

Программа утверждена на заседании кафедры \_\_\_\_\_  
Протокол № \_\_\_\_\_

### Рабочая программа дисциплины (модуля)

1. Код и наименование дисциплины (модуля): «Методы и средства защиты информации, информационная безопасность. Комплексный подход к проблеме обеспечения»
2. Уровень высшего образования – подготовка научно-педагогических кадров в аспирантуре.
3. Направление подготовки: «10.06.01 Информационная безопасность». Направленность программы: «Методы и системы защиты информации, информационная безопасность» (научная специальность 05.13.19).
4. Место дисциплины (модуля) в структуре ООП: вариативная часть ООП, элективный курс по выбору кафедры, обязателен для освоения не позднее второго года обучения.
5. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников)

| <b>Формируемые компетенции<br/>(код компетенции)</b> | <b>Планируемые результаты обучения по дисциплине (модулю)</b>  |
|--|--|
| УК-1, УК-3   | З1 (УК-1) ЗНАТЬ: методы критического анализа и оценки современных научных достижений, а также методы генерирования новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях<br>У1 (УК-1) УМЕТЬ: анализировать альтернативные варианты решения исследовательских и практических задач и оценивать потенциальные выигрыши/проигрыши реализации этих вариантов<br>У2 (УК-1) УМЕТЬ: при решении исследовательских и практических задач генерировать новые идеи, поддающиеся операционализации исходя из наличных ресурсов и ограничений |

|           |  |
|-----------|--|
|           | <p>31 (УК-3) ЗНАТЬ: особенности представления результатов научной деятельности в устной и письменной форме при работе в российских и международных исследовательских коллективах</p> <p>У1 (УК-3) УМЕТЬ: следовать нормам, принятым в научном общении при работе в российских и международных исследовательских коллективах с целью решения научных и научно-образовательных задач</p> <p>У2 (УК-3) УМЕТЬ: осуществлять личностный выбор в процессе работы в российских и международных исследовательских коллективах, оценивать последствия принятого решения и нести за него ответственность перед собой, коллегами и обществом</p>  |
| ОПК-1     | <p>31 (ОПК-1) ЗНАТЬ: основные понятия, результаты и задачи информационной безопасности</p> <p>У1 (ОПК-1) УМЕТЬ: применять основные математические методы и алгоритмы для решения стандартных задач информационной безопасности</p> <p>В1 (ОПК-1) ВЛАДЕТЬ: методами математического моделирования</p>   |
| ПК-051319 | <p>31 (ПК-051319) ЗНАТЬ: организацию и состав мер на уровнях комплексного подхода к обеспечению информационной безопасности</p> <p>32 (ПК-051319) ЗНАТЬ: отечественные и международные нормативно-правовые основы обеспечения информационной безопасности</p> <p>33 (ПК-051319) ЗНАТЬ: принципы построения систем защиты в компьютерных системах и основные сервисы программно-технического уровня обеспечения информационной безопасности</p> <p>34 (ПК-051319) ЗНАТЬ: методы и механизмы идентификации, аутентификации, логического разграничения доступа и ограничения скрытых каналов в компьютерных системах</p> <p>35 (ПК-051319) ЗНАТЬ: методы и средства защиты информации в компьютерных сетях и распределенных системах</p> <p>36 (ПК-051319) ЗНАТЬ: методы протоколирования, активного аудита, обнаружения вторжений в компьютерных системах</p> <p>37 (ПК-051319) ЗНАТЬ: методы обнаружения уязвимостей программного обеспечения</p> |

6. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся:

объем дисциплины (модуля) составляет 2 зачетные единицы, всего 80 часов, из которых 44 часа составляет контактная работа аспиранта с преподавателем (36 часов — занятия лекционного типа, 8 часов — мероприятия промежуточной аттестации), 36 часов составляет самостоятельная работа аспиранта.

7. Входные требования для освоения дисциплины (модуля), предварительные условия:

- знание основных направлений, проблем, теорий и методов информатики, программирования, дискретной математики, математической логики, теории вероятностей;
- умение решать стандартные задачи дискретной математики, математической логики, теории вероятностей и применять идеи, использованные в их решениях, для решения аналогичных задач.

