

## ПРИЛОЖЕНИЕ 5

### Аннотация государственной итоговой аттестации

Трудоемкость в зачетных единицах	4 семестр – 6
Часов (всего) по учебному плану	216
включая:  подготовку к процедуре защиты и процедура защиты выпускной квалификационной работы	4 семестр – 216 часов

Цель государственной итоговой аттестации: оценка подготовленности обучающегося к решению задач профессиональной деятельности.

Примерная тематика выпускных квалификационных работ:

1. Управление событиями информационной безопасности в SIEM-системах.
2. Сравнительный анализ практических правил стандарта ГОСТ Р ИСО/МЭК 27002 и требований нормативных документов по защите КИИ.
3. Использование системы мониторинга Zabbix в качестве сканера безопасности.
4. Реагирование на инциденты информационной безопасности в банковской сфере с использованием платформы «SECURITY VISION».
5. Технологии внедрения облачной электронной подписи в ЕАИС ФТС РОССИИ
6. Мониторинг политики сетевой безопасности на основе модели сценариев атак.
7. Проблема создания единой методологии гарантированной защиты информации для различных видов тайн.
8. Разработка способа мониторинга безопасности IoT-устройств на базе MQTT-брокера.
9. Оценка возможности создания единой методики защиты информации.
10. Моделирование процессов непрерывности бизнеса в информационной безопасности.
11. Оценка эффективности систем управления информационной безопасности на имитационных моделях.
12. Повышение уровня доверия к технологии блокчейн с использованием подхода «Общих критериев».
13. Разработка описательных вариативных моделей объектов критической информационной инфраструктуры.
14. Разработка методики проведения теста на проникновение в информационные системы финансово-кредитных организаций на основе лучших практик.
15. Разработка научно-методического обеспечения обучения администрированию безопасности операционных систем.
16. Разработка алгоритмов и методик оценки эффективности систем обеспечения информационной безопасности на имитационных моделях
17. Разработка методики проведения выявления и расследования инцидентов утечки информации в корпоративных информационных системах с использованием DLP-систем.
18. Моделирование процессов влияния алгоритмов обработки информации на побочные электромагнитные излучения в ПЭВМ.

19. Моделирование и оценка уровня ПЭМИ для стационарных компьютеров организационно-техническими методами.
20. Применение технологий проактивной защиты SIEM при мониторинге событий информационной безопасности.
21. Проактивные системы информационной безопасности и особенности их применения в корпоративных информационных системах.
22. Научно-методическое обеспечение для обучения технологиям тестирования безопасности прикладного программного обеспечения, используемого в WEB-сервисах.
23. Научно-методическое обеспечение аудита информационной безопасности информационных систем.
24. Научно-методическое обеспечение обучения методам и технологиям администрирования сетевого оборудования в защищенных информационных системах.
25. Научно-методическое обеспечение обучения технологиям создания удостоверяющего центра на основе OpenSSL.
26. Научно-методическое обеспечение применения механизмов защиты конфиденциальной речевой информации в сегменте корпоративной сети VOIP.
27. Научно-методическое обеспечение защиты коммерческой тайны в корпоративной информационной системе.
28. Научно-методическое обеспечение расследования инцидентов информационной безопасности информационных систем.
29. Научно-методическое обеспечение обучения технологиям защиты информационных систем от кибератак в формате “attack-defense”.
30. Научно-методическое обеспечение для обучения технологиям криптографической защиты информации.