Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования «Новосибирский национальный исследовательский
государственный университет» (Новосибирский государственный университет, НГУ)

Факультет информационных технологий

СОГЛАСОВАНО
Декан ФИТ НГУ
_____ М.М. Лаврентьев
«03» июля 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информации

Направление подготовки: 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА
Направленность (профиль): Программная инженерия и компьютерные науки

Форма обучения: очная
Год обучения: 4, семестр: 7

№	Вид деятельности	Семестр
		7
1	Лекции, час.	32
2	Практические занятия, час.	
3	Лабораторные занятия, час.	32
4	Занятий в контактной форме без учета промежуточной аттестации, час, из них	64
5	в электронной форме, час.	
6	из них аудиторных занятий, час.	64
7	из них в активной и интерактивной форме, час.	26
8	консультаций, час.	
9	Самостоятельная работа, час.	42
10	в том числе на выполнение письменных работ, час	
11	Форма аттестации (экзамен, зачет, дифференцированный зачет), час	ДЗ, 2
12	Всего зачетных единиц[1]	3

Новосибирск 2019

1 С учетом выделенных часов на промежуточную аттестацию

Рабочая программа дисциплины составлена на основании федерального государственного образовательного стандарта (ФГОС) высшего образования - бакалавриат по направлению подготовки 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА.

Федеральный государственный образовательный стандарт (ФГОС) высшего образования - бакалавриат по направлению подготовки 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА введен в действие приказом Минобрнауки от 19.09.2017 № 929.

Место дисциплины в структуре учебного плана: Блок 1 Дисциплины (модули), обязательная часть, обязательная дисциплина.

Рабочая программа дисциплины утверждена решением Ученого совета факультета информационных технологий от 02.07.2019, протокол № 75.

Программу разработали:

доцент кафедры компьютерных систем ФИТ,
кандидат технических наук  Т.М. Пестунова

Заведующий кафедрой компьютерных систем ФИТ,

кандидат технических наук  Б.Н. Пищик

Ответственный за образовательную программу:

доцент кафедры систем информатики ФИТ,
кандидат технических наук  А.А. Романенко

Аннотация к рабочей программе дисциплины
«Защита информации»

Дисциплина «Защита информации» реализуется в рамках образовательной программы высшего образования – программы бакалавриата 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА, направленность (профиль): ПРОГРАММНАЯ ИНЖЕНЕРИЯ И КОМПЬЮТЕРНЫЕ НАУКИ по очной форме обучения на русском языке.

Место в образовательной программе: Дисциплина «Защита информации» развивает знания, умения и навыки, сформированные у обучающихся по результатам изучения следующих дисциплин: «Информатика», «Программирование», «Дискретная математика», «Математическая логика и теория алгоритмов».

Дисциплина «Защита информации» является базовой для прохождения производственной практики и написания выпускной квалификационной работы.

Дисциплина «Защита информации» реализуется в 7 семестре в рамках базовой части дисциплин (модулей) Блока 1 и является обязательной дисциплиной.

Дисциплина «Защита информации» направлена на формирование компетенций:

УК 2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

УК 2.3. Владеть: методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта, навыками работы с нормативно-правовой документацией

ОПК 3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК 3.1. Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК 3.2. Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК 3.3. Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

ОПК 9. Способен осваивать методики использования программных средств для решения практических задач

ОПК 9.1. Знать: классификацию программных средств и возможности их применения для решения практических задач

Перечень основных разделов (тем) дисциплины:

Тема 1. Основные понятия и концептуальные основы информационной безопасности.

Тема 2. Правовое обеспечение защиты информации.

Тема 3. Методологические и организационные аспекты защиты информации.

Тема 4. Типовые подсистемы и сервисы безопасности в информационных системах и компьютерных сетях.

Тема 5. Введение в криптографические методы защиты информации

Тема 6. Математические модели управления доступом и информационными потоками в компьютерных системах

Тема 7. Стандарты безопасности информационных технологий

Тема 8. Понятие безопасного программирования.

При освоении дисциплины предусмотрены лекции, лабораторные занятия, самостоятельная работа.

На лекциях рассматриваются методологические основы информационной безопасности, типовые угрозы и уязвимости, правовое регулирование и организационное обеспечение защиты информации, формирование требований по защите информации для информационных систем, в том числе информационных систем персональных данных, государственных информационных систем, объектах критической информационной инфраструктуры. Изучаются базовые криптографические методы, принципы и свойства дискреционных, мандатных и ролевых систем управления доступом в компьютерных системах. Даётся обзор стандартов информационной безопасности, классов защищённости, профилей защиты и оценочных уровней доверия. Обсуждаются принципы безопасного программирования, вопросы разработки безопасного программного обеспечения и создания защищённых информационных систем.

На практических занятиях студенты выполняют лабораторные работы по исследованию уязвимостей, моделированию угроз, программной реализации алгоритмов защиты информации, администрированию средств защиты информации, а также докладывают результаты своей аналитической работы. В учебном процессе используются активные и интерактивные формы занятий. На практических занятиях проводятся обсуждения результатов выполненных заданий в формате собеседования и докладов-презентаций, а также ряда практически значимых вопросов по заданной тематике. На лекциях проводятся экспресс-опросы, совместный анализ практических примеров, иллюстрирующих теоретические положения.

Самостоятельная работа включает: изучение учебного и информационного материала по тематике дисциплины, подготовку докладов, презентаций и отчётных работ по результатам лабораторных работ и самостоятельной домашней работы, подготовку к текущей и промежуточной аттестации.

При проведении лекций, практических и лабораторных занятий могут применяться дистанционные образовательные технологии.

Общий объем дисциплины – 3 зачетных единиц (108 часов).

Правила аттестации по дисциплине. Текущий контроль по дисциплине «Защита информации» осуществляется в форме защиты результатов лабораторных и аналитических работ с оценкой по 5-балльной системе «неудовлетворительно», «удовлетворительно», «хорошо», «отлично». Выполнение на положительную оценку всех предусмотренных программой лабораторных работ является необходимым условием успешного прохождения 1 этапа промежуточной аттестации к дифференцированному зачёту.

Промежуточная аттестация по дисциплине «Защита информации» проводится по завершению ее освоения в конце 7 семестра в форме дифференцированного зачёта, результаты которого оцениваются по шкале: «неудовлетворительно», «удовлетворительно», «хорошо», «отлично». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

Оценка за освоение дисциплины на дифференцированном зачёте выставляется на основе портфолио студента и письменного ответа на вопросы по билету. Портфолио включает: презентации и устные доклады по изучаемой тематике; отчёты о лабораторных работах. Вопросы билета составляются по тематике лекций, по его итогам студенты получают оценку за теорию по такой же шкале. Итоговая оценка определяется как среднее арифметическое баллов за портфолио и ответ по билету, в случае дробной части для округления в большую сторону преподаватель имеет право задать дополнительный вопрос.

Оценка «отлично» соответствует продвинутому уровню сформированности компетенции. Оценка «хорошо» соответствует базовому уровню сформированности

компетенции. Оценка «удовлетворительно» соответствует пороговому уровню сформированности компетенции.

Учебно-методическое обеспечение дисциплины.

Учебно-методический комплекс по дисциплине «Защита информации» в электронной информационно-образовательной среде НГУ:
https://classroom.google.com/w/MTUzMjk4MTE1ODMy/t/all

1. **Внешние требования к дисциплине**

Таблица 1.1

Компетенция УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
У -2.3. Владеть: методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта, навыками работы с нормативно-правовой документацией
Компетенция ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности
ОПК-3.1. Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности
ОПК-3.2. Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ОПК-3.3. Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно- исследовательской работе с учетом требований информационной безопасности
Компетенция ОПК-9. Способен осваивать методики использования программных средств для решения практических задач
ОПК-9.1. Знать: классификацию программных средств и возможности их применения для решения практических задач

2. **Требования к результатам освоения дисциплины**

Таблица 2.1

Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)		**Формы организации занятий**		
		Лекции	**Лабораторная**	**Самост. работа**
УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений **УК-2.3.** Владеть: методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта, навыками работы с нормативно-правовой документацией				
1	Иметь представление о современной проблематике информационной безопасности, как междисциплинарной предметной области, её роли в технологическом и социально-экономическом развитии общества, знать базовые понятия и определения.	+	+	+
2	Иметь представление об системе правового регулирования в области информационной безопасности в целом; знать сферу действия, основные положения и нормы соответствующих законов Российской Федерации и других базовых нормативно-правовых актов федерального уровня.	+	+	+
3	Знать методологические основы защиты информации: определение целей защиты информации, основные виды угроз безопасности информации и понятие модели угроз;	+	+	+

	принципы защиты информации, понятие и функции системы защиты информации, основные этапы создания системы защиты информации на основе оценки рисков.			
4	Знать организационно-управленческие аспекты обеспечения информационной безопасности: понятие политики безопасности и её примерную структуру, задачи информационной безопасности во взаимосвязи с жизненным циклом информационных систем, типовые организационные меры по защиты информации.	+	+	+
5	Владеть навыками применения положений законодательства и требований нормативно-правовых документов по защите информации при проектировании, разработке, внедрении и эксплуатации информационных систем персональных данных, государственных информационных систем, объектов критической информационной инфраструктуры, а также при обеспечении личной информационной безопасности.	+	+	+
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно - коммуникационных технологий и с учетом основных требований ИБ **ОПК-3.1.** Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности				
6	Иметь представление о принципах, моделях, методах и алгоритмах для решения задач защиты информации в компьютерных системах и сетях: знать формальные модели управления доступом в операционных системах и базах данных, основные принципы и примеры методов аутентификации, основные классы методов и примеры алгоритмов криптографической защиты информации, принципы и примеры алгоритмов стеганографии, принципы антивирусной защиты, обнаружения вторжений и мониторинга безопасности, принципы и примеры методов выявления уязвимостей и анализа защищённости.	+	+	+
7.	Знать суть понятия «безопасное программирование», угрозы информационной безопасности в процессе проектирования и разработки программного обеспечения, рекомендованные стандартом требования к организации процесса разработки безопасного ПО.	+	+	+
	ОПК-3.2. Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности			
8	Уметь принимать участие в разработке программного обеспечения для решения задач защиты информации.	+	+	+
9	Уметь выявлять проблемы защиты информации при решении профессиональных задач, осуществлять обоснованный выбор необходимого системного и прикладного программного обеспечения, в контексте требований по защите информации.	+	+	+
ОПК-3.3. Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности				
10	Владеть навыками освоения и применения для решения		+	+

	профессиональных задач средств защиты информации на примере доступных программных продуктов (встроенных сервисов безопасности операционных систем, средств криптографической защиты информации, средств анализа защищённости, обнаружения вторжений, VPN и др.)			
11	Владеть профессиональной терминологией в области информационной безопасности и защиты информации, уметь правильно использовать её в письменных работах (при подготовке обзоров, рефератов, публикаций, докладов) и в устной речи.		+	+
ОПК-9. Способен осваивать методики использования программных средств для решения практических задач **ОПК-9.1.** Знать: классификацию программных средств и возможности их применения для решения практических задач				
12	Знать основные подсистемы и средства для решения задач защиты информации в автоматизированных (информационных) системах, их назначение и возможности.	+	+	+
13	Знать стандарты обеспечения безопасности информационных технологий, принципы разработки и возможности использования профилей защиты программного обеспечения.	+		+
14	Знать закреплённые нормативными документами принципы и методики классификации программного обеспечения информационных (автоматизированных) системы по классам (уровням) защищённости	+	+	+
15	Иметь представление о требованиях к мерам и средствам защиты информации в автоматизированных (информационных) системах различных классов (уровней) защищённости.	+	+	+

3. Содержание и структура учебной дисциплины

Таблица 3.1

Темы лекций	Активные формы, час. (входит в общее кол-во часов)	Часы	Ссылки на результаты обучения
Семестр: 7			
Тема 1. Основные понятия и концептуальные основы информационной безопасности.	0	2	**1, 3, 9**
Тема 2. Правовое обеспечение защиты информации.	2	4	**2, 5, 14**
Тема 3. Методологические и организационные аспекты защиты информации.	2	4	**3, 4, 9, 12, 13**
Тема 4. Типовые подсистемы и средства обеспечения безопасности в информационных системах и компьютерных сетях.	0	4	**6, 9, 12**
Тема 5. Введение в криптографическую защиту информации и стеганографию	2	6	**6**, **8, 12**
Тема 6. Математические модели управления доступом и информационными потоками в компьютерных системах	2	6	**6, 8**
Тема 7. Стандарты безопасности информационных технологий.	2	4	**8, 12, 13, 15**,
Тема 8. Понятие безопасного программирования	0	2	**7, 8**
Итого:	**10**	**32**	

Таблица 3.2

Темы лабораторных занятий	**Активные формы, час.** (входит в общее кол-во часов)	**Часы**	**Ссылки на результаты обучения**	**Учебная деятельность**
Семестр: 7				
Тема 1. Основные понятия и концептуальные основы информационной безопасности.	1	2	**1, 3, 9**	Обучающиеся закрепляют основные понятия и принципы защиты информации на примерах, формируют тезаурус. Знакомятся с Интернет-ресурсами по угрозам, уязвимостям и средствам обеспечения информационной безопасности. Обсуждение в ходе группового опроса
Тема 2. Правовое обеспечение защиты информации.	1	2	**2, 5, 14**	Обучающиеся проводят анализ практических (модельных) примеров на применение положений законов и нормативно-правовых актов по защите информации; моделируют зависимости требований по защите информации от правового поля. Классифицируют информационные системы.
Тема 3. Методологические и организационные аспекты защиты информации.	2	4	**3, 4, 9, 11**	Обучающиеся выявляют угрозы и уязвимости web-систем для заданных ОС, СУБД и средств разработки web-приложения на основе анализа интернет-каталогов, выступают с краткими докладами, которые обсуждаются на занятии. Выполняют анализ рисков и оценку актуальности угроз в информационных системах по стандартным методикам с разрабатывают модель угроз и выбирают необходимые меры защиты.
Тема 4. Типовые подсистемы и сервисы безопасности в информационных системах и компьютерных сетях.	4	8	**9, 12, 10, 11, 15**	Обучающиеся изучают базовые средства защиты информации в информационных системах: средства анализа защищённости (сетевые сканеры), сервисы безопасности в операционных системах и базах данных, осваивают на практике работу со средствами защиты от несанкционированного доступа к информации для решения задач аутентификации, управления доступом, аудита безопасности,

