Автоматизация и моделирование в проектировании и управлении. 2024. № 1 (23). С. 73-80.
ISSN 2658-3488 print, ISSN 2658-6436 online
Automation and modeling in design and management. 2024. № 1 (23). P. 73-80.

Научная статья
Статья в открытом доступе
УДК 004.8
doi: 10.30987/2658-6436-2024-1-73-80

РАЗРАБОТКА АЛГОРИТМА ОЦЕНКИ ЭФФЕКТИВНОСТИ МЕР И СРЕДСТВ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В СФЕРЕ ЗДРАВООХРАНЕНИЯ

Кирилл Андреевич Седаков[1]✉, Михаил Юрьевич Рытов[2]
[1, 2] Брянский государственный технический университет, г. Брянск, Россия
[1]sekira98@mail.ru, https://orcid.org/0009-0002-9284-4624
[2]ozikts@yandex.ru, https://orcid.org/0009-0023-6345-5564

Аннотация. *Рассмотрены особенности существующих направлений и методов оценки эффективности мер защиты информации в медицинских учреждениях. Проведен комплексный анализ объектов и выявления угроз безопасности персональных данных. Установлены ключевые этапы исследования объектов, состоящие в определении стоимости информационных ресурсов, определении наиболее актуальных угроз и расчета ущерба от их применения. Выполнены анализ возможности реализации и устранения угроз, построена классификация наиболее критичных групп угроз. Основной научный результат выполненного исследования состоит в том, что применение данного алгоритма возможно, как в научных целях, так и для формирования эффективных систем защищенности персональных данных в различных организациях. Исходя из этого, данное исследование приведет к повышению уровня оценки эффективности мер защиты конфиденциальной информации в медицинских организациях.*

Ключевые слова: оценка эффективности информационной безопасности, категорирование уровня эффективности мер и средств конфиденциальной информации

Для цитирования: Седаков К.А., Рытов М.Ю. Разработка алгоритма оценки эффективности мер и средств защиты персональных данных // Автоматизация и моделирование в проектировании и управлении. 2024. №1 (23). С. 73-80. doi: 10.30987/2658-6436-2024-1-73-80.

Original article
Open Access Article

DEVELOPING AN ALGORITHM FOR ASSESSING THE EFFECTIVENESS OF MEASURES AND MEANS OF PERSONAL DATA PROTECTION IN THE HEALTHCARE SECTOR

Kirill A. Sedakov[1]✉, Mikhail Yu. Rytov[2]
[1, 2]Bryansk State Technical University, Bryansk, Russia
[1]sekira98@mail.ru✉, https://orcid.org/0009-0002-9284-4624
[2]ozikts@yandex.ru, https://orcid.org/0009-0023-6345-5564

Abstract. *The features of existing directions and methods for assessing the effectiveness of information protection measures in medical institutions are considered. A comprehensive analysis of objects and identifying threats to the security of personal data is carried out. The authors identify key stages of the object research, consisting of determining the cost of information resources, identifying the most relevant threats, and calculating the damage from their application. The analysis of the possibility of implementing and eliminating threats is performed; a classification of the most critical threat groups is built. The main scientific result of the performed research states that this algorithm application is possible both for scientific purposes and for forming effective personal data protection systems in various organizations. Based on this, this study will lead to increasing the level of the effectiveness assessment for the protection measures of confidential information in medical organizations*.

Keywords: effectiveness assessment of information security, categorizing the effectiveness level of measures and means of confidential information

For citation: Sedakov K.A., Rytov M.Yu. Developing an Algorithm for Assessing the Effectiveness of Measures and Means of Personal Data Protection in the Healthcare Sector. Automation and modeling in design and management, 2024, no. 1 (23). pp. 73-80. doi: 10.30987/2658-6436-2024-1-73-80.

Введение

На данный момент в информационном обществе важно обеспечить защиту информации от различных угроз и рисков. Каждый день мы сталкиваемся с новыми угрозами, связанными с хакерскими атаками, вирусами, кражей данных и другими событиями, которые могут нанести серьезный ущерб деловой репутации и потерю конфиденциальной информации. Поэтому актуальность разработки и применения эффективных методов оценки информационной безопасности никогда не была такой высокой.

