Вестник Физико-технического института
Крымского федерального университета имени В. И. Вернадского
Том 1 (67–69). № 4. 2017. С. 63–88
Journal of Physics and Technology Institute of V. I. Vernadsky Crimean Federal University
Volume 1 (67–69). No. 4. 2017. P. 63–88

УДК 004.056.54; 614.2

ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ДЛЯ ТИПОВОЙ МЕДИЦИНСКОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Григорьев П. Е.[1*], Оленчук А. В.[1], Гольдберг Д. Л.[1], Тишков А. В.[2], Лускова Ю. С.[3]

[1]Физико-технический институт, Крымский федеральный университет имени В.И. Вернадского, Симферополь 295007, Россия
[2]Первый Санкт-Петербургский государственный медицинский университет имени академика И. П. Павлова, Санкт-Петербург 197022, Россия
[3]Медицинская академия имени С. И. Георгиевского, Крымский федеральный университет имени В. И. Вернадского, Симферополь 295007, Россия
****E-mail: grigorievpe@cfuv.ru***

Статья посвящена рассмотрению ключевых этапов проектирования системы безопасности для типовой медицинской информационной системы. Актуализация данного вопроса обусловлена общемировой тенденцией увеличения количества кибератак на информационные системы в сфере здравоохранения за последние годы. Обеспечение необходимого уровня информационной безопасности регулируется нормативно-правовыми документами Правительства Российской Федерации, Федеральной службы безопасности, Федеральной службы по техническому и экспортному контролю, международными и национальными стандартами. Был проанализирован перечень актуальных документов, на основании которого рассмотрены основные аспекты при проектировании системы информационной безопасности. Определены: базовая модель угроз безопасности информации, базовый набор организационных и технических мер защиты информации, а также обоснован оптимальный класс защищенности для типовой медицинской информационной системы. Составлен алгоритм проектирования системы информационной безопасности, который может оказаться полезным для руководителей медицинских организаций, а также администраторов подсистемы безопасности в медицинской информационной системе.

Ключевые слова: информационная безопасность, персональные данные, медицинская информационная система, здравоохранение.

PACS: k 89.20.Ff

ВВЕДЕНИЕ

Процесс информатизации здравоохранения начался в Российской Федерации несколько десятилетий назад. Однако полномасштабное развитие данной отрасли было невозможным в силу ограниченных возможностей вычислительной техники и каналов связи. Начало XXI века ознаменовало новый виток в развитии информатизации здравоохранения в России. Была разработана и утверждена Концепция создания Единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ), с 2011 года начата ее реализация. В ближайшее время уже во всех регионах завершится период «базовой» информатизации здравоохранения, что является необходимым условием для развития Электронного здравоохранения РФ. По мнению экспертов в данной области, «точка невозврата» уже пройдена, и вопрос «быть или не быть информатизации здравоохранения РФ», уже не стоит [1]. Примечательно, что в ежегодном Послании Президента Федеральному Собранию за 2016 год В. В. Путин подчеркнул, что в будущем следует продолжать наращивать уровень информатизации, чтобы сделать удобной и

простой запись на прием, ведение документации. «Нужно освободить врачей от рутины, от заполнения вороха отчётов и справок, дать им больше времени для непосредственной работы с пациентом» [2].

Таким образом, наличие информационных систем (ИС) в каждом медицинском учреждении страны – это неотвратимое будущее, которое необходимо приближать и, к которому, в свою очередь, следует готовиться. Современные информационные системы имеют множество подсистем, отдельное место среди которых занимает подсистема информационной безопасности, выполняя одновременно сквозную и интегральную функцию по отношению ко всему функционалу системе. Однако, зачастую вопросами информационной безопасности в медицинских информационных системах (МИС) пренебрегают или уделяют недостаточное внимание.

Однако в свете постоянного ужесточения законодательства о защите информации и персональных данных (ПДн) [3, 4] актуальность приобретает комплексная проблема обоснования необходимого уровня информационной безопасности в МИС, с конкретными рекомендациями для разработчиков. Задачи данной работы:

- актуализировать проблемы информационной безопасности в сфере здравоохранения;
- описать алгоритм проектирования системы защиты для типовой МИС на основе существующих нормативно правовых актов РФ;
- проанализировать основные аспекты проектирования системы защиты для типовой МИС.

Для решения поставленных задач проанализированы нормативно-правовые акты по защите персональных данных в учреждениях здравоохранения и основные требования регулирующих органов, предъявляемые к аппаратным, программным и организационным средствам по защите персональных данных.

1. СТАТИСТИКА КИБЕРПРЕСТУПЛЕНИЙ В СФЕРЕ ЗДРАВООХРАНЕНИЯ

Информационные технологии, которые широко используются в современной медицине, наряду с преимуществами как для медицинских организаций, так и для пациентов, несут и значительные риски. Связаны они в первую очередь с обеспечением безопасности персональных данных (ПДн). Рассмотрим общемировые тенденции.

Исследование компании IBM [5] показало, что в 2015 году здравоохранение заняло первое место в рейтинге наиболее часто атакуемых отраслей. Пять из восьми самых крупных утечек медицинских данных с 2010 года, когда более миллиона записей были скомпрометированы хакерами, случились в первом полугодии 2015 года. В целом за 2015 год было скомпрометировано более 100 миллионов записей о пациентах. Отмечается, что за пять лет, в период с 2010 по 2015 гг. количество кибератак выросло на 125%. По данным опросов, личная информация о состоянии здоровья на черном рынке считается в 50 раз ценнее финансовой [6].

Согласно опубликованному в мае 2016 года исследованию института Ponemon [7], около 90% медицинских организаций подверглись хотя бы одной хакерской атаке на протяжении последних двух лет, а 45% из них претерпели более пяти атак в тот же период. Устранение последствий от подобных правонарушений обходится мировому здравоохранению в 6,2 млрд. долларов. В 2016 году произошел ряд киберпреступлений в сфере здравоохранения, которые получили широкую огласку. Так, например, в феврале кибератаке подвергся частный медицинский центр Hollywood Presbyterian Medical Center в Лос-Анджелесе (США). В результате атаки произошли неполадки в работе компьютерной сети учреждения, а подавляющее большинство файлов оказалось зашифрованным. Для восстановления информации медицинскому центру пришлось заплатить хакерам выкуп в размере около 17 тыс. долларов [8, 9]. В марте подобной атаке, после которой также пришлось заплатить выкуп, подверглась больница Henderson Methodist в Хендерсоне (США). В результате действий злоумышленников была нарушена работа электронных веб-услуг учреждения [10]. Две больницы, Chinese Valley Medical Center и Desert Valley Hospital, принадлежащие крупному провайдеру медицинских услуг в США (Prime Healthcare Management, Inc.), в марте также были атакованы киберперступниками, однако IT-специалистам удалось отразить действие вредоносного кода [11]. Киберпреступления против медицинских учреждений происходят не только в США. Так, например, по данным международной телерадиокомпании Deutsche Welle, в феврале несколько больниц в Германии пострадали от шифровальщиков, среди них – Lukas Hospital в Нойсе и Klinikum Arnsberg в Северном Рейне-Вестфалии [12]. В мае хакерская организация «Anonymous» провела кибератаку и проникла в систему серверов государственных больниц Турции. Хакеры скопировали базу данных пациентов, после чего удалили ее с серверов. В результате злоумышленникам удалось уничтожить базу данных пациентов 33 государственных госпиталей [13]. В феврале 2017 года информационные ресурсы Министерства здравоохранения Российской Федерации подверглись массированной хакерской атаке, которая в пиковом режиме достигала 4 млн. запросов в минуту. Серьезных последствий удалось избежать. ПДн или данные, составляющие врачебную тайну затронуты не были, поскольку находятся в защищенной части сети, не связанной с интернетом [14].

В целом, исходя из приведенной статистики киберпреступлений в сфере здравоохранения, следует, что спрос злоумышленников на личные медицинские сведения пациентов неуклонно растет. По мнению экспертов компании KPMG [15], особая важность медицинских данных о пациентах, по сравнению с другими персональными данными, объясняется тем, что последствия их утечки сложнее устранить. Более того, многие организации даже не знают, что они подвержены хакерским атакам, и поэтому недооценивают угрозу. Зачастую хакеры проникают в информационные системы организаций и предпочитают оставаться незамеченными до тех пор, пока не извлекут максимальный объем данных. В связи с этим медицинские учреждения, использующие информационные системы для обработки медицинских данных пациентов, обязаны обратить должное внимание на

обеспечение информационной безопасности и обеспечить оптимальный уровень защищенности данных.

