МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

УТВЕРЖДАЮ
Первый проректор-
проректор по научной работе
_____ О.В. Павленко
10.03. 2022 г.

МЕТОДОЛОГИЯ И МЕТОДЫ ИССЛЕДОВАНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины для подготовки аспирантов

2.3. Информационные технологии и телекоммуникации
(Шифр и наименование группы научных специальностей)

2.3.6. Методы и системы защиты информации, информационная безопасность

(Шифр и наименование научной специальности)

Москва 2022

МЕТОДОЛОГИЯ И МЕТОДЫ ИССЛЕДОВАНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины для подготовки аспирантов.
2.3. Информационные технологии и телекоммуникации. 2.3.6. Методы и системы защиты информации, информационная безопасность
.

Автор (составитель): Д.А. Митюшин,
кандидат технических наук

Программа утверждена
на заседании кафедры комплексной защиты информации
15 февраля 2022 г., протокол № 6/1

Программа утверждена
на заседании Совета ИИНТБ
17 февраля 2022 г., протокол № 7

Программа утверждена
на заседании Научно-методического совета
по аспирантуре и докторантуре
10 марта 2022 г., протокол № 1

Аннотация

Дисциплина «Методология и методы исследования систем защиты информации, информационной безопасности» является факультативной дисциплиной вариативной части направленности программ подготовки научно-педагогических кадров в аспирантуре «Методы и системы защиты информации, информационная безопасность».

Рабочая программа дисциплины разработана на кафедре комплексной защиты информации Института информационных наук и технологий безопасности.

Содержание дисциплины охватывает круг вопросов, связанных с рассмотрением совокупности проблем, связанных с информатизацией общества, с исследованием, разработкой, совершенствованием и применением моделей, методов, технологий, средств и систем защиты информации, а также обеспечением информационной безопасности объектов и процессов обработки, передачи информации во всех сферах деятельности от внешних и внутренних угроз.

Требования к результатам освоения дисциплины:

В результате изучения дисциплины аспирант должен:

знать: меры по обеспечению сохранности информации, основные задачи обеспечения безопасности информации в информационных системах; принципы исследования защищённости информационных систем.

уметь: решать задачи теоретического характера из различных разделов дисциплины, доказывать утверждения, строить примеры основных объектов и понятий.

владеть: навыками применения полученных знаний в научно-исследовательской работе и научно-педагогической работе.

Общая трудоёмкость освоения дисциплины составляет 2 зачётные единицы, 72 часа. Программой дисциплины предусмотрены лекционные занятия (18 часов), самостоятельная работа аспиранта (54 часа).

Программой дисциплины предусмотрены следующие виды контроля освоения дисциплины: текущий контроль в форме реферата, промежуточный контроль в виде зачёта.

1. Пояснительная записка

Цель дисциплины: сформировать у аспирантов представление о методах и системах защиты информации, информационной безопасности.

«Методология и методы исследования систем защиты информации, информационной безопасности» – это дисциплина, занимающаяся вопросами исследования качества защиты информации и информационной безопасности защищаемых объектов информатизации, автоматизированных систем, информационно-аналитических, информационно-телекоммуникационных и иных информационных систем.

Курс даёт возможность ознакомиться аспирантам по научной

специальности 2.3.6. с областями и результатами исследований по этой дисциплине.

Задачи дисциплины: раскрытие сущности и значения методологии и методов исследования систем защиты информации, информационной безопасности для обеспечения безопасности и защиты информации.

Место дисциплины в структуре программы подготовки научных и научно-педагогических кадров в аспирантуре:

Дисциплина «Методология и методы исследования систем защиты информации, информационной безопасности» принадлежит к специальным дисциплинам.

Данная дисциплина призвана, прежде всего, помочь аспиранту в его научной деятельности.

Требования к результатам освоения дисциплины:

В результате изучения дисциплины аспирант должен:

знать: меры по обеспечению сохранности информации, основные задачи обеспечения безопасности информации в информационных системах; принципы исследования защищённости информационных систем.

уметь: решать задачи теоретического характера из различных разделов дисциплины, доказывать утверждения, строить примеры основных объектов и понятий.

владеть: навыками применения полученных знаний в научно-исследовательской работе и научно-педагогической работе.

2. Структура дисциплины (тематический план)

Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы, 72 часа.

