УДК: 004.056.53:614.253.84

*А.А. Каблуков, Н.А. Иванькова*

# ЗАЩИТА ПЕРСОНИФИЦИРОВАННОЙ ИНФОРМАЦИИ В МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

*Запорожский государственный медицинский университет*

***Ключові слова:*** *інформаційні системи, бази даних, персоніфікований захист, інформація, безпека, електронний доступ, ідентифікація, криптографія.*

***Ключевые слова:*** *информационные системы, базы данных, персонифицированная защита, информация, безопасность, электронный, доступ, идентификация, криптография.*

***Key words:*** *information systems, database, personalized information security, information, electronic access, authentication, cryptography, complex.*

Розглянуто методи комплексного захисту і безпеки інформації у медичних інформаційних і навчальних системах, запровадження яких у медичних установах України є складовою частиною Закону України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр.». Сформульовано вимоги до системи захисту персоніфікованих даних в електронних системах і загальні положення політики безпеки у сфері захисту інформаційних систем.

Рассмотрены методы комплексной защиты и безопасности информации в медицинских информационных и обучающих системах, внедрение которых в медицинских учреждениях Украины является составной частью Закона Украины «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр.». Сформулированы требования к системе защиты персонифицированных данных в электронных системах и общие положения политики безопасности в области защиты информационных систем.

The article deals with the methods of complex protection and safety of information in medical information and leaning systems. Their introduction in medical institutions of Ukraine is constituent of Law of Ukraine «Basic principles of information society development in Ukraine for 2007–2015». Requirements to the system of personalized data protection in electronic systems are formulated as well as general regulations of security policy in the sphere of information systems protection.

Успешность любого вида врачебной деятельности во многом зависит от степени обеспечения ее соответствующей длительно накопленной и систематизированной информацией о пациентах, их заболеваниях, методах и средствах лечения, а также от возможности и умения врача пользоваться подобной информацией в своей деятельности. Возможность быстрого получения такой информации дают компьютерные информационные системы.

Медицинские информационные системы (МИС) используются в странах Европы, частично внедрены и используются в России и других странах СНГ. Внедрение МИС в практику лечебных учреждений Украины – вопрос ближайшего времени.

Внедрение МИС, централизация и укрупнение медицинских баз данных, увеличение риска их потери и порчи неизбежно приведет к поиску наиболее надежных и безопасных решений по защите персонифицированной информации, поэтому при внедрении МИС должны быть предусмотрены методы комплексной защиты и безопасности информации. Это масштабная задача, т. к. информационная целостность является балансом между безопасностью и доступностью.

## ЦЕЛЬ РАБОТЫ

Анализ существующих угроз нарушения целостности и безопасности хранения информации в электронных базах данных; формулировка требований к системе защиты персонифицированных данных в электронных системах с учетом вероятных угроз; определение основных критериев для политики безопасности в области защиты медицинских информационных и обучающих систем в соответствии с законами Украины «О защите персональных данных» и «О защите информации в информационно-телекоммуникационных системах».

Преступность в сфере использования компьютеров во всех формах в последние годы имеет устойчивую тенденцию к увеличению и наносит большой вред [1]. По данным аудиторской комиссии Великобритании, почти 60% организаций, использующих информационные технологии, не имеют вообще никаких систем безопасности, защищающие компьютеры. Большинство фирм не делает даже внутренней ревизии своей деятельности, хотя, по оценкам экспертов, 25% компьютерных преступлений совершается именно внутри организации их собственными сотрудниками [2].

Одной из форм неправомерного использования компьютерной информации, которая наиболее часто встречается, являются манипуляции с использованием вычислительной техники [3]. Речь идет об изменениях данных в корыстных целях. При этом, как правило, используются неверные данные. Манипуляции с данными могут осуществляться на всех этапах обработки:

- на этапе ввода информации – ввод неверных данных;
- на этапе обработки данных;
- на этапе вывода информации – фальсификация результата обработки информации.

Опасность этих манипуляций заключается в технической сложности ЭВМ, очень сложном процессе выявления манипуляций с данными.

