номеров телефонов и почти 3,4 млн уникальных адресов электронной почты. Сервис «Здравсити» позволяет делать онлайн-заказы на доставку лекарств, медицинских изделий, средств гигиены, БАДов, косметики и других товаров для здоровья и красоты. Маркетплейс работает 81 регионе России. Утечка информации, по всей видимости, связана со сменой совладельцев интернет-аптеки «Здравсити».*

Кроме того, медицинские учреждения часто фиксировали рискованное поведение (например, кража медицинского оборудования или распространение негативной информации) со стороны сотрудников (64%) и стороннюю занятость персонала (24%) [27]. По сравнению с 2021 годом снизилось число инцидентов, когда уволенные работники пытаются вредить организации. В 2022 году о таких случаях заявило 17% респондентов против 34% в 2021 году.

Пример 11. *Федеральная антимонопольная служба (ФАС) раскрыла картель поставщиков медицинской продукции. Участники сговора поддерживали цены на высоком уровне на торгах. В заключении и реализации антиконкурентного соглашения выявлены компании «Аксонмед», «Дивайс», «Интермед», «Лотос» и «Сатори». Их ценовой сговор действовал в рамках электронных аукционов на поставку инструментов, аппаратуры, расходных материалов и прочих медицинских изделий для нужд государственных*

и муниципальных учреждений здравоохранения.

Торги проходили в восьми российских регионах и завершались с минимальным снижением начальной цены контрактов.

Сумма ущерба в результате сговора компаний оценивается от 0,5 млн до 16 млн рублей каждая. А таких аукционов было проведено 19.

***Пример 12.** Картельный сговор при торгах на поставку медицинских изделий и лекарств был выявлен в Хакасии. В сговоре были задействованы 13 компаний, которые, по данным ФАС, заключили устное соглашение для поддержания цен на торгах, в результате чего аукционы завершались с минимальным снижением цены контракта.*

Подобные преступления в России совершаются достаточно часто. Ежегодно ФАС регистрирует на госзакупках лекарств и медицинских изделий около 19% от всех дел о картелях. Больше нарушений приходится только на строительный рынок.

ФАС разработала и внесла в Правительство РФ законопроект об ужесточении ответственности за участие в картельном сговоре [28].

6. Репутационный ущерб от утечки информации из медицинских учреждений

Репута́ция (англ. reputation), реноме́ (фр. renommée) – закрепившееся определённое мнение (более научно-социальная оценка) группы субъектов о человеке, группе людей или организации на основе определённого критерия. Упрощенно, репутация – это мнение кого-то о чем-то или о ком-то. Репутация есть у людей, организаций, событий, процессов…

Репутация – это оценочное суждение, а значит она существует у кого-то в голове. Ведь это чьё-то оценочное суждение, это чьё-то мнение. Предположим, что необходимо обратиться к стоматологу. Так вот у стоматологов государственных поликлиник есть своя репутация, при условии конечно, что хоть кто-то пользовался их услугами. И на основе этой репутации потенциальный клиент делает выбор между государственной стоматологической поликлиникой и конкурирующей частной.

Если в системе обязательного медицинского страхования можно получить квалифицированную медицинскую помощь в государственных медицинских учреждениях, то что нужно сделать чтобы потенциальный пациент сделал такой выбор, а не обратился в платное медицинское учреждение? Правильно – сформировать соответствующий образ в его голове. Образ, который будет предпочтительнее аналогов, образ, который будет манить и всячески стимулировать желание получить в своё распоряжение вожделенные медицинские услуги на платной основе. И надо признать, что не очень дешевые. Но на здоровье, как известно, не экономят.

Репутация не существует сама по себе. Даже при наличии Объекта, у него нет репутации пока нет аудитории, имеющей мнение по поводу этого Объекта (целевая аудитория). Объект конечно же в самом широком смысле: человек, организация, бренд, изделие, событие, территория… Поэтому говоря о репутации, подразумевается наличие того, чья это репутация и того или тех, из мнений кого складывается эта репутация. Мало того, у аудитории, чаще всего, складывается мнение не о самом объекте, а о некой его модели – образе, сформированном каналами связи, СМИ, социальными сетями, интернетом… А сам процесс «создания» такой модели уже есть формирование репутации.

Потенциальные пациенты еще не обращались за медицинской помощью в платные медицинские учреждения, а мнение по какой-то причине уже сформировали. Ведь репутация – это мнение конкретного человека, а это мнение можно сформировать на основе чужих оценочных суждений или на основе сравнения с аналогичными организациями (рис. 9).

По результатам опроса общественного мнения ситуацию в российском здравоохранении назвали удовлетворительной 45%. Это говорит о высоком уровне доверия к медицинским центрам и клиникам. При этом только 12% опрошенных считают,

