ФГБОУ ВО «Санкт-Петербургский университет ГПС МЧС России»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Специалитет по специальности
10.05.03 – Информационная безопасность автоматизированных систем

Специализация «Анализ безопасности информационных систем»

Санкт-Петербург

1. Цели и задачи дисциплины

Цель освоения дисциплины:

– является приобретение компетенций в области применения современных средств защиты информации компьютерных систем, овладение методами решения задач защиты информации от несанкционированного доступа.

Перечень компетенций, формируемых в процессе изучения дисциплины

Компетенции	Содержание
ОПК - 2	Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности
ОПК - 15	Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем
ОПК – 7.1	Способен использовать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем

Задачи дисциплины:

– ознакомить будущих специалистов с проблемными вопросами, решаемыми в области защиты компьютерной информации;

– показать роль современных программно-аппаратных средств защиты информации в обеспечении ее целостности конфиденциальности и доступности;

– показать необходимость усвоения знаний о методах и средствах защиты компьютерной информации;

– создать условия для качественного овладения обучающимися теоретических знании и практических навыков при решении типовых задач по обеспечению безопасности информационных технологий;

– подготовить обучающихся для самостоятельного использования полученных знаний для правильного выбора решений при применении комплексных систем защиты компьютерной информации

2. Перечень планируемых результатов обучения дисциплины, соотнесенных с планируемыми результатами освоения образовательной программы

Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
ОПК-2.1. Понимает состав, классификацию, особенности функционирования современных информационных технологий и программных средств, в том числе отечественного производства при решении задач профессиональной деятельности	**Знает** состав, классификацию, особенности функционирования современных информационных технологий и программных средств в защите информации, в том числе отечественного производства **Умеет** определять основные принципы функционирования и обеспечения защиты программно-аппаратных современных средств защиты информации
ОПК-2.2. Выбирает современные информационные технологии и программные средства, в том числе отечественного производства для решения задач профессиональной деятельности	**Знает** критерии оценки защищенности систем, о проблемах и направлениях развития аппаратных и программных средств защиты информации **Умеет** выбирать современные информационные технологии и программные средства защиты информации, в том числе отечественного производства
ОПК-2.3. Применяет современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности	**Знает** основные стандарты и спецификации в области обеспечения информационной безопасности, принципы обеспечения информационной безопасности в условиях современного информационного общества **Умеет** применять современные информационные технологии и программные средства защиты информации, в том числе отечественного производства
ОПК-15.1. Использует методы и инструментальные средства администрирования и контроля систем защиты автоматизированных систем	**Знает** возможности использования новых информационных технологий и их средств при практической реализации требований отечественных и международных стандартов информационной безопасности **Умеет** использовать методы и инструментальные средства администрирования и контроля систем защиты автоматизированных систем
ОПК-15.2. Осуществляет мониторинг и периодический контроль функционирования средств и систем защиты информации	**Знает** основные требования к мониторингу и периодическому контролю функционирования средств обеспечения информационной безопасности автоматизированных систем **Умеет** создавать условия безотказной эксплуатации программно-аппаратных

	средств обеспечения информационной безопасности автоматизированных систем
ОПК-15.3. Применяет инструментальные средства мониторинга и анализа состояния системы информационной безопасности	**Знает** принципы функционирования инструментальных средств мониторинга и анализа состояния системы информационной безопасности **Умеет** применять инструментальные средства мониторинга и анализа состояния системы информационной безопасности
ОПК-7.1.2. Осуществляет рациональный подбор состава программных и программно-аппаратных средств для моделирования и испытания систем защиты информационных систем	**Знает** основные тенденции развития рынка программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем управления организацией **Умеет** осуществлять рациональный подбор состава программных и программно-аппаратных средств для моделирования и испытания систем защиты информационных систем
ОПК-7.1.3. Обладает навыками администрирования и тестирования подсистем защиты информации автоматизированных систем	**Знает** функциональные возможности подсистем защиты информации автоматизированных систем **Умеет** обеспечивать конфигурирование программно-аппаратных средств защиты информации автоматизированных систем

3. Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Программно-аппаратные средства защиты информации» относится к обязательной части образовательной программы специалитета по специальности 10.05.03 – Информационная безопасность автоматизированных систем, специализация - Анализ безопасности информационных систем.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачётные единицы, 144 часа.