2. ОПРЕДЕЛЕНИЕ НЕОБХОДИМОГО УРОВНЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ И КЛАССА ЗАЩИЩЕННОСТИ МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ

В российском законодательстве имеется целый ряд нормативно-правовых документов, регламентирующих обеспечение информационной безопасности ПДн в ИС [16-21].

Система защиты ПДн должна включать в себя организационные и технические меры с учетом актуальных угроз безопасности ПДн и информационных технологий, используемых в ИС. Первоочередным в создании системы защиты ПДн является определение уровня защищенности ПДн. Уровень защищенности ПДн – это комплексный показатель, который характеризует выполнение требований, нейтрализующих угрозы безопасности информационных систем ПДн. В Постановлении Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [22] установлены 4 уровня защищенности ПДн. Необходимый уровень защищенности определяется: категорией обрабатываемых ПДн; видом обработки по форме отношений между субъектами и организацией; количеством субъектов; типом актуальных угроз.

В работе [23] был определен и обоснован необходимый уровень защищенности ПДн, обрабатываемых в медицинских информационных системах (МИС). Типовая МИС, реализующая электронный документооборот, электронную регистратуру и цифровую обработку данных мониторинга состояния пациента, является обработчиком данных специальной категории. Для МИС, субъектами ПДн которой являются менее 100 000 пациентов, достаточно обеспечения третьего уровня защищенности.

После того, как установлен необходимый уровень защищенности ПДн, следует определить класс защищенности ИС. Определение класса защищенности ИС проводится в соответствии с пунктом 14.2 Требований о защите информации, не составляющей государственную тайну, содержащуюся в государственных информационных системах, утвержденных ФСТЭК России от 11 февраля 2013 г. №17.

Устанавливаются четыре класса защищенности ИС (первый класс (К1), второй класс (К2), третий класс (К3), четвертый класс (К4)), определяющие уровни защищенности содержащейся в ней информации. Самый низкий класс – четвертый, самый высокий – первый.

Класс защищенности ИС определяется в зависимости от уровня значимости информации (УЗ), обрабатываемой в этой ИС, и масштаба ИС (федеральный, региональный, объектовый):

$$\text{Класс защищенности (К)} = F\,[\text{УЗ; масштаб системы}]. \quad (1)$$

Уровень значимости информации определяется степенью возможного ущерба для обладателя информации и оператора от нарушения конфиденциальности, целостности или доступности информации:

$$\text{УЗ} = F\,[(\text{конфиденциальность, степень ущерба});\ (\text{целостность, степень ущерба});\ (\text{доступность, степень ущерба})], \quad (2)$$

где степень возможного ущерба определяется обладателем информации и (или) оператором самостоятельно.

Степень возможного ущерба:

- высокая, если в результате нарушения одного из свойств безопасности информации (конфиденциальность, целостность, доступность) возможны существенные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и ИС или оператор не могут выполнять возложенные функции;
- средняя, если в результате нарушения одного из свойств безопасности информации (конфиденциальность, целостность, доступность) возможны умеренные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и ИС или оператор не могут выполнять возложенные функции;
- низкая, если в результате нарушения одного из свойств безопасности информации (конфиденциальность, целостность, доступность) возможны незначительные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и ИС или оператор могут выполнять возложенные функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных средств [24].

Информация имеет:

- высокий уровень значимости (УЗ 1), если хотя бы для одного из свойств безопасности информации (конфиденциальность, целостность, доступность) определена высокая степень ущерба;
- средний уровень значимости (УЗ 2), если хотя бы для одного из свойств безопасности информации (конфиденциальность, целостность, доступность) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба;
- низкий уровень значимости (УЗ 3), если для всех свойств безопасности информации (конфиденциальность, целостность, доступность) определена низкая степень ущерба;
- минимальный уровень значимости (УЗ4), если обладателем информации и (или) оператором степень ущерба от нарушения свойств безопасности информации не может быть определена, но при этом информация подлежит защите в соответствии с законодательством РФ [25].

Масштаб ИС определяется назначением и распределенностью сегментов ИС:

- федеральный масштаб, если она функционирует на территории РФ и имеет сегменты в субъектах РФ;
- региональный масштаб, если она функционирует на территории субъекта РФ и имеет сегменты в одном или нескольких муниципальных образованиях, подведомственных и иных организациях;
- объектовый масштаб, если она функционирует на объектах одного федерального органа государственной власти субъекта РФ и не имеет сегментов в территориальных органах, представительствах, филиалах, подведомственных и иных организациях [24].

Класс защищенности ИС определяется согласно [25] (табл. 1):

Таблица 1. Определение класса защищенности ИС

Уровень значимости информации	Масштаб информационной системы		
	Федеральный	Региональный	Объектовый
УЗ 1	К1	К1	К1
УЗ 2	К1	К2	К2
УЗ 3	К2	К3	К3
УЗ 4	К3	К3	К4

Одновременно с этим, определение класса защищенности ИС осуществляется с учетом требуемого уровня защищенности ПДн. В соответствии с пунктом 27 Требований Приказа ФСТЭК России от 11 февраля 2013 г. № 17, должно быть обеспечено соответствующее соотношение класса защищенности ИС с уровнем защищенности ПДн. В случае, если определенный уровень защищенности ПДн выше чем установленный класс защищенности ИС, то осуществляется повышение класса защищенности в соответствии со следующими требованиями [24]:

- для ИС 1 класса защищенности обеспечивают 1, 2, 3 и 4 уровни защищенности ПДн;
- для ИС 2 класса защищенности обеспечивают 2, 3 и 4 уровни защищенности ПДн;
- для ИС 3 класса защищенности обеспечивают 3 и 4 уровни защищенности ПДн;
- для ИС 4 класса защищенности обеспечивают 4 уровень защищенности ПДн [25].

Таким образом, на этапе определения класса защищенности ИС может возникнуть коллизия. Обусловлена она тем, что между уровнем защищенности ПДн и уровнем значимости информации, очевидно, должна существовать связь. Однако, в рассмотренных нормативно-правовых документах, соответствие между этими двумя параметрами однозначно не определено. С одной стороны, класс защищенности ИС определяется уровнем значимости информации и масштабом ИС, а с другой стороны – должен обеспечивать соответствующие уровни защищенности ПДн. Рассмотрим эту проблему на примере МИС. Ранее был определен и обоснован необходимый уровень защищенности ПДн в МИС [23] – для

реализации защиты ПДн МИС, субъектами которой являются менее 100 000 пациентов, достаточно обеспечить 3 уровень защищенности. Из соотношения класса защищенности ИС с уровнем защищенности ПДн видно, что подобной МИС должен быть присвоен 3 класс защищенности ИС – К3.

В то же время, определяя класс защищенности ИС с использованием показателей УЗ информации и масштаба ИС, можно получить иной класс. Большинству МИС, внедряемых в конкретную медицинскую организацию, можно присвоить объектовый масштаб. Если хотя бы одному из свойств информации (конфиденциальность, целостность, доступность) в МИС присвоить среднюю степень возможного ущерба, то информации будет присвоен УЗ 2. А данное сочетание масштаба ИС (объектовый) и уровня значимости информации (УЗ 2) соответствует 2 классу защищенности ИС – К2. Иными словами, установленный ранее уровень защищенности ПДн для МИС обеспечивается ИС с классом защищенности К3, но одновременно с тем, расчетное значение по показателям УЗ и масштаб может указывать на необходимость использования ИС с классом защищенности К2. К сожалению, в рассмотренных документах не указано, чем следует руководствоваться в подобных случаях. Какой из параметров: уровень защищенности ПДн, либо уровень значимости информации, является приоритетным в выборе класса защищенности ИС? Есть ли между ними однозначное соответствие? Вопросы эти остаются открытыми и требуют особого внимания, поскольку класс защищенности ИС определяет перечень необходимых для обеспечения информационной безопасности организационных и технических мер, выполнение которых может сопровождаться значительными финансовыми издержками.

