ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Трунова А.В.

Трунова Алла Владимировна - студент,
кафедра математики и информатики, факультет экономики и финансов,
Сибирский Институт управления - филиал
Российская академия народного хозяйства и государственной службы
при Президенте Российской Федерации, г. Новосибирск

Аннотация: *в данной статье рассматривается актуальная на данный момент проблема защиты информации на предприятиях, поскольку доступ к конфиденциальной информации и ее изменение могут нанести существенный урон финансовому положению компании. Отмечаются различные причины нарушения информационной безопасности в организации. А также авторы указывают на способы их предотвращения.*

Ключевые слова: *информационная безопасность на предприятии, угрозы, несанкционированный доступ, резервирование, защита информации.*

Одной из самых насущных проблем информационного общества является защита информации, поскольку всевозможные данные, обрабатываемые и накапливаемые вычислительной техникой, стали в последнее время определять направление деятельности и многие другие аспекты жизни современного социального организма. С помощью незаконного владения информацией можно осуществлять самые различные противоправные деяния, например, производить незаконный оборот финансовых средств, получать доступ к секретной коммерческой информации и т.д. Следует отметить, что конфиденциальная информация представляет огромный интерес для конкурирующих фирм. Именно она становится причиной посягательств со стороны злоумышленников.

Многие проблемы информационной безопасности связаны с недооценкой важности такой угрозы, как конфиденциальность информации. В результате для предприятия это может обернуться банкротством. Даже единичный случай халатности персонала предприятия может принести ему многомиллионные убытки, потерю репутации фирмы и доверия клиентов. Чтобы этого избежать, специалисты службы безопасности предприятия используют специальное оборудование, производящее анализ электромагнитных излучений, получаемых во время работы на компьютере.

Технологии обеспечения информационной безопасности можно подразделить на две группы:

- 1-я группа - защищающие программные и аппаратные средства для обработки и хранения информации от отказов, нарушений, способных возникнуть в результате случайной ошибки;
- 2-я группа - защищающие программные и аппаратные средства обработки информации от всевозможных преднамеренных угроз, которые заранее планируются злоумышленниками.

Полноценное обеспечение информационной безопасности на предприятии должно быть стандартизировано и находиться под полным контролем круглогодично, в реальном времени, в круглосуточном режиме. При этом система учитывает весь жизненный цикл информации, начиная с момента появления и до полного ее уничтожения или потери значимости для предприятия [1].

Целями системы защиты информации предприятия являются:

- Предотвращение утечки, хищения, утраты, искажения, подделки информации вследствие ее тиражируемости;

- Предотвращение угроз безопасности личности, предприятия, общества, государства вследствие разглашения или искажения информации;
- Предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации, что может привести к уменьшению ее потенциальной эффективности;
- Предотвращение различных форм незаконного вмешательства в информационные ресурсы и системы предприятия;
- Обеспечение правовой защиты информации как объекта собственности (исключение возможности ее незаконного тиражирования);
- Защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах предприятий;
- Сохранение конфиденциальности документированной информации в соответствии с законодательством (грифы секретности, прав доступа и распространения и т.д.) [2].

Следует заметить, что с целью защиты информации каждый пользователь обязан знать и осуществлять следующие меры:

1) контролировать доступ как к информации в компьютере, так и к прикладным программам. Необходимо иметь гарантии того, что только авторизованные пользователи смогут иметь доступ к информации и приложениям;

2) процедуры авторизации. Администратору следует разработать процедуры авторизации, определяющие, кто из пользователей может иметь доступ к тем или иным приложениям и информации, и предусмотреть соответствующие меры по внедрению в организацию таких процедур;

3) защита файлов. Следует разработать процедуры по ограничению доступа к файлам: для указания типа информации, содержащейся в файлах, и требуемого уровня безопасности использовать внешние и внутренние метки; ограничивать доступ в те помещения, в которых хранятся архивы, файлы и библиотеки данных; для ограничения доступа к файлам только авторизованных пользователей использовать организационные меры и программно-аппаратные средства;

