ОБРАЗОВАТЕЛЬНОЕ ЧАСТНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
ПРАВОСЛАВНЫЙ СВЯТО-ТИХОНОВСКИЙ ГУМАНИТАРНЫЙ УНИВЕРСИТЕТ
(ПСТГУ)

Факультет информатики и прикладной математики
Кафедра информатики

УТВЕРЖДАЮ

Проректор по учебной работе

_____ / Тарасова И.В. /

«_02_» _____января_____ 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы защиты информации и безопасности данных»

02.03.03 Математическое обеспечение и администрирование информационных систем

Профиль подготовки:
Администрирование информационных систем

Квалификация выпускника: бакалавр

Форма обучения: очная

Москва, 2021 г.

Год начала обучения по учебному плану: 2019

1. Цели освоения дисциплины

Целью изучения дисциплины является изучение основ защиты информации и безопасности данных.

Задачами изучения дисциплины являются знакомство с теоретическими основами защиты информации, знакомство с организационно-правовыми нормами обеспечения информационной безопасности, закрепление навыков обеспечения безопасности информационных систем на основе разработанных программ и методик.

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к блоку Б1.О.18 обязательной части образовательной программы.

Дисциплина изучается на 3 курсе, в 6 семестре.

Дисциплина призвана создать базу для формирования у студентов навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения дисциплины обучающийся должен продемонстрировать следующие результаты:

Коды компетенций	Наименование компетенции	Перечень планируемых результатов обучения по дисциплине
ОПК-2	Способен применять современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности	В результате освоения дисциплины обучающийся должен **ЗНАТЬ:** 1. современную постановку защиты информации 2. виды информационного оружия **3.** возможные угрозы информационным системам **УМЕТЬ:** 1. распознавать и предотвращать проникновение информационных инфекций **2.** использовать правовые акты для решения задач обеспечение информационной безопасности: разрабатывать и подготавливать к утверждению проекты нормативных и методических материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов **ВЛАДЕТЬ:** Навыком выполнения работ, связанных с обеспечением комплексной защиты информации

		на основе разработанных программ и методик.
ОПК-5	Способен инсталлировать и сопровождать программное обеспечение для информационных систем и баз данных, в том числе отечественного производства	В результате освоения дисциплины обучающийся должен **ЗНАТЬ:** 1. организационно-правовое обеспечение информационной безопасности **2.** классы безопасности компьютерных систем **УМЕТЬ:** **1.** эффективно использовать средства автоматического контроля, обнаружения возможных каналов утечки сведений, представляющих государственную, военную, служебную и коммерческую тайну **ВЛАДЕТЬ:** Навыком выполнения работ, связанных с обеспечением комплексной защиты информации на основе разработанных программ и методик.
ПК-3	Способен решать задачи в области развития науки, техники и технологии с учетом нормативного правового регулирования в сфере интеллектуальной собственности	В результате освоения дисциплины обучающийся должен **ЗНАТЬ:** **1.** организационно-правовое обеспечение информационной безопасности **УМЕТЬ:** 1. использовать правовые акты для решения задач обеспечение информационной безопасности: разрабатывать и подготавливать к утверждению проекты нормативных и методических материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов **ВЛАДЕТЬ:** Правовыми актами, связанными с решением задач обеспечения информационной безопасности информационной системы.

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

Общая трудоемкость (объем) дисциплины составляет 4 зачетные единицы, 144 академических часов.

На учебные занятия лекционного типа отводится 18 часов,

на занятия практического (семинарского) типа — 54 часов.

Самостоятельная работа составляет 45 часов.

Контроль – 27 часов.

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

5.1. Тематические разделы дисциплины и компетенции, которые формируются при их изучении

