


СОЦИОЛОГИЧЕСКИЕ НАУКИ



<https://doi.org/10.5281/zenodo.7341785>
УДК 316.7

Фоменков А.И., Фоменков В.А.

Фоменков Анатолий Иванович, кандидат педагогических наук, доцент, Смоленский государственный университет, Россия, 214000, г. Смоленск, ул. Пржевальского, д. 4. E-mail: ffortt@mail.ru.

Фоменков Виктор Анатольевич, Смоленский государственный университет, Россия, 214000, г. Смоленск, ул. Пржевальского, д. 4. E-mail: ffortt@mail.ru.

Кибербезопасность медицинских информационных систем в региональном здравоохранении: постановка проблемы исследования

Аннотация. В статье рассмотрены вопросы кибербезопасности медицинских информационных систем в региональном здравоохранении. В современных условиях повышается роль информации и знаний, а орудием труда непосредственно становятся информационные технологии. Это ставит вопрос о целесообразности построения системы информационной безопасности в рамках регионального здравоохранения, что сопряжено с трудностями реализации задачи сохранения здоровья граждан и выполнения главных целевых показателей в сфере охраны здоровья населения и развитие системы здравоохранения РФ. В ходе исследования выделены ключевые задачи для региональной системы здравоохранения в сфере кибербезопасности. Проведен анализ теоретико-методологических оснований данной проблемы. Отмечается, что существующие программные решения не могут быть интегрированы в современную систему информационной безопасности, а с имеющимся уровнем информатизации вопросы планирования и управления региональной системой здравоохранения оперативно не решаются. Указанные проблемы осложняются дефицитом квалифицированных кадров, способных решать сложные технические и технологические задачи и внедрять систему защиты информации в региональных органах здравоохранения.

Ключевые слова: информационная безопасность, кибербезопасность, ИТ-безопасность, медицинские информационные системы, информационно-коммуникационные технологии, социология медицины.

Fomenkov A.I., Fomenkov V.A.

Fomenkov Anatoly Ivanovich, Candidate of Pedagogical Sciences, Associate Professor, Smolensk State University, Russia, 214000, Smolensk, Przhevalskogo str., 4. E-mail: ffortt@mail.ru.

Fomenkov Viktor Anatolyevich, Smolensk State University, Russia, 214000, Smolensk, Przhevalskogo str., 4. E-mail: ffortt@mail.ru.

Cybersecurity of medical information systems in regional health care: formulation of the research problem

Abstract. The article discusses the issues of cybersecurity of medical information systems in regional healthcare. In modern conditions, the role of information and knowledge is increasing, and information technologies are directly becoming an instrument of labor. This raises the question of the expediency of building an information security system within the framework of regional healthcare, which is associated with difficulties in implementing the task of preserving the health of citizens and meeting the main targets in the field of public health and the development of the healthcare system of the Russian Federation. The study highlights the key tasks for the regional healthcare system in the field of cybersecurity. The analysis of the theoretical and methodological foundations of this problem is carried out. It is noted that existing software solutions cannot be integrated into a modern information security system, and with the existing level of informatization, the issues of planning and management of the regional health system are not solved promptly. These problems are complicated by a shortage of qualified personnel capable of solving complex technical and technological tasks and implementing an information protection system in regional health authorities.

Key words: information security, cybersecurity, IT security, medical information systems, information and communication technologies, sociology of medicine.

Актуальность настоящего исследования определена повышением роли информационных технологий в различных сферах общества, что ставит вопрос о создании систем информационной безопасности. В 2016 году Указом Президента РФ утверждена «Доктрина информационной безопасности РФ», которая является документом стратегического планирования в сфере обеспечения национальной безопасности РФ. В ней дается понимание информационной сферы, которая представляется объединением информации с объектами информатизации, сети «Интернет», информационных технологий и субъектами, связанными с обработкой информации и с обеспечением безопасности. Особо подчеркнем в этом определении значимость системы механизмов регулирования общественных отношений в информационной сфере [17].

