Примерные темы курсовых работ, НИР, ВКР по кафедре «Информационная безопасность и теория управления» у доцента кафедры Иванцов А.М.

Примерный перечень тем курсовых работ по дисциплине «Защита информации от утечки по техническим каналам”

1. Разработка системы защиты от электромагнитных каналов утечки информации.
2. Разработка системы защиты акустических каналов утечки информации.
3. Сравнительный анализ характеристик средств обнаружения радиозакладок.
4. Оптические каналы утечки информации и их локализация.
5. Реализация защиты информации от утечки через ПЭМИН.
6. Сравнительный анализ моделей безопасности компьютерных систем.
7. Сравнительный анализ методов защиты персональных данных.
8. Сравнительный анализ уязвимостей сайтов от возможных атак.
9. Сравнительный анализ методов аутентификации пользователей информационных систем.
10. Сравнительный анализ методов, используемых в типовых системах контроля и управления доступом (СКУД) предприятий.
11. Сравнительный анализ методов доступа в информационных системах.
12. Сравнительный анализ возможностей программно-аппаратных комплексов защиты информации от НСД.
13. Сравнительный анализ методов стеганографии для скрытия информации.
14. Сравнительный анализ методов защиты информации в базах данных.
15. Сравнительный анализ методов физической защиты объектов информатизации.

по дисциплине «Организация ЭВМ”

1. Разработка системы контроля и управления доступом предприятия.
2. Проблемы энергетического скрытия речевой информации в телефонных линиях связи и принципы их решения.
3. Разработка системы защиты от электромагнитных каналов утечки информации.
4. Разработка системы защиты акустических каналов утечки информации.
5. Анализ эффективности использования физических средств защиты.
6. Принципы обнаружения и локализации радиозакладок.
7. Сравнительный анализ характеристик средств обнаружения радиозакладок.
8. Оптические каналы утечки информации и их локализация.
9. Реализация защиты информации от утечки через ПЭМИН.
10. Предотвращение утечки информации по цепям электропитания и заземления.
11. Способы увеличения дальности скрытного наблюдения в оптическом видимом и инфракрасном диапазонах
12. Сравнительный анализ возможностей программно-аппаратных комплексов защиты информации от НСД.

Примерный перечень тем курсовых работ по дисциплине “Криптографические методы защиты информации”

1. Применение алгоритма ГОСТ Р34.11-2012 для хэширования ключевой информации.
2. Разработка диспетчера доступа для типовой информационной системы.
3. Аутентификация ОС МСВС.
4. Разработка системы аутентификации Windows для типового предприятия.
5. Разработка стеганографической подсистемы защиты информации предприятия на основе методов скрытия информации в аудиофайлах.
6. Разработка подсистемы защиты электронного документооборота предприятия.

7. Разработка подсистемы разграничения доступа к информации на основе модели Take-Grant.
8. Разработка подсистемы защиты сайта от SQL-инъекции.
9. Разработка системы аутентификации для информационной системы типового предприятия.
10. Безопасность обработки данных облачными сервисами.
11. Разработка стеганографической подсистемы защиты информации предприятия на основе использования методов текстовой стеганографии.
12. Разработка стеганографической подсистемы защиты информации предприятия на основе использования цифровых водяных знаков.
13. Разработка подсистемы защиты школьников от нежелательного контента.
14. Разработка системы защиты веб-ресурсов.

Примерный перечень тем курсовых работ
по дисциплине "Криптографические протоколы и стандарты

1. Разработка диспетчера доступа для типовой информационной системы.
2. Разработка подсистемы разграничения доступа СУБД предприятия.
3. Разработка стеганографической подсистемы защиты информации предприятия на основе методов скрытия информации в аудиофайлах.
4. Разработка подсистемы разграничения доступа СУБД предприятия.
5. Разработка подсистемы защиты электронного документооборота предприятия.
6. Разработка подсистемы разграничения доступа к информации на основе модели Харрисона-Руззо-Ульмана.
7. Разработка подсистемы защиты сайта от SQL-инъекции.
8. Разработка системы аутентификации для информационной системы типового предприятия.
9. Безопасность обработки данных облачными сервисами.
10. Модель администрирования ролевого управления доступом предприятия.
11. Разработка стеганографической подсистемы защиты информации предприятия на основе использования методов текстовой стеганографии.
12. Разработка подсистемы аутентификации веб-приложения предприятия.
13. Разработка полсистемы СКУД типового предприятия.
14. Разработка автоматизированной обучающей системы по изучению критических систем информационной инфраструктуры.

