

Эта часть работы выложена в ознакомительных целях. Если вы хотите получить работу полностью, то приобретите ее воспользовавшись формой заказа на странице с готовой работой:

<https://studservis.ru/gotovye-raboty/kursovaya-rabota/300484>

Тип работы: Курсовая работа

Предмет: Право

ВВЕДЕНИЕ 3

1 Теоретические основы охраны и безопасности предприятий 6

1.1 Основные термины и содержание охраны и безопасности предприятий 6

1.2 Анализ нормативно-правовой базы охраны и безопасности предприятий 10

2 Анализ системы охраны и характер защищаемой информации на примере ООО «ТКС» 13

3. Анализ методов защиты в организации охраны предприятий 15

3.1 Применение и выбор методов построения системы защиты информации 15

3.2 Выбор программного обеспечения для построенной системы защиты информации 17

3.3 Разработка должностной инструкции 18

3.4 Анализ работ разработанной системы защиты и ее экономическое обоснование 20

ЗАКЛЮЧЕНИЕ 23

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 25

Актуальность работы. Сегодня трудно представить организацию, которая не будет оснащена компьютерной техникой. Любая организация, которая широко использует компьютерные технологии в своей работе, рано или поздно столкнется с проблемами информационной безопасности.

Проблемы информационной безопасности, с которыми можно столкнуться сегодня, а также проблемы, которые, как ожидают образовательные учреждения, возникнут завтра, могут быть предсказаны с помощью долгосрочных исследований в разных странах и независимых структурах в других странах.

До недавнего времени информационная безопасность России серьезно пострадала только в банках, военных и государственных учреждениях. Время от времени проводилось несколько репрезентативных опросов, которые охватывают не все сферы деятельности, поэтому невозможно точно оценить потери, искажения и ущерб, вызванные несанкционированным использованием информации российскими компаниями и организациями.

В то же время можно судить о невнимательности и невежестве российских пользователей компьютеров в области информационной безопасности. Даже принимая во внимание заинтересованность компании в продаже своих продуктов и тот факт, что они занимаются разработкой систем информационной безопасности и антивирусного программного обеспечения, можно заметить, что большинство пользователей имеют очень небольшую квалификацию в области информационной безопасности.

Производители программного обеспечения перешли от непознаваемых к системам безопасности, то есть доминирующие и скрытые дефекты систем информационной безопасности не раскрываются и не известны широкому кругу пользователей, к полностью раскрытым системам безопасности, в которых все известные и потенциальные уязвимости в информационной системе публикуются на общедоступных ресурсах.

Злоумышленник может легально получить доступ к достаточной информации об обнаруженных уязвимостях безопасности, а организации, использующие определенные программные средства, еще не защищены, поскольку производитель не может устранить все обнаруженные уязвимости безопасности за короткое время.

Роль информации в процессе управления огромна, на всех уровнях и во всех областях: политике, экономике, науке, культуре и т.д. Следовательно, возрастает риск того, что информационные ресурсы, используемые информационными технологиями, могут быть скомпрометированы. Для того чтобы свести к минимуму возможность нанесения ущерба информационным ресурсам, необходимо серьезно отнестись к концепции информационной безопасности.

Объект исследования: ООО «ТКС»

Предмет исследования: методика организации охраны предприятия.

Цель исследования: проанализировать существующие методики организации охраны предприятия, а также изучить особенности их применения на примере ООО «ТКС».

Цель предопределяет задачи, которые предстоит решить:

1. Рассмотреть основные термины и содержание охраны и безопасности предприятий;

2. Провести анализ нормативно-правовой базы охраны и безопасности предприятий;
3. Дать анализ системы охраны и характер защищаемой информации на примере ООО «ТКС»;
4. Раскрыть применение и выбор методов построения системы защиты информации;
5. Осуществить выбор программного обеспечения для построенной системы защиты информации;
6. Провести разработку должностной инструкции;
7. Привести анализ работ разработанной системы защиты и ее экономическое обоснование.

Методы исследования: сравнительный метод, метод наблюдения, метод оценки, метод анализа, дедукция.

Теоретическая основа исходит из того, что в настоящее время имеется огромное количество ученых, изучающих данную проблематику: Галицкий А.В. «Защита информации в сети - анализ технологий и синтез решений», Малюк А. А. «Введение в защиту информации в автоматизированных системах» и т.д.

Структура. Курсовая работа включает в себя введение, три главы (теоретическая и практическая), заключение, список использованных источников и приложение. Введение состоит из актуальности, целей, задач, предмета, объекта и методов исследования.

Первая глава теоретического характера и в ней приведены теоретические аспекты охраны и безопасности предприятий.

Вторая глава носит практический характер и в ней проведен анализ системы охраны и характер защищаемой информации на примере ООО «ТКС».

В третьей главе приведен анализ методов защиты в организации охраны предприятий.

Заключение содержит обобщенные выводы

Список использованных источников состоит из 20 наименований.

1. Конституция Российской Федерации, принятая всенародным голосованием 12.12.1993 года с изменениями, одобренными в ходе голосования в 01.07.2020.
2. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 N 51-ФЗ (ред. от 08.12.2020).
3. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ (последняя редакция).
4. Указ Президента РФ от 22.05.2015 N 260 «О некоторых вопросах информационной безопасности Российской Федерации» (вместе с «Порядком подключения информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети Интернет»).
5. Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».
6. Закон РФ «О государственной тайне» от 21.07.1993 N 5485-1 (последняя редакция).
7. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации.
8. ГОСТ Р 51583-00. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.
9. Аверченков, В. И. Организационная защита информации / В.И. Аверченко. - М.: ФЛИНТА, 2021. - 184 с.
10. Емельянова, Н. З. Защита информации в персональном компьютере / Н.З. Емельянова. - М.: Форум, 2019. - 368 с.
11. Максименко, В. Н. Защита информации в сетях сотовой подвижной связи / В.Н. Максименко. - М.: Горячая линия - Телеком, 2018. - 360 с.
12. Малюк, А. А. Введение в защиту информации в автоматизированных системах / А.А. Малюк. - М.: Горячая линия - Телеком, 2019. - 147 с.
13. Малюк, А. А. Введение в защиту информации в автоматизированных системах / А.А. Малюк. - М.: Горячая линия - Телеком, 2021. - 146 с.
14. Мельников, В.В. Защита информации в компьютерных системах / В.В. Мельников. - М.: Электроинформ, 2019. - 368 с.
15. Мельников, В. П. Информационная безопасность и защита информации / В.П. Мельников. - М.: ИЦ «Академия», 2021. - 336 с.
16. Сергеева, Ю. С. Защита информации. Конспект лекций / Ю.С. Сергеева. - М.: А-Приор, 2019. - 128 с.
17. Соколов, А.В. Защита информации в распределенных корпоративных сетях и системах / А.В. Соколов. - М.: ДМК Пресс, 2020. - 656 с.
18. Спесивцев, А.В. Защита информации в персональных ЭВМ / А.В. Спесивцев, В.А. Вегнер, А.Ю. Крутяков. - М.: Радио и связь, 2019. - 192 с.
19. Степанов, Е.А. Информационная безопасность и защита информации. Учебное пособие / Е.А. Степанов. -

М.: ИНФРА-М, 2018. - 304 с.

20. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. - М.: ДМК пресс, 2020. - 592 с.

Эта часть работы выложена в ознакомительных целях. Если вы хотите получить работу полностью, то приобретите ее воспользовавшись формой заказа на странице с готовой работой:

<https://studservis.ru/gotovye-raboty/kurovaya-rabota/300484>