В своем обращении Президентом В.В. Путиным к Федеральному Собранию РФ (1.03.2018 г.) было сказано: «... важнейшая задача, которая касается каждого, – это доступность современной, качественной медицинской помощи. Мы должны ориентироваться здесь на самые высокие мировые стандарты» [19]. Реализация этой задачи постановлением Правительства РФ от 26 декабря 2017 г. № 1640 должна осуществляться в рамках выпол-

нения Государственной программы «Развитие здравоохранения».

В связи с этими тезисами можно выделить две ключевые задачи для региональной системы здравоохранения: 1) информационная безопасность посредством организации защиты информации в региональной системе здравоохранения; 2) совершенствование инфраструктуры региональной системы здравоохранения посредством: формирования единой профилактической региональной среды; повышения уровня подготовки медицинских кадров и заработной платы; повсеместной качественной медицинской помощи населению.

Сегодня не оспаривается роль информации в развитии личности, в жизни современного общества и государства. В условиях формирования в РФ информационного общества повышается роль информации и знаний, а орудием труда непосредственно становятся информационные технологии. Следовательно, существенно возрастает и необходимость защиты информации. Так, уже в 2016 году Президент РФ В.В. Путин в послании Федеральному Собранию подчеркнул: «...ближайшее время ожидается рост количества корпоративных информационных систем, так как руководством страны взят курс на формирование в стране цифровой экономики,

ориентированной на повышение эффективности всех отраслей за счет использования информационных технологий, а ИТ-индустрия стала одной из самых быстроразвивающихся отраслей, объем экспорта которой составляет 7 миллиардов долларов» [18].

Вопрос о целесообразности построения системы информационной безопасности в рамках регионального здравоохранения сопряжен с трудностями реализации задачи сохранения здоровья граждан и выполнения целевых показателей в сфере охраны здоровья населения и развитие системы здравоохранения РФ, возникшими в деятельности органов государственной власти РФ в условиях начавшейся в 2020 году пандемии.

Теоретико-методологические основания данной проблемы формируются на основе обширного спектра направлений научных исследований: подходы в оценке эффективности, модернизации и оптимизации государственного управления системой здравоохранения; региональный аспект проблемы функционирования системы здравоохранения; основные проблемы в сфере информационных технологий и пути их решения, анализ причин недостаточного уровня развития «электронного правительства», рассмотрение мотивации перехода к концепции «цифрового правительства»; разработка современной модели управления медицинскими учреждениями и структурно - функциональными преобразованиями; совершенствование методов управления здравоохранением и обеспечение населения качественной медицинской помощью; методические подходы к оценке эффективности функционирования системы здравоохранения и анализу её ключевых параметров, отдельных медицинских учреждений; организационное и финансовое обеспечение функционирования здравоохранения и актуальность его реформирования, оценка эффективности бюджетных расходов на медицину; особенности развития и проблемы медицинского страхования, вопросы управления рисками и государственно-

частное партнерство [См., например: 1, 2, 3, 5, 6, 7, 8, 10, 11, 12, 13, 14 и др.]. Таким образом, очевидно, что круг подлежащих рассмотрению проблем имеет междисциплинарный характер.

В структуру государственной системы защиты информации входят её региональные подсистемы, которые нуждаются, с учетом особенностей регионов, детальной разработки и внедрении. Исследований в решении этой важной региональной проблемы недостаточно, имеются попытки представить формализованную (обобщенную) структуру региональной системы защиты информации [См., например: 4], а о разработке системы защиты информации региональных учреждений и органов управления здравоохранением информация фрагментированная, имеющая в основном юридически-правовой характер. Несмотря на эти факты, заданный вектор государственной политики в отношении определения приоритетов и создания условий для развития отечественных информационных технологий в системе управления государством и регионами практически определил дальнейшую перспективу на годы вперед.

