Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Пермский национальный исследовательский политехнический университет»

УТВЕРЖДАЮ
Руководитель программы аспирантуры

_____ А.А. Южаков
д.т.н., профессор кафедры АТ

«20» «мая» 2022 г.

Рабочая программа дисциплины по программе аспирантуры

«Безопасность критической информационной инфраструктуры умного города»

Научная специальность	2.3.6. Методы и системы защиты информации, информационная безопасность
Направленность (профиль) программы аспирантуры	Информационная безопасность сервисов и систем умного города
Выпускающая(ие) кафедра(ы)	Автоматика и телемеханика (АТ)

Форма обучения Очная

Курс: 3 **Семестр (ы):** 5

Виды контроля с указанием семестра:
Экзамен: Зачет:**5** Диф.зачет

Пермь 2022

1. Общие положения

Рабочая программа дисциплины «Безопасность критической информационной инфраструктуры умного города» разработана на основании следующих нормативных документов:

- Приказ Минобрнауки России от 20.10.2021 N 951 "Об утверждении федеральных государственных требований к структуре программ подготовки научных и научно-педагогических кадров в аспирантуре (адъюнктуре), условиям их реализации, срокам освоения этих программ с учетом различных форм обучения, образовательных технологий и особенностей отдельных категорий аспирантов (адъюнктов)";
- Постановление Правительства РФ от 30.11.2021 N 2122 "Об утверждении Положения о подготовке научных и научно-педагогических кадров в аспирантуре (адъюнктуре)";
- Самостоятельно устанавливаемые требования к реализуемым программам подготовки научных и научно-педагогических кадров в аспирантуре Пермского национального исследовательского политехнического университета;
- Базовый план по программе аспирантуры;
- Паспорт научной специальности 2.3.6 Методы и системы защиты информации, информационная безопасность.

1.1 Цель учебной дисциплины – формирование комплекса знаний, умений и навыков в области методов и средств обеспечения безопасности критической информационной инфраструктуры умного города.

1.2 Место учебной дисциплины в структуре образовательной программы

Дисциплина «Безопасность критической информационной инфраструктуры умного города» является дисциплиной по выбору образовательного компонента плана аспиранта.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

В результате изучения дисциплины аспирант должен демонстрировать следующие результаты:

Знать:

- Принципы оценки защищенности критической информационной инфраструктуры умного города;
- Основные угрозы информационной безопасности критической информационной инфраструктуры умного города.

Уметь:

- Разрабатывать системы защиты критической информационной инфраструктуры умного города;
- Внедрять перспективные средства защиты информации в критическую информационную инфраструктуру умного города.

Владеть:

- методами и средствами рационального выбора технических средств защиты информации;
- методами и средствами комплексной оценки информационной безопасности.

3. Структура учебной дисциплины по видам и формам учебной работы

Таблица 1

Объем и виды учебной работы

№ п.п.	Вид учебной работы	Трудоемкость, ч
		4 семестр
1	Аудиторная работа	39
	В том числе:	
	Лекции (Л)	
	Практические занятия (ПЗ)	32
2	Контроль самостоятельной работы (КСР)	7
	Самостоятельная работа (СР)	69
	Форма итогового контроля:	Зачет

4. Содержание учебной дисциплины

4.1. Содержание разделов и тем учебной дисциплины

Раздел 1. Международные и отечественные стандарты защиты критической информационной инфраструктуры
(ПР - 8 , СР – 24)

Тема 1. Международные стандарты защиты информации систем и сервисов умного города

Тема 2. Нормативно-правовая база ФСТЭК России по защите КИИ

Раздел 2. Технологии обеспечения информационной безопасности КИИ
(ПР - 16, СР – 24)

Тема 3. Система защиты КИИ

Тема 4. Интеграция системы защиты информации с НКЦКИ (ГосСОПКА)

Раздел 3. Технологии обеспечения безопасности и надежности КИИ
(ПР - 8, СР – 21)

Тема 5. Методы повышения надежности КИИ

Тема 6. Методы защиты КИИ от угроз целостности и доступности

4.2. Перечень тем практических занятий

Таблица 2

Темы практических занятий (из пункта 4.1)

№ п.п.	Номер темы дисциплины	Наименование темы практического занятия	Наименование оценочного средства	Представление оценочного средства
1	1	Методика оценки угроз информационной безопасности критической информационной инфраструктуры	Собеседование. Творческое задание.	Вопросы по темам / разделам дисциплины. Темы творческих заданий.
2	2	Особенности формирования политики безопасности КИИ	Собеседование. Творческое задание.	Вопросы по темам / разделам дисциплины. Темы творческих заданий.
3	3	Особенности требований	Собеседование.	Вопросы по