8. Формат обучения: очные занятия

9. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических или астрономических часов и виды учебных занятий

| Наименование и краткое содержание разделов и тем дисциплины (модуля),<br><br>форма промежуточной аттестации по дисциплине (модулю)  | Всего (часы) | В том числе   |                           |                        |                             |  |   |                             |                             |       |
|---|--------------|---|---------------------------|------------------------|-----------------------------|--|---|-----------------------------|-----------------------------|-------|
|   |              | Контактная работа (работа во взаимодействии с преподавателем), часы<br>из них |                           |                        |                             |  | Самостоятельная работа обучающегося, часы<br>из них |                             |                             |       |
|   |              | Занятия лекционного типа  | Занятия семинарского типа | Групповые консультации | Индивидуальные консультации | Учебные занятия, направленные на проведение текущего контроля успеваемости (коллоквиумы, практические контрольные занятия и др.) | Всего   | Выполнение домашних заданий | Подготовка рефератов и т.п. | Всего |
| <b>Тема 1. Комплексный подход к проблеме обеспечения информационной безопасности (ИБ).</b><br>Выделение уровней комплексного подхода к обеспечению ИБ: законодательный, административно-организационный, операционный и программно-технический. Обзор мер и методов на уровнях комплексного подхода к обеспечению ИБ. | 4            | 2   |                           |                        |                             |  | 2   | 2                           |                             | 2     |

|  |    |    |  |  |  |  |    |    |  |    |
|--|----|----|--|--|--|--|----|----|--|----|
| <p><b>Тема 2. Отечественные и международные нормативно-правовые основы обеспечения информационной безопасности.</b><br/> Руководящие документы ФСТЭК России, международный стандарт ИСО/МЭК 15408, серии международных стандартов ИСО 27000, нормативные документы в области защиты персональных данных.</p>   | 4  | 2  |  |  |  |  | 2  | 2  |  | 2  |
| <p><b>Тема 3. Принципы построения систем защиты в компьютерных системах и основные сервисы программно-технического уровня обеспечения информационной безопасности.</b><br/> Модель угроз и модель нарушителя. Распространенные угрозы и атаки. Проектирование и выбор архитектуры системы защиты. Классификация программно-технических методов и средств защиты информации.</p>  | 8  | 4  |  |  |  |  | 4  | 4  |  | 4  |
| <p><b>Тема 4. Методы и механизмы идентификации, аутентификации, логического разграничения доступа и ограничения скрытых каналов в компьютерных системах.</b><br/> Общие положения создания и примеры реализации систем и механизмов идентификации и аутентификации. Подход к определению безопасности в терминах доступов. Принцип монитора обращений. Дискреционные модели разграничения доступа. Мандатные многоуровневые модели разграничения доступа. Ролевые модели разграничения доступа. Подходы к классификации скрытых каналов. Подходы к ограничению пропускной способности скрытых каналов.</p> | 24 | 12 |  |  |  |  | 12 | 12 |  | 12 |

|   |           |           |  |  |  |  |           |           |  |           |
|---|-----------|-----------|--|--|--|--|-----------|-----------|--|-----------|
| <b>Тема 5. Методы и средства защиты информации в компьютерных сетях и распределенных системах.</b><br>Межсетевые экраны: виды исполнения, основные компоненты, режимы функционирования, основные схемы сетевой защиты, примеры реализации. Методы и средства туннелирования и организации виртуальных частных сетей.  | 8         | 4         |  |  |  |  | 4         | 4         |  | 4         |
| <b>Тема 6. Методы протоколирования, активного аудита, обнаружения вторжений в компьютерных системах.</b><br>Протоколирование и активный аудит. Методы мониторинга и обнаружения вторжений в распределенных информационно-вычислительных системах. Основные методы анализа регистрационной информации.   | 8         | 4         |  |  |  |  | 4         | 4         |  | 4         |
| <b>Тема 7. Методы обнаружения уязвимостей программного обеспечения.</b><br>Распространенные уязвимости программного обеспечения. Подходы к классификации и примеры уязвимостей. Основные принципы безопасного программирования. Подходы к предотвращению возникновения уязвимостей. Обзор методов верификации программного обеспечения. Методы обнаружения программных закладок и недекларированных возможностей. Методы защиты программ от изучения и разрушающих программных воздействий. | 16        | 8         |  |  |  |  | 8         | 8         |  | 8         |
| Промежуточная аттестация в форме экзамена   | 8         | 8         |  |  |  |  |           |           |  |           |
| <b>Итого</b>  | <b>80</b> | <b>44</b> |  |  |  |  | <b>44</b> | <b>36</b> |  | <b>36</b> |

10. Перечень учебно-методического обеспечения для самостоятельной работы аспирантов по дисциплине (модулю).