№ п/п	Раздел дисциплины	Семестр	Виды учебной работы, включая самостоятельную работу аспирантов и трудоемкость (в часах)			Формы текущего контроля успеваемости Форма промежуточной аттестации
			Лекции	Практ. занятия	Самостоятельная работа	
1	Основы построения систем защиты информации	2	4		10 Реферирование российской и зарубежной литературы и статей, работа в интернет	собеседование
2	Оценка эффективности защиты информации	2	4		12 Реферирование российской и зарубежной литературы и статей, работа в интернет	собеседование
3	Системы обнаружения вторжений	2	4		20 Реферирование российской и зарубежной литературы и статей, работа в интернет	Контрольная работа
4	Аудит информационной	2	6		12 Реферирование российской	Собеседование Реферат

	безопасности				и зарубежной литературы и статей, работа в интернет	
5	**ИТОГО:**		**18**		**54**	**Зачёт**

Структура дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

№ п/п	**Раздел дисциплины**	**Семестр**	**Виды учебной работы, включая самостоятельную работу аспирантов и трудоемкость (в часах)**			**Формы текущего контроля успеваемости** **Форма промежуточной аттестации**
			Лек-ции	**Практ. занятия**	**Самостоятельная работа**	
1	Основы построения систем защиты информации	2	4		10 Реферирование российской и зарубежной литературы и статей, работа в интернет	собеседование
2	Оценка эффективности защиты информации	2	6		12 Реферирование российской и зарубежной литературы и статей, работа в интернет	собеседование
3	Системы обнаружения вторжений	2	4		20 Реферирование российской и зарубежной литературы и статей, работа в интернет	Контрольная работа
4	Аудит информационной безопасности	2	6		10 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование Реферат
9	**ИТОГО:**		**20**		**52**	**Зачёт**

3. Содержание дисциплины

Тема 1. Основы построения систем защиты информации

Цель и задачи информационной безопасности (ИБ). Угрозы ИБ и их источники.

Понятие системы. Системный подход в построении систем защиты информации и в обеспечении информационной безопасности.

Модель построения системы информационной безопасности предприятия. Разработка концепция обеспечения ИБ.

Основные принципы защиты информации. Целеустремлённость, непрерывность, скрытность, комплексность.

Подсистемы защиты информации. Инженерно-техническая защита. Системы охраны и контроля и управления доступом. Программно-аппаратная защита информации. Криптографическая защита информации.

Комплексное обеспечение защиты информации.

Тема 2. Оценка эффективности защиты информации

Понятие эффективности. Показатели и критерии эффективности. Отношение «эффективность/стоимость».

Эффективность технических средств охраны. Эффективность систем

ИТЗИ. Эффективность программно-аппаратных средств защиты.

Эффективность комплексной системы защиты информации и обеспечения информационной безопасности.

Тема 3. Системы обнаружения вторжений

Модели систем обнаружения вторжений. Модель Д. Деннинг. Модель CIDF. Классификация систем обнаружения вторжений. Обнаружение сигнатур. Система обнаружения вторжений Snort. Декодер пакетов. Препроцессоры. Препроцессоры сборки пакетов. Препроцессоры нормализации протоколов. Препроцессоры обнаружения аномалий. Процессор обнаружения. Модули вывода. Правила Snort. Примеры правил. Обнаружение аномалий. Методы Data Mining. Методы технологии мобильных агентов. Методы построения иммунных систем. Применение генетических алгоритмов. Применение нейронных сетей. Языки описания атак. Другие методы обнаружения вторжений. Системы анализа защищённости. Системы анализа целостности. Вспомогательные средства обнаружения. Методы обхода систем обнаружения вторжений. Методы обхода сетевых систем обнаружения вторжений. Методы обхода хостовых систем обнаружения вторжений. Динамические методы обхода. Тестирование систем обнаружения вторжений. Тестирование коммерческих систем. Тестирование исследовательских прототипов. Методы формирования тестовых наборов. Матрица несоответствий. Системы предупреждения вторжений.

Тема 4. Аудит информационной безопасности

Аудит безопасности и методы его проведения. Понятие аудита безопасности. Методы анализа данных при аудите ИБ.

4. Информационные и образовательные технологии

В учебном процессе широко используются активные и интерактивные формы проведения занятий:

– традиционные формы подачи лекционного материала;

– лекции с использованием мультимедийной техники;

– использование локальной сети компьютерного класса с выходом в интернет;

– методы сетевого взаимодействия и контроля;

– самостоятельная работа аспирантов в виде аннотирования и реферирования научной литературы, статей отечественных и зарубежных авторов, работа в интернет и использованием компьютеров (библиотека РГГУ), личных компьютеров, мобильных устройств.

5. Система текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

Система текущего контроля успеваемости по дисциплине включает реферат.

Система промежуточной аттестации по итогам освоения дисциплины включает зачёт.

Объем реферата по дисциплине – 15-25 страниц печатного текста. При защите реферата аспирант кратко излагает концепцию реферата и основные выводы, отвечает на поставленные вопросы.

