УДК 004.056 Вестник УрФО № 4(42) / 2021, с. 15–23

Акбулякова Л.М., Шабуров А.С.

DOI: 10.14529/secur210402

О СОВЕРШЕНСТВОВАНИИ АРХИТЕКТУРЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ВЗАИМОДЕЙСТВИИ ОПЕРАТОРА С СЕГМЕНТОМ «ЕГИСЗ»

В статье проанализирована структура и основные задачи, решаемые на основе внедрения Единой государственной информационной системой в сфере здравоохранения (ЕГИСЗ). Сформулирована проблема безопасного взаимодействия автоматизированных рабочих мест работников с ЕГИСЗ. Обозначены уязвимости действующей модели информационного взаимодействия. Предложена универсальная математическая модель поиска оптимальных структур информационных систем. Разработан алгоритм выбора варианта схемы подключения к ЕГИЗС при передаче персональных данных (ПДн). Сформированы основные схемы подключения, с помощью которых разработана усовершенствованная схема подключения ЕГИСЗ, позволяющая реализовать требования по защите информации.

Ключевые слова: *государственная информационная система, персональные данные, защита информации, морфологический подход.*

ON IMPROVING THE ARCHITECTURE OF THE PERSONAL DATA INFORMATION SYSTEM WHEN THE OPERATOR INTERACTS WITH THE EGISZ SEGMENT

The article analyzes the structure and main tasks solved on the basis of the introduction of a Unified state information system in the field of healthcare (EGISZ). The problem of safe interaction of automated workplaces of employees with EGISZ is formulated. The vulnerabilities of the current model of information interaction are identified. A universal mathematical model of the search for optimal structures of information systems is proposed. The article draws attention to the developed algorithm for selecting a variant of the connection scheme to the EGISZ when transferring personal data (PDt). The basic connection schemes have been formed, with the help of which an improved EGISZ connection scheme has been developed, which allows implementing information security requirements.

Keywords: *state information system, personal data, information protection, morphological approach.*

Активное развитие цифровых отношений в современном обществе обуславливают увеличение интенсивности информационного обмена, совершенствование механизмов обработки информации, качества предоставляемых сервисов и услуг. В то же время, процесс «цифровизации» способствует проявлению новых уязвимостей и угроз, связанных с внедрением передовых технологий, что требует выхода на новый качественный уровень решения проблемы обеспечения информационной безопасности.

Создание единых центров обработки данных, объединяющих многоуровневые и многофункциональные информационные системы, предполагает разработку и внедрение новых решений, сервисов и служб поддержки, основанных на современных технологиях и оптимальных алгоритмах. В тоже время, способы проникновения вредоносной информации в подобные информационные системы также стремительно модифицируются, что делает процесс защиты информации более трудоемким, требующим поиска и применения как новых средстви методов защиты, так и оптимизации архитектуры информационных систем.

Одним из примеров подобного класса сложных систем является Единая государственная информационная система в сфере здравоохранения (ЕГИСЗ), включающая множество подсистем, информационных реестров и ресурсов, в том числе конфиденциальной информации, относящейся к специальной категории персональных данных граждан Российской Федерации [1].

Основными задачами ЕГИСЗна сегодняшний день являются:

1) информационное обеспечение государственного регулирования в сфере здравоохранения;

2) информационная поддержка деятельности медицинских организаций, включая поддержку осуществления медицинской деятельности;

3) информационное взаимодействие по-

ставщиков информации в единую систему и пользователей информации, содержащейся в единой системе;

4) информирование населения по вопросам ведения здорового образа жизни, профилактики заболеваний, получения медицинской помощи, передачи сведений о выданных рецептах на лекарственные препараты из медицинских информационных систем медицинских организаций в информационные системы фармацевтических организаций;

5) обеспечение доступа граждан к услугам в сфере здравоохранения в электронной форме, а также взаимодействия информационных систем, информационных систем государственных внебюджетных фондов.

