ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ДАННЫХ В ОБЛАСТИ ЭЛЕКТРОННОГО ЗДРАВООХРАНЕНИЯ

Ржевская Н.В.[1], Лапина М.А.[2], Бабенко М.Г.[3]

Ключевые слова: *электронное здравоохранение, защита данных, угрозы, методология, эффективность, оценка.*

Аннотация

Цель исследования: проведение анализа текущего состояния системы защиты медицинской информации, формирование рекомендаций по улучшению комплексной защиты электронного здравоохранения.

Методы исследования: системный анализ, классификация, сравнительно-правовой метод, практическое моделирование.

Результаты исследования: разработка методологии оценки эффективности в данной области. Разработанная методология представляет собой систематизированный подход к оценке уровня защиты данных в электронном здравоохранении. Она включает в себя процесс анализа уязвимостей, оценку текущих мер защиты, идентификацию рисков и предложение конкретных рекомендаций по улучшению защиты информации. Предложенный подход помогает не только определить уровень угроз и уязвимостей, но и предлагает практические шаги по их устранению и предотвращению.

Новизна исследования: впервые предложена методология оценки эффективности защиты данных в электронном здравоохранении, которая позволит провести комплексную оценку защищенности данной области. Полученные результаты могут быть использованы для повышения уровня безопасности данных в электронном здравоохранении, а также для разработки и внедрения эффективных мер по защите информации в данной сфере.

DOI: 10.24682/1994-1404-2024-3-68-85

Введение

Электронное здравоохранение стало катализатором значительной эволюции в медицинской сфере, особенно это актуально в последние годы. Термин «электронное здравоохранение» расширил потенциал в этой области.

Электронное здравоохранение (англ. eHealth, electronic healthcare) — это термин, охватывающий ряд процессов и практик, в которых используются информационные и коммуникационные технологии для сбора, хранения, обработки, передачи и анализа данных и информации о здоровье с целью повышения качества здравоохранения, расширения доступа к медицинским услугам и повышение эффективности управления здравоохранением.

Основным преимуществом этого нововведения стало улучшенное управление медицинской информацией. Несмотря на преимущества этого явления, при попытке защитить важную медицинскую информацию возникают дополнительные опасности. Без комплексной защиты этих данных конфиденциальная медицинская информация пациентов находится под угрозой.

Медицинская информация пациентов чрезвычайно чувствительна и подвержена риску утечки и хакерских атак. Улучшенные системы защиты также помогут снизить риски утечек данных и хакерских атак, что способствует стабильности системы электронного здравоох-

[1] ***Ржевская Наталья Витальевна,*** *ассистент кафедры вычислительной математики и кибернетики Северо-Кавказского федерального университета, г. Ставрополь, Российская Федерация. ORCID: 0009-0002-1285-4196.*

E-mail: natalia070901@gmail.com

[2] ***Лапина Мария Анатольевна,*** *научный руководитель, кандидат физико-математических наук, доцент, доцент кафедры информационной безопасности автоматизированных систем Северо-Кавказского федерального университета, г. Ставрополь, Российская Федерация. ORCID: 0000-0001-8117-9142.*

E-mail: mlapina@ncfu.ru

[3] ***Бабенко Михаил Григорьевич,*** *научный руководитель, доктор физико-математических наук, доцент, заведующий кафедрой вычислительной математики и кибернетики Северо-Кавказского федерального университета, г. Ставрополь, Российская Федерация. ORCID: 0000-0001-7066-0061.*

E-mail: mgbabenko@ncfu.ru

ранения и уменьшению финансовых и репутационных потерь. Экономические выгоды также очевидны, поскольку предотвращение инцидентов в области безопасности может сэкономить огромные ресурсы, которые в противном случае могли бы быть направлены на расследование и восстановление после нарушений данных.

Постановка задачи

Задачей данного исследования является проведение детального анализа текущего состояния системы защиты медицинской информации и формирование рекомендаций по улучшению комплексной защиты электронного здравоохранения. В рамках исследования предполагается изучение существующих стандартов и нормативных актов, регламентирующих защиту медицинских данных, оценка соответствия медицинских учреждений этим стандартам, а также анализ технологий и средств защиты, применяемых в данной области. Важно выявить основные угрозы и уязвимости, определить наиболее частые векторы атак на медицинские информационные системы, и проанализировать инциденты безопасности и их последствия. На основе этого анализа будут разработаны рекомендации по внедрению передовых технологий и практик, совершенствованию нормативной базы и процессов управления информационной безопасностью. Реализация данных задач позволит создать комплексную стратегию защиты медицинских данных, учитывающую современные угрозы и технологии, и повысить уровень защищенности электронного здравоохранения.

Обзор литературы

1. Российская практика

Уязвимость медицинских данных должна быть учтена при создании единого информационного пространства здравоохранения. При этом должна быть составлена модель защиты прав пациента, закрепленной законодательно, а также определены полномочия при обмене информацией между субъектами этой системы. При обеспечении информационной безопасности в медицинской сфере необходимо руководствоваться тремя принципами: целостностью, доступностью и конфиденциальностью [1, 3].

Изучение использования телемедицинских технологий невозможна без учета анализа обеспечения конфиденциальности персональных данных пациентов. В соответствие с нормативной документацией Российской Федерации, персональная медицинская информация признается особой категорией персональных данных, что говорит о том, что ее необходимо эксплуатировать, соблюдая определенные требования. Соблюдая данные требования, такая информация должна храниться на более высоком уровне. Утечка таких данных потенциально угрожает субъектам персональных данных, а обработка вышеупомянутой информации допускается только в определенных случаях. При этом необходимо соблюдать условие, что обработкой персональных данных занимается лицо, осуществляющее медицинскую деятельность и обязанное в соответствии с законодательством Российской Федерации соблюдать медицинскую тайну.

Таким образом, использование телемедицинских технологий приводит к росту ответственности медицинских учреждений за обработку данных [2]. Однако отсутствие специальных норм, касающихся ответственности операторов персональных данных при предоставлении телемедицинских услуг, позволяет учреждениям передавать эту задачу третьим лицам, что влечет за собой увеличение риска утечки информации.

Согласно Федеральному закону от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [29] фактически все медицинские организации являются субъектами критической информационной инфраструктуры. В соответствии также с Постановлением Правительства РФ № 127 [30] можно сказать, что организации здравоохранения относятся к первой категории значимой критической информационной инфраструктуры. Полагаясь на это согласно требованиям законодательства РФ для реализации итогового набора мер, должны применяться средства защиты информации, прошедшие оценку на соответствие требованиям по безопасности в формах сертификации, а также данные средства должны соответствовать классу защиты. Сертифицированные СрЗИ и используемые средства вычислительной техники должны подбираться в соответствии с категорией значимости объектов КИИ.

Существует обширное законодательное поле, требующее, чтобы медицинские учреждения, как частные, так и государственные, обеспечивали защиту медицинской информации своих пациентов. Эти законы предписывают, что персональные данные, в том числе медицинские, должны быть защищены соответствующими мерами безопасности, такими как шифрование, контроль доступа и т. д.

Так как информация, относящаяся к врачебной тайне, является конфиденциальной и такие персональные данные относятся к специальной и биометрической категориям ПДн, то согласно Приказу ФСТЭК России № 21 [34] такие информационные системы персональных данных относится к первому уровню защищённости персональных данных. Для данных системы необходимо придерживаться требованиям к мерам защиты информации.

На сегодняшний момент имеется огромная нормативная база как в области обеспечения информационной безопасности, как и электронного здравоохранения в целом (*рис.* 1).