				обнаружения атак, антивирусной защиты.
Тема 5. Введение в криптографическую защиту информации и стеганографию	6	12	**6, 8, 10**	Обучающиеся решают задачи на основные понятия и методы шифрования, исследуют реализации криптоалгоритмов, методы стеганографического внедрения информации. Выполняют установку и администрирование программных средств криптографической защиты
Тема 8. Понятие безопасного программирования	2	4	**7, 8, 11**	Обучающиеся знакомятся с практическими аспектами применения принципов безопасного программирования и предотвращения уязвимостей при разработке ПО. Результаты представляется в форме эссе и обсуждаются на занятии.
Итого:	**16**	**32**		

4. Самостоятельная работа студентов

Таблица 4.1

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 7				
1	Подготовка к практическим занятиям по теме 1.	**1, 3, 9**	4	
	Обучающиеся повторяют материал лекции 1, для самоконтроля выполняют тест по терминологии (https://classroom.google.com/w/MTUzMjk4MTE1ODMy/t/all). При необходимости следует воспользоваться ГОСТ 50922-2006 «Защита информации. Основные термины и определения». ГОСТ 51275-2006 «Факторы, воздействующие на информацию», ГОСТ Р 53114-2008 «Обеспечение информационной безопасности организации»). Далее нужно познакомиться с материалами об актуальных угрозах и уязвимостях на специализированных сайтах по информационной безопасности: https://www.kaspersky.ru (в частности, отчёт https://tproger.ru/news/kaspersky-lab-industrial-report и др.), https://securelist.ru, https://www.drweb.ru, https://www.securitylab.ru, https://safe-surf.ru/, https://www.ptsecurity.com/ru-ru/research, и др. По результатам изучения материалов (с учётом своего личного опыта) составить и аргументировать свою версию Top-10 угроз, актуальных для организаций (группы организаций, отобранных по какому-либо признаку) или пользователей информационных технологий на текущий момент. Защита работы производится на занятии в форме устного сообщения с последующим обсуждением.			
2	Подготовка к практическим занятиям по теме 2.	**2, 5, 14, 15**	4	
	Обучающиеся повторяют материал лекций по данной теме. Знакомятся с назначением, сферой действия, базовой терминологией и основными положениями Федеральных законов, приведённых в списке нормативно-правовых документов. Постановлений правительства в области обеспечения безопасности в информационных систем персональных данных, категорирования объектов критической информационной инфраструктуры и приказом ФСТЭК России об обеспечении безопасности государственных информационных систем. Изучают классификацию информационных систем персональных данных и государственных информационных систем, принципы категорирования объектов критической инфраструктуры. Сравнивают требования к защите информации в информационных системах разной архитектуры и разных классов (уровней) защищённости.			
3	Подготовка к практическим занятиям по теме 3.	**3, 4, 9, 11**	8	
	1. Изучить каталоги актуальных уязвимостей Open Web Application Security Project (OWASP), Web Application Security Consortium(WASC), ссылки на которые приведены в списке литературы (раздел «информационные источники»). Ознакомиться с соответствующими классификациями уязвимостей. Ответить на контрольные вопросы и дать описания распространённых типов атак. Выбрать вариант комплекса средств создания web-приложений (ОС, СУБД, средство разработки программного кода) из числа предложенных вариантов, определить для него известные уязвимости и возможные атаки. Подробное задание и методические рекомендации по подготовке отчётности и презентаций представлены в приложении к рабочей программе дисциплины: https://classroom.google.com/w/MTUzMjk4MTE1ODMy/t/all На занятии результаты представляются в форме краткого сообщения (доклада с презентацией) с			

	последующим общим обсуждением. 2. В соответствии с вариантом модельной информационной системы организации классифицировать её в соответствии с требованиями законодательства, построить проект модели угроз. Применив одну из изученных методик оценки рисков, определить актуальные угрозы. При формировании модели угроз рекомендуется использовать Базовую модель угроз безопасности в информационных системах персональных данных (доступна на сайте ФСТЭК России fstec.ru) и банк данных угроз bdu.fstec.ru. Отчётность оформляется в форме проекта модели угроз. Консультации и защита задания проводятся на занятиях. 3. Разработать одну из частных политик безопасности для изученной информационной системы (варианты определяется по согласованию с преподавателем). Разработанный проект документа представляется включается в отчёт			
4	Подготовка к практическим занятиям по теме 4	**10, 11, 12, 15**	8	
	Обучающиеся изучают учебные материалы, техническую документацию, информационные источники на сайтах производителей средств защиты информации для подготовки к выполнению лабораторных работ, связанных с установкой и администрированием средств защиты информации: - типовые сервисы безопасности, встроенные в операционные системы Windows и Linux доступных версий. - типовые функции средств анализа уязвимостей (сканеров безопасности). - типовые функции антивирусных систем, средств обнаружения вторжений и межсетевых экранов; Методические указания к выполнению лабораторных работ размещаются и актуализируются на https://classroom.google.com/w/MTUzMjk4MTE1ODMy/t/all Оформляют отчётность по итогам выполнения лабораторных работ. Отчёты о выполнении лабораторных работ защищаются индивидуально.			
5	Подготовка к практическим занятиям по теме 5.	**6, 8, 10**	4	
	Обучающиеся повторяют материал лекций, основные понятия и методы криптографии. Знакомятся с отечественными криптографическими стандартами, приведёнными в списке литературы. Для подготовки к лабораторной работе осуществляют выбор реализуемых криптографических средств защиты информации, анализируют особенности изученных криптоалгоритмов, формулирует концепцию их реализации на одном из языков программирования, готовят отчётность по лабораторной работе для защиты. Для подготовки к лабораторной работе выбирают программные средства внедрения цифровой информации и стегоанализа (напр., свободное ПО OpenStego), анализируют особенности алгоритмов стеганографии в контексте их программной реализации, готовятся отчётность о выполнении лабораторной работы для защиты. Изучают принципы создания, особенности структуры и применения виртуальных частных сетей, в частности, методические материалы по установке, администрированию программных средств криптографической защиты информации, построения инфраструктуры открытых ключей с целью шифрования информации и формирования электронной подписи. Знакомятся со средствами построения VPN-сетей. Методические материалы размещаются и актуализируются на ресурсе https://classroom.google.com/w/MTUzMjk4MTE1ODMy/t/all Для решения задач берётся программное обеспечение, ссылки на которое даны ниже в соответствующем разделе данной рабочей программы. Необходимая техническая документация берётся с сайтов производителей.			
6	Подготовка к практическим	**7, 8, 11**	4	

	занятиям по теме 8.			
	Обучающиеся повторяют материал лекций, изучают РД Гостехкомиссии о классификации программного обеспечения по уровню контроля отсутствия недекларированных возможностей, требования к использованию методов безопасного программирования и анализу уязвимостей при разработке программного обеспечения защиты информации в ГОСТ Р 15408 -2013 (ч.3.), детализации анализа уязвимостей в соответствии с ГОСТ Р 58142-2018 (ч.1 и ч.2), угрозы безопасности при разработке программного обеспечения в соответствии с ГОСТ 58412—2019, общие требования к разработке безопасного программного обеспечения в соответствии с ГОСТ Р 56939-2016, требования к процессу создания автоматизированных систем в защищённом исполнении в соответствии с ГОСТ 51583-2000. Опираясь на нормативно-правовую документацию, материалы лекций и доступные интернет-ресурсы формируют свое понимание безопасного программирования, эссе по теме и подготавливаются к обсуждению его на занятиях. Методические материалы по теме размещены: https://classroom.google.com/w/MTUzMjk4MTE1ODMy/t/all			
7	Подготовка к дифференцированному зачету	1-15	10	
	Повторение теоретического материала по вопросам, совпадающим с темами лекций			
	Итого:		**42**	

5. Образовательные технологии

В ходе учебного процесса по дисциплине проводятся лекционные и практические (лабораторные) занятия. Как правило, знания по вопросам, рассматриваемым на лекциях и изучаемые самостоятельно, закрепляются и углубляются на практических (лабораторных) занятиях, при этом уровень формирования компетенций повышается за счёт получения опыта практического применения изученных теоретических положений и методик, освоения программного инструментария для решения задач защиты информации и самостоятельной программной реализации некоторых алгоритмов защиты информации. По вопросам, вызывающим затруднения, проводятся консультации.

На лекциях излагаются основные концептуальные, нормативно-правовые, методологические и математические положения в соответствии с изучаемой тематикой. В целях закрепления новых понятий, подходов, методов проводятся экспресс-опросы с последующим анализом допущенных ошибок, совместный анализ проблем на примере приближённых к реалиям модельных ситуаций.

В ходе практических (лабораторных) занятий работа студентов выполняется в следующих формах:

- подготовка аналитических отчётов, докладов, презентаций по заданной тематике на основе изучения нормативно-правовых актов, учебной и научной литературы, поисковой работы в интернет с использованием профессиональных интернет-ресурсов по информационной безопасности;
- установка, конфигурирование и администрирование программного обеспечения для решения задач защиты информации (выполняется, как правило, на виртуальных машинах, доступных в компьютерных классах; виртуальные машины с изучаемыми средствами или непосредственно изучаемое программное обеспечение могут быть установлены также в ряде случаев и на личные ноутбуки обучающихся, что позволяет часть работы выполнять дома);
- разработка типовой документации, необходимой в процессе создания и эксплуатации систем информационной безопасности;
- программная реализация алгоритмов защиты информации;
- защита результатов выполненных работ в публичной (выступления с докладами и презентациями в форме конференций с последующим осуждением доложенных результатов всеми студентами) или индивидуальной (собеседования с

преподавателем) формах.

В ходе реализации учебного процесса по дисциплине применяются такие формы проведения практических занятий, как дискуссии, обсуждение и защита результатов работы, а также применяются следующие интерактивные формы обучения (таблица 5.1).

Таблица 5.1

1	Технологии проблемного обучения	УК-2.3 ОПК-3.2, ОПК – 3.3, ОПК-9.1.
Формируемые умения: 5. Владеть навыками применения положений законодательства и требований нормативно-правовых документов по защите информации при проектировании, разработке, внедрении и эксплуатации информационных систем персональных данных, государственных информационных систем, объектов критической информационной инфраструктуры, а также при обеспечении личной информационной безопасности. **1**. Иметь представление о современной проблематике и понятийном аппарате информационной безопасности, как междисциплинарной предметной области, её роли в технологическом и социально-экономическом развитии общества. **3.** Знать методологические основы защиты информации: определение целей защиты информации, основные виды угроз безопасности информации и понятие модели угроз; принципы защиты информации, понятие и функции системы защиты информации, основные этапы создания системы защиты информации на основе оценки рисков. **8**. Уметь принимать участие в разработке программного обеспечения для решения задач защиты информации. **9.** Уметь выявлять проблемы защиты информации при решении профессиональных задач, осуществлять обоснованный выбор необходимого системного и прикладного программного обеспечения, в контексте требований по защите информации. **11.** Владеть профессиональной терминологией в области информационной безопасности и защиты информации, уметь правильно использовать её в письменных работах (при подготовке обзоров, рефератов, эссе, публикаций, докладов) и в устной речи. **14.** Знать закреплённые нормативными документами принципы и методики классификации информационных (автоматизированных) системы по классам (уровням) защищённости		
Краткое описание применения: активизация познавательной деятельности студента за счет ассоциации собственного опыта с предметом изучения: постановка самостоятельно или под руководством преподавателя проблемных задач из профессиональной деятельности ИТ-специалиста, в том числе на основе собственного жизненного опыта студентов, и активная самостоятельная деятельность обучающихся по их разрешению, сопровождающаяся обсуждением результатов.		
2	Портфолио	УК-2.3. ОПК-3.1. ОПК-3.2. ОПК-3.3. ОПК-9.1.
Формируемые умения: 5. Владеть навыками применения положений законодательства и требований нормативно-правовых документов по защите информации при проектировании, разработке, внедрении и эксплуатации информационных систем персональных данных, государственных информационных систем, объектов критической информационной инфраструктуры, а также при обеспечении личной информационной безопасности. **3.** Знать методологические основы защиты информации: определение целей защиты информации, основные виды угроз безопасности информации и понятие модели угроз; принципы защиты информации, понятие и функции системы защиты информации, основные этапы создания системы защиты информации на основе оценки рисков. **4.** Знать организационно-управленческие аспекты обеспечения информационной безопасности: понятие политики безопасности и её примерную структуру, задачи информационной безопасности во взаимосвязи с жизненным циклом информационных систем, типовые организационные меры по защите информации. **7.** Знать суть понятия «безопасное программирование», угрозы		

информационной безопасности в процессе проектирования и разработки программного обеспечения, рекомендованные стандартом требования к организации процесса разработки безопасного ПО. **8.** Уметь принимать участие в разработке программного обеспечения для решения задач защиты информации. **10**. Владеть навыками освоения и применения для решения профессиональных задач средств защиты информации на примере доступных программных продуктов (встроенных сервисов безопасности ОС, средств криптографической защиты информации, средств анализа защищённости, обнаружения вторжений, VPN и др.) **11**. Владеть профессиональной терминологией в области информационной безопасности и защиты информации, уметь правильно использовать её в письменных работах (при подготовке обзоров, рефератов, эссе, публикаций, докладов) и в устной речи. **15.** Иметь представление о требованиях к мерам и средствам защиты информации в автоматизированных (информационных) системах различных классов (уровней) защищённости
Краткое описание применения: студенты ведут портфолио (коллекцию работ), которое учитывается при проведении аттестации по дисциплине.
2 Индивидуальное обучение: ОПК 3.2. ОПК 3.3.
Формируемые умения: 8. Уметь принимать участие в разработке программного обеспечения для решения задач защиты информации. **9.** Уметь выявлять проблемы защиты информации при решении профессиональных задач, осуществлять обоснованный выбор необходимого программного обеспечения, в контексте требований по защите информации. **10.** Владеть навыками освоения и применения для решения профессиональных задач средств защиты информации на примере доступных программных продуктов (встроенных сервисов безопасности ОС, средств криптографической защиты информации, средств анализа защищённости, обнаружения вторжений, VPN и др.)
Краткое описание применения: выстраивание студентом собственной образовательной траектории на основе формирования индивидуальной образовательной программы с учетом интересов студента за счёт предоставляемых возможностей выбора объектов, методов и инструментария при выполнении аналитических и практических работ по изучаемым тематикам с учетом интересов .