Ключевым принципом организации информационного взаимодействия в Едином цифровом контуре здравоохранения является обеспечение возможности обмена данными между информационными системами о случаях оказания медицинской помощи в электронном виде в объеме, необходимом и достаточном для обеспечения преемственности, и непрерывности процессов оказания медицинской помощи в отношении каждого отдельно взятого пациента [2].

Внедрение ЕГИСЗ является важной частью программы модернизации системы здравоохранения, главной задачей которой является создание целостногои доступного информационного пространства для всех участников информационного обмена в условиях обеспечения информационной безопасности.

В настоящее время ЕГИСЗ представляет собой информационную систему, обеспечивающую взаимодействие различных подсистем (рис. 1):

1) федерального сегмента и региональных сегментов ЕГИСЗ;

2) системы межведомственного электронного взаимодействия (СМЭВ);

3) web-порталов Министерства здравоохранения РФ и Правительства РФ - Единого портала государственных и муниципальных услуг (ЕПГУ);

4) системы удостоверяющих центров Министерства здравоохранения РФ;

5) защищенной сети передачи данных.

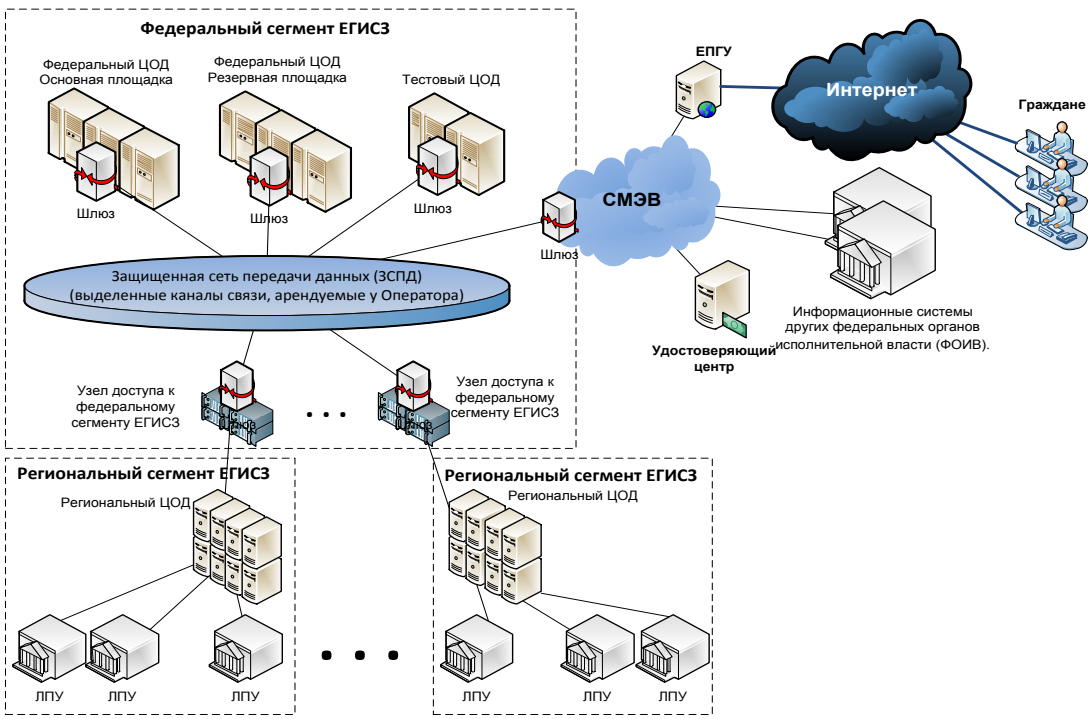

Рис. 1. Схема взаимосвязи компонентов ЕГИСЗ

Для решения задач обеспечения информационной безопасности АРМ медицинских организаций, подключенных к ЕГИСЗ необходима реализация оптимальной схемы подключения, которая смогла бы в полном объеме реализовать требования защищенной передачи персональных данных граждан [3]. При этом, на уровне федерального сегмента ЕГИСЗ предполагается обработка ПДн, примерно 145 млн. пользователей, являющихся

гражданами Российской Федерации. В приведенной схеме отражена логическая взаимосвязь основных компонентов федерального сегмента ЕГИСЗ с иными компонентами ЕГИСЗ и информационными системами.

