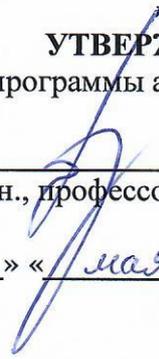


Министерство науки и высшего образования Российской Федерации  
Федеральное государственное автономное образовательное учреждение  
высшего образования

**«Пермский национальный исследовательский  
политехнический университет»**

**УТВЕРЖДАЮ**

Руководитель программы аспирантуры

  
\_\_\_\_\_  
А.А. Южаков  
д.т.н., профессор кафедры АТ

«20» «мая» 2021 г.

**Рабочая программа дисциплины по программе аспирантуры**

**«Методы и системы защиты информации, информационная  
безопасность»**

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

|                       |                       |
|-----------------------|-----------------------|
| <b>Форма обучения</b> | Очная                 |
| <b>Курс: 3</b>        | <b>Семестр (ы): 5</b> |

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

Пермь 2022

## **1. Общие положения**

Рабочая программа дисциплины «Информационная безопасность сервисов и систем 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 10.06.01 Информационная безопасность;
- 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 информационной безопасности сервисов и систем умного города.

### **1.2 Место учебной дисциплины в структуре образовательной программы**

Дисциплина «Методы и системы защиты информации, информационная безопасность» является обязательной дисциплиной образовательного компонента плана аспиранта.

Дисциплина используется при подготовке к сдаче кандидатского экзамена по специальности 2.3.6. - Методы и системы защиты информации, информационная безопасность.

Кандидатский экзамен представляют собой форму оценки степени подготовленности соискателя ученой степени кандидата наук к проведению научных исследований по конкретной научной специальности и отрасли науки, по которой подготавливается или подготовлена диссертация.

## **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 работы, технические характеристики, конструктивные особенности систем защиты информации;
- принципы построения защищенных распределенных информационно-управляющих систем.

### **Уметь:**

- разрабатывать комплексные системы защиты информации систем и сервисов умного города
- разрабатывать компоненты программно-аппаратного обеспечения средств защиты информации .

### **Владеть:**

- методами и средствами рационального выбора технических средств защиты информации;
- методами и средствами оптимизации системы защиты информации.

### 3. Структура учебной дисциплины по видам и формам учебной работы

Таблица 1

Объем и виды учебной работы

| № п.п. | Вид учебной работы                    | Трудоемкость, ч |
|--------|---------------------------------------|-----------------|
|        |                                       | 5 семестр       |
| 1      | Аудиторная работа                     | 20              |
|        | В том числе:                          |                 |
|        | Лекции (Л)                            | 5               |
|        | Практические занятия (ПЗ)             | 6               |
| 2      | Контроль самостоятельной работы (КСР) | 9               |
|        | Самостоятельная работа (СР)           | 88              |
|        | Форма итогового контроля:             | Экзамен         |

### 4. Содержание учебной дисциплины

#### 4.1. Содержание разделов и тем учебной дисциплины

Раздел 1. Теория информационной безопасности

(Л – 1, ПР - 2, СР – 32)

Тема 1. Теория и методология обеспечения информационной безопасности и защиты информации

Тема 2. Модели и методы оценки защищенности информации и информационной безопасности объекта

Раздел 2. Методы защиты информации от несанкционированного доступа

(Л – 1, ПР - 2, СР – 32)

Тема 3. Методы, модели и средства (комплексы средств) противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет

Тема 4. Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях

Раздел 3. Защищенные информационные системы

(Л – 2, ПР - 2, СР – 24)

Тема 5. Защищенные системы электронного документооборота

Тема 6. Модели и методы управления информационной безопасностью, непрерывным функционированием и восстановлением систем, противодействия отказам в обслуживании

