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

# БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.03.01 Информационная безопасность
*Код и наименование направления подготовки/специальности*

«Организация и технологии защиты информации
(по отрасли или в сфере профессиональной деятельности)»
*Наименование направленности (профиля)/ специализации*

Уровень высшего образования: *бакалавриат*

Форма обучения: *очная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2024

БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ
Рабочая программа дисциплины

Составитель:
Кандидат технических наук, доцент кафедры КЗИ А.С. Моляков

Ответственный редактор
Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты информации
№ 8 от 14.03.2024

# Оглавление

## 1. Пояснительная записка

### 1.1. Цель и задачи дисциплины

*Цель дисциплины*: приобретение знаний о базовых методах и способах защиты программного обеспечения (ПО)автоматизированных систем и умений применять на практике средства защиты программ, имеющиеся на отечественном рынке продукции и услуг в области защиты информации от несанкционированного доступа.

*Задачи дисциплины*:рассмотрение следующих вопросов: основные понятия теории алгоритмов и теории сложности вычислений; методы анализа ПО; методы защиты разрабатываемых программ от автоматической генерации инструментальными средствами программных средств скрытого воздействия; методы идентификации программ и их характеристик; методы защиты программ от компьютерных вирусов; методы защиты программ от исследования; методы обфускации программ; методы защиты программ от несанкционированного копирования; средства и системы тестирования программного обеспечения при испытаниях его на безопасность; операционные системы в защищённом исполнении.

### 1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине

| **Компетенция** (код и наименование) | **Индикаторы компетенций** (код и наименование) | **Результаты обучения** |
|---|---|---|
| ПК-6<br>Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации | ПК-6.1<br>Знает оценки работоспособности применяемых средств защиты информации с использованием штатных средств и методик | Знать: принципы работы программных средств системного, прикладного и специального назначения, инструментальных средств. |
| | ПК-6.2<br>Умеет оценить эффективности применяемых средств защиты информации с использованием штатных средств и методик | Уметь: выбирать, устанавливать и настраивать средства системного, прикладного и специального назначения. |
| | ПК-6.3<br>Владеет навыками определения уровня защищенности и доверия средств защиты информации | Владеть: навыками настройки и эксплуатации инструментальные средства, языки и системы программирования для решения профессиональных задач с соблюдением требований по защите информации. |
| ПК-3<br>Способен администрировать подсистемы информационной безопасности объекта защиты | ПК-3.1<br>Знает требования к встроенным средствам защиты информации программного обеспечения | Знать: основные методы управления защитой информации, информационные ресурсы и базовой модели нарушителя ФСТЭК России |
| | ПК-3.2<br>Умеет анализировать угрозы безопасности информации программного обеспечения, формулировать и обосновывать правила безопасной эксплуатации программного обеспечения, производить проверку соответствия реальных характеристик программно- | Уметь: классифицировать угрозы, разрабатывать технические предложения по совершенствованию системы управления защиты информации автоматизированных систем, проводить аудит с |

| | | |
|---|---|---|
| | аппаратных средств защиты информации заявленным в их технической документации | целью оценки рисков |
| | ПК-3.3<br>Владеет навыками ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования | Владеть: навыками по разработке организационно-технических по защите информации, приемы и принципы в соответствие с ЕСКД, ЕСПД и другими нормативно-правовыми документами |

### 1.3. Место дисциплины в структуре основной образовательной программы

Дисциплина «Безопасность программного обеспечения автоматизированных систем» относится к части, формируемой участниками образовательных отношений блока дисциплин учебного плана.

Для освоения дисциплины необходимы компетенции, сформированные в ходе изучения следующих дисциплин: «Теория вероятностей и математическая статистика», «Дискретная математика», «Технология и методы программирования».

В результате освоения дисциплины формируются компетенции, необходимые для изучения следующих дисциплин и прохождения практик: «Безопасность критически важных систем», «Защита информации от вредоносного программного обеспечения», «Преддипломная практика».