Пользователями данной системы являются как граждане, так и сотрудники, осуществляющие взаимодействие через единый портал государственных и муниципальных услуг (ЕПГУ) и сети связи общего пользования. Подобное взаимодействие предполагает, что АРМ пользователей требуют защищенного соединения. Для этого данное взаимодействие осуществляется через СМЭВ, на выделенных для этой цели технических средствах Министерства здравоохранения и Правительства РФ, не имеющих прямого подключения к Федеральному центру обработки данных (ФЦОД).

В целях обеспечения достоверности передаваемых данных происходит взаимодействие с системой удостоверяющих центров Министерства здравоохранения при обеспечении участников информационного взаимодействия квалифицированными сертификатами электронной подписи, а также реализации функции по их проверке. Система удостоверяющих центров обеспечивает юридическую значимость передаваемых данных между участниками информационного обмена. Кроме того, для защиты информации на объекте информатизации реализованы организационные и технические меры, в соответствии с требованиями приказов ФСТЭК России. Перечень защитных мер адаптирован применительно к структурно-функциональным характеристикам выбранной информационной системы и особенностям её функционирования.

В то же время, при реализации базовых требований по защите информации на конкретных объектах не в полной мере учитываются особенности инфраструктуры и алгоритмов взаимодействия в подсистемах. Так, например, при удаленном подключении к АРМ работника, обрабатывающего конфиденциальную информацию, допускается подключения к общей сети внутри учреждения, где подключены и АРМ, которые не предназначенных для обработки персональных данных. При этом, допускается подключение к другим информационным системам, доступ которых осуществляется без использования программного комплекса средств защиты информации. Наличие подобных уязвимостей требует поиска новых, более совершенных, с точки зрения информационной безопасности, системных решений, а также оптимизации процедур взаимодействия элементов ЕГИСЗ.

В целях оптимизации информационных систем, при их разделении на подсистемы, целесообразно использовать морфологический подход, который широко применяется в проектировании сложных систем [3]. В этом случае предполагается, что любой вариант системы имеет определенную структуру, то есть состоит из конечного числа элементов (подсистем), и распределение, или перераспределение системных функций среди них могут быть выполнены с помощью конечного числа методов.

Процесс формирования множества допустимых вариантов системы можно представить посредством функциональной декомпозиции, в виде набора элементов в следующем виде:

$$\left\{ f_i, i = \overline{1, L}, \bigcup_{i=1}^{N} f_i = f \right\}. \quad (1)$$

Это предполагает разбиение конечного набора элементов системы S на N морфологических классов m(l), l=$\overline{1, L}$ таких, что $m(l) \cap m(l') = \emptyset$ при l ≠ l/.

Введем понятие морфологического пространства F ⊆ 2^{ε}, все элементы которого являются морфологическими вариантами системы $f = (f_1, f_2, ..., f_L)$. Каждый морфологический вариант f представляет собой определенный набор экземпляров класса $f(l) \in m(l)$. В данном случае для любого $f \in F$ и любого l=$\overline{1, L}$ множество $f \in F$ содержит один элемент.

Если предположить, что существует множество способов реализации каждой подсистемы $f_{lk}, k = \overline{1, K}, l = \overline{1, L}$, тогда общее количество возможных морфологических вариантов системы можно определить как:

$$Q = \prod_{l=1}^{L} K_l. \quad (2)$$

При формировании множества допустимых вариантов системы необходимо учитывать ограничения, накладываемые как на структуру, так и параметры, и техническую реализацию всех элементов системы. Кроме того, на систему в целом, а также допустимые варианты соединений элементов и ограничения на значения показателей качества системы. При учете всех этих показателей могут возникать противоречия в требованиях. С одной стороны, желательно, представить все

возможные варианты системы во всей их полноте, чтобы не пропустить потенциально лучшие варианты. С другой стороны, существуют ограничения, предусмотренные значением допустимых расходов (времени и средств) на проектирование системы. После определения множества возможных вариантов системы в терминах конкретной структуры, вычисляются значения показателей качества, и выделяются множество Парето-оптимальных вариантов, которое может сокращаться до единственного, наиболее предпочтительного, варианта [4]. Применение подобных оптимизационных подходов основывается на определении множества допустимых вариантов структуры системы, а также вариантов информационного взаимодействия ее элементов.

