004.056.53

Защита данных при их обработке в информационной системе льготного лекарственного обеспечения Краснодарского края

А.А. Кошкаров
аспирант, Кубанский государственный университет (г. Краснодар)
E-mail: Koshkarov17@yandex.ru
С.В. Лысков
начальник отдела информационной безопасности,
ГБУЗ «Медицинский информационно-аналитический центр»
министерства здравоохранения Краснодарского края, г. Краснодар, Россия
А.А. Халафян
д.т.н., профессор, ФГБОУ ВПО Кубанский государственный университет, г. Краснодар,
Россия, профессор кафедры прикладной математики, факультет Компьютерных технологий и прикладной математики.

Предложена модель идентификации угроз безопасности информационных систем. Определены актуальные угрозы для информационной системы льготного лекарственного обеспечения Краснодарского края, рекомендованы меры по предотвращению их реализации.

Ключевые слова: *информационная безопасность, защита персональных данных, модель угроз, льготное лекарственное обеспечение.*

In this regard, it has become an urgent task to provide protection in the information system of personal data of preferential medicinal maintenance of the Krasnodar region. The article suggests the model of threats to security of the relevant information system. The investigation results in identification of the existing actual threats and in recommendation of preventive measures.

Keywords: *information security, personal data protection, the threat model, preferential medicinal maintenance.*

Одним из базовых мероприятий для обеспечения безопасности персональных данных является определение угроз безопасности при их обработке в информационных системах персональных данных (ИСПДн) и уровня защищенности персональных данных[1]. Учитывая особую социальную значимость создания и функционирования единого программного продукта с возможностями выписки, отпуска, управления товарными запасами и контроля реализации программ льготного лекарственного обеспечения (ЛЛО), проблема информационной безопасности в этой сфере становится особенно актуальной.

Ц е л ь исследования – выявить актуальные угрозы безопасности для обеспечения защиты персональных данных при их автоматизированной обработке в сфере ЛЛО Краснодарского края, разработать схему бизнес-процессов идентификации актуальных угроз в аналогичных информационных системах.

Под *угрозами безопасности персональных данных* понимают совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в ИСПДн. Под уровнем защищенности персональных данных понимают комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в ИСПДн [1].

В работе дано описание потенциального нарушителя и предложена модель актуальных угроз безопасности персональных данных, с учетом особенностей существующей информационной системы «Льготного лекарственного обеспечения» (ИС «ЛЛО») государственного бюджетного учреждения здравоохранения «Медицинский информационно-аналитический центр» министерства здраво-

охранения Краснодарского края. *Модель угроз* – это документ, разработанный в соответствии с требованиями нормативных документов ФСТЭК России и ФСБ России, описывающий перечень возможных угроз ИС «ЛЛО».

Исходными данными для построения модели угроз стали материалы проведенного аудита информационной безопасности ИС «ЛЛО» с привлечением специалистов компании-лицензиата ФСБ России и ФСТЭК России. Угрозы безопасности персональных данных выявлены на основе экспертного метода, в том числе путем опроса обслуживающего персонала ИС «ЛЛО».

Модель угроз предназначена для решения следующих задач:

анализ угроз без опасности персональных данных;

анализ защищенности ИСПДн от угроз безопасности персональных данных;

определение уровня криптографической защиты персональных данных при использовании криптосредств;

определение мер для разработки системы защиты ИСПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего уровня защищенности;

определение мер контроля уровня защищенности обрабатываемых персональных данных.

Разработанная модель содержит описание последовательности мероприятий: построение модели нарушителя; определение исходного уровня защищенности ИС «ЛЛО»; определение вероятности, возможности реализации, опасности и актуальности каждой из угроз; описание возможных мер нейтрализации актуальных угроз.