## 2. Структура дисциплины

Общая трудоемкость дисциплины составляет 3зачетные единицы, 108 часов

**Структура дисциплины для очной формы обучения**

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

| Семестр | Тип учебных занятий | Количество часов |
|---|---|---|
| **6** | Лекции | **26** |
| **6** | Лабораторные работы | **32** |
| | Всего: | **58** |

Объем дисциплины в форме самостоятельной работы обучающихся составляет _50_ академических часов.

## 3. Содержание дисциплины

| № | Наименование раздела дисциплины | Содержание |
|---|---|---|
| **1** | **Введение в теорию и практику защиты программного обеспечения** | Проблема защиты программного обеспечения автоматизированных систем. Объекты защиты. Системное и общесистемное программное обеспечение. Специальное программное обеспечение. Прикладное программное обеспечение. Языки, системы и оболочки программирования, инструментальные средства автоматизации программирования.<br>Защита программного обеспечения как система науч- |

| | | |
|---|---|---|
| | | ных дисциплин. Угрозы безопасности программного обеспечения. Принятая аксиоматика и терминология. Жизненный цикл программного обеспечения автоматизированных систем. Технологическая и эксплуатационная безопасность программного обеспечения. Модели угроз безопасности программного обеспечения. Основные принципы обеспечения безопасности программного обеспечения |
| **2** | **Основные положения, понятия и определения, используемые при защите программного обеспечения** | Базовые научные положения и основания теории защиты программ. Основы теории алгоритмов. Элементы теории сложности вычислений. Элементы криптологии. Конфиденциальные вычисления |
| **3** | **Методы обеспечения технологической и эксплуатационной безопасности программного обеспечения** | Методы анализа безопасности программного обеспечения. Методы идентификации программ и их характеристик. Методы защиты программ от компьютерных вирусов. Методы защиты программ от исследования. Обфускация программ. Методы и средства обеспечения целостности и достоверности используемого программного кода. Методы защиты программ от несанкционированного копирования.<br>Создание защищенных операционных систем. Использование программы PGP. |
| **4** | **Средства и системы защиты программного обеспечения** | Средства и системы тестирования программного обеспечения при испытаниях его на технологическую безопасность.<br>Средства и комплексы защиты программ от компьютерных вирусов. Обфускаторы программ. Средства обеспечения целостности и достоверности используемого программного кода. Средства защиты программ от несанкционированного копирования.<br>Операционные системы в защищенном исполнении. Использование программы TrueCrypt |
| **5** | **Исследование программного обеспечения на предмет отсутствия недекларированных возможностей** | Подготовка к исследованию программного обеспечения на предмет отсутствия недекларированных возможностей. Контроль и фиксация исходного состояния программного обеспечения. |
| **6** | **Отечественные нормативные акты, регламентирующие деятельность в области защиты программного обеспечения** | Федеральный закон «Об информации, информационных технологиях и о защите информации». ГОСТ Р ИСО/МЭК 12207-2010. ГОСТ Р ИСО/МЭК 15408-2013. ГОСТ Р МЭК 61508-2012.<br>Руководящий документ ФСТЭК России. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей. |

## 4. Образовательные технологии

| **№ п/п** | **Наименование темы** | **Виды учебных занятий** | **Образовательныетехнологии** |
|---|---|---|---|
| **1** | **2** | **3** | **4** |
| 1 | Введение<br>в теорию и практику защиты программного обеспечения | Лекция 1<br><br><br>Самостоятельная работа | Традиционная с использованием презентаций<br><br>Изучение материалов лекций |
| 2 | Основные положения, поня- | Лекция 2.1 | Лекция-дискуссия |