Анализ моделей информационного взаимодействия типовых элементов информационной системы, в первую очередь, предполагает изучение порядка функционирования и разработку моделей основных информационных связей, возникающих вследствие обработки информации. Для ЕГИС – функционирование при организации оказания различных медицинских услуг.

В первую очередь необходимо проанализировать варианты подключения медицинских организаций (МО), АРМ которых взаимодействуют непосредственно с медицинской информационной системой - ЕГИСЗ, при необходимости выполнении требований по безопасности информации [5]. При этом, выбор схемы подключения зависит от количества необходимых АРМ, потребностей пакетной обработки ПДн, а также наличии в организации защищенной сети. Варианты информационного взаимодействия медицинской информационной системы с АРМ работника характеризуется следующими признаками:

1. Масштаб медицинской организации.

2. Количество обрабатываемых персональных данных.

3. Применение программно-аппаратного комплекса.

Для оптимального выбора схемы подключения АРМ МО к ЕГИСЗ разработан алгоритм выбора варианта схемы подключения (рис.2).

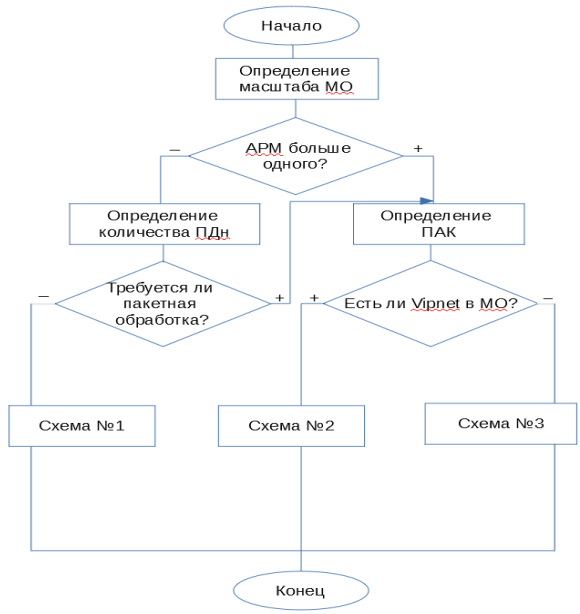

Рис. 2. Варианты информационного взаимодействия медицинской информационной системой с АРМ работника

Анализ различных вариантов информационного взаимодействия медицинской информационной системой с АРМ работника позволил сформировать несколько основных моделей подключения.

Схема подключения №1 ЕГИСЗ к АРМ работника для оказания медицинских услуг (рис.3) предполагает защиту информации конфиденциального характера, на основе применения сертифицированных шифровальных средств на базе продуктов семейства ViPNet. Данная схема предполагает под-

ключение с использованием изолированного автоматизированного рабочего места с локальным доступом в сеть Интернет и без доступа к локальной сети организации.

Данная схема предполагает следующие ограничения. ПДн обрабатываются только на выделенном АРМ, в режиме ручной обработки информации. В связи с данными ограничениями, подобная схема рекомендуется к использованию учреждениям с незначительным объемом обработки ПДн.

Схема подключения №2 (рис.4) является наиболее распространённой и рассчитана на подключение одного АРМ. Подключение и передача данных осуществляется с помощью программного комплекса ViPNet Client. Подключение по данной схеме обеспечивает большую защищенность данных при автоматизированной обработке ПДн, что позволяет произвести обмен данными с федеральными информационными системами. Подобная схема рассчитана на крупные медицинские учреждения и значительные потоки информационного взаимодействия.