Данные нормативные документы являются базовыми в области обеспечения защиты персональных данных в целом. Необходимо отметить, что при комплексной защите персональных данным в области здравоох-

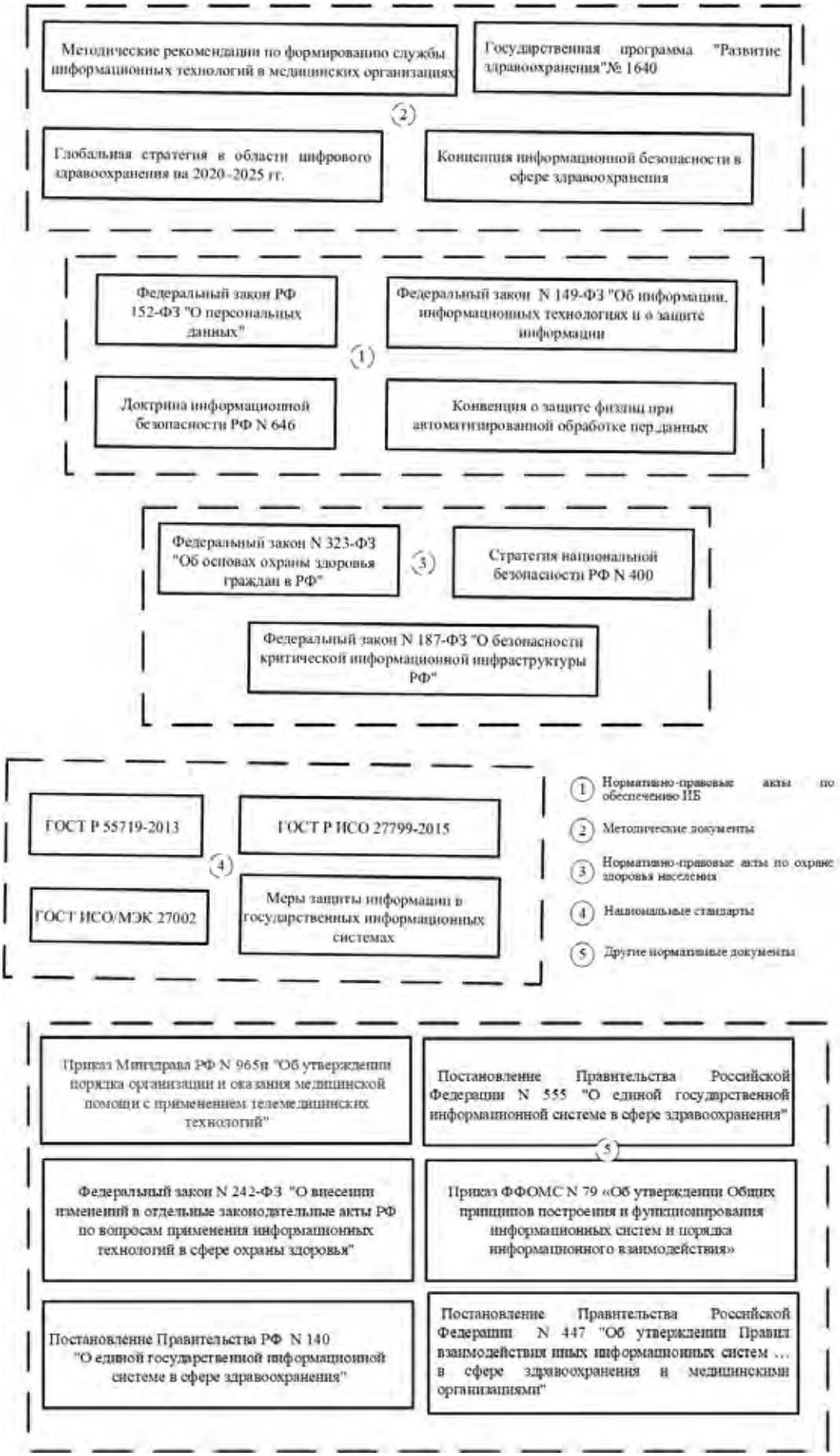

Рис 1. Нормативно-правовая база в области электронного здравоохранения

ранения необходимо, также учитывать другие правовые документы по данному вопросу.

Проанализировав всю нормативно-правовую базу, можно сделать вывод о сложности и многоуровневости национальной нормативно-правовой базы в области персональных данных, охраны здоровья и критической информационной инфраструктуры, а также электронного здравоохранения в целом. Такая обширная и детализированная правовая база позволяет обеспечить взаимодействие различных участников и обеспечить более высокий уровень безопасности и качества медицинских услуг.

2. Международная практика

Международная практика в области защиты данных электронного здравоохранения демонстрирует разнообразие подходов и мер, направленных на защиту конфиденциальной информации пациентов. Изучение нормативных актов, таких как HIPAA в США, и интеграция передовых технологий и практик, представленных в различных исследованиях и публикациях, позволяет оценить эффективность текущих мер и разработать рекомендации по их совершенствованию.

Исследование [8] подчеркивает важность адаптации существующих нормативных актов к новым реалиям телемедицины, возникшим в период пандемии COVID-19. В условиях стремительного роста использования телемедицинских услуг актуальность и значимость Правила безопасности HIPAA (HIPAA Security Rule) стали еще более очевидными. Правила безопасности HIPAA включает три основных компонента: административные, технические и физические меры безопасности. Административные меры включают разработку политик и процедур безопасности, обучение сотрудников и проведение регулярных аудитов. Технические средства защиты включают в себя шифрование информации, контроль доступа и подтверждение личности пользователей, в то время как физические меры фокусируются на охране оборудования и данных от несанкционированного доступа [9].

В ряде исследований [10, 15—16] детализируются основные технические, административные и физические защитные меры, предусмотренные законом HIPAA. К ним относятся шифрование данных, подтверждение пользователей, контроль доступа и ведение журналов активности. Пандемия COVID-19 подтолкнула к широкому применению решений электронного здравоохранения (e-health) для поддержки персонализированного здравоохранения. Так, по данных исследования [24], Финляндия демонстрирует успешную интеграцию электронного здравоохранения (e-health) и электронного социального обеспечения (e-welfare), ставя акцент на безопасность данных.

Однако внедрение таких технологий потребовало усиления мер безопасности и конфиденциальности данных [22]. Различные технологии электронного здравоохранения значительно повысили доступность медицинских услуг, но также увеличили риски кибератак и утечек данных, что требует постоянного совершенствования мер безопасности [11, 12].

Временные послабления, введенные для поддержки телемедицины, привели к возникновению новых угроз и уязвимостей, таких как фишинг и атаки на видеоконференции, что требует дополнительных мер безопасности. Современные облачные технологии играют ключевую роль в улучшении усилий информационной безопасности, обеспечивая автоматизацию процессов управления безопасностью и улучшая масштабируемость систем [13].

Кроме того, в исследованиях [8, 14] акцентируется внимание на необходимости выбора проверенных и защищенных телемедицинских платформ, а также на важности обеспечения безопасности видеоконференций через использование шифрования и паролей. Внедрение облачных технологий также связано с новыми вызовами, такими как управление доступом и контроль прав пользователей. Исследования показывают, что выбор надежных облачных провайдеров и разработка политик безопасности являются критическими для соблюдения международных стандартов [20, 23].

Особое внимание уделяется постоянному обучению сотрудников, проведению регулярных аудитов безопасности и тестированию на проникновение для выявления уязвимостей [15—19]. Разработка и внедрение планов реагирования на инциденты безопасности рассматриваются как критически важные меры для защиты данных в условиях развития телемедицины.

Применение различных решений электронного здравоохранения в развивающихся странах также демонстрирует важность адаптации технологий к местным условиям и обеспечения доступности медицинских услуг для широкого круга пользователей, таких как использование мобильных клиник и других портативных решений [17, 27].

Использование блокчейн и искусственного интеллекта в электронном здравоохранении открывает новые возможности для обеспечения безопасности и конфиденциальности данных [25]. Однако безопасность и конфиденциальность в облачных системах электронного здравоохранения остаются важными вызовами, требующими инновационных решений [26].

Глобальная политика в данной области требует стратегического подхода к обеспечению безопасности данных на международном уровне [28]. Эти аспекты международной практики подчеркивают необходимость постоянного совершенствования мер безопасности для обеспечения устойчивой защиты электронного здравоохранения.

