

Содержание

Введение.....	7
1 Исследование информационной системы ОАО "Хабаровское автолесовозное хозяйство"	13
1.1 Общая информация о предприятии.....	13
1.2 Общие сведения об информационных системах, эксплуатируемых ОАО "Хабаровское автолесовозное хозяйство".....	14
1.2.1 ИСПДн «Кадровый и бухгалтерский учет»	15
1.2.2 ИСПДн «Продажа и складирование леса»	18
1.3 Определение исходного уровня защищенности персональных данных в ИСПДн ОАО "Хабаровское автолесовозное хозяйство"	21
1.4 Существующие меры защиты ПДн.....	24
1.5 Исследование актуальных угроз информационной безопасности для ИСПДн ОАО "Хабаровское автолесовозное хозяйство"	25
1.5.1 Актуальные угрозы для ИСПДн «КБУ».....	37
1.5.2 Актуальные угрозы для ИСПДн «ПСЛ»	41
1.6 Требования к ИСПДн «КБУ» и ИСПДн «ПСЛ» в части соблюдения уровня защищенности.....	47
1.7 Выводы по главе.....	49
2 Организационно-правовое направление защиты ИСПДн ОАО "Хабаровское автолесовозное хозяйство"	50
2.1 Программно-аппаратное направление защиты	51
2.1.1 СрЗИ НСД «Блокхост-сеть»	51
2.1.2 ABC. Dr.Web Enterprise Security Suite 6.0	53
2.1.3 САЗ «Аргус».....	54
2.1.4 МЭ «IdecoICS 3»	55
2.2 Определение исходного уровня защищенности персональных данных в ИСПДн ОАО "Хабаровское автолесовозное хозяйство"	57

2.2.1 Общие требования	57
2.2.2 Организационные меры по размещению ТС	57
2.2.3 Организационные меры по работе со съемными носителями информации	58
2.2.4 Организация работы администратора безопасности	59
2.2.5 Организационные меры по противодействию утечки информации	61
2.2.6 Порядок и правила использования паролей пользователей ИСПДн.....	61
2.3 Инженерно-технические направление защиты.....	62
2.4 Меры защиты информации в целях нейтрализации актуальных угроз	63
2.5 Схемы построения СЗИ в ИС ОАО "Хабаровское автолесовозное хозяйство"	67
2.6 Выводы по главе.....	69
3 Обоснование экономической эффективности проектирования и внедрения профиля ЗИ в ИС ОАО "Хабаровское автолесовозное хозяйство"	70
3.1 Планирование и организация процесса проектирования и внедрения профиля ЗИ в ИС ОАО "Хабаровское автолесовозное хозяйство"	70
3.2 Расчет сметной стоимости проектирования и внедрения профиля ЗИ в ИС ОАО "Хабаровское автолесовозное хозяйство"	75
4 Безопасность и экологичность.....	80
4.1 Анализ вероятных вредных и опасных факторов при работе с персональным компьютером.....	80
4.1.1 Электромагнитное излучение.....	80
4.1.2 Психофизиологические факторы	81
4.1.3 Микроклимат.....	83
4.2 Чрезвычайные ситуации.....	87
4.3 Защита от вероятных и опасных процессов.....	88
4.3.1 Требования по пожарной безопасности	88
4.3.2 Электробезопасность.....	90

4.3.3 Требования безопасности во время эксплуатации ЭВМ	91
4.4 Экологичность.....	92
Заключение	93
Список используемой литературы	94
Приложение А	98

Введение

Для современного этапа развития общества характерен непрерывный процесс информатизации. С внедрением информационных технологий во все сферы жизнедеятельности человека проблемы информационной безопасности с каждым годом становятся всё более сложными и многогранными. Область применения информационных систем также не является исключением и постоянно расширяется, затрагивая организацию деятельности в различных сферах жизни общества.

Открывая новые возможности перед человеком в части модернизации различных технологических и управленческих процессов, повышения качества и эффективности работы, на информационные системы возлагается существенная ответственность за сохранность и безопасность информации. Для правильной работы информационных систем осуществляется телекоммуникационное и информационное взаимодействие подсистем различного назначения (общего пользования, частных, производственных, ведомственных). Поддержание взаимодействия отдельных территориально-распределенных подсистем внутри информационной системы, а также между отдельными системами происходит посредством постоянного предоставления услуг информационного и аналитического характера, администрирования единого информационного пространства и средств безопасности. Временная недоступность критически важного узла информационной системы или его несанкционированное использование может не только нанести владельцу системы значительный материальный ущерб, но и привести к экологической или техногенной катастрофе.

Вместе с тем необходимо учитывать, что уязвимость таких информационных систем существенно превышает уязвимость отдельно взятых узлов, так как такие системы функционируют и проектируются с учетом использования в них технологии межсетевого взаимодействия, а

число угроз информационной безопасности и способов их реализации постоянно растет.

В этой связи важнейшей задачей является обеспечение достаточной степени защищенности таких систем для их эффективного функционирования в условиях проявления внутренних и внешних информационных угроз.

Цели, задачи и принципы обеспечения информационной безопасности сформулированы в ряде руководящих и нормативных документов, ключевым из которых на сегодняшний день является Доктрина информационной безопасности Российской Федерации, утверждённая Приказом Президента РФ №1895 от 9 сентября 2000 г.