Исходя из трудностей с финансированием у многих медицинских организаций, дополнительные финансовые издержки, связанные с обеспечением информационной безопасности ИС, могут оказаться критическими. Поэтому, руководствуясь документом [24], в котором указано, что уровень защищенности определяет оператор самостоятельно, важно обосновать наиболее оптимальный класс защищенности ИС для типичной МИС, которым, с нашей точки зрения, является третий класс защищенности ИС – К3.

3. ВЫБОР МЕР ЗАЩИТЫ ИНФОРМАЦИИ В МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Выбор мер защиты информации осуществляется исходя из класса защищенности ИС, угроз безопасности информации (УБИ), включенных в модель угроз, а также с учетом структурно-функциональных характеристик ИС.

Меры защиты информации в ИС должны быть направлены на обеспечение:

- конфиденциальности информации (исключение ее неправомерного доступа, копирования, предоставления и распространения);
- целостности информации (исключение ее неправомерного уничтожения или модифицирования);
- доступности информации (исключение ее неправомерного блокирования) [24].

Меры защиты информации, выбираемые для реализации в ИС, должны обеспечивать блокирование одной или нескольких УБИ, включенных в модель угроз безопасности информации.

Состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИС определяется:

- приказом ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении Требований по защите информации, не составляющих государственную тайну, содержащейся в государственных информационных системах»;
- приказом ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- приказом ФСБ России от 10.07.2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

Из анализа вышеперечисленных документов следует, что в ИС третьего класса защищенности должны быть реализованы технические меры с применением:

- средств вычислительной техники не ниже пятого класса;
- системы обнаружения вторжений и средства антивирусной защиты не ниже четвертого класса в случае взаимодействия ИС с информационно-телекоммуникационными сетями международного информационного обмена;
- межсетевых экранов не ниже третьего класса в случае взаимодействия ИС с информационно-телекоммуникационными сетями международного информационного обмена [25].

Под средствами вычислительной техники понимается совокупность программных и технических элементов системы обработки данных, способных функционировать самостоятельно или в составе других систем. Классификация средств вычислительной техники по уровню защищенности от несанкционированного доступа установлена руководящим документом «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», утвержденным Государственной технической комиссией (ныне ФСТЭК) при Президенте РФ от 30 марта 1992 г. [26].

Выбор организационных мер защиты информации для их реализации в ИС включает (рис. 1):

- определение базового набора мер защиты информации для установленного класса защищенности ИС;
- адаптацию базового набора мер защиты информации для установленного класса защищенности ИС;

- уточнение адаптированного базового набора мер защиты информации с учетом не выбранных ранее мер защиты информации для нейтрализации УБИ, включенных в модель угроз безопасности;
- дополнение уточненного адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативно-правовыми актами в области защиты информации.

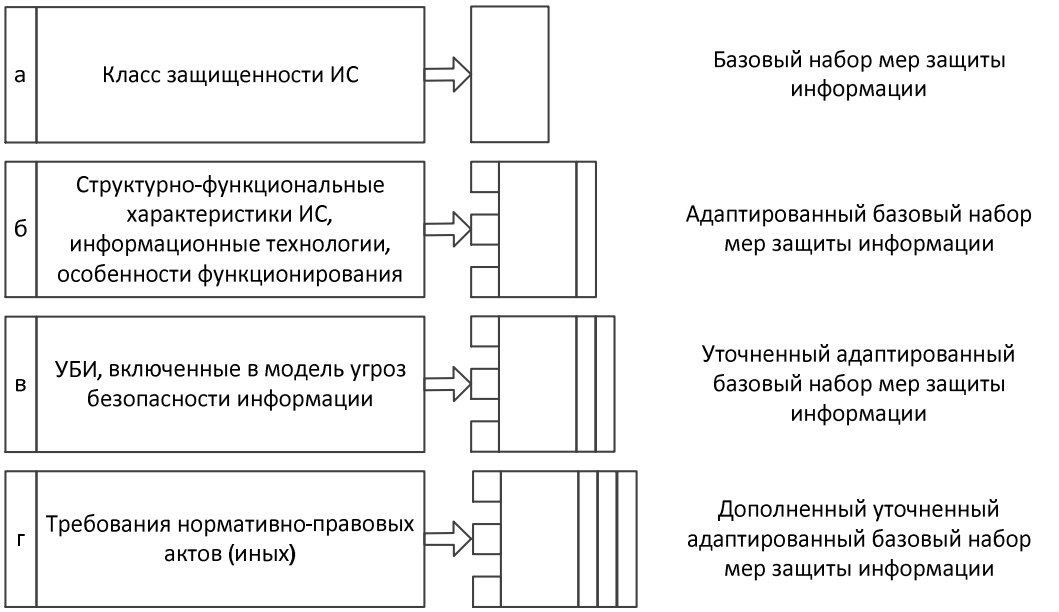

Рис. 1. Общий порядок действий по выбору мер защиты информации для их реализации в ИС

Определение базового набора мер защиты информации является первым шагом в выборе мер защиты информации, подлежащих реализации в ИС, и основывается на классе защищенности ИС [24].

Для типовой МИС был определен третий класс защищенности ИС, поэтому, руководствуясь методическим документом «Меры защиты информации в государственных информационных системах», должны быть обеспечены следующие базовые меры защиты информации.

I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ):

ИАФ.1. Идентификация и аутентификация пользователей, являющихся работниками оператора.

ИАФ.3. Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов. Требования к усилению: 1) оператором должно быть исключено повторное использование идентификатора пользователя в течение периода более года; 2) оператором должно быть обеспечено блокирование

идентификатора пользователя через период времени не более 90 дней неиспользования.

ИАФ.4. Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации. Требования к усилению: в случае использования в ИС механизмов аутентификации на основе пароля или применения пароля в качестве одного из факторов многофакторной аутентификации, его характеристики должны быть следующими: длина пароля не менее шести символов, алфавит пароля не менее 60 символов, максимальное количество неуспешных попыток аутентификации до блокировки от 3 до 10 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 5 до 30 минут, смена паролей не более чем через 120 дней.

ИАФ.5. Защита обратной связи при вводе аутентификационной информации.

ИАФ.6. Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей).

II. Управление доступом субъектов доступа к объектам доступа (УПД):

УПД.1. Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей. Требования к усилению: 1) оператором должны использоваться автоматизированные средства поддержки управления учетными записями; 2) в ИС должно осуществляться автоматическое блокирование временных учетных записей пользователей по окончании установленного периода времени для их использования.

УПД.2. Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа. Требования к усилению: 1) в ИС правила разграничения доступа должны обеспечивать управление доступом субъектов при входе в ИС; 2) в ИС правила разграничения доступа должны обеспечивать управление доступом субъектов к техническим средства, устройствам, внешним устройствам; 3) в ИС правила разграничения доступа должны обеспечивать управление доступом субъектов к объектам, создаваемым общесистемным программным обеспечением.

УПД.4. Разделение обязанностей полномочий (ролей), администраторов и лиц, обеспечивающих функционирование ИС.

УПД.5. Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС.

УПД.6. Ограничение неуспешных попыток входа в ИС.

УПД.10. Блокирование сеанса доступа в ИС после установленного времени бездействия (неактивности) пользователя или по его запросу.

УПД.11. Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации.

УПД.13. Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети. Требования к усилению: 1) в ИС используется ограниченное (минимально необходимое) количество точек подключения к ИС при организации удаленного доступа к объектам доступа ИС; 2) в ИС исключается удаленный доступ от имени привилегированных учетных записей (администраторов) для администрирования ИС и ее системы защиты информации.

УПД.14. Регламентация и контроль использования в ИС технологий беспроводного доступа. Требования к усилению: идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных.

УПД.15. Регламентация и контроль использования в ИС мобильных технических средств.

УПД.16. Управление взаимодействием с ИС сторонних организаций. Требования к усилению: оператор предоставляет доступ к ИС авторизованным (уполномоченным) пользователям внешних ИС или разрешает обработку, хранение и передачу информации с использованием внешней ИС при выполнении следующих условий: 1) при наличии договора (соглашения) об информационном взаимодействии с оператором внешней ИС; 2) при наличии подтверждения выполнения во внешней ИС предъявленных к ней требований о защите информации (наличие аттестата соответствия требованиям по безопасности информации или иного подтверждения).