№ п/п	Наименование раздела дисциплины	Содержание раздела	Код формируемой компетенции
1.	Понятие национальной безопасности. Информационная безопасность РФ. Терминологические основы информационной безопасности: основные понятия и определения. Угрозы информационной безопасности. Критерии классификации угроз.	Цели и направления защиты. Виды безопасности. Национальные интересы в информационной сфере. Основные понятия и принципы обеспечения информационной безопасности. Информация, как наиболее ценный ресурс современного общества. Проблемы информационной войны. Современная постановка задачи защиты информации. Основные требования к системе защиты информации. Концептуальные модели обеспечения безопасности личности, продукции, информации. Виды угроз и их классификация.	ОПК-2; ОПК-5; ПК-3
2.	Законодательный уровень информационной безопасности	Правовые аспекты общего назначения, затрагивающие вопросы информационной безопасности в Конституции РФ, Гражданском и Уголовном кодексах. Закон «Об информации, информационных технологиях и о защите информации», Законы о защите персональных данных, об электронной цифровой подписи Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента Российской Федерации от 05.12.2016 №646).	ОПК-2; ОПК-5; ПК-3
3.	Уровни политики безопасности. Стандарты построения защищенных информационных систем.	Требования к безопасности информационных систем в США, ЕС и РФ. Стандарт Министерства обороны США "Критерии оценки доверенных компьютерных систем" («Оранжевая книга»). Рекомендации X.800. Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий". Гармонизированные критерии ЕС. Руководящие документы Гостехкомиссии и ФСТЭК России.	ОПК-2; ОПК-5; ПК-3
4.	Организационный уровень информационной безопасности. Основные	Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима	ОПК-2; ОПК-5; ПК-3

	классы мер процедурного уровня. Управление рисками.	безопасности. Планирование восстановительных работ. Подготовительные и основные этапы управления рисками.	
5.	Виды уязвимостей информации и борьба с ними. Идентификация и аутентификация. Протоколирование и аудит.	Методы и модели оценки уязвимости информации. Рекомендации по использованию моделей. Требования к защите информации.	ОПК-2; ОПК-5; ПК-3
6.	Межсетевые экраны. Архитектурные аспекты. Системы обнаружения вторжений (IDS).	Принцип эшелонированной обороны. Демилитаризованные зоны. Классификация межсетевых экранов. Доступность и основные меры её обеспечения. Классификация IDS.	ОПК-2; ОПК-5; ПК-3
7.	Функции и задачи защиты информации. Основные этапы проектирования защищенной информационной системы.	Особенности современных информационных систем, существенные с точки зрения безопасности. Архитектурная безопасность. Принципы обеспечения архитектурной безопасности.	ОПК-2; ОПК-5; ПК-3

5.2. Разделы дисциплины, виды учебных занятий и формы текущего контроля успеваемости

№ семестра	**Наименование раздела дисциплины (модуля)**	**Трудоемкость в часах**					**Формы СРС**	**Формы текущего контроля**	**Формы текущего контроля с указанием баллов (при использовании балльной системы оценивания)**
		Всего (вкл. СРС)	На контактную работу по видам учебных занятий		На СРС	Контроль			
			Л	ПЗ					
1.	Понятие национальной безопасности. Информационная безопасность РФ. Терминологические основы информационной безопасности: основные понятия и определения. Угрозы информационной безопасности. Критерии классификации угроз.	14	3	6	5				
2.	Законодательный уровень	13	3	6	4				

	информационной безопасности								
3.	Уровни политики безопасности. Стандарты построения защищенных информационных систем.	19	2	7	10			Коллок.	10
4.	Организационный уровень информационной безопасности. Основные классы мер процедурного уровня. Управление рисками.	17	3	10	4				
5.	Виды уязвимостей информация и борьба с ними. Идентификация и аутентификация. Протоколирование и аудит.	22	2	10	10			Коллок.	10
6.	Межсетевые экраны. Архитектурные аспекты. Системы обнаружения вторжений.	13	2	7	4				
7.	Функции и задачи защиты информации. Основные этапы проектирования защищенной информационной системы.	19	3	8	8			ДЗ	50
8.	Экзамен	27				27		Экзамен	30
	ИТОГО:	144	18	54	45	27			100

Виды учебных занятий указаны в сокращенном виде: Л — лекция, ПЗ — практическое занятие (семинар), СРС — самостоятельная работа, Коллоквиумы – Коллок.

6. Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине

Планируются следующие виды самостоятельной работы обучающихся: подготовка к устным опросам (коллоквиумам), проработка лекций, выполнение комплексного индивидуального домашнего задания.

Студентам выдается: программа курса (примерный список вопросов к зачету), список тем для обсуждения на коллоквиумах, темы индивидуальных комплексных домашних заданий.

7. Проведение промежуточной аттестации обучающихся по дисциплине

7.1. Общие условия

Промежуточная аттестация по дисциплине – экзамен, проводится на основании результатов текущего контроля и результата, полученного на экзамене. Экзамен проводится в форме устного опроса.

