УДК 004.056:614.2

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИЯХ ЗДРАВООХРАНЕНИЯ

[1, 2] Е.А.Каршакевич, [1] Г.Н.Здор

[1] Белорусский национальный технический университет,
пр. Независимости, 65, 220013, г. Минск, Республика Беларусь
[2] 19-я центральная районная поликлиника Первомайского района г. Минска,
пр. Независимости, 119, 220114, г. Минск, Республика Беларусь

В статье рассматриваются общие вопросы построения политики информационной безопасности при эксплуатации информационных систем медицинского назначения в организациях здравоохранения. Описаны основные методики, применяемые для обеспечения информационной безопасности, даны соответствующие пояснения с учетом сложившегося практического опыта.

Ключевые слова: информационная безопасность; защита информации; медицинские информационные системы.

Деятельность организаций здравоохранения (ОЗ) направлена на оказание доступной и качественной медицинской помощи для сохранения и укрепления здоровья населения. Одним из методов, позволяющих улучшить качество и доступность медицинской помощи, а также упорядочить ведение медицинской документации и документооборот в ОЗ, является внедрение информационных технологий в повседневную практику специалистов всех структурных подразделений. Применение информационных технологий в ОЗ позволяет упорядочить весь процесс обработки, хранения и обмена данными, но, в то же время, реализация процессов информатизации требует решения ряда злободневных вопросов.

Среди актуальных вопросов, стоящих как перед отдельно взятыми ОЗ, так и перед всей системой в целом, можно выделить следующие: создание единого информационного пространства (инфраструктуры) для всех заинтересованных сторон (пациентов, медицинских работников, организаций и органов управления здравоохранением и т.д.); укрепление и совершенствование материально-технической базы; обеспечение информационной безопасности в соответствии с современными требованиями.

Медицинская информация всегда была закрытой, а в условиях современных проектов, связанных с централизованным обменом и обработкой данных о пациентах, и вовсе представляет собой информацию ограниченного распространения. В связи с этим, вопросы информационной безопасности (ИБ) отрасли постепенно выходят на первый план.

Обеспечение ИБ в рамках отдельно взятой ОЗ требует особого внимания со стороны лиц, ответственных за ИБ, пользователей и администрации организаций здравоохранения. Основные свойства информации и систем ее обработки, которые должны поддерживаться в информационно-вычислительных системах (ИВС):

целостность информации – способность системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения);

конфиденциальность информации – субъективно определяемая характеристика информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на доступ к ней;

доступность информации – способность системы обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации [1].

Системы управления базами данных, в особенности реляционные СУБД, стали доминирующим инструментом в здравоохранении. Обеспечение информационной безопасности СУБД приобретает решающее значение при выборе конкретного средства обеспечения необходимого уровня безопасности организации в целом.

Работоспособность ИВС может быть нарушена вследствие воздействий различной природы. Безопасность достигается принятием определенных мер по обеспечению конфиденциальности, це-

лостности и доступности информации. Организации здравоохранения определяют приемлемые для себя методы из множества существующих, которые складываются в политику информационной безопасности ОЗ.

Политика информационной безопасности организации – это совокупность документированных управленческих решений, направленных на защиту информации и ассоциируемых с ней ресурсов. Политика безопасности определяет стратегию управления в области информационной безопасности, а также ту меру внимания и количества ресурсов, которые считает целесообразным выделить на эти цели руководство [2]. В политике информационной безопасности излагаются руководящие принципы использования сотрудниками информационных ресурсов организации и предусмотрена ответственность пользователей в случае их нарушений.

Существует ряд методов, которые могут быть применимы на практике с целью обеспечения ИБ в ОЗ, работающих с медицинскими информационными системами (МИС).

Аутентификация пользователей используется для обеспечения того, чтобы лицо, получающее доступ к информации, действительно было тем, кем они себя представляют. Например, наиболее распространенной формой аутентификации пользователей в ИВС и в МИС сегодня является идентификатор пользователя и пароль. В этом случае аутентификация выполняется путем подтверждения того, что пользователь их (идентификатор и пароль) знает. Но эта форма аутентификации зачастую легко может быть скомпрометирована, да и в случае работы с закрытой информацией необходимы более сильные формы аутентификации.

Рассуждая о безопасности паролей, необходимо ввести правильные политики паролей, чтобы гарантировать, что пароли не могут быть скомпрометированы. Например, пароль не должен быть простым или быть словом, которое можно найти в словаре. В современной практике политики паролей рекомендуется использовать как минимум восемь символов и, по крайней мере, одну букву верхнего регистра, один специальный символ и одну цифру. Очень важно, чтобы пользователи меняли свои пароли на регулярной основе каждые 60–90 дней. В то же время, в реальных условиях, требования к паролю должны быть доступными для запоминания, чтобы пользователю не пришлось его записывать. Необходимо постоянно проводить обучение сотрудников не разглашать пароли.