ИС «ЛЛО» предназначена для хранения и обработки персональных данных граждан, получивших услуги в медицинских организациях: фамилия, имя, отчество; пол; дата рождения; место рождения; гражданство; данные документа, удостоверяющего личность; место жительства; место регистрации; дата регистрации; страховой номер индивидуального лицевого счета (СНИЛС), принятый в соответствии с законодательством Российской Федерации об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования; номер полиса обязательного медицинского страхования застрахованного лица; сведения о праве на получение государственной социальной помощи; данные документа, дающего право на получение государственной социальной помощи; данные выписанных рецептов (включая сведения об отпущенных лекарственных препаратах); код заболевания по МКБ-10.

ИС «ЛЛО» обладает техническими и эксплуатационными характеристиками [2], приведенными в табл. 1.

Таблица 1. ***Технические и эксплуатационные характеристики***

Технические и эксплуатационные характеристики ИСПДн	Исходные характеристики ИС «ЛЛО»
Территориальное размещение	Распределенная
Наличие соединения с сетями общего пользования	Одноточечный выход в сеть общего пользования
Встроенные операции с записями баз персональных данных	Запись, чтение, удаление, сортировка, поиск
Разграничение прав доступа к персональным данным	В соответствии с перечнем определен доступ сотрудникам организации – владельцу ИС «ЛЛО»
Наличие соединений с другими базами персональных данных иных ИСПДн	Используется одна база персональных данных, принадлежащая организации – владельцу ИС «ЛЛО»
Уровень (обезличивания) персональных данных	Предоставляемые пользователю данные не являются обезличенными
Объем персональных данных, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	Предоставляется часть персональных данных
Объем обрабатываемых персональных данных	Обрабатываются данные более 100 000 субъектов, не являющихся сотрудниками оператора персональных данных
Категория обрабатываемых персональных данных	Специальная (данные, касающиеся состояния здоровья субъектов персональных данных)

Источниками угроз в ИСПДн могут быть: аппаратная закладка, носитель вредоносной программы, нарушитель. Экспертным путем определено, что угрозы безопасности персональных данных, связанные с внедрением аппаратных закладок в ИС «ЛЛО», неактуальны. Носителями вредоносной программы в ИСПДн могут быть: отчуждаемый носитель (флеш-память, оптический диск, отчуждаемый винчестер, дискета и т.д.); встроенные носители информации (винчестеры); пакеты передаваемых по компьютерной сети сообщений; файлы (текстовые, графические, исполняемые и т.д.).

Нарушителем является физическое лицо (лица), случайно или преднамеренно совершающее действия, повлекшие нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах [2]. Потенциальные нарушители могут быть внешними, осуществляющими атаки из-за пределов контролируемой зоны ИСПДн, и внутренними – в пределах контролируемой зоны.

Модель угроз основана на предположении, что внешний нарушитель может воздействовать на защищаемую информацию только во время ее передачи по каналам связи вне контролируемой зоны или может воздействовать на элементы ИСПДн из сети международного информационного обмена. Исходили из того, что ИС «ЛЛО» – распределенная информационная система; ее элементы, непосредственно хранящие и обрабатывающие персональные данные, расположены на территории контролируемой зоны, кроме каналов линии связи, по которым осуществлена передача данных. При этом исключено несанкционированное пребывание посторонних лиц на территории контролируемой зоны.

Для защиты персональных данных от действий внешнего нарушителя при их передаче по сетям международного информационного обмена в модели угроз предусмотрены средства криптографической защиты информации (СКЗИ), которые должны противостоять действиям конкретного типа нарушителя, располагающего только доступными в свободной продаже аппаратными компонентами и средой функционирования криптосредства [5]. Таким образом, СКЗИ должны обеспечить криптографическую защиту персональных данных, не содержащих сведений, составляющих государственную тайну.

Внутренние потенциальные нарушители разделены на восемь категорий в зависимости от способа доступа и полномочий доступа к персональным данным [6]. Учитывая характеристики ИС «ЛЛО», способ и полномочия доступа к ИСПДн, предположения о возможностях нарушителя, степени его информированности, определены две вероятные категории:

1) лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к персональным данным (категория I);

2) зарегистрированные пользователи ИСПДн, осуществляющие удаленный доступ к персональным данным по локальной информационной сети (категория III).