III. Ограничение программной среды (ОПС):

ОПС.3. Установка (инсталляция) только разрешенного к использованию программного обеспечения и его компонентов.

IV. Защита машинных носителей информации (ЗНИ):

ЗНИ.1. Учет машинных носителей информации.

ЗНИ.2. Управление доступом к машинным носителям информации.

ЗНИ.8. Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания). Требования к усилению: 1) оператором должны быть обеспечены регистрация и контроль действий по удалению защищаемой информации и уничтожению машинных носителей информации; 2) оператором должны применяться следующие меры по уничтожению (стиранию) информации на машинных носителях, исключающие возможность восстановления защищаемой информации: перезапись уничтожаемых (стираемых) файлов случайной битовой последовательностью, удаление записи о файлах, обнуление журнала файловой системы и полная перезапись всего адресного пространства машинного носителя информации случайной битовой последовательностью с последующим форматированием.

V. Регистрация событий безопасности (РСБ):

РСБ.1. Определение событий безопасности, подлежащих регистрации, и сроков их хранения.

РСБ.2. Определение состава и содержания информации о событиях безопасности, подлежащих регистрации.

РСБ.3. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения.

РСБ.4. Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти.

РСБ.5. Мониторинг (просмотр, анализ) результатов регистрации событий.

РСБ.6. Генерирование временных меток и (или) синхронизация системного времени в ИС.

РСБ.7. Защита информации о событиях безопасности.

VI. Антивирусная защита (АВЗ):

АВЗ.1. Реализация антивирусной защиты. Требования к усилению: в ИС должно обеспечиваться предоставление прав по управлению (администрированию) средствами антивирусной защиты администратору безопасности.

АВЗ.2. Обновление базы данных признаков вредоносных компьютерных программ (вирусов).

VII. Контроль (анализ) защищенности информации (АНЗ):

АНЗ.1. Выявление, анализ уязвимостей ИС и оперативное устранение вновь выявленных уязвимостей. Требования к усилению: 1) оператором обеспечивается использование для выявления (поиска) уязвимостей средств анализа (контроля) защищенности (сканеров безопасности), имеющих стандартизованные (унифицированные) в соответствии с национальными стандартами описание и перечни программно-аппаратных платформ, уязвимостей, проверочных списков, процедур тестирования и языка тестирования ИС на наличие уязвимостей, оценки последствий уязвимостей, имеющих возможность оперативного обновления базы данных выявляемых уязвимостей; 2) оператором предоставляется доступ только администраторам к функциям выявления (поиска) уязвимостей (предоставление такой возможности только администраторам безопасности).

АНЗ.2. Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.

АНЗ.3. Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации.

АНЗ.4. Контроль состава технических средств, программного обеспечения и средств защиты информации.

АНЗ.5. Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИС.

IX. Обеспечение целостности информационной системы и информации (ОЦЛ):

ОЦЛ.3. Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций.

XI. Защита среды виртуализации (ЗСВ):

ЗСВ.1. Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации.

ЗСВ.2. Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин. Требования к усилению: 1) в ИС должен обеспечиваться доступ к операциям, выполняемым с помощью средств управления виртуальными машинами, в том числе к операциям создания, запуска, останова, создания копий, удаления виртуальных машин, который должен быть разрешен только администраторам виртуальной инфраструктуры; 2) в ИС должен обеспечиваться доступ к конфигурации виртуальных машин только администраторам виртуальной инфраструктуры.

ЗСВ.3. Регистрация событий безопасности в виртуальной инфраструктуре.

ЗСВ.9. Реализация и управление антивирусной защитой в виртуальной инфраструктуре.

XII. Защита технических средств (ЗТС):

ЗТС.2. Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования.

ЗТС.3. Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования ИС и помещения и сооружения, в которых они установлены.

ЗТС.4. Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.

XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС):

ЗИС.3. Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи.

ЗИС.5. Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств.

ЗИС.20. Защита беспроводных соединений, применяемых в ИС.

ЗИС.30. Защита мобильных технических средств, применяемых в ИС [24].

После того, как определен базовый набор мер защиты информации, следует этап адаптации базового набора. На этом этапе учитываются структурно-функциональные характеристики конкретной ИС, применяемые информационные технологии, особенности функционирования ИС. В частности, адаптация базового набора мер защиты информации предусматривает исключение мер, непосредственно связанных с информационными технологиями, не используемыми в ИС. Так, в случае, если в ИС не применяются технологии виртуализации, то меры по защите среды виртуализации следует исключить. В данном контексте «виртуализация» – это технология преобразования формата или параметров программных либо сетевых запросов к компьютерным ресурсам с целью

обеспечения независимости процессов обработки информации от программной или аппаратной платформы ИС.

На следующем этапе проектирования системы информационной безопасности выполняется уточнение адаптированного базового набора мер защиты информации с учетом возможности адекватно блокировать все УБИ, включенные в модель угроз безопасности информации, или же снизить вероятность их реализации. В качестве исходных данных выбирается перечень УБИ и их характеристики (потенциал, оснащенность, мотивация), включенные в модель угроз безопасности. Затем каждой УБИ сопоставляется мера защиты информации (из адаптированного базового набора мер защиты информации), которая обеспечивает блокирование или снижает вероятность ее реализации. В том случае, если адаптированный базовый набор мер защиты информации не обеспечивает блокирование всех угроз безопасности, в него дополнительно включаются меры защиты информации, не указанные ранее.

Дополнение уточненного адаптированного базового набора мер защиты информации осуществляется в случае предъявления дополнительных требований к защите информации в ИС, не указанных в вышеперечисленных нормативных актах. В случае, если сформированный набор мер защиты информации содержит меры защиты информации, которые невозможно или затруднительно реализовать в силу каких-либо причин (высокая стоимость, большие сроки реализации и другие), должны быть реализованы компенсирующие меры защиты. Исходные данные для разработки компенсирующих мер защиты информации следует выбирать в первую очередь из требований о защите информации [25], методического документа ФСТЭК по мерам защиты [24], международных и национальных стандартов, стандартов организаций в области информационной безопасности. Кроме этого, в качестве компенсирующих мер защиты информации могут быть использованы результаты собственных научно-исследовательских и опытно-конструкторских работ. При этом использование компенсирующих мер защиты должно быть обосновано и аргументировано [24].

На этапе уточнения адаптированного базового набора мер защиты информации используется модель угроз безопасности, которая составляется на основании методического документа «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» [27].

4. СОСТАВЛЕНИЕ МОДЕЛИ УГРОЗ И ВЫБОР АКТУАЛЬНЫХ УГРОЗ

В зависимости от технологий, состава и характеристик технических средств ИС ПДн, а также опасности реализации угроз безопасности ПДн и наступления последствий в результате несанкционированного или случайного доступа выделяют следующие типы ИС ПДн:

- автоматизированные рабочие места, не подключенные к сетям общего пользования и международного информационного обмена;
- автоматизированные рабочие места, подключенные к сетям общего пользования и международного информационного обмена;

- локальные ИС ПДн, не имеющие подключение к сетям связи общего пользования и международного информационного обмена;
- локальные ИС ПДн, имеющие подключение к сетям связи общего пользования и сетям международного информационного обмена;
- распределенные ИС ПДн, не подключенные к сетям связи общего пользования и сетям международного информационного обмена;
- распределенные ИС ПДн, подключенные к сетям связи общего пользования и сетям международного информационного обмена.

Для каждого типа ИС ПДн из представленных выше разработана типовая модель угроз безопасности ПДн, которая может быть дополнена, исходя из структурно-функциональных характеристик конкретной ИС.

Исходя из структуры медицинских организаций и внедряемых в них МИС, можно сделать вывод, что наибольшее распространение получили локальные ИС ПДн, имеющие подключение к сетям связи общего пользования и сетям международного информационного обмена. Согласно типовой модели угроз для данной ИС ПДн возможна реализация следующих угроз безопасности ПДн:

- угрозы утечки информации по техническим каналам;
- угрозы несанкционированного доступа к ПДн, обрабатываемым на автоматизированном рабочем месте.