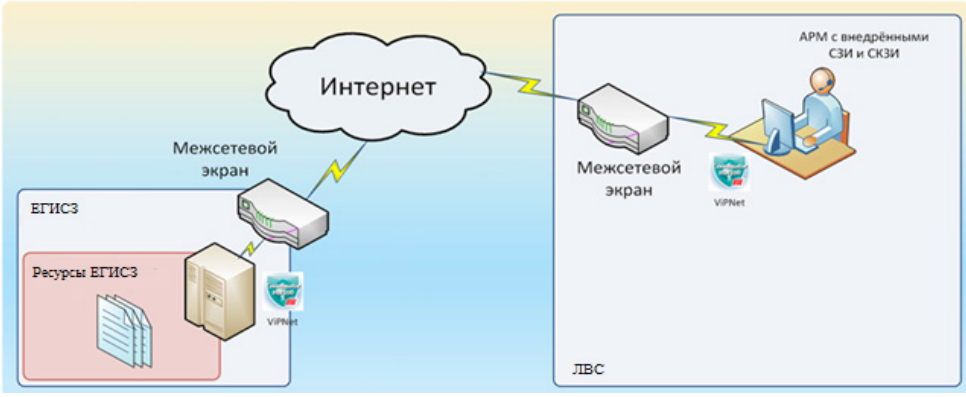

Рис. 3. Схема подключения №1

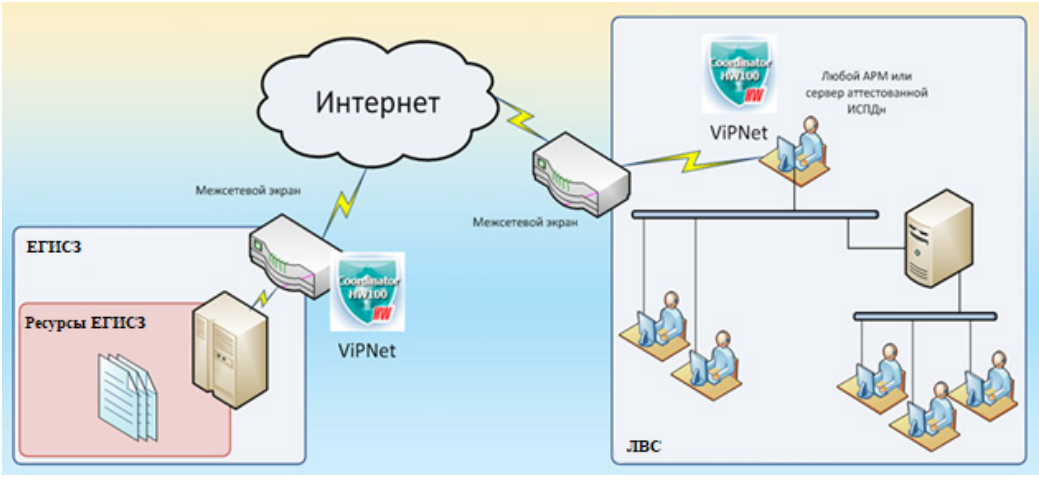

Рис. 4. Схема подключения №2

Схема подключения №3 (рис.5) предполагает возможность выделение отдельного сегмента, предназначенного для передачи данных, который может состоять из одного рабочего места и с которого может осуществляться загрузка данных. Подключение и передача данных осуществляется с помощью программно-аппаратного комплекса ViPNet Coordinator и рассчитана на количество от двух АРМ, поддерживает как ручной ввод информации, так и пакетную выгрузку персональных данных.

Таким образом, проанализированные схемы подключения позволяют систематизировать подходы к обработке информации и проанализировать основные методы защиты информации на типовых объектах информатизации учреждений здравоохранения.