Актуальной считают угрозу, которая представляет опасность для персональных данных и может быть реализована [2]. На рисунке приведена схема идентификации актуальных угроз ИС «ЛЛО», на которой изображен последовательный ход выполнения процедур определения актуальности для каждой из угроз.

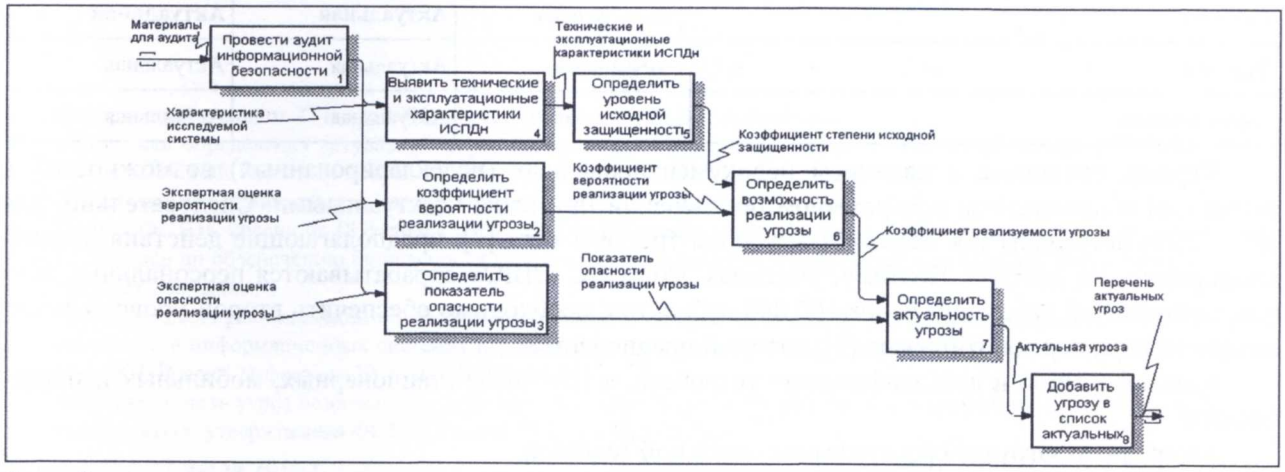

Схема бизнес-процессов идентификации актуальных угроз

Под *уровнем исходной защищенности* понимают обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн, приведенных в табл. 1 и называемый коэффициентом степени исходной защищенности (Y_1) [2]. Коэффициент Y_1 оценивают согласно таблицам соответствия по методике, изложенной в [2] в балльной шкале в соответствии со следующей градацией: 0 – для высокой степени; 5 – для средней степени; 10 – для низкой степени.

Вероятность реализации каждой из угроз определяют посредством показателя, называемого *коэффициентом вероятности реализации угрозы* (Y_2). Коэффициент Y_2 также оценивают в балльной шкале в соответствии со следующей градацией: 0 – маловероятная, 2 – низкая, 5 – средняя, 10 – высокая. Коэффициент Y_2 определяют для каждой из угроз путем экспертной оценки по установленной шкале.

По коэффициентам Y_1 и Y_2 рассчитывают обобщенный коэффициент Y реализуемости угроз

$$Y = (Y_1 + Y_2) / 20 . \quad (1)$$

Если коэффициент $Y \in [0, 0,3)$, то возможность реализации угрозы считают низкой; если $Y \in [0,3, 0,6)$ – средней; если $Y \in [0,6, 0,8)$ – высокой; если Y принимает значения не менее 0,8 – очень высокой [2]. Анализ безопасности ИС «ЛЛО» показал, что коэффициенту Y_1 соответствует значение 5 (средняя степень). Показатель опасности реализации каждой из угроз определен экспертным путем по шкале: «низкая», «средняя», «высокая».