		безопасности КИИ	Творческое задание.	темам / разделам дисциплины. Темы творческих заданий.
4	4	Методика взаимодействия с НКЦКИ (ГосСОПКА)	Собеседование. Творческое задание.	Вопросы по темам / разделам дисциплины. Темы творческих заданий.
5	5	Методы резервирования в системе защиты критической информационной инфраструктуры	Собеседование. Творческое задание.	Вопросы по темам / разделам дисциплины. Темы творческих заданий.
6	6	Защита критической информационной инфраструктуры от DDoS-атак	Собеседование. Творческое задание.	Вопросы по темам / разделам дисциплины. Темы творческих заданий.

4.3. Перечень тем для самостоятельной работы аспирантов

Самостоятельная работа аспирантов заключается в теоретическом изучении конкретных вопросов и выполнении творческих заданий.

Таблица 3

Темы самостоятельных заданий

№ п.п.	Номер темы дисциплины	Наименование темы самостоятельной работы	Наименование оценочного средства	Представление оценочного средства
1	1,2	Стандарты в области информационной безопасности КИИ и АСУ ТП	Собеседование	Вопросы по темам / разделам дисциплины
2	3,4,5	Цели и функции ГосСОПКА и SOC центров	Творческое задание	Темы творческих заданий
3	6,7	Проблемы защиты инфраструктуры от DDoS-атак	Творческое задание	Темы творческих заданий

5. Методические указания для аспирантов по изучению дисциплины

При изучении дисциплины «Технологии защиты программного обеспечения систем и сервисов умного города» аспирантам целесообразно выполнять следующие рекомендации:

1. Изучение учебной дисциплины должно вестись систематически;

2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела;

3. Вся тематика вопросов, изучаемых самостоятельно, задается преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции;

6. Перечень учебно-методического, библиотечно-справочного и информационного, информационно-справочного обеспечения для работы аспиранта по дисциплине

6.1. Библиотечные фонды и библиотечно-справочные системы

№	**Библиографическое описание** *(автор, заглавие, вид издания, место, издательство, год издания, количество страниц)*	**Количество экземпляров** в библиотеке+кафедре; **местонахождение электронных изданий**
1	2	3
1 Основная литература		
1	Лысов А. В. Обеспечение безопасности значимых объектов критической информационной инфраструктуры. – 2019.	
2	Kleidermacher D., Kleidermacher M. Embedded systems security: practical methods for safe and secure software and systems development. – Elsevier, 2012.	
2 Дополнительная литература		
2.1 Учебно-методические, научные издания		
1	Мельников Д. А. Информационная безопасность открытых систем : учебник / Д. А. Мельников. - Москва: Флинта, Наука, 2013.	
2	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.	
2.2 Периодические издания		
1	Вопросы защиты информации	
2	Программная инженерия и информационная безопасность	
3	Управление информационными рисками и обеспечение безопасности инфокоммуникационных систем	
2.3 Нормативно-технические издания		
1	*Не используются*	
2.4 Официальные издания		
1	*Не используются*	

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

6.2.1. Информационные и информационно-справочные системы

Наименование	Ссылка на информационный ресурс
Электронно-библиотечеая система Лань	https://e.lanbook.com/
Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru/
Информационные ресурсы Сети КонсультантПлюс	http://www.consultant.ru/
Информационные ресурсы Сети КонсультантПлюс	http://www.consultant.ru/
База данных компании EBSCO	https://www.ebsco.com/
Информационно-справочная система нормативно-технической документации "Техэксперт: нормы, правила, стандарты и законодательства России"	https://техэксперт.сайт/

7. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

7.1. Основное учебное оборудование. Рабочее место аспиранта.

Таблица 4

№ п.п.	Наименование и марка оборудования (стенда, макета, плаката, лабораторное оборудование)	Кол-во, ед.	Форма приобретения / владения (собственность, оперативное управление, аренда и т.п.)	Номер аудитории
1	2	3	4	5
1	Персональные компьютеры (локальная компьютерная сеть)	12	Собственность	312
2	Сервер для моделирования информационных систем	1	Собственность	312

8. Фонд оценочных средств

Освоение учебного материала дисциплины запланировано в течение одного семестра. Формой контроля освоения результатов обучения по дисциплине является зачет, проводимый с учетом результатов текущего контроля.