В результате анализа характеристик можно выбрать оптимальную схему подключения, что обеспечивает необходимые процессы обработки ПДн, но не в полном объеме может гарантировать безопасность передачи

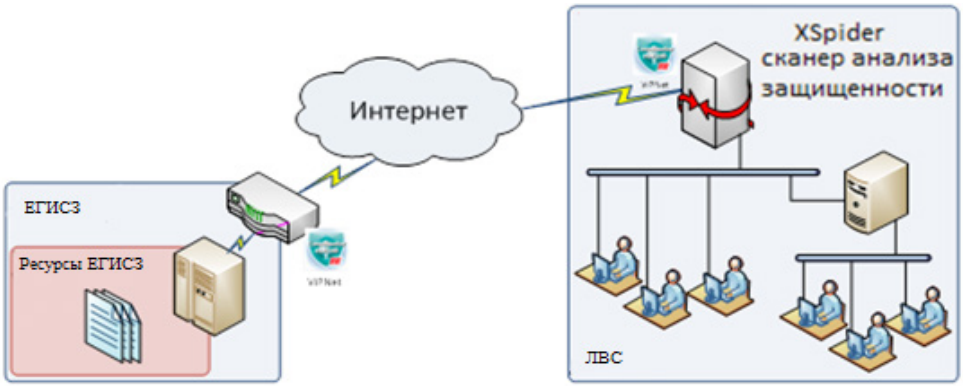

Рис. 5. Схема подключения №3

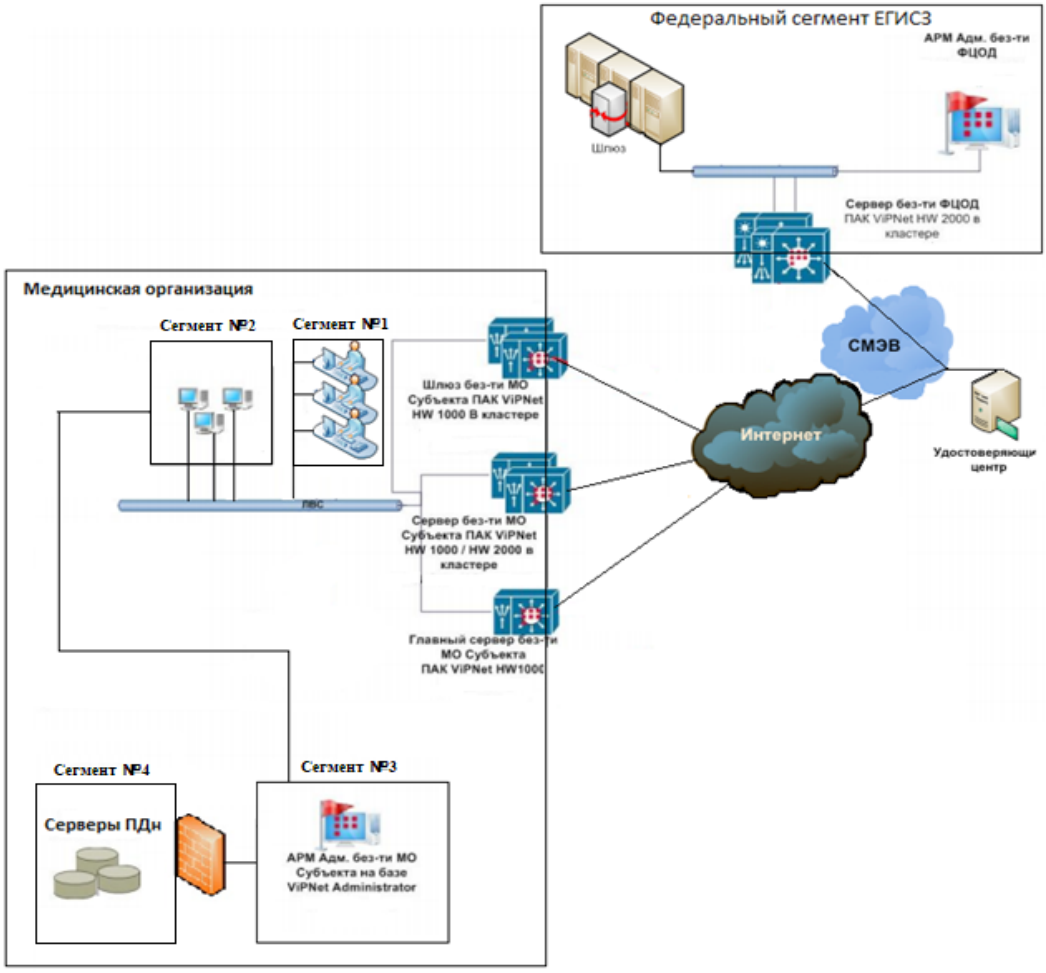

Рис. 6. Сегментированная структура сети

персональных данных из самих АРМ МО в сегмент ЕГИСЗ [6]. То есть, сохраняется недостаток архитектуры информационной системы, состоящий в сохранении возможности подключения АРМ МО к общей сети, в том числе и не предназначенных для обработки ПДн через сегмент ЕГИСЗ, подключенных к иным информационным системам, доступ которых осуществляется без требуемых средств защиты информации (VipNet) [7].

Для устранения данной уязвимости предлагается оптимизировать архитектуру информационной системы путем разделение ее на необходимое в конкретном случае количество сегментов (рис.6).

Обновленная архитектура отличается от

базовых схем подключения тем, что подсистема, предназначенная для обработки защищаемой информации (ПДн) разделена на 4 сегмента.

В первый сегмент включаются АРМ работников, не предназначенные для обработки защищаемой информации, или подключенные к другим информационным системам [8]. Выделение данного сегмента позволит устранить проблему, связанную с конфликтом доступа с одного физического устройства со своими установленными средствами защиты информации в разные информационные системы, требующих использования разных средств защиты информации для полноценного функционирования.

Во второй сегмент включаются АРМ сотрудников, на который поступает запрос от ЕГИСЗ и осуществляет перенаправление его на третий сегмент. Выделение данного сегмента позволяет разграничить права доступа сотрудников организации, а именно: определить тех, кто осуществляет работу с ЕГИСЗ, а кто нет. Это позволяет контролировать процесс распространения ПДн в организации. При этом, введенные ограничения не допускают обработку ПДн теми сотрудниками, которые не допущенных до данного процесса обработки.