При выборе средств и методов защиты персонифицированной медицинской информации необходимо учесть опыт защиты информации и электронных баз данных банковскими и силовыми структурами [4,15,16]. Приоритетным в этих структурах являются схемы компьютерных сетей с центральным сервером. Используются два подхода к построению защиты электронных систем: фрагментарный – противодействие определенным угрозам при определенных условиях (например, специализированные антивирусные средства, автономные средства шифрования и т. д.); и комплексный подход – создание защитной среды обработки информации, объединяющей разнородные меры противодействия угрозам (физические, организационные, программно-технические). Комплексный подход применяют для защиты больших систем (например, SWIFT) или небольших систем, которые обрабатывают важную информацию или выполняют ответственные задачи.

При физическом обеспечении защиты компьютерной информации на первом плане стоит выбор места, на котором находится соответствующий компьютер, в нашем случае, сервер медицинского учреждения (организации). Контроль за несанкционированным проникновением в помещение, где находится сервер (специально охраняемые окна и двери, устройства аварийной сигнализации, камеры контроля и т. п.), должен обеспечиваться автоматически. Наиболее надежным при защите компьютера от несанкционированного доступа является так называемый «шлюз доступа». При этом вестибюль, к которому непосредственно примыкает помещение с сервером, оборудуется соответствующими техническими средствами контроля. Во-вторых, доступ к компьютеру становится возможным только при наборе определенного кода (числовой код или магнитная карточка при входе в помещение). Защита при наличии шлюза доступа дополняется установкой видеоконтролирующего устройства, доступного дежурному.

При организационном обеспечении защиты информации одной из организационных мер является разделение функций на большое количество функциональных участков, которыми занимаются разные сотрудники. При организационных мероприятиях осуществляется регулярная смена персонала в пределах области задач. Таким образом, отдельный сотрудник не может объективно оценить, насколько он способен осуществить манипуляции с информацией, что является сдерживающим фактором для недобросовестных сотрудников.

Программно-техническая защита информации носит предупредительный характер [5]. Он осуществляется соответствующей программой или определенными программными средствами, включающими:

1) Проверку на приемлемость. Программа, которая устанавливается в соответствующую область программного обеспечения сервера. В рамках проверки приемлемости программа должна «подавать сигнал тревоги», если, например, введена заработная плата выше реальной, этот факт должен быть раскрыт программой или просто не поддаваться обработке;

2) Защиту ввода данных. Сначала сотрудник, имеющий право на ввод данных, должен ввести свой числовой код, после чего он получает доступ к самому процессу обработки данных. При этом соответствующая программа в виде протокола регистрирует и записывает, кто, когда и какие операции по обработке данных сделал.

Также к основным методам программно-технической защиты информации можно отнести:

*Идентификация* (узнавание). Это средство наиболее часто используется в арсенале защиты компьютерной информации. Идентификация обычно позволяет или не позволяет доступ данного пользователя в сеть или компьютер. Процедура происходит с помощью пароля, который должен знать только законный пользователь. Все современные парольные схемы полагаются на шифровальную технологию, не допускает выхода паролей в сеть, где они могут быть расшифрованы.

*Криптография* (шифрование) – технология, позволяющая хранить информацию в секрете. Эта область чрезвычайно специализированная и находится в постоянном развитии. Подробные материалы по текущим тенденциям в криптографии могут быть найдены в некоторых специализированных разделах сети INTERNET.

Цифровые сигнатуры используются в криптографической технике. Их задача – подтвердить, что объект (документ) не изменен.

*Ручные идентификаторы* представляют собой устройства размером в кредитную карту, которые могут делать специализированные криптографические расчеты. Конечно, когда пользователь входит в систему, сервер выдает цифровую последовательность (так называемое «требование» – challenge), которое появляется на экране [6]. Пользователь вводит это требование в свой идентификатор, дает ответ также в виде цифровой последовательности, используемой как пароль. Поскольку для того, чтобы воспользоваться ручным идентификатором, необходимо ввести свой персональный номер (PIN), утерянный идентификатор не может быть использован другими лицами. Точно так же, если администратор удалил идентификатор у пользователей, то его доступ в сеть прекращается автоматически и немедленно.

