УДК 681.518.3:616-71/-78
DOI: 10.25206/1813-8225-2021-179-74-79

В. А. МАЙСТРЕНКО[1]
О. А. БЕЗРОДНЫХ[1]
Р. А. ДОРОХИН[2]

[1]Омский государственный технический университет, г. Омск

[2]Московский государственный технический университет имени Н. Э. Баумана (национальный исследовательский университет), г. Москва

МЕТОДИКА ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В МЕДИЦИНСКОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ

В данной статье на основе обработки статистических данных из различных электронных ресурсов выделены наиболее частые виды угроз безопасности информации (УБИ) для медицинских информационных систем (МИС) и проведена их классификация.

Рассмотрены вопросы определения актуальных УБИ при создании МИС, обрабатывающих персональные данные по специфической технологии экспертной оценки. Предлагаемая методика определения актуальных угроз информационной безопасности для МИС, по сравнению с используемыми, устраняет субъективные оценки, являющиеся характерной чертой традиционных экспертных оценок. Ее применение также позволяет производить оценку актуальности угроз информационной безопасности для МИС, не имеющих в штате медицинского учреждения квалифицированных специалистов в области защиты информации, что является актуальным для большого количества медицинских учреждений.

Авторами исследованы практические возможности использования теории нечетких множеств (ТНМ) и нечеткой логики при определении актуальных УБИ для МИС различного назначения.

Ключевые слова: медицинская информационная система, типы медицинских информационных систем, защита персональных данных, нечеткая логика, нечеткая оценка, методики оценки угроз безопасности информации.

Введение. В настоящее время информационные технологии активно внедряются в медицинскую сферу деятельности. Одним из направлений применения информационных технологий в медицине является создание информационных систем (ИС), включающих в себя базы данных, содержащие персональные данные (ПД). Согласно Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» [1], ПД, используемые в медицинских ИС, входят в специальную категорию ПД. Оператор же при обработке ПД обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПД от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении ПД [1].

Обеспечение безопасности ПД достигается, в частности, определением и устранением угроз ПД данных при их обработке в информационных системах персональных данных (ИСПДн).

Целью разработки методик оценивания угроз безопасности информации (УБИ) является выявление совокупности условий и факторов, которые приводят или могут привести к нарушению безопасности обрабатываемой в системах и сетях информации: нарушению конфиденциальности (НК), целостности (НЦ), доступности (НД). В результате угроз безопасности информации должен быть сформирован перечень угроз безопасности информации, реализуемых для рассматриваемой архитектуры и условий функционирования информационных систем и сетей [2, 3].

Методика определения актуальных угроз безопасности информации. Руководящие документы

ФСТЭК России [2–5] предлагают следующий процесс оценки уровня опасности УБИ и определения актуальных угроз безопасности информации:

1) определение возможных негативных последствий от реализации угроз безопасности информации;

2) определение условий для реализации угроз безопасности информации;

3) определение источников угроз безопасности информации (УБИ) и оценка возможностей нарушителей;

4) определение сценариев реализации УБИ;

5) оценку уровня опасности УБИ и выделение актуальных угроз.

Кроме нормативно-правовых актов (НПА) регулятора Министерство здравоохранения выпустило внутренние НПА, в которых содержатся требования к государственным информационным системам в сфере здравоохранения (все ИСПДн медицинского назначения являются таковыми) и методические рекомендации по защите медицинских информационных систем (МИС) [6, 7].

Согласно этим рекомендациям, оценочные мероприятия при определении актуальных угроз безопасности предлагается производить экспертным методом, что не всегда возможно и приемлемо для ИСПДн медицинского назначения. Сотрудники, привлекаемые в качестве экспертов, могут не обладать необходимой квалификацией при оценке угроз, также оценка может иметь субъективный характер. Согласно статистическим данным в сфере здравоохранения только в 29 % случаев ИС их защитой занимаются профильные специалисты, а выделенные отделы информационной безопасности существуют только в 10 % медицинских организаций [8]. Особенно эти проблемы актуальны при создании ИСПДн медицинского назначения для отдельных медицинских учреждений.

Для оценки уровня угроз безопасности информации ИСПДн медицинского назначения предлагается методика, включающая в себя следующую последовательность действий при анализе УБИ:

1) определение перечня возможных угроз на основе их систематизации;

2) определение уровня опасности угроз из полученного перечня при помощи статистических данных;

3) оценка актуальности УБИ.