Третий сегмент представляет собой АРМ администратора безопасности МО и получает перенаправленный запрос от второго сегмента. Кроме того, из данного сегмента может осуществляться доступ к серверным станциям (базам данных ПДн), в отличие от других АРМ. Данный сегмент также предполагает возможность определения прав доступа к базам данных.

В четвертый сегмент включаются серверные станции для хранения баз данных (ПДн). При этом, из четвертого сегмента не может осуществляться прямое взаимодействие с первым и вторым сегментом, или наоборот. Подобная конфигурация позволяет устранить противоречие в разграничении прав доступа для сотрудников, непосредственно работающих с ЕГИСЗ, а также позволяет осуществлять контроль процесса доступа и работы с ПДн.

Таким образом, проведенный анализ функционирования информационной системы, а также системы защиты ИСПДн позволил выявить уязвимости взаимодействия с ЕГИСЗ при передаче данных. Усовершенствованная архитектура взаимодействия в сети медицинской организации позволяет решить проблему одновременного доступа к разным информационным системам, при работе с разными категориями ПДн. При этом совершенствование архитектуры подобной системы позволяет устранить уязвимость без значительных ресурсных затрат, с сохранением требуемой технологии обработки информации.

Литература

1. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». -URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения 15.11.2021).

2. Постановление Правительства РФ от 05.05.2018 № 555 «О единой государственной информационной системе в сфере здравоохранения» //Собрание законодательства РФ. – 25.05.2018. - № 28. - Ст. 4241.

3. Золотарев А. В. Методы оптимизации распределительных процессов / А. В. Золотарев: ЛитРес, 2014. С. 22-34.

4. Подиновский В.В. Парето-оптимальные решения многокритериальных задач / В.В. Подиновский. – М.: Наука, 1982. – 256 с.

5. Князюк Н.Ф. Методические подходы к внедрению международного стандарта iso/iec 27001:2005 при построении системы управления информационной безопасностью медицинской организации/ Н.Ф.Князюк, И.С. Кицул. – Москва: Юрайт, 2018. – 102 с. (Менеджер здравоохранения). ISBN 978-5-534-02989-5.