Исследование предметной области

Развитие электронного здравоохранения предъявило медицинским организациям новые требования, связанные с защитой критически важной информацией и сопоставимости данным требованиям [5, 7].

Ключевыми проблемами, с которыми медицинские учреждения сталкиваются в процессе цифровой трансформации, являются низкий уровень осведомленности сотрудников о вопросах информационной безопасности, растущий интерес со стороны киберпреступников к медицинским данным, а также нехватка квалифицированных кадров в области информационной безопасности в здравоохранении. Часто работники здравоохранения не осознают значимость аспектов информационной безопасности, что открывает возможности для атак злоумышленников.

Очевидно, что информационная безопасность в сфере здравоохранения не рассматривается как приоритетное направление в данной области. Так, аргументируя это недостаточностью финансового обеспечения, медицинские организации не способны нанять грамотных экспертов в области кибербезопасности или обучить уже имеющихся специалистов, что приводит к громким скандалам с кражей персональных данных, а в дальнейшем и к финансовым и репутационным потерям. Все эти обстоятельства приводят к серьезных угрозам информационной безопасности (*рис.* 2).

Рис 2. Основные угрозы электронного здравоохранения

Особое внимание в сфере охраны персональных данных пациентов уделяется правильному хранению и защите баз данных медицинских организаций. Значительными слабыми местами в данном вопросе являются:

– недостаточное шифрование данных;
– проблемы в системе хранения;
– отсутствие резервного копирования данных.

Использовав данные уязвимости киберпреступник, получит доступ к конфиденциальной информации, что может привести к большим проблемам для медицинских организаций вплоть до потери медицинских записей.

Внедрение новых технологий в медицинских учреждениях требует не только активного использования персоналом ноутбуков и гаджетов, но и подключаемых к Интернету устройств. Угрозы утечек данных остаются актуальными, так как в отрасли еще не в полной мере осознали важность обеспечения безопасности информации [1]. Для улучшения ситуации медицинским организациям, их ИТ-отделам, необходимо внедрять комплексные меры цифровой безопасности. Нарастающая угроза программ-вымогателей и неопытность некоторых сотрудников в области кибербезопасности создают дополнительные сложности для специалистов в этой области. Такие сведения подчеркивают актуальность данного исследования.

Также немаловажной проблемой в сфере здравоохранения является использование неактуальных программных продуктов, а также неполадки в системах безопасности. Все перечисленные проблемы способствуют возникновению дополнительных возможностей для нарушителей. Кроме того, социальная инженерия, вызванная недостаточной обученностью персонала в области безопасности и безрассудным обращением с конфиденциальной информацией, представляет дополнительный риск для раскрытия чувствительных данных.

Медицинская тайна охватывает личные данные пациентов, которые могут быть получены врачами и другими медицинскими работниками в процессе оказания медицинских услуг. Похищенная конфиденциальная информация пациентов может быть использована различными способами, для осуществления противоправных действий киберпреступниками.

При анализе угроз безопасности информации в информационных системах в сфере здравоохранения, использовались методы, утвержденные методическим документом «Методика оценки угроз безопасности информации» ФСТЭК России [33]. Данный подход основывался на информации о системах здравоохранения и данных, содержащихся в банке угроз безопасности информации ФСТЭК России.

Полагаясь также на Концепцию информационной безопасности в сфере здравоохранения [4, 6], можно выделить основные угрозы в данной области (*рис.* 3).

Согласно Федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [32], угрозы, которые могут быть применены к системам электронного здравоохранения подразделяются на следующие виды:

– создаваемые нарушителем (внутренним и внешним);
– создаваемые вредоносными программами и воздействиями.

При этом под внешнем нарушителям подразумеваются лица или организации, не имеющие официального доступа или разрешения на доступ к электронным системам здравоохранения, но стремящиеся получить несанкционированный доступ или нанести вред таким системам.

Рис 3. Основные угрозы в сфере электронного здравоохранения

Под внутренними нарушителями могут пониматься следующие категории лиц:

- медицинские работники: врачи, медсестры, администраторы, фармацевты и другие сотрудники, у которых есть доступ к электронному здравоохранению и к конфиденциальной медицинской информации пациентов;
- административный персонал: руководители, администраторы баз данных, системные администраторы и другие сотрудники, которые управляют инфраструктурой электронного здравоохранения;
- внешние поставщики услуг: поставщики облачных сервисов, разработчики программного обеспечения, внешние службы поддержки и другие третьи лица, которые имеют доступ к системе электронного здравоохранения.

Проектирование

Проектирование методологии оценки эффективности защиты данных в электронном здравоохранении необходимо начинать с определения целей и задачи данного процесса. В данном случае необходимая цель, которую требуется достичь — это обеспечения надежной защиты медицинской информации от несанкционированного доступа, а также предотвращение утечки и неправомерного использование защищаемых данных.

За основу для разработки собственной методологии были использованы следующие нормативные документы:

- постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [38];
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных от 14 февраля 2008 г. [33];
- приказ ФСТЭК РФ от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [34];
- ГОСТ Р ИСО 27799-2015 Информатизация здоровья. Менеджмент защиты информации в здравоохранении по ИСО/МЭК 27002 [31];
- банк данных угроз безопасности информации ФСТЭК России.

Ключевым и одним из самых важных этапов в разработки описываемой методологии является определение критериев оценки эффективности защиты данных. Каждый критерий должен быть ясно определен и иметь критерии оценки, которые позволят сравнить различные системы защиты данных (*рис.* 5).

