Федеральное государственное бюджетное образовательное учреждение высшего образования

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «МЭИ»

«УТВЕРЖДАЮ»

Проректор ФГБОУ ВО «НИУ «МЭИ»

по научной работе

Драгунов В.К.

_____

«____» _____ 2023 г.

ПРОГРАММА ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ ПО СПЕЦИАЛЬНОЙ ДИСЦИПЛИНЕ ПРИ ПОСТУПЛЕНИИ В АСПИРАНТУРУ

Группа научных специальностей – 2.3 Информационные технологии и телекоммуникации

Научная специальность – 2.3.6 Методы и системы защиты информации, информационная безопасность

Москва, 2023

Программа по специальной дисциплине по кафедре БИТ

1. Теоретические основы информационных технологий и информационной безопасности

Основной контекст информационной безопасности: понятие, содержание, место информационной безопасности в современной системе национальной безопасности РФ. Основные понятия безопасности информации: перечень, сущность, классификация.

Современные концепции создания систем защиты информации в информационных системах и АСУ.

Основы системного подхода к обеспечению информационной безопасности в организации.

2. Организационное и правовое обеспечение информационной безопасности

2.1. Общая характеристика системы законодательного и нормативного регулирования информационной безопасности в РФ. Общая характеристика и полномочия «регуляторов» в области ИБ. Полномочия и деятельность Федеральной службы по техническому и экспортному контролю (ФСТЭК) России

2.2 Актуальные вопросы законодательного и нормативного регулирования защиты отдельных видов информации и обрабатывающих ее систем. Обеспечение персональных данных: современные аспекты проблемы, угрозы и вызовы.

Защита объектов критической информационной инфраструктуры (КИИ) РФ (на примере объектов энергетики). Система законодательных и нормативных требований по защите КИИ. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА): организация, структура, техническое обеспечение и порядок эксплуатации системы.

Защита государственных информационных систем (ГИС) РФ: нормативное регулирование обеспечения безопасности ГИС, комплекс требований по защите информации в ГИС.

Законодательное и нормативное регулирование обеспечения безопасности коммерческой тайны в РФ. Понятие режима коммерческой тайны и порядок его организации.

2.3. Нормативное регулирование менеджмента информационной безопасности

Система стандартов ГОСТ Р ИСО/МЭК 27000: состав, перечень, основные положения менеджмента информационной безопасности. Контекст менеджмента ИБ. Построение СМИБ на основе норм и правил. Связь и организация совместного использования для управления информационной безопасностью норм и правил менеджмента ИБ и менеджмента качества.

Лицензирование и сертификация средств и систем информационной безопасности. Система лицензирования и сертификации в РФ в области защиты информации. Правовая основа системы.

Лицензирование деятельности по защите информации: принципы; уполномоченные органы; последовательность действий организации при лицензировании деятельности по защите информации.

Сертификация средств защиты информации: принципы; порядок проведения сертификации; особенности сертификации средств криптографической защиты.

Управление рисками информационной безопасности и непрерывность бизнеса. Процесс менеджмента риска информационной безопасности на основе ГОСТ Р ИСО/МЭК 27005:2010. Общая характеристика видов деятельности, связанных с менеджментом риска ИБ: установление контекста; оценка; обработка; принятие; коммуникация; мониторинг и переоценка. Аспекты ИБ в рамках менеджмента непрерывности деятельности организации.

Обеспечение информационной безопасности на основе «лучших практик».

3. Программное и программно-аппаратное обеспечение информационной безопасности

3.1. Систематизация программных и программно-аппаратных средств защиты информации.

Общая характеристика, состав, основные функции и характеристика механизмов безопасности средств и систем:

- аутентификации и авторизации;
- защиты информации от вредоносного кода;
- обеспечения сетевой безопасности;
- резервирования и резервного копирования;
- контроля защищенности информационных систем;
- управления событиями и инцидентами в информационных системах;
- криптографической защиты информации.

3.2. Актуальные вопросы импортозамещения в программных и программно-аппаратных средствах защиты информации. Требования в области импортозамещения. Современное состояние импортозамещения в области программных и программно-аппаратных СЗИ, примеры. Пути решения проблемы импортозамещения. Перспективы решения проблемы импортозамещения.

4. Архитектура современной системы обеспечения информационной безопасности (СОИБП) предприятия (организации). Методы создания, организации, контроля и совершенствования СОИБП.

