УДК 004.056.52

СИСТЕМНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ КОНФИДЕНЦИАЛЬНОСТИ ОБЕЗЛИЧЕННЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ В УЧРЕЖДЕНИЯХ ЗДРАВООХРАНЕНИЯ

Ажмухамедов И.М.[1], Демина Р.Ю.[2], Сафаров И.В.[3]

[1]ФБГОУ ВПО Астраханский государственный технический университет, Астрахань, Россия, (414056, г. Астрахань, ул. Татищева, 16), aim_agtu@mail.ru
[2]ООО «СекьюритиСтронгхолд», Астрахань, Россия, (414056, г. Астрахань, ул. Татищева, 43б, офис 41), leo_nom1@mail.ru
[3]ФБГОУ ВПО Астраханский государственный университет, Астрахань, Россия, (414056, г. Астрахань, ул. Татищева, 20А), ilnyr1001@gmail.com

Обеспечение защиты персональных данных (ПДн) для учреждений здравоохранения имеет особое значение. Это связано с тем, что большая часть ПДн относится к специальной категории, т.к. содержит информацию о расовой принадлежности, состояния здоровья, интимной жизни пациентов. Нарушение любого из свойств информационной безопасности этих данных приводит к существенному нарушению конституционных прав граждан, к финансовым и репутационным потерям организации. Для соблюдения требований руководящих документов, регламентирующих защиту ПДн, необходимы значительные финансовые средства, в которых большинство учреждений здравоохранения весьма ограничены. Использование обезличивания персональных данных позволяет снизить требования к обеспечению конфиденциальности. При этом наиболее простым и эффективным способом обезличивания ПДн является метод введения идентификаторов, который предусматривает раздельное хранение данных о пациенте и его идентификационных параметров. Для восстановления целостности информации о пациенте используются создаваемые при присвоении идентификаторов таблицы соответствия. Обеспечение защиты этих таблиц от несанкционированного доступа может осуществляться криптографическими методами, а также методами блокирования доступа к файлу. Применение системного подхода позволило разработать схему использования этих методов, обладающую синергетическим эффектом и позволяющую увеличить надежность защиты ПДн пациентов.

Ключевые слова: персональные данные, системный подход, блокирование доступа к файлу, криптографическая защита информации, конфиденциальность информации, синергетический эффект.

SYSTEMATIC APPROACH TO ENSURE CONFIDENTIALITY OF IMPERSONAL DATA IN HEALTH CARE ESTABLISHMENTS

Azhmuhamedov I.M.[1], Demina R.Y.[2], Safarov I.V.[3]

[1]Astrakhan State Technical University, Astrakhan, Russia, (414056, Astrakhan, Tatischevast., 16), aim_agtu@mail.ru
[2]Ltd. "SecurityStronghold", Astrakhan, Russia, (414056, Astrakhan, Tatischevast., 43b, room 41), leo_nom1@mail.ru
[3]Astrakhan State University, Astrakhan, Russia, (414056, Astrakhan, Tatischevast., 20A), ilnyr1001@gmail.com

Ensuring personal data (PD) security is particularly important for health care establishments. This is due to the fact, that most of PD belongs to special category, cause contains information about the race, health state, patient's sexual life. Breach of any of this data information security's services leads to significant violation of the citizen's constitutional rights, establishment's financial and reputational losses. Directive document's requirements of PD protection's adherence require significant financial resources, which are very limited in health care establishments. Using data's impersonalizing allows bringing down confidentiality's requirements.The most simple and effective way of depersonalization PD method is the identifiers' introduction, which provides patient personal data's and his identification parameters' separate storage. Correspondence tables created in assigning identifiers used for restoring patients information's completeness. This tables' protection ensuring from unauthorized access can be realized by cryptographic methods and file blocking access methods. System approach using allowed to create scheme of both methods' joint use, which have synergistic effect and allows increase patients PD security's reliability.

Keywords: personal data, system approach, blocking access to the file, cryptographic information protection, the confidentiality of information, synergistic effect.

Информатизация здравоохранения является одним из важных направлений модернизации медицинских учреждений. Использование информационных технологий

позволяет в значительной степени повысить качество их работы. Оказание медицинских услуг связано с обработкой персональных данных (ПДн) пациентов. При этом большая часть ПДн относится к специальной категории, т.к. содержит информацию о расовой принадлежности, состояния здоровья, интимной жизни пациента.

Обработка ПДн регламентируется федеральным законом № 152 «О персональных данных» от 27 июля 2006 года и рядом руководящих документов: приказом ФСТЭК от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»; постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»; «Методическими рекомендациями для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости» ФСТЭК и Минздравсоцразвития от 23 декабря 2009 года.

Согласно требованиям руководящих документов, к защите персональных данных специальной категории предъявляются жесткие требования. Для их обеспечения необходимы значительные финансовые средства, в которых большинство бюджетных учреждений здравоохранения весьма ограничено.