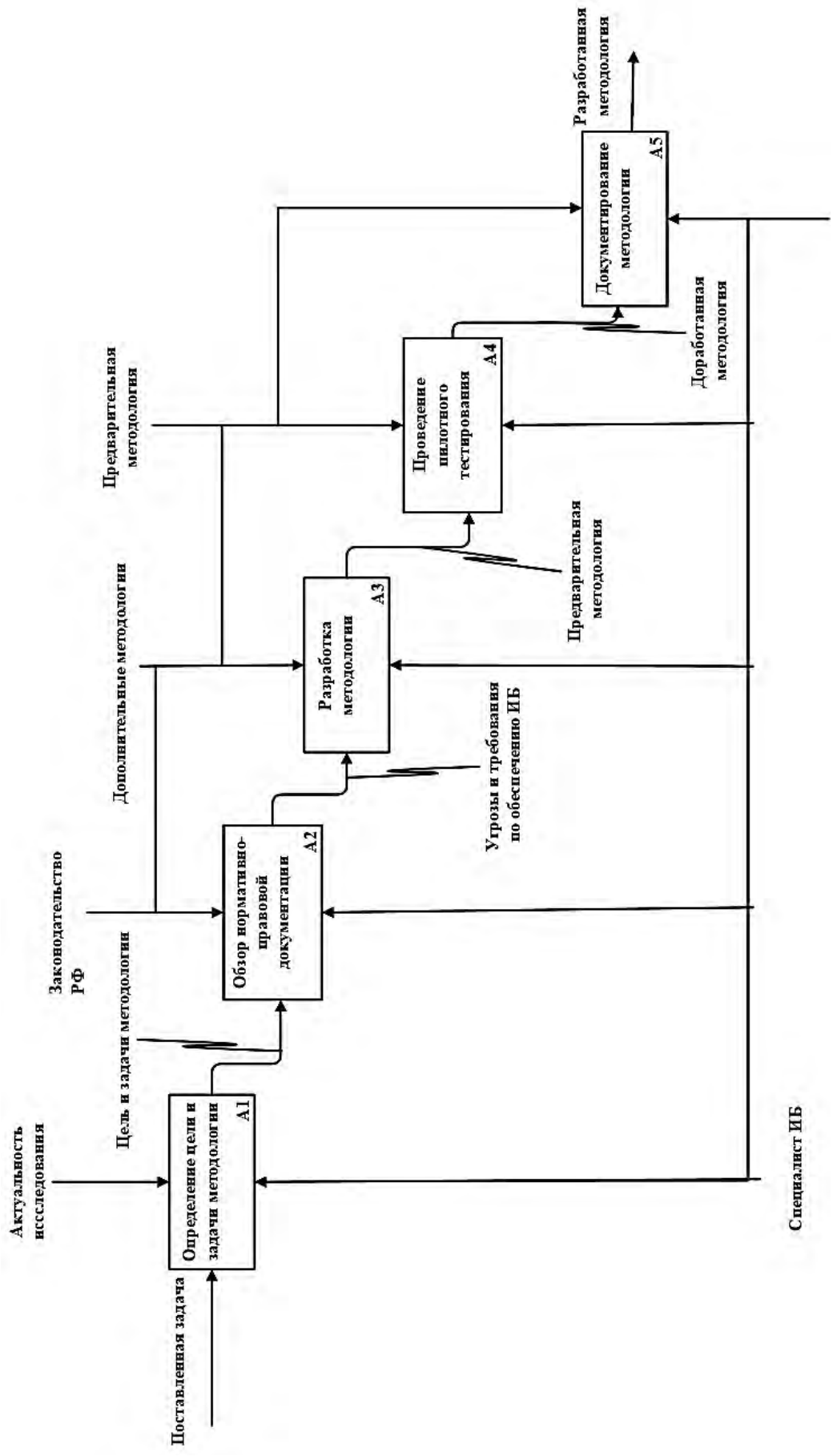

Рис 4. Алгоритм разработки методологии

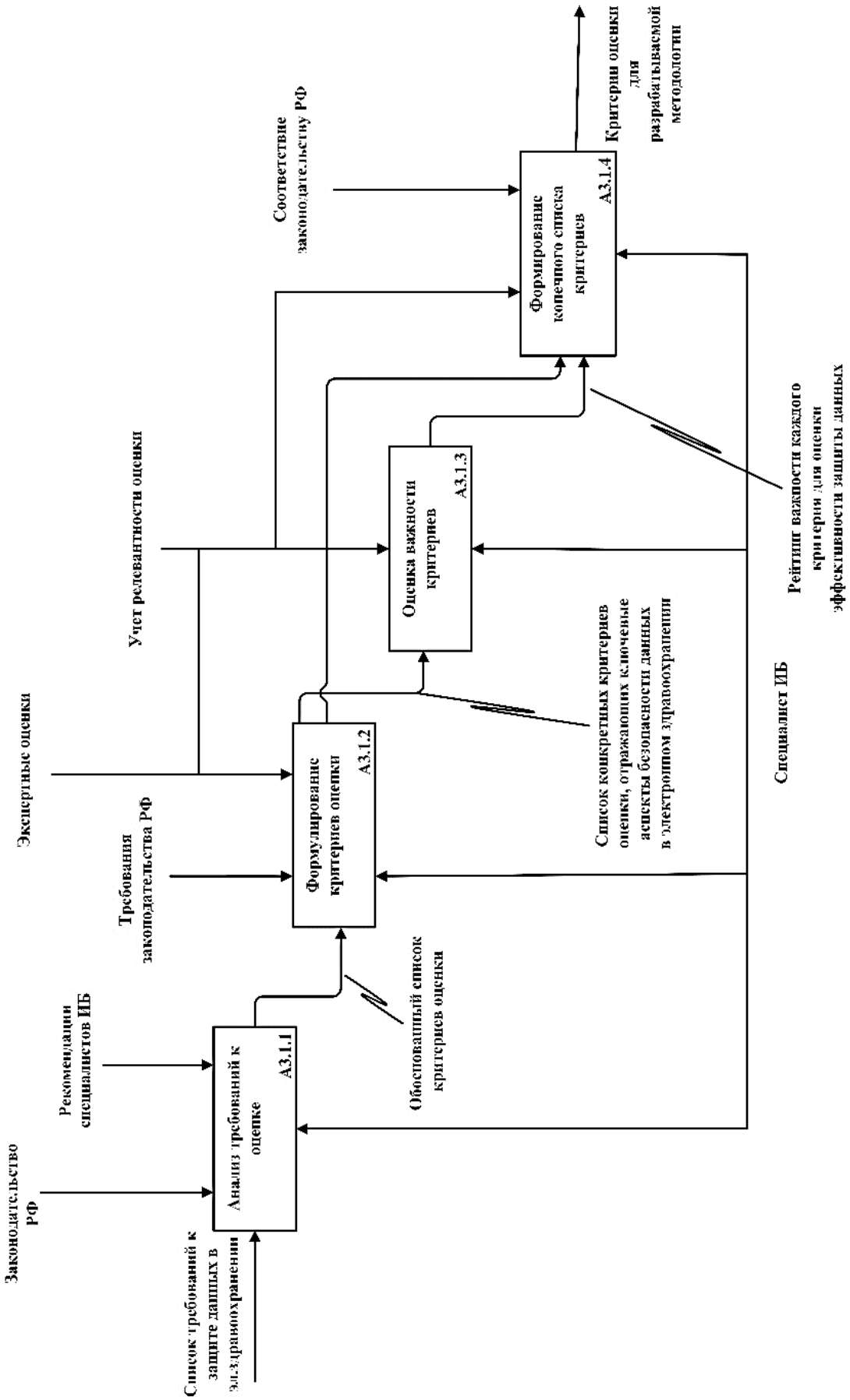

Рис 5. Алгоритм определения критериев оценки методологии

Основными критериями, показывающими хорошо защищённую информационную систему, хранящую чувствительную информацию, являются:

– конфиденциальность;
– целостность;
– доступность.

Таким образом, для обеспечения эффективной защиты медицинских данных, в том числе при использование электронного здравоохранения необходимо придерживаться данными принципами, которые послужат основами критериями оценки защищенности данных. Именно этим критериям будет отдаваться приоритетное значение при оценке защиты данных.

Моделирование

Первым этапом при оценке защищенности ИС является сбор информации об исследуемой системы. Следует изучить типы используемых систем, алгоритмы шифрования данных, механизмы аутентификации и авторизации, а также ознакомится и другими используемыми средствами защиты информации. Данный анализ позволит определить преимущества и недостатки защиты информационной системы (*табл.* 1).

Таблица 1

Пример анализа СЗИ на реализуемые меры защиты

№ п/п	Название СЗИ	Область реализации защиты
1	Dr.Web Enterprise Security Suite	ИАФ.1-6, УПД.1-6, УПД.10-11, 13-15, АВЗ.1, 2, СОВ.1, АНЗ.1-4, ОЦЛ.1, ОЦЛ.4-6, РСБ.1-3, РСБ.7, ЗИС.3, 11, 15, ИНЦ.2-6, УКФ.1-4
2	Dallas Lock 8.0-K	ИАФ.1-6, УПД.1-6, УПД.10-11, 13-17, ОПС.2, 3, ЗНИ.1, 2, 8, РСБ.1-3, 5, 7, АНЗ.1-4, ОЦЛ.1, 4, 5, ЗСВ.1-3, 6-10 ЗТС.3, 4, ЗИС.3, 11, 15, 17, ИНЦ.1- 6, УКФ.1-4
3	XSpider 7.8.25	РСБ.1-3, СОВ.1-2, АНЗ.1-4, ОЦЛ.1, 4, 5, ИНЦ.1-6.
4	ViPNet Client	ИАФ.1-6, УПД.1-6, 10-11, 13-17, АВЗ.1, 2, ЗНИ.1, 2, 8, РСБ.1-3, 7, ЗИС.3, 11, 15, ИНЦ.2-6, УКФ.1- 4

После сбора необходимой информации об анализируемой информационной системе, для качественной оценки эффективности защиты данных в электронном здравоохранении можно использовать различные методологии и системные подходы. Так основой может послужит международные и отечественные стандарты, а также служебные рекомендации.

Не стоит также забывать об необходимости учета законодательных требований и нормативных актов. В частности, стоит уделить особое внимание различным правовым актам в области персональных данных, защиты информационных систем и охраны здоровья граждан.