Примерный перечень тем курсовых работ
по дисциплине «Методы алгебраической геометрии в криптографии»

1. Разработка лабораторного практикума по изучению СЗИ от НСД Dallas Lock 8.0.
2. Разработка системы защиты электронного документооборота учебного заведения.
3. Модель администрирования ролевого управления доступом предприятия.
4. Разработка защищённой системы контроля компьютеров, периферийного оборудования и программного обеспечения в доменной сети УлГУ.

Примерный перечень тем НИР (КБ-6 курс)

1. Разработка защищённой автоматизированной обучающей системы для освоения системы защиты информации «Dallas Losk».

2. Разработка защищённой информационной системы по контролю ИТ-активов УлГУ.
3. Программная реализация криптографической защиты подсистемы мониторинга USB-устройств.
4. Программная реализация подсистемы контроля целостности данных системы управления базами данных предприятия.
5. Применение российских стандартов шифрования для защиты электронного документооборота предприятия.
6. Программная реализация передачи ключей в криптографической подсистеме СКУД.
7. Применение USB-токена на базе «КриптоПро» для обеспечения усиленной аутентификации операционной системы WINDOWS.
8. Программная реализация контроля целостности данных СУБД на основе отечественных криптографических стандартов.
9. Распределение и хранение ключей в системе защищенного документооборота предприятия.
10. Разработка системы защиты информации ограниченного доступа СУБД средствами динамического разграничения прав доступа.
11. Программная реализация централизованного сбора информации о нарушениях ИБ в информационной системе предприятия.
12. Разработка криптографической системы безопасного хранилища ключевой информации

Примерный перечень тем НИР (ИБАС-5 курс)

1. Разработка веб-приложения для защиты персональных данных в веб-ресурсах.
2. Программная реализация криптографической защиты подсистемы мониторинга USB-устройств.
3. Программная реализация подсистемы контроля целостности данных системы управления базами данных предприятия.
6. Разработка алгоритма оценки защищенности информационной системы от НСД к информации.
4. Программная реализация определения скрытого содержимого изображений для выявления фактов несанкционированной утечки информации
7. Программная реализация определения скрытого содержимого аудиофайлов для выявления фактов несанкционированной утечки информации.
8. Применение российских стандартов шифрования для усиленной аутентификации операционной системы.
9. Разработка защищённого веб-приложения для удалённой работы с сервером организации.
10. Применение низкоскоресурсной криптографии для RFID-меток в СКУД предприятия.
11. Исследование стойкости внедрённого ЦВЗ к различным видам воздействий.
12. Разработка программного комплекса аудита информационной безопасности для администратора безопасности предприятия.
13. Программная реализация централизованного сбора информации о нарушениях ИБ в информационной системе предприятия.

Примерный перечень тем ВКР

1. Обеспечение целостности информации СУБД предприятия за счёт использования ГОСТ Р 34.11-2012.
2. Разработка системы защищённого электронного документооборота предприятия на основе облачной инфраструктуры.
3. Разработка системы защиты персональных данных в веб-ресурсах.

4. Разработка защищённой автоматизированной обучающей системы для освоения системы защиты информации «Dallas Losk.
5. Мониторинг защищённости информационной системы предприятия.
7. Аутентификация информационных систем.
8. Стеганографическая подсистема защиты информации предприятия.
9. Система разграничения доступа СУБД предприятия.
10. Система контроля целостности данных с помощью хеш-функций.
11. Система контроля и управления доступом предприятия.
12. Повышение безопасности систем электронного документооборота предприятия.
13. Повышение защищённости ключевой информации на основе использования автономного микроконтроллера.
14. Повышение уровня физической защиты объектов информатизации.
15. Повышение уровня информационной безопасности банковских систем.
16. Применение облачных технологий для безопасного хранения информации.
17. Повышение защищённости информации предприятия за счёт внедрения цифровых водяных знаков.
18. Применение мандатной модели для управления доступом в информационной системе предприятия.
19. Повышение уровня информационной безопасности системы аутентификации Windows.
20. Применение расширенной модели Take-Grant для управления доступом информационной системы предприятия.