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 ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Направление подготовки 10.03.01 Информационная безопасность
Направленность (профиль) подготовки
Безопасность автоматизированных систем
Уровень квалификации выпускника – бакалавр

Форма обучения – очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2021

Безопасность программного обеспечения автоматизированных систем
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
№ 10 от 20.05.2021 г.

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**
ОПК-4.2 *Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем*	*ОПК-4.2.1* *Знает средства, методы и протоколы идентификации, аутентификации и авторизации*	*Знать: методики, обработку, принципы ААА, оценку достоверности результатов тестирования разных протоколов идентификации/аутентификации.*
	ОПК-4.2.2 *Умеет устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации*	*Уметь: проводить эксперименты и оценивать результаты тестирования. исследовать средства защиты информации, уметь оценивать по функциональным возможностям, надежности функционирования, эффективности обнаружения попыток НСД*
	ОПК-4.2.3 *Владеет навыками управления полномочиями пользователей*	*Владеть: навыками проводить эксперименты по заданной методике; навыки работы с дискреционной и мандатной политиками доступа.*
ПК-1 *Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации*	*ПК-1.1* *Знает порядок установки, настройки и обслуживания программного обеспечения, систем управления базами данных, средств электронного документооборота и средств защиты информации*	*Знать: принципы работы программных средств системного, прикладного и специального назначения, инструментальных средств.*

	ПК-1.2 *Умеет устанавливать программное обеспечение в соответствии с технической документацией, выполнять настройку параметров работы программного обеспечения, включая системы управления базами данных и средства электронного документооборота, формулировать правила безопасной эксплуатации*	*Уметь: выбирать, устанавливать и настраивать средства средства системного, прикладного и специального назначения.*
	ПК-1.3 *Владеет навыками по установке, настройке и обслуживанию программного обеспечения, программно-аппаратных и технических средств защиты информации с соблюдением требований по защите информации*	*Владеть: навыками настройки и эксплуатации инструментальные средства, языки и системы программирования для решения профессиональных задач с соблюдением требований по защите информации.*
ПК-3 *Способен управлять защитой информации в автоматизированных системах*	*ПК-3.1* *Знает основные методы управления защитой информации, информационные ресурсы автоматизированных систем, подлежащие защите; основные угрозы безопасности информации, модели нарушителя в автоматизированных системах*	*Знать: основные методы управления защитой информации, информационные ресурсы и базовой модели нарушителя ФСТЭК РФ*
	ПК-3.2 *Умеет разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем; классифицировать и оценивать угрозы безопасности информации; оценивать информационные риски в автоматизированных системах*	*Уметь: классифицировать угрозы, разрабатывать технические предложения по совершенствованию системы управления защиты информации автоматизированных систем, проводить аудит с целью оценки рисков*
	ПК-3.3 *Владеет навыками составления комплекса правил, процедур, практических*	*Владеть: навыками по разработке организационно-технических по защите информации, приемы и принципы в соответствие с*

	приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	*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», «Информационные технологии».

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

Структура дисциплины для очной формы обучения

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 114 часов, в том числе контактная работа обучающихся с преподавателем 60 ч., самостоятельная работа обучающихся 54 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	Введение в теорию и практику защиты программного обеспечения	6	2					2	Опрос
2	Основные положения, понятия и определения, используемые при защите программного обеспечения	6	4					4	Опрос
3	Методы обеспечения технологической и эксплуатационной безопасности программного обеспечения	6	4			8		8	Оценка выполнения практических и внеаудиторных заданий
4	Средства и системы защиты программного обеспечения	6	4			8		10	Оценка выполнения практических и внеаудиторных заданий

5	Исследование программного обеспечения на предмет отсутствия недекларированных возможностей	6	6			8		16	Оценка выполнения практических и внеаудиторных заданий
6	Отечественные нормативные акты, регламентирующие деятельность в области защиты программного обеспечения	6	4			10		10	Опрос
7	*Зачет*					2		4	Зачет по билетам
	Итого:		**24**			**36**		**54**	

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. Защита программного обеспечения как система научных 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 несанкциони-

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

При реализации рабочей программы дисциплины «Безопасность программного обеспечения» используются следующие образовательные технологии.