#### 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      | 2                     | Оценка защищенности сложных систем      | Собеседование.<br>Творческое задание. | Вопросы по темам / разделам дисциплины.<br>Темы творческих заданий. |
| 2      | 4                     | Методика организация                    | Собеседование.                        | Вопросы по  |

|   |   |  |                                       |   |
|---|---|--|---------------------------------------|---|
|   |   | мониторинга распределенной информационной системы      | Творческое задание.                   | темам / разделам дисциплины.<br>Темы творческих заданий.            |
| 3 | 6 | Управление информационной безопасностью сложных систем | Собеседование.<br>Творческое задание. | Вопросы по темам / разделам дисциплины.<br>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                     | Методология защиты информации от несанкционированного доступа | Собеседование                    | Вопросы по темам / разделам дисциплины |
| 2      | 3                     | Проблематика оценки угроз информационной безопасности         | Творческое задание               | Темы творческих заданий                |
| 3      | 5                     | Оценка защищенности систем электронного документооборота      | Творческое задание               | Темы творческих заданий                |

#### 5. Методические указания для аспирантов по изучению дисциплины

При изучении дисциплины «Информационная безопасность сервисов и систем 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<br>(автор, заглавие, вид издания, место, издательство, год издания, количество страниц)      | Количество экземпляров в библиотеке+кафедре; местонахождение электронных изданий |
|------------------------------|---|--|
| 1                            | 2   | 3  |
| <b>1 Основная литература</b> |   |  |
| 1                            | Мельников Д. А. Информационная безопасность открытых систем : учебник / Д. А. Мельников. - Москва: Флинта, Наука, 2013. |  |

| <b>№</b>  | <b>Библиографическое описание</b><br>(автор, заглавие, вид издания, место, издательство,<br>год издания, количество страниц)  | <b>Количество</b><br>экземпляров в<br>библиотеке+кафедре;<br><b>местонахождение</b><br><b>электронных изданий</b> |
|---|---|---|
| 1   | 2   | 3   |
| 2   | Милославская Н. Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса : учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - Москва: Горячая линия-Телеком, 2014. |   |
| <b>2 Дополнительная литература</b>              |   |   |
| <b>2.1 Учебно-методические, научные издания</b> |   |   |
| 1   | Анисимов А. А. Менеджмент в сфере информационной безопасности: учебное пособие / А. А. Анисимов. - Москва: ИНТУИТ, БИНОМ.Лаб. знаний, 2010.   |   |
| 2   | Конеев И. Р. Информационная безопасность предприятия / И. Р. Конеев, А. В. Беляев. - Санкт-Петербург: БХВ-Петербург, 2003   |   |
| <b>2.2 Периодические издания</b>                |   |   |
| 1   | Вопросы защиты информации   |   |
| 2   | Программная инженерия и информационная безопасность   |   |
| 3   | Управление информационными рисками и обеспечение безопасности инфокоммуникационных систем   |   |
| <b>2.3 Нормативно-технические издания</b>       |   |   |
| 1   | <i>Не используются</i>  |   |
| <b>2.4 Официальные издания</b>                  |   |   |
| 1   | <i>Не используются</i>  |   |

## 6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

### 6.2.1. Информационные и информационно-справочные системы

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

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

### 7.1. Основное учебное оборудование. Рабочее место аспиранта.

Таблица 4

| <b>№ п.п.</b> | <b>Наименование и марка оборудования (стенда, макета, плаката,</b> | <b>Кол-во ед.</b> | <b>Форма приобретения / владения (собственность, оперативное управление, аренда и т.п.)</b> | <b>Номер аудитории</b> |
|---------------|--|-------------------|---|------------------------|
|---------------|--|-------------------|---|------------------------|

|   | <b>лабораторное оборудование)</b>                     |    |               |     |
|---|---|----|---------------|-----|
| 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 кандидатский экзамен, 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 экзамена по дисциплине, в устно-письменной форме по билетам. Билет содержит теоретические вопросы (ТВ) и практическое задание (ПЗ).

Билет формируется таким образом, чтобы в него попали вопросы и практические задания. Пример билета представлен в приложении 1.

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

Оценка результатов обучения по дисциплине проводится по 5-балльной системе оценивания путем выборочного контроля во время экзамена.