Для организации и контроля самостоятельной работы студентов, а также проведения консультаций применяются информационно-коммуникационные технологии (таблица 5.2).

Таблица 5.2

Информирование	https://classroom.google.com/w/MTUzMjk4MTE1ODMy/t/all официальные адреса групп студентов на *@g.nsu.ru
Консультирование	t.pestunova@g.nsu.ru, ptm@ngs.ru (лекции) a.perov@g.nsu.ru, perov_artem@inbox.ru, (практика) a.balabanov@g.nsu.ru, baatob@gmail.com. (практика) y.kopolovets@g.nsu.ru, yurakop25@ya.ru (практика) Личный кабинет студента в Гугл-классе (ссылка на ресурс приведена ниже) Взаимодействие с преподавателем организуется также через личный кабинет студента в Гугл-классе (ссылка на ресурс приведена ниже) Интерактивное дистанционное консультирование осуществляется с использованием электронных сервисов, применяемых при проведении дистанционных лекций (табл. 5.3).
Контроль	Все задания, выносимые на контроль в рамках практических (лабораторных) занятий сдаются преподавателю в компьютерном классе во время занятий занятий или с использованием дистанционных технологий, при этом защита выполненных заданий на компьютере осуществляется в режиме демонстрации экрана или с использованием видеокамеры. Выполняемые действия

	студент комментирует устно. Отчётность, предоставляемая в рамках выполнения практических заданий, может предоставляться в электронном виде по адресам, указанным в строке «консультирование»
Размещение учебных материалов	https://classroom.google.com/w/MTUzMjk4MTE1ODMy/t/all

При проведении лекций, практических и лабораторных занятий могут применяться дистанционные образовательные технологии (таблица 5.3). Применение дистанционных образовательных технологий позволяет обеспечить эффективное взаимодействие преподавателя со студентами в различных ситуациях, когда преподаватель или студенты не могут территориально присутствовать в помещениях НГУ в силу объективных и уважительных субъективных факторов. Дистанционные технологии могут применяться в том числе и в «смешанном формате»: при проведении лекционных и практических занятий преподаватель дополнительно подключает дистанционный сервис, позволяющий участвовать в занятии студентам, которые по каким- либо причинам не могут присутствовать в классе.

Таблица 5.3

Лекции	С использованием сервиса “google meet”, ссылка размещается на главной странице курса в гугл-классе и доступна всем студентам, обучающимся по данному курсу https://classroom.google.com/w/MTUzMjk4MTE1ODMy/t/all Вопросы задаются с использованием микрофона или чата. Для демонстрации удаленным слушателям записей преподавателя на доске в классе используется видеокамера. Резервный канал организуется с помощью других доступных в НГУ сервисов. В случае недоступности в какой-то момент дистанционных сервисов НГУ, используется Яндекс-телемост через личный аккаунт преподавателя (для лекций с адреса tmrp54@yandex.ru), ссылка на него высылается на электронные адреса студентов студентам *@g.nsu.ru накануне подключения. Лекции и общие методические материалы размещаются в ленте курса.
Практические и лабораторные задания	t.pestunova@g.nsu.ru, tmrp54.yandex.ru (лекции) a.perov@g.nsu.ru, perov_arte@inbox.ru, (практика) a.balabanov@g.nsu.ru, baatob@gmail.com, (практика) y.kopolovets@g.nsu.ru, yurakop25@ya.ru (практика) Методические рекомендации по выполнении лабораторных (практических работ) озвучиваются преподавателем с использованием сервисов видеосвязи (аналогичных используемым на лекционных занятиях) и при необходимости сопровождаются пояснениями в режиме демонстрации экрана. Практические задания создаются и принимаются в разделе «Задания». Преподаватель создаёт соответствующее задание, размещает необходимые методические материалы). В течение практического (лабораторного) занятия преподаватель находится на связи с применением этих же электронных сервисов. При дистанционном выполнении практических (лабораторных) заданий отчетную документацию (написанные программы, аналитические обзоры, решенные задачи и т.п.) студент предоставляет также через личный кабинет в гугл-классе. Защита выполненных заданий на компьютере осуществляется в режиме демонстрации экрана или с использованием видеокамеры. Выполняемые действия студент комментирует устно. В ходе проверки присланной отчётности преподаватель может задавать вопросы и делать замечания в форме комментарии в чате со

	студентом в гугл-классе.
Размещение учебных материалов	https://classroom.google.com/w/MTUzMjk4MTE1ODMy/t/all Презентации к лекциям, текстовые и другие общие методические материалы — в ленте курса. Практические задания создаются в разделе «Задания»

6. Правила аттестации студентов по учебной дисциплине

По дисциплине «Защита информации» проводится текущая и промежуточная аттестация (итоговая по дисциплине).

Текущий контроль по дисциплине «Защита информации» осуществляется в форме защиты результатов выполненных лабораторных работ и аналитических заданий на практических занятиях. Защита проводится индивидуально и заключается в презентации и защите докладов по основным разделам дисциплины, по итогам которых выставляется оценка по 4-балльной шкале «неудовлетворительно», «удовлетворительно», «хорошо», «отлично». Выполнение на положительную оценку всех предусмотренных программой лабораторных работ является необходимым условием успешного прохождения 1 этапа промежуточной аттестации к дифференцированному зачёту.

Промежуточная аттестация по дисциплине «Защита информации» проводится по завершению ее освоения в конце 7 семестра в форме дифференцированного зачёта. Результаты промежуточной аттестации по дисциплине оцениваются по 4-балльной шкале «неудовлетворительно», «удовлетворительно», «хорошо», «отлично». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

Оценка за освоение дисциплины в рамках дифференцированного зачёта выставляется по результатам оценивания портфолио работ студента и результатов контрольного задания по теоретическому (лекционному) материалу, выполняемого непосредственно в ходе проведения дифференцированного зачёта.

Портфолио включает в себя работы, выполненные в рамках лабораторных занятий и самостоятельной работы:

1) презентации и устные доклады на темы, соответствующие разделам дисциплины;
2) устные и (или) письменные отчёты о результатах лабораторных и аналитических работ.

За каждый артефакт портфолио выставляется оценка O_i по 5-балльной шкале, где i=1,2,.., $N_{пр}$, $N_{пр}$ — количество оцениваемых артефактов портфолио по итогам практикума, исходя из следующих критериев.

«Отлично» (5 баллов): задание выполнено полностью и правильно, все выводы корректно убедительно аргументированы, грамотно изложены (в письменном и / или устном виде), аккуратно оформлены (для письменных артефактов и презентаций), студентом корректно используется профессиональная терминология, правильно формулируются понятия и категории предметной области дисциплины, студентом продемонстрирован высокий уровень владения материалом по теме задания на содержательном уровне, при подготовке используется актуальная литература и качественно подобранные интернет-источники. Для заданий в письменном виде допускаются отдельные незначительные погрешности оформления, не снижающие общего впечатления от выполненной работы.

«Хорошо» (4 балла): недостаточно полное раскрытие темы, отдельные ошибки при выполнении и объяснении процесса выполнения и полученных результатов, которые студент способен исправить самостоятельно или при небольшой подсказке преподавателя; несущественные ошибки в определении понятий и категорий, а также в аргументации решений и выводов, кардинально не меняющих правильную суть изложения; частичное использование неактуальных источников, незначительные погрешности грамотности изложения

«Удовлетворительно» (3 балла): общая правильная направленность действий в рамках выполнения задания, неполная и не всегда убедительная аргументация, наличие существенных ошибок и (или) множественных несущественных ошибок в определении понятий и в содержательной части работы, использование значительной части устаревшей учебной литературы и других источников, неполнота ответа, неспособность целостно осветить проблематику вопроса. Частично способен исправить ошибки при подсказке преподавателя.

«Неудовлетворительно» (0 баллов): недоведенное до конца выполнение задания, качественно неверный результат; большое количество существенных ошибок в процессе выполнения, неправильное (неубедительное) объяснение результатов или отсутствие такого объяснения; необоснованная и некачественная подборка литературы и информационных источников; слабое знание или незнание профессиональной терминологии, неспособность осветить проблематику вопроса, неспособность исправить ошибки даже при наводящей подсказке преподавателя.

В конце семестра определяется итоговый балл за портфолио ($\mathbf{O_{пр)}}$ как среднее арифметическое значение от количества баллов за каждый артефакт:

$$\mathbf{O_{пр}} = (O_1 + O_2 + \ldots + O_{Nпр})/N_{пр}.$$

Контрольное занятие по теоретическому (лекционному) материалу на дифференцированном зачёте проводится по билетам в письменной форме по тематике лекций, по итогам студенты получают оценку за теорию, которая также нормируется в 5-балльную шкалу ($\mathbf{O_т}$).

При аттестации по билетам студенту выдается билет с 6 вопросами, оценка определяется в зависимости количества правильных и полных ответов на поставленные вопросы в соответствии со следующими критериями.

«отлично» (5 баллов) — если не менее чем на 5 вопросов даны правильные аргументированные ответы (в правильном ответе допускается одна несущественная ошибка, которую студент смог самостоятельно исправить при указании на нее преподавателем), ответ на оставшийся вопрос может быть неполным, но с правильным общим направлением мысли;

«хорошо» (4 балла) — если студент ответил правильно на 4 вопроса, при ответе остальные вопросы допустил существенные ошибки при общем правильном направлении мысли, один вопрос может остаться без ответа;

«удовлетворительно» (3 балла) — если имеет место одна из двух ситуаций: а) студент смог правильно ответить на 3 вопроса, а на три других либо не ответил, либо допустил существенные ошибки; б) студент попытался ответить более, чем на 3 вопроса, не менее двух ответов правильные или почти правильные (с 1-2 несущественными ошибками), а остальные не доведены до конца, но при этом как минимум в ответах на два из них присутствует правильное общее направление мысли.

Итоговая оценка **О** за освоение дисциплины определяется как среднее арифметическое количества баллов за теорию и практику $\mathbf{O} = (\mathbf{O_{пр}} + \mathbf{O_т}) / 2$. При возникновении дробной части для принятия решения об округлении в б***о***льшую сторону преподаватель имеет право задать дополнительный вопрос.

Оценка «отлично» соответствует продвинутому уровню сформированности компетенции.

Оценка «хорошо» соответствует базовому уровню сформированности компетенции.

Оценка «удовлетворительно» соответствует пороговому уровню сформированности компетенции.

В таблице 6.1 представлено соответствие форм аттестации заявляемым требованиям к результатам освоения дисциплины.

Таблица 6.1

Коды компетенций ФГОС	**Результаты обучения**	**Формы аттестации**	
		Портфолио	**Дифференци-рованный зачет**

УК-2	**УК 2.3.** Владеть методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта, навыками работы с нормативно-правовой документацией	+	+
ОПК-3	**ОПК 3.1.** Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	+	+
	ОПК 3.2. Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	+	
	ОПК 3.3. Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	+	
ОПК 9	**ОПК 9.1.** Знать: классификацию программных средств и возможности их применения для решения практических задач	+	+

Требования к структуре и содержанию портфолио, оценочные средства, а также критерии оценки сформированности компетенций и освоения дисциплины в целом, представлены в Фонде оценочных средств, являющемся приложением 1 к настоящей рабочей программе дисциплины.

7. Перечень учебной литературы

1. Нестеров, С.А. Основы информационной безопасности : учебное пособие (бакалавриат) / С.А. Нестеров .— 4-е изд., стереот. — Москва : Лань, 2018 .— 324 с. ; [Электронный ресурс]. - URL: https://e.lanbook.com/book/103908#authors
2. Ковалев, Д.В. Информационная безопасность : учебное пособие / Д.В. Ковалев, Е.А. Богданова ; Министерство образования и науки РФ, Южный федеральный университет. - Ростов-на-Дону : Издательство Южного федерального университета, 2016. - 74 с. : схем., табл., ил. - Библиогр. в кн. - ISBN 978-5-9275-2364-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=493175
3. Скрипник, Д.А. Общие вопросы технической защиты информации / Д.А. Скрипник. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=429070
4. Спицын, В.Г. Информационная безопасность вычислительной техники : учебное

пособие / В.Г. Спицын ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). - Томск : Эль Контент, 2011. - 148 с. : ил.,табл., схем. - ISBN 978-5-4332-0020-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=208694
5. Лапонина, О.Р. Криптографические основы безопасности / О.Р. Лапонина. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 244 с. : ил. - (Основы информационных технологий). - Библиогр. в кн. - ISBN 5-9556-00020-5 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=429092
6. Лапонина, О.Р. Межсетевые экраны : учебное пособие / О.Р. Лапонина. - 2-е изд., исправ. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 466 с. : ил. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=429093
7. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - Москва ; Берлин : Директ-Медиа, 2015. - 253 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557
7. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - Москва ; Берлин : Директ-Медиа, 2015. - 253 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557
8. Тушко, Т.А. Информатика : учебное пособие / Т.А. Тушко, Т.М. Пестунова ; Сибирский федеральный университет. – Красноярск : Сибирский федеральный университет (СФУ), 2017. – 204 с. : ил. - Библиогр. в кн. – ISBN 978-5-7638-3604-2 ; – URL: https://biblioclub.ru/index.php?page=book&id=497738

8. Перечень ресурсов информационно-коммуникационной сети «Интернет», необходимых для освоения дисциплины

При освоении дисциплины используются следующие ресурсы:

- электронная информационно-образовательная среда НГУ (ЭИОС);
- образовательные интернет-порталы;
- информационно-телекоммуникационная сеть Интернет.