Материалы исследования

В современном обществе угрозам информационной безопасности подвержен не только каждый человек, но и каждая организация, медицинские организации в том числе [1, 7, 12]. Оценка уровня реализуемости угроз безопасности информации не является исключением и для организаций медицинского назначения, так как в данных учреждения обрабатывается информация конфиденциального характера. В последнее время на медицинскую инфраструктуру увеличивается количество хакерских атак. Интерес к медицинским учреждениям для нарушителей объясняется тем, что в информационных системах обрабатывается большое количество информации конфиденциального характера, включая различные медицинские сведения, личные данные пациентов, номера банковских карт. Обработка персональных медицинских данных является важным аспектом в сфере здравоохранения. Защита конфиденциальности этих данных является не только юридическим требованием, но и этической обязанностью организаций, работающих с медицинской информацией. Для обеспечения достаточной безопасности персональных медицинских данных необходимо осуществлять организационные и технические мероприятия. В данной статье будет рассмотрен анализ существующих организационных и технических мероприятий, а также предложения по их усовершенствованию [4, 11].

В 2022 году здравоохранение стало самой атакуемой сферой, доля медицинских учреждений в статистике жертв преступников постоянно увеличивалась: с 8 % в 1 квартале до 12 % в конце года. По данным исследования PositiveTechnologies, преступники чаще всего похищали персональные данные клиентов и сотрудников, а именно 39 % от общей доли похищенных данных. Помимо персональных данных, также хищению подвергалась и медицинская информация, общая доля похищенной информации которой составляла 36 % [2, 6].

В медицинских организациях похищенную информацию могут использовать для различных целей:

1. Финансовые. Использование данной информации в фальсификационных банковских действиях.
2. Идентификационные. Использование украденной информации для получения поддельных удостоверениях личности. Помимо этого, использовать данную информацию для взлома учетных записей пациентов на различных онлайн платформах.
3. Медицинские. Использование медицинской информации для получения медицинских услуг или препаратов на имя другого человека, оставляя счета и ответственность за оплату на пострадавшего.
4. Вымогательские. Шантаж медицинской организации или пациента для получения выкупа.
5. Социальный инжиниринг. Использование данных для получения дополнительных данных и доступа к системе у пациента.
6. Сбор персональных данных. Сбор информации для спама и мошеннических сообщений [8, 9].

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

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. Особенно эти проблемы актуальны при создании ИСПДн медицинского назначения для отдельных медицинских учреждений [3, 5].

Обработка персональных медицинских данных является важным аспектом в сфере здравоохранения. Защита конфиденциальности этих данных является не только юридическим требованием, но и этической обязанностью организаций, работающих с медицинской информацией. Для обеспечения достаточной защищенности персональных медицинских данных необходимо осуществлять организационные и технические мероприятия, но для этого необходимо оценивать эффективность защиты персональных данных в различных организациях, с помощью которого можно рассчитать показатель эффективности наборов контрмер для снижения риска утечки персональных данных [6, 10].

Алгоритм оценки эффективности мер и средств защиты персональных данных

Разработанный алгоритм оценки эффективности мер и средств защиты персональных данных в медицинских организациях предложен на рис. 1.

Рис. 1. Алгоритм оценки эффективности мер защиты персональных данных
Fig. 1. Algorithm for evaluating the effectiveness of personal data protection measures

Главным преимуществом предложенного алгоритма является возможность оценки уровня остаточного риска от практической реализации разработанного набора контрмер и расчета степени влияния конкретных средств и методов защиты на общую защищенность организации сферы здравоохранения. Для определения оценки риска синтезирован алгоритм оценки ущерба от нарушения свойств защищенности, который базируется на экспертно-статистической оценке, особенностью которого является использование метода прогнозного графа. Алгоритм позволяет определять качественную и количественную оценку возможного ущерба персональным данным.

1. Определение и оценка персональных данных. На начальном этапе оценки эффективности средств защиты персональных данных в рамках определенной организации

сферы здравоохранения, необходимо выполнить анализ максимального финансового ущерба от реализации угроз целостности, доступности и конфиденциальности (размер штрафов, вызванных нарушением требований, действующих нормативно-правовых актов, а также стоимость восстановления информации при появлении деструктивных последствий. В результате выполнения данного этапа должны быть сформированы расчетные показатели, стоимости утечки персональных данных не только клиентов (пациентов), но и сотрудников данного учреждения. Данные показатели должны обрабатываться на объекте с учетом суммы наносимого ущерба, стоимости их восстановления и ряда других показателей.

2. Анализ и формирование групп угроз безопасности информации. На втором этапе нужно определить актуальные угрозы и выявить вероятность реализации угрозы. Помимо этого, в рамках работы на данном этапе должны быть сформированы группы угроз, чтобы определить степень вариативности реализации угроз.