Для ИС «ЛЛО» наибольший интерес представляют угрозы случайных действий (сд) пользователей и преднамеренных действий (пд) внутренних нарушителей, которые идентифицированы как угрозы соответственно средней и высокой опасности. Вероятности реализации каждой из этих угроз определены как низкие с коэффициентами $Y_2^{сд} = 2$ и $Y_2^{пд} = 2$. Учитывая, что коэффициент Y_1 для обеих угроз принимает одинаковое значение, равное 5, по формуле (1) легко рассчитать $Y^{сд} = 0,35$ и $Y^{пд} = 0,35$. Таким образом, возможность реализации каждой из угроз признана средней. Табл. 2 представляет собою правило идентификации угроз – характер угрозы (актуальная, неактуальная) определяют записью в ячейке таблицы, расположенной на пересечении строки и столбца [2]. По таблице легко видеть, что для ИС «ЛЛО» угрозы случайных действий пользователей и преднамеренных действий внутренних нарушителей следует идентифицировать как актуальные – соответствующие ячейки в табл. 2 выделены полужирным шрифтом.

Таблица 2. ***Правило определения угрозы***

Возможность реализации угрозы (Y)	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	Неактуальная	Неактуальная	Актуальная
Средняя	Неактуальная	**Актуальная**	**Актуальная**
Высокая	Актуальная	Актуальная	Актуальная
Очень высокая	Актуальная	Актуальная	Актуальная

Угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении признаны неактуальными. Следовательно, для ИС «ЛЛО» актуальны так называемые угрозы третьего типа [3], предполагающие действия несанкционированного доступа. Поэтому, учитывая, что в ИС «ЛЛО» обрабатываются персональные данные специальной категории более 100 000 субъектов, необходимо обеспечить второй уровень защищенности из четырех возможных [3], который предполагает:

идентификацию и аутентификацию устройств, в том числе стационарных, мобильных и портативных;

доверенную загрузку средств вычислительной техники;

учёт и управление доступом к машинным носителям персональных данных;

мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них;

применение системы обнаружения вторжений;

контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации;

возможность восстановления персональных данных с резервных машинных носителей персональных данных;

подлинность сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов;

обнаружение, идентификацию и регистрацию инцидентов.

В модели угроз представлены меры по обеспечению требуемого уровня защищенности ИС «ЛЛО» в соответствии с нормативно-правовыми актами регулирующих органов, с учётом характеристик системы и особенностей среды её функционирования в сфере льготного лекарственного обеспечения. Высокие требования к защите данных в этой области обусловлены большим количеством участников информационного обмена на разных уровнях управления здравоохранением Краснодарского края: медицинские и аптечные организации, муниципальные органы управления здравоохранения, министерство здравоохранения Краснодарского края и подведомственные ему организации.

В соответствии с базовым набором мер [4] по обеспечению второго уровня защищенности сформирован адаптированный и уточненный для ИС «ЛЛО» набор мер, с учётом ее структурно-функциональных характеристик и выявленных актуальных угроз безопасности. Составленный набор мер может быть реализован с применением имеющихся средств защиты информации и выполнением утвержденных организационных мероприятий. При этом реализация выбранных мер не приведет к увеличению сложности эксплуатации и повышению требований к квалификации обслуживающего персонала ИС «ЛЛО».

- Полученные результаты проведенного исследования дали общее представление о защищенности персональных данных в ИС «ЛЛО», позволили выявить уязвимые места информационной системы, подобрать меры по обеспечению безопасности и спланировать её дальнейшее развитие в направлении защиты информации. Даны рекомендации по обеспечению конфиденциальности, доступности и целостности защищаемых данных в ИС «ЛЛО», обрабатываемых всеми участниками информационного обмена.

  Результаты представленных исследований могут быть использованы при составлении организационно-распорядительных документов, регламентирующих обработку персональных данных, в том числе должностных инструкций и регламентов работ; при разработке моделей угроз безопасности персональных данных идентичных информационных систем.

ЛИТЕРАТУРА

1. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных».
2. «Методика определения актуальных угроз безопасности персональных данных при их обработке в ИСПДн», утверждённая ФСТЭК России 14 февраля 2008 года.
3. Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119.
4. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
5. «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утверждённые ФСБ России 21 февраля 2008 года № 149/54-144.
6. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная ФСТЭК России 15 февраля 2008 года.