При анализе угроз из состава Банка данных угроз (БДУ) ФСТЭК [9] необходимо производить систематизацию перечисленных угроз [10]. Угрозы можно разделить на две большие категории:

— постоянные угрозы;

— угрозы при определенных условиях эксплуатации.

В первую группу входят угрозы, представляющие опасность для всех создаваемых информационных систем (ИС). Вторая же категория угроз появляется при использовании различных компонент ИС.

В свою очередь, постоянные угрозы подразделяются на следующие группы:

— угрозы BIOS;

— угрозы объектам файловой системы и носителям информации;

— угрозы технических отказов по различным причинам;

— угрозы вредоносного программного обеспечения;

— угрозы средствам защиты информации;

— угрозы несанкционированного доступа.

Угрозы при определенных условиях эксплуатации подразделяются на группы:

— угрозы при использовании виртуализации;

— угрозы при использовании внешних облачных технологий;

— угрозы при наличии подключения к Интернету или иным сетям;

— угрозы при использовании Wi-Fi;

— угрозы при использовании мобильных устройств;

— угрозы при использовании грид-систем;

— угрозы при использовании систем больших данных и суперкомпьютеров;

— угрозы, актуальные при обновлении программного обеспечения BIOS и микропрограммного обеспечения используемого оборудования;

— угрозы при возможном физическом доступе посторонних лиц;

— угрозы при использовании несертифицированного программного обеспечения.

Такое разделение позволяет упростить и оптимизировать определение угроз для ИСПДн медицинского назначения и, как следствие, проектирование систем защиты информации.

Создание систем информационной безопасности для ИСПДн медицинского назначения имеет свои особенности.

В п. 5.2 [7] описаны типы используемых в медицинских организациях информационных систем. В их состав входят следующие системы:

— 6 автономных (автономное рабочее место);

— 2 типа локальных ИС (рабочие места, объединённые в локальную вычислительную сеть в пределах одного здания);

— 2 типа распределенных систем (локальные вычислительные сети, расположенные в различных зданиях, контролируемых зонах, объединенные в одну информационную систему) [7].

Наиболее часто встречающимися являются много пользовательские МИС

(90 %) с сегментами, расположенными в различных или одной контролируемых зонах: локальной (57 %) или распределенной (43 %) [8].

В данной статье рассмотрим наиболее часто встречающийся тип информационной системы медицинских учреждений — локальная информационная система (ЛИС) 2-го типа с разграничением прав доступа, имеющая подключение к сетям связи общего пользования и (или) сетям международного информационного обмена, например, к сети Интернет.

Особенностями данной ИСПДн медицинского назначения являются:

— подключение ИСПДн к сети Интернет;

— запрет на применение мобильных устройств;

— запрет на применение Wi-Fi;

— использование средств защиты, прошедших сертификацию ФСТЭК России или других регуляторов.

Таким образом, в перечне возможных актуальных угроз остаются:

— все постоянные угрозы;

— угрозы при использовании виртуализации (если таковая используется);

— угрозы при наличии подключения к сети Интернет;

— угрозы при возможном физическом доступе посторонних лиц.

Предполагается, что внешний нарушитель не может воздействовать на защищаемую информа-

Таблица 1

Наиболее частые УБИ

Наименование УБИ	Частота угрозы в %	Частота угрозы средняя в %
Угроза неправомерного ознакомления с информацией	62 – 100	81
Угроза несанкционированного копирования информации	46 – 92	69
Угроза внедрения кода или данных	52 – 92	72
Угроза распространения «почтовых червей»	46 – 87	67
Угроза заражения компьютера при посещении неблагонадежных сайтов	50 – 87	69
Угроза несанкционированной модификации защищаемой информации	67 – 83	75
«Кража» учетной записи доступа к сетевым сервисам	48 – 69	59
Угроза приведения системы в состояние «отказ в обслуживании» (DOS)	38 – 83	61
Угроза утраты носителей информации	62 – 87	75

