Аннотация к рабочей программе дисциплины «Программно-аппаратные средства защиты информации»

Цель преподавания дисциплины

Целью преподавания дисциплины «Программно-аппаратные средства защиты информации» является ознакомление студентов с современными средствами защиты информации в компьютерных системах, овладение методами решения профессиональных задач по защите информации.

Задачи изучения дисциплины

В результате изучения дисциплины студенты должны:

– получить знания о назначении, принципах функционирования и структуре программных, программно-аппаратных и аппаратных систем защиты информации;

– получить знания о функционировании подсистем управления системами защиты информации;

– получить знания о методах идентификации пользователей в компьютерных системах;

– изучить используемые в системах защиты информации технологии аутентификации;

– получить представление об особенностях встраивания в компьютерные системы средств криптографической защиты информации;

– изучить методы защиты программного обеспечения от несанкционированного копирования, изучения и отладки;

– получить сведения о деструктивных программных воздействиях и методах и средствах противодействия им;

– изучить альтернативные традиционным архитектуры защищённых компьютерных систем.

Компетенции, формируемые в результате освоения дисциплины

Способен определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7);

Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);

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

Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9);

Способень участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности (ПСК-4.4).

Разделы дисциплины

Введение. Доступ к данным. идентификация и аутентификация субъектов доступа. Аппаратная идентификация пользователей. Технологии аутентификации. Системы аппаратной поддержки механизмов разграничения доступа. Принципы организации контроллера защиты информации. Аппаратные системы разграничения доступа. Программно – аппаратные криптосистемы. Технологии шифрования. Защита программ от несанкционированного копирования. Защита программ от изучения. Деструктивные программные воздействия. Кейлоггеры.

МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Декан факультета
фундаментальной и прикладной
(наименование ф-та полностью)
информатики

Т.А. Ширабакина
(подпись, инициалы, фамилия)
«1» февраля 20 17 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Программно-аппаратные средства защиты информации

направление подготовки (специальность) *10.03.01*
(шифр согласно ФГОС
Информационная безопасность
и наименование направление подготовки (специальности)

Безопасность автоматизированных систем
наименование профиля, специализации или магистерской программы

форма обучения *очная*
очная, очно-заочная, заочная

Курск – 2017

2

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования направления подготовки 10.03.01 Информационная безопасность и на основании учебного плана направления подготовки 10.03.01 Информационная безопасность, одобренного Учёным советом университета, протокол № 5 «30» января 2017г.

Рабочая программа обсуждена и рекомендована к применению в учебном процессе для обучения студентов по направлению подготовки 10.03.01 Информационная безопасность на заседании кафедры информационной безопасности № 9 «1» февраля 2017г.

Зав. кафедрой ИБ Таныгин М.О.
Разработчик программы
Доцент кафедры ИБ Таныгин М.О.

Согласовано:

Директор научной библиотеки Макаровская В.Г.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 Информационная безопасность, одобренного Ученым советом университета протокол № 5 «30» января 2017г. на заседании кафедры информационной безопасности 28.08.2017, №1
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ к.т.н., доцент Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 Информационная безопасность, одобренного Ученым советом университета протокол № 9 «26» марта 2018г. на заседании кафедры информационной безопасности 29.06.2018, №12
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ к.т.н., доцент Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 Информационная безопасность, одобренного Ученым советом университета протокол № «» 20 г. на заседании кафедры информационной безопасности 27.06.2019, №11
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ к.т.н., доцент Таныгин М.О.

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол №1 от «31» 08 2020г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол №11 от «28» 06 2021 г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол №11 от «30» 06 2022 г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол №1 от «30» 08 2023 г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №__ «___» _____ 20__ г. на заседании кафедры информационной безопасности. Протокол №__ от «__»_____20__г.