Угрозы утечки информации по техническим каналам включают в себя: угрозы утечки акустической (речевой) информации, угрозы утечки видовой (графической, видео- и буквенно-цифровой) информации, угрозы утечки информации по каналу побочных электромагнитных излучений и наводок.

Угрозы несанкционированного доступа связаны с действиями нарушителей, реализующих угрозы непосредственно в ИСПДн, в том числе, при помощи аппаратных закладок и отчуждаемых носителей вредоносных программ, а также нарушителей, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и сетей международного информационного обмена.

Угрозы из внешних сетей включают:

- угрозы «Анализа сетевого трафика» с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации;
- угрозы сканирования, направленные на выявление типа операционной системы ИСПДн, сетевых адресов рабочих станций, открытых портов и служб, открытых соединений и др.;
- угрозы выявления паролей;
- угрозы получения несанкционированного доступа путем подмены доверенного объекта;
- угрозы типа «Отказ в обслуживании»;
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ.

С целью адаптации модели угроз под конкретную МИС, важной задачей является определение актуальных угроз безопасности.

УБИ определяются по результатам оценки возможностей внешних и внутренних нарушителей, анализа возможных уязвимостей ИС, возможных

способов реализации УБИ и последствий от нарушения свойств безопасности информации. Эффективность принимаемых мер защиты информации в ИС зависит от качества определениям УБИ для конкретной ИС в конкретных условиях ее функционирования. Поэтому для ИС разрабатывается модель угроз, которая представляет собой формализованное описание УБИ [24]. Актуальной считается угроза, которая может быть реализована в ИС ПДн и представляет опасность для ПДн. Для оценки возможности реализации угрозы применяются два показателя: уровень исходной защищенности ИС ПДн и частота (вероятность) реализации рассматриваемой угрозы.

Под уровнем исходной защищенности ИС ПДн понимается обобщенный показатель, зависящий от следующих технических и эксплуатационных характеристик:

- территориальное размещение;
- наличие соединения с сетями общего пользования;
- встроенные операции с записями баз ПДн;
- разграничение доступа к ПДн;
- наличие соединения с другими базами ПДн иных ИС ПДн;
- уровень обезличивания ПДн;
- объем ПДн, предоставляются сторонним пользователям ИСПДн без предварительной обработки [27].

Исходная степень защищенности определяется по методике, указанной в документе «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» и может иметь несколько уровней исходной защищенности. Причем каждому уровню ставится в соответствие числовой коэффициент Y_1:

- $Y_1 = 0$, если присвоен высокий уровень исходной защищенности;
- $Y_1 = 5$, если присвоен средний уровень исходной защищенности;
- $Y_1 = 10$, если присвоен низкий уровень исходной защищенности.

Частота (вероятность) реализации угрозы определяется экспертным путем, также имеет градацию, и ей в соответствие ставится числовой коэффициент Y_2:

- $Y_2 = 0$, для маловероятной угрозы, когда отсутствуют объективные предпосылки для осуществления угрозы;
- $Y_2 = 2$, для низкой вероятности угрозы, когда объективные предпосылки для осуществления угрозы существуют, но принятые меры существенно затрудняют ее реализацию;
- $Y_2 = 5$, для средней вероятности угрозы, когда объективные предпосылки для осуществления угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;

- $Y_2 = 10$, для высокой вероятности угрозы, когда объективные предпосылки для осуществления угрозы существуют и меры по обеспечению безопасности ПДн не приняты.

С учетом изложенного коэффициент реализуемости угрозы Y будет определяться следующим соотношением:

$$Y = (Y_1 + Y_2) / 20 \quad (3)$$

Интерпретация реализуемости угрозы проводится так:

- при $0 \le Y \le 0,3$ возможность реализации угрозы низкая;
- при $0,3 \le Y \le 0,6$ – средняя;
- при $0,6 \le Y \le 0,8$ – высокая;
- при $Y > 0,8$ – очень высокая [28].

Далее на основе экспертной оценки определяется уровень опасности каждой угрозы. Оценка выполняется с использованием Общей системы оценки уязвимостей (Common Vulnerability Scoring System – CVSS) [29]. В настоящее время наибольшее распространение в практической деятельности по оценке опасности уязвимостей получила версия 2.0 общей системы оценки уязвимостей, хотя существует и более новая версия 3.0. Система оценки CVSS v 2.0 состоит из трех групп метрик (критериев): базовых, временных и контекстных. На основании этих метрик строятся векторы уязвимости. Группа базовых метрик (критериев) отражает аспекты опасности уязвимости, влияющие на доступность, целостность и конфиденциальность информации. Группа временных метрик (критериев) отражает характеристики уязвимости, которые изменяются со временем (подтверждение технических параметров уязвимости, статус исправления уязвимости и доступность технологии эксплуатации), но не зависят от среды функционирования программного обеспечения. Группа контекстных метрик (критериев) отражает характеристики уязвимости, зависящие от среды функционирования программного обеспечения.

Количественная оценка степени опасности уязвимости проводится по результатам анализа базового вектора уязвимости. Временные и контекстные векторы применяются только в тех случаях, когда возникает необходимость уточнения базового вектора.

Численное значение базового вектора уязвимости (базовая оценка) может варьироваться в пределах от 0 до 10.

На основе численного значения базового вектора *V* уязвимости (базовой оценки) присваиваются один из четырех уровней опасности:

- при $0,0 \le V \le 3,9$ присваивается низкий уровень опасности, реализация угрозы может привести к незначительным негативным последствиям для субъектов ПДн;
- при $4,0 \le V \le 6,9$ присваивается средний уровень опасности, реализация угрозы может привести к негативным последствиям для субъектов ПДн;

- при $7,0 \le V \le 9,9$ присваивается высокий уровень опасности, реализация угрозы может привести к значительным негативным последствиям для субъектов ПДн;
- при $V = 10,0$ присваивается критический уровень опасности, реализация угрозы может привести к критическим негативным последствиям для субъектов ПДн.

Более подробную информацию о расчете численного значения базового вектора *V* можно найти на официальном сайте ФСТЭК [30].

После выполнения всех вышеописанных операций, определяется перечень актуальных угроз [28] (табл. 2):

Таблица 2. Определение актуальности угрозы

Возможность реализации угрозы	Уровень опасности угрозы		
	Низкий	Средний	Высокий (Критический)
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Таким образом, для конкретной МИС разрабатывается модель угроз, с учетом ее структурно-функциональных характеристик, применяемых информационных технологий и особенностей функционирования. Исходя из вышесказанного, построен алгоритм проектирования системы защиты для типовой МИС (рис. 2).

Пунктирная стрелка на рис. 2 между этапами определения уровня защищенности ПДн и уровня значимости информации сигнализирует о наличии между ними связи, не до конца определенной в имеющихся нормативно-правовых документах.

Следует также отметить, что в процессе классификации для снижения затрат на средства защиты ПДн и оптимизации работы подсистемы безопасности ИС можно провести логическую и (или) физическую сегментацию ИС ПДн. Таким образом, в зависимости от характеристик обрабатываемой информации конкретному сегменту ИС присваивается свой класс защищенности.