После проведения оценки необходимо описать результаты и предложить рекомендации по улучшению системы защиты данных. Описание результатов должно включать в себя анализ выявленных уязвимостей и проблем, а также оценку эффективности текущей системы защиты данных. Рекомендации по улучшению системы защиты данных должны быть конкретными и основываться на анализе результатов оценки.

Таким образом, разрабатываемая методология будет служить помощником для оценки уровня безопасности в системах электронного здравоохранения, а также поможет выявить потенциальные уязвимости, которые могут быть использованы злоумышленником. После сбора информации о системе необходимо категорировать компоненты системы.

В *табл.* 2 наглядно представлен процесс оценки компонентов информационной системы электронного здравоохранения:

Таблица 2

Процесс расчета показателя T1

№	Название компонента системы	τ1	τ2	τ3	Ср. значение	T1
1	Медицинская электронная карта	5	5	5	5	I
2	Электронный рецепт	5	5	5	5	I
3	ЭКГ	4	5	5	4,6	I
4	Компонент 4	1	3	5	3	III
N	Компонент N	2	3	5	3,3	III

Для наглядности были выбраны следующие численные критерии оценки чувствительности компонентов:

1 — низкая чувствительность критерия;
2 — частичная чувствительность критерия;
3 — в целом чувствительный критерий;
4 — чувствительный критерий;
5 — сверхчувствительность критерия.

В данной таблице τ1 — коэффициент чувствительности конфиденциальности, τ2 — коэффициент чувствительности доступности, τ3 — коэффициент чувствительности целостности.

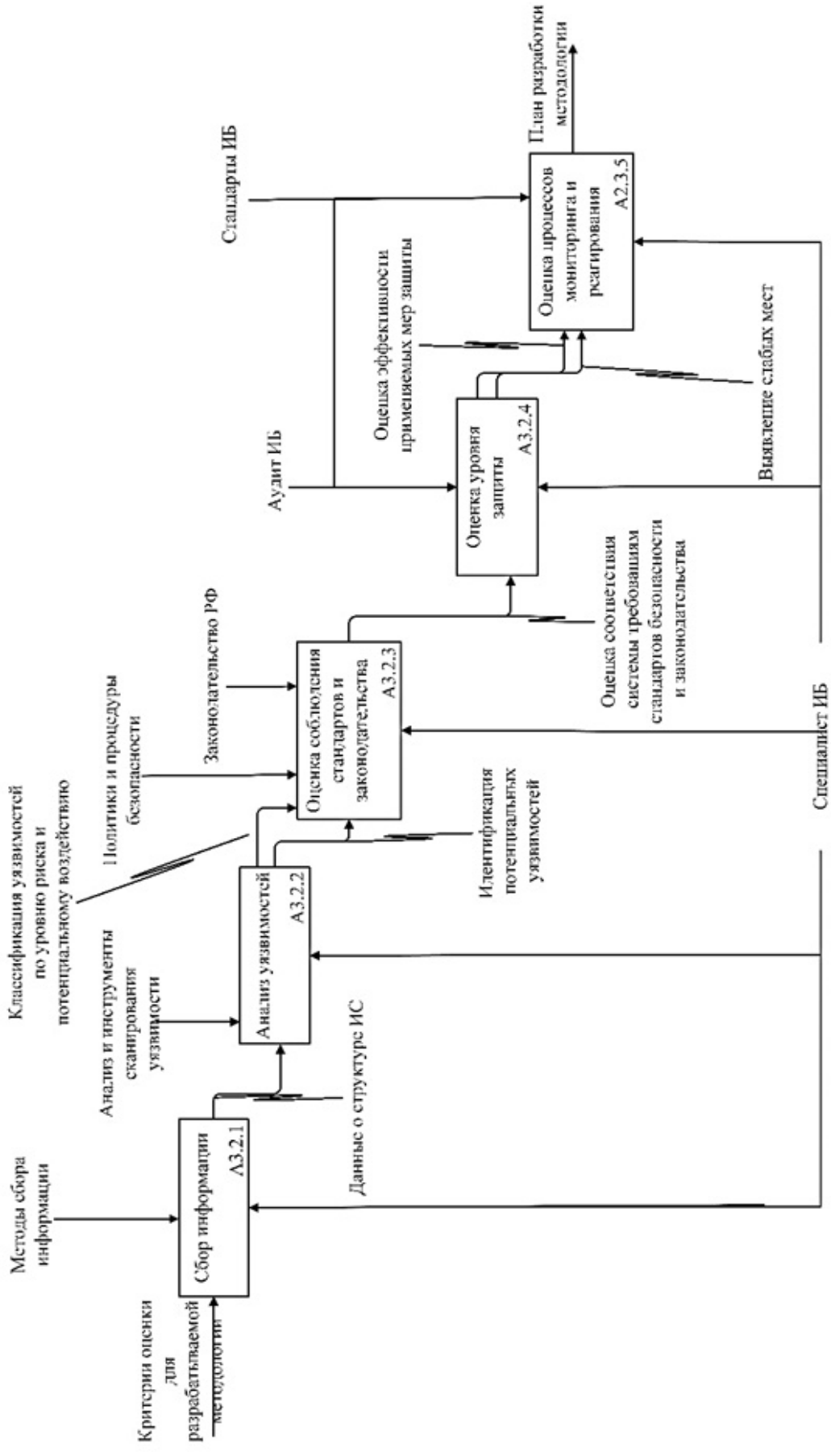

Рис 6. Алгоритм оценки эффективности защиты данных в электронном здравоохранении

Т1 отражает показатель оценки чувствительности компонента системы. В свою очередь Т1(общ) отражаем уровень чувствительности системы здравоохранения в целом, Т1(балл) показатель, отражающий значение чувствительности системы в процентном соотношении. Данные показатели оцениваются исходя из следующих правил (*табл.* 3):

Таблица 3

Правила определения показателя Т1 и Т1(общ)

Обозначение показателя		Диапазон ср. значения	Балл защищенности Т1(балл)
VI	НЧ — не чувствителен	1—2	0
III	ТВ — требует внимания	2,1—3,6	0,3
II	ДЧ — достаточно чувствителен	3,7—4,1	0,7
I	СЧ — сверхчувствителен	4,2—5	1

Таким образом, данные показатели отражают значимость составляющих информационной безопасности для компонента электронного здравоохранения с чувствительной информацией.

Каждая оценка показывает чувствительность поддержания конфиденциальности, доступности и целостности компонента информационной системы. Таким образом, показатели Т1 и Т1(общ) способствуют проведению анализа как отдельных компонентов системы, так и общей системы электронного здравоохранения организации (*табл.* 4).

Таблица 4

Пример расчета показателя Т1 и Т1(общ)

№ п/п	Название компонента системы		т1	т2	т3	Среднее значение показателей	Т1
1	Электронная медицинская карта		5	5	5	5,00	1
2	Результат анализа		4	4	5	4,33	2
3	Электронный репепт		5	4	5	4,67	1
4	Электронный медицинский стандарт		1	3	5	3,00	3
5	Онлайн-консультация		5	4	5	4,67	1
6	Запись о здоровье в мобильном приложении		5	5	5	5,00	1
7	Онлайн-консилиум врачей		5	5	5	5,00	1
8	Анонимное обращение		1	3	4	2,67	3
9	Результаты ЭКГ		5	5	5	5,00	1
10	Результат анализа		4	4	5	4,33	2
11	Онлайн-консультация		5	4	5	4,67	1
12	Электронный рецепт		5	4	5	4,67	1
13	Электронная медицинская карта		5	5	5	5,00	1
14	Электронный медицинский стандарт		1	3	5	3,00	3
15	Анонимное обращение		1	3	4	2,67	3
Значимость чувствительности показателя			4	4	5	2	
Среднее значение чувствительности системы			4,24				

Следующим этапом проводится анализ соответствия мер защиты информации в анализируемой системе требованиям законодательства по обеспечению защиты данных, в соответствии с собранными данными о информационной системе и средствах защиты информации.