| № п/п | Наименование темы | Виды учебных занятий | Образовательныетехнологии |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| | тия и определения, используемые при защите программного обеспечения | Лекция 2.2<br><br>Самостоятельная работа | Традиционная<br><br>Изучение материалов лекций |
| 3 | Методы обеспечения технологической и эксплуатационной безопасности программного обеспечения | Лекция 3.1<br>Лекция 3.2<br><br>Лабораторнаяработа1.<br><br>Самостоятельная работа | Лекция-дискуссия<br>Традиционная<br><br>Выполнение задания в виртуальной машине CentOS 7.<br><br>Изучение материалов лекций, доклады |
| 4 | Средства и системы защиты программного обеспечения | Лекция 4.1<br>Лекция 4.2<br><br>Лабораторная работа 2.<br><br>Самостоятельная работа | Проблемная лекция<br>Традиционная с использованием презентаций<br><br>Выполнение задания в виртуальной машине CentOS 7. Изучение материалов лекций<br>Изучение материалов лекций, доклады |
| 5 | Исследование программного обеспечения на предмет отсутствия недекларированных возможностей | Лекция 5.1<br>Лекция 5.2<br>Лекция 5.3<br><br>Лабораторная работа3.<br><br>Самостоятельная работа | Лекция с разбором конкретных ситуаций<br>Традиционная<br><br>Выполнение задания в виртуальной машине CentOS 7.<br><br>Изучение материалов лекций |
| 6 | Отечественные нормативные акты, регламентирующие деятельность в области защиты программного обеспечения | Лекция 6.1<br>Лекция 6.2<br><br>Лабораторная работа 4<br><br>Самостоятельная работа | Лекция-дискуссия<br><br><br>Выполнение задания в виртуальной машине CentOS 7.<br>Изучение материалов лекций, доклады |

## 5. Оценка планируемых результатов обучения

### 5.1. Система оценивания

| Форма контроля | Макс. количество баллов | |
|---|---|---|
| | За одну работу | Всего |
| Текущий контроль: | | |
| - доклад | 5 баллов | 30 баллов |
| - участие в дискуссии на занятии | 5 баллов | 10 баллов |
| - лабораторная работа (темы 3-4) | 10 баллов | 10 баллов |
| - лабораторная работа (тема 5-6) | 10 баллов | 10 баллов |
| Промежуточная аттестация - зачет (тестирование) | | 40 баллов |
| **Итого за семестр** | | 100 баллов |

Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины представляется в виде таблицы:

| № п/п | Контролируемые разделы дисциплины | Код контролируемой компетенции | Наименование оценочного средства |
|---|---|---|---|

| | | | |
|---|---|---|---|
| | | | |
| 1. | Темы 1 – 6 | ПК-3. | Опрос |
| 2. | Лабораторные занятия 1 – 4 | ПК-6 | Отчет |

### 5.2.Критерии выставления оценки по дисциплине

| **Баллы/ Шкала ECTS** | **Оценка по дисциплине** | **Критерии оценки результатов обучения по дисциплине** |
|---|---|---|
| 100-83/ A,B | зачтено | Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации.<br>Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения.<br>Свободно ориентируется в учебной и профессиональной литературе.<br>Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.<br>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий». |
| 82-68/ C | зачтено | Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей.<br>Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами.<br>Достаточно хорошо ориентируется в учебной и профессиональной литературе.<br>Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.<br>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший». |
| 67-50/ D,E | зачтено | Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации.<br>Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами.<br>Демонстрирует достаточный уровень знания учебной литературы по дисциплине.<br>Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.<br>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный». |
| 49-0/ F,FX | не зачтено | Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации.<br>Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами.<br>Демонстрирует фрагментарные знания учебной литературы по дисциплине.<br>Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.<br>Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы. |