- цели, назначение и задачи СОИБП;
- структурная декомпозиция СОИБП. Вертикальная и горизонтальная декомпозиция. Перечень подсистем и элементов;
- подсистема организационно-правового обеспечения СОИБП: вертикальная и горизонтальная декомпозиция подсистемы;
- политика ИБ как инструмент управления функционированием подсистемы организационно-правового обеспечения;

- подсистема кадрового обеспечения СОИБП: состав, назначение, общая характеристика, перечень требований к должностным лицам, обеспечивающим информационную безопасность;

- декомпозиция подсистема кадрового обеспечения СОИБП;

- профессиональная этика в области обеспечения информационной безопасности предприятия: понятие, цель, перечень норм;

- подсистема финансово-экономического обеспечения СОИБП. Вертикальная и горизонтальная декомпозиция подсистемы;

- финансово-экономическое обоснование СОИБП на основе экономических моделей оценки совокупной стоимости владения и возврата инвестиций в инфраструктуру предприятия. Математическая интерпретация моделей;

- подсистема инженерно-технического обеспечения СОИБП. Назначение, понятие и общая характеристика;

- вертикальная и горизонтальная декомпозиция подсистемы инженерно-технического обеспечения СОИБП;

- комплекс средств инженерно-технической защиты территорий и помещений: перечень, назначение, состав, классификация и краткая характеристика;

- комплекс средств обнаружения и защиты технических каналов утечки информации: назначение, состав, классификация и краткая характеристика;

- подсистема программно-аппаратного обеспечения СОИБП. Вертикальная и горизонтальная декомпозиция подсистемы;

- комплекс средств программной и программно-аппаратной защиты информации: назначение, состав, классификация, краткая характеристика;

- подсистема аудита информационной безопасности предприятия: понятие, цель, требования руководящих документов к организации аудита;

- вертикальная и горизонтальная декомпозиция подсистемы аудита информационной безопасности предприятия;

- виды, задачи, последовательность и особенности проведения аудита информационной безопасности предприятия.

5. Современные проблемы информационной безопасности

5.1. Безопасность киберфизических систем (КФС). Особенности угроз и уязвимостей КФС и их компонентов, особенности защиты КФС от вредоносного программного обеспечения, методы выявления вредоносных возможностей в функциональных механизмах КФС. Методы защиты КФС от целенаправленных атак.

5.2. Квантовые технологии в системах защиты информации. Преобразование и передача информации в квантовых системах. Квантовая криптография и квантовый криптоанализ: перспективы и проблемы. Квантовая гонка.

5.3. Технологии распределенного реестра и смарт-контракты в системах защиты информации. Технология блокчейн. Сети распределенных реестров, классификация, отличия. Порядок достижения консессуса. Перспективы практического использования технологий в решении задач информационной безопасности: смарт-контракты, обеспечение доверия и безопасности. Преимущества и недостатки технологий.

5.4. Оценка безопасности информационных технологий. Проблема и критерии оценки безопасности информационных технологий. Международный опыт разработки «Общих критериев» оценки безопасности информационных технологий. Система стандартов ГОСТ Р ИСО/МЭК 15408 и поддерживающих их документов. Понятие и иерархия функциональных компонентов безопасности. Понятие и иерархия функциональных компонентов доверия к безопасности. Шкала доверия к безопасности информационных технологий. Понятие и содержание оценочного уровня доверия к безопасности. Практическое применение подхода «Общих критериев» к оценке безопасности информационных технологий.

5.5. Оценка защищенности и эффективности информационных систем. Организация мониторинга и оценки защищенности: сбор информации, анализ, оценка значений, информирование заинтересованных сторон. Особенности работы с результатами мониторинга и анализа защищенности с учетом конфиденциальности информации.

5.6. Применение методов и технологий искусственного интеллекта в системах информационной безопасности. Обеспечение оперативности реагирования на инциденты ИБ. Помощь в выполнении рутинных процедур обработки событий безопасности. Процедуры детектирования угроз, корреляции и машинного обучения в SIEM, IDS/IPS- и других решениях.