Зав. кафедрой _____

1. Цель и задачи дисциплины. Перечень планируемых результатов обучения, соотнесённых с планируемыми результатами освоения образовательной программы

1.1. Цель преподавания дисциплины

Целью преподавания дисциплины «Программно-аппаратные средства защиты информации» является ознакомление студентов с современными средствами защиты информации в компьютерных системах, овладение методами решения профессиональных задач по защите информации.

1.2. Задачи изучения дисциплины

В результате изучения дисциплины студенты должны:

- получить знания о назначении, принципах функционирования и структуре программных, программно-аппаратных и аппаратных систем защиты информации;
- получить знания о функционировании подсистем управления системами защиты информации;
- получить знания о методах идентификации пользователей в компьютерных системах;
- изучить используемые в системах защиты информации технологии аутентификации
- получить представление об особенностях встраивания в компьютерные системы средств криптографической защиты информации;
- изучить методы защиты программного обеспечения от несанкционированного копирования, изучения и отладки
- получить сведения о деструктивных программных воздействиях и методах и средствах противодействия им
- изучить альтернативные традиционным архитектуры защищённых компьютерных систем.

1.3. Перечень планируемых результатов обучения, соотнесённых с планируемыми результатами освоения образовательной программы

Обучающиеся должны **знать:**

- номенклатуру современных программно-аппаратных средств защиты информации;
- назначение, организацию и принципы функционировании программно-аппаратных средств защиты информации;
- механизмы защиты объектов, реализованные программно-аппаратных средств защиты информации

уметь:

- администрировать современные программно-аппаратные системы защиты информации

– устанавливать и настраивать операционные системы и их подсистемы обеспечения информационной безопасности;

– уметь сопоставлять структурную и функциональную организацию программных и аппаратных средств защиты информации требованиям политики безопасности

владеть:

– навыками реализации требуемых политик безопасности с помощью современных программно-аппаратных средств защиты информации

– проведения проверок работоспособности и эффективности применения программно-аппаратных средств защиты информации

Процесс изучения дисциплины направлен на формирование следующих компетенций*:*

– способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)

– способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);

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

– способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9)

– способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности (ПСК-4.4).

2. Указание места дисциплины в структуре образовательной программы

Дисциплина относится к базовой части теоретического курса (Б1.Б.15). Изучается на 4 курсе в 8 семестре

3. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоёмкость (объём) дисциплины составляет 5 зачётных единиц, 180 часов

Таблица 3.1 – Объём дисциплины по видам учебных занятий

Общая трудоемкость дисциплины	180
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	72,15
лекции	36
лабораторные занятия	36
практические занятия	
экзамен	0,15
зачет	
курсовая работа (проект)	
расчетно-графическая (контрольная) работа	
Аудиторная работа (всего):	72
в том числе:	
лекции	36
лабораторные занятия	36
практические занятия	
Самостоятельная работа обучающихся (всего)	71,85
Контроль/экз (подготовка к экзамену)	36

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Содержание дисциплины

Таблица 4.1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1.	Введение.	Цели и задачи программно–аппаратной защиты информации
2.	Доступ к данным. идентификация и аутентификация субъектов доступа.	Идентификация и аутентификация субъектов доступа. Разграничение доступа к устройствам. Замкнутая программная среда. Вопросы корректности идентификации объекта доступа.
3.	Аппаратная идентификация пользователей.	Основные виды аппаратной идентификации.Электронные устройства ввода идентификационных признаков. Биометрическая идентификация пользователей.
4.	Технологии аутентификации.	Протоколы аутентификации.
5.	Системы аппаратной поддержки механизмов разграничения доступа.	Организация, функции, компоненты, защитные механизмы
6.	Принципы организации контроллера защиты информации.	Реализация средства аппаратной поддержки. Основные функции аппаратного контроллера.
7.	Аппаратные системы	Использование архитектур, отличных от фоннеймановской.

