**Содержание**

Введение

1. Системный подход к анализу и управлению безопасностью
2. Особенности управления безопасностью в медицинских учреждениях
3. Рекомендации по созданию систем информационной безопасностью

Заключение

Список используемой литературы

**Введение**

В настоящее время благополучие и даже жизнь многих людей зависят от обеспечения информационной безопасности множества компьютерных систем обработки информации, контроля и управления различными объектами. К таким системам относятся и медицинские информационные системы.

Их особенностью является, прежде всего, то, что в них хранится и обрабатывается информация, всесторонне определяющая социальный статус человека, а это обусловливает особую форму отношений между теми, кто ее формирует, и теми, кто использует. Значит, наряду с повышенными требованиями к достоверности информации должны накладываться нравственные ограничения на доступ к ней, а также юридическая ответственность предоставляющих ее лиц.

Любой медицинский работник несет полную ответственность (моральную, административную и уголовную) за конфиденциальность информации, к которой он получает доступ в ходе своей профессиональной деятельности.

Актуальность темы обеспечения информационной безопасности в медицине подтверждается тем, что в большинстве медицинских учреждений вопросы информационной безопасности не рассматриваются в принципе, а также отсутствием каких либо мероприятий направленных на обеспечение информационной безопасности и сохранении врачебной тайны.

Проблема безопасности информационных технологий возникла на пересечении двух активно развивающихся и, наверное, самых передовых в плане использования технических достижений направлений — безопасности технологий и информатизации. Сама проблема безопасности, конечно, не является новой, ведь обеспечение собственной безопасности — задача первостепенной важности для любой системы независимо от ее сложности и назначения будь то социальное образование, биологический организм или система обработки информации. Однако, в условиях, когда защищаемый объект представляет собой информационную систему, или когда средства нападения имеют форму информационных воздействий, необходимо разрабатывать и применять совершенно новые технологии и методы.

Предмет исследования – система управления безопасностью.

Объект исследования особенности управления безопасностью медицинскими учреждениями.

Цель исследования – охарактеризовать особенности систем анализа и управления безопасностью в медицинских учреждениях.

Достижение данной цели предполагает решение следующих задач:

1. Охарактеризовать основные черты анализа и управления безопасностью.

2. Выделить основные особенности управления безопасностью в медицинских учреждениях.

3. Сформулировать основные рекомендации по созданию систем информационной безопасностью.

Анализ литературы убеждает, что до настоящего времени как в нашей стране, так и в зарубежных странах, не создано трудов, в которых комплексно и детально была бы рассмотрена проблема управления медико-социальными системами медицины катастроф с использованием экономических методов.

**1. Системный подход к анализу и управлению безопасностью**

Системный подход к анализу и управлению безопасностью непосредственно связан с определением факторов непосредственного риска.

Для определения реальный (возможный) риск этих опасных факторов, надо сначала их идентифицировать. В целях идентификации можно использовать результаты аттестации рабочих мест по условиям труда и травмоопасности. Это позволит резко сократить количество опасных факторов за счет тех, которые по результатам аттестации не представляют реальную опасность.

Затем, используя качественный и количественный метод оценки рисков (на базе прошлого опыта и путем анализа статистических данных за последние 10-15 лет, выделяем наиболее высокие (неприемлемые) риски, и проводим их детальный анализ с помощью соответствующих методов:

* анализ опасности и связь с утратой трудоспособности;
* анализ "дерева отказов";
* анализ "дерева событий".

Рис. 1 Сущность системного подхода к управлению безопасностью

К основным мероприятиям по обеспечению безопасности населения в чрезвычайных ситуациях относятся следующие: прогнозирование и оценка возможности последствий чрезвычайных ситуаций; разработка мероприятий, направленных на предотвращение или снижение вероятности возникновения таких ситуаций, а также на уменьшение их последствий. Кроме того, очень важным является обучение населения действиям в чрезвычайных ситуациях и разработка эффективных способов его защиты.

Прогнозирование чрезвычайных ситуаций – это метод ориентировочного выявления и оценки обстановки, складывающейся в результате стихийных бедствий, аварий и катастроф. Различают долгосрочные и краткосрочные прогнозы. Долгосрочные прогнозы направлены на изучение и определение сейсмических районов, территорий, где возможны селевые потоки или оползни, границ зон вероятного затопления при авариях плотин или природных наводнениях, а также границ очагов поражения при техногенных авариях. Краткосрочные прогнозы используются для ориентировочного определения времени возникновения чрезвычайной ситуации.

Для составления прогнозов используются различные статистические данные, а также сведения о некоторых физических и химических характеристиках окружающих природных сред. Так, для прогнозирования землетрясений в сейсмоопасных районах изучают изменение химического состава природных вод, проводят наблюдение за изменением уровня воды в колодцах, определяют механические и физические (электрические и магнитные) свойства грунта. Значительную информацию для прогноза землетрясений может дать наблюдение за поведением некоторых животных.