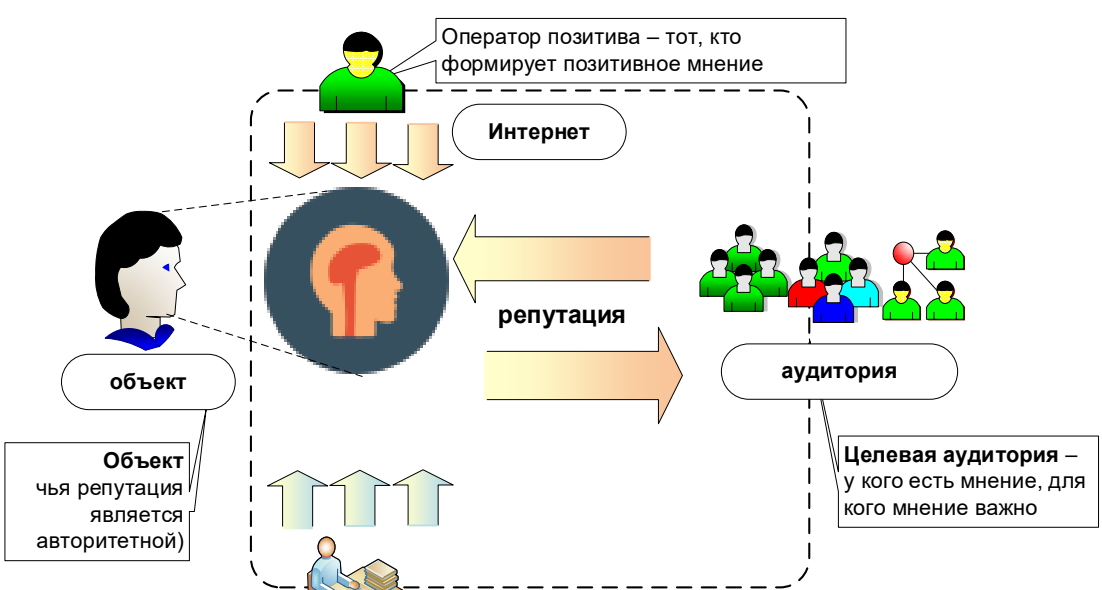


Рисунок 9 – Формирование репутации организаций и специалистов

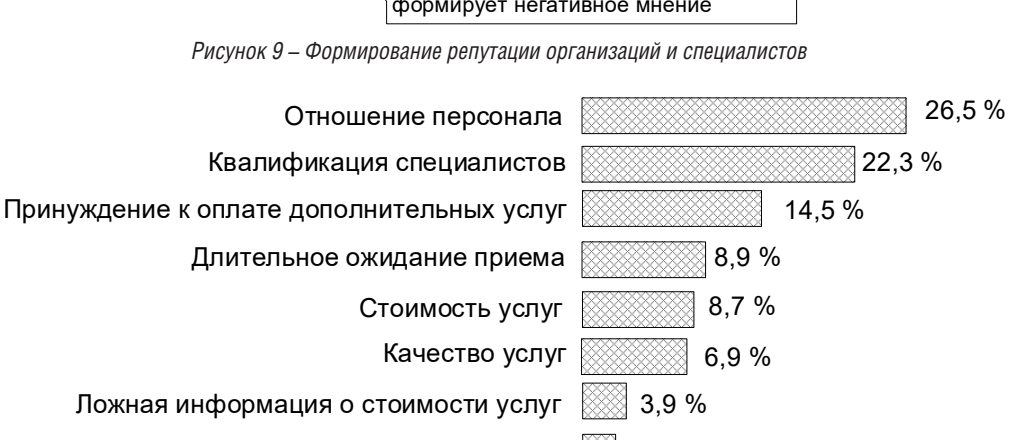


Рисунок 10 – Топ 10 жалоб пациентов

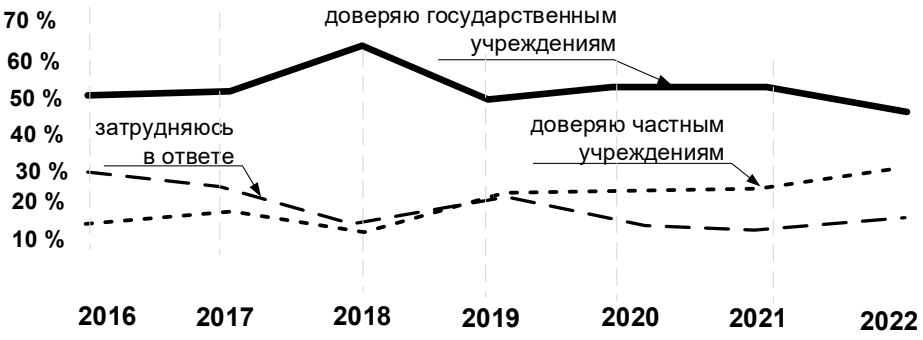
что в системе здравоохранения все в порядке, то есть уровень критики достаточно высокий.

Большинство граждан РФ доверяют врачам и считают эту профессию престижной. Им доверяют больше, чем журналистам, священнослужителям, политикам, блогерам. Следовательно, в обществе профессия врача является уважаемой, а ее представители – теми, к кому общественность прислушивается.

Граждане выделяют конкретные критические стороны медицинского обеспечения, из-за которых посещение медицинских учреждений доставляет дискомфорт. На что пациенты жалуются чаще всего – представлено на рис. 10.

В чем особенности образа частной медицины? Согласно многим исследованиям, можно установить рост доверия к частным медицинским центрам. Доверие зависит от деятельности в сфере информационных услуг: утечка информации из государственных медицинских учреждений; угрозы и ущерб от действия хакеров; некоторых сотрудников учреждений, действующих в корыстных целях; атаки на репутацию этих учреждений и т.д.

На графике ниже (рис. 11) отражены имеющиеся данные с 2016 по 2022 годы. Они показывают, что доверие к государственным медицинским учреждениям, к сожалению, снижается.



	2016	2017	2018	2019	2020	2021	2022
доверяю государственным учреждениям	52 %	55 %	65 %	51 %	55 %	54 %	48 %
доверяю частным учреждениям	18 %	19 %	17 %	24 %	26 %	28 %	32 %
затрудняюсь в ответе	30 %	26 %	18 %	26 %	19 %	18 %	20 %

Рисунок 11 – Уровень доверия к медицинским учреждениям

Снижение уровня доверия к государственной медицине коррелирует не столько с возрастом пациентов, сколько с географическим положением медучреждения. Важен тот факт, что качество обслуживания по ОМС, к сожалению, отличается в разных регионах.

Некоторые государственные поликлиники и больницы внедряют в качестве процесса управления репутацией ответы на отзывы на сторонних площадках. Но это слабая тенденция в отличие от личных брендов врачей. Специалисты часто работают и в государственных, и в частных учреждениях, развитие их личного бренда влияет на репутацию и тех, и других организаций.

Выбор медицинского учреждения пациентами осуществляется на основе популярных источников информации, на основании выбора специалистов. Процент доверия людей указан согласно данным исследования Delloite «Медиапотребление в России 2021» [29]. Рассмотрим их подробнее ниже в порядке убывания процента доверия (рис. 12).

1. Рекомендации родных, близких, знакомых, коллег – тех, с кем клиент напрямую взаимодействует и чей релевантный опыт он готов принять. Это ключевой параметр, на который наиболее сложно повлиять со стороны клиники.

2. Интернет: социальные сети и медиа, профильные порталы, отзывы в картографических сервисах и на сайтах. Сюда входят все источники, где пользователь может ознакомиться с релевантным опытом незнакомых ему клиентов – людей, которые формируют информационное поле.

Среди откликов в интернете стоит выделить отзывы реальных пациентов о реальных врачах. Чем более подробно описан опыт, тем более полезна информация с точки зрения потенци-

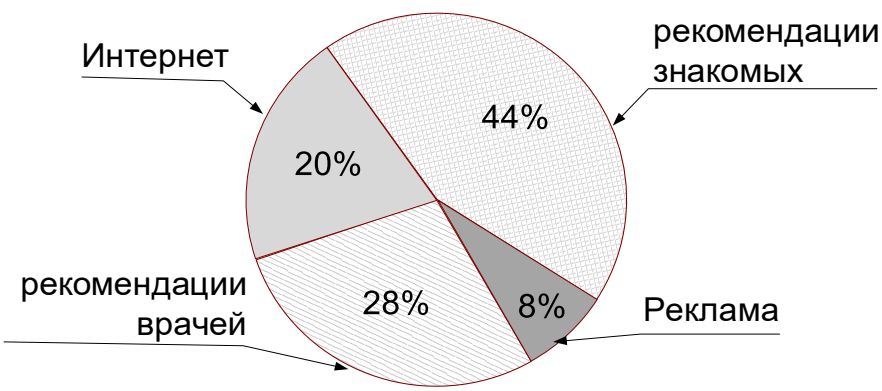


Рисунок 12 – Источник информации пациентов при выборе клиники

ального пациента, тем ощутимее она влияет на решение.

3. Рекомендации врачей, потому что, как было сказано выше, это та прослойка общества, которой доверяют больше прочих.

4. Прямая реклама: интерес к этому источнику снижается и замещается на доверие к конкретным персоналиям. Это могут быть знакомые, лидеры общественного мнения, незнакомые участники социальных сетей.

Важны следующие особенности взаимодействия с клиникой:

Персонализируйте предложения клиники с учетом возможностей цифровизации. Например, дайте пациентам возможность видеть результаты анализов онлайн, иметь возможность записаться или поменять время записи на прием через приложение 24 часа в сутки, получать обратную связь в приложении. Причем все это должно быть защищено от утечек.

Понятие «репутация компании» часто подменяется понятием «имидж». Это образ в сознании человека, который влияет на его эмоции и поведение. Именно поэтому любому медицинскому учреждению важно создавать положительный имидж. В его формировании важны как фирменный стиль учреждения (логотип и слоган, дизайн сайта, корпоративные визитки, бланки и конверты, фирменная одежда, рекламная полиграфия и т.д.), так и отзывы о его работе в Интернете и других источниках.

Деловая репутация является нематериальным благом (ст. 150 ГК РФ). Ее правовую защиту гарантирует ст. 152 ГК РФ. Заявитель вправе требовать по суду опровержения порочащих деловую репутацию сведений, если лицо, распространившее их, не докажет, что они соответствуют действительности.

Особенности защиты деловой репутации в суде раскрываются в Постановлении Пленума Верховного Суда РФ от 24 февраля 2005 г. № 3 «О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц» [30].

В этом постановлении указано, что обстоятельствами, имеющими значение для дел о защите деловой репутации, являются:

1) факт распространения ответчиком сведений об истце;

2) порочащий характер этих сведений;

3) несоответствие их действительности.

При отсутствии хотя бы одного из указанных обстоятельств иск не может быть удовлетворен судом.

Обязанность доказывать соответствие действительности распространенных сведений лежит на ответчике (п. 1 ст. 152 ГК РФ). Истец обязан доказать факт распространения сведений лицом, к которому предъявлен иск, и их порочащий характер. Но чтобы доказывать эти обстоятельства, нужно понимать, что такое порочащие и не соответствующие действительности сведения и что подразумевается под их распространением.

Под распространением сведений, порочащих деловую репутацию, следует понимать опубликование их в печати, трансляцию по радио и телевидению, демонстрацию в кинохроникальных программах и других СМИ, распространение в Интернете, изложение в служебных характеристиках, публичных выступлениях, заявлениях, адресованных должностным лицам, или сообщение их хотя бы одному человеку. При этом сообщение таких сведений человеку, которого они касаются, не может признаваться их распространением при одном условии: если тот, кто сообщил сведения, принял достаточные меры конфиденциальности, чтобы они не стали известны кому-то еще.

Не соответствующими действительности сведениями являются утверждения о фактах или событиях, которые не имели места в реальности, к которым относятся оспариваемые сведения. При этом не могут рассматриваться как не соответствующие действительности сведения, содержащиеся в официальных документах.