Взаимодействие обучающегося с преподавателем (синхронное и (или) асинхронное) осуществляется через личный кабинет студента в ЭИОС

Таблица 8.1

№ п/п	Наименование Интернет-ресурса	Краткое описание
1	Безопасность информационных технологий / - [Электронный ресурс] / Режим доступа: https://bit.mephi.ru/index.php/bit/index	
2	Вестник УрФО. Безопасность в информационной сфере/ - [Электронный ресурс] / Режим доступа: http://www.info-secur.ru	
3	Category:OWASP Top Ten Project [Электронный ресурс] / Режим доступа: https://www.owasp.org/index.php/Top_10_2013-Top_10 – Загл. с экрана	Открытый проект по анализу уязвимостей (с 2013 года).
4	The WASC Threat Classification v2.0 ENG - [Электронный ресурс] / Режим доступа: http://projects.webappsec.org/w/page/13246978/Threat%20Classification - Загл. с экрана	Ресурс по классификации угроз безопасности Web-приложений, поддержи-ваемый консорциумом “The Web Application” Security Consortium
5	CVE. Common Vulnerabilities and Exposures. - [Электронный ресурс] / Режим доступа: http://cve.mitre.org/ - Загл. с экрана	База стандартных идентификаторов для общеизвестных ИТ-уязвимостей
6	Банк данных угроз безопасности информации -	Банк данных угроз

	[Электронный ресурс] / Режим доступа: http://bdu.fstec.ru/ - Загл. с экрана	безопасности информации в ИС, уязвимостей программного обеспечения и аппаратных платформ. Официальный ресурс ФСТЭК России.
7	ФСТЭК России. Федеральная служба по техническому и экспортному контролю Российской федерации - [Электронный ресурс] / Режим доступа: https://fstec.ru/ - Загл. с экрана	Официальный сайт ФСТЭК России.
8	Федеральная безопасности Российской федерации - [Электронный ресурс] / Режим доступа: http://www.fsb.ru/ - Загл. с экрана	Официальный сайт ФСБ России.
9	Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. - [Электронный ресурс] / Режим доступа: https://rkn.gov.ru/ - Загл. с экрана	Официальный сайт . Роскомнадзора
10	Управление Роскомнадзора по Сибирскому федеральному округу. - [Электронный ресурс] / Режим доступа: http://54.rkn.gov.ru - Загл. с экрана	Официальный сайт территор. управл. Роскомнадзора
11	Росстандарт. - [Электронный ресурс] / Режим доступа: https://www.gost.ru/portal/gost/ - Загл. с экрана	Официальный сайт Федер. агентства по техническому регулированию.
12	IB-BANK.RU. Отраслевой портал. - [Электронный ресурс] / Режим доступа : https://ib-bank.ru/ - Загл. с экрана	Отраслевой портал по ИБ в финансовой сфере
13	BIS Journal − Информационная безопасность банков / - [Электронный ресурс] / Режим доступа: https://journal.ib-bank.ru/journal - Загл. с экрана	Электронный журнал по ИБ в банковской сфере
14	SecurityLab.ru by Positive Technology− Информационная безопасность банков / - [Электронный ресурс] / Режим доступа https://www.securitylab.ru/ - Загл. с экрана	Информац. порталы о событиях в сфере защиты информации, интернет-права, уязвимостях, угрозах, инцидентах и методах защиты информации.
15	Kaspersky Lab. Secure List. - [Электронный ресурс] / Режим доступа https://securelist.ru, - Загл. с экрана	
16	Безопасность пользователей в сети Интернет - [Электронный ресурс] / Режим доступа: https://safe-surf.ru/ - Загл. с экрана	
17	AM. Anti-malware. - [Электронный ресурс] / Режим доступа https://www.anti-malware.ru/security - Загл. с экрана	
18	Positive Technology. - [Электронный ресурс]* / Режим доступа https://www.ptsecurity.com/ru-ru/ - Загл. с экрана	Информация о сертифицированных. средствах защиты информации на сайтах производителей. *Примечание: также статьи и аналитика по информационной безопасности, материалы вебинаров.
19	Kaspersky Lab. Secure List. - [Электронный ресурс] / Режим доступа : https://www.kaspersky.ru - Загл. с экрана	
20	Dr. Web. Антивирус - [Электронный ресурс] / Режим доступа : https://www.drweb.ru - Загл. с экрана	
21	Infotecs. - [Электронный ресурс]* / Режим доступа : https://infotecs.ru/ - Загл. с экрана	
22	РУСБИТЕХ. - [Электронный ресурс] / Режим доступа http://rusbitech.ru/ - Загл. с экрана	
23	Директор по безопасности - [Электронный ресурс] / Режим доступа: http://www.s-director.ru/magazine/latestnumber.html	Специализированное издание по корпоративной безопасности

24	Информационная безопасность - [Электронный ресурс] / Режим доступа: http://www.itsec.ru/	Периодическое информационно-справочное издание для ИТ- и ИБ-директоров
25	Лаборатория пен-теста.- [Электронный ресурс] / Режим доступа: https://habr.com/ru/company/pentestit/blog/332902/	Интерактивый виртуальный полигон для практического знакомства с активными методами анализа уязвимостей

9. Учебно-методическое и программное обеспечение дисциплины

9.1. Перечень учебно-методических материалов по самостоятельной работе обучающихся

Для обеспечения самостоятельной работы обучающихся при изучении дисциплины используются следующие учебно-методические материалы:

1. Настоящая рабочая программа дисциплины, соответствующие разделы.
2. Учебники, учебные пособия и дополнительные материалы.
3. Перечень ресурсов информационно-коммуникационной сети «Интернет».
4. Методические указания для обучающихся по освоению дисциплины, обеспечивающие самостоятельную работу студента при подготовке к учебным занятиям, выполнении домашних работ, подготовке к контрольным мероприятиям и аттестациям, приведенные в Приложении к настоящей рабочей программе дисциплины.
5. Пестунова Т.М. Защита информации [Электронный ресурс] : электронный учебно-методический комплекс / Т.М.Пестунова ; Новосиб. гос. ун-т. - Новосибирск [2021] - Режим доступа: https://classroom.google.com/w/MTUzMjk4MTE1ODMy/t/all - Загл. с экрана.

9.2. Программное обеспечение

Для обеспечения реализации дисциплины используются:

- стандартный комплект программного обеспечения (ПО), включающий регулярно обновляемое лицензионное ПО Windows и MS Office;
- Файловый архиватор 7-Zip v16.04;
- Офисный пакет LibreOffice v6.x**;**
- Браузеры: Google Chrome, Internet Explorer, Mozilla Firefox;
- Программа просмотра злектронных публикаций в формате PDF**:** Adobe Acrobat Reader DC v15.020.

Перечень специализированного программного обеспечения для изучения дисциплины представлен в таблице 9.1. В случае появления в течение семестра возможности использования в учебном процессе нового программного обеспечения (например, в результате заключения соответствующих договоров с производителями), оно также может рассматриваться в процессе изучения курса. Порядок доступа к нему доводится до студентов в рабочем порядке.

Специализированное программное обеспечение

Таблица 9.1

№	Наименование ПО	Назначение
1	Microsoft Visual Studio Professional 2019	Среда разработки приложений
2	Eclipse 2019	Среда разработки приложений
3	OpenVPN v2.3.11	Технологии виртуальной частной сети
4	Oracle VM VirtualBox 6.0.10	Программный продукт виртуализации для операционных систем

5	7-Zip v16.04	Средство свободной файловой архивации с высокой степенью сжатия данных
6	LibreOffice v6.x	Офисный пакет
7	Gpg4win Vanilla	Средство криптографической защиты и шифрования файлов

***Примечание:** программное обеспечения со свободными лицензиями. Скачивается студентами самостоятельно, устанавливается на виртуальные машины с использованием доступного в классах программного обеспечения для виртуализации (Oracle VM VirtualBox 6.0.10), после чего запускается в любом компьютерном классе.

10. Профессиональные базы данных и информационные справочные системы

1. Электронная библиотека диссертаций Российской государственной библиотеки (ЭБД РГБ)
2. Лицензионные материалы на сайте eLibrary.ru
3. Правовая БД «Консультант Плюс»
4. Правовая БД «Гарант»

11. Материально-техническое обеспечение

Для реализации дисциплины используются специальные помещения:

1. Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля, промежуточной и итоговой аттестации;

2. Помещения для самостоятельной работы обучающихся;

Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду НГУ.

Для проведения занятий лекционного типа предлагаются следующие наборы демонстрационного оборудования и учебно-наглядных пособий:

- комплект лекций-презентаций по темам дисциплины;

Таблица 11.1

№	Наименование	Назначение
1	Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления)	Для проведения лекционных занятий
2	Компьютерный класс (с выходом в Internet)	Для проведения лабораторных занятий и организации самостоятельной работы

Материально-техническое обеспечение образовательного процесса по дисциплине для обучающихся из числа лиц с ограниченными возможностями здоровья осуществляется согласно «Порядку организации и осуществления образовательной деятельности по образовательным программам для инвалидов и лиц с ограниченными возможностями здоровья в Новосибирском государственном университете».

Лист актуализации рабочей программы дисциплины
«Защита информации»

№	Характеристика внесенных изменений (с указанием пунктов документа)	Дата и № протокола Ученого совета ФИТ	Подпись ответственного
1	Актуализирован на 2020-2021 уч.год	22.07.2020 №77	
2	Актуализирован на 2021-2022 уч. год	26.04.2021 №80	
3	Дополнено применение дистанционных образовательных технологий П.5	31.08.2022 №87	

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования «Новосибирский национальный исследовательский
государственный университет» (Новосибирский государственный университет, НГУ)

Факультет информационных технологий

СОГЛАСОВАНО
Декан ФИТ НГУ

М.М. Лаврентьев
«03» июля 2019 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ
по дисциплине Защита информации

Направление подготовки: 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

Направленность (профиль): Программная инженерия и компьютерные науки

Квалификация: бакалавр

Форма обучения: очная

Год обучения: 4, семестр 7

Форма аттестации	Семестр
Дифференцированный зачет	7

Новосибирск 2019

Фонд оценочных средств промежуточной аттестации по дисциплине является **Приложением 1** к рабочей программе дисциплины «Защита информации», реализуемой в рамках образовательной программы высшего образования – программы бакалавриата 09.03.01 Информатика и вычислительная техника, направленность (профиль): Программная инженерия и компьютерные науки.

Фонд оценочных средств промежуточной аттестации по дисциплине утвержден решением ученого совета факультета информационных технологий, протокол № 75 от 02.07.2019.

Разработчики:
доцент кафедры компьютерных систем ФИТ,
кандидат технических наук, доцент Т.М.Пестунова

Заведующий кафедрой компьютерных систем ФИТ,
кандидат технических наук Б.Н. Пищик

Ответственный за образовательную программу:

доцент кафедры систем информатики ФИТ,

кандидат технических наук А.А. Романенко

1. Содержание и порядок проведения промежуточной аттестации по дисциплине

1.1. Общая характеристика содержания промежуточной аттестации

Промежуточная аттестация по дисциплине «Защита информации» проводится по завершению периода освоения образовательной программы (семестра) для оценки сформированности компетенций в части следующих индикаторов достижения компетенции (таблица П1.1).

Таблица П1.1

Код	Компетенции, формируемые в рамках дисциплины «Защита информации»	Семестр 7	
		Портфолио	Дифференцированный зачет
	УК 2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений		
УК 2.3	Владеть методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта, навыками работы с нормативно-правовой документацией	**+**	**+**
	ОПК 3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности		
ОПК-3.1	Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**+**	**+**
ОПК-3.2	Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**+**	**+**
ОПК-3.3	Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	**+**	
	ОПК 9. Способен осваивать методики использования программных средств для решения практических задач		

ОПК-9.1	Знать: классификацию программных средств и возможности их применения для решения практических задач		**+**

1.2. Порядок проведения промежуточной аттестации по дисциплине

Промежуточная аттестация проводится в форме дифференцированного зачёта (далее – диф.зачёта). Необходимым условием допуска к диф.зачёту является наличие положительной оценки по результатам всех выполненных и сданных в течение семестра заданий на лабораторных работах, которые составляют портфолио. Оценка за портфолио (средний балл по всем выполненным заданиям) учитывается при выставлении итоговой оценки за освоение дисциплины на диф.зачёте.

Диф.зачёт проводится в письменной форме: студенты получают билет из 6 вопросов с открытым ответом. Вопросы формулируются таким образом, чтобы ответы на них были краткими и занимали объём примерно полстраницы. На диф.зачёте не разрешается пользоваться литературой, калькуляторами и электронными устройствами доступа к информационным источникам.

Портфолио включает в себя работы, выполненные в рамках лабораторных занятий и самостоятельной работы, с учётом результатов защиты (обсуждения) в коллективном или индивидуальном формате:

1) результаты аналитической работы «Top-10 угроз ИТ-безопасности»;
2) результаты обсуждения проблемных ситуаций в контексте правового поля в области защиты информации;
3) доклад и презентация по результатам аналитической работы «уязвимости и угрозы Web-ресурсов»;
4) отчёт о разработке модели угроз, анализу рисков и частной политики безопасности для модельной информационной системы;
5) отчёт о лабораторной работе «сканеры защищённости автоматизированных рабочих мест и типовые средства безопасности системного и прикладного программного обеспечения»;
6) отчёт о лабораторной работе «программные реализации криптографических алгоритмов»;
7) отчёт о лабораторной работе «установка и настройка средств криптографической защиты информации, создание защищённого сетевого соединения (VPN)»;
8) эссе по теме «понятие и практические примеры безопасного программирования».