4.1 Распределение трудоемкости дисциплины по видам работ по семестрам для очной формы обучения

Вид учебной работы	Трудоемкость		
	з.е.	час.	по семестрам
			7
Общая трудоемкость дисциплины по учебному плану	**4**	**144**	**144**
Контактная работа		**92**	**92**
Лекции		26	26
Практические занятия		60	60
Лабораторные работы		4	4
Консультация		**2**	**2**
Самостоятельная работа		**16**	**16**
Экзамен		**36**	**36**

4.2. Тематический план, структурированный по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий для очной формы обучения

Наименование разделов	**Всего часов**	**Количество часов по видам занятий**					**Самостоятельная работа**
		Лекции	**Практические занятия**	**Лабораторные работы**	**Консультации**	**Контроль**	
7 семестр							
Раздел 1. Программно-аппаратные средства разграничения доступа к компьютерной информации	26	6	12	4			4
Раздел 2. Программно-аппаратные средства криптографической защиты информации	26	6	16				4
Раздел 3. Программно-аппаратные средства защиты программного обеспечения от копирования и изучения	28	8	16				4
Раздел 4. Программно-аппаратная защита компьютерной информации от разрушающих программных воздействий	26	6	16				4
Консультации	2				2		
Экзамен	36					36	
итого за 7 семестр	**144**	**26**	**60**	**4**	**2**	**36**	**16**
Всего	**144**	**26**	**60**	**4**	**2**	**36**	**16**

4.3 Содержание дисциплины для очной формы обучения

Раздел 1. Программно-аппаратные средства разграничения доступа к компьютерной информации

Лекции. Введение. Цели и задачи дисциплины. Основные понятия и определения в области защиты компьютерной информации. Современная ситуация в области защиты компьютерной информации. Основы защиты компьютерной информации от несанкционированного доступа. Основные термины и определения в области защиты компьютерной информации от НСД. Основные принципы и направления защиты от НСД. Формальные модели управления доступом. Понятие идентификации и аутентификации субъекта.

Практические занятия. Алгоритмы аутентификации пользователей. Секретная информация, используемая для контроля доступа: ключи и пароли. Злоумышленник и ключи. Классификация средств хранения ключей и идентифицирующей информации. Магнитные диски прямого доступа. Магнитные и интеллектуальные. Средство Touch Memory.

Лабораторная работа.

Настройка дискреционного и мандатного доступа в операционной системе Astra Linux. Настройка прав доступа пользователей в соответствии с разрешительной системой доступа. Применение заданных настроек контроля доступа.

Самостоятельная работа. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности. Основные подходы к защите данных от НСД.

Рекомендуемая литература:

Основная литература: [1, 2];

Дополнительная литература:[1,2]

Раздел 2. Программно-аппаратные средства криптографической защиты информации

Лекции. Роль и место криптографических методов и средств в обеспечении безопасности компьютерной информации. Основные понятия и процедуры технологии управления криптографическими ключами.

Практические занятия. Аппаратные и программно-аппаратные средства криптозащиты данных. Построение аппаратных компонент криптозащиты данных, специализированные СБИС как носители алгоритма шифрования. Защита алгоритма шифрования; принцип чувствительной области и принцип главного ключа. Необходимые и достаточные функции аппаратного средства криптозащиты. Секретная информация, используемая для контроля доступа: ключи и пароли.

Самостоятельная работа. Защита компонентов ПЭВМ. Методы и средства привязки программного обеспечения к аппаратному окружению и

физическим носителям. Биометрические средства защиты информации и разграничения доступа.

Рекомендуемая литература:

Основная литература:[1,2];

Дополнительная литература: [1,2]

Раздел 3. Программно-аппаратные средства защиты программного обеспечения от копирования и изучения

Лекции. Несанкционированное копирование программ как тип НСД. Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования. Разновидности задач защиты от копирования. Привязка ПО к аппаратному окружению и физическим носителям как единственное средство защиты от копирования ПО.