Образовательные технологии

№ п/п	**Наименование темы**	**Виды учебных занятий**	**Образовательные технологии**
1	**2**	**3**	**4**
1	*Введение в теорию и практику защиты программного обеспечения*	*Лекция 1* *Самостоятельная работа*	*Традиционная с использованием презентаций* *Изучение материалов лекций*
2	*Основные положе-*	*Лекция 2.1*	*Лекция-дискуссия*

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

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: *- опрос* *- участие в дискуссии на семинаре* *- практическая работа (темы 3-4)* *- практическая работа (тема 5-6)*	 *5 баллов* *5 баллов* *10 баллов* *10 баллов*	 *30 баллов* *10 баллов* *10 баллов* *10 баллов*
Промежуточная аттестация *Зачет*		*40 баллов*
Итого за семестр *Зачет*		*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	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-1.3; ПК-1.2; ПК-1.1; ПК-3.3, ПК-3,2, ПК-3.1	Опрос
2.	Лабораторные занятия 1 – 4	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-1.3; ПК-1.2; ПК-1.1; ПК-3.3, ПК-3,2, ПК-3.1	Отчет

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2.Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	«отлично»/ «зачтено (отлично)»/	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
	«зачтено»	промежуточной аттестации. 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. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	«хорошо»/ «зачтено (хорошо)»/ «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. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	«удовлетворительно»/ «зачтено (удовлетвори-тельно)»/ «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. 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. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	«неудовлетворительно»/ 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. Обучающийся испытывает серьёзные затруднения в

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. 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 - проверка сформированности компетенции ОПК-4.2, ПК-1,ПК-3

Контрольные вопросы и задания	Реализуемые компетенции
1.Наиболее вероятный объект воздействия в АС? Дайте определения «защищенности ПО АС» и «уровня безопасности ПО». Технологическая и эксплуатационная безопасность ПО.	ПК-1.3; ПК-1.2; ПК-1.1; ПК-3.3, ПК-3,2, ПК-3.1
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.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-1.3; ПК-1.2; ПК-1.1; ПК-3.3, ПК-3,2, ПК-3.1
3. Угрозы и модели угроз безопасности ПО. Основные принципы обеспечения безопасности программного обеспечения.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-1.3; ПК-1.2; ПК-1.1; ПК-3.3, ПК-3,2, ПК-3.1
4. Модели вычислений: Машина Тьюринга, машина Поста, RAM-машина, РАСП-машина и их разновидности. Схемы. Булевы схемы. Процессоры и сети процессоров.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3
5. Символ О-большое и Омега-большое. Вычислимые функции и разрешимые предикаты. Сложность и классы вычислений. Односторонние функции и функции с секретом. Псевдослучайные генераторы.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-1.3; ПК-1.2; ПК-1.1; ПК-3.3, ПК-3,2, ПК-3.1
6. Криптосистемы с секретным и открытым ключом. Схемы электронной подписи. Схемы хэширования. Схемы построения псевдослучайных генераторов. Схемы вероятностного шифрования. Конфиденциальные вычисления.	*ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-1.3; ПК-1.2; ПК-1.1*
7. Методы анализа безопасности программного обеспечения. Контрольно-испытательные методы анализа безопасности программного обеспечения. Логико-аналитические методы контроля безопасности программ. Сравнение логико-аналитических и контрольно-испытательных методов анализа безопасности программ.	*ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-1.3; ПК-1.2; ПК-1.1; ПК-3.3, ПК-3,2, ПК-3.1*
8. Методы защиты разрабатываемых программ от автоматической генерации инструментальными средствами ПССИВ. Способы внедрения ПССИВ посредством инструментальных средств. Возможные методы защиты	*ПК-1.3; ПК-1.2; ПК-1.1; ПК-3.3, ПК-3,2, ПК-3.1*

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.	*ПК-1.3; ПК-1.2; ПК-1.1; ПК-3.3, ПК-3,2, ПК-3.1*
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.	*ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-1.3; ПК-1.2; ПК-1.1; ПК-3.3, ПК-3,2, ПК-3.1*
11. Методы защиты программ от исследования. Классификация средств исследования программ. Способы защиты программ от исследования. Способы встраивания защитных механизмов в программное обеспечение. Обфускация программ.	*ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-1.3; ПК-1.2; ПК-1.1; ПК-3.3, ПК-3,2, ПК-3.1*
12. Методы и средства обеспечения целостности и достоверности используемого программного кода.	*ПК-1.3; ПК-1.2; ПК-1.1; ПК-3.3, ПК-3,2, ПК-3.1*
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.	*ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-1.3; ПК-1.2; ПК-1.1; ПК-3.3, ПК-3,2, ПК-3.1*
14. Создание защищенных операционных систем.	*ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-1.3; ПК-1.2; ПК-1.1; ПК-3.3, ПК-3,2, ПК-3.1*
15. Наиболее вероятный объект воздействия в АС? Дайте определения «защищенности ПО АС» и «уровня безопасности ПО». Технологическая и эксплуатационная безопасность ПО.	*ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-1.3; ПК-1.2; ПК-1.1; ПК-3.3, ПК-3,2, ПК-3.1*

Примерные темы докладов, вопросов для тестирования - проверка сформированности компетенции ОПК-4.2, ПК-1,ПК-3