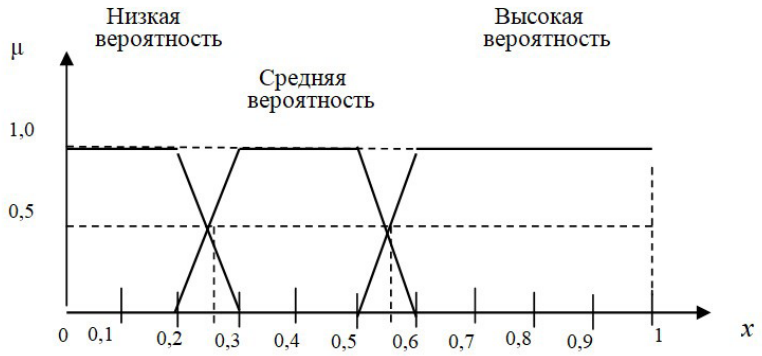

Рис. 1. Функции принадлежностей областей вероятности: «низкая», «средняя», «высокая»

цию по техническим каналам утечки, так как объем информации, хранимой и обрабатываемой в МИС, является недостаточным для возможной мотивации внешнего нарушителя к осуществлению действий, направленных на утечку информации по техническим каналам утечки.

Следовательно, можно заключить, что угрозы от внешнего нарушителя с высоким и средним потенциалом являются неактуальными.

Наиболее объективным будет определение частоты возникновения угрозы с использованием статистических данных и информации о самих угрозах. Причем рассматривается статистическая информация не только относительно МИС, но и ИСПДн другого назначения. Исходя из этих соображений можно выделить угрозы, представляющие наибольшую опасность, и присвоить каждой угрозе числовое значение оценки.

Анализируя статистические данные различных источников [8, 11—14], получаем данные о частоте возникновения различных угроз безопасности информации для МИС (табл. 1).

Такие угрозы информационной безопасности, как отказ подсистемы обеспечения температурного режима и физического устаревания аппаратных компонентов, будут являться актуальными всегда, и противостоять им можно только используя организационно-технические меры, оговариваемые при проектировании технической составляющей информационной системы.

Угрозы информации, не нашедшие отражения в статистических данных, можно считать маловероятными.

Исходя из систематизации угроз безопасности, статистических данных, определяющих частоту возникновения угрозы и ущерба от реализации угрозы, можно определить степени опасности УБИ для МИС. Прибегнув к методам нечеткой логики и нечеткой оценки [15 – 17], формируем вербальное значение и соответствующее ему численное значение возможности возникновения угрозы.

Рассмотрим методику формирования вербальных оценок.

В нашем случае универсальным множеством U является вероятностная шкала, которая разбивается на подобласти: 0 – 0,20; 0,20 – 0,50; 0,50 – 1 с вербальными высказываниями: «низкая вероятность», «средняя вероятность», «высокая вероятность» соответственно. Функции принадлежности для соответствующих областей пусть имеют вид (рис. 1).

Согласно теории нечетких множеств, можно определить среднее (взвешенное) нечеткое математическое ожидание функции принадлежности. Такая операция в принятии решения называется дефазификация и определяется из выражения:

$$y^{\star} = \frac{\sum_{r=1}^{Y\max} y_r \mu_{B'}(y)}{\sum_{r=1}^{Y\max} \mu_{B'}(y)}, \qquad (1)$$

где y^* — четкое значение выходной переменной, рассчитывается как центр тяжести функции принадлежности; Y_{max} — число элементов y_r в дискретизированной для вычисления «центра тяжести».

С учетом вышеизложенного можно определить среднюю (взвешенную) нечеткую вероятность из выражения

$$p_{CB}(\tilde{x}) = \frac{\sum_{i=1}^{n} \mu(x_i) p(x_i)}{\sum_{i=1}^{n} \mu(x_i)}, \quad \forall x \in U, \qquad (2)$$

$$p_{CB}(\tilde{x} - \textit{низкая вероятность}) = \frac{1 \cdot 0{,}1 + 1 \cdot 0{,}2}{2} = 0{,}15.$$

$$p_{CB}(\tilde{x} - \textit{средняя вероятность}) =$$

$$= \frac{1 \cdot 0{,}3 + 1 \cdot 0{,}4 + 1 \cdot 0{,}5}{3} = 0{,}4.$$

$$p_{CB}(\tilde{x} - \textit{высокая вероятность}) =$$

$$= \frac{1 \cdot 0{,}6 + 1 \cdot 0{,}7 + 1 \cdot 0{,}8 + 1 \cdot 0{,}9 + 1 \cdot 1}{5} = 0{,}8.$$

Результаты расчета представим в виде табл. 2.

