УДК: 004.056

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Алиева М.С.[1], Богданов С.И.[2]
[1-2] ФГБОУ ВО «Уральский государственный медицинский университет» Минздрава России, Екатеринбург, Российская Федерация
[2]madinka.alieva588@mail.ru

Аннотация

Введение. Системы защиты информации могут помочь решить проблему нарушений целостности и конфиденциальности ресурсов.

Прогресс в новейших информационных технологиях делает весьма уязвимым любое общество. Активное развитие информационных технологий обуславливает актуальность изучения проблем информационной безопасности. В данной статье представлен обзор на информационную безопасность пользователей. Процесс цифровизации захватил и здравоохранение как отрасль экономики. В силу этого обстоятельства вопросы информационной безопасности весьма актуален для медицинской практики. **Цель исследования** – провести анализ данных о различных видах защиты информации в здравоохранении. **Материалы и методы**. Нами были изучены данные научных материалов и реальных моделей информационной безопасности в здравоохранении. **Результаты**. Когда вы идёте на осознанное нарушение в информационной безопасности, вы должны хорошо понимать последствия. К примеру, многие данные в медучреждениях попадают в категорию врачебной тайны, здесь же хранятся персональные данные, причем как клиентов, так и сотрудников. Поэтому уровень информационной безопасности в каждом медицинском учреждении просто обязан быть самым высоким, защита данных — надежной, а подход к работе с данными, их хранению и обработке должен быть проработанным до самых мелочей. **Обсуждение.** Анализ угроз и систем защиты информационной безопасности позволяет избежать компьютерные преступления.

Выводы. В ходе исследования были проанализированы особенности информационной безопасности. **Ключевые слова:** информационная безопасность, IT в здравоохранении.

Absctract

Modern society is called information society. Thanks to new information technologies, the production and non-production activities of a person, his everyday sphere of communication is expanding without limit due to the involvement of experience, knowledge and spiritual values developed by world civilization, and the economy itself is less and less characterized as the production of material goods and more and more - as the dissemination of information. products and services. Progress in the latest information technologies makes any society very vulnerable. The active development of information technologies determines the relevance of studying the

problems of information security. This article provides an overview on the information security of users. The digitalization process has also captured healthcare as a branch of the economy. Due to this circumstance information security issues are very relevant for medical practice. **The aim of the study** - is to analyze data on various types of information security in healthcare. **Materials and methods.** We have studied the data of scientific materials and real models of information security in healthcare. **Results.** When you make a deliberate breach in information security, you must understand the consequences well. For example, many data in medical institutions fall into the category of medical secrecy, and personal data is stored here, both clients and employees. Therefore, the level of information security in each medical institution simply must be the highest, data protection must be reliable, and the approach to working with data, storing and processing it must be worked out to the smallest detail. **Discussion.** Analysis of threats and information security protection systems helps to avoid computer crimes. **Findings.** In the course of the study, the features of information security were analyzed. **Key words:** information security, IT in healthcare.

ВВЕДЕНИЕ

С развитием человеческого общества, появлением частной собственности, государственного строя, борьбой за власть и дальнейшим расширением масштабов человеческой деятельности информация приобретает цену. Ценной становится та информация, обладание которой позволит ее существующему и потенциальному владельцам получить какой-либо выигрыш: материальный, политический, военный и т. д. [1]. Еще 25-30 лет назад задача защиты информации могла быть эффективно решена с помощью организационных мер и отдельных программно-аппаратных средств разграничения доступа и шифрования. Появление локальных и глобальных сетей, спутниковых каналов связи, эффективной технической разведки и конфиденциальной информации существенно обострило проблему защиты информации. Проблема надежного обеспечения сохранности информации является одной из важнейших проблем современности [2]. В большинстве коммерческих и государственных организаций, не говоря о простых пользователях, в качестве средств защиты используются только антивирусные программы и разграничение прав доступа пользователей на основе паролей. Деятельность любой организации в наше время связана с получением и передачей информации. Информация в настоящее время является стратегически важным товаром. Потеря информационных ресурсов или завладение секретной информацией конкурентами, как правило, наносит предприятию значительный ущерб и даже может привести к банкротству [2].

Главный тренд последнего десятилетия - цифровизация в сфере здравоохранения, которая повышает эффективность оказания медицинских услуг. Но такая цифровизация имеет и обратную сторону — повышаются риски нарушения информационной безопасности, когда информация из электронных баз данных больниц и клиник используют в корыстных целях. В связи с этим

вопросы защиты информации и индивидуальных данных о пациентах является важнейшим в настоящее время [3].

