*Магистрант первого курса Можаров Н.В.*

*Направление 09.04.03. «Прикладная информатика в экономике»*

Отчет об актуальности сферы исследования

Современные предприятия, независимо от сферы деятельности, большое количество средств и ресурсов выделяют на обеспечение сохранности конфиденциальных данных. Делается это по различным причинам. В экономической сфере защита информации дает возможность иметь высокие доходы, заключать выгодные сделки, избегать экономического ущерба, добиваться преимущества над конкурентами. В социальной сфере – в правовых, политических и других областях, защита информации направлена на улучшение морального и материального благосостояния человека. В свою очередь, неправомерное искажение или фальсификация, уничтожение или разглашение определённой части информации, равно как и дезорганизация процессов ее обработки и передачи в информационно-управляющих системах наносят серьезный материальный и моральный урон предприятиям, участвующим в процессах автоматизированного информационного взаимодействия.

Актуальность проблемы обеспечения информационной безопасности предприятия, защиты его законных интересов при использовании информационных и управляющих систем все более возрастает. Этому есть ряд причин. Прежде всего – это расширение сферы применения вычислительной техники и возросший уровень доверия к автоматизированным системам. Осуществление перехода к рыночным отношениям в области создания и предоставления информационных услуг. Развитие и распространение вычислительных сетей и территориально распределенных систем. Доступность средств вычислительной техники и прежде всего персональных компьютеров привела к распространению компьютерной грамотности. Еще одним весомым аргументом является бурное развитие и распространение компьютерных вирусов. Все эти аргументы способствуют усилению внимания к вопросам безопасности информационных систем.

На основе проведенных исследований был составлен индивидуальный план работы магистранта и утверждена тема НИР «Исследование методов и алгоритмов защиты информации в социально-экономических системах» решением кафедры, протокол от 30.09.2015г., № 3.

*Магистрант первого курса Можаров Н.В.*

*Направление 09.04.03. «Прикладная информатика в экономике»*

Информационные источники, содержащие сведения о современных методах защиты информации

Федеральный закон «Об электронной цифровой подписи» от 10 января 2002г. № 1-ФЗ

Федеральный закон «Об информации, информатизации и защите информации» № 24-ФЗ от 20.02.95г.

Мельников В. - «Защита информации в компьютерных системах» - М.: Финансы и статистика, Электроинформ, 1997г.

Сайт [www.Cryptocom.ru](http://www.Cryptocom.ru)

Петренко С.А., Курбатов В.А. - «Политики безопасности компании при работе в интернете»

Блинов А.М. - «Информационная безопасность»

Горбатов и Полянская - «Основы технологии PKI»

Гафнер В.В, - «Информационная безопасность»

Климентьев К.Е. – «Компьютерные вирусы и антивирусы: взгляд программиста»

Смирнов С.Н. – «Безопасность систем баз данных»

*Магистрант первого курса Можаров Н.В.*

*Направление 09.04.03. «Прикладная информатика в экономике»*

Анализ способов предотвращения утечки или хищения информации

Нынешнее развитие вычислительных сетей, в ряде случаев, способствует хищению информации. Человеческий фактор играет не меньшую роль в деле хищения, порчи информации.

* Существующие виды утечки информации:
* Радиоизлучение монитора
* Микрофонный эффект, закладки в телефонном аппарате.
* Стекло вибрация, видеонаблюдение.
* Вибрация стен, перекрытий, систем отопления, вентиляции, дверей.
* Анализ передаваемых данных.
* Прослушивание телефонного и факс-модемного трафика.
* Жучки, направленные микрофоны.
* Доступ посторонних лиц.
* Человеческий фактор.

К другим способам получения необходимых данных можно отнести:

* Анализ открытых источников информации.
* Анализ деятельности предприятия.
* Шантаж.
* Слежка.

Радиоизлучение монитора. Перехват изображения монитора достаточно распространенный способ хищения информации. Основной защитой можно считать экранирование помещения, металлический корпус ПЭВМ, а также использование устройств маскирующих побочное магнитное излучение.

Микрофонный эффект. Акустические колебания микрофона или обмоток звонка возникают при положенной трубке и могут быть сняты с телефонного кабеля, например на АТС. Таким образом, для защиты от такого перехвата можно использовать устройства, подавляющие эти колебания.

Считывание вибрации стекла. Такое удаленное действие возможно с помощью лазера. Основная защита: использование двойных стекол, установка устройств виброакустической защиты.

Утечка информации при организации корпоративной сети. Для обеспечения сохранности информации в корпоративной сети используют.

* Антивирусные средства;
* Межсетевые экраны;
* Системы обнаружения атак;
* Анализаторы системных журналов;
* Криптомаршрутизаторы;
* Системы анализа уязвимостей.

Руководствуясь перечисленным выше, а также используя принцип разумной достаточности, организация сможет исключить возможность утечки или хищения информации.