2. Требования к структуре и содержанию фонда оценочных средств промежуточной аттестации по дисциплине

Перечень оценочных средств, применяемых на каждом этапе проведения промежуточной аттестации по дисциплине, представлен в таблице П1.2.

Таблица П1.2

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1.	Портфолио	Целевая подборка работ студента, раскрывающая его индивидуальные образовательные достижения по дисциплине.	Структура портфолио
2.	Билет для дифференцированного зачета	Комплекс вопросов позволяющих оценивать и диагностировать знание фактического материала и умение правильно использовать специальные термины и понятия, узнавание объектов изучения в рамках определенного раздела дисциплины;	Список теоретических вопросов

2.1 Требования к структуре и содержанию оценочных средств аттестации

2.1.1 Требования к структуре и содержанию портфолио

Портфолио должно содержать отчётность в указанной форме по перечисленным ниже заданиям, включая результаты устной защиты. Студенты, которые по уважительным причинам отсутствовали на занятии, защищают свои работы преподавателю в индивидуальном порядке в назначенное им время.

Тема 1.

Задание 1.

Студенты готовят короткое устное сообщение (доклад) по результату самостоятельной аналитической домашней работы, в ходе которой они должны составить и обосновать свою версию «Top-10 угроз безопасности (в информационных технологиях)». Для ознакомления с угрозами и уязвимостями используются официальные каталоги и классификации угроз и уязвимостей, поддерживаемые отечественными и международными организациями, в частности: Open Web Application Security Project (OWASP), Web Application Security Consortium (WASC), Common Vulnerabilities and Exposures (CVE), Банк данных об угрозах ФСТЭК России.

Студенты представляют свое сообщение с опорой на краткие тезисы или презентацию, отвечают на вопросы преподавателя и других студентов.

Тема 2.

Задание 2.

Студентам предлагаются для анализа различные реальные или приближённые к реальным модельные ситуации, которые необходимо проанализировать и предложить решение, соответствующее действующим нормам законодательства в области защиты информации.

Анализ проблемных ситуаций проводится в форме обсуждения по соответствующим вопросам.

Оценка выставляется по результатам анализа студентом своего варианта и активности участия в обсуждении.

Варианты модельных проблемных ситуаций для подготовки к обсуждению.

1. Как в соответствии с законом о персональных данных (ПД) должна организовываться адресная рассылка информации потребителям услуг в целях маркетинга и рекламы? Как должен поступить человек в ситуации, когда он получает навязчивую адресную рассылку от банка с предложениями о кредитах, а банк отказывается исключить его из рассылки?

2. Что понимается под коммерческой тайной? Приведите примеры информации для организации, относящейся к системе управления организацией, которая может / не может составлять коммерческую тайну. Приведите примеры информации, которую целесообразно отнести к коммерческой тайне в организации, работающей в сфере программной инженерии.

3. Что обязан делать работодатель в целях охраны конфиденциальности информации, составляющей коммерческую тайну? При каких условиях меры по охране конфиденциальности информации признаются разумно достаточными?

4. Каковы принципы обработки персональных данных (ПД)? Приведите примеры реализации этих требований на примере известной Вам организации.

5. Каковы условия обработки персональных данных (ПД)? Опишите ситуации, когда кредитно-финансовая организация на законном основании может обрабатывать персональные данные клиентов без их согласия?

6. Какие права имеет обладатель информации, составляющей коммерческую тайну? Существуют ли случаи обязательного предоставления информации, составляющей коммерческую тайну?

7. Как осуществить трансграничную передачу персональных данных (ПД) с соблюдением требований закона о персональных данных? Ответ поясните на примере. В качестве примера можно рассмотреть ситуацию, когда студент обучается по программе «двойной диплом», в которой партнёром российской образовательной организации является зарубежный вуз.

8. Кто может являться оператором персональных данных (ПД)? Кто является оператором в ситуации, когда компания «Орг» передаёт на аутсорсинг в специализированную фирму «Бухгалтерия» функции бухгалтерского учёта и начисления заработной платы? Ответ обосновать.

9. В каких случаях для обработки персональных данных (ПД) не требуется согласия субъекта ПД? Опишите 2-3 такие ситуации на примере известной Вам организации (такие примеры есть в любой организации).

10. В каких случаях оператор вправе осуществлять обработку персональных данных (ПД) без уведомления Уполномоченного органа по защите прав субъектов ПД? Приведите конкретный пример такой ситуации.

11. Кто отвечает за соблюдение законности обработки персональных данных (ПД) на предприятии? Как, на Ваш взгляд, должен действовать сотрудник предприятия, если, по его мнению, при обработке ПД предприятием нарушаются его права как субъекта ПД?

12. Кто должен запрашивать согласие работников предприятия на обработку персональных данных (ПД) при их передаче для обработки другому оператору? Рассмотрите эту ситуацию на конкретном примере: предприятие «Пред» поручает охранной организации «Охр» осуществлять контроль доступа внешних посетителей на территорию «Орг», фиксируя идентификационные данные о них (ФИО, серия, номер и дата выдачи паспорта) в журнале разовых посещений.

13. Какие минимально необходимые требования должны быть выполнены в рамках режима коммерческой тайны? Рассмотрите этот вопрос на примере малого инновационного предприятия, которое занимается коммерциализацией разработок своих сотрудников и занимает половину этажа в технопарке. Как обеспечить требование конфиденциальности при передаче части информации, содержащей сведения, составляющие коммерческую тайну, организации-партнёру по бизнесу?

Список проблемных ситуаций может быть дополняться и корректироваться.

Тема 3.

Задание 3

Часть 1. Студенты выбирают один из предложенных преподавателем вариантов системного и прикладного программного обеспечения, применяемого для создания некоторого web-ресурса. Для выбранного варианта составить таблицу, в которой указаны следующие данные: название и версия компонента; номер и описание известных уязвимостей для компонента согласно базе данных CVE; классификация найденных уязвимостей по спискам OWASP TOP 10 и (или) WASC; сведения об уязвимости по банку угроз ФСТЭК России и связанные с этой уязвимостью возможные угрозы.

Необходимо учитывать, что уязвимость программного обеспечения, представленного в варианте, может относиться к нескольким его версиям. Например, уязвимость, характерная для версий MySQL с 5.0 до 5.1 будет относиться и к промежуточным версиям 5.0.1, 5.0.2 и т. д.

При проверке уязвимости, найденной в базе CVE, по классификациям OWASP или WASC, необходимо соотнести её описание в базе CVE с описанием класса OWASP или WASC. Например, уязвимость «CVE-2015-5346: Session fixation vulnerability in Apache Tomcat 7.x …» будет соответствовать классу «Фиксация сессии (session fixation)» в классификации WASC и «A2-Broken Authentication and Session Management» в OWASP TOP 10.

Примеры вариантов части 1 задания 3 приведены ниже. По согласованию с преподавателем студент может выбрать и другие средства реализации компонентов web-ресурса для исследования.

Примеры вариантов части 1 задания 3

№	Веб-сервер	Сервер баз данных	Интерпретатор сценариев
1	Apache Tomcat 8.4.2	MySQL 5.1.50	PHP 5.5.31
2	Apache Tomcat 7.0.65	PostgreSQL 8.4.19	PHP 5.6.18
3	Apache Tomcat 5.5.33	MySQL 5.0	Perl 5.8.2
4	Apache HTTP Server 2.4.18	MariaDB 5.1.1	PHP 5.5.21
5	Apache HTTP Server 2.2.0	Oracle MySQL 5.7.2	Ruby on Rails 3.2.22
6	nginx 0.5.6	SQLite 3.8.8	Ruby 1.9.3
7	nginx 0.8.36	MariaDB 5.5.34	PHP 7.0.2
8	Yaws 1.85	MongoDB 2.4.12	PHP 5.6.18
9	thttpd 2.25b0	SQLite 1.2.2	Perl 5.10.1
10	mini_httpd 1.19	PostgreSQL 9.0.19	Python 2.5
11	AOLserver 4.5.1	PostgreSQL 8.4.19	PHP 5.0.0
12	AOLserver 3.0	MongoDB 2.4.12	Ruby on Rails 3.0.17
13	AOLserver 3.2	MySQL 5.1.61	CPython 2.7.8
14	Microsoft Internet Information Services (IIS) 5.0	Microsoft SQL Server 2000	ASP.NET + Microsoft .NET Framework 1.1 SP1
15	Apache Tomcat 8.4.2	Oracle MySQL 5.7.2	Ruby on Rails 3.0.17
16	Apache Tomcat 7.0.65	PostgreSQL 8.4.19	PHP 5.5.31
17	Apache Tomcat 5.5.33	MariaDB 5.5.34	Perl 5.8.2
18	Apache HTTP Server 2.4.18	Oracle MySQL 5.5.19	Ruby on Rails 1.9.3
19	Apache HTTP Server 2.2.0	MySQL 5.1.50	PHP 5.0.0
20	nginx 0.5.6	SQLite 1.2.2	Ruby on Rails 3.2.22
21	nginx 0.8.36	MariaDB 5.1.1	PHP 5.6.18
22	Yaws 1.85	MySQL 5.1.61	PHP 5.5.21
23	thttpd 2.25b0	PostgreSQL 9.0.19	PHP 5.5.31

Задание 3

Часть 2.

Изучить, в чем заключаются уязвимости и атаки (см. список ниже). Выбрать и описать кратко принципы (схемы, примеры) реализации трёх атак из данного списка. Описание представить в виде 2-3 слайдов или в виде текста объемом ~ 0,5 стр. для каждого пункта. Подготовить краткое сообщение на занятии по описанным атакам.

Примеры атак для изучения: Brute Force, Buffer Overflow, Content Spoofing, Credential/Session Prediction, Cross-Site Scripting, Cross-Site Request Forgery, Denial of Service, Fingerprinting, Format String, HTTP Request Smuggling, HTTP Request Splitting, LDAP Injection, Null Byte Injection, Path Traversal, Predictable Resource Location, Remote File Inclusion (RFI), Session Fixation, SSI Injection, SQL Injection, URL Redirector Abuse, XPath Injection, XML Injection, Xquery Injection, Directory Indexing, Insecure Indexing, Insufficient Authentication, Insufficient Authorization, Insufficient Password Recovery, Server Misconfiguration.

В связи с непрерывным появлением новых уязвимостей и атак, студент по согласованию с преподавателем может выбрать для исследования иные атаки, не перечисленные в данном перечне.

Задание 4.

Для заданного преподавателем варианта информационной системы в организации:

- классифицировать ИСПДн по уровням защищённости;
- разработать модель потенциальных угроз;
- используя одну из стандартных методик провести оценку рисков и сформировать на её основе список актуальных угроз;
- разработать одну из политик безопасности для данного объекта;

Оформить отчёт о выполненной работе. Оценка выставляется на основании отчёта. При необходимости преподаватель может назначить дополнительно устную защиту.

Примерные варианты заданий для разработки моделей угроз.

1. Негосударственный пенсионный фонд находится в городе N (областной центр), есть филиал в г. М (райцентр). Общее число сотрудников – 40 человек. Три информационных системы персональных данных: ИСПДн бухгалтерии; ИСПДн по негосударственному пенсионному обеспечению участников Фонда; ИСПДн по обязательному пенсионному страхованию.

2. Территориальный фонд обязательного медицинского страхования N-ской области: общее число сотрудников 100 человек, ИСПДн, где ведется

обработка персональных данных сотрудников, состоит из трех рабочих станций и одного сервера, ИСПДн «Медис» - программа установлена на пяти рабочих станциях, идет обмен персональными данными с лечебно-профилактическими учреждениями и страховыми медицинскими компаниями.

3. Управление по делам ЗАГС N-ской области. Состоит из отделов ЗАГС г. N (областной центр), отделов ЗАГС городов области и отделов ЗАГС районов области (всего 43 отдела). Программа «ЗАГС-Находка» установлена на 310 рабочих станциях (во всех отделах), сервер.

4. Крупная транспортная компания – доставки грузов по России и ближнему зарубежью. ИСПДн «1С: Зарплата и управление персоналом» (порядка 3 000 записей); ИСПДн «Лоджистик» - включает данные о сотрудниках и клиентах: отправителях и получателях грузов, и представителях юридических лиц (порядка 75 000 записей). Центральный офис компании - в областном центре, 50 грузовых терминалов (филиалов) расположены в разных городах России, в каждом терминале по 1-2 компьютера с «Лоджистик».

5. Негосударственный учебный центр – языковые курсы. ИСПДн «1С Зарплата и управление персоналом» - 1 рабочее место. ИСПДн с реестром граждан, заключивших договор на обучение – 3 рабочих места.

6.Сеть частных стоматологических поликлиник – в 10 городах России 15 филиалов, всего 22 рабочих станции, на которых ведется обработка персональных данных обратившихся в поликлинику граждан, сервер в центральном офисе.

7. Министерство здравоохранения N-ской области. ИСПДн «Кадры и аттестация врачей» 1 сервер и 8 рабочих мест. ИСПДн «Обращения граждан» - 7 рабочих мест. ИСПДн «Льготные лекарства»- 5 рабочих мест.

8. Служба занятости населения N-ской области и 42 центра занятости населения по области. Программа «Катарсис» установлена в общей сложности на 320 рабочих станциях, сервер – в каждом из центров занятости.

9. Областной фонд развития жилищного строительства N-ской области. ИСПДн – бухгалтерии (сотрудников 20 человек) и ИСПДн «предоставление гражданам льготных бюджетных займов и социальных выплат для приобретения или строительства жилья» (участников Фонда 10 000 человек). Располагается на двух этажах одиннадцатиэтажного здания в областном центре и один филиал в городе областного подчинения.