А.Р. Дабагов в своих исследованиях проблем построения интегрированных медицинских информационных систем, делает выводы и дает конкретные рекомендации, суть которых заключается в утверждении, что в полном объеме интеграция глобальных медицинских систем является вопросом будущего развития, а сегодня теория открытых систем и построение их среды, пригодной для всех субъектов управления, является главным инструментом методов интеграции. Автор выделяет факторы препятствующие развитию: сложность анализа; оптимизация и интеграция разнородных систем, например: с современными диагностическими системами CDSS – Clinical decision support system (система поддержки принятия клинических решений) и нашим аналогом СППВР (система поддержки принятия врачебных решений); различного ряда риски. А.Р. Дабаговым также проведен

анализ тенденций в сфере применения информационных технологий в медицине, которые имеют специфические особенности (методы сбора, обработки и хранения информации, взаимодействия между учреждениями в системе здравоохранения) [См.: 5].

На сегодняшний день разработано много медицинских информационных систем (МИС), которые описаны в научных работах [См.: 15]. В одной из последних коллективных монографий опубликованы работы, посвященные развитию электронных медицинских систем и технологий в РФ [См.: 9]. Согласно работе Г.И. Назаренко, Я.И. Гулиева, Д.Е. Ермакова «Медицинские информационные системы: теория и практика», в эксплуатации находятся много ИТ-систем от разных производителей с различной функциональностью: а) локального уровня с узким кругом задач; б) допускающие значительный уровень интеграции как в отдельном учреждении, так и в региональных системах [См. 15]. Как показывают исследования, сегодня недостаточно распространены полнофункциональные системы в связи с тем, что:

а) практика направлена на автоматизацию в основном фискальных и отчетных функций;

б) сложность внедрения связана с рядом проблем: большое количество классификаций;

в) недостаточная стандартизация информационного обеспечения (не связанная терминология, отсутствие отраслевых тезаурусов, терминологические нестыковки в толковании основных понятий» [См.: 16].

Полагаем, что на основе анализа научной литературы по проблеме кибербезопасности в системе регионального здравоохранения можно выделить актуальные социальные противоречия:

- между бурным развитием информационно-коммуникационных технологий (ИКТ) в условиях развития и кризиса процесса глобализации ведёт к появлению качественно новых информационных мето-

дов и технологий борьбы, которые могут принимать форму «сетевых», «кибер», «гибридных» и «информационных» войн и запаздыванием контр мер на новых уровнях технологий по поддержанию своего информационного суверенитета и государственной самостоятельности.

- между наличием медицинских данных, которые на всех уровнях представляют собой ценный стратегический ресурс, доступ к которому необходимо строго контролировать, регламентировать, обеспечивая безопасное хранение данных и необходимостью широкого использования информации в системе здравоохранения, которая нуждается в обеспечении информационной защиты используемых персонализированных данных, касающихся здоровья или относящихся к разряду конфиденциальных;

- между уже разработанными информационными системами, которые, как правило: а) носят узконаправленный характер, ориентированный на обеспечение частных функций и задач; б) отсутствует единый подход при их развитии, а в процессе эксплуатации приводят к возникновению серьезных технологических проблем, в результате которых существующие информационные системы представляют собой комплекс разрозненных автоматизированных рабочих мест (АРМ), а не единую информационную среду и необходимый уровень информатизации системы здравоохранения, который позволит оперативно решать вопросы планирования и управления региональными системами здравоохранения (в перспективе всей отрасли) для достижения существующих целевых показателей;

- между широким использованием в медицине компьютеров, информационных технологий, что позволило решить задачу автоматизации обработки постоянно нарастающих объемов медицинской информации и возникшей проблемой – уязвимостью этих процессов по отношению к безопасности, что остро поставило необходимость решения проблемы информационной защиты, заключающуюся в мони-

торинге основных факторов: субъективных – люди и процедуры; объективных – технические устройства и программное обеспечение, причем касающиеся как внешней, так и внутренней сред учреждений (организаций);