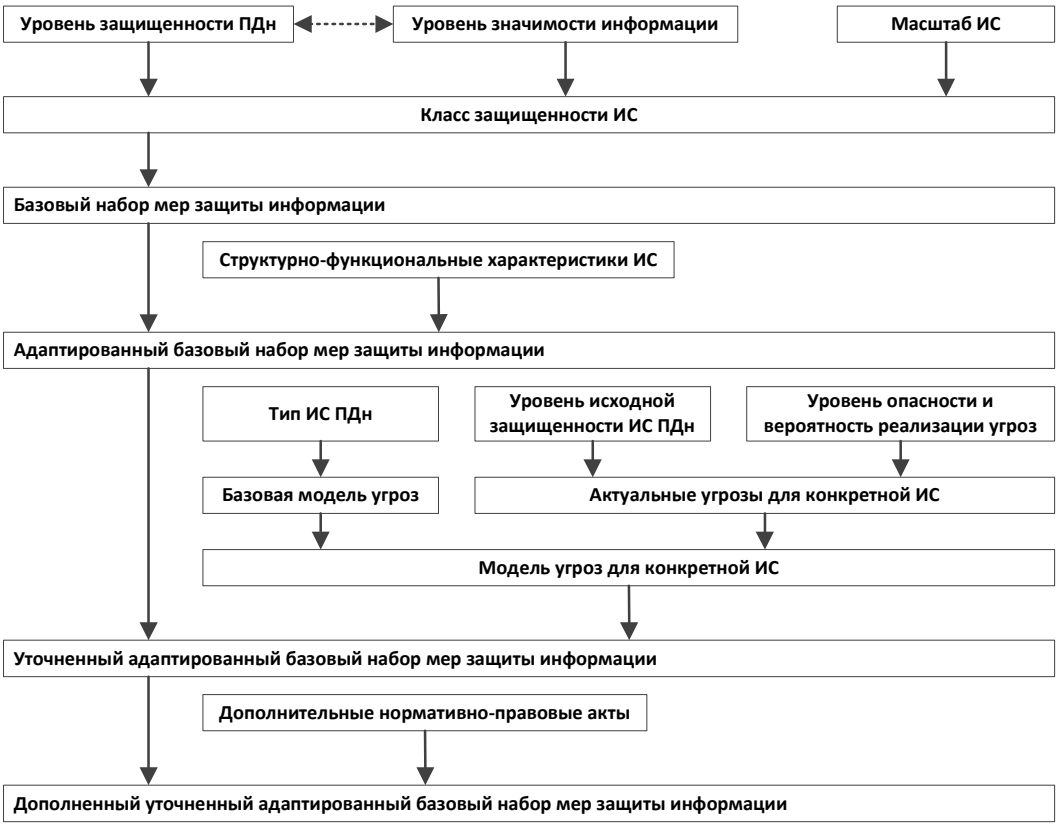

Рис. 2. Алгоритм проектирования системы защиты для типовой МИС

При составлении алгоритма проектирования системы защиты для типовой МИС нельзя обойти вниманием такие документы, как «Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости» [31] и «Методические рекомендации по составлению Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений здравоохранения, социальной сферы, труда и занятости» [32]. Обусловлено это тем, что указанные методические рекомендации разъясняют многие аспекты по интерпретации Федерального закона от 27.07.2006 N 152-ФЗ о персональных данных [33] относительно МИС. Они содержат в себе описание конкретных шагов при разработке и внедрении подсистемы безопасности МИС, что, безусловно, будет полезным для руководителей медицинских организаций и администраторов системы. В то же время, понимая их значимость и важность, по ряду причин авторы статьи намеренно не акцентируют внимание на этих двух документах.

Во-первых, авторы статьи старались абстрагироваться от описания решений для конкретных МИС. Основной направленностью исследования являлось

освещение общих этапов проектирования и задание своего рода «дорожной карты» при разработке подсистемы информационной безопасности, вне зависимости от индивидуальных особенностей, имеющихся в тех или иных медицинских организациях. В связи с этим мы намеренно избегали избыточной детализации при описании ключевых этапов проектирования подсистемы информационной безопасности, сохраняя логическую дистанцию и не преступая границу между обобщенными рекомендациями и кейсовым решением. Поэтому разработка кейсовых решений – отдельный вид деятельности, который не вписывается в рамки данной статьи.

Во-вторых, упомянутые методические рекомендации [31, 32] являются вторичными текстами, которые ссылаются, в том числе, на первичные документы [27, 28, 33], проанализированные в статье.

В-третьих, часть информации, представленной в данных рекомендациях, является устаревшей и не актуальной. Обусловлено это тем, что в них не учитываются изменения и поправки, которые произошли в нормативно-правовой документации, после издания рекомендаций. К примеру, в указанных методических рекомендациях предлагается проводить классификацию ИС ПДн согласно Приказу ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 N 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных», который на сегодняшний день отменен и признан утратившим силу. Другой пример, в этих методических рекомендациях порой используют термины, которые не являются официально признанными и которые нельзя использовать при формировании официальных документов. Данные примеры свидетельствуют о том, что неумелое использование упомянутых методических рекомендаций может привести к негативным последствиям для медицинской организации, внедряющей у себя подсистему информационной безопасности.

ЗАКЛЮЧЕНИЕ

Вопросу информационной безопасности в МИС следует уделять пристальное внимание, что связано с участившимися случаями киберпреступлений в сфере здравоохранения. В статье описаны основные этапы проектирования системы защиты ПДн в типовой МИС. В частности, обоснован оптимальный класс защищенности ИС, исходя из которого перечислены базовые технические и организационные меры защиты информации. Выбрана оптимальная типовая модель угроз для МИС и указаны рекомендации к определению актуальных угроз.

Проведенный в статье анализ зиждется на нормативно-правовых актах в области защиты ПДн. Рекомендации, изложенные в статье, могут быть полезны для руководителей медицинских организаций в качестве отправной точки при проектировании системы безопасности в ИС и конкретизации требований к разработчикам МИС.

Список литературы

1. Зарубина Т. В. // Сибирский вестник медицинской информатики и информатизации здравоохранения. 2016. №1. С. 6–11.
2. Послание Президента Федеральному Собранию [электронный ресурс] URL : http://kremlin.ru/events/president/news/53379 (дата обращения : 23.11.2017).
3. О внесении изменений в Кодекс Российской Федерации об административных правонарушениях [электронный ресурс] URL : http://kremlin.ru/acts/news/53836 (дата обращения : 23.11.2017).
4. Путин подписал закон о персональных данных [электронный ресурс] URL : https://ria.ru/society/20170207/1487378476.html (дата обращения : 23.11.2017).
5. Reviewing a year of serious data breaches, major attacks and new vulnerabilities. Analysis of cyber attack and incident from IBM's worldwide security services operations [электронный ресурс] URL : http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03133USEN&attachment=SEW03133USEN.PDF (дата обращения : 25.11.2017).
6. Healthcare underspends on cybersecurity as attacks accelerate [электронный ресурс] URL : http://www.modernhealthcare.com/article/20160303/NEWS/160309922/healthcare-underspends-on-cybersecurity-as-attacks-accelerate (дата обращения : 25.02.2017).
7. Sixth annual benchmark study on privacy & security of healthcare data. Ponemon Institute LLC. 2016. 50 с. [электронный ресурс] URL : https://media.scmagazine.com/documents/232/sixth_annual_benchmark_study_o_57783.pdf (дата обращения : 11.09.2017).
8. Клиника выплатила выкуп хакерам: киберпреступность в медицине [электронный ресурс] URL : https://www.health-ua.org/news/21266.html (дата обращения : 13.08.2017).
9. Булович С. Кибербезопасность информационных систем. Подход “Лаборатории Касперского” [электронный ресурс] URL : http://compaslidera.ru/files/documents/Dopmaterial/ZPD-19042016/Kaspersky.pdf (дата обращения : 11.10.2017).
10. Backup And Recovery System Allows Methodist Hospital To Regain Control After Ransomware Attack. Health IT Outcomes [электронный ресурс] URL : https://www.healthitoutcomes.com/doc/backup-recovery-system-control-ransomware-attack-0001 (дата обращения : 14.11.2017).
11. Two more healthcare networks caught up in outbreak of hospital ransomware [электронный ресурс] URL : https://arstechnica.com/security/2016/03/two-more-healthcare-networks-caught-up-in-outbreak-of-hospital-ransomware/ (дата обращения : 23.09.2017).
12. Hackers hold German hospital data hostage [электронный ресурс] URL : http://www.dw.com/en/hackers-hold-german-hospital-data-hostage/a-19076030 (дата обращения : 23.09.2017).
13. Хакеры Anonymous атаковали больничную систему Турции [электронный ресурс] URL : http://newsturk.ru/2016/05/18/hakeryi-anonymous-atakovali-bolnichnuyu-sistemu-turtsii/ (дата обращения : 23.02.2017).
14. Технические службы Минздрава России отразили самую масштабную за последние годы хакерскую атаку [электронный ресурс] URL : https://www.rosminzdrav.ru/news/2017/02/11/5085-tehnicheskie-sluzhby-minzdrava-rossii-otrazili-samuyu-masshtabnuyu-za-poslednie-gody-hakerskuyu-ataku (дата обращения : 14.11.2017).
15. Health care and cyber security : increasing threats require increased capabilities [электронный ресурс] URL : https://assets.kpmg.com/content/dam/kpmg/pdf/2015/09/cyber-health-care-survey-kpmg-2015.pdf (дата обращения : 14.08.2017).
16. Указ Президента Российской Федерации от 06 марта 1997 № 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера».
17. Указ Президента Российской Федерации от 17 марта 2008 № 351 (ред. от 22.05.2015) «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
18. Постановление Правительства Российской Федерации от 06 июля 2008 N 512 (ред. от 27.12.2012) «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