Недостающая в описании варианта информация моделируется студентом, в затруднительных случаях он может получить консультацию преподавателя.

Студент может по согласованию с преподавателем может сформировать индивидуальный вариант, отсутствующий в указанном перечне, выбрав другой профиль организации и другие информационные системы в соответствии со своим опытом и интересами. Помимо ИСПДн могут рассматриваться и классифицироваться государственные информационные системы, объекты критической инфраструктуры, а также информационные системы в различ-

ных отраслях, для которых могут быть применены известные классификации или профили защиты.

Тема 4.

Задание 5.

Используя свободное или доступное в НГУ сертифицированное программное обеспечение для сканирования сетей, определить уязвимости хоста (список имеющегося в НГУ специализированного программного обеспечения указан в рабочей программе дисциплины). В качества хоста используется предоставленная преподавателем виртуальная машина. Может быть также использован любой сетевой компьютер, к которому у студента имеется законный доступ (домашний компьютер, личный ноутбук и т. п.)

По результатам оформляется первая часть отчёта, в котором сравниваются результаты, полученные разными инструментами и даётся описание и способы устранения выявленных уязвимостей.

Во второй части отчёта даётся краткая характеристика встроенных инструментов безопасности в операционных системах, примеры их реализации в ОС Windows (доступной версии) и Linux, проводится анализ возможности использования этих инструментов для нейтрализации угроз, обусловленных выявленными уязвимостями.

Отчёт сдаётся преподавателю и защищается в индивидуальном формате.

Тема 5.

Задание 6.

Реализовать криптографический или стенографический алгоритм. Вариант алгоритма выдаётся преподавателем или выбирается студентом в инициативном порядке при условии обязательного согласования выбранного варианта с преподавателем.

По результатам работы оформляется отчёт, в котором описывается назначение алгоритма, особенности реализации, тестовые задачи и прилагается текст программы.

Защита производится в индивидуальном формате, включает демонстрацию работоспособности программы и ответы на вопросы по её работе и тексту отчёта.

Задание 7.

Создать защищённое соединения с применением доступного программного обеспечения: OpenVPN или аналоги.

Оформить отчёт с подробным описанием конфигурации защищённой сети и настроек соответствующих механизмов защиты.

Защита производится в индивидуальном формате, включает демонстрацию работоспособности программы и ответы на вопросы по её работе и тексту отчёта.

Тема 8.

Задание 8.

Проанализировать современные интерпретации понятия «безопасное программирование». Систематизировать все аспекты, которые охватываются данным понятием. Привести соответствующие примеры. Написать краткое эссе на тему: «Суть понятия и примеры безопасного программирования». Подготовить краткое сообщение по материалам эссе.

Оценка за задание выставляется по результатам проверки эссе и оценивания устного выступления и качества ответов на вопросы преподавателя и слушателей по сделанному докладу.

2.1.2 Оценочные средства при проведении дифзачёта.

Форма и перечень вопросов билета дифференцированного зачета приведены в таблице П 1.3. При составлении билетов два вопроса из категории 1 в одном билете должны относиться к разным сферам правового регулирования в сфере защиты информации.

Форма билета к дифференцированному зачету

Таблица П1.3

Новосибирский государственный университет
Дифференцированный зачет

Защита информации
наименование дисциплины

09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА
Программная инженерия и компьютерные науки
наименование образовательной программы

БИЛЕТ К ДИФФЕРЕНЦИРОВАННОМУ ЗАЧЕТУ №

1. Вопрос из категории 1
2. Вопрос из категории 2
3. Вопрос из категории 3
4. Вопрос из категории 4
5. Вопрос из категории 5
6. Вопрос из категорий 1, 2 или 3 (на выбор преподавателя)

Составитель
_____ Ф.И.О
(подпись)

Ответственный за образовательную программу
_____ А.А. Романенко

(подпись)

«____»_____20 г.

В билет включаются вопросы из разных категорий.

Формулировка вопроса в билете может охватывать часть формулировки пунктов из таблицы П1.4, либо объединять несколько пунктов (в зависимости от охватываемого вопросом объёма информации)

Перечень примерных вопросов для диф.фзачёта, структурированный по категориям, представлен в таблице П1.4

Таблица П1.4

Категория	Примерные вопросы
Категория 1 УК 2.3 (2).	Закон об информации, информационных технологиях и защите информации 1. Дать определение и привести примеры, поясняющие основные понятия, используемые в законе: информация, информационные технологии, информационная система (далее- ИС), информационно-телекоммуникационная сеть, электронное сообщение, документированная информация, доступ к информации, обладатель информации, распространение и предоставление информации, оператор информационной системы. 2. Классификация информации в зависимости от категории доступа к ней, от порядка её распространения и предоставления. Основания для ограничения доступа к информации. 3. Права и обязанности оператора по использованию информации и её защите. Требования к распространению общедоступной информации. Информация, доступ к которой не может быть ограничен. 4. Требования по защите информации, предъявляемые к организаторам её распространения в сети Интернет. 5. Понятие защиты информации. Обязанности обладателя информации по выполнению требований по защите информации. 6. Государственные, муниципальные и иные ИС. Требования к информационным технологиям государственных ИС. Понятие реестра Российского программного обеспечения, условия включения программ в этот реестр. Закон о государственной тайне. 7. Понятие государственной тайны, допуска к ней, грифа секретности. Области деятельности, информация которых может составлять государственную тайну. 8. Принципы отнесения информации к государственной тайне, степени секретности информации, составляющей государственную тайну. Ограничение прав собственности юридических и физических лиц на информацию в связи с её засекречиванием. 9. Допуск к сведениям, составляющим государственную тайну, должностных лиц и граждан. Формы допуска. Требования для допуска организаций, предприятий и учреждений к работе со сведениями, составляющими государственную тайну. Законодательство о персональных данных. 10. Основные понятия закона: персональные данные (далее — ПД), оператор, обработка ПД, обезличивание ПД, распространение и предоставление ПД, информационная система ПД (далее — ИСПДн), трансграничная передача ПД. 11. Принципы и условия обработки ПД. Согласие на обработку ПД. Специальные и биометрические ПД, особенности их обработки.

	12. Уведомление об обработке ПД и реестр операторов. Уполномоченный орган по обеспечению прав субъектов ПД (Роскомнадзор), его функции и полномочия. Формы проведения проверок, наиболее типичные выявляемые нарушения. 13. Лицо ответственное за организацию обработки ПД и его обязанности. Права субъекта ПД. Обязанности оператора. 14. Основные меры, направленные на достижение безопасности ПД 15. Влияние Конвенции Совета Европы №108 и связанных с ней директив на развитие российского законодательства в сфере персональных данных. 16. Проблемы защиты персональных данных в условиях цифровизации экономики и общественной жизни. Влияние принятого странами Евросоюза нового документа GDPR (General Data Protection Rools) на российское правовое поле. Закон о коммерческой тайне. 17. Понятие коммерческой тайны (далее - КТ). Информация, составляющая КТ. Законное и незаконное получение информации, составляющей КТ. Права обладателя информации, составляющей КТ, по её защите. 18. Меры по охране конфиденциальности КТ, которые необходимы для установления режима КТ. 19. Критерии разумной достаточности мер по охране конфиденциальности информации, составляющей КТ. Меры, принимаемые обладателем КТ по охране её конфиденциальности в рамках трудовых отношений. Закон о безопасности критической информационной инфраструктуры. 20. Основные понятия закона: автоматизированная система управления, критическая информационная инфраструктура (далее — КИИ), объекты КИИ, субъекты КИИ, безопасность КИИ, значимый объект КИИ, компьютерный инцидент, компьютерная атака. 21. Критерии и возможные результаты категорирования объектов КИИ. Понятие и назначение реестра объектов КИИ. Уполномоченный орган федеральной исполнительной власти по вопросам обеспечения безопасности КИИ. 22. Закон об электронной подписи. 23. Основные понятия закона: электронная подпись (далее - ЭП), ключ ЭП, ключ проверки ЭП, удостоверяющий центр (далее - УЦ), сертификат ключа проверки ЭП, квалифицированный сертификат ключа проверки ЭП, средства ЭП. 24. Виды ЭП, их свойства и способность обеспечить контроль целостности сообщения, аутентификации автора, неотказуемость. Примеры реализации ЭП разных видов. 25. Условия признания электронных документов, подписанных разными видами ЭП, равнозначными документам на бумажном носителе с собственноручной подписью. 26. Условия использования простой ЭП. Обязанности участников взаимодействия при использовании усиленных ЭП. 27. Понятие Удостоверяющего центра (УЦ). Функции УЦ. 28. Понятие аккредитованного УЦ. Требования к аккредитованным УЦ. Официальный интернет ресурс о деятельности аккредитованный удостоверяющих центров. 29. Понятие квалифицированного сертификата. Условия прекращения

	действия сертификата. 30. Обязанности владельца квалифицированного сертификата по его использованию и действия при подозрении на нарушение конфиденциальности ключа подписи. <u>Закон о лицензировании отдельных видов деятельности.</u> 31. Виды деятельности в области защиты информации, подлежащие лицензированию. 32. Уполномоченные федеральные органы госвласти, осуществляющие лицензирование, а) права деятельности в области технической защиты информации; б) права деятельности в области защиты информации с использованием шифровальных (криптографических) средств; в) права деятельности в области работы с информацией, содержащей сведения, составляющие государственную тайну. 33. Уполномоченные федеральные органы госвласти, осуществляющие сертификацию, а) технических средств защиты информации; б) шифровальных (криптографических) средств защиты информации. <u>Другие НПА.</u> 34. Уполномоченный орган по обеспечению безопасности объектов КИИ (указ Президента РФ от 25.11.2017 №569) 35. Понятие государственной системы обнаружения и предупреждения компьютерных атак (ГосСОПКА) на КИИ (указ Президента РФ от 03.02.2012 №803) 36. Задачи системы ГосСОПКА и уполномоченный федеральный орган госвласти в данной области (указ Президента РФ от 22.12.2017 №620) 37. Уголовная ответственность за преступления в сфере компьютерной информации, коммерческой и профессиональных тайн (УК РФ, ст. 183, 272, 273, 274, 274.1) 38. Административная ответственность за правонарушения в сфере защиты информации и соблюдения прав субъектов ПД (КоАП РФ, ст. 13.6, 13-11-13.14, 13.33) 39. Обеспечение работодателем безопасности персональных данных работника (Трудовой кодекс, гл. 14). 40. Информация конфиденциального характера (указ Президента РФ №188). Информация ограниченного доступа, на содержащей сведения, составляющие гостайну (примеры информации и источники для составления перечня такой информации в организациях).
Категория 2 УК 2.3. (1,3,4)	1. Основные понятия информационной безопасности и защиты информации (по ГОСТ 50922-2006, ГОСТ 51275-2006, ГОСТ 53114-2008). 2. Доктрина информационной безопасности: статус и цели принятия документа, понятия «информационная сфера» и «информационная безопасность», угроза информационной безопасности, основные классы угроз актуальных угроз информационной безопасности России, примеры угроз (3 угрозы на выбор обучающегося, наиболее значимые с его точки зрения). 3. Этапы развития проблематики информационной безопасности в зависимости от уровня информационных технологий. 4. Конфиденциальность, целостность, доступность информации. Примеры других значимых свойства информации и способы их оценки. 5. Актуальные направления информационной безопасности в условиях цифровизации. Проблема личной информационной безопасности.

	6. Угрозы безопасности информации: определение, параметры классификации угроз, примеры типовых угроз в информационных технологиях, примеры угроз утечки информации по техническим каналам. 7. Принципы защиты информации: суть и примеры их практического применения. 8. Понятие системы защиты информации. Функции системы защиты информации и примеры их реализации. 9. Контекст обеспечения информационной безопасности и определение целей защиты информации. 10. Анализ информационных активов и определение состава защищаемой информации. 11. Понятие риска. Действия по отношению к рискам. Основные этапы управления рисками, задачи и особенности на каждом этапе. 12. Понятие модели угроз. Основные параметры идентификации угроз. Примеры. 13. Базовая модель угроз безопасности в информационных системах персональных данных: общая структура, понятие типовых моделей угроз, практическое значение. 14. Понятие уязвимости. Источники информации об актуальных угрозах и уязвимостях. Рейтинги уязвимостей. 15. Методы выявления уязвимостей информационных систем (ГОСТ Р 56545-2015). 16. Выявление уязвимостей и угроз с использованием bdu.fstec.ru. Расчёт вектора CVSS. Программное средство ScanOVAL. 17. Угрозы непосредственного доступа в компьютерную среду. 18. Угрозы сетевого (межсетевого) взаимодействия 19. Угрозы доступности информации. 20. Угрозы целостности информации. 21. Угрозы, связанные с социальной инженерией. 22. Методы выявления уязвимостей информационных систем. 23. Понятие модели нарушителя. Примеры методик составления моделей нарушителя и угроз, доступных нарушителям разных категорий. 24. Понятие потенциала нарушителя. Примеры угроз, реализуемых нарушителями с разным потенциалом. 25. Оценка рисков: общий подход и примеры методик. 26. Понятие политики безопасности. Структура политик безопасности в соответствии с ГОСТ Р ИСО\МЭК 27002-2012 27. Вопросы, выносимые в политики безопасности верхнего, среднего и нижнего уровня. Вопросы информационной безопасности во взаимосвязи с жизненным циклом ИС. 28. Требования по информационной безопасности при управлении персоналом. 29. Меры физической защиты носителей информации и информационной инфраструктуры. 30. Основные организационные меры обеспечения безопасности парольной и ключевой информации. 31. Типовые аспекты, отражаемые в политиках категории «обеспечение соответствия требованиям» («complience») 32. Основные организационные меры по обеспечению непрерывности бизнеса. 33. Понятие аудита информационной безопасности, цели, краткая характеристика процесса, примеры стандартов аудита.