Критерии оценки за реферат

Оценка	Содержание
Отлично	Реферат написан четко и грамотно. Тема реферата хорошо раскрыта. Приведена качественно подобранная российская и зарубежная литература. Ответы на дополнительные вопросы по реферату правильные.
Хорошо	Реферат написан четко и грамотно. Тема реферата раскрыта не полностью. Приведена российская и зарубежная литература. Ответы на дополнительные вопросы по реферату правильные.
Удовлетворительно	Тема реферата раскрыта не полностью. Ответы на дополнительные вопросы по реферату правильные, но неполные.
Неудовлетворительно	Тема реферата не раскрыта. Ответы на дополнительные вопросы по реферату неправильные.

Критерии оценки по итогам промежуточной аттестации

Оценка	Содержание
Отлично	Аспирант способен обобщить материал, сделать собственные выводы, выразить свое мнение, привести иллюстрирующие примеры.
Хорошо	Ответ аспиранта правильный, но неполный. Не приведены иллюстрирующие примеры, обобщающее мнение аспиранта недостаточно четко выражено.
Удовлетворительно	Ответ правильный в основных положениях, отсутствуют иллюстрирующие примеры, собственное мнение аспиранта, имеются ошибки в деталях.
Неудовлетворительно	В ответе аспиранта существенные ошибки в основных аспектах темы.
Зачтено	Аспирант способен обобщить материал, сделать собственные выводы, выразить свое мнение, привести иллюстрирующие примеры.

Не зачтено	В ответе аспиранта существенные ошибки в основных аспектах темы.

6. Фонд оценочных средств для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

№ пп	Примерная тематика рефератов
1.	Системный анализ в подходе к информационной безопасности.
2.	Эффективность применения технических средств охраны
3.	Эффективность применения систем видеонаблюдения при охране объектов информатизации
4.	Методы обнаружения вторжений
5.	Методы и средства информационного противодействия угрозам нарушения информационной безопасности в сети Интернет.
6.	Анализ рисков нарушения информационной безопасности и уязвимости систем инженерно-технической защиты информации
7.	Анализ рисков нарушения информационной безопасности и уязвимости систем программно-аппаратных средств защиты информации
8.	Модели и методы оценки защищённости информации на объекте информатизации.
9.	Модели и методы оценки эффективности систем обеспечения информационной безопасности объектов информатизации.
10.	Мероприятия и механизмы аудита информационной безопасности предприятия.
11.	Модели, методы и средства обеспечения внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности.

№ пп	Перечень проблем, выносимых на зачёт
1.	Системный подход в построении систем защиты информации и в обеспечении информационной безопасности.
2.	Модель построения системы информационной безопасности организации.
3.	Основные принципы защиты информации.
4.	Разработка концепции обеспечения ИБ.
5.	Понятие эффективности. Показатели и критерии эффективности. Отношение «эффективность/стоимость».
6.	Эффективность комплексной системы защиты информации и обеспечения информационной безопасности
7.	Модели систем обнаружения вторжений. Классификация систем обнаружения вторжений.
8.	Система обнаружения вторжений Snort. Правила Snort. Примеры правил.
9.	Обнаружение аномалий. Методы Data Mining.
10.	Системы анализа защищённости. Системы анализа целостности.

	Вспомогательные средства обнаружения.
11.	Методы обхода сетевых и хостовых систем обнаружения вторжений.
12.	Системы предупреждения вторжений.
13.	Аудит безопасности информации предприятия и методы его проведения

7. Учебно-методическое и информационное обеспечение дисциплины

Список источников и литературы

Основные источники

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (последняя редакция). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.
2. ГОСТы по информационной безопасности и защите информации

Основная литература

3. Шелухин, О. И. Обнаружение вторжений в компьютерные сети (сетевые аномалии): Учебное пособие для вузов / О.И. Шелухин, Д.Ж. Сакалема, А.С. Филинова. - Москва : Гор. линия-Телеком, 2013. - 220 с.: ил.; . ISBN 978-5-9912-0323-4, 500 экз. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/421968 (дата обращения: 02.02.2022)
4. Баранова, Е. К. Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. – 4-е изд., перераб. и доп. – Москва : РИОР : ИНФРА-М, 2019. – 322 с. – (Высшее образование). – ww.dx.doi.org/10.12737/11380. - ISBN 978-5-16-106532-7. – Текст : электронный. – URL: https://new.znanium.com/catalog/product/1009606 (дата обращения: 02.02.2022)
5. Грекул, В. И. Аудит информационных технологий: Учебник для вузов / Грекул В.И. - Москва :Гор. линия-Телеком, 2015. - 154 с. (Специальность) ISBN 978-5-9912-0528-3. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/555524 (дата обращения: 02.02.2022)
6. Зайцев, А. П. Технические средства и методы защиты информации: Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков; Под ред. А.П. Зайцева - 7 изд., исправ. - Москва : Гор. линия-Телеком, 2012. - 442с.; - (Уч. для вузов). ISBN 978-5-9912-0233-6. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/390284 (дата обращения: 02.02.2022)
7. Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика».