Урон от реализации угрозы безопасности информации можно представить высказываниями, представленными в виде функций принадлежности (рис. 2).

Согласно рис. 2, нечеткие множества соответствуют: «незначительный урон» = $\mu_{НЗУ}(\tilde{x})$ {0/1; 0,1/0,4; 0,15/0}; «низкий урон» = $\mu_{НУ}(y)$ ={0,1/0,4; 0,2/0,5; 0,25/1; 0,3/0}; «средний урон»= $\mu_{СУ}(y)$= ={0,25/0; 0,3/0,2; 0,4/0,6; 0,5/1; 0,6/0}; «высокий урон» = $\mu_{ДУ}(y)$ = {0,5/0; 0,6/0,3; 0,7/0,8; 0,75/1; 0,8/0,5; 0,85/0}; «очень высокий урон» = $\mu_{ОУ}(y)$ = ={0,75/0; 0,8/0,2; 0,85/0,3; 0,9/0,6; 1/1}.

Степень значения урона от реализации угрозы безопасности информации от соответствующих множеств «ущерба» определяется из выражения:

$$y^* = \arg \max_{y \in Y} \mu_y(y). \qquad (3)$$

С учетом последнего выражения заполняется табл. 3.

Актуальность угрозы безопасности информации определяется исходя из численного показателя ее опасности ($Y_{УБИ}$), получаемого суммированием численного значения частоты возникновения угрозы ($Y_{час}$) с численным значением уровня урона от реализации угрозы ($Y_{урон}$):

$$Y_{УБИ} = Y_{час} + Y_{урон}. \qquad (4)$$

Просуммировав численные показатели в результате, получаем матрицу со следующими значениями $Y_{УБИ}$ (табл. 4) [18].

Среднее арифметическое значение элементов массива будет являться числом ($Y_{средн}$):

$$Y_{сред} = \frac{\sum Y_{УБИ}}{N}, \qquad (5)$$

где N — число элементов массива, т.е. $N = 20$.

Получаем $Y_{средн} = 0{,}835$.

Актуальными будут являться угрозы безопасности информации, у которых $Y_{УБИ} \geq Y_{средн} \geq 0{,}835$.

Таблица 2

Вербальные и вероятностные характеристики частоты УБИ

Частота угрозы средняя в %	Вербальное определение вероятности угрозы	Численное значение частоты возникновения угрозы $Y_{час}$
~0	маловероятная	0
0 – 30	низкая вероятность	0,15
20 – 60	средняя вероятность	0,4
50 – 100	высокая вероятность	0,8

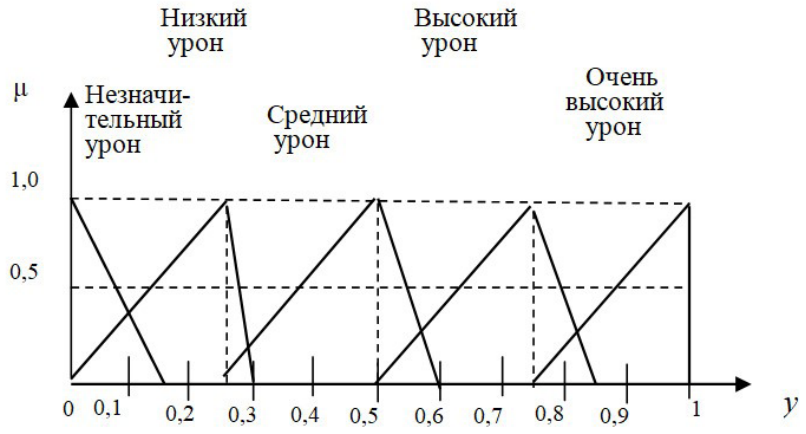

Рис. 2. Функции принадлежностей областей урона: «незначительный», «низкий», «средний», «высокий», «очень высокий»

Таблица 3

Значения урона от реализации угрозы безопасности информации

Вербальное определение урона от реализации угрозы	Численное значение уровня урона от реализации угрозы $Y_{урон}$
Незначительный	0
Низкий	0,25
Средний	0,5
Высокий	0,75
Очень высокий	1