4) защита целостности информации. Вводимую информацию следует подвергать проверкам на ошибки, она должна быть авторизованной, полной и точной. Точность информации необходимо проверять с помощью процедур сравнения полученных результатов обработки с предполагаемыми;

5) защита системных программ. При разработке программ меры защиты должны включать в себя процедуры по внесению изменений в программу, ее приемки и тестирования до ввода в эксплуатацию;

6) становление мер защиты более адекватными за счет привлечения специализированных организаций;

7) рассмотрение вопроса о коммуникационной безопасности. Данные, передаваемые по незащищенным линиям, могут быть перехвачены [1].

На государственном уровне правовая защита регулируется государственными и ведомственными актами. В нашей стране регуляторами являются: Конституция, законы Российской Федерации, гражданское, административное и уголовное право. Ведомственные нормативные акты определяются приказами, руководствами, положениями и инструкциями, которые издаются самими ведомствами, организациями, а также предприятиями, действующими в рамках определенных структур [3].

В заключение следует отметить, что комплексную защиту организаций сегодня осуществляет значительное количество специализированных охранно-детективных предприятий и служб безопасности. Они проводят различные виды работ по физической, экономической и информационной безопасности, поскольку в современной обстановке без решения этих вопросов любой вид деятельности не сможет быть эффективным и прибыльным [1].

Подведя итог всему вышесказанному, хочется заметить, что защищаться от всего невозможно, из всех возможных угроз на предприятии нужно выбрать то, что наиболее существенно и важно. А выбранная верно система обеспечения информационной безопасности поможет сохранить это [4].

Список литературы

1. *Мамаева Л.Н., Кондратьева О.А*. Основные направления обеспечения информационной безопасности предприятия // Информационная безопасность регионов, 2016. № 2. С. 5-9.
2. *Кожунова Е.А.* Обеспечение информационной безопасности на современном предприятии // Школа науки, 2018. № 2. С. 19-21.
3. *Чернышов Б.В.* Определение приоритетных задач в политике (теория научного выбора и опыт истории) // Информационная безопасность регионов.. 2014. № 1 (14).
4. *Сенаторова А.С., Захарова Е.А*. Обеспечение информационной безопасности на предприятии // Современная техника и технологии, 2015. № 4. С. 45-47.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ИХ ПРИМЕНЕНИЕ В СОВРЕМЕННОЙ СИСТЕМЕ ЗДРАВООХРАНЕНИЯ

Лапкова А.К.

Лапкова Арина Константиновна – студент,
кафедра информатики и математики, факультет экономики и финансов,
Сибирский Институт управления - филиал
Российская Академия народного хозяйства и государственной службы
при Президенте Российской Федерации, г. Новосибирск

Аннотация: *в рамках данной статьи рассмотрены некоторые задачи и проблемы внедрения информационных технологий в медицину. Создание и внедрение информационных технологий обусловлены возрастающим объемом информации и усложнением процессов управления в здравоохранении. Современные технологии создают все новые возможности для медицины. Актуальность внедрения современных информационных технологий в медицину заключается не только в том, что это выводит здравоохранение на новый уровень, а также в том, что это существенно сокращает время на доступ, поиск и обмен информацией, а время очень часто играет очень большую роль.*

Ключевые слова: *здравоохранение, информационные технологии, автоматизация, задачи.*

Буквально несколько лет назад об автоматизации системы здравоохранения никто не задумывался. Все документы, включая карты, бюллетени, рецепты на лекарственные препараты, выписывались вручную на бумаге. Это не только сказывалось на скорости работы врачей и медсестер, но и оказывало влияние на качество обслуживания пациентов медицинским персоналом, вело к наличию врачебных ошибок и большим временным затратам на заполнение необходимых документов.

Весь процесс информатизации здравоохранения направлен на создание единого медицинского информационного пространства, позволяющего врачам общаться друг с другом, обращаться к архивам и библиотекам медицинских знаний и технологий, а также взаимодействовать с функционирующей аппаратурой непосредственно с рабочего места и в реальном времени.