Постановка задачи

Одним из методов, позволяющим снизить требования к обеспечению уровня конфиденциальности, и, как следствие, сократить затраты на приобретение и поддержание системы защиты информации (СЗИ), является обезличивание, в результате которого становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту.

Наиболее простым и эффективным способом обезличивания медицинской информации является метод введения идентификаторов. Он реализуется заменой части персональных данных, позволяющих идентифицировать субъект, идентификатором и созданием таблиц соответствия, доступ к которым строго ограничивается.

Для обеспечения конфиденциальности в основном используются криптографические методы защиты, применение которых делает невозможным ознакомление с содержимым файла без знания ключевой информации. При этом надежность криптографической защиты, согласно принципу Керкхофса, должна зависеть только от сложности ключа и не должна опираться на секретность алгоритма [3-4].

Наиболее часто для обеспечения конфиденциальности хранимой на компьютере информации используются симметричные алгоритмы шифрования в связи с их высокой

эффективностью. Однако увеличение максимальной длины ключа в симметричных криптоалгоритмах обычно невозможно без внесения изменений в сам алгоритм. Поэтому дальнейшее увеличение надежности защиты данных этим способом становится невозможным.

Кроме криптографических методов защиты конфиденциальность может обеспечиваться путем блокирования доступа к файлу. Надежность данного метода основана на стойкости парольной защиты, позволяющей блокировать доступ к файлу для нелегитимного пользователя [5]. Однако «цена» взлома пароля в данном случае может быть резко снижена за счет использования заранее собранных данных о пользователе и методов атаки по словарю. Таким образом, данный метод в большинстве случаев не является достаточно надежным.

Исходя из этого, возникает задача объединения двух вышеизложенных методов защиты таблиц соответствия обезличенных данных в рамках единого метода, обеспечивающего большую надежность защиты ПДн и основанного на соблюдении принципов многорубежности и системности.

Решение задачи

Схема с последовательным применением криптографии и блокирования

При последовательном применении криптографического преобразования и блокирования доступа к таблицам соответствия работа системы защиты осуществляется следующим образом.

Исходный файл шифруется с помощью криптографического алгоритма и сохраняется на электронном носителе. После чего незашифрованный вариант безвозвратно удаляется многократной перезаписью, например, с помощью программного продукта, описанного в [1], с целью обеспечения невозможности его восстановления по остаточной намагниченности специальными средствами [2]. Далее осуществляется блокирование доступа к зашифрованному файлу.

Для получения исходной таблицы соответствия легальный пользователь должен сначала ввести пароль для разблокирования, потом ключ для расшифрования. Злоумышленнику же понадобится подобрать пароль, после чего подвергнуть криптоанализу зашифрованный файл.

Таким образом, в данном случае общее время, необходимое для получения НСД к таблице соответствия, а, следовательно, и к ПДн пациентов, будет определяться по следующей формуле:

$$T_{\text{послед}} = t_{\text{б}} + t_{\text{к}}, \qquad (1)$$

где $t_б$ – время, затрачиваемое на подбор пароля для снятия блокирования, а $t_к$ – время, затрачиваемое на взлом криптосистемы.

Как видно из формулы (1), общее время, затрачиваемое злоумышленником для получения НСД, равно сумме времен, необходимых для преодоления каждого из рубежей защиты. В данном случае механизмы защиты не объединены в систему, так как между ними нет взаимосвязи. Несоблюдение принципа системности приводит к отсутствию синергетического эффекта, который мог бы усилить надежность защиты ПДн.

Для устранения данного недостатка предлагается следующая схема объединения указанных методов в единую систему защиты информации.

Схема обеспечения конфиденциальности с синергетическим эффектом

В отличие от последовательной схемы, в схеме с синергетическим эффектом после шифрования вычисляется хэш-функция зашифрованного файла, которая записывается на съемный носитель и хранится в секрете (рис. 1).

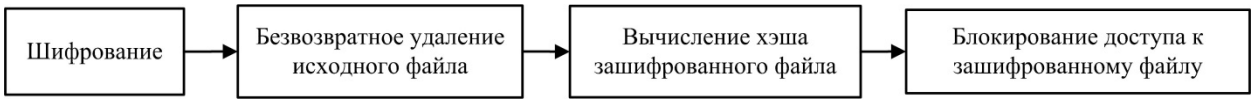

Рис. 1. Схема с синергетическим эффектом

Процедура получения доступа к исходному файлу показана на рис. 2. Она включает в себя следующие шаги:

1. Получение доступа к *зашифрованному* файлу.

1.1. Пользователь вводит пароль доступа к зашифрованному файлу.

1.2. Производится анализ введенного пароля.

1.2.1. Если пароль введен корректно, то пользователю предоставляется доступ к зашифрованному файлу и начинается его расшифрование (п.2).