Для комплексной защиты информации необходимо применять базовый набор мер защиты информации, а именно:

– проводить идентификацию, аутентификацию и управление идентификаторами пользователей и устройств;

– проводить мониторинг и запись всех попыток входа в систему, а также ограничить количество неудачных попыток за определенный период времени;
– управлять учетными записями, разграничивать доступ, а также разделять полномочия пользователей;
– контролировать информационные потоки, взаимодействиями с внешними системами и машинными носителями информации;
– регламентировать и контролировать использование беспроводных и мобильных устройств;
– обеспечить систему средствами доверенной загрузки и средствами вычислительной техники и защиты архивных файлов;
– контролировать использование интерфейсов ввода-вывода;
– обеспечить систему антивирусной защитой и средствами обнаружения вторжений;
– организовать меры защиты информации при передаче по каналам связи и беспроводным соединениям;
– исключить доступ предыдущих пользователей к информации и защитить систему от отказа в обслуживании.

Далее экспертом определены меры защиты, которые необходим реализовать для качественной защиты системы с определенным уровнем чувствительности (*табл.* 5).

Таблица 5

Меры защиты для *n*-уровня чувствительности

№ п/п	Условное обозначение	Уровень чувствительности			
		1	2	3	4
1	ИАФ.1	+	+	+	+
2	ИАФ.2	+	+	+	+
3	ИАФ.3-4	+	+	+	+
4	ИАФ.5	+	-	-	-
5	ИАФ.6	+	+	-	-
6	УПД.1	+	+	+	-
.....					
46	УКФ.4	+	-	-	-
Итого баллов (Т2(зак))		46	42	25	17

Специалистам информационной безопасности необходимо соотнести количество мер, которые реализуют СЗИ системы к требуемому количеству необходимых баллов, обозначенных для системы с определенный уровнем чувствительности информации. Уровень чувствительности информации соответствует показателю $T1$(общ).

Для определения соответствия средств защиты информации требованиям законодательства необходимо определить данный показатель $T2(общ)$:

$$T2(общ) = \frac{T2}{T(зак)} \cdot 100\%$$

где $T2$ — показатель реализованной защиты информации, а $T(зак)$ —показатель необходимой, согласно законодательству, защиты.

Если показатель $T2(общ)$ имеет значение менее 70% или 0,7, то меры, реализованные для защиты данной системы недостаточны с точки зрения законодательства для данной системы. В другом случаи реализованные меры в такой системе соответствуют требованиям законодательства. Стоит отметить, что если показатель $T2(общ)$ имеет значение более 100% или 1, то для простоты дальнейших подсчетов значение можно округлить до 1. Пример данного расчета представлен в *табл.* 6.

Таблица 6

Пример расчета показателя *T2* и *T2(общ)*

№ п/п	Условное обозначение	Уровень чувствительности				Реализованные меры
		1	2	3	4	
1	ИАФ.1	1	1	1	1	1
2	ИАФ.2	1	1	1	1	1
3	ИАФ.3-4	1	1	1	1	1

(продолжение)

№ п/п	Условное обозначение	Уровень чувствительности				Реализованные меры
		1	2	3	4	
4	ИАФ.5	1	0	0	0	0
5	ИАФ.6	1	1	0	0	1
6	УПД.1	1	1	1	0	1
7	УПД.2	1	1	0	0	1
8	УПД.3	1	1	1	1	1
9	УПД.4	1	1	0	0	0
10	УПД.5	1	1	1	0	1
11	УПД.10	1	1	0	0	1
12	УПД.11	1	1	0	0	0
13	УПД.13	1	1	1	1	1
14	УПД.14-15	1	1	0	0	0
15	УПД.16	1	1	1	0	1
16	ОПС.1	1	1	0	0	1
17	ОПС.2	1	1	1	1	1
18	ЗНИ.2	1	1	1	1	1
19	ЗНИ.4	1	1	1	1	1
20	ЗНИ.8	1	1	0	0	0
21	РСБ.3	1	1	0	0	0
22	АВЗ.1	1	1	1	0	1
23	АВЗ.2	1	1	0	0	0
24	СОВ.1	1	1	0	0	0
25	АНЗ.1	1	1	1	1	1
26	АНЗ.2	1	0	0	0	0
27	АНЗ.3	1	1	1	1	1
28	АНЗ.4	1	1	1	1	1
29	АНЗ.5	1	1	0	0	0
30	ОЦЛ.1-2	1	1	1	0	1
31	ОЦЛ.3	1	1	1	0	1
32	ОЦЛ.7	1	1	1	1	1
33	ОДТ.5	1	1	0	0	0
34	ЗСВ.4	1	1	0	0	1
35	ЗСВ.7	1	1	1	0	1
36	ЗТС.1	1	1	1	1	1
37	ЗТС.3	1	1	1	0	1

(продолжение)

№ п/п	Условное обозначение	Уровень чувствительности				Реализованные меры
		1	2	3	4	
38	ЗИС.3	1	1	1	1	1
39	ЗИС.9	1	1	0	0	0
40	ЗИС.12-13	1	1	1	1	1
41	ЗИС.15	1	1	1	1	1
42	ЗИС.20	1	1	1	1	1
43	ИНЦ.1-6	1	0	0	0	0
44	УКФ.2	1	1	0	0	0
45	УКФ.3	1	1	0	0	0
46	УКФ.4	1	0	0	0	0
Т2(зак)		46	42	25	17	
Т2		**30**				
Т2(общ)		**0,7**		**ДОСТАТОЧНЫ**		

После определения показателей *Т1(балл)* и *Т2(общ)* рассчитывается показатель эффективности защиты данных в электронном здравоохранении Д. Данный показатель рассчитывается по формуле:

$$Д = \frac{Т1(балл) + Т2(общ)}{2} \quad (2)$$

Полученный результат можно интерпретировать исходя из значений *табл.* 8.

Таблица 7

Определение уровня эффективности защиты данных в электронном здравоохранении

№ п/п	Условное обозначение	Значение показателя	Диапазон значений
1	I	Достаточная эффективность	0,5—1
2	II	Недостаточная эффективность	0—0,5
3	СВ	Сверхэффективность защиты	<1

При этом стоит отметить, что в случае, если показатель *Т2(общ)* имеет значение менее 0,7 или 70%, то эффективность защиты данных в информационной системе является недостаточной и показателю Д присваивается значение II.

Также стоит учитывать, что если показатель Д имеет значение более 100% или 1, то эффективность защиты данных в такой системе является сверхэффективной, что может быть нерационально с точки зрения экономических расходов.

Таблица 8

Пример расчета показателя Д

Т1(общ)	Т1(балл)	Т2(общ)	Д	Д(балл)
2	0, 7	0, 7	1	0, 7

Расчёт данных показателей принадлежит зоне ответственности специалистов по защите информации организации. Также данный анализ могут проводить по средствам экспертной оценки, при этом последнее слова о присвоение значения показателю лежит за старшем специалистом. Присвоение значение компоненту системы проводиться по мере необходимости, при появлении нового компонента в системе, но не реже чем раз в 3 дня.

Вывод

Таким образом, данное исследование предлагает системный подход к оценке эффективности зашиты данных в электронном здравоохранении, включая учет международных и отечественных стандартов, законодательных требований и нормативов.

Предлагается алгоритм оценки, который начинается с сбора информации о системе, ее компонентах и уровне чувствительности информации. Затем производится анализ соответствия мер защиты требованиям законодательства, после чего определяются необходимые меры для обеспечения безопасности данных. Ключевым моментом является расчет показателей эффективности защиты данных (Д), который основывается на уровне чувствительности системы и соответствии реализованных мер защиты законодательным требованиям.

Данная методология представляет собой системный подход к оценке эффективности защиты данных в электронном здравоохранении, который учитывает как технические, так и правовые аспекты защиты информации. Исследование является практическим инструментом для выявления и устранения уязвимостей в системах здравоохранения, что является критически важным в контексте сохранности конфиденциальной медицинской информации. Результаты данного исследования являются важным вкладом в развитие электронного здравоохранения и смежных областей, а также позволяют выявить возможности для оптимизации и совершенствования системы электронного здравоохранения в целом.