Объектами защиты в информационной системе являются приложения, информационные ресурсы и средства обеспечения функционирования информационной системы. При обеспечении информационной безопасности должна гарантироваться защита от:

1. комплексного воздействия, направленного на нарушение функционирования непосредственной среды;
2. несанкционированного нелегитимного доступа к технологической (служебной) и иной информации, связанной с работой информационной сети;
3. разрушения встроенных средств защиты.

Для описания множества угроз безопасности, задач защиты, а также требований безопасности, используется профиль защиты информации. Такой документ имеет жесткую структуру и разрабатывается для конкретной информационной системы.

Информационные системы хозяйствующих субъектов не являются исключением, и требуют обеспечения достаточного уровня информационной безопасности посредством внедрения средств и проведения мероприятий, что обуславливает необходимость разработки профиля информационной безопасности таких систем. Вместе с тем актуальность проблемы и

необходимость в разработке профиля защиты информации подтверждается большим объемом данных, циркулирующих в информационной системе.

Таким образом, с целью эффективной организации информационной безопасности необходима разработка и использование профиля защиты информации, согласующего средства защиты всех узлов и подсистем информационных системах.

В данной работе необходимо провести разработку профиля защиты информации в информационной системе ОАО "Хабаровское автолесовозное хозяйство", основным видом деятельности которого является предоставление услуг по перевалке, складированию, переработке леса и лесоматериалов.

В настоящее время общество перевозку леса не осуществляет, так как весь автопарк исчерпал свой ресурс и пришел в негодное состояние. Несмотря на вышесказанное ОАО "Хабаровское автолесовозное хозяйство" успешно функционирует и ведет хозяйственную деятельность, сменив направление на сдачу помещений и земель в аренду.

Дело в том, что на сегодняшний день коммерческая аренда является приоритетным направлением по той причине, что многие предприятия не в состоянии купить собственные помещения и здания. В связи с этим основным видом деятельности ОАО "Хабаровское автолесовозное хозяйство" на сегодня является сдача офисных и производственных помещений в аренду, а также предоставление услуг железнодорожного тупика, погрузке и выгрузке, складирования лесоматериалов.

Несмотря на смену направления деятельности, предприятие имеет широкую территориально распределенную информационную систему, в которой циркулирует большой объем информации. В составе информационной системы ОАО "Хабаровское автолесовозное хозяйство" можно выделить следующие элементы:

1. серверы, хранящие и обрабатывающие информацию;

2. рабочие станции, которые служат для ввода запросов к базам данных, получения и обработки результатов запросов, а также выполнения других задач сотрудников предприятия;

3. коммуникационные каналы – линии связи, по которым данные передаются между узлами информационной системы. Коммуникационные каналы рассматриваемого предприятия используют различные типы среды передачи данных: телефонные линии, волоконно-оптический кабель, коаксиальный кабель, беспроводные и другие каналы связи;

4. активное оборудование – модемы, сетевые адаптеры, концентраторы, коммутаторы, маршрутизаторы, которые необходимы для передачи и приема данных;

5. сетевое программное обеспечение, управляющее процессом передачи и приема данных и контролирующее работу отдельных частей информационной системы;

6. технические системы и средства защиты информации, помещения, где располагаются большинство узлов информационной системы ОАО "Хабаровское автолесовозное хозяйство".

Существует множество естественных и искусственных потенциальных угроз информационной безопасности исследуемой информационной системы ОАО "Хабаровское автолесовозное хозяйство", которые необходимо отразить в профиле информационной безопасности. Кроме того, в связи с тем, что данная информационная система имеет доступ к сети Интернет, ключевое внимание в данной работе предполагается уделить угрозам реализации несанкционированного доступа.

В части определения комплекса мер и средств защиты разработку профиля необходимо проводить с учетом таких технологий, как:

1. технология защиты распределенных информационных ресурсов;
2. технология защиты целостности и подлинности информации;
3. технология защиты сетей и каналов;
4. технология защиты информации от утечки по техническим каналам;

5. технология поддержки доверенной общесистемной программной среды;

6. администрирование системы безопасности.

Таким образом, целью работы является проектирование профиля защиты информации в информационной системе ОАО "Хабаровское автолесовозное хозяйство". Вместе с тем необходимо, чтобы проектируемая система защиты информации соответствовала требованиям действующего законодательства Российской Федерации в целом и руководящим документам в частности.

Объектом исследования является информационная система ОАО "Хабаровское автолесовозное хозяйство".

Предметом исследования является профиль защиты информации в информационной системе ОАО "Хабаровское автолесовозное хозяйство".

Для реализации вышеуказанной цели исследования необходимо решить приведенные ниже задачи:

1. изучить нормативно-методические документы (НМД) в области защиты информации;

2. провести исследование информационных систем ОАО "Хабаровское автолесовозное хозяйство", включая анализ внедренных средств защиты информации;

3. разработать эффективный, удовлетворяющий всем НПА и НМД профиль защиты информации в информационной системе ОАО "Хабаровское автолесовозное хозяйство".

В ходе исследования информационной системы ОАО "Хабаровское автолесовозное хозяйство" были определены:

- состав и структура объектов защиты;
- конфигурация и структура информационной системы;
- перечень лиц, участвующих в обработке информации;
- права доступа лиц, допущенных к обработке информации;
- существующие меры защиты;
- угрозы информационной безопасности.