1.2.2. Если пароль введен некорректно, то пользователь получает отказ в доступе и файл случайное число раз изменяется с помощью обратимых преобразований. При этом секретом являются не сами преобразования, а их количество. Оно неизвестно никому, в том числе и легальному пользователю.

2. Расшифрование файла.

2.1. Сравнение хэш-функции, хранимой в секрете, с хэш-функцией файла, к которому обращается пользователь.

2.1.1. Если хэш-функции совпадают, то файл пригоден для расшифрования, которое осуществляется после ввода ключа.

2.1.2. Если хэш-функции не совпадают, то необходимо произвести обратное п.1.2.2 преобразование файла и вернуться к пункту 2.1. Таким образом, злоумышленник, не

владея хэш-функцией зашифрованного файла, будет вынужден «взламывать» криптосистему после каждого обратного преобразования.

При использовании данной схемы защиты общее время получения НСД к файлу определяется следующим образом. Пусть n_{min}и n_{max} – соответственно минимальное и максимальное количества преобразований, производимых над таблицей соответствия, при одной неудачной попытке разблокировать файл, K – количество введенных пользователем вариантов пароля.

Тогда после каждого неверного ввода пароля файл может находиться в одном из N состояний, где $N = n_{max} - n_{min}$. Следовательно, время, необходимое для получения НСД, в данном случае составит

$$T_{синерг} = t_б + K*N*t_к = T_{послед} + (K*N - 1) *t_к \qquad (2).$$

Таким образом, как видно из формул (1) и (2) в случае использования схемы с синергетическим эффектом общее время необходимое для получения НСД увеличивается на величину

$$\Delta T = T_{синерг} - T_{послед} = (K*N - 1) *t_к . \qquad (3)$$

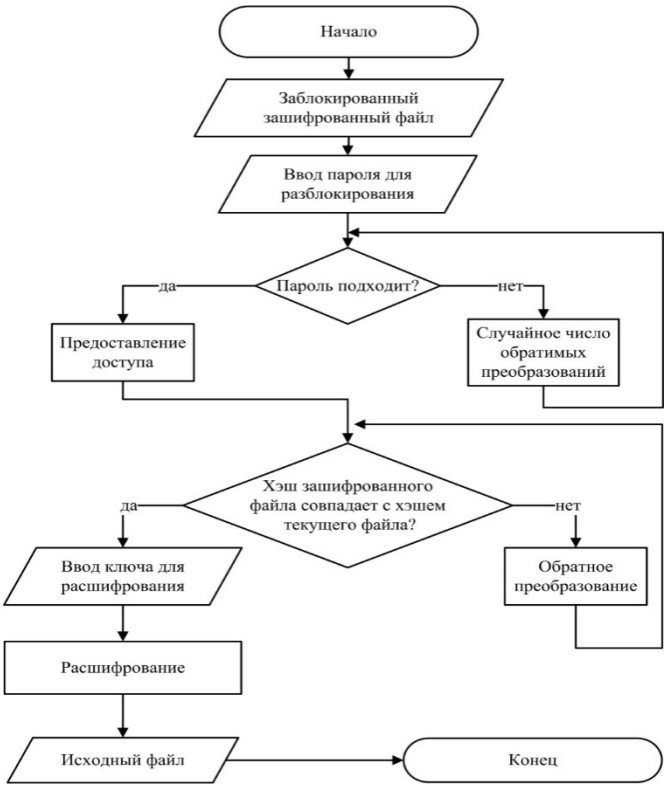

Рис. 2. Получение доступа к исходному файлу

Выводы

Таким образом, применение системного подхода позволило разработать схему использования механизмов криптографической защиты и блокирования доступа к файлу, обладающую синергетическим эффектом и позволяющую увеличить надежность защиты

персональных данных пациентов. Предложенная схема может быть положена в основу соответствующего программного продукта.

Список литературы

1. Ажмухамедов И.М., Переверзева Р.Ю. Безопасное удаление файлов. // Свидетельство о государственной регистрации программ для ЭВМ №2012615468. Зарегистрировано в реестре программ для ЭВМ 18 июня 2012 г.
2. Ардатов В.И. Безвозвратное удаление информации // http://avicorp.ru/index.php?option=com_content&view=article&id=30%3Abud1&catid=2%3Akstat&Itemid=9&lang=ru(дата обращения: 25.03.2015).
3. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. – С.-П.: Лань, 2000. – 224 с.
4. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке С. – М.: Триумф, 2002. – 816 с.
5. Компьютерная безопасность. Вопросы и решения. // http://comp-bez.ru/?p=5 (дата обращения: 25.03.2015).

Рецензенты:

Попов Г.А., д.т.н., профессор, заведующий кафедрой «Информационная безопасность», ФГБОУ ВПО АГТУ, г. Астрахань;

Лихтер А.М., д.т.н., доцент, зав. кафедрой «Общей физики», ФГБОУ ВПО АГУ, г. Астрахань.