	разграничения доступа.	Системы перлюстрации запросов на обращения к данным. Защита от считывания со сменных носителей.
8.	Программно – аппаратные криптосистемы. Технологии шифрования.	Пригодность различных подходов к шифрованию данных. Общие сведения об аппаратных криптосистемах. Механизмы аппаратной шифрации. Криптографический контроль целостности. Варианты реализации криптосистем. Сравнение аппаратных и программных шифраторов.
9.	Защита программ от несанкционированного копирования	Защита программ от несанкционированного копирования
10.	Защита программ от изучения.	Цели, методы и средства изучения программ. Защита программ от дизассемблирования. Борьба с трассировкой программы пошаговыми отладчиками. Ошибки в созданных и предлагаемых защитах от копирования.
11.	Деструктивные программные воздействия.	Компьютерные вирусы. Шпионские программы. Методы противодействия.
12.	Кейлоггеры.	Программные кейлоггеры. Принципы построения и работы программных кейлоггеров, варианты реализации. Аппаратные кейлоггеры. Устройство, назначение, меры борьбы.

Таблица 4.2 –Содержание дисциплины и её методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек., час	№ лб.	№ пр.			
1	2	3	4	5	6	7	8
1.	Введение.	3			У-1 МО-7	С	ПК-9, ПСК-4.4
2.	Доступ к данным. идентификация и аутентификация субъектов доступа.	3	1		У-1-3, 6, МО-1,7	С,Т	ПК-1, ПК-6
3.	Аппаратная идентификация пользователей.	3	2		У-1,4-6 МО-1,7	С	ПК-1, ПСК-4.4
4.	Технологии аутентификации.	3	3		У-2,8 МО-2,7	С	ОПК-7, ПСК-4.4
5.	Системы аппаратной поддержки механизмов разграничения доступа.	3			У-1,9-12 МО-7	С	ПК-9, ПСК-4.4
6.	Принципы организации контроллера защиты информации.	3	4		У-1,4-6 МО-3,7	С	ПК-1, ПСК-4.4

1	2	3	4	5	6	7	8
7.	Аппаратные системы разграничения доступа.	3			У-1,8-10	С, Т	ПК-1, ПК-6, ПСК-4.4
8.	Программно – аппаратные криптосистемы. Технологии шифрования.	3	5		У-1,4-6 МО-4,7	С	ПК-1, ПК-6
9.	Защита программ от несанкционированного копирования	3	6		У-1,4-6 МО-5,7	С	ПК-9, ПСК-4.4
10.	Защита программ от изучения.	3	7		У-2,9-13 МО-6,7	С	ОПК-7, ПСК-4.4
11.	Деструктивные программные воздействия.	3			У-3,12, МО-7	С,Т	ПК-9, ПСК-4.4
12.	Кейлоггеры.	3			У-3,12 МО-7	С	ПК-9, ПСК-4.4

С – собеседование, Т – тест

4.2. Лабораторные работы и практические занятия

4.2.1. Лабораторные работы

Таблица 4.3 – Лабораторные работы

№	Наименование лабораторной работы	Объем, час.
1.	Администрирование клиентской части СЗИ SecretNet (сетевой вариант)	4
2.	Администрирование серверной части СЗИ SecretNet (сетевой вариант)	6
3.	Администрирование СЗИ DallasLock 8.0	4
4.	Администрирование СЗИ Accord	6
5.	Администрирование СЗИ SecretNet (автономный вариант)	6
6.	Определение характеристик ЭВМ и привязка программного обеспечения к оборудованию	4
7.	Изучение и отладка приложений win32 и способы изменения хода их выполнения с помощью отладчика уровня пользователя	6
Итого		36

4.3. Самостоятельная работа студентов (СРС)

Таблица 4.4 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1.	Введение.	1-2 недели	4
2.	Доступ к данным. идентификация и аутентификация субъектов доступа.	2-3 недели	5
3.	Аппаратная идентификация пользователей.	3-4 недели	6
4.	Технологии аутентификации.	5-6	8