- между необходимостью в оперативном управлении и стратегическом планировании ресурсов системы здравоохранения, повышения доступности и качества медицинской помощи гражданам РФ в рамках Программы государственных гарантий Министерства здравоохранения РФ и сложностью создания и ввода планируемой государственной информационной системы персонифицированного учета оказания медицинской помощи (географическая информационная система – ГИС «Здравоохранение»);

- между созданными в субъектах РФ медицинских информационно - аналитических центров, автоматизированных информационных систем фондов обязательного медицинского страхования (ОМС) и страховых медицинских организаций и острой нехваткой квалифицированного персонала способного решать сложные технические и технологические задачи;

- между высокими требованиями к персоналу медицинских учреждений (организаций) отвечающих за безопасность имеющейся информации, способных реализовать региональные проекты систем защиты информации и острым дефицитом квалифицированных кадров способных решать данные проблемы.

- между потребностью в эффективной защите информации в системе здравоохранения Смоленской области и социологического мониторинга эффективности защиты информации в медицинских учреждениях и организациях, органах управления региональным здравоохранением и фактическим отсутствием в управленческой практике данных систем;

- между необходимостью принятия организации комплекса мер защиты информации, обрабатываемой в организационной информационной системе, в которых ключевым является обучение персо-

нала правилам информационной безопасности и практическим отсутствием обучения с необходимой периодичностью соответствующей потребности конкретной организации (учреждению);

- между фактическим объемом используемых на практике технических ресурсов для эффективной защиты информации и потенциальными возможностями их применения административным персоналом, учитывающими материально-технические, кадровые особенности и возможности конкретного учреждения (организации);

- между слабым развитием профессиональных навыков по эффективной защите информации у административного аппарата учреждений (организаций) и представлениями о современном квалифицированном персонале, обладающим высоким уровнем компетентности – специализированной подготовки по защите информации.

Указанные противоречия позволяют констатировать, что сегодня отсутствует система защиты информации региональных органов управления здравоохранением, а также нет единой концепции разработки, организации внедрения и использования информационно-коммуникационных технологий (ИКТ) в медицинских учреждениях (организациях). Это ставит перед исследователями вопрос о том, каким образом на основе научного обоснования создать оптимально возможную систему защиты информации медицинских учреждений и организаций, органов управления региональным здравоохранением?

Краткий обзор проблемы кибербезопасности в сфере регионального здравоохранения позволяет сделать следующие выводы:

1) существующие программные решения пока на данном этапе не могут быть интегрированы в современную систему информационной безопасности;

2) с имеющимся уровнем информатизации вопросы планирования и управления региональной системой здравоохранения оперативно не могут быть решены;

3) дефицит квалифицированных кадров (персонала учреждений и организаций) усложняет решение сложных технических

и технологических задач и внедрения системы защиты информации в региональных органах здравоохранения.