Литература:

1) Основы информационной безопасности: учебное пособие. / В. А. Галатенко. Под редакцией академика РАН В. Б. Бетелина – 4-е изд. – М.: Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 2008. – 205 с.: ил. – (Серия «Основы информационных технологий»).

2) Теоретические основы компьютерной безопасности: учеб. пособие для студентов высш. учеб. заведений. / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. – М.: Издательский центр «Академия», 2009. – 272 с.

11. Фонд оценочных средств для промежуточной аттестации по дисциплине (модулю).

| РЕЗУЛЬТАТ<br>ОБУЧЕНИЯ<br>по<br>дисциплине<br>(модулю)   | КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТА ОБУЧЕНИЯ<br>по дисциплине (модулю) и<br>ШКАЛА оценивания |  |   |  |  | ПРОЦЕДУРЫ<br>ОЦЕНИВАНИЯ |
|---|---|--|---|--|--|-------------------------|
|   | 1   | 2  | 3   | 4  | 5  |                         |
| З1 (УК-1)<br>ЗНАТЬ: методы критического анализа и оценки современных научных достижений, а также методы генерирования новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях | Отсутствие знаний   | Фрагментарные знания методов критического анализа и оценки современных научных достижений, а также методов генерирования новых идей при решении исследовательских и практических задач | Общие, но не структурированные знания методов критического анализа и оценки современных научных достижений, а также методов генерирования новых идей при решении исследовательских и практических задач | Сформированные, но содержащие отдельные пробелы знания основных методов критического анализа и оценки современных научных достижений, а также методов генерирования новых идей при решении исследовательских и практических задач, в том числе междисциплинарных | Сформированные систематические знания методов критического анализа и оценки современных научных достижений, а также методов генерирования новых идей при решении исследовательских и практических задач, в том числе междисциплинарных |                         |

|   |                   |   |  |   |   |  |
|---|-------------------|---|--|---|---|--|
| <p>У1 (УК-1)<br/>УМЕТЬ:<br/>анализировать альтернативные варианты решения исследовательских и практических задач и оценивать потенциальные выигрыши/проигрыши реализации этих вариантов</p> | Отсутствие умений | Частично освоенное умение анализировать альтернативные варианты решения исследовательских и практических задач и оценивать потенциальные выигрыши/проигрыши реализации этих вариантов | В целом успешно, но не систематически осуществляемые анализ альтернативных вариантов решения исследовательских и практических задач и оценка потенциальных выигрышей/проигрышей реализации этих вариантов  | В целом успешно, но содержащие отдельные пробелы анализ альтернативных вариантов решения исследовательских задач и оценка потенциальных выигрышей/проигрышей реализации этих вариантов  | Сформированное умение анализировать альтернативные варианты решения исследовательских и практических задач и оценивать потенциальные выигрыши/проигрыши реализации этих вариантов                     |  |
| <p>У2 (УК-1)<br/>УМЕТЬ: при решении исследовательских и практических задач генерировать новые идеи, поддающиеся операционализации исходя из наличных ресурсов и ограничений</p>             | Отсутствие умений | Частично освоенное умение при решении исследовательских и практических задач генерировать идеи, поддающиеся операционализации исходя из наличных ресурсов и ограничений               | В целом успешное, но не систематически осуществляемое умение при решении исследовательских и практических задач генерировать идеи, поддающиеся операционализации исходя из наличных ресурсов и ограничений | В целом успешное, но содержащее отдельные пробелы умение при решении исследовательских и практических задач генерировать идеи, поддающиеся операционализации исходя из наличных ресурсов и ограничений                        | Сформированное умение при решении исследовательских и практических задач генерировать идеи, поддающиеся операционализации исходя из наличных ресурсов и ограничений                                   |  |
| <p>З1 (УК-3)<br/>ЗНАТЬ: особенности представления результатов научной деятельности в устной и письменной форме при работе в российских и международных исследовательских коллективах</p>    | Отсутствие знаний | Фрагментарные знания особенностей представления результатов научной деятельности в устной и письменной форме  | Неполные знания особенностей представления результатов научной деятельности в устной и письменной форме, при работе в российских и международных коллективах   | Сформированные, но содержащие отдельные пробелы знания основных особенностей представления результатов научной деятельности в устной и письменной форме при работе в российских и международных исследовательских коллективах | Сформированные и систематические знания особенностей представления результатов научной деятельности в устной и письменной форме при работе в российских и международных исследовательских коллективах |  |