Порочащими являются сведения, содержащие утверждения о нарушении гражданином или юрлицом законодательства, совершении нечестного поступка, неправильном или неэтич-

ном поведении, недобросовестности при осуществлении производственно-хозяйственной и предпринимательской деятельности, нарушении деловой этики или обычаев делового оборота, которые умаляют деловую репутацию.

Надлежащими ответчиками по искам о защите деловой репутации являются авторы не соответствующих действительности и умаляющих репутацию сведений, а также их распространители. Если оспариваемые сведения были распространены в СМИ, то надлежащими ответчиками будут автор и редакция, а также лицо, являющееся источником сведений, если оно было указано. В случае если сведения были распространены без обозначения имени автора, надлежащим ответчиком по делу считается редакция СМИ. Если редакция не является юрлицом, к участию в деле в качестве ответчика может быть привлечен учредитель СМИ.

Судебная защита деловой репутации не исключается даже тогда, когда невозможно установить лицо, распространившее порочащие сведения (например, при направлении анонимных писем в адрес граждан и организаций или распространении сведений в Интернете лицом, которое невозможно идентифицировать). В этом случае суд вправе по заявлению заинтересованного лица признать распространенные в отношении него сведения не соответствующими действительности (п. 8 ст. 152 ГК РФ).

7. Безопасность в сфере фармацевтики

7.1. Производство и распространение фальсифицированной продукции

Одной из угроз в сфере фармацевтики является производство и распространение фальсифицированной продукции. Это и появление на рынке поддельной продукции и возможная информационная репутационная дискредитация брендов производителей, которые завоевали имидж надежных и выпускающих качественную продукцию.

Выбор потребителями более дешевых лекарств ставит под угрозу потери премиальности, что в итоге приводит к снижению интереса со стороны покупателей к надежным производителям. Низкокачественные подделки лекарственных препаратов могут нанести вред здоровью потребителя и негативно отразиться на репутации бренда.

Массовая миграция продавцов всех видов продукции в онлайн-сектор поднимает на новый уровень проблему обеспечения информационной безопасности брендов. Угрозы проведения кибератак и учащения случаев цифрового мошенничества являются ключевыми проблемами любого перехода на электронную коммерцию (e-commerce).

Существуют результаты анализа, проведенного некоторыми корпорациями, например Group-IB Brand Protection [31], каналов продвижения и объемов фальсифицированной фармакологической продукции, распространяемой через интернет. На основе исследования сотен тысяч ресурсов по:

- доменным именам;
- мобильным приложениям;
- страницам в социальных сетях,

ресурсов, направленных на продажу продукции под именами известных «брендов-гиганты» крупнейших производителей фармацевтических препаратов в категориях:

- жаропонижающие и болеутоляющие средства;
- препараты для лечения никотиновой зависимости;
- для потенции;
- для лечения сахарного диабета.

Специалисты Group-IB Brand Protection установили взаимосвязи между регистрационными и контактными данными, IP-адресами и доменными именами, а также вычислили аффилированность рассматриваемых ресурсов.

Целевой аудиторией исследования были бренды всего международного рынка.

Анализу подверглись:

- методы распространения и привлечения трафика;
- наиболее часто атакуемые категории препаратов;

– площадки для сбыта фальсифицированной продукции.

Были рассмотрены и проанализированы упоминания и объявления о продаже препаратов, размещенных на следующих ресурсах в русском и англоязычном интернет-сегменте:

– поисковые системы Yandex и Google;
– социальные сети;
– интернет-магазины.

Установлено, что мошенники активно используют различные ресурсы, с помощью которых распространяют поддельные препараты или привлекают дешевый трафик.

10 % мирового рынка – фальсифицированные лекарственные препараты.

9 из 10 российских интернет-аптек распространяют подделки.

Пока производители конкурируют между собой, разрабатывая новые препараты, и отвечают за качество готовой продукции, мошенники просто паразитируют и зарабатывают на чужом имени и популярности (рис. 13).

Новые мошеннические схемы появляются и исчезают каждый день. В большинстве своем они объединены в сети, имеют идентичный бренд, дизайн и конкретные признаки.

В результате можно выделить четыре категории ресурсов, которые представляют наибольшую опасность для брендов.

1. Посвященные конкретному бренду.

Полностью или частично скопированные с официальных ресурсов сайты с измененными ценами на товар и неверными контактными данными.

2. Посвященные категории товара.

Ресурсы с различными товарами одного типа. Ассортимент таких сайтов – это, как правило, самые популярные модели внутри одного товарного сегмента.

3. Направленные на кражу персональных данных.

Схожесть мошеннических ресурсов с официальными сайтами вводит неподготовленного пользователя в заблуждение.

4. Осуществляющие мультибрендовую продажу товаров различных категорий.

Таким образом мошеннический ресурс может маскироваться под обычную интернет-аптеку, создавать иллюзию массовых продаж и тем самым получать доверие потребителя, который даже не задумается, что может стать жертвой мошенников.

Мошеннические ресурсы опасны не только распространением контрафакта, но они представляют угрозу репутации и значительно влияют на размер выручки от продаж, которую недополучают бренды.

7.2. Некоторые виды угроз в фармакологии

Доменные имена

Анализ позволяет установить множество схожих с официальными доменных имен, которые потенциально могут использоваться в мошеннических целях.

При этом не все ресурсы содержат противо-

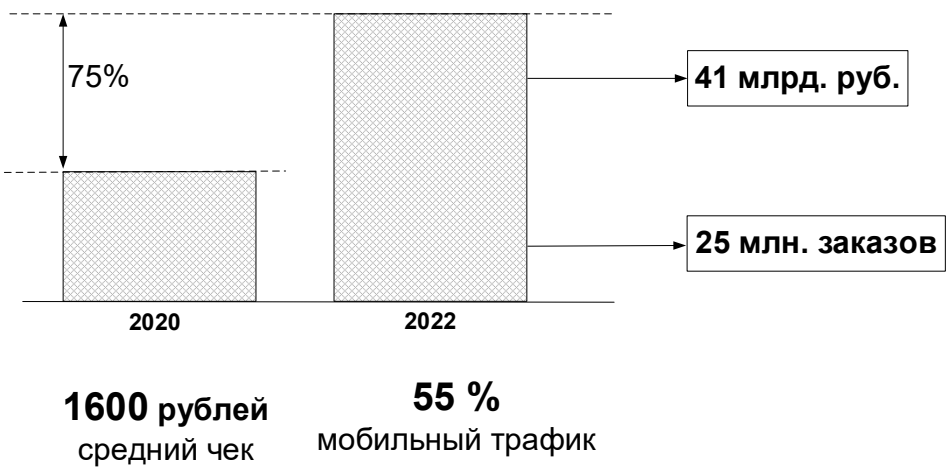


Рисунок 13 – Характеристики заказов в интернет-аптеках

правный контент. Так, например, все 60 доменов, обнаруженных по одной из фармацевтических компаний, оказались «чистыми», то есть на них пока не было размещено никакой информации. Впрочем, это не исключает возможного появления на них противоправного контента в любой момент.

Также в ходе исследования можно выявить ресурсы, обещавшие посетителю вознаграждение при переходе по сомнительной ссылке, либо предлагавшие скачать программное обеспечение неизвестного происхождения.

Как злоумышленники используют схожие доменные имена?

Рекламируют собственные сервисы.

Мошенники мимикрируют под известные бренды для раскрутки собственных сайтов и привлечения трафика.

Представляются партнерами известного бренда.

Мошенники используют чужой логотип или название компании в знак подтверждения делового партнерства, которое по факту является ложным. Некачественно или вообще не оказанные мошенниками услуги потребители начинают ассоциировать с известной компанией, что может повлечь за собой претензии, обращения в компанию, а также нанести репутационный ущерб.

Указывают недостоверную информацию.

Ложные сведения могут вводить в заблуждение потенциальных клиентов или сотрудников компании.

Теневые форумы

На теневых форумах также производится продажа продукции под исследуемыми брендами и рекламируются существующие мошеннические ресурсы (в основном, в комментариях).

Всего за один месяц (сентябрь 2023 г.) было обнаружено более 1.000 сообщений о продаже препаратов для потенции. Часть продавцов распространяет товар сразу на нескольких форумах.