Системы защиты информации могут помочь решить проблему нарушений целостности и конфиденциальности ресурсов.

Цель исследования – провести анализ данных о различных видах защиты информации в здравоохранении.

МАТЕРИАЛЫ И МЕТОДЫ

Нами были изучены данные научных материалов и реальных моделей информационной безопасности в здравоохранении.

РЕЗУЛЬТАТЫ

Когда вы идёте на осознанное нарушение в информационной безопасности, вы должны хорошо понимать последствия. Бесполезно писать регламенты, заставлять, наказывать людей за то, что их пароли слишком простые. Если человек не понимает почему пароль должен быть сложным, длинным, не понимает почему его нельзя клеить на монитор или класть на рабочий стол – бесполезно действовать силой. Точно также, абсолютно, не нужны никакие регламенты, если человек понимает последствия от тех или иных нарушений в области информационной безопасности. Люди в целом доверчивы, не обращают на детали, вся суть в мелочах.

К примеру, многие данные в медучреждениях попадают в категорию врачебной тайны, здесь же хранятся персональные данные, причем как клиентов, так и сотрудников. Сведения о состоянии здоровья — одни из самых интимных, их разглашение может привести ко многим негативным последствиям. Если кто-то получит доступ к такой информации и захочет использовать ее для своих личных выгод, он сможет причинить ощутимый вред людям. Например, хакеры могут продавать украденные данные на черном рынке или использовать их в мошеннических целях, а также шантажировать организации, допустившие утечку данных. Поэтому уровень информационной безопасности в каждом медицинском учреждении просто обязан быть самым высоким, защита данных — надежной, а подход к работе с данными, их хранению и обработке должен быть проработанным до самых мелочей.

Информационная безопасность — состояние сохранности информационных ресурсов и защищенности законных прав личности и общества в информационной сфере.

Информационная безопасность делится на основных 3 блока:

- Документальный блок, то есть это регламенты, политики, документы и т.д. Очень важный блок, казалось бы, это бумажки, которые не могут защитить организацию от хакерской атаки, но зачастую они позволяют систематизировать эту работу на предприятии

- Второй блок, аппаратно-программная составляющая информационной безопасности, обычно об этом говорят с системными администраторами, говорят об уязвимостях в аппаратной части, то есть в межсетевых экранах, системы обнаружения вторжений. Соответственно, программные части: антивирусы, системы контроля, которые обеспечивают информационную безопасность на аппаратно-программном уровне

- И третий блок, ключевой блок - информационная безопасность пользователей, то есть сотрудников, об этом можно говорить в ракурсе своей личной информационной безопасности и также информационной безопасности на предприятии.

К объектам информационной безопасности на предприятии относят:

- информационные ресурсы, содержащие сведения, отнесенные к коммерческой тайне, и конфиденциальную информацию, представленную в виде информационных массивов и баз данных;

- средства и системы информатизации - средства вычислительной и организационной техники, сети и системы, общесистемное и прикладное программное обеспечение, автоматизированные системы и т.д.

Угрозы информационной безопасности:

1. Уничтожение информационных объектов
2. Утечка информации
3. Искажение информации
4. Блокирование объекта информации

Попытка реализации угрозы называется атакой.

Один из способов проведения атаки – вредоносное ПО, так называются программы, предназначенные для незаконного доступа к информации, для скрытого использования компьютера или для нарушения работы компьютера, и компьютерных связей.

Методы обеспечения информационной безопасности:

- программные средства защиты – это самый распространённый метод защиты информации в компьютерах и информационных сетях. Обычно они применяются при затруднении использования некоторых других методов и средств. Проверка подлинности пользователя обычно осуществляется операционной системой. Пользователь идентифицируется своим именем, а средством аутентификации служит пароль.

- криптография - это тайнопись, система изменения информации с целью её защиты от несанкционированных воздействий, а также обеспечения достоверности передаваемых данных.

- электронная подпись

Цифровая подпись представляет последовательность символов. Она зависит от самого сообщения и от секретного ключа, известного только подписывающему это сообщение.

- биометрические методы защиты

Биометрические системы позволяют идентифицировать человека по присущим ему специфическим признакам, то есть по его статическим (отпечаткам пальцев, роговице глаза, форме руки и лица, генетическому коду, запаху и др.) и динамическим (голосу, почерку, поведению и др.) характеристикам. Уникальные биологические, физиологические и поведенческие характеристики, индивидуальные для каждого человека. Они называются биологическим кодом человека.

