**Перечень примерных тем ВКР (бакалавриат) 2024/2025 уч.г.**

10.03.01 Информационная безопасность

|  |  |
| --- | --- |
|  | Минимизация рисков информационной безопасности в компании при обеспечении доступа в Интернет. |
|  | Обеспечение информационной безопасности компании с помощью внедрения DLP системы. |
|  | Организация центра мониторинга и оперативного реагирования на инциденты информационной безопасности (SOC) в компании. |
|  | Минимизация рисков информационной безопасности электронного документооборота в корпоративной сети компании. |
|  | DDoS-атаки как угроза для бизнеса в Интернете: методы и средства защиты (на примере конкретной организации). |
|  | Анализ угроз и внедрение управления рисками информационной безопасности в системах электронного бизнеса компании. |
|  | Методы статистического распознавания образов в задачах информационной безопасности. |
|  | Методы факторного анализа в задачах информационной безопасности. |
|  | Анализ и усовершенствование системы защиты Face Pay в московском метро. |
|  | Анализ алгоритмов сертификата электронной подписи в системе документооборота. |
|  | Разработка проекта системы защищенного электронного документооборота на предприятии коммерческой сферы. |
|  | Разработка проекта защиты информации каршеринговой компании. |
|  | Совершенствование обеспечения кибербезопасности на объекте КИИ. |
|  | Практическое применение норм технического регулирования при обеспечении безопасности объектов цифровой инфраструктуры. |
|  | Обеспечение информационной безопасности при обработке персональных данных в сфере гражданской авиации. |
|  | Внедрение программы повышения осведомленности персонала в области информационной безопасности. |
|  | Внедрение инструментов обеспечения информационной безопасности на предприятиях малого и среднего бизнеса. |
|  | Использование правового режима коммерческой тайны для обеспечения информационной безопасности. |
|  | Предотвращение рисков информационной безопасности обработки персональных данных на примере (объекта защиты). |
|  | Совершенствование алгоритмов проведения внутреннего аудита информационной безопасности в компании. |
|  | Разработка рекомендаций по защите объектов интеллектуальной собственности в предприятиях различных организационно-правовых форм. |
|  | Разработка системы комплексной защиты информации на объектах кредитно-финансовой сферы. |
|  | Разработка системы взаимосвязи организационных, правовых и технических методов защиты информации на объектах кредитно-финансовой сферы. |
|  | Разработка методики, концепции информационной безопасности и плана мероприятий по ее реализации на объектах кредитно-финансовой сферы. |
|  | Автоматизация экспертно-статистических, аналитических методов исследования информационных рисков и системы защиты объекта кредитно-финансовой сферы. |
|  | Разработка основных принципов применения технических средств и систем для обеспечения информационной безопасности объектов кредитно-финансовой сферы. |
|  | Разработка методики комплексного подхода к обеспечению информационной безопасности объекта кредитно-финансовой сферы. |
|  | Разработка проекта интегрированной системы безопасности объекта кредитно-финансовой сферы. |
|  | Проведение информационно-аналитической работы по обеспечению комплексной зашиты объекта информатизации кредитно-финансовой сферы. |
|  | Совершенствование алгоритмов хэширования для использования в условиях ограниченных ресурсов. |
|  | Совершенствование режимов работы блочных шифров для полнодискового шифрования. |
|  | Применение системы поведенческого анализа и обнаружения аномалий в продукте Турбо Трекинг. |
|  | Применение DevSecOps и организации архитектуры на базе отечественных решений. |
|  | Обеспечение ИБ финансовой организации методами киберразведки. |
|  | Организация противодействия утечки информации в организациях финансовой сферы. |
|  | Организация процесса безопасной разработки и внедрения ПО в финансовой организации. |
|  | Организация риск-ориентированной аутентификации в системах ДБО. |
|  | Организация защиты систем ДБО от DDOS-атак. |
|  | Организация противодействия операциям без согласия клиентов в банковской сфере. |
|  | Обеспечение защиты финансовой организации от угроз внутреннего злоумышленника. |
|  | Организация непрерывности бизнеса процессов обслуживания физических лиц в кредитно-финансовых организациях. |
|  | Обеспечение безопасности переводов денежных средств на базе электронных средств платежа. |
|  | Разработка методики проведения фаззинг-тестирования программного обеспечения с открытым кодом. |
|  | Разработка методики оценки соответствия банковских систем (ДБО, АБС) требованиям ЦБ. |
|  | Разработка методики противодействия протестному программному обеспечению с открытым кодом. |
|  | Разработка методики выявления компьютерных атак на основе поведенческого анализа. |
|  | Применение систем онлайн мониторинга при проведении финансовых транзакций в условиях санкций западных стран. |
|  | Использование технологий больших данных в области информационного противоборства. |
|  | Стрессо- и отказоустойчивые кластеры хранения информации, созданные на базе отечественного ПО и решений с открытым исходным кодом. |
|  | Организация защиты использования сети Интернет и электронной почты. |
|  | Совершенствование организации защиты информации с использованием криптографических средств. |
|  | Разработка стратегии кибербезопасности финансовой организации. |
|  | Разработка архитектуры информационной безопасности на объекте кредитно-финансовой сферы. |
|  | Разработка стратегии информационной безопасности на предприятии. |