Встречаются предложения оптовой продажи, в названии которых упоминается сразу несколько брендов.

Социальные сети

Результаты анализа различных групп и аккаунтов в социальных сетях, использующих средства индивидуализации фармацевтических компаний и популярных препаратов, в том числе, в целях продажи представлены на рис. 14.

Обнаружено более 380 групп аккаунтов, использующих исключительно наименование препаратов или средства индивидуализации фармкомпаний.

65.000 человек составляет аудитория этих групп и аккаунтов.

Лишь 40% обнаруженных групп и аккаунтов приходится на международные социальные сети, остальные 60% – на отечественные. Часть групп занимается распространением препаратов централизованно.

Большинство групп и аккаунтов находится Вконтакте (98%) и занимаются распространением нелегальных препаратов для повышения потенции.

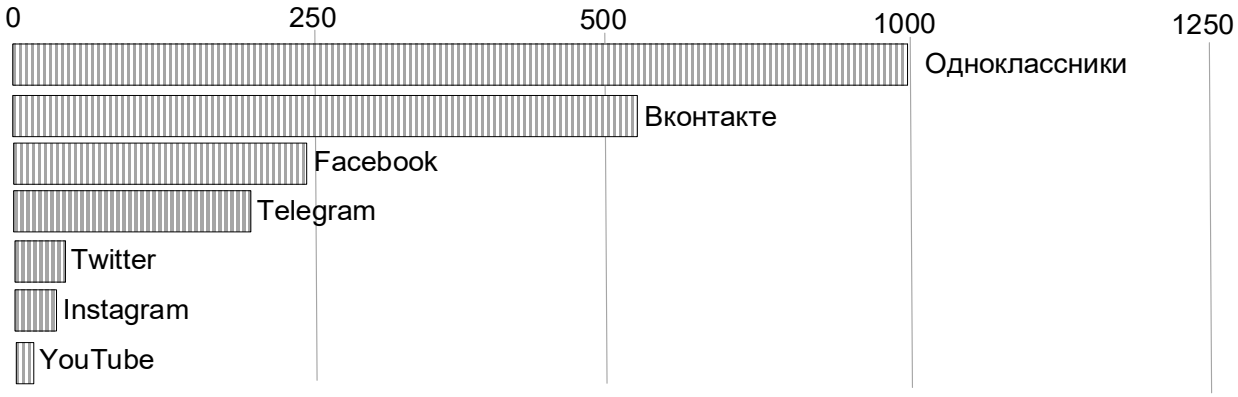


Рисунок 14 – Распределение количества упоминаний брендов в разных социальных сетях

Важную роль в незаконном распространении фармацевтических препаратов играет реклама и продвижение онлайн-магазинов и Telegram-каналов. В ходе исследования обнаружено 23 связанных между собой аккаунта Вконтакте, которые ведут на Telegram-канал, специализирующийся на продаже препаратов для потенции.

Интернет-магазины

Анализ объявлений о продаже показывает, что большая часть фальсифицированных препаратов реализуется на общих агрегированных площадках. Мошенники активно используют мультибрендовые сайты из-за их доступности. И популярность препаратов идёт им только на руку.

Более 20.000 предложений обнаружено в интернет-магазинах под брендом препарата для потенции.

80-100.000 объявлений может приходиться на один бренд.

Около 70% объявлений приходится на препараты для потенции, 30% – на противовирусные.

Если рассматривать продажу препаратов для лечения диабета, то большинство из них в рунете не продается. Все предложения продавцов на русскоязычных площадках – это запросы о наличии препарата в той или иной аптеке.

Мобильные приложения

Существует большое количество разнообразных мобильных приложений, которые могут как целенаправленно использовать наименование и товарные знаки бренда, так и не концентрироваться именно на нём, а осуществлять продажу по типу мультибрендовой интернет-аптеки.

Часть из них легитимна, а часть зарегистрирована на неопределенных людей, которые занимаются продажей поддельных товаров.

Опасность неофициальных мобильных приложений состоит в том, что существует:

1. Риск заразить пользовательское устройство вредоносным программным обеспечением.

Заражённое устройство может открывать доступ к управлению устройством, похищать или передавать злоумышленнику персональные данные пользователя.

2. Введение потребителя в заблуждение.

Более 400 мобильных приложений было найдено по 7 препаратам и 5 брендам фармацевтических кампаний.

Подобные приложения могут подолгу не обновляться или содержать недостоверную и неактуальную информацию о препаратах, тем самым представляя опасность для здоровья пользователя.

Самые часто подделываемые препараты

Мошенники предпочитают подделывать наиболее популярные на текущий момент бренды лекарственных препаратов, которые определяют при помощи легитимных инструментов анализа рынка.

В результате анализа можно выделить три категории препаратов, чьи бренды чаще всего использовались мошенниками для копирования (рис. 15):

– чаще всего подделывают препараты для потенции. Их доля в e-commerce составляет 57,5% от всех предложений;

– на втором месте – анальгетики и жаропонижающие средства с долей 40%;

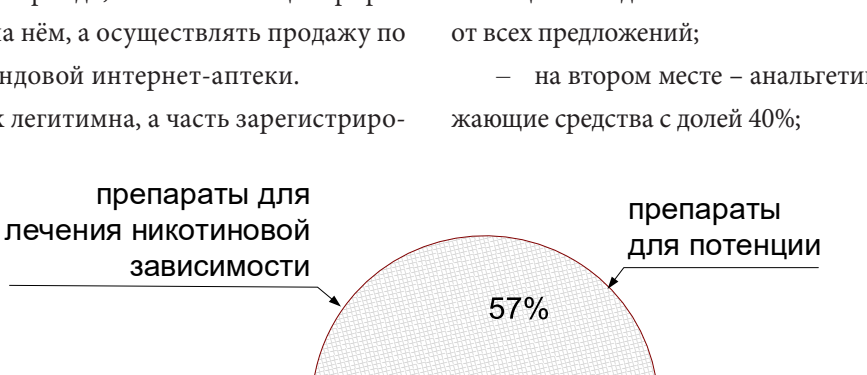


Рисунок 15 – Категории препаратов, становящихся мишенью интернет-мошенников

– на третьем месте – препараты для лечения никотиновой зависимости с 2%;

– минимальная доля подделок приходится на препараты для лечения диабета – 1%.

Поисковые запросы

Предваряющий покупку поиск является идеальным моментом для мошенников – именно на этом этапе проще всего привлечь потенциального покупателя выгодным предложением. Затраты мошенников в таком случае минимальны, ведь какой бы метод продвижения своих ресурсов они ни выбрали, он будет приносить результат и прибыль.

Анализ поисковых запросов позволяет выявить десятки сайтов по продаже, включая доски объявлений и социальные сети. Помимо выдачи по запросу, поисковые системы также предлагают аудитории контекстную рекламу мошеннических ресурсов, которая вводит неподготовленного потребителя в заблуждение.

Реклама

Для привлечения аудитории на свои ресурсы мошенники используют различные каналы:

– контекстную рекламу;

– таргетированные СМС-рассылки;

– рассылки в мессенджерах.

Подобная деятельность существенно влияет на отношение целевой аудитории к брендам и ведёт к репутационным потерям. Отдельно стоит учитывать рекламу мошеннических ресурсов, которые распространяют объявления о продаже контрафактных препаратов на форумах и социальных сетях.

7.3. Потенциальный ущерб

Анализ показывает, что только 12% интернет-ресурсов занимаются перепродажей оригинальных препаратов. Следовательно, остальные 88% – предлагают контрафактные лекарственные средства, представляющие опасность для здоровья покупателей.

Потенциальный ущерб фармацевтических компаний от продажи контрафакта представлен в таблице 1.

Конверсия в интернет-аптеках (соотношение числа заказов в месяц к количеству посетителей) равна 8%.

Потенциально недополученная прибыль *= (средний чек)× (конверсия)× (количество ресурсов, продающих монобренд)× (среднее количество посетителей) + (средний чек х конверсия)× (количество мультибрендовых ресурсов)× (среднее количество посетителей)× (среднее количество пользователей, пришедших за данным препаратом)× (процент фальсифицированных препаратов)*

Оценка объема торговли поддельной продукцией одного из топ-5 брендов за год массовой продажи (препарат для лечения потенции) достигает более 18 миллиардов рублей. Такие крупные обороты достигаются мошенниками с минимальными затратами на распространение фальсификата через простые в использовании интернет-каналы.