	34. Организация процесса расследования инцидентов информационной безопасности (ГОСТ Р ИСО\МЭК 18044-2007).
Категория 3. ОПК 3.1 (6)	1. Основные понятия субъектно-объектного подхода: субъекты, объекты, контейнеры, сущности, доступ, информационный поток. Классификация моделей управления доступом. 2. Принципы дискреционного и мандатного управления доступом, их достоинства и недостатки, примеры реализации в ОС, СУБД и средствах защиты информации. 3. Модели ХРУ: основные компоненты, операторы и команды, теоремы безопасности и вытекающие из них ограничения использования. 4. Концепция модели типизированных матриц доступа (далее - ТМД): исходные данные модели, граф создания, история, теоремы о проверке безопасности моделей ТМД и принципы алгоритмов проверки безопасности исходного состояния. 5. Концепция модели “Take-grant”: назначение, исходные данные и структура модели, правила преобразования графа доступов, формализация свойств безопасности в модели “Take-grant”, примеры практического применения. 6. Концепция расширенной модели “Take-grant”: назначение, исходные данные и структура модели, правила «де-юре» и «де-факто», правила анализа информационных потоков, формализация свойств безопасности. 7. Концепция модели Белла — Ла Падулы: назначение, исходные данные и структура модели, правила функционирования модели, свойства безопасности модели Белла — Ла Падулы, концепции алгоритмов проверки безопасности, уязвимости модели. 8. Концепция модели контроля целостности Кларка-Вилсона: исходные данные, понятие процедур контроля целостности и правил преобразования, основные принципы контроля отсутствия ненадлежащих изменений и примеры их реализации в реальных системах. 9. Концепция ролевого управления доступом (RBAC): основные понятия, исходные данные и концептуальная модель RBAC, примеры реализации в программном обеспечении информационных систем. 10. Иерархия ролей RBAC. Отношение наследования и его свойства. Примеры реализации в программном обеспечении информационных систем. 11. Статические и статические и динамические ограничения (виды, примеры). Примеры реализации в программном обеспечении информационных систем. 12. Модель администрирования ролей (ARBAC): основные компоненты модели, исходные данные и концептуальная модель ARBAC. 13. Основные функции для администрирования ролей и примеры их реализации. 14. Понятие идентификации и аутентификации, основные подходы к их созданию, понятие многофакторной аутентификации, примеры. 15. Парольные системы, способы хранения паролей, угрозы и уязвимости, меры защиты. 16. Аутентификация на основе “токенов”: принципы действия, возможные атаки, меры защиты. 17. Биометрическая аутентификация: применяемые характеристики, уязвимости и атаки, меры защиты.

	18. Протоколы аутентификации: обзор и примеры. Аутентификация на основе одноразовых паролей, система SKEY. 19. Основные понятия криптографии, принципы замены и перестановки. Примеры. 20. Классические шифры замены (шифр Цезаря, Вижинера, простой замены) и их уязвимости 21. Понятие о криптоанализе. Виды криптоанализа. 22. Понятие и условия абсолютно стойкого шифра. Шифр Вернама. Понятие ложных ключей. Расстояние единственности. 23. Блочные шифры: понятие, примеры, сферы применения. Режимы блочных шифров. Понятие имитовставки. 24. Поточные шифры. понятие, примеры, сферы применения. Особенности реализации. 25. Назначение и принципы работы стеганографических алгоритмов. LSB-внедрение. 26. Односторонние функции: понятие, свойства, примеры. Принцип асимметричной криптографии, сильные стороны и уязвимости. 27. Алгоритм Дифи-Хеллмана: назначение, пошаговая схема, примеры практического использования, уязвимости. 28. Алгоритм RSA: назначение, пошаговая схема, примеры практического использования, уязвимости 29. Понятие электронной цифровой подписи. Примеры алгоритмов. Соотношение данного понятия с понятием электронной подписи, применяемом в законодательстве. 30. Атака посредника и инфраструктура открытых ключей. 31. Хеш-функции: типы (ключевые и бесключевые), их основные свойства и сфера применения. 32. Понятие об эллиптических кривых. Операции в группе точек на эллиптической кривой. Аналоги труднорешаемых задач на эллиптических кривых и практические преимущества соответствующих алгоритмов. 33. Основные криптографические стандарты (обзорно) и их назначение. 34. Понятие протокола «нулевого знания». Свойства протокола. Примеры протоколов и их практического применения. 35. Принципы квантовой криптографии, преимущества и уязвимости квантового распределения ключей. Практические достижения и перспективы. 36. Протоколы электронных платежей: виды и примеры электронных денег, проблемы безопасности, практические аспекты применения. 37. Технологии «блок-чейн»: общие принципы и проблемы безопасности. Практическое применение и перспективы. 38. Классификации вредоносных программ. 39. Принципы сигнатурного и эвристического анализа. Примеры. 40. Обнаружение вторжений: принципы и способы выявления компьютерных атак.
Категория 4 ОПК 3.1 (7)	1. Проблема защиты программного обеспечения. Объекты защиты. Технологическая и эксплуатационная безопасность. 2. Основные классы и примеры угроз информационной безопасности при разработке программного обеспечения. 3. Понятие безопасного программного обеспечения. Основные принципы обеспечения безопасности программного обеспечения.

	4. Требования к применению методик безопасного программирования при разработке программного обеспечения, оцениваемого на основе требований по разным ОУД. 5. Уязвимости программного обеспечения, источники их возникновения. 6. Угрозы безопасности и меры по разработке безопасного программного обеспечения на этапе анализа требований к программному обеспечению, их цели и результаты. 7. Угрозы безопасности и меры по разработке безопасного программного обеспечения при проектировании программного обеспечения, их цели и результаты. 8. Угрозы безопасности и меры по разработке безопасного программного обеспечения при конструировании и комплексировании программного обеспечения, их цели и результаты. 9. Угрозы безопасности и меры по разработке безопасного программного обеспечения на этапе квалификационного тестирования программного обеспечения, их цели и результаты. 10. Угрозы безопасности и меры по разработке безопасного программного обеспечения при выполнении инсталляции программы и поддержки приёмки программного обеспечения, их цели и результаты. 11. Угрозы безопасности и меры по разработке безопасного программного обеспечения при решении проблем программного обеспечения, возникающих в ходе эксплуатации, их цели и результаты 12. Угрозы безопасности и меры по разработке безопасного программного обеспечения в процессе управления документацией и конфигурацией программного обеспечения, их цели и результаты. 13. Угрозы безопасности и меры по разработке безопасного программного обеспечения в процессе управления инфраструктурной средой разработки программного обеспечения, их цели и результаты. 14. Угрозы безопасности и меры по разработке безопасного программного обеспечения в процессе управления человеческими ресурсами, их цели и результаты. 15. Тестирование программного обеспечения на его защищённость: виды тестирования, их цели, критерии успешности. Понятие о фаззинге программ. 16. Защита программного обеспечения от несанкционированного исследования программ: классификация способов и их краткая характеристика. 17. Понятие об обфускации программ, классификация методов в зависимости от объекта обфускации, их смысл и примеры. 18. Понятие о методах деобфускации программ: статический и динамический анализ, принципы и ограничения статического анализа, примеры приёмов динамического анализа. 19. Методы защиты программ от несанкционированного копирования: основные классы методов и их краткая характеристика (суть). 20. Понятие защищённых операционных систем: общие подходы к разработке, характеристика архитектуры защищённой ОС (на примере по выбору обучающегося)
Категория 5 ОПК 9.1	1. Уровни защищённости ИСПДн и критерии классификации, основные группы мер защиты в ИСПДн, понятие базового, адаптированного, уточненного наборов мер защиты информации в ИСПДн. 2. Классы защищённости государственных ИС: критерии классифика-

	ции и примеры систем разных классов, выбор мер защиты в государственных ИС разных классов. 3. Связь классификации государственных ИС и ИСПДн. Определение требований по защите информации, являющихся ИСПДн и одновременно государственной ИС. 4. Принципы категорирования объектов КИИ. Уровни значимости объектов КИИ, обзор требований безопасности для значимых объектов КИИ. 5. Принципы классификации средств вычислительной техники (далее — СВТ) и автоматизированных систем по классам защищённости, структура классов и основные группы показателей защищённости, примеры их реализации. 6. Классификация защищённости межсетевых экранов, основные группы показателей защищённости, рекомендации по применению классифицированных межсетевых экранов в информационных системах различного назначения, примеры программных и программно-аппаратных реализаций межсетевых экранов. 7. Классификация программного обеспечения по уровню контроля отсутствия недекларированных возможностей (далее — НДВ): требования к документированию ПО, требования к методам анализа программного кода, обзор классов защищённости. 8. Подсистемы антивирусной защиты: основные функции, используемые методы, классификация ФСТЭК по типам, группы требований для разных классов, примеры программного обеспечения. 9. Подсистемы обнаружения вторжений: назначение, основные возможности, основные критерии классификации и группы требований для разных классов, примеры программного обеспечения. 10. Подсистемы анализа защищённости: назначение, типовая функциональность, примеры программного обеспечения. 11. Системы предотвращения внутренних утечек (DLP-системы): назначение, виды DLP-систем и их основные возможности, используемые методы и алгоритмы. 12. Средства доверенной загрузки и подсистемы защиты от несанкционированного доступа в компьютерные системы: назначение, типовые функции и возможности, используемые методы и модели. 13. Принципы классификации криптографических средств защиты информации. 14. ГОСТ Р ИСО\МЭК 15408: назначение и целевая аудитория, принципиальные отличия от всех остальных стандартов, понятие объекта оценки, контекст безопасности. 15. Понятие профиля защиты, назначение и структура. 16. Понятие задания по безопасности, назначение и структура 17. Обобщённая схема формирования требований по безопасности при разработке и оценке программного обеспечения и информационных систем в соответствии с ГОСТ Р ИСО\МЭК 15408. 18. Основные классы функциональных требований безопасности, примеры семейств функциональных требований и структура описания компонентов (на примере одного из компонентов, выбор – на усмотрение обучающегося) 19. Основные классы требований доверия, примеры семейств требований доверия и структура описания компонентов (на примере одного из компонентов, выбор – на усмотрение обучающегося)

	20. Понятие оценочного уровня доверия (далее - ОУД). Обзор системы ОУД в ГОСТ Р ИСО\МЭК 15408. 21. Краткая характеристика ОУД 1 и ОУД 2, рекомендации по их применению. 22. Структура требований безопасности в ГОСТ Р ИСО\МЭК 15408. Примеры требований разных классов и семейств. 23. Основные стадии создания автоматизированных (информационных) систем в защищённом исполнении и содержание соответствующих работ.

Набор билетов к дифференцированному зачету формируется и утверждается в установленном порядке в начале учебного года при наличии контингента обучающихся, завершающих освоение дисциплины «Защита информации» в текущем учебном году.

3. Критерии оценки сформированности компетенций в рамках промежуточной аттестации по дисциплине

Таблица П1.5

Шифр компетенций	Структурные элементы оценочных средств	Показатель сформированности	Не сформирован (2 балла)	Пороговый уровень (3 балла)	Базовый уровень (4 балла)	Продвинутый (5 баллов)
УК 2.	Портфолио Вопросы категорий 1 и 2 в билете для дифзачёта	УК 2.3. Владеть методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта, навыками работы с нормативно-правовой документацией	Фрагментарные знания законодательства в сфере защиты информации, отсутствие целостного представления о правом регулировании вопросов защиты информации. Слабо ориентируется в современной проблематике информационной безопасности. Фрагментарно знает методологические основы и организационные аспект защиты информации. Допускает множественные ошибки в понятийном аппарате предметной области, в выполнении заданий портфолио и в изложении ответов на вопросы на дифзачёте. Как правило, не способен исправить допущенные ошибки	Знает, в целом, сферу действия изученных законов, но затрудняется при их использовании для обоснования практических ситуаций Понимает современную проблематику информационной безопасности. Имеет общее представление о методологических и организационно-управленческих аспектах предметной области. Допускает существенные ошибки при выполнении заданий портфолио и ответах на вопросы дифзачёта по методологическим и организационно-управленческим аспектам предметной области, часть их может исправить с подсказкой преподавателя	Знает сферу действия и основные положения изученных нормативно-правовых актов. Как правило, может оценить необходимость их использования в конкретных ситуациях, но допускает ошибки в процессе применения. При подсказке преподавателя может разобраться в ситуации. В целом, умеет использовать справочно-правовые системы, научные и учебные источники, электронные ресурсы по исследуемым вопросам. Знает понятийный аппарат, допускает ошибки в заданиях портфолио и ответах на вопросы дифзачёта по методологическим и организационно-управленческим аспектам предметной области, большинство из них мо-	Уверенно знает сферу действия и основные положения изученных нормативно-правовых актов, имеет целостное представление о правовом регулировании сферы защиты информации. Способен разрешить проблемную ситуацию, опираясь на изученные законы и нормативно-правовые акты. Для актуализации знаний эффективно использует справочно-правовые системы, научные и официальные электронные ресурсы уполномоченных органов власти. Уверенно знает понятий аппарат, методологические и организационные аспекты предметной области. Возможны отдельные несуще-

			даже при наводящей подсказке преподавателя.		жет исправить при наводящих подсказках преподавателя.	ственные ошибки, которые способен исправить самостоятельно.
ОПК-3	Портфолио Вопросы категории 3,4 в билете для дифзачёта	ОПК 3.1. Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных	Имеет несистемные, очень поверхностные знания формальных моделей управления доступом, методов аутентификации, основ криптографической защиты информации, стеганографии, принципов антивирусной защиты, обнаружения вторже-	Знает с отдельными существенными ошибками основные виды формальных моделей управления доступом, принципы и алгоритмы их функционирования принципы и примеры методов аутентификации, основные классы методов и примеры алгоритмов криптографи-	Знает, в целом, основные виды формальных моделей управления доступом, принципы и алгоритмы их функционирования принципы и примеры методов аутентификации, основные классы методов и примеры алгоритмов криптографической защиты информации,	Знает основные виды моделей управления доступом, принципы и алгоритмы их функционирования, принципы и примеры методов аутентификации, основные классы методов и примеры алгоритмов криптографической защиты информации,

