Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение

высшего образования

**«Пермский национальный исследовательский**

**политехнический университет»**

**ПРОГРАММА**

**вступительного испытания по специальной дисциплине по программе подготовки научных и научно-педагогических кадров в аспирантуре**

|  |  |
| --- | --- |
|  |  |
|  |  |
| **Научная специальность** | 2.3.6. Методы и системы защиты  |
|  | информации, информационная безопасность |
|  |  |
| **Направленность (профиль)****программы аспирантуры** | Информационная безопасность сервисов и систем умного города |
| **Обеспечивающие кафедры:** | Автоматика и телемеханика (АТ) |

Руководитель программы:

Южаков А.А., заведующий кафедрой АТ/

**Пермь 2022 г.**

**Для поступающих на кафедру**

**«АВТОМАТИКА И ТЕЛЕМЕХАНИКА»**

**1. Вопросы**

1.1. *Технология защиты информации в открытых информационно-управляющих системах*

1.1.1 Методы и средства идентификации и аутентификации. Многофакторная аутентификация. Проблемы биометрических систем аутентификации.

1.1.2 Методы и средства авторизация. Формальные модели управления доступом. Проблемы авторизации в p2p и m2m системах.

1.1.3 Методы и средства криптографической защиты информации при передаче по каналам связи. Протоколы VPN. Стандарт PKCS. Протокол TLS. Протокол IPSec.

1.1.4 Методы и средства мониторинга распределенных систем.

1.1.5 Традиционные и современные архитектуры защиты открытых систем. Проблемы традиционных архитектуры безопасности. Концепция нулевого доверия.

1.1.6 Инфраструктура открытых ключей всети интернет. Принципы работы. Проблемы безопасности.

1.1.7 Симметричные и ассиметричные криптографические алгоритмы. Проблемы протокола RSA. Криптография на эллиптических кривых. Хэш-функции.

1.1.8 Аудит информационной безопасности в открытых информационно-управляющих система. Пассивные и активные методы аудита безопасности.

1.1.9 Методы аутентификации и авторизации в микросервисных архитектурах.

1.1.10 Проблемы управления защитой информации в распределенных информационно-управляющих системах

1.2. *Методология оценки рисков информационной безопасности*

1.2.1 Методология оценки угроз безопасности информации. Модель нарушителя. Формальные модели угроз.

1.2.2 Методология оценки рисков информационной безопасности. Понятие риска информационной безопасности. Классификация рисков.

1.2.3 Методология оценки рисков информационной безопасности OWASP.

1.2.4 Методология оценки угроз безопасности STRIDE&DREAD

1.2.5 Понятие цепочки кибер-атаки. Матрица MITREATT&CK

1.2.6 Методика оценки угроз безопасности ФСТЭК. Понятия поверхности атаки и защиты.

1.2.7 Методика оценки угроз КИИ. Проблемы оценки угроз безопасности КИИ.

1.3. *Управление информационной безопасностью*

1.3.1 Взаимосвязь понятий «управление» «процесс» и «система». Сущность системного подхода. Понятие системы управления и ее структура. Сущность и функции управления.

1.3.2.Цель и задачи управления информационной безопасностью (ИБ). Этапы развития стандартов серии ISO/IEC 27000. Преимущества и недостатки внедрения системы управления ИБ, в соответствии со стандартами ISO.

1.3.3.Отраслевые стандарты и рекомендации по стандартизации серии СТО БР ИББС РФ.

1.3.4.Стандарты CoBiT. Показатели эффективности CoBiT.

* + 1. Требования и принципы при разработке и внедрении политики ИБ предприятия (организации). Содержание и жизненный цикл политики ИБ.
		2. Система управления информационной безопасностью (СУИБ) организации и цель ее разработки. Требования к СУИБ. Цели процесса управления в соответствии с SLA.
		3. Событие и инцидент. Управление инцидентами ИБ. Цели организации по управлению инцидентами ИБ. Этапы процесса управления инцидентами ИБ, в соответствии с моделью PDCA.
		4. Виды проверок СУИБ. Мониторинг и самооценка ИБ.
		5. Понятие, нормативное обеспечение, цели и виды аудита ИБ. Принципы проведения аудита. Программа аудита ИБ. Управление программой аудита ИБ.
		6. Измерение эффективности СУИБ. Метрики эффективности. Содержание и организация процесса аудита ИБ.

