Тема выпускной квалификационной работы: Разработка алгоритма удаленной аутентификации для входа в базу данных по незащищенному каналу связи (на примере ФГУП СК Ставрополькрайводоканал «Пятигорский водоканал», г. Пятигорск)
Автор ВКР: Минсков Владислав Денисович
Научный руководитель ВКР: канд. техн. наук, доцент кафедры информационно-коммуникационных технологий, математики и информационной безопасности В. А. Козлов
Сведения об организации-заказчике: ФГБОУ ВО «Пятигорский государственный университет»
Актуальность темы исследования: Процедура входа в БД всегда является актуальной с точки зрения НСД к БД.
поэтому разрабатываемый нами алгоритм аутентификации на основе криптографических преобразований является актуальной научной задачей
Цель работы: является применить приобретённые теоретические знания на практике в процессе обработки собранного материала с целью оформления дипломного проекта, наработав профессиональные навыки и умения в сфере инженерно-технической защиты информации на предприятии.
Задачи:

- ознакомиться с назначением и деятельностью различных подразделений предприятия «Пятигорский водоканал»;
- оценить материально-техническое обеспечение предприятия;
- изучить системы инженерно-технического обеспечения защиты информации функционирующие на предприятии;
- выполнить постановку задачи и проверить криптографическую стойкость алгоритмов взаимной удаленной аутентификации на данном предприятии;
- разработать предложения по совершенствованию инженерно-технического обеспечения защиты информации предприятия.

Теоретическая и практическая значимость исследования:
Теоретическая значимость:
- выявлены недостатки действующей на исследуемом объекте удаленной аутентификации;
- проанализированы нормативно-правовые и законодательные документы касающиеся защиты информации и информационной безопасности предприятия;
- изучены функционирующие на объекте исследования системы программных и технических средств защиты информации;
- разработана математическая модель и алгоритм ее реализации модуля удаленной аутентификации на базе гибридной вероятностной модели криптографических преобразований.

Практическая значимость результатов:
- проанализированы и исследованы возможные варианты и типы систем удаленной аутентификации;

- предложена математическая модель и алгоритм решения задачи передачи информации по незащищенным беспроводным каналам связи .

Результаты исследования: аутентификация на базе гибридной вероятностной модели криптографических преобразований.

позволит значительно повысить надежность аутентификации человека, получающего доступ к БД

Рекомендации:

- Аутентификация на базе гибридной вероятностной модели криптографических преобразований.
- Протоколы сетевой аутентификации Kerberos. Одним из главных преимуществ протокола Kerberos, которое гарантированно обеспечивает высокий уровень сетевой безопасности, базируется на том, что во всех сетевых взаимодействиях клиент-сервер не передаются ни пароли, ни хэши паролей в открытом виде.