6. Методические рекомендации медицинским организациям по организации криптографической защиты каналов при взаимодействии в рамках единой государственной информационной системы в сфере здравоохранения: официальный сайт. – Москва. - 2018. - URL: https://portal.egisz.rosminzdrav.ru (дата обращения 15.11.2021).

7. Решения по комплексному обеспечению информационной безопасности в ЕГИСЗ: официальный сайт. – Москва. - 2019. - URL: https://portal.egisz.rosminzdrav.ru(дата обращения 15.11.2021).

8. Техническое задание «Оказание услуги комплексного сервиса в целях обеспечения сервисной поддержки функционирования медицинской организации в рамках регионального сегмента единой

государственной информационной системы в сфере здравоохранения»:официальный сайт. – Москва. - 2020. - URL: https://vkr.pspu.ru/uploads (дата обращения 15.11.2021).

References

1. Federal'nyj zakonot 27 iyulya 2006 g. № 152-FZ «O personal'nyh dannyh». - URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (data obrashcheniya 15.11.2021).

2. Postanovlenie Pravitel'stva RF ot 05.05.2018 № 555 "O edinoj gosudarstvennoj informacionnoj sisteme v sfere zdravoohranenija" // Sobranie zakonodatel'stva RF. – 25.05.2018. - № 28. - St. 4241.

3. Zolotarev, A. V. Metody optimizacii raspredelitel'nyh processov / A. V. Zolotarev: LitRes, 2014. S. 22-34.

4. Podinovskij, V.V. Pareto-optimal'nye reshenija mnogokriterial'nyh zadach / V.V. Podinovskij. – M.: Nauka, 1982. – 256 c.

5. Knjazjuk, N.F. Metodicheskiepodhody k vnedreniju mezhdunarodnogo standarta iso/iec 27001:2005 pripostroenii sistemy upravlenija informacionnoj bezopasnost'ju medicinskoj organizacii/ N.F. Knjazjuk, I.S. Kicul. – Moskva: Jurajt, 2018. – 102 s. (Menedzherzdravoohranenija). ISBN 978-5-534-02989-5.

6. Metodicheskie rekomendacii medicinskim organizacijam po organizacii kriptograficheskoj zashhity kanalov pri vzaimodejstvii v ramkah edinoj gosudarstvennoj informacionnoj sistemy v sfere zdravoohranenija: oficial'nyj sajt. – Moskva. - 2018. - URL: https://portal.egisz.rosminzdrav.ru (data obrashhenija 15.11.2021).

7. Reshenija po kompleksnomu obespecheniju informacionnoj bezopasnosti v EGISZ: oficial'nyj sajt. – Moskva. - 2019. - URL: https://portal.egisz.rosminzdrav.ru (data obrashhenija 15.11.2021).

8. Tehnicheskoe zadanie «Okazanie uslugi kompleksnogo servisa v celjah obespechenija servisnoj podderzhki funkcionirovanija medicinskoj organizacii v ramkah regional'nogo segmenta edinoj gosudarstvennoj informacionnoj sistemy v sfere zdravoohranenija»: oficial'nyj sajt. – Moskva. - 2020. - URL: https://vkr.pspu.ru/uploads (dataobrashhenija 15.11.2021).

ШАБУРОВ Андрей Сергеевич, кандидат технических наук, доцент, доцент кафедры автоматики и телемеханики, Пермский национальный исследовательский политехнический университет. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: shans@at.pstu.ru.

АКБУЛЯКОВА Лилия Маратовна, студент Пермского национального исследовательского политехнического университета. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: akbulyakowa@mail.ru.

SHABUROV Andrey Sergeevich, Candidate of Technical Sciences, Associate Professor of the Department of Automation and Telemechanics. Perm National Research Polytechnic University. 614990, Perm, Komsomolsky Ave, 29. E-mail: shans@at.pstu.ru

AKBULYAKOVA Liliya Maratovna, student, Department of Automation and Telemechanics. Perm National Research Polytechnic University. 614990, Perm, 29, Komsomolskypr. E-mail: akbulyakowa@mail.ru.