При анализе угроз из состава банка данных угроз (БДУ) ФСТЭК необходимо производить систематизацию перечисленных угроз. Подробная систематизация выполнена в работе [4].

Анализ результатов работы и ряда других источников позволил ранжировать данные о частоте возникновения различных угроз безопасности информации (УБИ) для медицинских учреждений (табл. 1).

Таблица 1

Наиболее частые УБИ в медицинских учреждениях

Table 1

Most common UBIs in health care settings

Наименование УБИ		Частота угрозы в %	Частота угрозы средняя в %
УБИ.006	Угроза внедрения кода или данных	52…92	72
УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	50…87	69
УБИ.050	Угроза неверного определения формата входных данных, поступающих в хранилище больших данных	48…69	59
УБИ.052	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения	48…59	52
УБИ.057	Угроза неконтролируемого копирования данных внутри хранилища больших данных	46…87	67
УБИ.063	Угроза некорректного использования функционала программного и аппаратного обеспечения	50…89	70
УБИ.067	Угроза неправомерного ознакомления с информацией	62…100	81
УБИ.088	Угрозы несанкционированного копирования данных	46…92	69
УБИ.135	Угроза потери и утечки данных, обрабатываемых в облаке	48…69	59
УБИ.138	Угроза потери управления собственной инфраструктурой при переносе её в облако	48…59	52
УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании» (DOS)	46…87	67
УБИ.156	Угроза утраты носителей информации	62…100	81
УБИ.164	Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре	67…83	75
УБИ.167	Угроза заражения компьютера при посещении неблагонадежных сайтов	50…87	69
УБИ.168	Угроза «кражи» учетной записи доступа к сетевым сервисам	48…69	59
УБИ.170	Угроза неправомерного шифрования информации	38…69	47
УБИ.172	Угроза распространения «почтовых червей»	46…87	67
УБИ.175	Угроза «фишинга»	62…100	81
УБИ.179	Угроза несанкционированной модификации защищаемой информации	67…83	75
УБИ.197	Угроза хищения аутентификационной информации из временных файлов cookie	67…100	83

3. Определение параметров риска для каждой группы угроз. Осуществление дифференциации групп угроз и выделение критичной группы угроз на основании параметров: *ki* – ответ на *i* вопрос опросника, *ai* – коэффициент важности, определяющийся экспертным методом и удовлетворяющий условию (1).

$$\sum_{i=1}^{n} a_i = 1. \quad (1)$$

4. Оценка вероятности реализации выявленных угроз. Оценка вероятности реализации выявленных угроз проводится экспертным методом (2).

$$V_{ry} = \sum_{i=1}^{n} k_i \cdot a_i. \quad (2)$$

Определение вероятности реализации определенной угрозы рассмотрим на примере угрозы УБИ.067«Угроза неправомерного ознакомления с информацией» (табл. 2).

Таблица 2

Пример определения возможности реализации УБИ. 067

Table 2

An example of determining the possibility of implementing UBI. 067

№ угрозы	Название угрозы безопасности информации	Уязвимости	*ki*	Коэффициент важности *ai*	Возможность реализации угрозы *Vr*
УБИ.067	Угроза неправомерного ознакомления с информацией	Не назначен администратор ИБ / управление ИБ для регулярной проверки логов (системных событий)	0	0,4	0,4
		Установлена многофакторная аутентификации для DNS-сервера	1	0,4	
		Переговорные не проходили аттестацию (проходили более 5 лет назад)	0	0,2	

V_r на пример УБИ.067 вычисляется следующим образом:

$$V_r = (0 \cdot 0{,}4) + (1 \cdot 0{,}4) + (0 \cdot 0{,}2) = 0{,}4.$$

5. Определение средней вероятности реализации угроз. Следующим этапом является определение среднего значения возможности реализации угроз:

$$Vry = \frac{Vr1+Vr2+\cdots+Vrn}{Ny} \cdot 100 \quad (3)$$

где V_{ry} – среднее значение возможности реализации угроз; N_y – общее количество угроз, выявленных для данной организации.

В заключении данного этапа необходимо перевести количественный средний показатель возможности реализации угрозы (*Vry*) в качественный показатель возможности возникновения угрозы (ПВВУ): 0…40 (V_{ry}) – показатель «низкий» (ПВВУ); 41…70 (V_{ry}) – показатель «средний» (ПВВУ); 71…100(V_{ry}) – показатель «высокий» (ПВВУ).