**5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине**

***Примерные вопросы и задания для практических заданий-***

| **Контрольные вопросы и задания** |
|---|
| 1.Наиболее вероятный объект воздействия в АС? Дайте определения «защищенности ПО АС» и «уровня безопасности ПО». Технологическая и эксплуатационная безопасность ПО. |
| 2. Объекты защиты. Системное и общесистемное ПО. ПО промежуточного слоя. Специальное и прикладное ПО. Языки, системы и оболочки программирования. Защита программного обеспечения как система научных дисциплин. |
| 3. Угрозы и модели угроз безопасности ПО. Основные принципы обеспечения безопасности программного обеспечения. |
| 4. Модели вычислений: Машина Тьюринга, машина Поста, RAM-машина, РАСП-машина и их разновидности. Схемы. Булевы схемы. Процессоры и сети процессоров. |
| 5. Символ О-большое и Омега-большое. Вычислимые функции и разрешимые предикаты. Сложность и классы вычислений. Односторонние функции и функции с секретом. Псевдослучайные генераторы. |
| 6. Криптосистемы с секретным и открытым ключом. Схемы электронной подписи. Схемы хэширования. Схемы построения псевдослучайных генераторов. Схемы вероятностного шифрования. Конфиденциальные вычисления. |
| 7. Методы анализа безопасности программного обеспечения. Контрольно-испытательные методы анализа безопасности программного обеспечения. Логико-аналитические методы контроля безопасности программ. Сравнениелогико-аналитическихи контрольно-испытательных методов анализа безопасности программ. |
| 8. Методы защиты разрабатываемых программ от автоматической генерации инструментальными средствами ПССИВ. Способы внедрения ПССИВ посредством инструментальных средств. Возможные методы защиты программ от потенциально опасных инструментальных средств. |
| 9. Методы идентификации программ и их характеристик. Идентификация программ по внутренним характеристикам. Способы оценки подобия целевой и исследуемой программ с точки зрения наличия программных дефектов. |
| 10. Методы защиты программ от компьютерных вирусов. Общая характеристика и классификация компьютерных вирусов. Общая характеристика средств нейтрализации компьютерных вирусов. Классификация методов защиты от компьютерных вирусов. |
| 11. Методы защиты программ от исследования. Классификация средств исследования программ. Способы защиты программ от исследования. Способы встраивания защитных механизмов в программное обеспечение. Обфускация программ. |
| 12. Методы и средства обеспечения целостности и достоверности используемого программного кода. |
| 13. Методы защиты программ от несанкционированного копирования. Криптографические методы защиты от копирования. Метод привязки к идентификатору. Методы, основанные на работе с переходами и стеком. Манипуляции с кодом программы. Методы противодействия динамическим способам снятия защиты программ от копирования. |
| 14. Создание защищенных операционных систем. |
| 15. Наиболее вероятный объект воздействия в АС? Дайте определения «защищенности ПО АС» и «уровня безопасности ПО». Технологическая и эксплуатационная безопасность ПО. |

***Примерные темы докладов, вопросов для тестирования***

| **Темы докладов** |
|---|
| Проблема защиты программного обеспечения автоматизированных систем. |
| 2. Защита программного обеспечения как система научных дисциплин. |
| 3. Угрозы безопасности программного обеспечения. |
| 4. Технологическая и эксплуатационная безопасность программного обеспечения. |
| 5. Модели угроз безопасности программного обеспечения. |

| |
|---|
| 6. Основные принципы обеспечения безопасности программного обеспечения. |
| 7. Методы анализа безопасности программного обеспечения. |
| 8. Методы защиты разрабатываемых программ от автоматической генерации инструментальными средствами ПССИВ. |
| 9. Методы идентификации программ и их характеристик. |
| 10. Методы защиты программ от компьютерных вирусов. |
| 11. Методы защиты программ от исследования. |
| 12.Обфускация программ. |
| 13. Методы и средства обеспечения целостности и достоверности используемого программного кода. |
| 14. Методы защиты программ от несанкционированного копирования |

***Примерные задания для тестирования****-проверка сформированности компетенции ПК-1,ПК-3*

**1. ССИВ - это:**
*а) средства скрытого информационного воздействия*
б) средства связи типа “волновод”
в) средство контроля радиоизлучений.

**2. Обфускация программ - это:**
а) сетевое устройство, подключаемое к двум и более.
*б)запутывание кода — приведение исходного текста или исполняемого кода програмы к виду, сохраняющему её функциональность, но затрудняющему анализ, понимание алгоритмов работы и модификацию при декомпиляции.*
в) процессорный модуль.

## 6. Учебно-методическое и информационное обеспечение дисциплины

### 6.1. Список источников и литературы

Источники

Основные


1. *Базовая модель угроз безопасности* персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г. [Электронный ресурс] / ФСТЭК России. – Режим доступа : https://fstec.ru/files/492/---15--2008-/887/---15--2008-.pdf, свободный. – Загл. с экрана.
2. *ГОСТ Р 50922-2006*. Защита информации. Основные термины и определения. [Электронный ресурс] / Режим доступа : https://protect.gost.ru/document1.aspx?control=31&baseC=6&page=0&month=3&year=2024&search=50922&id=129024, свободный. – Загл. с экрана
3. *Методика определения актуальных угроз безопасности* персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г. [Электронный ресурс] / ФСТЭК России. – Режим доступа : https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodika-ot-14-fevralya-2008-g, свободный. – Загл. с экрана.
4. *Методические рекомендации по разработке* нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности. Утверждены руководством 8 Центра ФСБ России от 31 марта 2015 года № 149/7/2/6-432 [Электронный ресурс] / ФСТЭК России. – Режим доступа : https://www.consultant.ru/document/cons_doc_LAW_185051/, свободный. – Загл. с экрана.