Таким образом, по самым минимальным подсчётам оборот онлайн-рынка розничных и оптовых продаж семи контрафактных фармацевтических препаратов, подвергнутые исследованию, составляет 2,6 млрд руб. в месяц или 31,5 млрд руб. в год.

Таким образом, можно кратко сформулировать рекомендации для фармацевтических компаний.

1) Провести первичный мониторинг информационного поля.

Основная цель – оценить масштаб проблемы (количество нарушений, неправомерно исполь-

Таблица 1 – Показатели продаж на фармрынке

Показатели	Группа фармпрепаратов	
	Болеутоляющие и жаропонижающие	Препараты для потенции
Средний чек	330	1150
Количество интернет-магазинов	50000	20000
Оборот, мес.	52 млн. руб.	Более 1 млрд. руб.

зующих ваш бренд) и определить приоритетные источники.

Также первичный мониторинг укажет, необходимо ли предпринимать меры по реагированию. Даже, если на данный момент нарушений нет, это не значит, что они не появятся в будущем: часть нарушений носит временный характер, часть возможно выявить только после глубокого анализа информации.

2) Запустить релевантную систему мониторинга.

Чтобы знать ситуацию в точках сбыта фальсифицированной продукции, необходим систематизированный мониторинг интернет-пространства. Его цель – определить фронт работ для устранения нарушений.

Важно, чтобы система мониторинга учитывала интересы потребителей и параллельно анализировала ранее полученные результаты. Для этого нужно применять соответствующие пользовательские запросы и искать в самых популярных среди покупателей источниках.

3) Повышать уровень осведомленности покупателей.

Потребители не всегда разбираются в технологиях производства фирменной продукции и в её отличиях от подделок. Большинство людей легко ввести в заблуждение. Поэтому крайне важно проводить кампании по осведомлению и обучению потенциальных потребителей характеристикам оригинальных препаратов, на которые им стоит обращать особое внимание.

7.4. Фармацевтические преступления

Фармацевтическими преступлениями считаются различные правонарушения, связанные с лекарствами, с сырьём для производства лекарств, с приборами и приспособлениями медицинского назначения и с фармацевтическими средствами. Внедрение подобных препаратов в систему распространения и продажи, в первую очередь, ставит в опасность здравоохранение населения, а также наносит социальный и экономический ущерб.

Поддельные лекарства – речь идёт о лекарствах и медицинских препаратах, изготовленных незарегистрированными производителями, неодобренными Министерством здравоохранения. Эти лекарства и препараты выпускаются под различными торговыми марками. Эти лекарства и препараты выдаются за лекарства, устраняющие различные проблемы со здоровьем (например, поддельное лекарство для лечения импотенции или для похудения); либо лекарства и препараты выдаются за известные, одобренные оригинальные лекарства, на самом деле не являясь ими, так как они не были изготовлены зарегистрированными производителями и не были одобрены Министерством здравоохранения.

Поддельные пищевые добавки – в состав пищевых добавок входит лекарственное активное вещество несмотря на то, что по определению, они вовсе не должны быть в составе пищевых добавок; либо пищевые добавки выдаются за известные на рынке оригинальные пищевые добавки несмотря на то, что они не были изготовлены оригинальным производителем и не были одобрены службой питания.

Поддельные средства медицинского назначения (например, тесты на беременность, приборы для определения уровня сахара в крови, шприцы, презервативы и т.д.), произведённые незарегистрированными производителями и не одобренные Министерством здравоохранения. Средства медицинского назначения выпускаются под различными торговыми марками, либо выдаются за известные на рынке оригинальные средства, несмотря на то, что они не были изготовлены оригинальным производителем.

Лекарства, пищевые добавки и средства медицинского назначения могут быть поддельными и повреждёнными, либо краденными и ввезёнными контрабандным путём. Общее между всеми ними – то, что невозможно установить качество и безопасность этих препаратов, так как они не имеют лицензии на производство в соответствии с Федеральным законом от 12.04.2010 № 61-ФЗ «Об обращении лекарственных средств».

В состав поддельных лекарств/препаратов может входить активное вещество в дозировках,

превышающих дозировку, считающуюся безопасной. Иными словами, человек, принявший подобный препарат, может быть подвергнут чрезмерным количествам активного вещества, и это может быть опасно. В составе препаратов/лекарств также вообще может не быть активного лекарственного вещества, и состояние человека, принявшего их, не улучшится, и его здоровью может быть даже нанесён вред.

Качество поддельных препаратов и лекарств в большинстве случаев низкое, и состав двух порций одного и того же препарата/лекарства может очень сильно отличаться. Таким образом, влияние разных порций может быть разным на отрезке от ядовитости до просто неэффективности.

Поддельные лекарства, препараты, пищевые добавки и средства медицинского назначения не производятся в надлежащих условиях, и поэтому могут содержать инфекции и вредные и опасные для здоровья побочные вещества.

Поддельные лекарства и медицинские препараты принимаются без необходимого медицинского присмотра и наблюдения, и поэтому пациент, принимающий подобные препараты, может подвергать себя опасности. Отсутствие необходимого медицинского присмотра означает, что состояние здоровья человека, принимающего поддельный препарат, не учитывается, и никто не устанавливает, можно ли пациенту принимать этот препарат, учитывая состояние его здоровья, и не нанесёт ли приём этого препарата вред его здоровью.

Настораживающие признаки поддельных лекарств:

– лекарство/препарат не были приобретены в лицензированной аптеке, а по интернету, в продуктовом магазине, ларьке, киоске и т.д.;

– на упаковке препарата есть настораживающие признаки, как, например: надписи на иностранном языке, например: китайском, таиландском, хинди и др.;

– на упаковке есть текст с ошибками/опечатками;

– на упаковке отсутствует информация, которая должна быть обязательно указана, как, например: наименование производителя, срок годности, номер серии;

– внутри упаковки с лекарством/оборудованием медицинского назначения нет вкладыша с информацией для потребителей;

– лекарство не упомянуто в базе данных лекарств, одобренных Министерством здравоохранения.

Откуда поступают поддельные и неисправные медицинские препараты? Поддельные, неисправные, краденые и контрабандные лекарства, пищевые добавки и препараты медицинского назначения продаются в большинстве случаев не в аптеках, медицинских институтах и стоматологических клиниках, а как правило следующими способами:

– через интернет – существенная часть препаратов, которые продаются в интернете, – поддельные. Даже если речь идёт об оригинальном препарате, во время его пересылки по почте, он содержится в ненадлежащих условиях с точки зрения среды и температуры, и это может ухудшить его качество;

– в ларьках и киосках;

– в таких заведениях, как парикмахерские, кабинеты косметолога, салоны красоты (в особенности средства для похудения);

– продаются частными лицами через объявления в газетах, на досках объявлений, в спортзалах.

8. Некоторые рекомендации по повышению информационной безопасности в системе здравоохранения

Объектами защиты в системе здравоохранения являются:

– Персональные данные.
– Производственная тайна:
  - Формулы, способ производства и другое.
  - Химический состав продукции.
  - Данные об исследованиях и испытаниях.
– Коммерческая тайна:
  - Результаты тендерной деятельности
  - Данные договоров с партнерами и подрядчиками, условия работы
  - Цены на поставляемые услуги
  - Планы развития торговых сетей

– Веб-ресурсы учреждения:
  • Доступность веб-портала
– Репутация компании:
  • Репутация компании, ключевых лиц, продуктов компании.

8.1. Правовые меры по предотвращению утечки персональных данных

Проекты об оборотных штрафах за утечки персональных данных.

На конец 2023 г. В Государственной Думе Российской Федерации обсуждают изменение законодательства, направленного на ужесточение ответственности за утечку персональных данных. Внесены тексты проектов ФЗ о внесении изменений в КоАП РФ и УК РФ. Речь идет об оборотных штрафах за утечки персональных данных.

Поручение рассмотреть вопрос об усилении ответственности за незаконный оборот персональных данных было дано Президентом РФ по итогам заседания Совета по развитию гражданского общества и правам человека еще в конце 2022 года. Предлагаемые инициативы.

Административная ответственность за персональные данные

Предложенные изменения в КоАП РФ предусматривают увеличение штрафов за персональные данные по статье 13.11.