СПИСОК ЛИТЕРАТУРЫ

1. Архипова, З. В. Трансформация «электронного правительства» в «цифровое правительство» / З. В. Архипова // Известия Байкальского государственного университета. 2016. Т. 26, № 5. С. 818-824.
2. Васильков, А. В. Безопасность и управление доступом в информационных системах / А. В. Васильков, И. А. Васильков. М.: ФОРУМ: ИНФРА-М, 2013. 368 с.
3. Гайдамакин, Н. А. Разграничение доступа к информации в компьютерных системах / Н. А. Гайдамакин. Екатеринбург: Изд-во Урал. ун-та, 2003. 328 с.
4. Горбачева А. В. Особенности формирования региональных систем защиты информации // Вестник Воронежского института МВД России. Воронеж: Изд-во Воронежского института МВД Российской Федерации. 2007. №2. С. 208–212.
5. Дабагов, А. Р. Информатизация здравоохранения и некоторые проблемы построения интегрированных медицинских информационных систем / А. Р. Дабагов // Журнал радиоэлектроники. 2011. № 9. [Электронный ресурс]. URL: <http://jre.cplire.ru/jre/sep11/index.html>
6. Данилова, Л. В. Проблемы информатизации регионального здравоохранения / Л. В. Данилова, Е. Л. Боршук, С. Б. Чалоян, Р. Г. Гильмутдинов // Медицинский альманах. 2013. № 6(30). С. 12-15.
7. Жигулин, Г. П. Организационное и правовое обеспечение информационной безопасности / Г. П. Жигулин. СПб.: СПбНИУИТМО, 2014. 173 с.
8. Зегжда, Д. П. Основы безопасности информационных систем / Д. П. Зегжда, А. М. Ивашко. М.: Горячая линия-Телеком, 2000. 452 с.
9. Информационные технологии в медицине 2009-2010: коллективная монография / под ред. Г. С. Лебедева, О. В. Симакова, Ю. Ю. Мухина. М.: ЗАО ИПРЖР, 2010.
10. Лобачев, В. В. Эффективное управление региональной системой здравоохранения автореф. дис.... канд. экон. наук. : 08.00.05. Курск, 2018. 24 с.
11. Лобкова, Е. В. Управление эффективностью региональной системы здравоохранения / Е. В. Лобкова, А. С. Петриченко / Региональная экономика: теория и практика. 2018. Т. 16, вып. 2. С. 274-295.
12. Мамедова, К. А. Основные принципы обеспечения информационной безопасности страны / К. А. Мамедова // Информационная безопасность регионов. 2016. № 1(22). С. 16–20.
13. Малюк, А. А. Введение в защиту информации в автоматизированных системах / А. А. Малюк, С. В. Пазизин, Н. С. Погожин. М.: Горячая линия-Телеком, 2001. 148 с.
14. Мельников, В. В. Безопасность информации в автоматизированных системах / В. В. Мельников. М.: Финансы и статистика, 2003. 368 с.
15. Назаренко, Г. И. Медицинские информационные системы: теория и практика / Г. И. Назаренко, Я. И. Гулиев, Д. Е. Ермаков. М.: ФИЗМАТЛИТ, 2005. 320 с.
16. Симаков, О. В. Основные задачи информационно-телекоммуникационных технологий в здравоохранении Российской Федерации / О. В. Симаков, Г. С. Лебедев; ред. О. В. Симаков, Ю. Ю. Мухин, Г. С. Лебедев // Информационные технологии в медицине. М.: ЗАО «Издательство Радиотехника», 2010. С. 7-19.
17. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646). URL: <https://www.garant.ru/products/ipo/prime/doc/71456224/#0> (дата обращения: 02.07.2020).
18. Послание Президента Российской Федерации Федеральному Собранию Российской Федерации 01.12.2016. <http://kremlin.ru/events/president/news/53379> (дата обращения: 02.07.2021)
19. Путин В.В. Послание Президента Федеральному собранию – URL: <http://www.kremlin.ru/acts/bank/42902> (дата обращения 12.10.2021)

REFERENCES (TRANSLITERATED)