8.1. Описание показателей и критериев оценивания, описание шкал оценивания.

Контроль качества освоения дисциплины включает в себя текущий контроль успеваемости и промежуточную аттестацию аспирантов

Текущий контроль

Текущий контроль успеваемости обеспечивает оценку освоения дисциплин и проводится в форме собеседования и защиты отчета о творческом задании.

- **Собеседование**

Для оценки **знаний** аспирантов проводится собеседование в виде специальной беседы преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной для выяснения объема знаний по определенному разделу, теме, проблеме.

Собеседование может выполняться в индивидуальном порядке или группой аспирантов.

- **Защита отчета о творческом задании**

Для оценки **умений и владений** аспирантов используется творческое задание, имеющее нестандартное решение и позволяющее интегрировать знания различных областей, аргументировать собственную точку зрения.

Творческие задания могут выполняться в индивидуальном порядке или группой аспирантов.

Промежуточная аттестация

Допуск к промежуточной аттестации осуществляется по результатам текущего

контроля. Промежуточная аттестация проводится в виде зачета по дисциплине, в формате собеседования.

- **Шкалы оценивания результатов обучения при сдаче зачета:**

Шкалы и критерии оценки результатов обучения при сдаче зачета приведены в табл. 5.

Таблица 5

Шкала оценивания результатов освоения на **зачете**

Оценка	Критерии оценивания
зачет	Аспирант продемонстрировал сформированные и систематические знания при ответе на теоретический вопрос билета. Показал отличные **знания** в рамках усвоенного учебного материала. Ответил на все или большинство дополнительных вопросов. Аспирант правильно выполнил контрольное задание билета. Показал успешное и систематическое **применение** полученных знаний и **умений** при решении профессиональных задач в рамках усвоенного учебного материала. Ответил на все или большинство дополнительных вопросов.
зачет	Аспирант продемонстрировал сформированные, но содержащие отдельные пробелы знания при ответе на теоретический вопрос билета. Показал недостаточно уверенные **знания** в рамках усвоенного учебного материала. Ответил на большинство дополнительных вопросов. Аспирант выполнил контрольное задание билета с небольшими неточностями. Показал в целом успешное, но сопровождающееся отдельными ошибками применение **навыков** полученных знаний и **умений** при решении профессиональных задач в рамках усвоенного учебного материала. Ответил на большинство дополнительных вопросов.
незачет	Аспирант продемонстрировал неполные знания при ответе на теоретический вопрос билета с существенными неточностями. Показал неуверенные **знания** в рамках усвоенного учебного материала. При ответах на дополнительные вопросы было допущено много неточностей. Аспирант выполнил контрольное задание билета с существенными неточностями. Показал в целом успешное, но не систематическое **применение** полученных знаний и **умений** при решении профессиональных задач в рамках усвоенного учебного материала. При ответах на дополнительные вопросы было допущено много неточностей.
незачет	При ответе на теоретический вопрос билета аспирант продемонстрировал фрагментарные **знания** при ответе на теоретический вопрос билета. При ответах на дополнительные вопросы было допущено множество неправильных ответов. При выполнении контрольного задания билета аспирант продемонстрировал частично освоенное **умение** и **применение** полученных навыков при решении профессиональных задач в рамках усвоенного учебного материала. При ответах на дополнительные вопросы было допущено множество неточностей.

9. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине

Задания для текущего контроля и проведения промежуточной аттестации должны быть направлены на оценивание:

1. уровня освоения теоретических понятий, научных основ профессиональной деятельности;
2. степени готовности аспиранта применять теоретические знания и профессионально значимую информацию и оценивание сформированности когнитивных умений.
3. приобретенных умений, профессионально значимых для профессиональной

деятельности.

10. Типовые контрольные вопросы и задания или иные материалы, необходимые для оценки результатов освоения дисциплины

Типовые творческие задания:

1. Оценить требуемый уровень доверия для заданного сервиса инфраструктуры умного города;
2. Оценить и обосновать требования политики информационной безопасности;
3. Сформировать функциональные требования к информационной безопасности объекта инфраструктуры;
4. Сформировать требования доверия к объекту инфраструктуры
5. Сформировать модель угроз для заданного объекта инфраструктуры
6. Обосновать и аргументировать ключевые риски соответствующие заданной модели угроз

Лист регистрации изменений

№ п.п.	Содержание изменения	Дата, номер протокола заседания кафедры. Подпись заведующего кафедрой
1	2	3
1		
2		
3		
4		