Дисциплина оценивается по 100-балльной системе. Максимальное количество баллов, которое студент может набрать за один семестр – 70. Максимальное количество баллов, которое студент может набрать за ответ на экзамене – 30.

7.2. Критерии и шкалы оценивания результатов обучения по дисциплине

Код компетенции	Показатели достижения результатов обучения	Критерии и шкала оценивания			Перечень оценочных средств
		удовлетворительно	хорошо	Отлично	
ОПК-2	В результате освоения дисциплины обучающийся должен **ЗНАТЬ:** 4. современную постановку защиты информации 5. виды информационного оружия **6.** возможные угрозы информационным системам **УМЕТЬ:** 3. распознавать и предотвращать проникновение информационных инфекций **4.** использовать правовые акты для решения задач обеспечение информационной безопасности: разрабатывать и подготавливать к утверждению проекты нормативных и методических материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов **ВЛАДЕТЬ:** Навыком выполнения работ, связанных с обеспечением комплексной защиты информации на основе разработанных программ и методик.	Удовлетворительное владение основными понятиями Умение применять знания в стандартной ситуации	хорошее владение основными понятиями Умение применять знания в сложной стандартной ситуации	свободное владение основными понятиями Умение применять знания в сложной нестандартной ситуации	Экзамен

ОПК-5	В результате освоения дисциплины обучающийся должен **ЗНАТЬ:** 3. организационно-правовое обеспечение информационной безопасности **4.** классы безопасности компьютерных систем **УМЕТЬ:** **2.** эффективно использовать средства автоматического контроля, обнаружения возможных каналов утечки сведений, представляющих государственную, военную, служебную и коммерческую тайну **ВЛАДЕТЬ:** Навыком выполнения работ, связанных с обеспечением комплексной защиты информации на основе разработанных программ и методик.	Удовлетворительное владение основными понятиями Умение применять знания в стандартной ситуации	хорошее владение основными понятиями Умение применять знания в сложной стандартной ситуации	свободное владение основными понятиями Умение применять знания в сложной нестандартной ситуации	Экзамен
ПК-3	В результате освоения дисциплины обучающийся должен **ЗНАТЬ:** **2.** организационно-правовое обеспечение информационной безопасности **УМЕТЬ:** 2. использовать правовые акты для решения задач обеспечение информационной безопасности: разрабатывать и подготавливать к утверждению проекты нормативных и методических материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов **ВЛАДЕТЬ:** **Правовыми актами, связанными с решением задач обеспечения информационной безопасности информационной системы.**	Удовлетворительное владение основными понятиями Умение применять знания в стандартной ситуации	хорошее владение основными понятиями Умение применять знания в сложной стандартной ситуации	свободное владение основными понятиями Умение применять знания в сложной нестандартной ситуации	Экзамен

7.3. Оценочные средства для промежуточной аттестации

Промежуточная аттестация производится на 6 семестре.

Форма аттестации - Экзамен.

Аттестация проходит по результатам текущего контроля и по результату, полученному на экзамене в конце семестра. Экзамен проходит в форме устного опроса.

Примерный перечень вопросов к экзамену:

1. Теория защиты информации. Основные направления.
2. Обеспечение информационно безопасности. Основные направления.
3. Комплексность (целевая, инструментальная, структурная, функцио-нальная, временная)
4. Требования к системе защиты информации
5. Угрозы информации
6. Виды угроз. Основные нарушения.
7. Характер происхождения угроз.
8. Источники угроз. Предпосылки угроз.
9. Система защиты информации.
10. Классы каналов несанкционированного получения информации.
11. Причины нарушения целостности информации.
12. Методы и модели оценки уязвимости информации.
13. Общая модель воздействия на информацию.
14. Общая модель процесса нарушения физической целостности информации.
15. Структурированная схема потенциально возможных злоумышленных действий в АСОД.
16. Методологические подходы к оценке уязвимости информации.
17. Модель защиты системы с полным перекрытием.
18. Рекомендации по использованию моделей оценки уязвимости информации.
19. Допущения в моделях оценки уязвимости информации.
20. Методы определения требований к защите информации.
21. Классификация требований к средствам защиты информации.
22. Требования к защите, обусловленные спецификой АСОД.
23. Анализ существующих методик определения требований к защите информации.
24. Стандарт США «Критерии оценки гарантировано защищенных вычислительных систем в интересах Министерства обороны США». Основные положения.
25. О Руководящем документе Гостехкомиссии России «Классификация автоматизированных систем и требований к защите информации». Ч.1

7.4. Шкала перевода оценок

Итоговое оценивание сформированности компетенций производится на основании результатов текущей аттестации и результата, полученного на экзамене.