5. *Руководящий документ*. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-30-marta-1992-g-3, свободный. – Загл. с экрана.
6. *Руководящий документ*. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-30-marta-1992-g-2, свободный. – Загл. с экрана.
7. *Руководящий документ*. Средства вычислительной техники. Межсетевые экраны Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-25-iyulya-1997-g, свободный. – Загл. с экрана.

Дополнительные

8. *Руководящий докумен*т. Защита от несанкционированного доступа к информации. Термины и определения. Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-30-marta-1992-g-1, свободный. – Загл. с экрана.
9. Руководящий документ ФСТЭК России. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей. [Электронный ресурс]. – Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-4-iyunya-1999-g-n-114.
10. *Федеральный закон* «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ . [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.
11. Приказ ФСБ России от 27.12.2011 N 796 (ред. от 13.04.2022) "Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра" [Электронный ресурс]. – Режим доступа : https://www.consultant.ru/document/cons_doc_LAW_126209/, свободный в комм. версии. – Загл. с экрана.
12. Приказ ФСТЭК России от 29.04.2021 г. № 77 [Электронный ресурс] / ФСТЭК России. – Режим доступа : https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-29-aprelya-2021-g-n-77, свободный. – Загл. с экрана.

Литература

Основная

Флоу, С. Занимайся хакингом как невидимка. Искусство взлома облачных инфраструктур : руководство / С. Флоу ; перевод с английского В. С. Яценкова. — Москва : ДМК Пресс, 2023. — 272 с. — ISBN 978-5-97060-977-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/314924

Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений / С. Н. Никифоров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2023. — 96 с. — ISBN 978-5-507-45868-4. —

Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/288974

Прохорова, О. В. Информационная безопасность и защита информации / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург : Лань, 2023. — 124 с. — ISBN 978-5-507-46010-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/293009

Музипов, Х. Н. Программно-технические комплексы автоматизированных систем управления : учебное пособие / Х. Н. Музипов. — Санкт-Петербург : Лань, 2022. — 164 с. — ISBN 978-5-8114-3133-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/213098

Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/165837

Маршаков, Д. В. Программно-аппаратные средства защиты информации : учебное пособие / Д. В. Маршаков, Д. В. Фатхи. — Ростов-на-Дону : Донской ГТУ, 2021. — 228 с. — ISBN 978-5-7890-1878-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/237770

Ларина, Т. Б. Администрирование операционных систем. Управление системой : учебное пособие / Т. Б. Ларина. — Москва : РУТ (МИИТ), 2020. — 71 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/175980. — Режим доступа: для авториз. пользователей.

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

1. Варновский Н.П. Курс лекций по математической криптографии [Электронный ресурс]. – Режим доступа: http://cryptography.ru/wp-content/uploads/2014/11/varn_lectures_long.pdf
2. Гарант [Электронный ресурс]: информационно-правовой портал. – Электрон.дан. – М.: НПП "ГАРАНТ-СЕРВИС", cop. 2012. – Режим доступа: www.garant.ru.
3. КонсультантПлюс [Электронный ресурс]. – Электрон.дан. – М.: КонсультантПлюс, cop. 1997-2012. – Режим доступа: www.consultant.ru.

Национальная электронная библиотека (НЭБ) www.rusneb.ru
ELibrary.ru Научная электронная библиотека www.elibrary.ru

**Профессиональные базы данных и информационно-справочные системы**

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:
1. Консультант Плюс
2. Гарант

## 7. Материально-техническое обеспечение дисциплины

Для обеспечения дисциплины используется материально-техническая база образовательного учреждения:

1) для лекционных занятий - учебная аудитория, доска, компьютер или ноутбук, проектор (стационарный или переносной) для демонстрации учебных материалов.