В ч. 1 за обработку персональных данных, не совпадающую с целью сбора:

– для гражданских лиц вместо 2-6 тыс. руб. – от 10 до 15 тыс. руб.;

– для должностных лиц вместо 10-20 тыс. руб. – от 50 до 100 тыс. руб.;

– для юридических лиц вместо 60-100 тыс. руб. – от 150 до 300 тыс. руб.

За повторное нарушение штрафы составят:

– для гражданских лиц – от 15 до 30 тыс. руб.;

– для должностных лиц – от 100 до 200 тыс. руб.;

– для юридических лиц – от 300 до 500 тыс. руб.

Статью также предлагают дополнить частями 10-17.

Штрафы за отсутствие уведомления или несвоевременное уведомление об обработке и утечках персональных данных (ч. 10 и ч. 11).

Штрафы за отсутствие уведомления или несвоевременное уведомление оператором о намерении осуществлять обработку персональных данных:

– для гражданских лиц – от 5 до 10 тыс. руб.;

– для должностных лиц – от 30 до 50 тыс. руб.;

– для юридических лиц – от 100 до 300 тыс. руб.

Штрафы за отсутствие уведомления или несвоевременное уведомление оператором об утечке персональных данных:

– для гражданских лиц – от 50 до 100 тыс. руб.;

– для должностных лиц – от 100 до 300 тыс. руб.;

– для юридических лиц – от 400 до 800 тыс. руб.

Штрафы за утечки персональных данных, которые не содержат признаки уголовного преступления (ч. 12 – ч. 17).

От 1 до 10 тысяч человек (или от 10 тыс. до 100 тыс. идентификаторов):

– для гражданских лиц – от 100 до 200 тыс. руб.;

– для должностных лиц – от 800 тыс. руб. до 1 млн руб.;

– для юридических лиц – от 3 млн до 5 млн руб.

От 10 тыс. до 100 тыс. человек (или от 100 тыс. до 1 млн идентификаторов):

– для гражданских лиц – от 200 до 300 тыс. руб.;

– для должностных лиц – от 1 млн руб. до 1,5 млн руб.;

– для юридических лиц – от 5 млн до 10 млн руб.

За утечку персональных данных более 100 тыс. человек (или более 1 млн идентификаторов):

– для гражданских лиц – от 300 до 400 тыс. руб.;

– для должностных лиц – от 1,5 млн руб. до 2 млн руб.;

– для юридических лиц – от 10 млн до 15 млн руб.

За повторную утечку персональных данных:

– для гражданских лиц – от 400 до 600 тыс. руб.;

– для должностных лиц – от 2 млн руб. до 4 млн руб.;

– для юридических лиц – оборотный штраф в размере от 0,1% до 3% совокупной выручки за календарный год, предшествующий году, в котором было выявлено нарушение.

Штрафы за утечку специальной категории персональных данных:

– для гражданских лиц – от 300 до 400 тыс. руб.;

– для должностных лиц – от 1,5 млн руб. до 2 млн руб.;

– для юридических лиц – от 10 млн до 15 млн руб.

За повторную утечку данных специальной категории и случае третьего нарушения по остальным категориям персональных данных:

– для гражданских лиц – от 500 до 800 тыс. руб.;

– для должностных лиц – от 3 млн руб. до 5 млн руб;.

– для юридических лиц – оборотный штраф в размере от 0,1% до 3% совокупной выручки за календарный год, предшествующий году, в котором было выявлено нарушение, но не менее 20 млн руб. и не более 500 млн руб.

Текущая версия законопроекта не рассматривает смягчающих обстоятельств для снижения штрафов для тех организаций, которые обеспечили информационную безопасность персональных данных, а также не рассмотрены условия компенсации за утечки для субъектов персональных данных.

Уголовная ответственность за персональные данные

УК РФ предлагают дополнить статьей 272.1 «Незаконные использование и(или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконного хранения и (или) распространения».

В рамках предлагаемой статьи предусматривается ответственность за незаконные использование, передачу, сбор и хранение компьютерной информации, содержащей персональные данные, полученной путем неправомерного доступа:

– Наказание штрафом до 300 тыс. руб. либо принудительными работами на срок до 4 лет, либо лишением свободы на тот же срок.

– То же деяние в отношении компьютерной информации, содержащей специальные категории персональных данных и биометрические персональные данные, наказывается штрафом до 700 тыс. руб. или в размере зарплаты или иного дохода осужденного до 1 года с лишением права заниматься деятельностью до 2 лет, либо принудительными работами до 5 лет, либо лишением свободы на тот же срок.

– Если деяния совершены из корыстной заинтересованности, повлекли крупный ущерб, совершены группой по сговору или с использованием служебного положения, то они наказываются штрафом до 1 млн руб. или иного дохода за период до 2 лет с лишением права занимать определенные должности, либо принудительными работами на срок до 5 лет со штрафом в размере до 1 млн руб., либо лишение свободы на срок до 6 лет со штрафом до 1 млн руб.

Ужесточается ответственность в случае, если данные нарушения сопряжены с трансграничной передачей данных или повлекли тяжкие последствия (приостановка или нарушение работы оператора персональных данных, нарушение целостности информационной системы, предоставление доступа к персональным данным с целью причинения вреда здоровью, имуществу, ущерба обороне и др.), либо совершены организованной группой.

8.2. Технические средства защиты

Внедряемые технические средства защиты позволяют:

– защитить критически важную информацию и персональные данные клиентов;

– защитить бизнес-процессы, связанные с обработкой конфиденциальных данных;

– выявить нелояльных сотрудников и злоумышленников, сговоры;

– снизить репутационные риски, связанные с возможными утечками информации в социальных сетях;

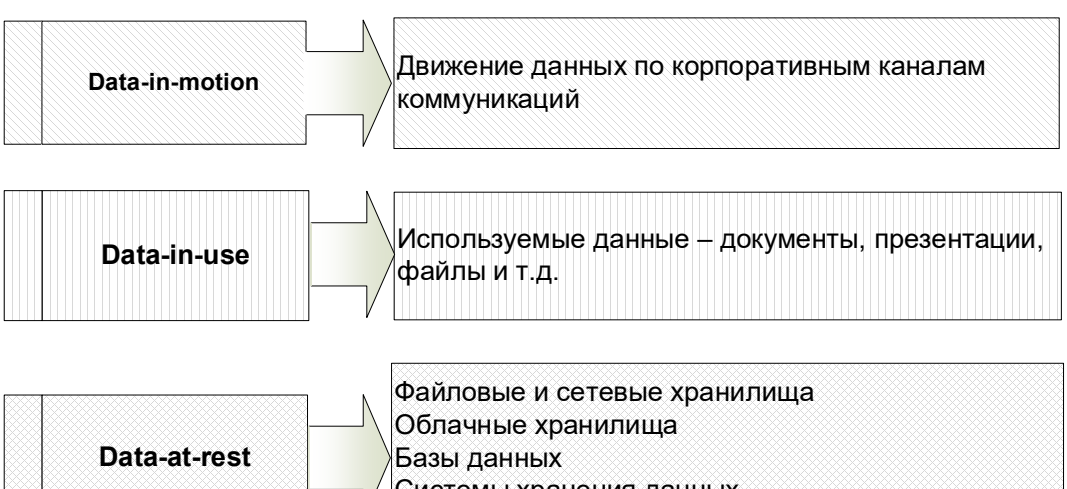


Рисунок 16 – Типы данных

– предотвратить атаки на веб-ресурсы;

– контролировать нецелевое использование служебных информационных систем;

– защитить и консолидировать в едином хранилище всю информацию, собираемую с множества географически распределенных площадок.

Чтобы обеспечить безопасность от утечки информации в медицинских учреждениях, необходимо учитывать, как она обрабатывается и хранится в конкретной организации (рис. 16):

1. Данные, которые постоянно перемещаются и передаются. Например, по электронной почте, в мессенджерах, между автоматизированными информационными системами внутри организации, а также между медицинскими и немедицинскими учреждениями (провайдеры, поставщики, партнеры и т. д.). Данные, находящиеся в движении, можно перехватывать, проверять на предмет содержания конфиденциальных сведений и в случае необходимости блокировать их передачу, например, с помощью Solar Dozor.

2. Используемые данные – данные, с которыми работают сотрудники медицинских учреждений. Они требуют классификации, категоризации и постоянного мониторинга за их перемещением. С этой задачей справляются DLP-системы, которые, как правило, содержат встроенные инструменты классификации, а также решения класса DAM (Database Activity Monitoring) – системы контроля доступа к базам данных [32].