Поступила 17 июля 2015 г.

Data security at their processing within the information system of preferential medicinal maintenance Krasnodar region

A.A. Koshkarov
Post-graduate Student, Kuban State University, Krasnodar city, Russia
E-mail: Koshkarov17@yandex.ru
S.V. Lyskov
Head of information security,
Medical Centre for Information and Analysis of the Ministry of Health Care of Krasnodar Region, Krasnodar city, Russia
E-mail: slyskov@miackuban.ru
A.A. Khalafyan
Ph.D. (Eng.), Professor, Department of computer technology and applied mathematics faculty, Kuban State University, Krasnodar city
E-mail: khaliphyan@kubannet.ru

The article raises the problem of information security in the sphere of preferential provision of medicines on the territory of Krasnodar region. The scientific direction of the work is protection against unauthorized access. The article provides an overview of existing methods to ensure the protection of personal data. The article suggests the model of threats to security of the information system in the sphere of preferential medicinal provision of Krasnodar region. The investigation results in identification of the existing actual threats and in recommendation of preventive measures.

One of the basic measures to ensure the security of personal data is the identification of security threats at their processing in information systems of personal data and the protection level of personal data. Given the special social importance of the establishment and functioning of a unified software product with the capabilities of the prescriptions, service, inventory management and supervising the implementation of programs of preferential provision of medicines, the problem of information security in this area is especially important.

The aim of the studying is to identify the current security threats to ensure the protection of personal data during their automated processing in the field of preferential medicinal maintenance of the Krasnodar region, to develop a scheme of business processes of identify relevant threats in similar information systems.

The study developed a threat model that includes a description of a potential intruder and actual threats to the security of personal data, taking into account the peculiarities of the existing information system of «Preferential medicinal maintenance» of Medical Centre for Information and Analysis of the Ministry of Health Care of Krasnodar Region.

The developed threat model includes a description of activities carried out: building a model of the offender; identification of the initial level of security of information system «Preferential medicinal maintenance»; identification of probability, feasibility, risks and relevance of each threat; possible measures of overcoming the actual threats.

Thus, there are two main threats to the security of personal data in the information system of «Preferential medicinal maintenance», which relate to threats of random user's actions and intentional actions of insiders.

The results of the conducted research gave an overview of the protection of personal data in the information system of «Preferential medicinal maintenance», allowed to reveal the vulnerabilities and prospects for further development in the direction of information protection. They can be used to write administrative documents regulating the processing of personal data, including job descriptions and regulations.

REFERENCES

1. Federal'ny'j zakon ot 27 iyulya 2006 g. N 152-FZ «O personal'ny'x danny'x».
2. «Metodika opredeleniya aktual'ny'x ugroz bezopasnosti personal'ny'x danny'x pri ix obrabotke v ISPDn», utverzhdyonnaya FSTE'K Rossii 14 fevralya 2008 goda.
3. Postanovlenie Pravitel'stva Rossijskoj Federaczii ot 1 noyabrya 2012 goda № 1119.
4. Prikaz FSTE'K Rossii ot 18 fevralya 2013 g. № 21 «Ob utverzhdenii Sostava i soderzhaniya organizaczionny'x i texnicheskix mer po obespecheniyu bezopasnosti personal'ny'x danny'x pri ix obrabotke v informaczionny'x sistemax personal'ny'x danny'x».
5. «Metodicheskie rekomendaczii po obespecheniyu s pomoshh'yu kriptosredstv bezopasnosti personal'ny'x danny'x pri ix obrabotke v informaczionny'x sistemax personal'ny'x danny'x s ispol'zovaniem sredstv avtomatizaczii», utverzhdyonny'e FSB Rossii 21 fevralya 2008 goda № 149/54-144.
6. «Bazovaya model' ugroz bezopasnosti personal'ny'x danny'x pri ix obrabotke v informaczionny'x sistemax personal'ny'x danny'x», utverzhdennaya FSTE'K Rossii 15 fevralya 2008 goda.