*К дополнительным мерам* повышения информационной безопасности можно отнести:

- установление служебной ответственности сотрудников за несанкционированный доступ к программам или данным;

- разработка порядка идентификации пользователя и контроля за доступом к информации, осуществление технического обслуживания компьютерной сети;

- определение порядка рассмотрения инцидентов и проведения контрольных проверок с целью установления, что подключение к INTERNET не противоречит политике безопасности;

- обучение персонала вопросам безопасности;

- кодирование информации перед введением в сеть для обеспечения конфиденциальности в процессе движения по сети INTERNET. Проверка целостности информации и детальных оценок ее источники могут подтвердить, что

она не была искажена в процессе передачи;

- использование программных и других средств для оценки технической уязвимости и устранения выявленных недостатков с точки зрения безопасности передачи данных;

- подбор кадров для разработки, внедрения и обслуживания компьютерной техники, включая тщательное изучение рекомендаций и проверку кандидатов на ответственные должности.

**ВЫВОДЫ**

В результате анализа специализированной литературы и технической документации сформулированы требования к системе защиты персонифицированных данных в электронных системах с учетом вероятных угроз, а также общие положения политики безопасности в области защиты медицинских информационных систем.

**СПИСОК ЛИТЕРАТУРЫ**


1. *Біленчук П.Д.* Організована транснаціональна комп'ютерна злочинність: глобальна проблема третього тисячоліття / *Біленчук П.Д.* – Режим доступу: http://www.crime-research.ru/library/Bilukr.htm
2. *Голубєв В.* Деякі особливості тактики окремих слідчих дій при розслідуванні комп'ютерних злочинів – Режим доступу: http://www.crime-research.ru/library/Golubev0105.html
3. *Шеломенцев В.П.* Протидія злочинності у сфері інформаційно-комунікаційних технологій / *Шеломенцев В.П.* – Режим доступа: http://mndc.naiau.kiev.ua/Gurnal/9text/g9_25.htm/
4. *Вертузаев Н.С., Голубев В.А., Котляревский А.И., Юрченко А.Н.* Безопасность компьютерных систем: преступность в сфере компьютерной информаци и ее предупреждение / *Вертузаев Н.С., Голубев В.А., Котляревский А.И., Юрченко А.Н.*; под общ. ред. д.ю.н. А.П. Снигерева. – Запорожье, 1998. – 316 с.
5. Додаток до декларації про конфіденційність служби Windows Live – Режим доступу: http://privacy.microsoft.com/uk-ua/windowslive.mspx.
6. Словарь Хак Терминов – Режим доступа: http://hackwiki.org/
7. *Вєртузаєв М.С.* Захист інформації в комп'ютерних системах від несанкціонованого доступу: Навч. посібник / *Вєртузаєв М.С., Юрченко О.М.; за ред. С.Г. Лаптєва*. – К.: Видавництво Європейського університету, 2001. – 201 с.
8. *Петраков А.В.* Основы практической защиты информации / *Петраков А.В.* – М.: Радио и связь, 1999. – 386 с.
9. *Романец Ю.В.* Защита информации в компьютерных системах и сетях / *Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф.* – М: Радио и связь, 2001.
10. Компьютерная преступность и кибертерроризм: Сборник научных статей / Под ред. *Голубева В.А., Ахтырской Н.Н.* – Запорожье: Центр исследования компьютерной преступности, 2004. – Вып. 1. – 326 с.
11. *Хорошко В.А., Чекатов А.А.* Методы и средства защиты информации – Режим доступа: www.junior.com.ua
12. *Барабаш А.В.* История криптографии. Ч. 1. / *Барабаш А.В., Шанкин Г.П.* – М.: Гелиос АРВ, 2002. – 240 с.
13. Закон Украины «О защите персональных данных».
14. Закон Украины «О защите информации в информационно-телекоммуникационных системах».
15. Наказ МВС України № 737 від 19 серпня 2001 р. «Про затвердження Типового положення про підрозділи ДСБЕЗ по боротьбі з правопорушеннями у сфері інтелектуальної власності та високих технологій».
16. Наказ МВС України № 429 від 31 травня 2001 р. «Про створення у структурі ДСБЕЗ підрозділів по боротьбі з правопорушеннями у сфері інтелектуальної власності та високих технологій».



***Сведения об авторах:***

Каблуков А.А., к. тех. н., доцент каф. медицинской и фармацевтической информатики ЗГМУ.

Иванькова Н.А., к. пед. н., доцент каф. медицинской и фармацевтической информатики ЗГМУ.