19. Постановление Правительства Российской Федерации от 06 июля 2008 N 512 (ред. от 27.12.2012) «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
20. Постановление Правительства Российской Федерации от 06 июля 2008 N 512 (ред. от 27.12.2012) «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
21. Приказ Роскомнадзора от 30 мая 2017 года № 94 «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения».
22. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
23. Гольдберг Д. Л., Григорьев П. Е., Оленчук А. В. // Биотехносфера. 2016. № 2 (44). С. 12–16.
24. Методический документ. Меры защиты информации в государственных информационных системах: утв. ФСТЭК России от 11 февраля 2014 г. [электронный ресурс] URL : http://bdu.fstec.ru/documents/24 (дата обращения : 15.09.2017).
25. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: утв. приказом ФСТЭК России от 11 февраля 2013 г. № 17. 2013. [электронный ресурс] URL : http://bdu.fstec.ru/documents/21 (дата обращения : 18.10.2017).
26. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации: утв. решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [электронный ресурс] URL : http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/385-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g2 (дата обращения : 18.10.2017).
27. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка): утв. заместителем директора ФСТЭК России от 15 февраля 2008 г. [электронный ресурс] URL : http://bdu.fstec.ru/documents/16 (дата обращения : 20.10.2017).
28. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах: утв. заместителем директора ФСТЭК России от 14 февраля 2008 г. [электронный ресурс] URL : http://bdu.fstec.ru/documents/18 (дата обращения : 14.09.2017).
29. Официальный сайт некоммерческой организации FIRST [электронный ресурс] URL : https://www.first.org/cvss/v2 (дата обращения : 23.02.2017).
30. Банк данных угроз безопасности информации ФСТЭК России [электронный ресурс] URL : http://bdu.fstec.ru/cvss2 (дата обращения : 23.02.2017).
31. Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости: согласовано с начальником 2 управления ФСТЭК от 22 декабря 2009 г., утверждено директором Департамента информатизации Министерства здравоохранения и социального развития Российской Федерации от 23 декабря 2009 г. М. : Министерство здравоохранения и социального развития, 2009. 94 с.
32. Методические рекомендации по составлению Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений здравоохранения, социальной сферы, труда и занятости: согласовано с начальником 2 управления ФСТЭК от 22 декабря 2009 г., утверждено директором Департамента информатизации Министерства здравоохранения и социального развития Российской Федерации от 23 декабря 2009 г. М. : Министерство здравоохранения и социального развития, 2009. 215 с.
33. Федеральный закон от 27.07.2006 г. № 152-ФЗ (ред. от 04.06.2014 г.) «О персональных данных».

ELABORATION OF SECURITY SYSTEM FOR A TYPICAL MEDICAL INFORMATION SYSTEM

Grigoriev P. E [1*], Olenchuk A. V. [1], Goldberg D. L. [1], Tishkov A. V. [2], Luskova Yu. S. [3]

[1]Physics and Technology Institute, V. I. Vernadsky Crimean Federal University, Simferopol 295007, Russia
[2]Pavlov First Saint Petersburg State Medical University, Saint Petersburg 197022, Russia
[3]Medical Academy named after S. I. Georgievsky, V. I. Vernadsky Crimean Federal University, Simferopol 295007, Russia
**E-mail: grigorievpe@cfuv.ru*

The article is dedicated the key stages of development of security system stages for a typical medical information system. The actualization of this problem is due to a global trend of increasing of cyberattacks for information systems in the healthcare in recent years. Providing the necessary level of information security is governed by the legal documents of the Russian Federation, the Federal Security Service, the Federal Service for Technical and Export Control, the international and national standards. Relevant documents were analyzed, based on which the basic aspects of the design of information security were considered. The basic model of information security threats, set of organizational and technical actions to protect information were defined, as well as optimal protection class for a typical health information system is grounded. An algorithm for the security system design development, which can be useful for the leaders of medical institutions, as well as the security subsystem administrators in the medical information system is proposed.

Keywords: information security, personal data, medical information system, healthcare.

References

1. T. V. Zarubina, *Sibirskij vestnik medicinskoj informatiki i informatizacii zdravoohranenija,* No 1, 6–11 (2016) [in Russian].
2. Poslanie Prezidenta Federal'nomu Sobraniju [Message from the President to the Federal Assembly], Available : http://kremlin.ru/events/president/news/53379 [in Russian].
3. O vnesenii izmenenij v Kodeks Rossijskoj Federacii ob administrativnyh pravonarushenijah [Amendments to the Russian Federation Code of Administrative Offences]. Oficial'nyj sajt Prezidenta Rossijskoj Federacii [The official website of the Russian President]. Available : http://kremlin.ru/acts/news/53836 [in Russian].
4. Putin podpisal zakon o personal'nyh dannyh [Putin signed a law on personal data]. RIA Novosti [RIA News]. Available : https://ria.ru/society/20170207/1487378476.html [in Russian].
5. Reviewing a year of serious data breaches, major attacks and new vulnerabilities. Analysis of cyber attack and incident from IBM's worldwide security services operations. IBM. Available : http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03133USEN&attachment=SEW03133USEN.PDF
6. Healthcare underspends on cybersecurity as attacks accelerate. Available: http://www.modernhealthcare.com/article/20160303/NEWS/160309922/healthcare-underspends-on-cybersecurity-as-attacks-accelerate
7. Sixth annual benchmark study on privacy & security of healthcare data. Available : https://media.scmagazine.com/documents/232/sixth_annual_benchmark_study_o_57783.pdf
8. Klinika vyplatila vykup hakeram: kiberprestupnost' v medicine [Clinic ransom hackers to cybercrime in medicine]. Available : https://www.health-ua.org/news/21266.html [in Russian].

