Федеральное государственное бюджетное образовательное

учреждение высшего образования

Московский государственный университет имени М.В. Ломоносова

Факультет вычислительной математики и кибернетики

**УТВЕРЖДАЮ**

декан факультета вычислительной математики и кибернетики

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_/И.А. Соколов /**

**«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_г.**

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Наименование дисциплины:**

**Программно-аппаратные средства защиты информации**

**Уровень высшего образования:**

**бакалавриат**

**Направление подготовки / специальность:**

**01.03.02 «Прикладная математика и информатика» (3++)**

**Направленность (профиль):**

**Математические методы обработки информации и принятия решений**

**Форма обучения:**

**очная**

**Москва 2023**

Рабочая программа дисциплины (модуля) разработана в соответствии с самостоятельно установленным МГУ образовательным стандартом (ОС МГУ) для реализуемых основных профессиональных образовательных программ высшего образования по направлению подготовки 01.03.02, 01.04.02 "Прикладная математика и информатика" программы бакалавриата Утвержден приказом МГУ от 30 августа 2019 года № 1041 (в редакции приказов МГУ от 11 сентября 2019 года № 1109, от 10 июня 2021 года № 609, от 7 октября 2021 года № 1048, от 21 декабря 2021 года № 1404, от 2 ноября 2022 года № 1299)

**1.** Дисциплина относится к вариативной части ОПОП ВО.

**2.** Входные требования для освоения дисциплины (модуля): учащиеся должны владеть знаниями поматематическому анализу и линейной алгебре в объеме, соответствующем программе первого года обучения основных образовательных программ бакалавриата по укрупненным группам направлений и специальностей 01.00.00 «Математика и механика», 02.00.00 «Компьютерные и информационные науки».

**3.** Результаты обучения по дисциплине (модулю), соотнесенные с требуемыми компетенциями выпускников*.*

Компетенции выпускников, частично формируемые при реализации дисциплины (модуля):

* **ПК-5.Б** Способность определить совокупность математических методов и программных решений для отдельного этапа решения прикладной задачи в рамках заданной схемы.

Планируемые результаты обучения по дисциплине (модулю):

**Знать:**

1. основные понятия, определения и факты в области программно-аппаратных средств защиты информации;

**Уметь:**

1. применять на практике основные методы обеспечения безопасности программного обеспечения в компьютерных системах;
2. применять на компьютерные технологии для решения различных задач компьютерной безопасности;
3. находить, анализировать и обрабатывать научно-техническую информацию;
4. извлекать полезную научно-техническую информацию из электронных библиотек, реферативных журналов;
5. демонстрировать способность к анализу и синтезу;
6. демонстрировать способность к письменному и устному общению на русском языке;
7. публично представить собственные и известные научные результаты;

**Владеть:**

1. навыками решения практических задач в области программно-аппаратных средств защиты информации;
2. методами использования теории построения политик безопасности компьютерных систем;
3. проведения анализа угроз и поиска уязвимостей в компьютерных системах.

**4.** Формат обучения: занятия проводятся с использованием меловой или маркерной доски, интерактивные материалы демонстрируются с помощью ноутбука и проектора.

**5.** Объем дисциплины (модуля) составляет 2 з.е., в том числе 36 академических часа, отведенных на контактную работу обучающихся с преподавателем, 36 академических часов на самостоятельную работу обучающихся.

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Наименование и краткое содержание разделов и тем дисциплины (модуля),**  **Форма промежуточной аттестации по дисциплине (модулю)** | **Всего**  **(часы**) | В том числе | | | |
| **Контактная работа  (работа во взаимодействии с преподавателем)**  **Виды контактной работы, часы** | | | **Самостоятельная работа обучающегося,**  **часы** |
| Занятия лекционного типа\* | Занятия семинарского типа\* | **Всего** |  |
| 1. Введение | **2** | 2 | – | **2** | **–** |
| 2. Информационная безопасность и управление рисками | **8** | 4 | – | **4** | **4** |
| 3. Управление доступом | **8** | 4 | – | **4** | **4** |
| 4. Архитектура и модель безопасности | **8** | 4 | – | **4** | **4** |
| 5. Физическая безопасность и безопасность окружения | **4** | 2 | – | **2** | **2** |
| 6. Телекоммуникационная и сетевая безопасности | **8** | 4 | – | **4** | **4** |
| 7. Криптография | **8** | 4 | – | **4** | **4** |
| 8. Непрерывность бизнеса и восстановление после аварий | **4** | 2 | – | **2** | **2** |
| 9. Законодательство, требование, соответствие, расследования | **4** | 2 | – | **2** | **2** |
| 10. Безопасность приложений | **10** | 4 | – | **4** | **6** |
| 11. Операционная безопасность | **4** | 2 | – | **2** | **2** |
| 12. Требования и особенности законодательства РФ | **4** | 2 | – | **2** | **2** |
| Итого | **72** | 36 | – |  | **36** |