Состав программного обеспечения:
1. Windows
2. MicrosoftOffice

3. KasperskyEndpointSecurity

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

2) для практических занятий – компьютерный класс или лаборатория, доска, проектор (стационарный или переносной), компьютер или ноутбук для преподавателя, компьютеры для обучающихся.

Состав программного обеспечения:
1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security
4. Mozilla Firefox
5. Microsoft Share Point 2010
6. Vmware Player 15.5
7. OllyDebugger 1.10
8. Hashcalc 2.02
9. XSpider 7.0

## 8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:

– лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

– письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;

– обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

– для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;

– письменные задания оформляются увеличенным шрифтом;

– экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих:

– лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;

– письменные задания выполняются на компьютере в письменной форме;

– экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата:

– лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

– письменные задания выполняются на компьютере со специализированным программным обеспечением;

– экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с

учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:

– в печатной форме увеличенным шрифтом;
– в форме электронного документа;
– в форме аудиофайла.

- для глухих и слабослышащих:

– в печатной форме;
– в форме электронного документа.

- для обучающихся с нарушениями опорно-двигательного аппарата:

– в печатной форме;
– в форме электронного документа;
– в форме аудиофайла.

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 слепых и слабовидящих:

– устройством для сканирования и чтения с камерой SARA CE;
– дисплеем Брайля PAC Mate 20;
– принтером Брайля EmBrailleViewPlus;

- для глухих и слабослышащих:

– автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
– акустический усилитель и колонки;

- для обучающихся с нарушениями опорно-двигательного аппарата:

– передвижными, регулируемыми эргономическими партами СИ-1;
– компьютерной техникой со специальным программным обеспечением.

## 9. Методические материалы

### 9.1. Планы лабораторных занятий

Темы учебной дисциплины предусматривают проведение лабораторных работ, которые служат как целям текущего и промежуточного контроля за подготовкой студентов, так и целям получения практических навыков применения методов выработки решений, закрепления изученного материала, развития умений, приобретения опыта решения конкретных проблем, ведения дискуссий, аргументации и защиты выбранного решения.

Помощь в этом оказывают задания для лабораторных работ, выдаваемые преподавателем на каждом занятии, задания на самостоятельную подготовку, перечень вопросов для подготовки к экзамену и контрольные домашние задания для самостоятельной работы студентов.

Целью лабораторных работ является закрепление теоретического материала и приобретение практических навыков использования методов применения пакетов компьютерной математики в профессиональной деятельности, применять навыки для принятия наиболее эф-

фективных решений в условиях быстро меняющейся реальности, для быстрой адаптации к изменяющимся условиям деятельности.

Тематика лабораторных работ соответствует программе курса.

**Лабораторная работа № 1 (8 часов). Методы обеспечения технологической и эксплуатационной безопасности программного обеспечения**-проверка сформированности компетенции *ПК-1,ПК-3*

*Цель занятия:* получение практических навыков в защите программ от ПССИВ и их несанкционированного исследования, копирования и распространения.

*Указания по выполнению задания:* обратить внимание на свойства защищенности программ на этапах производства, поставки и эксплуатации программных комплексов.

*Вопросы для изучения и обсуждения:*

1. Методы анализа безопасности программного обеспечения.

2. Методы защиты разрабатываемых программ от автоматической генерации инструментальными средствами ПССИВ.

3. Методы идентификации программ и их характеристик.

4. Методы защиты программ от компьютерных вирусов.

5. Методы защиты программ от исследования.

6. Методы обфускации программ. Методы и средства обеспечения целостности и достоверности используемого программного кода.

7. Методы защиты программ от несанкционированного копирования.

8. Создание защищенных операционных систем.

*Контрольные вопросы:*

1. В чем состоят недостатки и достоинства контрольно-испытательных и логико-аналитических методов анализа программного обеспечения?

2. Что представляет собой статический и динамический анализ программ. При помощи каких средств проводится такой анализ?

3. Опишите способы внедрения ПССИВ посредством средств автоматизации программирования (трансляторов, компиляторов, интерпретаторов, отладчиков и др.).

4. Как оценивается подобие целевой и исследуемой программ с точки зрения наличия ПССИВ?