Практические занятия. Привязка программ к гибким магнитным дискам (ГМД). Привязка программ к жестким магнитным дискам (ЖМД). Особенности привязки к ЖМД. Виды меток на ЖМД. Привязка к прочим компонентам штатного оборудования ПЭВМ. Привязка к внешним (добавляемым) элементам ПЭВМ. Привязка к портовым ключам. Использование дополнительных плат расширения. Методы "водяных знаков" и методы "отпечатков пальцев". Понятие изучения и обратного проектирования ПО. Цели и задачи изучения работы ПО. Способы изучения ПО: статическое и динамическое изучение. Роль программной и аппаратной среды. Временная надежность (невозможность обеспечения гарантированной надежности).

Самостоятельная работа. Защита от отладки. Динамическое преобразование кода. Принцип ловушек и избыточного кода. Защита от дизассемблирования. Принцип внешней загрузки файлов. Динамическая модификация программы. Защита от трассировки по прерываниям.

Рекомендуемая литература:

Основная литература: [1, 2,];

Дополнительная литература: [1, 2]

Раздел 4. Программно-аппаратная защита компьютерной информации от разрушающих программных воздействий.

Лекции. Защита от разрушающих программных воздействий. Вирусы как особый класс разрушающих программных воздействий. Необходимые и достаточные условия недопущения разрушающего воздействия. Понятие изолированной программной среды.

Практические занятия. Программные средства антивирусной защиты: основные характеристики, принципы построения и применения.

Самостоятельная работа. Защита от разрушающих программных воздействий. Вирусы как особый класс разрушающих программных воздействий. Необходимые и достаточные условия недопущения разрушающего воздействия. Понятие изолированной программной среды.

Программные средства антивирусной защиты: основные характеристики, принципы построения и применения.

Рекомендуемая литература:

Основная литература: [1,2];

Дополнительная литература: [1,2]

5. Методические рекомендации по организации изучения дисциплины

При реализации программы дисциплины используются лекционные и практические занятия.

Общими целями занятий являются:

– обобщение, систематизация, углубление, закрепление теоретических знаний по конкретным темам дисциплины;

– формирование умений применять полученные знания на практике, реализация единства интеллектуальной и практической деятельности;

– выработка при решении поставленных задач профессионально значимых качеств: самостоятельности, ответственности, точности, творческой инициативы.

Целями лекции являются:

– систематизированные основы научных знаний по дисциплине, раскрывать состояние и перспективы развития соответствующей области науки и техники;

– концентрировать внимание обучающихся на наиболее сложных и узловых вопросах;

– стимулировать их активную познавательную деятельность и способствовать формированию творческого мышления.

В ходе практического занятия обеспечивается процесс активного взаимодействия обучающихся с преподавателем; приобретаются практические навыки и умения. Цели практического занятия: выработка практических умений и приобретение навыков, закрепление пройденного материала по соответствующей теме дисциплины.

Целями лабораторной работы являются: формирование исследовательских умений и навыков; развитие аналитических, проектировочных и конструктивных умений. выработка самостоятельности, ответственности и творческой инициативы.

Самостоятельная работа обучающихся направлена на углубление и закрепление знаний, полученных на лекциях и других занятиях, выработку навыков самостоятельного активного приобретения новых, дополнительных знаний, подготовку к предстоящим занятиям.

6. Оценочные материалы по дисциплине

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины, проводится в соответствии с содержанием дисциплины по видам занятий в форме опроса и тестирования.

Промежуточная аттестация обеспечивает оценивание промежуточных и окончательных результатов обучения по дисциплине, проводится в форме экзамена.