7. Фонд оценочных средств (ФОС) для оценивания результатов обучения по дисциплине (модулю)

7.1. Типовые контрольные задания или иные материалы для проведения текущего контроля успеваемости.

Текущий контроль успеваемости и самостоятельной работы студентов оценивается по глубине вопросов, задаваемых студентами на консультациях и в ходе лабораторных работ.

7.2. Типовые контрольные задания или иные материалы для проведения промежуточной аттестации.

Вопросы к индивидуальному собеседованию.

1. Подход “сверху-вниз”. Типы защитных мер. Активы. Безопасность посредством неизвестности.
2. Должная забота и должная осмотрительность. Различия. AIC-триада. Уязвимость. Угроза. Риск. Воздействие. Контрмеры. Взаимосвязь.Правильная последовательность оценки угроз.
3. Организационная модель безопасности. Виды целей модели безопасности. Программа безопасности.
4. Стратегическое управление безопасностью. Необходимость стандартов. BS 7799. ISO/IEC 27001. ISO/IEC 27002Атаки типа «переполнение буфера».
5. Управление информационными рисками. Анализ рисков. Ценность информации и активом. FMEA.
6. SLE, ALE, EF, ARO. Общий и остаточный риск. Стоимость защитных мер. Обработка риска.
7. Типы аутентификации. Смарт-карта. Токен. SSO. Каталоги. Управление паролями. Биометрия. Принцип необходимо знать и наименьших привилегий.
8. Управление доступом. Доступ. Субъект. Объект. Домен. Идентификация. Аутентификация. Авторизация.
9. Kerberos. Radius. Diameter.
10. Модель доступа. Управление доступом: дискреционное, мандатное, ролевое. Техники управления доступом. Уровни управления доступом. Функциональное управление доступом.
11. IDS. IPS. Cнифферы. honeypot. Угрозы по управлению доступом.
12. Модель конечных автоматов. Модель Bell-Lapadula. Модель Biba. Модель Clark-Wilson. Модель информационных потоков. Модель не влияния. Сетчатая модель.
13. Режимы безопасности функционирования. NDA. Оранжевая книга. Радужная серия. Красная книга. Общие критерии. Сертификация. Аккредитация. Открытые и закрытые системы.
14. Физическая безопасность. Типы угроз. CPTED. Подход, нацеленный на укрепленность. Точки входа. Система жизнеобеспечения здания. Безопасность периметра. Системы обнаружения вторжений.
15. Непрерывность бизнеса и восстановление после аварий. Важность данной тематики в ИБ.
16. Проблемы киберправа.
17. Сложности борьбы с киберпереступностью. Коммерческая тайна. Авторское право. Патент. Торговая марка. Неприкосновенность частной жизни.
18. Компьютерная криминалистика и сбор. Виды доказательств. Этика. Совет по архитектуре интернета.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ результатов обучения (РО) по дисциплине (модулю)** | | | | |
| Оценка  РО и соответствующие виды оценочных средств | 2 | 3 | 4 | 5 |
| **Знания**  *Индивидуальное собеседование* | Отсутствие знаний | Фрагментарные знания об основных понятиях, определениях и фактах в области программно-аппаратных средств защиты информации | Общие, но не структурированные знания об  основных понятиях, определениях и фактах в области программно-аппаратных средств защиты информации | Сформированные систематические знания об основных понятиях, определениях и фактах в области программно-аппаратных средств защиты информации |
| **Умения**  *Индивидуальное собеседование* | Отсутствие умений | В целом успешное, но не систематическое умение применять на практике основные методы обеспечения безопасности программного обеспечения в компьютерных системах; | В целом успешное, но содержащее отдельные пробелы умение (допускает неточности непринципи-ального характера) применять на практике основные методы обеспечения безопасности программного обеспечения в компьютерных системах; | Успешное и систематическое умение применять на практике основные методы обеспечения безопасности программного обеспечения в компьютерных системах; |
| **Навыки  (владения, опыт деятельности)**  *Индивидуальное собеседование* | Отсутствие навыков (владений, опыта) | Наличие отдельных навыков (наличие фрагментарного опыта) решения практических задач в области программно-аппаратных средств защиты информации; | В целом, сформированные навыки (владения), но используемые не в активной форме решения практических задач в области программно-аппаратных средств защиты информации; | Сформированные навыки (владения), применяемые при решении практических задач в области программно-аппаратных средств защиты информации; |