		недели	
5.	Системы аппаратной поддержки механизмов разграничения доступа.	6-8 недели	10
6.	Принципы организации контроллера защиты информации.	8-9 недели	5
7.	Аппаратные системы разграничения доступа.	9-10 недели	8
8.	Программно – аппаратные криптосистемы. Технологии шифрования.	11-12 недели	5
9.	Защита программ от несанкционированного копирования	12-14 недели	5
10.	Защита программ от изучения.	14-15 недели	6
11.	Деструктивные программные воздействия.	15-16 недели	5
12.	Кейлоггеры.	16-18 недели	5
Итого			72

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

– библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с данной РПД;

– имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

– путем обеспечения доступности всего необходимого учебно-методического и справочного материала;

– путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

– путем разработки вопросов к экзамену, методических указаний к выполнению лабораторных и практических работ.

типографией университета:

– путем помощи авторам в подготовке и издании научной, учебной, учебно-методической литературы;

– путем удовлетворения потребностей в тиражировании научной, учебной, учебно-методической литературы.

6. Образовательные технологии

В соответствии с требованиями ФГОС и Приказа Министерства образования и науки РФ от 05 апреля 2017 г. №301 реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов. Удельный вес занятий, проводимых в интерактивных формах, составляет 24.8% от аудиторных занятий согласно УП. Средствами промежуточного контроля успеваемости студентов являются защита лабораторных работ, опросы на практических занятиях по темам лекций.

Таблица 6.1 – Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела	Используемые интерактивные образовательные технологии	Объём, час.
1.	Выполнение работы №1 «Администрирование клиентской части СЗИ SecretNet (сетевой вариант)»	Выполнение студентом интерактивных заданий по реализации требуемых политик безопасности	6
2.	Выполнение лабораторной работы №3 «Администрирование СЗИ Accord»	Выполнение студентом интерактивных заданий по реализации требуемых политик безопасности	6
3.	Выполнение работы №5 «Определение характеристик ЭВМ и привязка программного обеспечения к оборудованию»	Выполнение студентом интерактивных заданий по определению основных характеристик ЭВМ с возможностью выбора студентом способа получения сведений и способа привязки программного обеспечения	6
4.	Защита работы №6 «Изучение и отладка приложений win32 и способы изменения хода их выполнения с помощью отладчика уровня пользователя»	Выполнение реальной задачи, связанной с изучением исполняемого кода программы со встроенными механизмами защиты от несанкционированного копирования	6
	Итого		24

7. Фонд оценочных средств для проведения промежуточной аттестации

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Таблица 7.1 – Этапы формирования компетенций

Код и содержание компетенции	Этапы формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
- способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)	Информационные технологии Практика по получению первичных профессиональных умений и навыков	Основы управления информационной безопасностью Безопасность операционных систем Безопасность сетей ЭВМ Технические средства охраны Системы контроля доступа и видеонаблюдения	Программно-аппаратные средства защиты информации Техническая защита информации Сети и системы передачи информации Администрирование вычислительных сетей Защита информационных процессов в компьютерных системах Преддипломная практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)	Ознакомительная практика	Введение в криптографию; Аппаратные средства вычислительной техники; Криптографические методы защиты информации; Безопасность сетей ЭВМ; Технические средства охраны;	Программно-аппаратные средства защиты информации; Инженерно-техническая защита информации; Эксплуатационная практика; Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру

		Системы контроля доступа и видеонаблюдения; Технологическая практика	защиты
способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6)		Методы защиты программного обеспечения; Основы риверсинжиниринга программных средств	Программно-аппаратные средства защиты информации; Техническая защита информации; Защита информационных процессов в компьютерных системах; Эксплуатационная практика; Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9)	Русский язык и культура речи; Ознакомительная практика	Программно-аппаратные средства защиты информации; Учебно-исследовательская работа студентов	Инженерно-техническая защита информации; Преддипломная практика; Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением		Аппаратные средства вычислительной техники;	Программно-аппаратные средства защиты информации;

информационной безопасности (ПСК-4.4)		Организация ЭВМ и вычислительных систем; Проектно-технологическая практика	Специализированные вычислительные устройства защиты информации; Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

