- Вторая линия состоит из разнообразных внутренних мониторов, контролирующих доступ и анализирующих деятельность пользователей уже допущенных в защищенную информационную среду пользователей.

При использовании данных сервисов и механизмов существует момент, когда аутентификация с помощью пароля или общего секрета защищает двух или более участников взаимодействующих в защищаемой информационной среде от нарушителей, но не защищает от нарушения осуществляемого друг перед другом (как вариант нарушения – использование чужих научных трудов). В этой ситуации необходимо применить более действенный способ, чем аутентификация на основе общего секрета. Как вариант решения данной проблемы можно предложить использование электронно-цифровой подписи.

Данная подпись должна обладать обязательными свойствами такими как:

- ЭЦП должна использовать уникальную информацию отправителя;
- ЭЦП должна зависеть от сообщения, которое она заверяет;
- ЭЦП должна легко генерироваться и проверяться.

Значительное увеличение за последние годы применяемых информационных технологий в деятельности вуза и, как следствие, расширение информационного пространства должны существенно расширить методы и способы, регулирующие вопросы информационной безопасности. Оптимальным решением вопроса при создании защищенной информационной среды вуза и организации дистанционного образования является использование удостоверяющих центров, обеспечивающих посредством электронно-цифровой подписи и защищенных каналов связи решение задач по обеспечению должного уровня безопасности.

Библиографический список

1. *Васильев В.И., Савина И.А., Шарипова И.И.* «Построение нечетких когнективных карт для анализа и управления информационными рисками вуза»/ Вестник ИГАТУ, т.10, № 2(27), с. 199-209

2. *Зуев В.Е.* «Безопасность электронного обучения», Международная конференция "Информационные технологии в образовании" "ИТО-Москва-2010".

Л.Ю. Овсяницкая

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК КЛЮЧЕВОЙ ВОПРОС ПОДГОТОВКИ СПЕЦИАЛИСТОВ ЗДРАВООХРАНЕНИЯ К РАБОТЕ В УСЛОВИЯХ ФОРМИРОВАНИЯ ЕДИНОЙ ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СРЕДЫ

larovs@rambler.ru

Уральский социально-экономический институт (филиал) ОУП ВПО «АТиСО», г. Челябинск

The article focuses on information security problems that need to pay attention during the computer science postgraduate medical education. The obtained knowledge will allow the doctors to use the advantages of the unified state information environment and to protect confidential personal and business information from the illegal distribution.

В 2011 г. утверждена Концепция создания единой государственной информационной системы в сфере здравоохранения. Основной целью создания системы является повышение качества оказания медицинской помощи на основе совершенствования информационно-технологического обеспечения медицинских и фармацевтических организаций.

Все данные о состоянии здоровья граждан России относятся к числу конфиденциальных. Защита персональных данных граждан в единой системе обеспечивается использованием

инфраструктуры открытых ключей электронной цифровой подписи (ЭЦП) и шифрования данных; обезличивания персональных данных, получаемых из медицинских информационных систем для централизованной обработки, передачи по каналам связи; использования организационных мер управления доступа к системе.

Обязательное последипломное образование врачей-организаторов здравоохранения предполагает занятия по информатике. На наш взгляд, ключевым вопросом, рассматриваемым на этом предмете, должна быть информационная безопасность. Любой аспект изучения информатики: новые программные и аппаратные медицинские комплексы, автоматизация документооборота, телемедицина, должны рассматриваться именно с точки зрения соответствия их современным нормам безопасности.

Большое внимание в Уральской государственной медицинской академии дополнительного образования уделялось автором обсуждению правовых, организационных и технических аспектов перехода к безбумажному документообороту, которые предполагают качественное изменение принципов работы. По нашему мнению, главной задачей данного раздела является формирование ответственного и серьезного отношения к цифровым ключам:

1. Собственноручная подпись у человека одна для любой ситуации. При работе с ЭЦП человек может иметь неограниченное количество ключей для удостоверения документов в разных организациях. При соблюдении установленных требований, все ключи будут являться аналогами собственноручной подписи.

2. Собственноручная подпись человека практически не меняется в течение жизни. Ключи ЭЦП должны меняться по истечении определенного времени. Однако всегда может возникнуть юридический спор относительно данного электронного документа. Поэтому закрытый ключ должен стираться с носителя с применением специальных программных средств или физически уничтожаться вместе с носителем, а открытый ключ должен тщательно храниться в течение времени исковой давности документа для обеспечения при необходимости аутентификации автора и для подтверждения подлинности и целостности документа.

3. Носитель закрытого ключа должен храниться в сейфе или запираемом шкафу и вставляться в соответствующий порт только в момент подписания документа; доступ к ключу должен иметь только его владелец; на носителе не должна храниться никакая посторонняя информация.

4. Математически подпись не поддается дешифровке в разумное время, однако, использование паролей, основанных на ассиметрии базовой секретной информации (содержащих личную информацию автора, сокращающую пространство подбора), значительно снижает криптостойкость алгоритма.

Таким образом, соблюдать элементарные организационные правила не сложно, и знания, полученные на занятиях, позволят специалистам здравоохранения как использовать все преимущества единой государственной информационной среды, так и обезопасить личную и профессиональную конфиденциальную информацию от незаконного распространения и хищения.