*1.4. Правовая защита информации*

1.4.1. Информация как объект правоотношений, категории информации. Понятие и виды информации ограниченного доступа.

1.4.2. Основные виды конфиденциальной информации, в соответствии с требованиями российской нормативно-правовой базы. Правовой режим конфиденциальной информации.

1.4.2. Основные понятия и содержание закона РФ «О персональных данных». Подзаконные нормативно-правовые документы о порядке правовой защиты персональных данных.

1.4.3. Государственный надзор и контроль обработки персональных данных, ответственность за нарушения российского законодательства в области обработки и защиты персональных данных.

1.4.4. Правовые основы лицензирования и сертификации в области защиты информации.

1.4.5. Особенности правонарушений в информационной сфере. Преступления в сфере компьютерной информации: виды, состав.

1.4.6.Приказы и специальные нормативные документы ФСТЭК России по защите информационных систем.

1.4.7. Правовые основы применения электронной подписи.

1.4.8. Правовая защита результатов интеллектуальной деятельности. Результаты интеллектуальной деятельности. Права на средства индивидуализации.

1.4.9. Система нормативных правовых актов по вопросам обеспечения безопасности КИИ РФ. Ответственность за нарушение законодательства о безопасности КИИ РФ.

1.4.10. Основные мероприятия по категорированию объектов КИИ. Порядок формирования требований по обеспечению защиты значимых объектов КИИ. Требования к созданию систем безопасности значимых объектов КИИ.

**2. Рекомендуемая литература, информационные ресурсы**

1. Основы управления информационной безопасностью: учебное пособие для вузов / А. П. Курило [и др.] .— 2-е изд., испр.— Москва : Горячая линия-Телеком, 2014.- 243 с.
2. Милославская Н. Г. Проверка и оценка деятельности по управлению информационной безопасностью: учебное пособие для вузов / Н. Г. Милославская, А. И. Толстой, М. Ю. Сенаторов. - Москва: Горячая линия-Телеком, 2018.
3. Милославская Н. Г. Технические, организационные и кадровые аспекты управления информационной безопасностью: учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - Москва: Горячая линия-Телеком, 2012.
4. Милославская Н. Г. Управление инцидентами информационной безопасности и неперерывностью бизнеса : учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - Москва: Горячая линия-Телеком, 2014.
5. Милославская Н. Г. Управление рисками информационной безопасности : учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - Москва: Горячая линия-Телеком, 2014.
6. Ажмухамедов И. М., Князева О.М. Основы организационно-правового обеспечения информационной безопасности. Учебное пособие СПб.: «Интермедия», 2017.— 264 с.
7. Северин В.А. Правовая защита информации в коммерческих организациях : учебное пособие для вузов / В.А. Северин. - Москва: Академия, 2009.

**3. Пример экзаменационного билета**

|  |  |
| --- | --- |
| ПЕРМСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ | УТВЕРЖДАЮЗаведующий кафедрой«Автоматика и телемеханика»Вступительные испытания по специальной дисциплине, соответствующей научной специальностиИнформационная безопасность умного города |
| *2.3.6. Методы и системы защиты информации, информационная безопасность* |
| ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №11. Методы и средства идентификации и аутентификации. Многофакторная аутентификация. Проблемы биометрических систем аутентификации.
2. Методика оценки угроз безопасности ФСТЭК. Понятия поверхности атаки и защиты.
3. Событие и инцидент. Управление инцидентами ИБ. Цели организации по управлению инцидентами ИБ. Этапы процесса управления инцидентами ИБ, в соответствии с моделью PDCA.
 |