- сетевые методы защиты

техническим устройством эффективной защиты в компьютерных сетях является маршрутизатор. Он осуществляет фильтрацию пакетов передаваемых данных. В результате появляется возможность запретить доступ некоторым пользователям к определённому «хосту», программно осуществлять детальный контроль адресов отправителей и получателей. Так же можно ограничить доступ всем или определённым категориям пользователей к различным серверам, например, ведущим распространение противоправной или антисоциальной информации (пропаганда насилия и т.п.).

Например, В РФ создают Единую государственную информационную систему в сфере здравоохранения (ЕГИСЗ). Согласно проекту ЕГИСЗ, сейчас выполняются следующие работы:

- создаются региональные программы модернизации здравоохранения;
- медучреждения оснащают телекоммуникационным и компьютерным оборудованием, а также средствами информационной безопасности;
- вводятся стандарты информационного обмена в пределах системы;
- создается федеральный центр обработки данных.

149-ФЗ «Об информации, информационных технологиях и о защите информации»

149-ФЗ — главный закон об информации в России. Он определяет ключевые термины, например, говорит, что информация — это любые данные, сведения и сообщения, представляемые в любой форме. Также там описано, что такое сайт, электронное сообщение и поисковая система. Именно на этот закон и эти определения нужно ссылаться при составлении документов по информационной безопасности.

В 149-ФЗ сказано, какая информация считается конфиденциальной, а какая — общедоступной, когда и как можно ограничивать доступ к информации, как происходит обмен данными. Также именно здесь прописаны основные требования к защите информации и ответственность за нарушения при работе с ней.

ОБСУЖДЕНИЕ

Анализ угроз и систем защиты информационной безопасности позволяет избежать компьютерные преступления.

Зная все возможные угрозы информационной безопасности, человек способен предотвратить последствия деятельности хакеров.

Методы информационной безопасности позволяют защитить информационные ресурсы как организациям, так и простым пользователям.

Опираясь на закон «Об информации, информационных технологиях и о защите информации» можно понять какая информация является конфиденциальной, а какая информация доступна всем.

ВЫВОДЫ

В ходе исследования были проанализированы особенности информационной безопасности.

1. Проблема надежного обеспечения сохранности информации является одной из важнейших проблем современности.

2. В наше время злоумышленники могут получить доступ не только к открытой информации, но и к информации, содержащей государственную и коммерческую тайну. Особенно это касается защиты личных данных больных.

СПИСОК ИСТОЧНИКОВ

1. Введение – Безопасность и управление доступом в информационных системах https://studref.com/482324/informatika/vvedenie
2. Актуальность информационной безопасности, понятия и определения https://zdamsam.ru/a60323.html
3. Информационная безопасность в здравоохранении – особенности защиты https://www.smart-soft.ru/blog/informatsionnaja_bezopasnost_v_zdravoohranenii/
4. Introduction to information security [Электронный ресурс]: https://af.attachmail.ru/cgi-bin/readmsg/%D0%92%D0%B2%D0%B5%D0%B4%D0%B5%D0%BD%D0%B8%D0%B5+%D0%B2+%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%83%D1%8E+%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C.mp4?x-email=madinka.alieva588@mail.ru&rid=421370468190300019838798706784077489098&&id=1649072254085612978 6%3B0%3B1&notype=1&x-email=madinka.alieva588%40mail.ru (дата обращения: 08.04.2022)

Сведения об авторах
М.С. Алиева – студент
С.И. Богданов – доцент, доктор медицинских наук
Information about the authors
M.S. Alieva – student
S.I. Bogdanov – Doctor of Medicine, Associate professor

УДК 614.253.8:004:311.14

ИСПОЛЬЗОВАНИЕ ШАБЛОНОВ ВИЗУАЛИЗАЦИИ EXCEL ДЛЯ АНАЛИЗА МЕДИЦИНСКИХ ПОКАЗАТЕЛЕЙ ПАЦИЕНТОВ

Темирхан Казымбекович Баяхметов[1], Жандос Айдосұлы Айдосов[2], Июнгуль Сулжановна Мусатаева[3]
[1-3]НАО «Медицинский университет Семей», Семей, Казахстан
[1]bayakhmetovt@gmail.com

Аннотация
Введение. Всё большую популярность и востребованность приобретает визуализационные исследования. Так, например, для анализа медицинских показателей здоровья пациентов большую роль играет компьютерная визуализация данных на основе графических возможностей прикладных программ. Графическая интерпретация медицинских данных способствует повышению оперативности и эффективности принятия клинических решений.