7.2. Описание показателей и критериев оценивания компетенций на раз- личных этапах их формирования, описание шкал оценивания

Таблица 7.2 – Критерии и шкала оценивания компетенций

Наименование компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
ОПК - 7/ *основной*	*1.Доля освоенных обучающимся знаний, умений навыков от общего объема ЗУН, установленных в п.1.ЗРПД* *2.Качество освоенных обучающи-мися знаний, умений, навыков* *3. Умение применять знания, умения, навыки в типовых и нестандартных ситуациях*	**Знать**: -основные понятия курса. **Уметь**: - применять теоретические сведения при решении типовых задач. **Владеть**: - навыками анализа структуры систем по передаче информации.	**Знать**: -основные характеристики сигналов; -основные протоколы взаимодействия компонентов операционных систем. **Уметь**: - применять знания о системах для решения задач по созданию защищенных информационных систем; **Владеть**: - навыками анализа основных характеристик операционных систем.	**Знать**: - характеристики операционных систем; - принципы построения и функционирования систем информации; - способы обработки информации в компьютерных системах; **Уметь**: - применять знания о системах электрической связи для решения типовых и нестандартных задач по созданию защищенных операционных систем; - анализировать тенденции развития

				систем обеспечения информационной безопасности. **Владеть**: - навыками анализа характеристик и возможностей операционных систем по защищённой обработке данных.
способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)	1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД 2.Качество освоенных обучающимся знаний, умений, навыков 3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях	**Знать**: понятие подсистему управления ИБ, основные её функции **Уметь**: выполнять сервисные мероприятия с системами программно-аппаратной защиты информации **Владеть навыками**: эксплуатации различных компонентов подсистем обеспечения ИБ	**Знать**: принципы организации подситем безопасности предприятий **Уметь**: настраивать программно-аппаратные системы защиты информации **Владеть навыками**: администрирования программно-аппаратных СЗИ	**Знать**: критерии соответствия функционала подсистем информационной безопасности угрозам для объектов информатизации **Уметь**: выбирать требуемы политики безопасности при настройке программно-аппаратных СЗИ **Владеть навыками**: реагировании на нештатные ситуации, возникающие при эксплуатации программно-аппаратных СЗИ
способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности	1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД 2.Качество освоенных обучающимся знаний, умений, навыков	**Знать**: принципы организации проверок программно-аппаратных СЗИ **Уметь**: анализировать нормативную документацию для проведения проверок программно-аппартаных СЗИ **Владеть**	**Знать**: инструментальные средства проведения проверок программно-аппаратных СЗИ **Уметь**: выполнять декомпозицию кода программных СЗИ **Владеть навыками**:	**Знать**: основные угрозы работоспособности программно-аппаратных СЗИ **Уметь**: выявлять недекларируемые возможности техничских систем **Владеть навыками**: проведения атак на разнообразные СЗИ

применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6)	3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях	**навыками**: организации контрольных проверок программно-аппаратных СЗИ	риверс-инжиниринга программных средств	
способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9)	1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД 2.Качество освоенных обучающимся знаний, умений, навыков 3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях	**Знает**: поверхностно понятие и виды защищаемой информации. **Умеет**: в недостаточной мере применять информационно-коммуникационные технологии. Владеет: слабо владеет навыками решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры. .	**Знает**: Углубленно, но с некоторыми пробелами в отдельных областях, особенности конфиденциальной информации и интеллектуальной собственности как вида защищаемой информации. **Умеет**: в достаточной мере применять на практике современные информационно-коммуникационные технологии. **Владеет**: навыками решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с обоснованием своей точки зрения и	**Знает**: Углубленно особенности конфиденциальной информации и интеллектуальной собственности как вида защищаемой информации, а также основные требования информационной безопасности. **Умеет**: успешно применять на практике современные информационно-коммуникационные технологии. **Владеет**: развитыми навыками решения в том числе и нестандартных задач профессиональной деятельности на основе информационной и библиографической культуры с обоснованием своей точки зрения и аргументированных выступлений по профессиональной тематике.