		технологий и с учетом основных требований информационной безопасности	ний. Слабое понимание проблем защиты программного обеспечения и «безопасного программирования». Допускает множественные ошибки при выполнении заданий портфолио и в изложении ответов на вопросы на дифзачёте. Как правило, не способен исправить допущенные ошибки даже при наводящей подсказке преподавателя.	ческой защиты информации, принципы стеганографии, антивирусной защиты, обнаружения вторжений. Имеет общее представление о проблемах защиты программного обеспечения и сути «безопасного программирования». Допускает ошибки при выполнении заданий портфолио и ответах на вопросы дифзачёта соответствующих категорий, часть их может исправить с подсказкой преподавателя .	принципы и примеры алгоритмов стеганографии, принципы антивирусной защиты, обнаружения вторжений, принципы и примеры методов выявления уязвимостей и анализа защищённости. Понимает в целом проблематику защиты программного обеспечения и суть «безопасного программирования». Допускает ошибки в заданиях портфолио и ответах на вопросы соответствующих категорий, большинство из них может исправить при наводящих вопросах и незначительных подсказках преподавателя.	принципы и примеры алгоритмов стеганографии, принципы антивирусной защиты, обнаружения вторжений Понимает угрозы в процессе в процессе разработки ПО, источники их возникновения и меры защиты, проблематику защиты программного обеспечения имеет целостное представление о принципах безопасного программирования. Способен убедительно аргументировать ответ. Возможны отдельные несущественные ошибки, которые способен исправить самостоятельно или при наводящих вопросах преподавателя.
	Портфолио	ОПК 3.2. Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиогра-	Имеет слабое представление об основных источниках требований к защите информации в автоматизированных (информационных) системах.	Знает основные источники требований к защите информации в АС и ИС. Имеет общее понятие о базовых стандартах и методиках ИТ-безопасности, процессе	Знает основные источники требований к защите информации в АС и ИС. Способен, с некоторыми погрешностями, опираться при разработке ПО на базовые стан-	Уверенно знает основные подсистемы и средства защиты информации и критерии их применения для конкретных ИС. Способен обосновать вы-

		фической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Не способен обосновать выбор необходимого программного обеспечения, опираясь на понимание проблем безопасности информации, классификаций ИС и средств защиты информации, ошибается с выбором методических документов и стандартов, актуальных для поставленной задачи. Не может корректно изложить практические примеры безопасного программирования. Умеет разработать и программно реализовать отдельные алгоритмы для решения задач защиты информации, но допускает ошибки, не позволяющие добиться полного выполнения поставленных заданий.	создания защищённых автоматизированных систем. Не всегда способен определить проблемы безопасности информации. Не всегда верно выбирает подходящие классификации, методики и стандарты, актуальные для поставленной задачи. Имеет общее представление об основах безопасного программирования и защиты ПО, но неубедительно, с ошибками представляет практические примеры. Умеет, как правило, разработать и программно реализовать отдельные алгоритмы для задач защиты информации в соответствии с поставленной целью. Понять и исправить ошибки может только при подсказках преподавателя.	дарты ИТ-безопасности и методики классификации, основные этапы создания автоматизированных систем в защищённом исполнении. Как правило, может обосновать выбор ПО на основе классификаций ИС и средств защиты информации, допускает отдельные ошибки при применении методик, нормативно-методических документов и стандартов, актуальных для поставленной задачи. Понимает практические аспекты безопасного программирования и защиты программного обеспечения. Умеет, как правило, разработать и программно реализовать алгоритмы для решения задач защиты информации в соответствии с поставленной целью. Способен при небольшой подсказке преподавателя исправить ошибки.	бор необходимого ПО, опираясь на понимание угроз и уязвимостей, нормативные требования и классификации ИС и средств защиты информации. Способен продемонстрировать и обосновать практические применения различных аспектов безопасного программирования и защиты программного обеспечения. Умеет разработать и программно реализовать алгоритмы для решения задач защиты информации в соответствии с поставленной целью. Допускаются отдельные непринципиальные погрешности, которые способен исправить самостоятельно или при незначительной подсказке преподавателя.
	Портфолио дифзачёт	ОПК 3.3 Владеть: навыками подготовки обзоров, ан-	Способен осваивать на уровне пользователя и администрато-	Не в полной мере научился осваивать программные средства	Способен в целом осваивать на уровне пользователя и администрато-	Способен достаточно глубоко осваивать на уровне пользователя

		нотаций, составления рефератов, научных докладов, публикаций и библиографии по научно- исследовательской работе с учетом требований информационной безопасности	ра программные средства для обеспечения безопасности в компьютерной и сетевой среде на примере установки, администрирования и использования подсистем средств защиты информации в соответствии с заданиями лабораторных и практических заданий, предусмотренных в ходе учебного процесса. Не умеет правильно применять терминологию и основные понятия предметной области, что проявляется в профессионально неграмотном изложении результатов в отчётах, эссе, докладах, выступления, ответах на вопросы преподавателя.	для обеспечения безопасности в компьютерной и сетевой среде допускает ошибки при установке, администрировании и использовании подсистем и средств защиты информации по тематике лабораторных и практических заданий, предусмотренных в ходе учебного процесса. В отчётах, эссе, докладах, выступлениях, ответах на вопросы преподавателя, а также в процессе дифференцированного зачёта часто встречаются ошибки в употреблении и толковании терминов по защите информации.	ра программные средства для обеспечения безопасности в компьютерной и сетевой среде на примере установки, администрирования и использования подсистем средств защиты информации в соответствии с заданиями лабораторных и практических заданий, предусмотренных в ходе учебного процесса, но встречаются отдельные ошибки, приводящие к некорректным результатам. В отчётах, эссе, докладах, выступлениях, ответах на вопросы преподавателя отмечаются отдельные ошибки в употреблении и толковании терминов по защите информации.	и администратора программные средства для обеспечения безопасности в компьютерной и сетевой среде на примере установки, администрирования и использования подсистем и средств защиты информации в соответствии с заданиями лабораторных и практических заданий, предусмотренных в ходе учебного процесса. При представлении результатов в форме отчётов, эссе, докладов и выступлений, ответов на вопросы преподавателя, в том числе на диффзачёте, показал уверенное владение профессиональными терминами предметной области.
ОПК-9	Портфолио Вопросы категории 5 в билете для дифзачёта	ОПК-9.1. Знать: классификацию программных средств и возможности их примене-	Не знает или знает очень слабо основные подсистемы и средства для решения задач защиты информа-	Знает в целом основные подсистемы и средства защиты информации, их назначение, знает их возможности фрагмен-	Знает основные подсистемы и средства защиты информации их назначение, фрагментарно знает их возмож-	Уверенно знает основные подсистемы средства защиты информации их назначение и основные

		ния для решения практических задач	ции в АС и ИС, их назначение и возможности. Слабо ориентируется в стандартах ИТ-безопасности, не знает понятия профиля защиты и их применения при разработке программного обеспечения. Имеет фрагментарное представление принципы и методиках классификации программного обеспечения АС и ИС по классам (уровням, профилям) защищённости. Слабо представляет меры и средства защиты информации в АС и ИС разных классов (уровней, профилей) защищённости. Не способен разобраться в вопросе даже при подсказке преподавателя.	тарно. Имеет общее представление об основных стандартах ИТ-безопасности, профилях защиты, не в полной мере понимает их назначение для разработки и использования ПО защиты информации. Имеет общее представление о методиках категорирования и классификации ПО, АС и ИС, и практическом применении некоторых их них. Фрагментарно представляет меры и средства защиты информации АС и ИС системах разных классов (уровней, профилей) защищённости. При подсказке преподавателя частично способен разобраться в вопросах.	ности. Знает в целом основные стандартах ИТ-безопасности, назначение профилей защиты для разработки и использования ПО защиты информации. Знает, с некоторыми недочётами, методики категорирования и классификации программного обеспечения, АС и ИС, сферу их практического применения. Имеет не совсем полное представление о мерах и средствах защиты информации в автоматизированных (информационных) системах различных классов (уровней, профилей) защищённости. Способен разобраться в вопросах при незначительных подсказках преподавателя	возможности. принципы и основные. Понимает методологию стандартов ИТ-безопасности, применение пролей защиты для разработки и использования программного обеспечения. Знает методики категорирования и классификации программного обеспечения, АС и ИС, понимает, где и как они применяются на практике. Имеет достаточно полное представление о мерах и средствах защиты информации в автоматизированных (информационных) системах разных классов (уровней, профилей) защищённости, может подтвердить знания практическими примерами.

4. Критерии выставления оценок по результатам промежуточной аттестации по дисциплине

Результаты промежуточной аттестации в 7 семестре определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

Выставление оценки за портфолио.

За каждый артефакт портфолио выставляется оценка O_i по 5-балльной шкале, где i=1,2,.., $N_{пр}$, $N_{пр}$ — количество оцениваемых артефактов портфолио по итогам практикума, исходя из следующих критериев.

«Отлично» (5 баллов): задание выполнено полностью и правильно, все выводы корректно убедительно аргументированы, грамотно изложены (в письменном и / или устном виде), аккуратно оформлены (для письменных артефактов и презентаций), студентом корректно используется профессиональная терминология, правильно формулируются понятия и категории предметной области дисциплины, студентом продемонстрирован высокий уровень владения материалом по теме задания на содержательном уровне, при подготовке используется актуальная литература и качественно подобранные интернет-источники. Для заданий в письменном виде допускаются отдельные незначительные погрешности оформления, не снижающие общего впечатления от выполненной работы. В устном ответе допускаются отдельные неточности, которые студент способен исправить самостоятельно при наводящих на них вопросах преподавателя.

«Хорошо» (4 балла): недостаточно полное раскрытие темы, отдельные ошибки в работе, объяснении процесса её выполнения и полученных результатов, которые студент способен исправить при наводящей подсказке преподавателя; несущественные ошибки в определении понятий и категорий, а также в аргументации решений и выводов, кардинально не меняющих правильную суть изложения; частичное использование неактуальных источников, незначительные погрешности грамотности изложения.

«Удовлетворительно» (3 балла): общая правильная направленность действий в рамках выполнения задания, неполная и не всегда убедительная аргументация, наличие существенных ошибок и (или) множественных несущественных ошибок в определении понятий и в содержательной части работы, использование значительной части неактуальной (некачественно) литературы и источников, неполнота ответа, неспособность целостно осветить проблематику вопроса. Частично способен исправить ошибки при подсказке преподавателя.

«Неудовлетворительно» (0 баллов): не доведенное до конца выполнение задания, качественно неверный результат; большое количество существенных ошибок в процессе выполнения, неправильное (неубедительное) объяснение результатов или отсутствие такого объяснения; необоснованная и некачественная подборка литературы и информационных источников; слабое знание

или незнание терминов и понятий, неспособность осветить проблематику вопроса, неспособность исправить большинство ошибок даже при подсказке преподавателя.

В конце семестра определяется итоговый балл за портфолио ($\mathbf{О_{пр)}}$ как среднее арифметическое значение от количества баллов за каждый артефакт:

$$\mathbf{О_{пр}} = (О_1 + О_2 + \ldots + О_{Nпр})/N_{пр}.$$

Оценка за ответы по билетам на диф.зачёте

При аттестации по билетам с теоретическими вопросами студенту выдается билет с 6 вопросами, оценка $\mathbf{О_т}$ определяется в зависимости количества правильных и полных ответов на поставленные вопросы в соответствии со следующими критериями.

«отлично» (5 баллов) — если не менее чем на 5 вопросов даны правильные развернутые ответы (в правильном ответе допускаются одна-две неточности или несущественная ошибка, которые студент смог самостоятельно исправить при наводящем вопросе преподавателя), ответ на оставшийся вопрос может быть неполным, но с правильным общим направлением мысли;

«хорошо» (4 балла) — если студент ответил правильно на 4 вопроса, при ответе на остальные вопросы допустил существенные ошибки при общем правильном направлении мысли, один вопрос может остаться без ответа;

«удовлетворительно» (3 балла) — если имеет место одна из двух ситуаций: а) студент смог правильно ответить на 3 вопроса, а на 3 других либо не ответил, либо допустил существенные ошибки; б) студент попытался ответить более, чем на 3 вопроса, не менее двух ответов правильные или почти правильные (с одной несущественной ошибкой), а остальные не доведены до конца, но при этом, как минимум, в ответах на два из них присутствует правильное общее направление мысли.

Итоговая оценка результатов промежуточной аттестации

Итоговая оценка **О** за освоение дисциплины определяется как среднее арифметическое количества баллов за теорию и практику $\mathbf{О} = (\mathbf{О_{пр}} + \mathbf{О_т}) / 2$. При возникновении дробной части преподаватель имеет право задать дополнительный вопрос, требующий короткого однозначного ответа. При правильно ответе итог округляется в большую сторону, при неправильном — в меньшую.

Оценка «отлично» соответствует продвинутому уровню сформированности компетенции.

Оценка «хорошо» соответствует базовому уровню сформированности компетенции.

Оценка «удовлетворительно» соответствует пороговому уровню сформированности компетенции.

Лист актуализации фонда оценочных средств промежуточной аттестации
по дисциплине
«Защита информации»

№	Характеристика внесенных изменений (с указанием пунктов документа)	Дата и № протокола Ученого совета ФИТ	Подпись ответственного
1	Актуализирован на 2020-2021 уч.год	22.07.2020 №77	
2	Актуализирован на 2021-2022 уч. год	26.04.2021 N80	
3	Актуализирован на 2022-2023 уч. год	31.08.2022 N87	