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

## Шкала оценивания результатов освоения на экзамене

| Оценка | Критерии оценивания  |
|--------|--|
| 5      | <p>Аспирант продемонстрировал сформированные и систематические знания при ответе на теоретический вопрос билета. Показал отличные <b>знания</b> в рамках усвоенного учебного материала. Ответил на все или большинство дополнительных вопросов.</p> <p>Аспирант правильно выполнил контрольное задание билета. Показал успешное и систематическое <b>применение</b> полученных знаний и <b>умений</b> при решении профессиональных задач в рамках усвоенного учебного материала. Ответил на все или большинство дополнительных вопросов.</p>   |
| 4      | <p>Аспирант продемонстрировал сформированные, но содержащие отдельные пробелы знания при ответе на теоретический вопрос билета. Показал недостаточно уверенные <b>знания</b> в рамках усвоенного учебного материала. Ответил на большинство дополнительных вопросов.</p> <p>Аспирант выполнил контрольное задание билета с небольшими неточностями. Показал в целом успешное, но сопровождающееся отдельными ошибками применение <b>навыков</b> полученных знаний и <b>умений</b> при решении профессиональных задач в рамках усвоенного учебного материала. Ответил на большинство дополнительных вопросов.</p>   |
| 3      | <p>Аспирант продемонстрировал неполные знания при ответе на теоретический вопрос билета с существенными неточностями. Показал неуверенные <b>знания</b> в рамках усвоенного учебного материала. При ответах на дополнительные вопросы было допущено много неточностей.</p> <p>Аспирант выполнил контрольное задание билета с существенными неточностями. Показал в целом успешное, но не систематическое <b>применение</b> полученных знаний и <b>умений</b> при решении профессиональных задач в рамках усвоенного учебного материала. При ответах на дополнительные вопросы было допущено много неточностей.</p> |
| 2      | <p>При ответе на теоретический вопрос билета аспирант продемонстрировал фрагментарные <b>знания</b> при ответе на теоретический вопрос билета. При ответах на дополнительные вопросы было допущено множество неправильных ответов.</p> <p>При выполнении контрольного задания билета аспирант продемонстрировал частично усвоенное <b>умение</b> и <b>применение</b> полученных навыков при решении профессиональных задач в рамках усвоенного учебного материала. При ответах на дополнительные вопросы было допущено множество неточностей.</p>  |

### 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

Перечень контрольных вопросов и заданий для сдачи кандидатского экзамена по научной специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность» разработан с учетом научных достижений научно-исследовательской школы кафедры.

Типовые творческие задания:

1. Оценить параметры угрозы типа «Отказ в обслуживании» для объекта КИИ
2. Предложить комплекс мер по защите сервиса удаленного доступа от угроз типа НСД
3. Сформировать ключевые положения политики информационной безопасности сервиса на основе машинного обучения
4. Обосновать и аргументировать ключевые риски соответствующие заданной модели угроз
5. Разработать систему многофакторной аутентификации заданного объекта
6. Предложить модель управления доступом для заданного сервиса

Типовые контрольные задания:

1. Провести расследование инцидента для заданного образа системы
2. Разработать модель угроз информационной безопасности робототехнического комплекса
3. Настроить защищенный канал связи для управления робототехническим комплексом

Полный комплект вопросов и заданий в форме утвержденных билетов хранится на кафедре «АТ».

**Программа**

Методы и системы защиты информации,  
информационная безопасность

**МИНОБРНАУКИ РОССИИ**  
**ФГАОУ ВО «Пермский национальный**  
**исследовательский политехнический**  
**университет» (ПНИПУ)**

**Кафедра**  
Автоматика и телемеханика

«Информационная безопасность сервисов и систем умного города»

**БИЛЕТ № 1**

1. Оценить параметры угрозы типа «Отказ в обслуживании» для объекта КИИ
2. Предложить модель управления доступом для заданного сервиса
3. Настроить защищенный канал связи для управления робототехническим комплексом

Заведующий кафедрой \_\_\_\_\_

(подпись)

Южаков А.А.

« \_\_\_\_ » \_\_\_\_\_ 202 \_\_\_\_ г.

**Лист регистрации изменений**

| <b>№<br/>п.п.</b> | <b>Содержание изменения</b> | <b>Дата,<br/>номер протокола<br/>заседания<br/>кафедры.<br/>Подпись<br/>заведующего<br/>кафедрой</b> |
|-------------------|-----------------------------|--|
| 1                 | 2                           | 3  |
| 1                 |                             |  |
| 2                 |                             |  |
| 3                 |                             |  |
| 4                 |                             |  |