			аргументированных выступлений по профессиональной тематике.	
способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности (ПСК-4.4)	1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД 2.Качество освоенных обучающимся знаний, умений, навыков 3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях	**Знать**: принципы проектирования программно-аппаратных СЗИ **Уметь**: интегрировать функциональные узлы в единую СЗИ **Владеть навыками**: организации межмодульного взаимодействия в СЗИ	**Знать**: инструментальные средства разработки программно-аппаратных СЗИ **Уметь**: выполнять работы по внедрению отдельных компонентов в многокомпонентную СЗИ **Владеть навыками**: проведения анализа технических требований к отдельным модулям проектируемой СЗИ	**Знать**: принципы декомпозиции при определении функциональности блоков разрабатываемых систем **Уметь**: анализ соответствия ункциональных возможностей компонентов СЗИ и требований политики безопасности **Владеть навыками**: формулирования требований к отдельным модулям проектируемой СЗИ

7.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля

п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1.	Введение.	ПК-9, ПСК-4.4	Лекция, СРС	собеседование	1-15	Согласно табл.7.2
2.	Доступ к данным.	ПК-1, ПК-6	Лекция, СРС	Собеседование	1-15	Согласно табл.7.2

	идентификация и аутентификация субъектов доступа.			контрольные вопросы к ЛР№1	1-5	
3.	Аппаратная идентификация пользователей.	ПК-1, ПСК-4.4	Лекция, СРС, лабораторная работа	собеседование		Согласно табл.7.2
				контрольные вопросы к ЛР№2	1-7	
				тестирование		
4.	Технологии аутентификации.	ОПК-7, ПСК-4.4	Лекция, СРС	собеседование		Согласно табл.7.2
				контрольные вопросы к ЛР№3		
5.	Системы аппаратной поддержки механизмов разграничения доступа.	ПК-9, ПСК-4.4	Лекция, СРС	собеседование		Согласно табл.7.2
6.	Принципы организации контроллера защиты информации.	ПК-1, ПСК-4.4	Лекция, СРС, лабораторная работа	собеседование		Согласно табл.7.2
				контрольные вопросы к ЛР№4	1-5	
7.	Аппаратные системы разграничения доступа.	ПК-1, ПК-6, ПСК-4.4	Лекция, СРС			Согласно табл.7.2
8.	Программно – аппаратные криптосистемы. Технологии шифрования. .	ПК-1, ПК-6 ПК-1, ПСК-4.4	Лекция, СРС, лабораторная работа	собеседование		Согласно табл.7.2
				контрольные вопросы к ЛР№4	1-7	
9.	Защита программ от несанкционир	ОПК-7, ПСК-4.4	Лекция, СРС, лабораторная работа	собеседование		Согласно табл.7.2

	ованного копирования			контрольные вопросы к ЛР№6	1-58	
10.	Защита программ от изучения.	ПК-9, ПСК-4.4	Лекция, СРС, лабораторная работа	собеседование		Согласно табл.7.2
				контрольные вопросы к ЛР№7	1-5	
11.	Деструктивные программные воздействия.	ПК-9, ПСК-4.4	Лекция, СРС	собеседование		Согласно табл.7.2
				Тестирование	-5	
12.	Кейлоггеры.	ПК-9, ПСК-4.4	Лекция, СРС	собеседование		Согласно табл.7.2

7.4. Рейтинговый контроль изучения учебной дисциплины

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

– Положение П 02.016–2015 «О балльно-рейтинговой системе оценки качества освоения образовательных программ»;

– методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля* по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
Выполнение лабораторной работы №1 «Администрирование клиентской части СЗИ SecretNet (сетевой вариант)»	3	Выполнил, но «не защитил»	6	Выполнил и «защитил»