3. Данные в покое – информация, которая хранится в файловых хранилищах (локальных и облачных), базах данных медицинского учреждения. Для защиты данных этого типа используются системы класса DLP, DCAP, DAM, а также отдельные решения класса eDiscovery.

Заключение

Зрелость функции информационной безопасности в медицинских учреждениях еще находится на низком уровне, и большинство сценариев утечки конфиденциальных данных можно предотвратить, используя системы защиты конфиденциальных данных от утечек (DLP-системы). Например, заблокировать скачивание клиентской базы частной медицинской клиники на съемный носитель (флешку).

В современных условиях, когда цифровизация медицинских учреждений идет быстрыми темпами и данные переводятся в электронный вид, очень важно осуществлять непрерывный мониторинг этих данных, защищать места их хранения, а также контролировать к ним доступ со стороны сотрудников медицинских учреждений и третьих лиц.

Список литературы

1. Стратегия национальной безопасности Российской Федерации. Указ Президента Российской Федерации от 02.07.2021 г. № 400. [Электронный ресурс]. – Режим доступа: http://

www.kremlin.ru/acts/bank/47046

2. Программа «Цифровая экономика Российской Федерации» (утверждена Постановлением правительства РФ от 28.07.2017 г. № 1632-р).

3. Федеральный закон № 242-ФЗ от 29 июля 2017 года «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационных технологий в сфере охраны здоровья».

4. *Варзин С.А., Матвеев В.В.* Прикладное применение искусственного интеллекта в обеспечение социальной и экономической безопасности // Теоретические и прикладные аспекты экономической безопасности в условиях цифровизации: Сборник статей / Под редакцией Р.В. Дронова, Е.Е. Шарафановой. – СПб: Санкт-Петербургский государственный экономический университет, 2020. – С. 22-49. – EDN SSIYHV.

5. *Матвеев А.В., Матвеев В.В.* Системно-кибернетический подход к определению понятия «безопасность» // Национальная безопасность и стратегическое планирование. – 2015. – № 1(9). – С. 18-25. – EDN THRQRD.

6. Мировой кризис 30: эволюция ренты и Домината. Блог А. Оноприенко [Электронный ресурс]. – Режим доступа: https://onoprienko.ru/mirovoj-krizis-30-evolyucziya-renty-i-domi/

7. Глобальный ВВП мира: 1980-2023 [Электронный ресурс]. – Режим доступа: http://global-finances.ru/vvp-mira-po-godam/?ysclid=lqj4ca6ftp656586032

8. Декларация лидеров G20: цифровая экономика, цифровое равенство, безопасность ИКТ [Электронный ресурс]. – Режим доступа: https://d-russia.ru/deklaratsiya-liderov-g20-tsifrovaya-ekonomika-tsifrovoe-ravenstvo-bezopasnost-ikt.html?ysclid=lqj4mdjqrs268298667

9. О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы. Указ Президента Российской Федерации от 09.05.2017 г. № 203. [Электронный ресурс]. – Режим доступа: http://www.kremlin.ru/acts/bank/41919

10. *Кошовец О.Б., Ганичев Н.А.* Глобальная цифровая трансформация и ее цели: декларации, реальность и новый механизм роста // Экономическая наука современной России. – 2018. – № 4(83). – С. 126-143. – EDN YUCCHZ.

11. Кибербезопасность в здравоохранении: атаки и ущерб растут [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/analytics/daydzhesty-i-obzory/kiberbezopasnost-v-zdravookhranenii-ataki-i-uscherb-rastut?ysclid=lq9edna8h2368744601

12. Оценка ущерба вследствие утечек информации [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/analytics/analitika/otsenka-uscherba-vsledstvie-utechek-informatsii

13. В Сеть утекли персональные данные миллионов пациентов [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/analytics/utechki-informatsii/v-set-utekli-personalnye-dannye-millionov-patsientov

14. *Мызрова К.А., Туганова Э.А.* Цифровизация здравоохранения как перспективное направление развития // Вопросы инновационной экономики. – 2018. – Т. 8, № 3. – С. 479-486. – DOI 10.18334/vinec.8.3.39355. – EDN YNASBV.

15. Утечка информации в медицинских учреждениях [Электронный ресурс]. – Режим доступа: https://rt-solar.ru/products/solar_dozor/blog/3025/

16. *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.

17. *Матвеев В.В., Зайцев А.К., Гайсина А.Р.* Обеспечение экономической безопасности при утечке конфиденциальной информации // Национальная безопасность и стратегическое планирование. – 2022. – № 3(39). – С. 52-75. – DOI 10.37468/2307-1400-2022-3-52-75. – EDN GMKMPB.

18. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных» [Электронный ресурс]. – Режим доступа: https://normativ.kontur.ru/document?moduleId=1&documentId=447363&ysclid=lq9mih9v565894592

19. Лаборатория Касперского Kaspersky [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/about/press-releases/2019_zdravoohranenie--novyy-chyornyy-dlya-zloumyshlennikov-dannye-medicinskih-kart-stoyat-dorozhe-bankovskih

20. Kaspersky research finds 174 municipal institutions targeted with ransomware in 2019 [Электронный ресурс]. – Режим доступа: https://www.kaspersky.co.uk/about/press-releases/2019_ransomare-vs-cities-in-2019-174-and-counting

21. Данные 9 миллионов пациентов были украдены после взлома американской медицинской компании по транскрипции [Электронный ресурс]. – Режим доступа: https://techcrunch.com/2023/11/15/9-million-patients-had-data-stolen-after-us-medical-transcription-firm-hacked/

22. Утекли персональные данные 2,2 млн пациентов в США [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/analytics/utechki-informatsii/utekli-personalnye-dannye-2-2-mln-patsientov-v-ssha

23. Информация о 5,6 миллионах посещений пациентов среди данных, украденных в результате атаки программы-вымогателя на больницы Онтарио [Электронный ресурс]. – Режим доступа: https://www.cbc.ca/news/canada/windsor/ransomware-attack-third-bunch-data-hospital-1.7019701

24. «Засекреченные» документы о российской вакцине «Спутник» выложили в сеть [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:%D0%A1%D0%BF%D1%83%D1%82%D0%BD%D0%B8%D0%BA_V_(%D0%B2%D0%B0%D0%BA%D1%86%D0%B8%D0%BD%D0%B0_%D0%BE%D1%82_%D0%BA%D0%BE%D1%80%D0%BE%D0%BD%D0%B0%D0%B2%D0%B8%D1%80%D1%83%D1%81%D0%B0_COVID-19).

25. DLBI: Data Leakage & Breach Intelligence [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:DLBI:_Data_Leakage_%26_Breach_Intelligence

26. Lehigh Valley Health Network [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.

27. Медицинское оборудование (рынок России) [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9C%D0%B5%D0%B4%D0%B8%D1%86%D0%B8%D0%BD%D1%81%D0%BA%D0%BE%D0%B5_%D0%BE%D0%B1%D0%BE%D1%80%D1%83%D0%B4%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_(%D1%80%D1%8B%D0%BD%D0%BE%D0%BA_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8).

28. Госдума приняла в первом чтении подготовленный фас законопроект об ужесточении ответственности за картели на обязательных торгах [Электронный ресурс]. – Режим доступа: https://fas.gov.ru/news/32350?ysclid=lqc92fnu40658284900

29. Куда только смотрят российские медиапотребители [Электронный ресурс]. – Режим доступа: https://adpass.ru/kuda-tolko-smotryat-rossijskie-mediapotrebiteli/?ysclid=lqczflh7wo34282335

30. Постановление Пленума Верховного Суда РФ от 24.02.2005 N 3 «О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц» [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_52017/?ysclid=lqd005i933341510918

31. Защитите свои цифровые активы [Электронный ресурс]. – Режим доступа: https://www.group-ib.com/products/digital-risk-protection/?ysclid=lqj9gc4h69274071424

32. *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.

References

1. National security strategy of the Russian Federation. Decree of the President of the Russian Federation dated July 2, 2021 No. 400. [Electronic resource]. – Access mode: http://www.kremlin.ru/acts/bank/47046

2. Program "Digital Economy of the Russian Federation" (approved by Decree of the Government of the Russian Federation of July 28, 2017 No. 1632-r).