Литература

1. Лаборатория Касперского. Кибербезопасность в здравоохранении: где болезнь, где болезнь роста. URL: https://www.kaspersky.ru/blog/healthcare-safeguarding-data/4474/
2. Иванова А.А. Применение big data в сфере здравоохранения: российский и зарубежный опыт // Научные записки молодых исследователей. 2020. № 5.
3. Андриянова Е.А., Гришечкина Н.В. Проблемы формирования системы электронного здравоохранения в России // Здравоохранение Российской Федерации. 2012. № 6. С. 27—30.
4. Административные регламенты по исполнению государственных функций // Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. URL: https://77.rkn.gov.ru/law/ (дата обращения: 30.11.2023).
5. Информатизация здоровья. Менеджмент защиты информации в здравоохранении по ИСО/МЭК 27002.
6. Концепция информационной безопасности в сфере здравоохранения. Утв. протоколом № 7 от 10.03.2022 президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности.
7. Морозов С.П., Владзимирский А.В. Методология и базовые модели организации телерадиологии для службы лучевой диагностики г. Москвы // Журнал телемедицины и электронного здравоохранения. 2017. № 3 (5). С. 137—143.
8. Liddick B.L. Defining HIPAA's Security Rule Within the COVID-19 Telehealth Era: thesis. Utica College, 2021.
9. Moore W., Frye S. Review of HIPAA, Part 1: History, Protected Health Information, and Privacy and Security Rules. Journal of nuclear medicine technology. 2019. Vol. 47. No. 4. Pp. 269–272.
10. A Brief History of Digital Health. URL: https://medium.com/that-medic-network/a-brief-history-of-digital-health-b238f1f5883c (дата обращения: 01.10.2023).
11. Darkins A.W., Cary M.A. Telemedicine and telehealth: principles, policies, performances and pitfalls. Springer publishing company, 2000. 316 pp.
12. Meskó B. et al. Digital health is a cultural transformation of traditional healthcare. Mhealth. 2017. Vol. 3.
13. Reid G.A. Improving HIPAA Compliance Efforts with Modern Cloud Technologies: thesis. Capitol Technology University, 2021.
14. Tebeje T.H., Klein J. Applications of e-health to support person-centered health care at the time of COVID-19 pandemic. Telemedicine and e-Health. 2021. Vol. 27. No. 2. Pp. 150–158.
15. McKeigue P.M. et al. Relation of incident type 1 diabetes to recent COVID-19 infection: cohort study using e-health record linkage in Scotland. Diabetes Care. 2023. Vol. 46. No. 5. Pp. 921–928.
16. Biancone P. et al. E-health for the future. Managerial perspectives using a multiple case study approach. Technovation. 2023. Vol. 120. P. 102406.
17. Hossain N. et al. Factors influencing rural end-users' acceptance of e-health in developing countries: a study on portable health clinic in Bangladesh. Telemedicine and e-Health. 2019. Vol. 25. No. 3. Pp. 221–229.
18. Wynn R. et al. Special issue on e-health services International Journal of Environmental Research and Public Health. 2020. Vol. 17. No. 8. P. 2885.
19. Leung L., Chen C. E-health/m-health adoption and lifestyle improvements: Exploring the roles of technology readiness, the expectation-confirmation model, and health-related information activities. Telecommunications Policy. 2019. Vol. 43. No. 6. Pp. 563–575.

20. Azeez N.A., Van der Vyver C. Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. Egyptian Informatics Journal. 2019. Vol. 20. No. 2. Pp. 97–108.
21. Buyl R. et al. e-Health interventions for healthy aging: a systematic review. Systematic reviews. 2020. Vol. 9. Pp. 1–15.
22. Wind T.R. et al. The COVID-19 pandemic: The 'black swan' for mental health care and a turning point for e-health. Internet interventions. 2020. Vol. 20.
23. Chenthara S. et al. Security and privacy-preserving challenges of e-health solutions in cloud computing. IEEE access. 2019. Vol. 7. Pp. 74361–74382.
24. Vehko T., Ruotsalainen S., Hyppönen H. E-health and e-welfare of Finland: check point 2018. 2019.
25. Tagde P. et al. Blockchain and artificial intelligence technology in e-Health. Environmental Science and Pollution Research. 2021. Vol. 28. Pp. 52810–52831.
26. Sivan R., Zukarnain Z.A. Security and privacy in cloud-based e-health system. Symmetry. 2021. Vol. 13. No. 5. P. 742.
27. Alanezi F. Factors affecting the adoption of e-health system in the Kingdom of Saudi Arabia. International Health. 2021. Vol. 13. No. 5. Pp. 456–470.
28. Scott R.E. Global e-health policy: From concept to strategy. Telehealth in the developing world. CRC Press, 2019. Pp. 55–67.
29. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // СПС «КонсультантПлюс».
30. Постановление Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» // СПС «КонсультантПлюс».
31. ГОСТ Р ИСО 27799-2015. Информатизация здоровья. Менеджмент защиты информации в здравоохранении по ИСО/МЭК 27002: утв. приказом Федерального агентства по техническому регулированию и метрологии от 28 декабря 2015 г. № 2219-ст. Москва, 2016.
32. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СПС «КонсультантПлюс».
33. Методика оценки угроз безопасности информации: утв. ФСТЭК России 05.02.2021 // СПС «КонсультантПлюс».
34. Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Зарегистрировано в Минюсте России 14.05.2013 № 28375 // СПС «КонсультантПлюс».
35. Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 28.05.2019) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». Зарегистрировано в Минюсте России 31.05.2013 № 28608) (с изм. и доп., вступ. в силу с 01.01.2021) // СПС «КонсультантПлюс».
36. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс».
37. Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» // СПС «КонсультантПлюс».
38. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // СПС «КонсультантПлюс».

SECTION:
INFORMATION AND COMPUTER SECURITY

A STUDY OF EFFICIENCY OF DATA PROTECTION IN THE ELECTRONIC HEALTHCARE FIELD

Natal'ia Rzhevskaia, *Assistant Professor at the Department of Computational Mathematics and Cybernetics of the North-Caucasus Federal University, Stavropol, Russian Federation. ORCID: 0009-0002-1285-4196.*
E-mail: natalia070901@gmail.com

Mariia Lapina, *research advisor, Ph.D. (Physics & Mathematics), Associate Professor at the Department of Information Security of Automated Systems of the North-Caucasus Federal University, Stavropol, Russian Federation. ORCID: 0000-0001-8117-9142.*
E-mail: mlapina@ncfu.ru

Mikhail Babenko, *research advisor, Dr.Sc. (Physics & Mathematics), Associate Professor, Head of the Department of Computational Mathematics and Cybernetics of the North-Caucasus Federal University, Stavropol, Russian Federation. ORCID: 0000-0001-7066-0061.*
E-mail: mgbabenko@ncfu.ru

Keywords: *electronic healthcare, data protection, threats, methodology, efficiency, assessment.*

Abstract

Purpose of the study: analysing the current state of the medical information protection system and working out recommendations for improving versatile protection of electronic healthcare.

Methods used in the study: system analysis, classification, the comparative legal method, practical modelling.

Study findings: working out a methodology for assessing efficiency in this field. The developed methodology is a systematic approach to assessing the data protection level in electronic healthcare. It includes analysing vulnerabilities, assessing current protection measures, identifying risks and putting forward specific recommendations for improving information protection. The proposed approach helps not only to determine the level of threats and vulnerabilities but also offers practical steps for their elimination and prevention.

Study novelty: for the first time, a methodology for assessing the efficiency of data protection in electronic healthcare was put forward which would make it possible to make a versatile assessment of protectedness in this field. The results obtained can be used to improve the data security level in electronic healthcare as well as to develop and implement efficient measures for protecting information in this sphere.