Оценка за ответ на экзамене выставляется на основе следующих критериев:

Шкала оценки		**Критерии оценки**
Оценка	**Баллы**	
5 (отлично)	27-30	Обучающийся: • полно излагает изученный материал, • дает правильное определение понятий; • обнаруживает понимание материала, • может обосновать свои суждения, • может привести необходимые примеры не только из учебных пособий, но и самостоятельно составленные; • количество небольших замечаний не более 5.
4 (хорошо)	23-26	Обучающийся: • полно излагает изученный материал, • дает правильное определение понятий; • обнаруживает понимание материала, • может обосновать свои суждения, • может привести примеры; • количество ошибок не более 5.
3 (удовлетворительно)	19-22	Обучающийся: • обнаруживает знание и понимание основных положений; • но излагает материал неполно и допускает неточности в определении понятий или формулировках; • не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; • количество серьезных ошибок не более 5.
2 (неудовлетворительно)	0	Обучающийся: • обнаруживает незнание большей части соответствующего раздела изучаемого материала, • допускает ошибки в формулировке определений, искажающие их смысл; • количество серьезных ошибок более 5.

Выставление итоговой оценки по результатам промежуточной аттестации

Форма промежуточной аттестации	Шкала оценивания		Критерии оценивания
	в оценках или баллах по 5-ти балльной шкале	в баллах по 100-балльной шкале	
Экзамен	удовлетворительно	Не менее 61	Начислено не менее 61 % максимального количества баллов(*)
Экзамен	хорошо	Не менее 74	Начислено не менее 74 % максимального количества баллов(*)
Экзамен	отлично	Не менее 91	Начислено не менее 91 % максимального количества баллов(*)

(*) максимального количества баллов, которое может быть начислено по результатам текущего контроля и за экзамен в сумме.

8. Перечень образовательных технологий

В процессе преподавания дисциплины используются следующие образовательные технологии:

1. Лекции с обсуждением проблемных мест,
2. Практические занятия с решением задач,
3. Разбор домашних заданий с элементами дискуссии и взаимопомощи обучающихся друг другу,
4. Устные опросы.

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

а) Основная литература

1. Расторгуев С.П. Основы информационной безопасности. Академия, сер. «Высшее профессиональное образование», 2009
2. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. М.: Горячая линия – Телеком, 2006

б) Дополнительная литература

1. Доктрина информационной безопасности Российской Федерации, N 646,2016, 05.12.2016
2. Гостехкомиссия России. Руководящий документ. Концепция защиты СВТ и АС от НСД к информации, Москва, 1992.
3. Федеральный Закон "Об информации, информатизации и защите информации" "Российская газета", N 165, 2006, 29 июля

4. Руководящий документ Гостехкомиссии России. Термины и определения в области защиты от НСД к информации. М.: ГТК РФ, 1992.
5. Руководящий документ Гостехкомиссии России. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. М.: ГТК РФ, 1992.
6. Руководящий документ Гостехкомиссии России. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности СВТ от НСД к информации. М.: ГТК РФ, 1992.
7. Руководящий документ Гостехкомиссии России. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. М.: ГТК РФ, 1992.

10. Перечень ресурсов информационно-телекомуникационной сети «Интернет», профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины

www.consultant.ru

11. Методические указания для обучающихся по освоению дисциплины

Студентам выдается список домашних заданий. Все домашние задания снабжены указаниями по их выполнению.

12. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

При освоении дисциплины для выполнения практических работ необходимы персональные компьютеры с выходом в Интернет.

13. Описание материально-технической базы, необходимой для осуществления Компьютерный класс, оснащенный рабочими станциями

Компьютерный класс, оснащенный компьютерами класса Pentium с выходом в Интернет, необходим персональный компьютер на каждого студента.

Разработчик программы:

профессор, к.т.н. Соловьев В.П.

Рецензент:

профессор, к.т.н. Соловьев В.П.

Программа одобрена на заседании кафедры Информатики от «28» мая 2021 года, протокол № 05-21