|  |                          |   |  |  |   |  |
|--|--------------------------|---|--|--|---|--|
| <p>У1 (УК-3)<br/>УМЕТЬ: следовать нормам, принятым в научном общении при работе в российских и международных исследовательских коллективах с целью решения научных и научно-образовательных задач</p>  | <p>Отсутствие умений</p> | <p>Фрагментарное следование нормам, принятым в научном общении при работе в российских и международных исследовательских коллективах с целью решения научных и научно-образовательных задач</p>   | <p>В целом успешное, но не систематическое следование нормам, принятым в научном общении при работе в российских и международных исследовательских коллективах с целью решения научных и научно-образовательных задач</p>  | <p>В целом успешное, но содержащее отдельные пробелы умение следовать основным нормам, принятым в научном общении при работе в российских и международных исследовательских коллективах с целью решения научных и научно-образовательных задач</p>                                 | <p>Успешное и систематическое следование нормам, принятым в научном общении, для успешной работы в российских и международных исследовательских коллективах с целью решения научных и научно-образовательных задач</p>                                      |  |
| <p>У2 (УК-3)<br/>УМЕТЬ: осуществлять личный выбор в процессе работы в российских и международных исследовательских коллективах, оценивать последствия принятого решения и нести за него ответственность перед собой, коллегами и обществом</p> | <p>Отсутствие умений</p> | <p>Частично освоенное умение осуществлять личный выбор в процессе работы в российских и международных исследовательских коллективах, оценивать последствия принятого решения и нести за него ответственность перед собой, коллегами и обществом</p> | <p>В целом успешное, но не систематическое умение осуществлять личный выбор в процессе работы в российских и международных исследовательских коллективах, оценивать последствия принятого решения и нести за него ответственность перед собой, коллегами и обществом</p> | <p>В целом успешное, но содержащее отдельные пробелы умение осуществлять личный выбор в процессе работы в российских и международных исследовательских коллективах, оценивать последствия принятого решения и нести за него ответственность перед собой, коллегами и обществом</p> | <p>Успешное и систематическое умение осуществлять личный выбор в процессе работы в российских и международных исследовательских коллективах, оценивать последствия принятого решения и нести за него ответственность перед собой, коллегами и обществом</p> |  |

|   |                              |   |  |   |  |  |
|---|------------------------------|---|--|---|--|--|
| 31 (ОПК-1)<br>ЗНАТЬ: основные понятия, результаты и задачи информационной безопасности.   | Отсутствие знаний            | Фрагментарные представления о результатах, проблемах, методах научных исследований в области информационной безопасности и смежных областях | Неполные представления о результатах, проблемах, методах научных исследований в области информационной безопасности и смежных областях                           | Сформированные, но содержащие отдельные пробелы представления о результатах, проблемах, методах научных исследований в области информационной безопасности и смежных областях | Сформированные систематические представления о результатах, проблемах, методах научных исследований в области информационной безопасности и смежных областях |  |
| У1 (ОПК-1)<br>УМЕТЬ: применять основные математические методы и алгоритмы для решения стандартных задач информационной безопасности | Отсутствие умений            | Фрагментарное умение разработки и применения методов и алгоритмов научных исследований  | В целом успешное, но не систематическое умение разработки и применения методов и алгоритмов научных исследований   | В целом успешное, но содержащее отдельные пробелы умение разработки и применения методов и алгоритмов научных исследований  | Сформированное умение разработки и применения методов и алгоритмов научных исследований  |  |
| В1 (ОПК-1)<br>ВЛАДЕТЬ: методами математического моделирования   | Отсутствие навыков           | Фрагментарное применение навыков построения и анализа математических моделей, решения задач при помощи современных программных средств      | В целом успешное, но не систематическое применение навыков построения и анализа математических моделей, решения задач при помощи современных программных средств | В целом успешное, но содержащее отдельные пробелы применение навыков построения и анализа математических моделей, решения задач при помощи современных программных средств    | Успешное и систематическое применение навыков построения и анализа математических моделей, решения задач при помощи современных программных средств          |  |
| 31 (ПК-051319)<br>ЗНАТЬ: организацию и состав мер на уровнях комплексного подхода к обеспечению информационной безопасности.        | Отсутствие знаний о предмете | Фрагментарные представления о предмете  | Неполные представления о предмете  | Сформированные, но содержащие отдельные пробелы представления о предмете  | Сформированные систематические представления о предмете  | Экзамен в форме индивидуального собеседования (оценка по пятибалльной шкале) |