References

1. Laboratoriia Kasperskogo. Kiberbezopasnost' v zdravookhranenii: gde bolezn', gde bolezn' rosta. URL: https://www.kaspersky.ru/blog/healthcare-safeguarding-data/4474/
2. Ivanova A.A. Primenenie big data v sfere zdravookhraneniia: rossiiskii i zarubezhnyi opyt. Nauchnye zapiski molodykh issledovatelei. 2020. No. 5.
3. Andriianova E.A., Grishechkina N.V. Problemy formirovaniia sistemy elektronnogo zdravookhraneniia v Rossii. Zdravookhranenie Rossiiskoi Federatsii. 2012. No. 6. Pp. 27–30.
4. Administrativnye reglamenty po ispolneniiu gosudarstvennykh funktsii. Federal'naia sluzhba po nadzoru v sfere sviazi, informatsionnykh tekhnologii i massovykh kommunikatsii. URL: https://77.rkn.gov.ru/law/ (data obrashcheniia: 30.11.2023).
5. Informatizatsiia zdorov'ia. Menedzhment zashchity informatsii v zdravookhranenii po ISO/MEK 27002.
6. Kontseptsiia informatsionnoi bezopasnosti v sfere zdravookhraneniia. Utv. protokolom No. 7 ot 10.03.2022 prezidiuma Pravitel'stvennoi komissii po tsifrovomu razvitiiu, ispol'zovaniiu informatsionnykh tekhnologii dlia uluchsheniia kachestva zhizni i uslovii vedeniia predprinimatel'skoi deiatel'nosti.
7. Morozov S.P., Vladzimirskii A.V. Metodologiia i bazovye modeli organizatsii teleradiologii dlia sluzhby luchevoi diagnostiki g. Moskvy. Zhurnal telemeditsiny i elektronnogo zdravookhraneniia. 2017. No. 3 (5). Pp. 137–143.
8. Liddick B.L. Defining HIPAA's Security Rule Within the COVID-19 Telehealth Era: thesis. Utica College, 2021.
9. Moore W., Frye S. Review of HIPAA, Part 1: History, Protected Health Information, and Privacy and Security Rules. Journal of nuclear medicine technology. 2019. Vol. 47. No. 4. Pp. 269–272.
10. A Brief History of Digital Health. URL: https://medium.com/that-medic-network/a-brief-history-of-digital-health-b238f1f5883c (data obrashcheniia: 01.10.2023).
11. Darkins A.W., Cary M.A. Telemedicine and telehealth: principles, policies, performances and pitfalls. Springer publishing company, 2000. 316 pp.
12. Meskó B. et al. Digital health is a cultural transformation of traditional healthcare. Mhealth. 2017. Vol. 3.
13. Reid G. A. Improving HIPAA Compliance Efforts with Modern Cloud Technologies: thesis. Capitol Technology University, 2021.
14. Tebeje T.H., Klein J. Applications of e-health to support person-centered health care at the time of COVID-19 pandemic. Telemedicine and e-Health. 2021. Vol. 27. No. 2. Pp. 150–158.
15. McKeigue P.M. et al. Relation of incident type 1 diabetes to recent COVID-19 infection: cohort study using e-health record linkage in Scotland. Diabetes Care. 2023. Vol. 46. No. 5. Pp. 921–928.
16. Biancone P. et al. E-health for the future. Managerial perspectives using a multiple case study approach. Technovation. 2023. Vol. 120. P. 102406.
17. Hossain N. et al. Factors influencing rural end-users' acceptance of e-health in developing countries: a study on portable health clinic in Bangladesh. Telemedicine and e-Health. 2019. Vol. 25. No. 3. Pp. 221–229.
18. Wynn R. et al. Special issue on e-health services International Journal of Environmental Research and Public Health. 2020. Vol. 17. No. 8. P. 2885.

19. Leung L., Chen C. E-health/m-health adoption and lifestyle improvements: Exploring the roles of technology readiness, the expectation-confirmation model, and health-related information activities. Telecommunications Policy. 2019. Vol. 43. No. 6. Pp. 563–575.
20. Azeez N.A., Van der Vyver C. Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. Egyptian Informatics Journal. 2019. Vol. 20. No. 2. Pp. 97–108.
21. Buyl R. et al. e-Health interventions for healthy aging: a systematic review. Systematic reviews. 2020. Vol. 9. Pp. 1–15.
22. Wind T. R. et al. The COVID-19 pandemic: The 'black swan' for mental health care and a turning point for e-health. Internet interventions. 2020. Vol. 20.
23. Chenthara S. et al. Security and privacy-preserving challenges of e-health solutions in cloud computing. IEEE access. 2019. Vol. 7. Pp. 74361–74382.
24. Vehko T., Ruotsalainen S., Hyppönen H. E-health and e-welfare of Finland: check point 2018. 2019.
25. Tagde P. et al. Blockchain and artificial intelligence technology in e-Health. Environmental Science and Pollution Research. 2021. Vol. 28. Pp. 52810–52831.
26. Sivan R., Zukarnain Z.A. Security and privacy in cloud-based e-health system. Symmetry. 2021. Vol. 13. No. 5. P. 742.
27. Alanezi F. Factors affecting the adoption of e-health system in the Kingdom of Saudi Arabia. International Health. 2021. Vol. 13. No. 5. Pp. 456–470.
28. Scott R.E. Global e-health policy: From concept to strategy. Telehealth in the developing world. CRC Press, 2019. Pp. 55–67.
29. Federal'nyi zakon ot 26.07.2017 No. 187-FZ "O bezopasnosti kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii". SPS "Konsul'tantPlius".
30. 30. Postanovlenie Pravitel'stva RF ot 8 fevralia 2018 g. No. 127 "Ob utverzhdenii Pravil kategorirovaniia ob"ektov kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii, a takzhe perechnia pokazatelei kriteriev znachimosti ob"ektov kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii i ikh znachenii". SPS "Konsul'tantPlius".
31. GOST R ISO 27799-2015. Informatizatsiia zdorov'ia. Menedzhment zashchity informatsii v zdravookhranenii po ISO/MEK 27002: utv. prikazom Federal'nogo agentstva po tekhnicheskomu regulirovaniiu i metrologii ot 28 dekabria 2015 g. No. 2219-st. Moskva, 2016.
32. Federal'nyi zakon ot 27.07.2006 No. 152-FZ "O personal'nykh dannykh". SPS "Konsul'tantPlius".
33. Metodika otsenki ugroz bezopasnosti informatsii: utv. FSTEK Rossii 05.02.2021. SPS "Konsul'tantPlius".
34. Prikaz FSTEK Rossii ot 18.02.2013 No. 21 (red. ot 14.05.2020) "Ob utverzhdenii Sostava i soderzhaniia organizatsionnykh i tekhnicheskikh mer po obespecheniiu bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh". Zaregistrirovano v Miniuste Rossii 14.05.2013 No. 28375. SPS "Konsul'tantPlius".
35. Prikaz FSTEK Rossii ot 11.02.2013 No. 17 (red. ot 28.05.2019) "Ob utverzhdenii Trebovanii o zashchite informatsii, ne sostavliaiushchei gosudarstvennuiu tainu, soderzhashcheisia v gosudarstvennykh informatsionnykh sistemakh". Zaregistrirovano v Miniuste Rossii 31.05.2013 No. 28608) (s izm. i dop., vstup. v silu s 01.01.2021). SPS "Konsul'tantPlius".
36. Federal'nyi zakon ot 27.07.2006 No. 149-FZ "Ob informatsii, informatsionnykh tekhnologiiakh i o zashchite informatsii". SPS "Konsul'tantPlius".
37. Federal'nyi zakon ot 21.11.2011 No. 323-FZ "Ob osnovakh okhrany zdorov'ia grazhdan v Rossiiskoi Federatsii". SPS "Konsul'tantPlius".
38. Postanovlenie Pravitel'stva RF ot 1 noiabria 2012 g. No. 1119 "Ob utverzhdenii trebovanii k zashchite personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh". SPS "Konsul'tantPlius".