Разработаны методы прогнозирования пожаров – лесных, торфяных и др. Для прогнозирования влияния скрытых очагов пожара (подземных или торфяных) на возможность возникновения лесных пожаров используется фотосъемка в инфракрасной части спектра, осуществляемая с самолетов или космических аппаратов.

Для прогнозирования обстановки, возникающей при развитии различных чрезвычайных ситуаций, применяют математические методы (математическое моделирование).

При прогнозировании чрезвычайной ситуации планируют постоянно проводимые, фоновые и защитные мероприятия.

К постоянно проводимым мероприятиям относятся постоянный контроль за качеством строительно-монтажных работ при возведении зданий и сооружений, создание надежной системы оповещения о возникновении чрезвычайной ситуации, строительство защитных укрытий и убежищ, снабжение населения средствами индивидуальной защиты (например, противогазами), обязательное обучение населения правилам поведения в чрезвычайных ситуациях, разработка планов ликвидации последствий чрезвычайных ситуаций и их финансовое и материальное обеспечение и др.

При предсказании момента чрезвычайной ситуации проверяются и приводятся в готовность система оповещения населения, а также аварийно-спасательные службы, развертывается система наблюдения и разведки, нейтрализуются особоопасные производства и объекты (химические предприятия, атомные электростанции и др.), проводится частичная эвакуация населения.

**2. Особенности управления безопасностью в медицинских учреждениях**

Среди мер для повышения надежность систем безопасности медицинских информационных систем целесообразно использовать следующие основные методы и способы защиты:

- кардинальное улучшение системы регистрации первичных медицинских данных на основе применения индивидуальных носителей информации (ИНИ);

- обязательное дублирование информации, хранимой в ИНИ, в базах данных различных уровней;

- периодическая (лучше ежедневная) актуализация всех баз данных в информационной системе (эта мера исключает возможность фальсификации медицинских сведений "задним числом");

- обеспечение доступа к информации различными путями: открыть часть информации для всех, открыть часть информации для пения и записи медицинским специалистам при условии их идентификации, и, наконец, часть информации открыть для чтения с разрешения пациента;

- для достижения необходимого уровня защиты информации со стороны программных средств использовать средства сетевых операционных систем.

Защита информации от несанкционированного доступа должна обеспечиваться блокированием доступа к информации:

- для СУБД - со стороны как персонала, так и тех задач системы, которым данная информация не требуется в силу функционального назначения;

- на рабочем месте - со стороны пользователей, не обладающих соответствующими полномочиями на доступ к различным информационным ресурсам;

- по каналам связи - со стороны сетевых пользователей и тех задач системы, которым данная информация не требуется опять-таки в силу функционального назначения.

Современный опыт решения проблем информационной безопасности показывает, что для достижения наибольшего эффекта при организации защиты информации необходимо руководствоваться рядом принципов.

Первым и наиболее важным является принцип непрерывности совершенствования и развития системы информационной безопасности: постоянный контроль функционирования системы, выявлении ее слабых мест, возможных каналов утечки информации и НСД, обновление и дополнение механизмов защиты в зависимости от изменения характера внутренних и внешних угроз, обоснование и реализация на этой основе наиболее рациональных методов, способов и путей защиты информации. Таким образом, обеспечение информационной безопасности не может быть разовым мероприятием.

Вторым является принцип комплексного использования всего арсенала имеющихся средств защиты во всех структурных элементах производства и на всех этапах технологического цикла обработки информации.

Комплексный характер защиты информации обусловлен действиями злоумышленников. Здесь правомерно утверждение, что оружие защиты должно быть адекватно оружию нападения. Кроме того, наибольший эффект достигается в том случае, когда все используемые средства, методы и мероприятия объединяются в единый, целостный механизм — систему информационной безопасности. Только в этом случае появляются системные свойства, не присущие ни одному из отдельных элементов системы защиты, а также возможность управлять системой, перераспределять ее ресурсы и применять современные методы повышения эффективности ее функционирования.

Важнейшими условиями обеспечения безопасности являются законность, достаточность, соблюдение баланса интересов личности и предприятия, высокий профессионализм представителей службы информационной безопасности, подготовка пользователей и соблюдение ими всех установленных правил сохранение конфиденциальности, взаимная ответственность персонала и руководства, взаимодействие с государственными правоохранительными органами. Без соблюдения этих условий никакая система информационной безопасности не может обеспечите требуемого уровня защиты.

**3. Рекомендации по созданию систем информационной безопасности**

Наряду с основными требованиями существует ряд устоявшихся рекомендаций, которые будут полезны, создателям систем информационной безопасности:

- средства защиты должны быть просты для технического обслуживания и «прозрачны» для пользователей;

- каждый пользователь должен иметь минимальный набор привилегий, необходимых для работы;

- возможность отключения защиты в особых случаях, например когда механизмы защиты реально мешают выполнению работ;

- независимость системы защиты от субъектов защиты

- разработчики должны предполагать, что пользователи имеют наихудшие намерения (враждебность окружения), что они будут совершать серьезные ошибки и искать к пути обхода механизмов защиты;

- отсутствие на предприятии излишней информации о существовании механизмов защиты [4, с. 83].