Основная литература:

1. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ (последняя редакция) \ КонсультантПлюс [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_220885.
2. Положение о Государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам. Положение «О государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам» [Электронный ресурс]. – Режим доступа: http://www.rfcmd.ru/sphider/docs/InfoSec/Postan_pravit_N 912_ot_15 _09 _93.htm.
3. Постановление Правительства РФ от 8 февраля 2018 г. N 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» [Электронный ресурс]. – Режим доступа: https://base.garant.ru /71876120/?ysclid=lblv64n63m345477409.
4. Приказ ФСТЭК от 18 февраля 2013 г. N 21 Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, https:// fstec.ru/tekhnicheskaya-zashchita-informatsii/ dokumenty/110-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21.
5. Приказ ФСТЭК 25 декабря 2017 г. N 239 Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры РФ, https://fstec.ru/ tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastru-ktury/288-prikazy/1592-prikaz-fstek-rossii-ot-25-de-kabrya-2017-g-n-239.

6. Минзов А.С., Баронов О.Р., Минзов С.А., Осипов П.А. Управление событиями информационной безопасности: Учебное пособие /Под редакцией профессора, д-ра техн. наук А.С. Минзова. — М. : ВНИИгеосистем, 2020. — 97 с. :ил.
7. Язов Ю., Соловьев С. В., Тарелкин М. А. Логико-лингвистическое моделирование угроз безопасности информации в информационных системах - //Вопросы кибербезопасности. – 2022. – №. 4. – С. 50.
8. Минзов А.С., Невский А.Ю., Баронов О.Р. Управление рисками информационной безопасности: Монография/ Под редакцией А.С. Минзова. — М. : ВНИИгеосистем, 2019. — 110 с. :ил.
9. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности ГОСТ Р ИСО/МЭК 27002-2021. [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/1200179669?ysclid=lblxx6v 8t1265273979.
10. ГОСТ Р ИСО/МЭК 27031-2012 ИТ. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru /document /1200105651?ysclid=lblw7kqt47444582468.
11. ГОСТ Р ИСО 22301-2014 Системы менеджмента непрерывности бизнеса. Общие требования [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/1200113802?ysclid=lblwbx fzi8470542616.
12. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. ГОСТ Р ИСО/МЭК 27001-2021 [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/ document/1200181890?ysclid=lblxsqiz5b453812468.
13. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения информационной безопасности. Менеджмент риска информационной безопасности. [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/ 1200084141?ysclid=lblxuuf 92p580200459.
14. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/ 1200101777?ysclid=lc90xrchwn717202223
15. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности. [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/1200105710?ysclid=lc911xata109864429
16. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности. [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/ document/1200105711?ysclid=lc913kse1n716516983
17. Программный комплекс UserGate Proxy & Firewall 5.2. F. Задание по безопасности UG_P&F_5.2.F.ЗБ, [Электронный ресурс], https://www.altx-soft.ru/files/groups/260.pdf.
18. Управление информационной безопасностью: учебное пособие для высшего профессионального образования / В.Т. Еременко, М.Ю. Рытов, П.Н. Рязанцев, М.Н. Орешина. – Орел: ФГБОУ ВПО «Госуниверситет - УНПК», 2015. – 265 с.

Дополнительная литература:

1. Куликов С. С. Модели безопасности компьютерных систем: учеб. пособие [Электронный ресурс]. – Электрон. текстовые, граф. данные (2,71 Мб) / С. С. Куликов. – Воронеж:
2. ГОСТ Р 57628-2017 Информационная технология. Методы и средства обеспечения безопасности.. Руководство по разработке профилей защиты и заданий по безопасности. [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/1200146707?ysclid=lc917gfix0105402730

3. ГОСТ Р ИСО/МЭК 18045-2013 Информационная технология. Методология оценки безопасности информационных технологий. [Электронный ресурс]. – Режим доступа:https://docs.cntd.ru/document/1200105309?ysclid=lc9199d1xy436637715
4. Назаров, Д. М. Интеллектуальные системы: основы теории нечетких множеств: учебное пособие для вузов / Д. М. Назаров, Л. К. Конышева. – 3-е изд., испр. и доп. – Москва: Издательство Юрайт, 2020. – 186 с.
5. Дорофеев А. В., Марков А. С. Планирование обеспечения непрерывности бизнеса и восстановления //Вопросы кибербезопасности. – 2015. – №. 3 (11). – С. 68-73.

«Согласовано»
Директор ИнЭИ
к.т.н., доцент

Невский А.Ю.