

Федеральное государственное образовательное бюджетное учреждение
высшего образования
«Финансовый университет при Правительстве РФ»
(Финансовый университет)

Колледж информатики и программирования

УТВЕРЖДАЮ

Заместитель директора
по учебной работе

 Н.Ю. Долгова

« 07 » октября 2025 г.

Примерный перечень курсовых проектов (работ)

по профессиональному модулю ПМ.03 Защита информации техническими
средствами

специальности 10.02.05 Обеспечение информационной безопасности
автоматизированных систем

Рассмотрены
предметной (цикловой) комиссией
Обеспечение информационной безопасности АС

«11» сентября 2025 г.

Протокол № 1

Председатель предметной (цикловой) комиссии:
Маринич А.Л.

Москва 2025

Примерные темы курсовых работ

1. Совершенствование комплексной системы безопасности образовательной организации дошкольного образования на примере...
2. Разработка интегрированной модели безопасности общеобразовательной организации на основе анализа рисков и угроз.
3. Анализ эффективности и разработка предложений по модернизации системы тревожной и охранной сигнализации розничного предприятия.
4. Проектирование интегрированной системы видеонаблюдения и охранной сигнализации для объекта с повышенной криминогенной нагрузкой.
5. Интеграция системы противопожарной сигнализации и системы оповещения и управления эвакуацией для объектов с массовым пребыванием людей.
6. Особенности построения системы пожарной сигнализации и СОУЭ на объектах складской логистики с учетом категории по взрывопожарной опасности.
7. Оптимизация системы контроля и управления доступом (СКУД) и видеонаблюдения (СОТ) в офисном центре арендного типа.
8. Разработка модели угроз и построение системы физической защиты центра обработки данных
9. Комплексный подход к обеспечению физической безопасности телекоммуникационной инфраструктуры интернет-провайдера.
10. Организация защиты помещения с ведением конфиденциального документооборота и переговоров от утечки информации по техническим каналам.
11. Разработка комплекса организационно-технических мероприятий по обеспечению безопасности конфиденциальных переговоров.

12. Методика выбора средств и комплексов физической защиты для объекта (на примере) информатизации в соответствии с моделью угроз.

13. Анализ технических средств обнаружения для систем физической защиты объектов информатизации.

14. Разработка частной модели угроз физической безопасности для объекта информатизации 1 или 2 класса защищенности (на примере).

15. Обеспечение отказоустойчивого электропитания критически важных компонентов объекта информатизации.

16. Повышение эффективности системы видеонаблюдения объекта информатизации за счет внедрения видеоаналитики.

17. Анализ эффективности биометрических методов аутентификации в системах контроля доступа на режимные объекты.

18. Интеграция подсистем периметральной сигнализации в единый комплекс безопасности распределенного объекта.

19. Анализ угроз, связанных с БПЛА, и разработка комплекса мер по защите критически важных объектов.

20. Разработка алгоритма машинного обучения для прогнозной аналитики и выявления аномалий в работе систем физической защиты.

21. Внедрение элементов искусственного интеллекта для автоматизации реакции на тревожные события системы безопасности.

22. Разработка регламента взаимодействия подсистем СКУД и СОТ для верификации событий доступа.

23. Создание единого управляющего контура для подсистем охранной сигнализации, видеонаблюдения и оповещения.

24. Разработка методики проведения испытаний и тренировок системы физической защиты на устойчивость к НСД.

25. Формирование пакета организационно-распорядительной документации для системы физической защиты объекта информатизации.

26. Совершенствование системы оповещения населения на муниципальном уровне с использованием современных технических средств.

27. Выбор оптимального типа системы автоматического пожаротушения для объекта информатизации с учетом сохранности оборудования.

28. Разработка методики проведения аттестационных испытаний системы физической защиты объекта информатизации на основе модели нарушителя