Приведенное преобразование от количественного показателя к качественному продиктовано необходимостью расчета риска в соответствии с матрицей, представленной в табл. 3. В матрице все значения для определения уровня эффективности мер защиты информации определены по качественным показателям. В рамках данного этапа должна сформироваться группа угроз и показатель вероятности реализации угроз безопасности персональных данных. Таким образом, это позволяет определить необходимые контрмеры, для минимизации этого риска.

6. Определение коэффициента риска информационной безопасности. На шестом этапе проводится оценка степени критичности групп угроз. Этот показатель можно рассчитать с помощью значения коэффициента риска (4).

$$K_d = \frac{Vry}{N_y}, \quad (4)$$

где K_d – коэффициент риска; *b* – последствия от реализации угрозы (ценность актива); N_y – количество определенных угроз.

7. Оценка уровня риска информационной безопасности. В рамках данного этапа должен быть определен показатель уровня риска ИБ. Показатель уровня риска информационной безопасности «*Yr*» – определяет будет ли реализована угроза в данном медицинском

учреждении с учетом вероятности реализации угрозы и уровня коэффициента риска информационной безопасности. Данное значение рассчитывается по формуле (5).

$$Yr = \frac{Vry+Kd}{2} \quad (5)$$

где Yr – уровень риска информационной безопасности, $0 \leq Yr \leq 50$; V_{ry} – возможность реализации угрозы, $0 \leq V_{ry} \leq 100$; K_d – коэффициент риска, $0 \leq K_d \leq 10$.

После расчета Yr будут получены количественные оценки. Чтобы понять их значение, переведем данный результат в качественные с помощью шкалы оценок. Данная шкала оценивания выглядит следующим образом:

Если $0 \leq Yr \leq 20$, то уровень риска является низким;

Если $20 < Yr \leq 30$, то уровень риска является средним;

Если $30 < Yr \leq 40$, то уровень риска является высоким;

Если $40 < Yr \leq 50$, то уровень риска является очень высоким.

8. Подведение итоговой оценки эффективности защиты персональных данных. На восьмом этапе определяется итоговая оценка эффективности защиты персональных данных. Оценка эффективности формируется благодаря сравнительному анализу, который был получен в результате просчета модели показателя уровня риска и рассчитанной вероятности реализации угроз. Уровень эффективности мер защиты информации производится согласно табл. 3.

Таблица 3

Уровень эффективности мер защиты информации

Table 3

Level of effectiveness of information security measures

Уровень риска ИБ (*Yr*)	Возможность реализации угроз(*Vry*)		
	Низкий	Средний	Высокий
Низкий	0	1	2
Средний	1	2	3
Высокий	2	3	4
Очень высокий	3	4	5

Данная шкала оценивания выглядит следующим образом:

Если 0…1, то уровень эффективности мер защиты конфиденциальной информации является достаточно высокой;

Если 2…3, то уровень эффективности мер защиты конфиденциальной информации является средней;

Если 4…5, то уровень эффективности мер защиты конфиденциальной информации является очень низкой.

Результаты

Особенностью разработанного алгоритма является возможность оценки уровня эффективности мер защиты конфиденциальной информации не только в медицинских, но и в других организациях. Для расчета оценки эффективности мер защиты разработан алгоритм оценки показателя вероятности реализации угроз, базирующийся на экспертно-статистической оценке. Данная математическая модель позволит рассчитать оптимальный показатель уровня эффективности мер защиты конфиденциальной информации.

Заключение

Разработанный алгоритм можно использовать для оценки эффективности защиты персональных данных в различных организациях. Исходя из этого, данное исследование приведет к повышению уровня оценки эффективности мер защиты конфиденциальной информации в медицинских организациях, что, в свою очередь, приведет к повышению эффективности работы сферы здравоохранения.

Список источников:

