

Перечень примерных тем ВКР (бакалавриат) 2026/2027 уч.г.

10.03.01 Информационная безопасность

1. Система предотвращения утечек конфиденциальной информации через каналы удаленной работы сотрудников
2. Модель анализа риска использования нейросетей и генеративного искусственного интеллекта в финансовых сервисах
3. Алгоритм устранения уязвимостей систем смарт-контрактов в децентрализованных финансовых сервисах
4. Модель минимизации рисков инсайдерских угроз в кредитной организации
5. Модель обеспечения комплексной безопасности веб-приложения с применением средств защиты на основе методов распознавания
6. Алгоритм генерации этапов проведения расследований компьютерных инцидентов в КФО
7. Алгоритм оценки рисков безопасности объектов банковской инфраструктуры с учетом требований регуляторов России
8. Система мониторинга и аудита инцидентов информационной безопасности в информационной инфраструктуре банка
9. Система межсетевого экранирования и сегментирования сети в инфраструктуре ЦОД
10. Алгоритм системы многофакторной аутентификации для сотрудников финансовой организации на базе концепции нулевого доверия
11. Модель безопасности финансовых транзакций в условиях санкционных ограничений
12. Модель внедрения технических средств, применяемых для обеспечения безопасности кредитно-финансовой организации
13. Алгоритм анализа производительности и стойкости к современным атакам актуальных симметричных алгоритмов
14. Система защиты передачи данных с гибридным шифрованием
15. Алгоритмы уязвимости и защита от атак на современные хеш-функции
16. Алгоритм применения постквантовых алгоритмов на примере Kyber
17. Алгоритм применения постквантовых алгоритмов на примере Dilithium
18. Микросегментированная корпоративная сеть с динамической проверкой эффективности защиты методом непрерывного тестирования
19. Метод выявления скрытых привилегированных учетных записей в Active Directory на основе анализа графа делегирования и истории изменений
20. Метод обнаружения атак типа «low and slow» в корпоративной сети на основе анализа временных рядов сетевого трафика
21. Метод оценки защищенности корпоративной сети на основе построения и анализа графа достижимости атакующего с учётом бизнес-критичности активов

22. Метод выявления аномального поведения пользователей в корпоративной сети на основе анализа последовательностей событий с помощью трансформерных моделей

23. Метод обнаружения DNS-туннелирования в корпоративной сети на основе анализа энтропии поддоменов и временных характеристик запросов

24. Метод выявления атак на цепочку поставок ПО в корпоративной среде на основе анализа различий сборки

25. Метод выявления аномалий в кредитных скоринговых системах на основе анализа поведения API и защиты от состязательных атак на входные данные

26. Метод выявления инсайдерских аномалий в корпоративной сети банка на основе анализа последовательностей действий в АБС и SIEM-событиях

27. Комплекс мер по защите информации от несанкционированного доступа в кредитно-финансовой организации (на конкретном примере)

28. Алгоритм организации системы безопасности на объекте кредитно-финансовой сферы с применением концепции нулевого доверия

29. Адаптация комплекса средств защиты PAM, SIEM и DLP под информационную инфраструктуру кредитно-финансовой организации

30. Модель оценки соответствия банковских систем (ДБО, АБС) требованиям ЦБ РФ

31. Модель защиты информации каршеринговой компании ...

32. Алгоритм организации безопасности при использовании облачных технологий в банковской сфере

33. Алгоритм устранения уязвимости в сетевой инфраструктуре цифрового рубля в кредитной организации

34. Модель криптографической защиты инфраструктуры доверия цифрового рубля в финансовой организации

35. Модель инфраструктуры доверия в системе защищенности цифрового рубля в кредитной организации

36. Модель защиты от социальной инженерии и фишинговых атак в кредитной организации

37. Система управления инцидентами информационной безопасности в кредитных организациях

38. Модель обеспечения безопасности данных в облачных хранилищах и сервисах в кредитных организациях

39. Модель влияния социальной инженерии на безопасность информационно-технологических систем инфраструктуры доверия цифрового рубля в кредитных организациях

40. Модель манипуляции клиентами с целью получения доступа к информации на примере кредитных организаций

41. Модель программно-аппаратного комплекса аудита безопасности интерфейсов ввода

42. Система защиты информации государственного учреждения в современных условиях импортозамещения
43. Алгоритм защиты от фишинга на основе искусственного интеллекта
44. Алгоритм применения искусственного интеллекта для обнаружения аномалий и верификации доверия в системах электронного документооборота
45. Алгоритм защиты и устойчивости моделей компьютерного зрения в автономных транспортных средствах
46. Модель обнаружения атак типа «инъекция промптов» в корпоративных больших языковых моделях с использованием анализа семантических отклонений
47. Алгоритм динамической оценки уровня доверия к пользовательским сессиям в архитектуре Zero Trust с учетом поведенческих биометрических факторов
48. Модель контроля целостности и выявления несанкционированных модификаций в программном обеспечении на базе отечественных операционных систем
49. Алгоритм прогнозирования инсайдерских угроз на основе графового анализа взаимодействий сотрудников с информационными активами организации
50. Модель детектирования синтезированного медиаконтента в корпоративных системах видеоконференцсвязи
51. Алгоритм планирования и внедрения системы обеспечения инфомационной безопасности в организации финансовой сферы
52. Алгоритм прогнозирования инцидентов на объектах оценки с использованием нейросетевых моделей
53. Алгоритм обеспечения ИБ на объектах КИИ (на примере конкретной организации)
54. Алгоритм управления доступом к информации в целях обеспечения ИБ в организации финансового сектора
55. Система анализа и детектирования туннельных атак в VPN-соединениях
56. Модель классификации сетевого трафика на основе статистического анализа потоков на уровне полезной нагрузки
57. Алгоритм интеграции IDS с системой управления доступом для динамической реакции на инциденты в VPN сегменте
58. Модель DLP-агента для рабочих станций с функцией контроля маршрутизации: выявление случаев отправки конфиденциальных файлов мимо VPN-интерфейса
59. Модель предотвращения утечек данных через побочные каналы VPN с реализацией в виде набора конфигураций, правил и шаблонов политик
60. Система категорирования объектов КИИ (на примере конкретной организации)

61. Модель организации безопасности корпоративной сети при гибридной модели работы

62. Алгоритм выявления теневого использования ИИ-сервисов в корпоративной инфраструктуре