9. Bulovich S. Kiberbezopasnost' informacionnyh sistem. Podhod "Laboratorii Kasperskogo" [Cybersecurity information systems. Approach "Kaspersky Lab"]. Available : http://compaslidera.ru/files/documents/Dopmaterial/ZPD-19042016/Kaspersky.pdf [in Russian].
10. Backup And Recovery System Allows Methodist Hospital To Regain Control After Ransomware Attack. Health IT Outcomes. Available : https://www.healthitoutcomes.com/doc/backup-recovery-system-control-ransomware-attack-0001
11. Two more healthcare networks caught up in outbreak of hospital ransomware. Ars Technica. Available : https://arstechnica.com/security/2016/03/two-more-healthcare-networks-caught-up-in-outbreak-of-hospital-ransomware/
12. Hackers hold German hospital data hostage. Deutsche Welle. Available: http://www.dw.com/en/hackers-hold-german-hospital-data-hostage/a-19076030
13. Hakery Anonymous atakovali bol'nichnuju sistemu Turcii [Anonymous Hackers attacked the hospital system in Turkey]. Available : http://newsturk.ru/2016/05/18/hakeryi-anonymous-atakovali-bolnichnuyu-sistemu-turtsii/ [in Russian].
14. Tehnicheskie sluzhby Minzdrava Rossii otrazili samuju masshtabnuju za poslednie gody hakerskuju ataku [Technical Service of the Russian Ministry of Health repel the most massive in recent years, hacker attack. Available : https://www.rosminzdrav.ru/news/2017/02/11/5085-tehnicheskie-sluzhby-minzdrava-rossii-otrazili-samuyu-masshtabnuyu-za-poslednie-gody-hakerskuyu-ataku [in Russian].
15. Health care and cyber security: increasing threats require increased capabilities. Available : https://assets.kpmg.com/content/dam/kpmg/pdf/2015/09/cyber-health-care-survey-kpmg-2015.pdf
16. Ukaz Prezidenta Rossiyskoy Federatsii ot 06 marta 1997 № 188 (red. ot 13.07.2015) «Ob utverzhdenii Perechnya svedeniy konfidentsial'nogo kharaktera» [Decree of the President of the Russian Federation of March 6, 1997 No. 188 (as amended on July 13, 2015) “On approval of the List of Confidential Information”] [in Russian].
17. Ukaz Prezidenta Rossiyskoy Federatsii ot 17 marta 2008 № 351 (red. ot 22.05.2015) «O merakh po obespecheniyu informatsionnoy bezopasnosti Rossiyskoy Federatsii pri ispol'zovanii informatsionno-telekommunikatsionnykh setey mezhdunarodnogo informatsionnogo obmena» [Presidential Decree of March 17, 2008 No. 351 (as amended on 05.22.2015) “On measures to ensure the information security of the Russian Federation when using information and telecommunication networks of international information exchange”] [in Russian].
18. Postanovleniye Pravitel'stva Rossiyskoy Federatsii ot 06 iyulya 2008 N 512 (red. ot 27.12.2012) «Ob utverzhdenii trebovaniy k material'nym nositelyam biometricheskikh personal'nykh dannykh i tekhnologiyam khraneniya takikh dannykh vne informatsionnykh sistem personal'nykh dannykh» [Decree of the Government of the Russian Federation dated July 6, 2008 N 512 (as amended on 12/27/2012) “On approval of requirements for tangible carriers of biometric personal data and technologies for storing such data outside of personal data information systems”] [in Russian].
19. Postanovleniye Pravitel'stva Rossiyskoy Federatsii ot 06 iyulya 2008 N 512 (red. ot 27.12.2012) «Ob utverzhdenii trebovaniy k material'nym nositelyam biometricheskikh personal'nykh dannykh i tekhnologiyam khraneniya takikh dannykh vne informatsionnykh sistem personal'nykh dannykh» [Decree of the Government of the Russian Federation dated July 6, 2008 N 512 (as amended on 12/27/2012) “On approval of requirements for tangible carriers of biometric personal data and technologies for storing such data outside of personal data information systems”] [in Russian].
20. Postanovleniye Pravitel'stva Rossiyskoy Federatsii ot 06 iyulya 2008 N 512 (red. ot 27.12.2012) «Ob utverzhdenii trebovaniy k material'nym nositelyam biometricheskikh personal'nykh dannykh i tekhnologiyam khraneniya takikh dannykh vne informatsionnykh sistem personal'nykh dannykh» [Decree of the Government of the Russian Federation dated July 6, 2008 N 512 (as amended on 12/27/2012) “On approval of requirements for tangible carriers of biometric personal data and technologies for storing such data outside of personal data information systems”] [in Russian].
21. Prikaz Roskomnadzora ot 30 maya 2017 goda № 94 «Ob utverzhdenii metodicheskikh rekomendatsiy po uvedomleniyu upolnomochennogo organa o nachale obrabotki personal'nykh dannykh i o vnesenii izmeneniy v raneye predstavlennyye svedeniya» [Order of Roskomnadzor dated May 30, 2017 No. 94 “On approval of guidelines for notifying the authorized body about the beginning of the processing of personal data and the introduction of changes to previously submitted information”] [in Russian].

22. Postanovlenie Pravitel'stva RF ot 01.11.2012 № 1119 «Ob utverzhdenii trebovanij k zashhite personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh» [Resolution of the RF Government of 01.11.2012 №1119 «On approval of requirements for the protection of personal data at their processing in information systems of personal data"] [in Russian].
23. D. L. Gol'dberg, P. E. Grigor'ev, A. V. Olenchuk, *Biotehnosfera,* No 2 (44), 12–16 (2016) [in Russian].
24. Metodicheskij dokument. Mery zashhity informacii v gosudarstvennyh informacionnyh sistemah: utv. FSTJeK Rossii ot 11 fevralja 2014 g. [Methodological document. Measures of information protection in state information systems: approved. FSTEC Russia on February 11, 2014]. Available : http://bdu.fstec.ru/documents/24 [in Russian].
25. Trebovanija o zashhite informacii, ne sostavljajushhej gosudarstvennuju tajnu, soderzhashhejsja v gosudarstvennyh informacionnyh sistemah: utv. prikazom FSTEK Rossii ot 11 fevralja 2013 g. № 17 [The data protection requirements, not the state secret contained in the state information systems : approved by FSTEC order of Russia from February 11, 2013 № 17]. Available : http://bdu.fstec.ru/documents/21 [in Russian].
26. Rukovodjashhij dokument. Sredstva vychislitel'noj tehniki. Zashhita ot nesankcionirovannogo dostupa k informacii. Pokazateli zashhishhennosti ot nesankcionirovannogo dostupa k informacii: utv. resheniem predsedatelja Gosudarstvennoj tehnicheskoj komissii pri Prezidente Rossijskoj Federacii ot 30 marta 1992 g. [Guidance document. Means of computer facilities. Protection against unauthorized access to information. Indicators of security against unauthorized access to information: approved. The decision of the Chairman of the State Technical Commission under the President of the Russian Federation of March 30, 1992]. Available: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/385-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g2 [in Russian].
27. Bazovaja model' ugroz bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh (vypiska): utv. zamestitelem direktora FSTJeK Rossii ot 15 fevralja 2008 g. [The basic model of personal data security threats at their processing within the information systems of personal data (excerpt): approved. Deputy Director FSTEC Russia on February 15, 2008]. Available : http://bdu.fstec.ru/documents/16 [in Russian].
28. Metodika opredelenija aktual'nyh ugroz bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah: utv. zamestitelem direktora FSTJeK Rossii ot 14 fevralja 2008 g. [Methods of determining the actual threats of personal data security at their processing in information systems: approved. Deputy Director FSTEC Russia of February 14, 2008]. Available : http://bdu.fstec.ru/documents/18 [in Russian].
29. Oficial'nyj sajt nekommercheskoj organizacii FIRST [The official website for a nonprofit organization FIRST]. Available : https://www.first.org/cvss/v2 [in Russian].
30. Bank dannyh ugroz bezopasnosti informacii [Data Bank information security threats]. Available : http://bdu.fstec.ru/cvss2 [in Russian].
31. Metodicheskie rekomendacii dlja organizacii zashhity informacii pri obrabotke personal'nyh dannyh v uchrezhdenijah zdravoohranenija, social'noj sfery, truda i zanjatosti: soglasovano s nachal'nikom 2 upravlenija FSTJeK ot 22 dekabrja 2009 g., utverzhdeno direktorom Departamenta informatizacii Ministerstva zdravoohranenija i social'nogo razvitija Rossijskoj Federacii ot 23 dekabrja 2009 g. [Guidelines for the organization of information security in the processing of personal data in health care, social services, labor and employment: agreed with the chief management FSTEC 2 of 22 December 2009, approved by the Director of the Ministry of Health of the Department of Informatization and Social Development of the Russian Federation of December 23, 2009.]. M., 2009. 94 p. [in Russian].
32. Metodicheskie rekomendacii po sostavleniju Chastnoj modeli ugroz bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh uchrezhdenij zdravoohranenija, social'noj sfery, truda i zanjatosti: soglasovano s nachal'nikom 2 upravlenija FSTJeK ot 22 dekabrja 2009 g., utverzhdeno direktorom Departamenta informatizacii Ministerstva zdravoohranenija i social'nogo razvitija Rossijskoj Federacii ot 23 dekabrja 2009 g. [Guidelines for the preparation of partial models of threats of personal data security at their processing within the information systems of personal data of health facilities, social services, labor and employment: agreed with the chief management FSTEC 2 of 22 December 2009, approved by the Director of the Ministry of Health and the Department of Informatization social development of the Russian Federation of December 23, 2009].

Ministerstvo zdravoohranenija i social'nogo razvitija [The Ministry of Health and Social Development]. M., 2009. 215 p. [in Russian].

33. Federal'nyj zakon ot 27.07.2006 g. № 152-FZ (red. ot 04.06.2014 g.) «O personal'nyh dannyh» [Federal Law of 27.07.2006 № 152-FL (ed. from 6.4.2014) "On personal data"].

Поступила в редакцию 05.11.2017 г. Принята к публикации 22.12.2017 г.
Received November 05, 2017. Accepted for publication December 22, 2017