6.1. Примерные оценочные материалы:

6.1.1. Текущего контроля

Типовые вопросы для опроса:

1. Основные понятия и определения в области защиты компьютерной информации.
2. Современная ситуация в области защиты компьютерной информации.
3. Требования к системам защиты информации.
4. Понятие угрозы безопасности компьютерной информации. Интервал потенциальной опасности.
5. Классификация угроз безопасности компьютерной информации.
6. Источники, риски и формы атак на информацию.
7. Принципы защиты компьютерной информации
8. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация
9. Основные подходы к защите данных от НСД (контроль доступа и разграничение доступа, иерархический доступ к файлу)
10. Формальные модели управления доступом
11. Классификация средств защиты компьютерной информации от НСД
12. Аутентификация пользователей. Основные алгоритмы (протоколы) аутентификации.
13. Администрирование сетей в аспекте безопасности информации
14. Защита сетевого файлового ресурса, фиксация доступа к файлам.
15. Доступ к данным со стороны процесса, способы фиксации факта доступа.

Типовые задания для тестирования:

1. Какой антивирусный продукт Лаборатории Касперского является базовым

1. Kaspersky Total Security
2. Kaspersky Anti-Virus
3.Kaspersky Internet Security
4. Kaspersky Safe Kids

2. Какие из названных систем резервного копирования являются отечественными.

1: Киберпротект.
2: RuBackup
3: Bacula.
4: Acronis True Image

3. Криптопровайдер – это:
1. Специальное ПО, реализующая криптографические алгоритмы
2. Программа, позволяющая формировать пары логин-пароль
3. Удостоверяющий центр, предоставляющий ключи доступа
4. Компания, предоставляющая ЭЦП

4. Простая электронная подпись представляет собой:
1. Логин и пароль
2. Аналог собственноручной подписи
3. Носитель информации с цифровой подписью
4. Подпись выданная на госуслугах.

5. Бесплатная лечащая утилита от отечественного производителя антивирусов называется:
1. CurtIt!
2. Spider
3. Katana
4. Salut.

6. Метод надежной передачи информации по открытому каналу связи использует:
1. Криптографию
2. Стеганографию
3. Симметричное шифрование
4. Кодирование.

Примерный перечень вопросов выносимых на экзамен
1. Надежность систем ограничения доступа
2. Защита файлов от изменения
3. Электронная цифровая подпись (ЭЦП)
4. Методы и средства ограничения доступа к компонентам ЭВМ
5. Программно-аппаратные средства шифрования
6. Построение аппаратных компонент криптозащиты данных
7. Защита алгоритма шифрования
8. Принцип чувствительной области и принцип главного ключа
9. Пароли и ключи, организация хранения ключей
10. Необходимые и достаточные функции аппаратного средства криптозащиты
11. Защита программ от несанкционированного копирования
12. Защита программ от изучения

13. Защита программ от отладки, защита от дизассемблирования
14. Защита программ от трассировки по прерываниям
15. Защита от разрушающих программных воздействий (РПВ)
16. Компьютерные вирусы как особый класс РПВ
17. Необходимые и достаточные условия недопущения разрушающего воздействия
18. Понятие изолированной программной среды
19. Общая характеристика и классификация вредоносных программ
20. Компьютерные вирусы. Классификация компьютерных вирусов
21. Основы технологии анализа защищенности компьютерных систем управления и обработки информации
22. Многоуровневая защита корпоративных сетей.

6.2. Шкала оценивания результатов промежуточной аттестации и критерии выставления оценок

Система оценивания включает:

Форма контроля	Показатели оценивания	Критерии выставления оценок	Шкала оценивания
Экзамен	правильность и полнота ответа; выполнение контрольных нормативов	дан правильный, полный ответ на поставленный вопрос, показана совокупность осознанных знаний по дисциплине, доказательно раскрыты основные положения вопросов; могут быть допущены недочеты, исправленные самостоятельно в процессе ответа.	Отлично
		дан правильный, недостаточно полный ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи; могут быть допущены недочеты, исправленные с помощью преподавателя.	Хорошо
		дан недостаточно правильный и полный ответ; логика и последовательность изложения имеют нарушения; в ответе отсутствуют выводы.	Удовлетворительно
		ответ представляет собой разрозненные знания с существенными ошибками по вопросу; присутствуют фрагментарность, нелогичность изложения; дополнительные и уточняющие вопросы не приводят к коррекции ответа на вопрос.	Неудовлетворительно

7. Ресурсное обеспечение дисциплины.