Другой метод – это идентификация пользователя с применением носителя ключевой информации, но он также может быть проблематичным, например, когда этот идентификационный носитель потерян или украден.

Метод, который гораздо сложнее скомпрометировать, – это идентификация пользователя с использованием физических характеристик, таких как сканирование глаз или отпечаток пальца.

Более безопасный способ аутентификации пользователя – многофакторная аутентификация, которая заключается в том, что кроме знания пароля (или PIN-кода) необходимо еще и наличие физического ключа.

После аутентификации пользователя следующий шаг – ***разграничение уровней доступа пользователей*** к соответствующим информационным ресурсам. Это делается с помощью контроля доступа, который определяет, какие пользователи имеют право читать, изменять, добавлять и/или удалять информацию, и разделением доступа к ресурсам путем деления сети на части. Для каждого информационного ресурса, которым организация хочет управлять, может быть создан список управления доступом пользователей (ACL), которые могут предпринимать конкретные действия. Если пользователя нет в списке, у него нет возможности даже знать, что существует информационный ресурс. Списки ACL просты в понимании и обслуживании. Однако, у них есть несколько недостатков. Основной недостаток заключается в том, что каждый информационный ресурс управляется отдельно, поэтому, если необходимо добавить или удалить пользователя из нескольких информационных ресурсов, то это было бы довольно сложно, и, по мере увеличения количества пользователей и ресурсов, поддержка ACL становится сложнее. Поэтому метод управления доступом усовершенствован, и организован контроль доступа на основе ролей или RBAC. В RBAC, вместо предоставления определенным пользователям прав доступа к информационному ресурсу, пользователи назначаются ролям, а затем этим ролям назначается доступ. Это позволяет осуществлять управление пользователями и ролями по отдельности, упрощая администрирование и, соответственно, улучшая безопасность.

В случаях передачи закрытой информации по каналам связи или посредством цифровых носителей даже при правильной проверке подлинности и управлении доступом несанкционированное лицо может получить доступ к данным. ***Шифрование*** – это процесс кодирования данных при их передаче или хранении, чтобы с ними могли ознакомиться только уполномоченные лица.

Шифрование выполняется компьютерной программой, которая кодирует данные, которые необходимо передать; получатель получает шифрованный текст и декодирует его (дешифрование). Отправителю и получателю необходимо согласовать метод кодирования, чтобы обе стороны могли правильно общаться. Обе стороны используют ключ шифрования, позволяющий им кодировать и декодировать сообщения друг друга. Такой тип шифрования с симметричным ключом несовершенен с точки зрения информационной безопасности, так как ключ доступен в двух разных местах.

Альтернативой *симметричному шифрованию* ключей является шифрование с открытым ключом – *асимметричное шифрование*. В шифровании с открытым ключом используются два ключа: открытый ключ и закрытый ключ. Чтобы отправить зашифрованное сообщение, вы получаете открытый ключ, кодируете сообщение и отправляете его. Затем получатель использует закрытый ключ для его декодирования. Открытый ключ может быть предоставлен всем, кто желает отправить получателю сообщение. Каждому пользователю просто нужен один закрытый ключ и один открытый ключ для защиты сообщений. При внедрении шифрования данных необходимо предусмотреть *управление криптосредствами*, в частности, криптоключами (ключевая инфраструктура) [2].

В условиях перехода от бумажного носителя в электронному важно спланировать и реализовать резервное копирование данных. Необходимы не только резервное копирование данных на серверах, но и резервные копии ключевых компьютеров. Для реализации ***плана резервного копирования*** необходимо определить:

полный перечень информационных ресурсов организации, которые должны быть скопированы, и выбрать лучший способ восстановления данных. Некоторые данные могут храниться на серверах, другие данные – на жестких дисках пользователей, некоторые – в облаке, а некоторые – на сторонних ресурсах;

расписание и частоту резервного копирования данных в зависимости от их значимости, скорости их изменения и с учетом возможности восстановления данных без потерь или с минимальными потерями;

возможность хранения резервных данных в удаленном месте на случай внештатных ситуаций, повлекших полное уничтожение основных носителей информации организации;

план проверки резервных копий путем восстановления, что гарантирует, что процесс резервного копирования работает в нормальном режиме.