1. Рытов М.Ю., Лексиков Е.В. Формализация методов анализа рисков информационной безопасности // Вестник БГТУ. – № 3. – 2018. – С. 141-146.
2. Конарева Л.А. Качество потребительских товаров как элемент национальной безопасности // США-Канада: экономика, политика, культура. – 2019. – № 11.
3. Котов В. Организация государственных (муниципальных) концессий и экономическая безопасность // Экономист. – 2020. – № 5.
4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
5. Мещеряков Р.В. Защита персональных данных в организациях здравоохранения. – М.: Горячая линия – Телеком, 2020. – 137 с.
6. Адамов Н.А., Морозова А.К., Морозов А.Ю., Хмелев С.А. Конкурентные преимущества как фактор обеспечения экономической безопасности потребительской кооперации // Russian Journal of Management. – 2019. – Т. 7. – № 3. – 61 с.
7. Басалай С.В. Построение системы управления рисками для повышения экономической безопасности // Микроэкономика. – 2019. – № 2.
8. Бауэр В.П. Экономическая безопасность и международные резервы Банка России / В.П.Бауэр, Е.М.Литвинова // ЭКО. – 2018. – № 9.
9. Бендиков М., Хрусталев Е. Экономическая безопасность наукоемких производств // Вопросы экономики. – 2019. – № 9.
10. Бендиков М.А., Хрусталев Е.Ю. Наукоемкие производства и экономическая безопасность // ЭКО. – 2020. – № 8.
11. Бекетов Н.В., Тарасов М.Е. Проблемы обеспечения экономической безопасности государства в сфере внешнеэкономической деятельности // Национальные интересы: приоритеты и безопасность. – 2019. – №8.
12. Рытов М.Ю., Седаков К.А. Анализ возможности применения методики определения актуальных угроз безопасности информации для медицинских учреждений // Информационные системы и технологии. – 2023. – № 5 (139). С. 112-119.
13. Седаков К.А., Рытов М.Ю. Анализ методик обеспечения информационной безопасности медицинских учреждений // Автоматизация и моделирование в проектировании и управлении. сборник научных статей Всероссийской конференции. – 2023. – С. 78-80.

References:

1. Rytov M.Yu., Leksikov E.V. Formalization of Methods for Analysis of Information Security Risks. Bulletin of BSTU. 2018;3:141-146.
2. Konareva L.A. The Quality of Consumer Goods as an Element of National Security. USA-Canada: Economics, Politics, Culture. 2019;11.
3. Kotov V. Organization of State (Municipal) Concessions and Economic Security. The Economist. 2020;5.
4. Federal Law From 2006 Jul 27 on Information, Information Technologies and the Protection of Information, no. 149-FZ (27-07-2006).
5. Meshcheryakov R.V. Protection of Personal Data in Healthcare Organizations. Moscow: Hotline-Telecom; 2020.
6. Adamov N.A., Morozova A.K., Morozov A.Yu., Khmelev S.A. Competitive Advantages as a Factor of Ensuring Economic Security of Consumer Cooperation. Russian Journal of Management. 2019;7(3):61.
7. Basalai S.V. Construction of a Risk Management System to Increase Economic Security. Microeconomics. 2019;2.
8. Bauer V.P., Litvinova E.M. Economic Security and International Reserves of the Bank of Russia. EKO. 2018;9.
9. Bendikov M., Khrustalev E. Economic Security of Science-Intensive Production. Voprosy Ekonomiki. 2019;9.
10. Bendikov M.A., Khrustalev E.Yu. Science-Intensive Production and Economic Security. ECO. 2020;8.
11. Beketov N.V., Tarasov M.E. Problems of Ensuring the Economic Security of the State in the Sphere of Foreign Economic Activity. National Interests: Priorities and Security. 2019;8.
12. Rytov M.Yu., Sedakov K.A. Analysis of the Possibility of Using the Methodology for Determining Current Threats to Information Security for Medical Institutions. Information Systems and Technologies. 2023;5(139):112-119.
13. Sedakov KA, Rytov MYu. Analysis of the Methods for Ensuring Information Security of Medical Institutions. In: Proceedings of the All-Russian Conference on Automation and Modelling in Design and Management: 2023. p. 78-80.

Информация об авторах:

Рытов Михаил Юрьевич
кандидат технических наук, доцент, зав. кафедрой «Системы информационной безопасности» Брянского государственного технического университета

Седаков Кирилл Андреевич
ассистент кафедры «Системы информационной безопасности» Брянского государственного технического университета

Information about the authors:

Rytov Mikhail Yurievich
Candidate of Technical Sciences, Associate Professor, Head of the Department «Information Security Systems» of Bryansk State Technical University

Sedakov Kirill Andreevich
Assistant of the Department «Information Security Systems» of Bryansk State Technical University

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации.
Contribution of the authors: the authors contributed equally to this article.

Авторы заявляют об отсутствии конфликта интересов.
The authors declare no conflicts of interests.

Статья поступила в редакцию 04.02.2024; одобрена после рецензирования 19.02.2024; принята к публикации 28.02.2024.
The article was submitted 04.02.2024; approved after reviewing 19.02.2024; accepted for publication 28.02.2024.
Рецензент – Еременко В.Т., доктор технических наук, профессор, Орловский государственный университет им. И.С. Тургенева.
Reviewer – Eremenko V.T., Doctor of Technical Sciences, Professor, Orel State University named after I.S. Turgenev.