7.1. Лицензионное и свободно распространяемое программное обеспечение

Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:

1. Лицензия №217800111-ore-2.12-client-6196

Выдана «ФГБОУ ВО Санкт-Петербургский университет ГПС МЧС России» на право использования: Astra Linux Common Edition релиз Орел

Срок действия: бессрочно

2. Лицензия №217800111-alse-1.7-client-medium-x86_64-0-14545

Выдана «ФГБОУ ВО Санкт-Петербургский университет ГПС МЧС России» на право использования: Astra Linux Special Edition

Срок действия: бессрочно

3. Лицензия №217800111-alse-1.7-client-medium-x86_64-0-14544

Выдана «ФГБОУ ВО Санкт-Петербургский университет ГПС МЧС России» на право использования Astra Linux Special Edition

Срок действия: бессрочно

4. ПО «Р7-Офис. Профессиональный»

Выдана: «ФГБОУ ВО Санкт-Петербургский университет МЧС России»

Срок действия: бессрочно

7.2. Профессиональные базы данных и информационные справочные системы

1. Сервер органов государственной власти Российской Федерации http://россия.рф/ (свободный доступ);
2. Портал открытых данных Российской Федерации https://data.gov.ru/ (свободный доступ);
3. Федеральный портал «Российское образование» http://www.edu.ru (свободный доступ);
4. Система официального опубликования правовых актов в электронном виде http://publication.pravo.gov.ru (свободный доступ);
5. Федеральный портал «Совершенствование государственного управления» https://ar.gov.ru (свободный доступ);
6. Электронная библиотека университета http://elib.igps.ru (авторизованный доступ);
7. Электронно-библиотечная система «ЭБС IPR BOOKS» http://www.iprbookshop.ru (авторизованный доступ).
8. Электроно-библиотечная система "Лань" https://e.lanbook.com (авторизованный доступ).

7.3. Литература

Основная литература:

1. Программно-аппаратные средства защиты информации. В 3 частях. Ч.1 : учебное пособие / В. А. Гриднев, Ю. А. Губсков, А. С. Дерябин, А. В. Яковлев. — Тамбов : Тамбовский государственный технический университет, ЭБС АСВ, 2022. — 81 с. — ISBN 978-5-8265-2464-0, 978-5-8265-2467-1 (ч.1). — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/133346.html (дата обращения: 25.02.2025). — Режим доступа: для авторизир. пользователей

2. Жмуров, Д. Б. Программно-аппаратные средства защиты информации : учебное пособие / Д. Б. Жмуров, С. В. Жуков. — Самара : Самарский университет, 2022. — 80 с. — ISBN 978-5-7883-1799-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/336515 (дата обращения: 25.02.2025). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

1. Программно-аппаратные средства защиты информации : учебно-методическое пособие / С. И. Штеренберг, А. М. Гельфанд, Д. В. Рыжаков, Р. А. Фатхутдинов. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2017. — 98 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180093 (дата обращения: 25.02.2025). — Режим доступа: для авториз. пользователей.

2. Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации / составители И. А. Денисов. — Москва : Московский технический университет связи и информатики, 2016. — 31 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/61529.html (дата обращения: 25.02.2025). — Режим доступа: для авторизир. пользователей

7.4. Материально-техническое обеспечение

Для проведения и обеспечения занятий используются помещения, которые представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой специалитета, оснащенные оборудованием и техническими средствами обучения: автоматизированное рабочее место преподавателя, маркерная доска, мультимедийный проектор, документ-камера, посадочные места обучающихся.

Лабораторные занятия на четвертом курсе обучения (7 семестр) проводятся в помещениях лаборатории программно-аппаратных средств защиты информации.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и

обеспечением доступа к электронной информационно-образовательной среде университета.

Автор: доктор технических наук, профессор Буйневич Михаил Викторович.