Также для повышения надежности информационных ресурсов необходимо использовать ***сетевые экраны*** (брандмауэр). Брандмауэр может быть исполнен как аппаратное устройство или программное обеспечение (или и то, и другое). *Аппаратный брандмауэр* – это устройство, которое подключено к сети и фильтрует пакеты на основе набора правил. *Брандмауэр программного обеспечения* работает в операционной системе и перехватывает пакеты по мере их поступления на компьютер. Брандмауэр регулирует поток трафика внутри сети. Возможно использование нескольких сетевых экранов для дополнительного контроля трафика внутри ИВС.

Для соединения основной ЛВС организации здравоохранения с ЛВС ее филиала или для связи между удаленными корпусами, лучше всего реализовать данный вид соединения с применением ***технологии виртуальных частных сетей (VPN)***. VPN позволяет пользователю, находящемуся за пределами корпоративной сети, совершить обход вокруг брандмауэра и получить доступ к внутренней сети извне. Благодаря сочетанию программного обеспечения и мер безопасности, это позволяет организации разрешить ограниченный доступ к своим сетям, в то же время, обеспечивая общую безопасность.

Другим устройством, которое может быть установлено в сети в целях дополнительной меры безопасности, является ***система обнаружения вторжений*** или IDS. IDS – это программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими.

Реализация ***физической безопасности*** – это защита аппаратных и сетевых компонентов, которые хранят и передают информационные ресурсы. Для обеспечения физической безопасности организация должна идентифицировать все уязвимые ресурсы и принять меры для обеспечения того, чтобы эти ресурсы не могли быть физически изменены или украдены.

При реализации ИБ МИС важно применять программное обеспечение реализующее ***антивирусную защиту*** от несанкционированного доступа и спама как на рабочих станциях, так и на серверах.

Для своевременного реагирования на все события, проходящие в ИС, аудита и восстановления информационной системы необходимо проводить ***событийное протоколирование***, которое включает в себя настройку выдачи логов, управление составом событий, по которым ведется про-

токолирование. Ведение логов позволяет восстановить очередность событий и найти уязвимости системы.

Помимо перечисленных выше технических средств и алгоритмов, организациям здравоохранения также необходимо ***своевременно актуализировать политики безопасности*** и применять их в качестве формы административного контроля. Фактически, эти политики должны стать отправной точкой при разработке общего плана обеспечения безопасности ИВС.

В общем случае обеспечение безопасности любой ИВС строится по определенному алгоритму (рис.) и предполагает постоянный, непрерывный процесс анализа информационных рисков и эффективности принятых мер по защите информации. *Анализ информационных рисков* – это процесс комплексной оценки защищенности информационной системы с переходом к количественным или качественным показателям рисков.

Весь комплекс принятых мер, направленных на обеспечение информационной безопасности в учреждении здравоохранения, должен быть «сбалансирован» так, чтобы пользователи МИС могли эффективно использовать в работе информационные технологии, а вся информация была защищена.

ЛИТЕРАТУРА

1. *Родичев, Ю.В.* Информационная безопасность: нормативно-правовые аспекты: учеб. пособие / Ю.В.Родичев. – СПб.: Питер, 2008. – 272 с.: ил. – С.23–25.
2. *Шаньгин, В.Ф.* Защита информации в компьютерных системах и сетях / В.Ф.Шаньгин. – М.: ДМК Пресс, 2012. – 592 с.: ил. – С.68–70, 531–532.

INFORMATION SECURITY POLICY IN HEALTHCARE ORGANIZATIONS

[1, 2] Ya.A.Karshakevich, [1] G.N.Zdor,

[1] Belarusian National Technical University, Nezavisimosti Ave. 65, 220013, Minsk, Republic of Belarus

Обеспечение безопасности информационной системы

[2] 19th Central Polyclinic of Pervomaisky District of Minsk City, Nezavisimosti Ave. 119, 220114, Minsk, Republic of Belarus

The article deals with general issues of the information security policy construction in the operation of medical information systems in healthcare institutions. The main techniques used to organize information security are described. The research paper presents corresponding explanations considering all the existing practical experience.

Keywords: information security; information protection; medical information systems.

Сведения об авторах:

Каршакевич Евгений Александрович, Белорусский национальный технический университет, факультет информационных технологий и робототехники, кафедра «Робототехнические системы», аспирант; УЗ «19-я центральная районная поликлиника Первомайского района г. Минска», инженер-электроник; тел.: (+37529) 5599046; e-mail: karshakevich.e@gmail.com.

Здор Геннадий Николаевич, д-р техн. наук, профессор; Белорусский национальный технический университет, факультет информационных технологий и робототехники, зав. кафедрой «Робототехнические системы».

Поступила 05.04.2017 г.