|  | Совершенствование защиты облачной инфраструктур от кибератак. |
|  | Методы машинного обучения для обнаружения спама в приложениях и платформах IoT (Методы машинного обучения для обеспечения безопасности IoT). |
|  | Обнаружение лавинных DOS и DDOS атак с использованием машинного обучения. |
|  | Совершенствование системы программно-аппаратной защиты информации организации. |
|  | Совершенствование системы криптографической защиты информации на предприятии. |
|  | Совершенствование системы технической защиты информации на предприятии. |
|  | Совершенствование инженерно-технической защиты информации кредитно-финансовой организации. |
|  | Разработка требований к реализации системы контроля и местоположения устройств интернета вещей. |
|  | Внедрение DLP-системы в организации.(по профилю). |
|  | Разработка и внедрение системы закупок отечественного программного обеспечения в сфере информационной безопасности по выбранным критериям. |
|  | Разработка и внедрение системы анализа и классификации статистики утечек информации по каналам связи сети Интернет. |
|  | Совершенствование защиты прикладных программных интерфейсов (API) финансовых услуг. |
|  | Система киберзащиты интернет-магазина. |
|  | Система киберзащиты корпоративного сайта. |
|  | Организация защиты предприятия от утечек информации с использованием DLP систем. |
|  | Обеспечение безопасности финансовых транзакций цифровых денег. |
|  | Обеспечение безопасности облачных сервисов организации. |
|  | Организация защиты устройств интернета вещей в инфраструктуре организации. |
|  | Дизайн и моделирования безопасных бизнес-процессов организации. |
|  | Экспериментальное исследование ключевого расписания на основе модифицированных аддитивных генераторов для симметричных блочных шифров, определяющих защищенность данных в информационных сетях финансовых организаций. |
|  | Экспериментальное исследование криптографических свойств генератора с перемежающимся шагом на основе линейного регистра сдвига и аддитивных генераторов, определяющие стойкость поточного шифрования в информационных сетях финансовых организаций. |
|  | Оценка параметров хэш-функций семейства Меркла-Дамгора, определяющих стойкость криптосистем, с помощью матрично-графового подхода к анализу нелинейности (MD5, SHA-1, SHA-2). |
|  | Оценка параметров хэш-функций типа ГОСТ 34.11-2018, определяющих стойкость криптосистем, с помощью матрично-графового подхода к анализу нелинейности. |
|  | Экспериментальное исследование автоматных моделей генераторов псевдослучайных последовательностей с большой длиной периода выхода для защиты данных в информационных сетях финансовых организаций. |
|  | Экспериментальное исследование семейства псевдослучайных s-боксов большого размера на основе модифицированных аддитивных генераторов для итеративных блочных шифров, определяющих защищенность данных в информационных сетях финансовых организаций. |
|  | Защита от интернет-мошенничества при помощи алгоритмов машинного обучения. |
|  | Совершенствование алгоритмов выявления спама и мошеннических сообщений. |
|  | Разработка и усовершенствование методов деперсонализации текстовой информации (автоматическое удаление/замена персональных данных из текста). |
|  | Исследование технических каналов утечки (отдельная для каждого канала) объекта(ов) информатизации финансовой организации (на примере конкретной организации или модели). |
|  | Исследование (разработка устройства/комплекса мер/методических рекомендаций) канала утечки информации по средствам модуляции видимого света светодиодного освещения на объекте финансовой организации (на примере конкретной организации или модели). |
|  | Проект систем технической охраны объектов информатизации финансовой организации (на примере конкретной организации или модели) в различных климатических зонах (или других ограничениях: температурных, ресурсных, повышенной нагрузки пользования, распределенность объекта, высокие требования отказоустойчивости, использование беспроводных интерфейсов, интернета вещей и т.д.) |
|  | Разработка (исследование/методические рекомендации) системы информационной безопасности финансовых подразделений в рамках безопасности АСУТП конкретного предприятия. |
|  | Разработка программно-аппаратных устройств (выявления/блокирования) (одного или несколько) каналов утечки. |
|  | Комплексная защита от утечки информации в финансовой организации (на примере конкретной организации или модели). |
|  | Исследование технических каналов утечки (каждый канал отдельная работа) терминалов платежных и банковских систем. |
|  | Разработка комплекса мер по защите информации от несанкционированного доступа в финансовой организации (на примере конкретной организации или модели). |
|  | Разработка комплекса мер по обеспечению информационной безопасности сетевой структуры в финансовой организации (на примере конкретной организации или модели). |
|  | Разработка политики нулевого доверия для кредитно-финансовой организации |
|  | Совершенствование защищенности API финансовых услуг |
|  | Совершенствование защиты среды контейнеризации |
|  | Автоматизация противодействия дезинформации о деятельности финансовой организации в социальных сетях |
|  | Совершенствование автоматического анализа и категорирования событий информационной безопасности |
|  | Применение технологии распределенных реестров в системах защиты информации |
|  | Практическое применение методов исследования операций в задачах обеспечения информационной безопасности |
|  | Практическое применение методв теории игр в задачах обеспечения информационной безопасности |