1. Arhipova, Z. V. Transformacija «jelektronnogo pravitel'stva» v «cifrovoe pravitel'stvo» / Z. V. Arhipova // Izvestija Bajkal'skogo gosudarstvennogo universiteta. 2016. T. 26, № 5. S. 818-824.
2. Vasil'kov, A. V. Bezopasnost' i upravlenie dostupom v informacionnyh sistemah / A. V. Vasil'kov, I. A. Vasil'kov. M.: FORUM: INFRA-M, 2013. 368 s.
3. Gajdamakin, N. A. Razgranichenie dostupa k informacii v komp'juternyh sistemah / N. A. Gajdamakin. Ekaterinburg: Izd-vo Ural. un-ta, 2003. 328 s.
4. Gorbacheva A. V. Osobennosti formirovanija regional'nyh sistem zashhity informacii // Vestnik Voronezhskogo instituta MVD Rossii. Voronezh: Izd-vo Voronezhskogo instituta MVD Rossijskoj Federacii. 2007. №2. S. 208–212.
5. Dabagov, A. R. Informatizacija zdavoohranenija i nekotorye problemy postroenija integrirovannyh medicinskih informacionnyh sistem / A. R. Dabagov // Zhurnal radioelektroniki. 2011. № 9. [Jelektronnyj resurs]. URL: <http://jre.cplire.ru/jre/sep11/index.html>
6. Danilova, L. V. Problemy informatizacii regional'nogo zdavoohranenija / L. V. Danilova, E. L. Borshuk, S. B. Chalozan, R. G. Gil'mutdinov // Medicinskij al'manah. 2013. № 6(30). S. 12–15.
7. Zhigulin, G. P. Organizacionnoe i pravovoe obespechenie informacionnoj bezopasnosti / G. P. Zhigulin. SPb.: SPbNIUITMO, 2014. 173 s.
8. Zegzhda, D. P. Osnovy bezopasnosti informacionnyh sistem / D. P. Zegzhda, A. M. Ivashko. M.: Gorjachaja linijaja-Telekom, 2000. 452 s.
9. Informacionnye tehnologii v medicine 2009-2010: kollektivnaja monografija / pod red. G. S. Lebedeva, O. V. Simakova, Ju. Ju. Muhina. M.: ZAO IPRZhR, 2010.
10. Lobachev, V. V. Jeffektivnoe upravlenie regional'noj sistemoj zdavoohranenija avtoref. dis.... kand. jekon. nauk. : 08.00.05. Kursk, 2018. 24 s.
11. Lobkova, E. V. Upravlenie jeffektivnost'ju regional'noj sistemy zdavoohranenija / E. V. Lobkova, A. S. Petrichenko / Regional'naja jekonomika: teorija i praktika. 2018. T. 16, vyp. 2. S. 274–295.
12. Mamedova, K. A. Osnovnye principy obespechenija informacionnoj bezopasnosti strany / K. A. Mamedova // Informacionnaja bezopasnost' regionov. 2016. № 1(22). S. 16–20.
13. Maljuk, A. A. Vvedenie v zashhitu informacii v avtomatizirovannyh sistemah / A. A. Maljuk, S. V. Pazizin, N. S. Pogozhin. M.: Gorjachaja linija-Telekom, 2001. 148 s.
14. Mel'nikov, V. V. Bezopasnost' informacii v avtomatizirovannyh sistemah / V. V. Mel'nikov. M.: Finansy i statistika, 2003. 368 s.
15. Nazarenko, G. I. Medicinskie informacionnye sistemy: teorija i praktika / G. I. Nazarenko, Ja. I. Guliev, D. E. Ermakov. M.: FIZMATLIT, 2005. 320 s.
16. Simakov, O. V. Osnovnye zadachi informacionno-telekommunikacionnyh tehnologij v zdavoohranenii Rossijskoj Federacii / O. V. Simakov, G. S. Lebedev; red. O. V. Simakov, Ju. Ju. Muhin, G. S. Lebedev // Informacionnye tehnologii v medicine. M.: ZAO «Izdatel'stvo Radiotekhnika», 2010.S.7-19.
17. Doktrina informacionnoj bezopasnosti Rossijskoj Federacii (utv. Ukazom Prezidenta RF ot 5 dekabrya 2016 g. № 646). URL: <https://www.garant.ru/products/ipo/prime/doc/71456224/#0> (data obrashhenija: 02.07.2020).
18. Poslanie Prezidenta Rossijskoj Federacii Federal'nomu Sobraniju Rossijskoj Federacii 01.12.2016. <http://kremlin.ru/events/president/news/53379> (data obrashhenija: 02.07.2021)
19. Putin V.V. Poslanie Prezidenta Federal'nomu sobraniju – URL: <http://www.kremlin.ru/acts/bank/42902> (data obrashhenija 12.10.2021)

Поступила в редакцию 18.10.2022.

Принята к публикации 22.10.2022.

Для цитирования:

Фоменков А.И., Фоменков В.А. Кибербезопасность медицинских информационных систем в региональном здравоохранении: постановка проблемы исследования // Гуманитарный научный вестник. 2022. №10. С. 18-24. URL: <http://naukavestnik.ru/doc/2022/10/Fomenkov.pdf>