Выполнение лабораторной работы №2 «Администрирование серверной части СЗИ SecretNet (сетевой вариант)»	3	Выполнил, но «не защитил»	6	Выполнил и «защитил»
Выполнение лабораторной работы №3 «Администрирование СЗИ Accord»	3	Выполнил, но «не защитил»	6	Выполнил и «защитил»
Выполнение лабораторной работы №4 «Администрирование СЗИ SecretNet (автономный вариант)»	3	Выполнил, но «не защитил»	6	Выполнил и «защитил»
Выполнение работы №5 «Определение характеристик ЭВМ и привязка программного обеспечения к оборудованию»	3	Выполнил, но «не защитил»	6	Выполнил и «защитил»
Защита работы №6 «Изучение и отладка приложений win32 и способы изменения хода их выполнения с помощью отладчика уровня пользователя»	3	Выполнил, но «не защитил»	6	Выполнил и «защитил»
СРС	6		12	
ИТОГО	24		48	
Посещаемость	0		16	
Экзамен	0		36	
ИТОГО	24		100	

При итоговом контроле (экзамен) в форме бланкового теста студенту предлагается 15 вопросов по различным темам курса. Полученную итоговую сумму условных баллов (максимум 15) переводят в баллы на экзамене (максимум 36) путём умножения на 2.4 и округления до целого значения.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1. Основная **литература**

1) Программно-аппаратные системы защиты информации [Текст]: учебное пособие / М. О. Таныгин ; Министерство образования и науки Российской Федерации, Юго-Западный государственный университет. - Курск : ЮЗГУ, 2012. - 147 с. : ил.табл..

2) Программно-аппаратные средства защиты информационных систем [Текст] : учебное пособие / И. В. Калуцкий, А. Г. Спеваков ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2014. - 179, [2] с.

3) Технические средства и методы защиты информации [Текст] : учебное пособие / под ред. А. П. Зайцева и А. А. Шелупанова. - М. : Горячая линия - Телеком, 2012. - 616 с.

8.2. Дополнительная литература

1) Информационная безопасность : учебник. [Текст] / Ярочкин В. И. - М.: Академический проект, 2008. - 544 с // http://biblioclub.ru / index.php?page = book&id=211164&sr=1

2) Правовое обеспечение информационной безопасности [Текст] : учебное пособие / под ред. С. Я. Казанцева. - 3-е изд., стер. - М.: Академия, 2008. - 240 с.

3) Стандарты информационной безопасности : Курс лекций [Текст] / под ред. В. Б. Бетелина. - М. : ИНТУИТ. РУ Интернет-университет Информационных Технологий, 2004.

4) Архитектура компьютера [Текст] / Э. Таненбаум - 4-е изд. - СПб. : Питер, 2003. - 704 с.

5) Комплексная защита информации в компьютерных системах [Текст]: учеб. Пособие для студентов вузов / В.И. Завгородний - М.: Логос, 2001.

6) Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах [Текст]: Учебное пособие для студ. вуз. / В. Г. Проскурин, С. В. Крутов, И. В. Мацкевич. - М. : Радио и связь, 2000. - 168 с. : ил.

7) Зегжда Д. П. Способы безопасности информационных систем : Учеб. пособие для студ. вуз. / А. М. Ивашко. - М. : Горячая линия - Телеком, 2000. - 452 с. : ил

8) Разрушающие программные воздействия. / А.В. Щербаков - М.: Эдэль, 1993.

9) Комплексная защита информации в компьютерных системах [Текст] : Учеб. пособие для студ. вуз. / Завгородний В. И. – 2001

8.3. Перечень методических указаний

1) Установка и настройка SECRETNET в сетевом режиме функционирования: методические указания по выполнению лабораторной работы / А.Г. Спеваков Курск: Юго–Зап. Гос. Ун-т, 2013. 51 с.

2) Администрирование клиентской и серверной части СЗИ DallasLock :методические указания к лабораторной работе по дисциплине «Программно-аппаратные средства защиты информации» (учебно-методическая разработка) / М.О. Таныгин - Курск: Юго–Зап. Гос. Ун-т, 2017. 10 с.