5. Признаки классификации компьютерных вирусов. Опишите различные типы вирусов в соответствии с этой классификацией. Приведите примеры компьютерных вирусов, с которыми вы сталкивались в повседневной жизни, К какому типу вирусов вы их отнесете? Опишите средства нейтрализации компьютерных вирусов. Приведите примеры использования антивирусных комплексов.

6. Приведите классификацию методов и средств защиты программ от исследования. В чем суть обфускации программ? Дайте определение эффективному вероятностному обфускатору.

7. Опишите методы и средства обеспечения целостности и достоверности используемого программного кода, в том числе криптографические. Опишите методы и средства защиты программ от копирования, в том числе криптографические.

8. Расскажите об отечественных защищенных операционных системах ос2000 и «Феникс».

9. Использование продукта PGP.Функциональные возможности

**Лабораторная работа№ 2 (8 часов). Средства и системы защиты программного обеспечения**-проверка сформированности компетенции*ПК-1,ПК-3*

*Цель 1занятия:* получение практических навыков в разработке и эксплуатации средств и систем защиты программного обеспечения.

*Указания по выполнению задания:* обратить внимание на прикладные области применения средств защиты программного обеспечения.

*Вопросы для изучения и обсуждения:*

1. Средства и системы тестирования программного обеспечения при испытаниях его на технологическую безопасность.

2. Опишите показатели качества программного обеспечения. Выбор номенклатуры показателей качества ПОс точки зрения его защищенности.

3. Организационные и методологические вопросы проведения испытаний ПО.

4. Построение программно-аппаратных комплексов для контроля технологической безопасности программ. Состав инструментальных средств контроля безопасности ПО при его разработке.

5. Структура и принципы построения программно-аппаратных средств контрольно-испытательного стенда испытания технологической безопасности ПО.

6. Средства и комплексы защиты программ от компьютерных вирусов. Обфускаторы программ. Средства обеспечения целостности и достоверности используемого программного кода. Средства защиты программ от несанкционированного копирования.

7. Операционные системы в защищенном исполнении. Создание операционных систем с открытым исходным кодом в защищенном исполнении.

*Контрольные вопросы:*

1. Статистические и динамические способы исследования ПО, в чем их достоинства и недостатки? В чем сущность работы дизассемблеров, дискомпиляторов, трассировщиков, следящих систем при исследовании ПО.

2. Опишите способы проведения испытаний ПО, оценки качества и сертификации программных средств. Состав методического обеспечения проведения испытаний программ. Опишите показатели качества ПО разных уровней.последовательность операций при выборе номенклатуры показателей качества ПО. Оценка значений показателей качества ПО.

3. Основные этапы проведения испытаний ПО и последовательность действий при этом.

4. Технология создания сложных программных комплексов и действия разработчиков при обеспечения технологической безопасности ПО.

5. Структурно-функциональная схема инструментальных средств поддержки создания безопасного программного обеспечения.

6. Опишите этапы контроля безопасности общего и специального ПО на этапе исследования и испытаний ПО.

7. Требования к контрольно-испытательному стенду испытания технологической безопасности ПО. Принципы его построения. Достоинства и недостатки существующих операционных сред для такого стенда.

8. Приведите примеры существующих на отечественном рынке антивирусных комплексов, их основные достоинства и недостатки. Базовый функционал антивирусных программ.

9. Как обеспечивается функциональная эквивалентность программ до и после их обфускации?

10. Приведите примеры существующих на отечественном рынке средств обеспечения целостности и достоверности используемого программного кода и средств защиты программ от несанкционированного копирования, их основные достоинства и недостатки.

11. Разработка такого дистрибутивов операционной системы с открытыми исходными кодами, который обеспечил бы учет специфики объектов, потенциально уязвимых для кибератак. Основные компоненты такого дистрибутива?

**Лабораторная работа№3 (10 часов). Исследование программного обеспечения спомощью сканера безопасности и отладчика**-проверка сформированности компетенции*ПК-1,ПК-3*

*Цель занятия:* получение практических навыков в исследовании конкретных программ при помощи отладчика Ollydebuggeи утилиты Hashcalc, сканера XSpider.