|  |  |
| --- | --- |
| **Соответствие результатов обучения и компетенций, в развитии которых участвует дисциплина (модуль)** | |
| Результаты обучения | Компетенция, с частичным формированием которой связано достижение результата обучения |
| **Знать:**   1. основные понятия, определения и факты в области программно-аппаратных средств защиты информации;   **Уметь:**   1. применять на практике основные методы обеспечения безопасности программного обеспечения в компьютерных системах; 2. применять на компьютерные технологии для решения различных задач компьютерной безопасности; 3. находить, анализировать и обрабатывать научно-техническую информацию; 4. извлекать полезную научно-техническую информацию из электронных библиотек, реферативных журналов; 5. демонстрировать способность к анализу и синтезу; 6. демонстрировать способность к письменному и устному общению на русском языке; 7. публично представить собственные и известные научные результаты;   **Владеть:**   1. навыками решения практических задач в области программно-аппаратных средств защиты информации; 2. методами использования теории построения политик безопасности компьютерных систем; 3. проведения анализа угроз и поиска уязвимостей в компьютерных системах. | ПК-5.Б |

8. Ресурсное обеспечение:

Основная литература:

1. Корт С.С. Теоретические основы защиты информации: Учебное пособие. – М.: Гелиос АРВ, 2004.
2. Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах. – Екатеринбург: изд-во Урал. Ун-та, 2003.
3. Теория и практика обеспечения информационной безопасности / Под ред. П.Д. Зегжды. М.:Яхтсмен, 1996.
4. Прокопьев И.В., Шрамков И.Г., Щербаков А.Ю. Введение в теоретические основы компьютерной безопасности : Уч. пособие. М., 1998.
5. Зегжда Д.П.,Ивашко А.М. Основы безопасности информационных систем. М.:Горячая линия - Телеком, 2000.
6. Теоретические основы компьютерной безопасности: Учеб. пособие для вузов / П.Н. Девянин, О.О.Михальский, Д.И.Правиков и др.- М.: Радио и Связь, 2000.
7. Шнайер Б. Прикладная криптография. М.: ТРИУМФ, 2002.

Дополнительная литература:

1. Microsoft Windows Internals: Windows Server 2003, Windows XP, and Windows 2000, М. Руссинович, Д. Соломон.
2. Windows Internals, 6th Edition, Mark E. Russinovich, David A. Solomon, Alex Ionescure.
3. METASPLOIT: The Penetration Tester’s Guide by David Kennedy, Jim O’Gorman, Devon Kearns, and Mati Aharoni.
4. Разработка ядра Linux, Роберт Лав.
5. Computer Networks, 5/e, Tanenbaum.
6. CISSP All-in-One Exam Guide, Shon Harris.

Материально-техническое обеспечение: Наличие литературы в отраслевой библиотеке, медиапроектор и компьютер для проведения лекций-презентаций, компьютерный класс для проведения лабораторных работ.

9. Язык преподавания: русский.

10. Преподаватели: М.н.с. Гилязов Руслан Раджабович (irusrubin@gmail.com)

11. Авторы программы: М.н.с. Гилязов Руслан Раджабович (irusrubin@gmail.com)