Предпринимаемые меры защиты должны быть адекватны вероятности осуществления данного типа угрозы и потенциальному ущербу, который может быть нанесен в том случае, если угроза осуществится (включая затраты на защиту от нее).

Выбирая защитные меры, приходиться учитывать не только прямые расходы на закупку оборудования и программ, но и расходы на их внедрение, в частности - на обучение и переподготовку персонала. Важным обстоятельством является совместимость нового средства со сложившейся аппаратно-программной структурой объекта.

По мнению специалистов, организационные мероприятия играют большую роль в создании надежного механизма защиты информации, так как возможности несанкционированного использования конфиденциальных сведений в значительной мере обусловлены не техническими аспектами, а злоумышленными действиями, нерадивостью, небрежностью и халатностью пользователей или персонала защиты.

Сформированная совокупность правовых, организационных и инженерно – технических мероприятий выливается в соответствующую политику безопасности, отраженную в концепции информационной безопасности предприятия.

Концепция разрабатывается на основе анализа современного состояния информационной безопасности, источников, видов угроз и динамики их развития. Концепция системы защиты представляет собой систематизированное изложение целей, задач, принципов и способов достижения информационной безопасности.

Концепция информационной безопасности должна содержать:

- общую характеристику объекта защиты (описание состава, функций и существующей технологии обработки информации);

- формулировку целей создания системы защиты, основных задач обеспечения информационной безопасности и путей достижения целей;

- основные классы угроз информационной безопасности, принимаемые во внимание при разработке подсистемы защиты;

- основные принципы и подходы к построению системы обеспечения информационной безопасности, меры, методы и средства достижения целей защиты.

Концепция представляет собой официальную принятую систему взглядов на проблему информационной безопасности и пути ее решения с учетом современных тенденций развития информатизации медицинского учреждения. Она является методологической основой политики в разработке практических мер по ее реализации.

**Заключение**

В настоящее время благополучие и даже жизнь многих людей зависят от обеспечения информационной безопасности множества компьютерных систем обработки информации, контроля и управления различными объектами. К таким системам относятся и медицинские информационные системы.

Их особенностью является, прежде всего, то, что в них хранится и обрабатывается информация, всесторонне определяющая социальный статус человека, а это обусловливает особую форму отношений между теми, кто ее формирует, и теми, кто использует. Значит, наряду с повышенными требованиями к достоверности информации должны накладываться нравственные ограничения на доступ к ней, а также юридическая ответственность предоставляющих ее лиц.

Любой медицинский работник несет полную ответственность (моральную, административную и уголовную) за конфиденциальность информации, к которой он получает доступ в ходе своей профессиональной деятельности.

Из рассмотренного становится очевидно, что обеспечение информационной безопасности является комплексной задачей. Это обусловлено тем, что информационная среда является сложным многоплановым механизмом, в котором действуют такие компоненты, как электронное оборудование, программное обеспечение, персонал.

Для решения проблемы обеспечения информационной безопасности необходимо применение законодательных, организационных и программно-технических мер. Пренебрежение хотя бы одним из аспектов этой проблемы может привести к утрате или утечке информации, стоимость и роль которой в жизни современного общества приобретает все более важное значение.

**Список использованной литературы**

1. Безопасность жизнедеятельности. Безопасность технологических процессов и производств: Охрана труда: Учеб. пособие/ Кукин П.П., Лапин В.Л., Пономарев Н.Л. Сердюк Н.И- 2-е изд. Испр, и доп.. -М.: Высшая школа, 2001. -318 с.
2. Безопасность жизнедеятельности. Учебник для вузов / К.З.Ушаков, Н.О. Каледина, Б.Ф. Кирин, М.А. Сребрый. Под ред. К.З.Ушакова М.: Моск. Гос. Горн. ун-т, 2000. – 430
3. Безопасность жизнедеятельности. Учебник для вузов/ С.В. Белов, А.В. Ильинская, А.Ф. Козьяков и др.; Под общ. Ред. С.В. Белова, - М.: Высш.шк., 2008. - 448 с.
4. Информационно-аналитические системы и технологии в здравоохранении и ОМС. «Сборник трудов Всероссийской конференции». Красноярск, 15 – 17 сентября 2004 г. С. 402 – 411.
5. Куликов Г.Б. Безопасность жизнедеятельности: Учебник для инж. направлений и спец. высш. учеб. заведений. - М.: Мир книги, 2008. - 269 с.
6. Русак О.Н., Малаян К.Р., Занько Н.Г. Безопасность жизнедеятельности. Учебное пособие СПб; Издательство «Лань», 2000 448 с.