Таблица 4

Значения численных показателей опасности угрозы безопасности информации

		Частота возникновения угрозы $Y_{час}$			
		0	0,15	0,4	0,8
Урон от реализации УБИ $Y_{урон}$	0	0	0,15	0,4	0,8
	0,25	0,25	0,35	0,65	1,05
	0,5	0,5	0,65	0,9	1,3
	0,75	0,75	0,9	1,15	1,55
	1	1	1,15	1,4	1,8

Так как рассматриваемые МИС содержат специальные персональные данные, то по уровню возможного урона при реализации угрозы, исходя из нормативных документов, их можно разделить на два типа:

1-й тип — система, обрабатывающая специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

2-й тип — МИС, обрабатывающие специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Реализация угроз относительно первого типа МИС представляет собой высокую опасность, а в отношении второго типа — среднюю. Рассмотрению подлежат УБИ, возможные в реализации применительно к заданной МИС [10].

То есть для МИС, обрабатывающих специальные категории персональных данных более чем 100000 субъектов персональных данных и не являющихся сотрудниками оператора, актуальными будут угрозы реализации в МИС с низкой, средней и большой вероятностями возникновения.

Для МИС, обрабатывающих специальные категории персональных данных сотрудников, операторов или специальные категории персональных данных менее чем 100000 субъектов, не являющихся сотрудниками оператора, актуальными являются угрозы со средней и большой вероятностями возникновения.

На примере УБИ 67 «Угроза неправомерного ознакомления с защищаемой информацией» для МИС 1-го типа определение ее актуальности выглядит следующим образом:

— частота возникновения данной угрозы, согласно статистике, — 81 %;

— вербальное значение частоты возникновения угрозы, согласно табл. 2, определяется как «Высокая вероятность», численное значение возможности возникновения угрозы — $Y_{возн} = 0,8$;

— реализация данной угрозы относительно первого типа МИС может нанести урон, имеющий вербальное определение «Высокий» и численное значение уровня урона от реализации угрозы ($Y_{урон}$), согласно табл. 3, составляет — 0,75;

— $Y_{УБИ} = Y_{час} + Y_{урон}$;

— $Y_{УБИ} = 0,8 + 0,75 = 1,55$.

Сравнивая $Y_{средн}$ и $Y_{УБИ}$ $0,835 < 1,55$, приходим к выводу, что угроза безопасности для МИС является актуальной.

На примере другой угрозы безопасности информации — УБИ 90 «Угроза несанкционированного создания учётной записи пользователя» для МИС 2-го типа определение ее актуальности имеет следующий вид:

— частота возникновения данной угрозы, согласно статистике, ~ 10 – 20 %;

— вербальное значение частоты возникновения угрозы, согласно табл. 2, определяется как «Низкая вероятность», численное значение возможности возникновения угрозы — $Y_{возн} = 0,15$;

— реализация данной угрозы относительно второго типа МИС может нанести урон, имеющий вербальное определение «Средний» и численное значение уровня урона от реализации угрозы ($Y_{урон}$), согласно табл. 3, равное 0,5:

$$Y_{УБИ} = Y_{возн} + Y_{урон}$$

$$Y_{УБИ} = 0,15 + 0,5 = 0,65.$$

Сравнивая $Y_{средн}$ и $Y_{УБИ}$: $0,835 > 0,65$, видим, что угроза безопасности для МИС является неактуальной.

Заключение. По результатам проведенного исследования установлено, что применение предложенной методики эффективно при определении актуальных угроз безопасности информации МИС. Предложенная методика, основываясь на статистической информации и применении нечетких вычислений, позволяет предотвратить субъективную оценку угроз, которая характерна для экспертного метода. Также подтверждается, что наиболее серьезные угрозы для МИС представляют несанкционированное копирование информации и несанкционированное ознакомление с ней. Именно на нейтрализацию этих угроз и должны быть ориентированы в первую очередь средства защиты информации, планируемые к использованию для защиты информационных систем.

Предложенная методика позволяет создать перечень актуальных УБИ для типовой МИС и проектировать системы защиты информации с использованием полученных результатов исследований.

Библиографический список

1. Российская Федерация. Законы. О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ. Доступ из справ.-правовой системы «Консультант Плюс».

2. Методика моделирования угроз безопасности информации. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/149-proekty (дата обращения: 18.06.2021).

3. Методика оценки угроз безопасности информации. ФСТЭК России. 2021 год. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021-g (дата обращения: 18.06.2021).

4. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: приказ ФСТЭК от 18 февраля 2013 года № 21 (ред. от 14.05.2020). Доступ из справ.-правовой системы «Консультант Плюс».

5. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК от 11 февраля 2013 года № 17 (ред. от 28.05.2019). Доступ из справ.-правовой системы «Консультант Плюс».

6. Об утверждении Требований к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций: приказ Министерства здравоохранения РФ от 24 декабря 2018 г. № 911н. URL: https://www.garant.ru/products/ipo/prime/doc/72117630/ (дата обращения: 21.06.2021).

7. Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости (включая «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» и приложения (26 шт.)). URL: https://minzdrav.gov.ru/documents/7570-recomendatsii (дата обращения: 21.06.2021).

8. Защита информации на рабочих станциях и серверах. Код безопасности. URL: https://www.securitycode.ru/documents/analytics/zaschita-informacii-rabochih-stanciy (дата обращения: 21.06.2021).

9. Банк данных угроз безопасности информации. URL: https://bdu.fstec.ru/threat (дата обращения: 21.06.2021).

10. Безродных О. А. Систематизация угроз безопасности информации для упрощения построения модели угроз // StudNe. 2021. Т. 4 (4). URL: https://stud.net.ru/sistematizaciya-ugroz-bezopasnosti-informacii-dlya-uproshheniya-postroeniya-modeli-ugroz/ (дата обращения: 21.06.2021).

11. Исследование утечек информации ограниченного доступа в госсекторе. Мир — Россия. 2018 год // Аналитический центр InfoWatch. URL: https://www.infowatch.ru/analytics/reports/20197 (дата обращения: 21.06.2021).

12. Утечки данных организаций по вине внутреннего нарушителя. Сравнительное исследование. 2013—2019 гг. URL: https://www.infowatch.ru/analytics/reports/24339 20197 (дата обращения: 21.06.2021).

13. Инсайдерские угрозы в России 2009 год. Perimetrix. URL: https://www.anti-malware.ru/files/PTX_Insider_Security_Threats_in_Russia_2009.pdf (дата обращения: 15.06.2021).

14. Безопасность информации в корпоративных информационных системах. Внутренние угрозы // Аналитический центр InfoWatch. URL: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Report_2013_ugroz.pdf (дата обращения: 15.06.2021).

15. Кульмамиров С. А., Рахимбердин Д. Р. Возможности теории нечеткой логики при анализе рисков систем информационной безопасности // Синергия наук. 2020. № 54. С. 817—831.

16. Савченко Д. В., Резникова К. М., Смышляева А. А. Нечеткая логика и нечеткие информационные технологии // Отходы и ресурсы. 2021. № 1 (8). URL: https://resources.today/PDF/10ECOR121.pdf (дата обращения: 15.06.2021).

17. Аникин И. В. Метод оценки рисков для уязвимостей информационных систем, основанный на нечёткой логике // Информационная безопасность. 2014.Т. 17, № 3. С. 468—471.

18. Безродных О. А. Оценка угроз информационной безопасности с использованием нечеткой логики // Инновации. Наука. Образование. 2021. № 36. С. 1078—1083.

МАЙСТРЕНКО Василий Андреевич, доктор технических наук, профессор (Россия), профессор кафедры «Средства связи и информационная безопасность» Омского государственного технического университета (ОмГТУ).
SPIN-код: 2706-9090
ORCID: 0000-0002-8785-1339
Author ID (SCOPUS): 7801670892
Researcher ID: H-5015-2013
Адрес для переписки: vasilii_maistrenko@mail.ru
БЕЗРОДНЫХ Олег Анатольевич, аспирант кафедры «Средства связи и информационная безопасность» ОмГТУ.
SPIN-код: 1574-8922
AuthorID (РИНЦ): 1107881
Адрес для переписки: oleg_ovo@mail.ru
ДОРОХИН Руслан Андреевич, аспирант кафедры «Защита информации» Московского государственного технического университета имени Н. Э. Баумана.
Адрес для переписки: ruslandorohin00@gmail.com

Для цитирования

Майстренко В. А., Безродных О. А., Дорохин Р. А. Моделирование угроз безопасности информации в медицинской информационной системе // Омский научный вестник. 2021. № 5 (179). С. 74—79. DOI: 10.25206/1813-8225-2021-179-74-79.

Статья поступила в редакцию 25.06.2021 г.