Дополнительная литература

8. Агапов, А. В. Обработка и обеспечение безопасности электронных данных [Электронный ресурс] : учеб. пособие / А. В. Агапов, Т. В. Алексеева, А. В. Васильев и др.; под ред. Д. В. Денисова. – Москва : МФПУ Синергия,

2012. – 592 с. – (Сдаём госэкзамен). – ISBN 978-5-4257-0074-2. – Текст : электронный. – URL: https://new.znanium.com/catalog/product/451354 (дата обращения: 02.02.2022)

9. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2019. – 592 с. – (Высшее образование: Бакалавриат). – ISBN 978-5-16-106148-0. – Текст : электронный. – URL: https://new.znanium.com/catalog/product/996789 (дата обращения: 02.02.2022)

Периодические и сериальные издания

1. Безопасность информационных технологий: научный журнал. - М.
2. Джет Инфо: бюллетень. - М.
3. Защита информации: научный журнал. - М.
4. Информационная безопасность: научный журнал. - СПб.
5. Информационные войны: научный журнал. - М.
6. Открытые Системы. СУБД: научный журнал. - М.

Ресурсы Интернет

1. Совет безопасности Российской Федерации [офиц. сайт]. http://www.scrf.gov.ru/
2. Федеральная служба по техническому и экспортному контролю [офиц. сайт], http://fstec.ru
3. Управление «К» МВД России [офиц. сайт]. https://мвд.рф/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii
4. Институт информационных наук и технологий безопасности РГГУ [офиц. сайт], http://www.rsuh.ru/iint
5. Методические пособия, рекомендации, перечни [офиц. сайт Федерального архивногоагентства], http://archives.ru/documents/methodics.shtml.
6. Информационная безопасность организаций банковской системы Российской Федерации [офиц. сайт Центрального банка Российской Федерации], http://www.cbr.ru/credit/gubzi_docs

8. Материально-техническое обеспечение дисциплины

Освоение дисциплины предполагает использование академической аудитории для проведения лекционных занятий и самостоятельной работы:

Компьютерный класс

12 компьютеров (Процессор: Celeron 2,6GHz. Оперативная память: 256Mb. Объем жесткого диска: 40Gb. Дисковод CD), проектор.

ПО: Windows 7, MS Office 2010, Microsoft Visual Studio 2012.

Для инвалидов и лиц с ограниченными возможностями здоровья: обеспечивается возможность беспрепятственного доступа обучающихся инвалидов в аудитории и другие помещения, а также их пребывания в указанных помещениях (наличие пандусов, лифтов, наличие специальных кресел и других приспособлений).

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным

оборудованием и учебными местами с техническими средствами обучения для обучающихся с ограниченными возможностями здоровья и обучающихся инвалидов с разными видами ограничений здоровья:

- с нарушениями зрения:
  - устройство для сканирования и чтения с камерой SARA CE;
  - дисплей Брайля PAC Mate 20;
  - принтер Брайля EmBraille ViewPlus;
- с нарушениями слуха:
  - автоматизированное рабочее место для людей с нарушением слуха и слабослышащих;
  - акустический усилитель и колонки;
- с нарушениями опорно-двигательного аппарата:
  - передвижные, регулируемые эргономические парты СИ-1;
  - компьютерная техника со специальным программным обеспечением.

9. Методические указания по организации практических занятий (при наличии в учебном плане подготовки аспирантов)

нет

10. Рекомендации по организации самостоятельной работы аспирантов

Самостоятельная работа аспирантов организуется в форме аннотирования и реферирования научной литературы, статей отечественных и зарубежных авторов. По итогам самостоятельной работы аспиранты готовят рефераты, лучшие из которых заслушиваются на научном семинаре кафедры, Гуманитарных чтениях РГГУ, профильных конференциях.

Готовя рефераты, аспиранты должны показать навыки научного поиска, используя литературу и источники, которые не нашли отражения в данной программе.

В ходе самостоятельной деятельности необходимо принимать во внимание векторы развития информатизации и глобализации общества, новые технологии и угрозы информационной безопасности личности, обществу, государству.

Организация самостоятельной работы аспирантов направлена на осуществление научно-исследовательской работы, подготовку научных статей, диссертационной работы, подготовку к преподавательской деятельности.

Сведения об авторах (составителях) рабочей программы дисциплины

Методология и методы исследования систем защиты информации, информационной безопасности

Д.А. Митюшин, кандидат технических наук _____

(Инициалы, фамилия, уч. степень, уч. звание) (подпись)

Лист изменений
в рабочей программе дисциплины
МЕТОДОЛОГИЯ И МЕТОДЫ ИССЛЕДОВАНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
(Название дисциплины)

№ п/п	Дата внесения изменений	Дата и № протокола заседания кафедры	Содержание изменения	Подпись