|   |                              |  |                                   |  |   |  |
|---|------------------------------|--|-----------------------------------|--|---|--|
| 32 (ПК-051319)<br>ЗНАТЬ:<br>отечественные и международные нормативно-правовые основы обеспечения информационной безопасности.   | Отсутствие знаний о предмете | Фрагментарные представления о предмете | Неполные представления о предмете | Сформированные, но содержащие отдельные пробелы представления о предмете | Сформированные систематические представления о предмете | Экзамен в форме индивидуального собеседования (оценка по пятибалльной шкале) |
| 33 (ПК-051319)<br>ЗНАТЬ: принципы построения систем защиты в компьютерных системах и основные сервисы программно-технического уровня обеспечения информационной безопасности. | Отсутствие знаний о предмете | Фрагментарные представления о предмете | Неполные представления о предмете | Сформированные, но содержащие отдельные пробелы представления о предмете | Сформированные систематические представления о предмете | Экзамен в форме индивидуального собеседования (оценка по пятибалльной шкале) |
| 34 (ПК-051319)<br>ЗНАТЬ: методы и механизмы идентификации, аутентификации, логического разграничения доступа и ограничения скрытых каналов в компьютерных системах.           | Отсутствие знаний о предмете | Фрагментарные представления о предмете | Неполные представления о предмете | Сформированные, но содержащие отдельные пробелы представления о предмете | Сформированные систематические представления о предмете | Экзамен в форме индивидуального собеседования (оценка по пятибалльной шкале) |
| 35 (ПК-051319)<br>ЗНАТЬ: методы и средства защиты информации в компьютерных сетях и распределенных системах.  | Отсутствие знаний о предмете | Фрагментарные представления о предмете | Неполные представления о предмете | Сформированные, но содержащие отдельные пробелы представления о предмете | Сформированные систематические представления о предмете | Экзамен в форме индивидуального собеседования (оценка по пятибалльной шкале) |

|  |                              |  |                                   |  |   |  |
|--|------------------------------|--|-----------------------------------|--|---|--|
| 36 (ПК-051319)<br>ЗНАТЬ: методы протоколирования, активного аудита, обнаружения вторжений в компьютерных системах. | Отсутствие знаний о предмете | Фрагментарные представления о предмете | Неполные представления о предмете | Сформированные, но содержащие отдельные пробелы представления о предмете | Сформированные систематические представления о предмете | Экзамен в форме индивидуального собеседования (оценка по пятибалльной шкале) |
| 37 (ПК-051319)<br>ЗНАТЬ: методы обнаружения уязвимостей программного обеспечения.                                  | Отсутствие знаний о предмете | Фрагментарные представления о предмете | Неполные представления о предмете | Сформированные, но содержащие отдельные пробелы представления о предмете | Сформированные систематические представления о предмете | Экзамен в форме индивидуального собеседования (оценка по пятибалльной шкале) |

## 12. Ресурсное обеспечение:

- Перечень основной и дополнительной учебной литературы.

1) Основы информационной безопасности: учебное пособие. / В. А. Галатенко. Под редакцией академика РАН В. Б. Бетелина – 4-е изд. – М.: Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 2008. – 205 с.: ил. – (Серия «Основы информационных технологий»).

2) Теоретические основы компьютерной безопасности: учеб. пособие для студентов высш. учеб. заведений. / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. – М.: Издательский центр «Академия», 2009. – 272 с.

3) Критически важные объекты и кибертерроризм. Часть 1. Системный подход к организации противодействия. / О. О. Андреев и др. Под ред. В. А. Васенина. — М.: МЦНМО, 2008. – 398 с.

4) Критически важные объекты и кибертерроризм. Часть 2. Аспекты программной реализации средств противодействия. / О. О. Андреев и др. Под ред. В. А. Васенина. — М.: МЦНМО, 2008. – 607 с.

## 13. Язык преподавания: русский.

## 14. Преподаватель (преподаватели):

д.ф.-м.н., проф. В.А.Васенин; к.ф.-м.н., с.н.с. А.В.Галатенко; к.ф.-м.н., с.н.с. Ф.М.Пучков; к.ф.-м.н., с.н.с. К.А.Шапченко.