Темы докладов	**Реализуемые компетенции**
Проблема защиты программного обеспечения автоматизированных систем.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-1.3; ПК-1.2; ПК-1.1; ПК-3.3, ПК-3,2, ПК-3.1
2. Защита программного обеспечения как система научных дисциплин.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-1.3; ПК-1.2; ПК-1.1; ПК-3.3, ПК-3,2, ПК-3.1
3. Угрозы безопасности программного обеспечения.	ПК-1.3; ПК-1.2; ПК-1.1; ПК-3.3, ПК-3,2, ПК-3.1
4. Технологическая и эксплуатационная безопасность программного обеспечения.	ПК-1.3; ПК-1.2; ПК-1.1; ПК-3.3, ПК-3,2, ПК-3.1
5. Модели угроз безопасности программного обеспечения.	ПК-1.3; ПК-1.2; ПК-1.1; ПК-3.3, ПК-3,2, ПК-3.1
6. Основные принципы обеспечения без-	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-1.3;

опасности программного обеспечения.	ПК-1.2; ПК-1.1
7. Методы анализа безопасности программного обеспечения.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-1.3; ПК-1.2; ПК-1.1; ПК-3.3, ПК-3,2, ПК-3.1
8. Методы защиты разрабатываемых программ от автоматической генерации инструментальными средствами ПССИВ.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-1.3; ПК-1.2; ПК-1.1; ПК-3.3, ПК-3,2, ПК-3.1
9. Методы идентификации программ и их характеристик.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-1.3; ПК-1.2; ПК-1.1; ПК-3.3, ПК-3,2, ПК-3.1
10. Методы защиты программ от компьютерных вирусов.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-1.3; ПК-1.2; ПК-1.1; ПК-3.3, ПК-3,2, ПК-3.1
11. Методы защиты программ от исследования.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-1.3; ПК-1.2; ПК-1.1; ПК-3.3, ПК-3,2, ПК-3.1
12. Обфускация программ.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-1.3; ПК-1.2; ПК-1.1; ПК-3.3, ПК-3,2, ПК-3.1
13. Методы и средства обеспечения целостности и достоверности используемого программного кода.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-1.3; ПК-1.2; ПК-1.1; ПК-3.3, ПК-3,2, ПК-3.1
14. Методы защиты программ от несанкционированного копирования	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-1.3; ПК-1.2; ПК-1.1; ПК-3.3, ПК-3,2, ПК-3.1

Примерные задания для тестирования- проверка сформированности компетенции

ОПК-4.2, 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. *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/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-

reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g3, свободный. – Загл. с экрана.
2. *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/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g, свободный. – Загл. с экрана.
3. *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/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/385-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g2, свободный. – Загл. с экрана.

Литература
Основная

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/452368
2. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/454453
3. Щеглов, А. Ю. Защита информации: основы теории: учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва: Издательство Юрайт, 2020. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449285
4. Гостев, И. М. Операционные системы : учебник и практикум для вузов / И. М. Гостев. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 164 с. — (Высшее образование). — ISBN 978-5-534-04520-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/451231
5. *Комплексная защита* информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2017. — 592 с. — (Высшее образование: Бакалавриат). - Режим доступа: http://znanium.com/catalog/product/546679
6. *Шаньгин В.Ф.* Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / В. Ф. Шаньгин. - М.: ДМК Пресс, 2010. - 544 с.: ил. - ISBN 978-5-94074-518-1. - Режим доступа: http://znanium.com/catalog/product/408107

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимый для освоения дисциплины

Адреса ресурсов 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 (дата обращения: август 2017).

2. Goldreich O. Foundations of cryptography. [Электронный ресурс]. – Режим доступа: http://www.twirpx.com/file/493751/ (дата обращения: август 2017).

3. Гарант [Электронный ресурс]: информационно-правовой портал. – Электрон. дан. – М.: НПП "ГАРАНТ-СЕРВИС", cop. 2012. – Режим доступа: www.garant.ru.

4. КонсультантПлюс [Электронный ресурс]. – Электрон. дан. – М.: КонсультантПлюс, cop. 1997-2012. – Режим доступа: www.consultant.ru.

7. Материально-техническое обеспечение дисциплины

Для проведения занятий необходимо следующее материально-техническое обеспечение:

1) для лекционных занятий – лекционный класс с видеопроектором и компьютером, на котором должны быть установлены следующее ПО:

№ п/п	Наименование ПО	Производитель	Способ распространения
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 10 Pro	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

2) для практических занятий – компьютерный класс, оборудованный современными персональными компьютерами для каждого студента. На компьютере должны быть установлено следующее ПО:

№п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 7 Pro	Microsoft	лицензионное
3	Microsoft Share Point 2010	Microsoft	лицензионное
4	Microsoft Office 2013	Microsoft	лицензионное
5	Windows 10 Pro	Microsoft	лицензионное
6	Kaspersky Endpoint Security	Kaspersky	Лицензионное
7	Vmware Player 15.5	VMWare	Режим доступа: https://www.vmware.com/products/ Демо-версия
8	OllyDebugger 1.10	OllyDbg	Свободное ПО, Режим доступа: http://www.ollydbg.de/ Демо-версия
9	Hashcalc 2.02	Astro	Свободное ПО, Режим доступа: https://hashcalc.ru.downloadastro.com/ Демо-версия

10	XSpider 7.0	Positive Technologies	Свободное ПО, Режим доступа: https://www.ptsecurity.com/ru-ru/ Демо-версия

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

Перечень БД и ИСС

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2020 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2020 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

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 EmBraille ViewPlus;

- 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 - проверка сформированности компетенций *ОПК-4.2, ПК-1,ПК-3*

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 эффективных 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 *ОПК-4.2, 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

Список литературы:

Приведён в п. 6 данной РПД

Материально-техническое обеспечение практического занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer, отладчик OllyDebugger и и утилита hashcalc.

Лабораторная работа № 2 (8 часов). Средства и системы защиты программного обеспечения - проверка сформированности компетенции *ОПК-4.2, ПК-1,ПК-3*

Цель 1 занятия: 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 ПО с 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?

Список литературы:
Приведён в п. 6 данной РПД

Материально-техническое обеспечение практического занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer, отладчик OllyDebugger и и утилита hashcalc.

Лабораторная работа №3 (8 часов). Исследование программного обеспечения с помощью сканера безопасности и отладчика - проверка сформированности компетенции *ОПК-4.2, ПК-1,ПК-3*

Цель занятия: получение практических навыков в исследовании конкретных программ при помощи отладчика Ollydebugger и 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.

Список литературы:

Приведён в п. 6 данной РПД

Материально-техническое обеспечение практического занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer, отладчика Ollydebugger и утилита hashcalc, сканер безопасности XSpider.

Лабораторная работа № 4 (10 часов). Архивация и поиск - проверка сформированности компетенции *ОПК-4.2, 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 find и wc получите 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.

Список литературы:

Приведён в п. 6 данной РПД

Материально-техническое обеспечение практического занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer с гостевой ОС CentOS 7. Занятия проводятся в специально оборудованном компьютерном классе.

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Безопасность программного обеспечения автоматизированных систем» реализуется на факультете информационных систем и безопасности на 3 курсе по направлению подготовки 10.03.01 «Информационная безопасность», (профиль подготовки – Безопасность автоматизированных систем) 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:

- ОПК-4.2 - Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем
- ОПК-4.2.1 -Знает средства, методы и протоколы идентификации, аутентификации и авторизации
- ОПК-4.2.2 -Умеет устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации
- ОПК-4.2.3 - Владеет навыками управления полномочиями пользователей
- ПК-1 - Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
- ПК-1.1 - Знает порядок установки, настройки и обслуживания программного обеспечения, систем управления базами данных, средств электронного документооборота и средств защиты информации
- ПК-1.2 -Умеет устанавливать программное обеспечение в соответствии с технической документацией, выполнять настройку параметров работы программного обеспечения, включая системы управления базами данных и средства электронного документооборота, формулировать правила безопасной эксплуатации
- ПК-1.3 - Владеет навыками по установке, настройке и обслуживанию программного обеспечения, программно-аппаратных и технических средств защиты информации с соблюдением требований по защите информации
- ПК-3 -Способен управлять защитой информации в автоматизированных системах
- ПК-3.1 - Знает основные методы управления защитой информации, информационные ресурсы автоматизированных систем, подлежащие защите; основные угрозы безопасности информации, модели нарушителя в автоматизированных системах
- ПК-3.2 - Умеет разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем; классифицировать и оценивать угрозы безопасности информации; оценивать информационные риски в автоматизированных системах

- ПК-3.3 - Владеет навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе

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.

Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса, контрольной работы , тестирования, промежуточная аттестация в форме зачета.

Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.

Приложение 2

УТВЕРЖДЕНО
Протокол заседания кафедры
№_____ от_____

ЛИСТ ИЗМЕНЕНИЙ

в рабочей программе дисциплины «Безопасность программного обеспечения автоматизированных систем» по направлению подготовки 10.03.01 «Информационная безопасность»

на 20__/20__ учебный год

1. В _____ вносятся следующие изменения:
(элемент рабочей программы)
1.1. ……..;
1.2. ……...;
…
1.9. …… .

2. В _____ вносятся следующие изменения:
(элемент рабочей программы)
2.1. ……..;
2.2. ……...;
…
2.9. …… .

3. В _____ вносятся следующие изменения:
(элемент рабочей программы)
3.1. ……..;
3.2. ……...;
…
3.9. …… .

Составитель *подпись* *расшифровка подписи*

дата