*Указания по выполнению задания:* обратить внимание на обязательность требований РД ФСТЭК России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей».

*Вопросы для изучения и обсуждения:*

1. Контроль и фиксация исходного состояния программного обеспечения.
2. Построения стендов для проведения анализа программного обеспечения.
3. Контроль состава и содержания документации на программное обеспечение.
4. Статический анализ исходных текстов программного обеспечения. Контроль полноты и отсутствия избыточности на уровне файлов и функциональных объектов. Проверка соответствия исходных файлов объектному коду. Контроль связей по управлению и информации.
5. Использование сканера XSpider при исследовании ПО.

*Выполнение задания:*

В ходе практической работы рассматривается пакет документов, необходимый для сертификации и эксплуатации ПО и собственно сертификат соответствия ПО нормативным документам и/или ТУ.

*Контрольные вопросы:*

1. В чем заключается контроль полноты и отсутствия избыточности на уровне файлов и функциональных объектов.
2. В чем заключается контроль связей по управлению и информации.
3. В чем заключается контроль выполнения функциональных объектов. Каким образом встраиваются датчики в исходный текст программ.

**Лабораторная работа № 4 (10 часов). Архивация и поиск**-проверка сформированности компетенции*ПК-1,ПК-3*

*Цель:*

Познакомиться с инструментами для работы с архивами. Получить представление о командах поиска, доступных пользователю командной строки.

*Задачи*

1. Прочитайте теоретический материал по лабораторной работе.
2. Ознакомьтесь с работой команд, приведенных в тексте лабораторной работы.
3. Получите для них страницы справочного руководства.
4. С помощью утилит findiwcполучите информацию о количестве файлов в домашнем каталоге пользователя.
5. Изучить команды which и locate.
6. Поработать с архиваторами RAR, Zip, gzip, bzip, bzip2, TAR.
7. Протестировать разные наборы архиваторов.
8. Научиться применять регулярные выражения при написании шаблона для поиска с помощью утилиты grep.

Приложение 1. Аннотация
рабочей программы дисциплины

# АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина «Безопасность операционных систем программного обеспечения» реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации.

Цель дисциплины: приобретение знаний о базовых методах и способах защиты программного обеспечения автоматизированных систем и умений применять на практике средства защиты программ, имеющиеся на отечественном рынке продукции и услуг в области защиты информации от несанкционированного доступа.

Задачи: рассмотрение следующих вопросов: основные понятия теории алгоритмов и теории сложности вычислений; методы анализа ПО; методы защиты разрабатываемых программ от автоматической генерации инструментальными средствами программных средств скрытого воздействия; методы идентификации программ и их характеристик; методы защиты программ от компьютерных вирусов; методы защиты программ от исследования; методы обфускации программ; методы защиты программ от несанкционированного копирования; средства и системы тестирования программного обеспечения при испытаниях его на безопасность; операционные системы в защищённом исполнении

Дисциплина направлена на формирование следующих компетенций:

ПК-6 – Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;

ПК-3 – Способен администрировать подсистемы информационной безопасности объекта защиты.

В результате освоения дисциплины (модуля) обучающийся должен:

Знать*:*

основные положения теории информационной безопасности и практики защиты информации от несанкционированного доступа;

нормативные правовые документы в области защиты информации;

математические модели безопасности и формальные модели доступа систем;

модели и методы защиты операционных систем;

принципы работы программных средств системного, прикладного и специального назначения, инструментальных средств;

основные проектные решения, средства и методы защиты информации от несанкционированного доступа.

Уметь:

решать типовые задачи с помощью методов защиты информации от несанкционированного доступа;

применять современные методы и методики защиты программ от программных средств скрытого информационного воздействия;

выбирать, устанавливать и настраивать средства системного, прикладного и специального назначения;применять современные методы и методики защиты программ от несанкционированного исследования, копирования, распространения и использования.

Владеть: методами разработки и использования средств защиты ПО;

навыками настройки и эксплуатации инструментальные средства, языки и системы программирования для решения профессиональных задач;

навыками эксплуатации защищенных программных средств, получивших широкое применение в современных автоматизированных системах.

По дисциплине предусмотрена промежуточная аттестация в форме зачета.

Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.