3) Администрирование СЗИ Accord:методические указания к лабораторной работе по дисциплине «Программно-аппаратные средства защиты информации» (учебно-методическая разработка) / М.О. Таныгин - Курск: Юго–Зап. Гос. Ун-т, 2017. 18 с.

4) Администрирование СЗИ SecretNet (автономный вариант): методические указания по выполнению лабораторной работы по дисциплине «Программно-аппаратные средства защиты информации» (учебно-методическая разработка) / М.О. Таныгин – Курск: Юго–Зап. Гос. Ун-т, 2017. 33 с.

5) Определение характеристик ЭВМ и привязка программного обеспечения к оборудованию : методические указания к лабораторной работе по дисциплине «Программно-аппаратные средства защиты информации» (учебно-методическая разработка) / М.О. Таныгин - Курск: Юго–Зап. Гос. Ун-т, 2017. Ун-т. 2018. 9 с.

6) Изучение и отладка приложений win32 и способы изменения хода их выполнения с помощью отладчика уровня пользователя : методические указания по выполнению лабораторной работы по дисциплине «Программно-аппаратные средства защиты информации» (учебно-методическая разработка) / М.О. Таныгин – Курск: Юго–Зап. Гос. Ун-т, 2017. 23 с.

7) Программно-аппаратные системы защиты информации: методические указания для самостоятельной работы (учебно-методическая разработка) / М.О. Таныгин – Курск: Юго–Зап. Гос. Ун-т, 2018. 11 с.

9. Перечень ресурсов информационно-телекоммуникационной сети Интернет

1) Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/
2) Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/
3) Сообщество Ubuntu [официальный сайт]. Режим доступа: http://ubuntu.com/
4) Корпорация Microsoft [официальный сайт]. Режим доступа: http://microsoft.com/
5) Электронно-библиотечная система «Университетская библиотека онлайн» Режим доступа: http://biblioclub.ru
6) Компания «Консультант Плюс» [официальный сайт]. Режим доступа: http://www.consultant.ru
7) Научно-информационный портал ВИНИТИ РАН [официальный сайт]. Режим доступа: http://www.consultant.ru/
8) База данных "Патенты России"

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Программно-аппаратные средства защиты информации» являются лекции и лабораторные занятия. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают лабораторные и практические занятия, которые обеспечивают: контроль подготовленности студента; за- крепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Лабораторному занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по лабораторным и практическим работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Программно-аппаратные системы защиты информации»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекции, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы и справочной документации составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепление освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Безопасность операционных систем» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Программно-аппаратные системы защиты информации» - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал», Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,Windows 7, договор IT000012385, Oracle Virtualbox (Бесплатная, GNU General Public License), редактор двоичных файлов Free Hex Editor Neo, (Свободное ПО http://www.hhdsoftware.com/free-hex-editor), открытая среда разработки программного обеспечения Lazarus (Свободное ПО http://www.lazarus.freepascal.org/) , отладчик уровня пользователя OllyDebugger (Свободное ПО http://www.ollydbg.de/) СЗИ DallasLock 8.0. (Лицензия 18815-4310-375) СЗИ SecretNet 7.0.Клиент (Лицензия TA25-00BL-BUH-00AC-00UJ-00L2-000D) СЗИ SecretNet 7.0.Клиент (Лицензия TA25-00BL-BUH2-00AC-00UJ-00L2-000D) СЗИ SecretNet 7.0.Сервер безопасности (Лицензия TA2S-0AMV-B66C-00AD-00PM-00L2-000Z)

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Учебная аудитория для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Компьютеры (10 шт) CPU AMD-Phenom, ОЗУ 16 GB, HDD 2 Tb, монитор Aok 21”. Проекционный экран на штативе; Мультимедиацентр: ноут- букASUSX50VLPMD-T2330/14"/1024Mb/160Gb/сумка/ проектор inFocusIN24+

СЗИ SecretNet 5.0 (PCI-card). СЗИ Accord NT,