3. Federal Law No. 242-FZ of July 29, 2017 "On amendments to certain legislative acts of the Russian Federation on the use of information technologies in the field of health care."

4. *Varzin S.A., Matveev V.V.* Applied application of artificial intelligence in ensuring social and economic security // Theoretical and applied aspects of economic security in the context of digitalization: Collection of articles / Edited by R.V. Dronova, E.E. Sharafanova. – St. Petersburg: St. Petersburg State Economic University, 2020. – P. 22-49. – EDN SSIYHV.

5. *Matveev A.V., Matveev V.V.* System-cybernetic approach to the definition of the concept of "security" // National security and strategic planning. – 2015. – No. 1(9). – P. 18-25. – EDN THRQRD.

6. World crisis 30: the evolution of rent and Dominance. Blog of A. Onoprienko [Electronic resource]. – Access mode: https://onoprienko.ru/mirovoj-krizis-30-evolyucziya-renty-i-domi/

7. Global GDP of the world: 1980-2023 [Electronic resource]. – Access mode: http://global-finances.ru/vvp-mira-po-godam/?ysclid=lqj4ca6ftp656586032

8. Declaration of G20 leaders: digital economy, digital equality, ICT security [Electronic resource]. – Access mode: https://d-russia.ru/deklaratsiya-liderov-g20-tsifrovaya-ekonomika-tsifrovoe-ravenstvo-bezopasnost-ikt.html?ysclid=lqj4mdjqrs268298667

9. On the Strategy for the Development of the Information Society in the Russian Federation for 2017-2030. Decree of the President of the Russian Federation dated 05/09/2017 No. 203. [Electronic resource]. – Access mode: http://www.kremlin.ru/acts/bank/41919

10. *Koshovets O.B., Ganichev N.A.* Global digital transformation and its goals: declarations, reality and a new growth mechanism // Economic science of modern Russia. – 2018. – No. 4(83). – pp. 126-143. – EDN YUCCHZ.

11. Cybersecurity in healthcare: attacks and damage are growing [Electronic resource]. – Access mode: https://www.infowatch.ru/analytics/daydzhesty-i-obzory/kiberbezopasnost-v-zdravookhranenii-ataki-i-uscherb-rastut?ysclid=lq9edna8h2368744601

12. Assessment of damage due to information leaks [Electronic resource]. – Access mode: https://www.infowatch.ru/analytics/analitika/otsenka-uscherba-vsledstvie-utechek-informatsii

13. Personal data of millions of patients leaked to the Internet [Electronic resource]. – Access mode: https://www.infowatch.ru/analytics/utechki-informatsii/v-set-utekli-personalnye-dannye-millionov-patsientov

14. *Myzrova K.A., Tuganova E.A.* Digitalization of healthcare as a promising direction of development // Issues of innovative economics. – 2018. – T. 8, No. 3. – P. 479-486. – DOI 10.18334/vinec.8.3.39355. – EDN YNASBV.

15. Information leakage in medical institutions [Electronic resource]. – Access mode: https://rt-solar.ru/products/solar_dozor/blog/3025/

16. 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.

17. *Matveev V.V., Zaitsev A.K., Gaisina A.R.* Ensuring economic security in case of leakage of confidential information // National security and strategic planning. – 2022. – No. 3(39). – P. 52-75. – DOI 10.37468/2307-1400-2022-3-52-75. – EDN GMKMPB.

18. Federal Law of July 27, 2006 N 152-FZ "On Personal Data" [Electronic resource]. – Access mode: https://normativ.kontur.ru/document?moduleId=1&documentId=447363&ysclid=lq9mih9v565894592

19. Kaspersky Lab Kaspersky [Electronic resource]. – Access mode: https://www.kaspersky.ru/about/press-releases/2019_zdravoohranenie--novyy-chyornyy-dlya-zloumyshlennikov-dannye-medicinskih-kart-stoyat-dorozhe-bankovskih

20. Kaspersky research finds 174 municipal

institutions targeted with ransomware in 2019 [Electronic resource]. – Access mode: https://www.kaspersky.co.uk/about/press-releases/2019_ransomare-vs-cities-in-2019-174-and-counting

21. Data of 9 million patients was stolen after an American medical transcription company was hacked [Electronic resource]. – Access mode: https://techcrunch.com/2023/11/15/9-million-patients-had-data-stolen-after-us-medical-transcription-firm-hacked/

22. Personal data of 2.2 million patients in the USA leaked [Electronic resource]. – Access mode: https://www.infowatch.ru/analytics/utechki-informatsii/utekli-personalnye-dannye-2-2-mln-patsientov-v-ssha

23. Information on 5.6 million patient visits among data stolen in a ransomware attack on Ontario hospitals [Electronic resource]. – Access mode: https://www.cbc.ca/news/canada/windsor/ransomware-attack-third-bunch-data-hospital-1.7019701

24. "Classified" documents about the Russian Sputnik vaccine were posted online [Electronic resource]. – Access mode: https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:%D0% A1%D0%BF%D1%83%D1%82%D0%BD%D0%B8%D0%BA_V_(%D0%B2%D0%B0%D0%BA%D1%86%D0%B8%D0%BD %D0%B0_%D0%BE%D1%82_%D0%BA%D0%BE%D1%80%D0%BE%D0%BD%D0%B0%D0%B2%D0%B8%D1%80%D1 %83%D1%81%D0%B0_COVID-19).

25. DLBI: Data Leakage & Breach Intelligence [Electronic resource]. – Access mode: https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:DLBI:_Data_Leakage_ %26_Breach_Intelligence

26. Lehigh Valley Health Network [Electronic resource]. – Access mode: https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F :Lehigh_Valley_Health_Network

27. Medical equipment (Russian market) [Electronic resource]. – Access mode: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9C%D0% B5%D0%B4%D0%B8%D1%86%D0%B8%D0%BD%D1%81%D0%BA%D0%BE%D0%B5_%D0%BE%D0%B1%D0%BE% D1%80%D1%83%D0%B4%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_(%D1%80%D1%8B%D0%BD%D0 %BE%D0%BA_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8).

28. The State Duma adopted in the first reading a draft bill on tightening liability for cartels in compulsory auctions [Electronic resource]. – Access mode: https://fas.gov.ru/news/32350?ysclid=lqc92fnu40658284900

29. Where Russian media consumers are looking [Electronic resource]. – Access mode: https://adpass.ru/kuda-tolko-smotryat-rossijskie-mediapotrebiteli/?ysclid=lqczflh7wo34282335

30. Resolution of the Plenum of the Supreme Court of the Russian Federation dated February 24, 2005 N 3 "On judicial practice in cases of protecting the honor and dignity of citizens, as well as the business reputation of citizens and legal entities" [Electronic resource]. – Access mode: https://www.consultant.ru/document/cons_doc_LAW_52017/?ysclid=lqd005i933341510918

31. Protect your digital assets [Electronic resource]. – Access mode: https://www.group-ib.com/products/digital-risk-protection/?ysclid=lqj9gc4h69274071424

32. Antonov A.E., Matveev V.V. Ensuring economic security using DLP systems (artificial intelligence) // Theoretical and applied issues of integrated security: Proceedings of the V International Scientific and Practical Conference, St. Petersburg, March 23, 2022. – St. Petersburg: St. Petersburg Institute of Environmental Management, Industrial Safety and Environmental Protection, 2022. – P. 251-257. – EDN DEOZZA.

Статья поступила в редакцию 6 июня 2023 г.
Принята к публикации 8 сентября 2023 г.

Ссылка для цитирования: Варзин С.А., Матвеев В.В. Обеспечение информационной безопасности в системе здравоохранения // Национальная безопасность и стратегическое планирование. 2023. № 3(43). С. 19-56. DOI: https://doi.org/10.37468/2307-1400-2023-3-19-56

For citation: Varzin S.A., Matveev V.V. Ensuring information security in the healthcare system // National security and strategic planning. 2023. № 3(43). pp. 19-56. DOI: https://doi.org/10.37468/2307-1400-2023-3-19-56

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 информационных технологий и высшей математики, Государственный институт экономики, финансов, права и технологий, 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 Department of Information Technology and Higher Mathematics, State Institute of Economics, Finance, Law and Technology, St. Petersburg, Russia*
SPIN: 6680-9575
e-mail: 070355mvv@gmail.com