МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан ФИТКБ

_____ /Гусев П.Ю./

27 сентября 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Методы и системы защиты информации, информационная безопасность»

Направление подготовки 2.3.6. Методы и системы защиты информации, информационная безопасность

Нормативный период обучения 3 года

Форма обучения очная

Год начала подготовки 2022

Автор программы _____ А.Г. Остапенко

Заведующий кафедрой систем информационной безопасности _____ А.Г. Остапенко

Руководитель ОПОП _____ А.Г. Остапенко

Воронеж 2022

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины является ознакомление с комплексом проблем информационной безопасности предпринимательских структур различных типов и направлений деятельности, построения и функционирования совокупности правовых, организационных, технических и технологических процессов, обеспечивающих информационную безопасность и формирующих структуру системы защиты ценной и конфиденциальной информации в сферах охраны интеллектуальной собственности предпринимателей и сохранности их информационных ресурсов.

1.2. Задачи освоения дисциплины

а) овладение теоретическими, практическими и методическими вопросами классификации угроз информационным ресурсам;

б) ознакомление с современными проблемами информационной безопасности, основными концептуальными положениями системы защиты информации;

в) изучение основных направлений обеспечения информационной безопасности, меры законодательного, административного, процедурного и программно-технического уровней при работе на вычислительной технике и в каналах связи;

г) приобретение теоретических и практических навыков по использованию современных методов защиты информации в компьютерных системах;

д) формирование практических навыков и способностей осуществления мероприятий по обеспечению информационной безопасности функционирования информационной системы при взаимодействии с информационными рынками по сетям или с использованием иных методов обмена данными.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Методы и системы защиты информации, информационная безопасность» является дисциплиной, направленной на подготовку к сдаче кандидатских экзаменов, образовательного компонента программы аспирантуры подготовки научных и научно-исследовательских кадров в аспирантуре по научной специальности 2.3.6 Методы и системы защиты информации, информационная безопасность.

Рабочая программа составлена в соответствии с Федеральными государственными требованиями к структуре программам подготовки научных и научно-педагогических кадров в аспирантуре (адъюнктуре)», утвержденных приказом Министерства науки и высшего образования Российской Федерации (Минобрнауки России) от 20 октября 2021 года № 951; Постановление Правительства Российской Федерации от 30.11.2021 № 2122 "Об утверждении

Положения о подготовке научных и научно-педагогических кадров в аспирантуре (адъюнктуре)".

Является неотъемлемой частью программы аспирантуры подготовки научных и научно-исследовательских кадров в аспирантуре. Дисциплина направлена на подготовку к сдаче кандидатского экзамена.

Дисциплина «Методы и системы защиты информации, информационная безопасность» относится к дисциплинам части, формируемой участниками образовательных отношений блока 2.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

В результате изучения дисциплины «Методы и системы защиты информации, информационная безопасность» аспирант должен:

Знать

теоретические основы и методологию обеспечения информационной безопасности и защиты информации;

технологии идентификации и аутентификации пользователей и субъектов информационных процессов;

особенности организации систем документооборота (вне зависимости от степени их компьютеризации) и средства зашиты циркулирующей в них информации;

методы управления информационной безопасностью, непрерывным функционированием и восстановлением систем, противодействия отказам в обслуживании;

методы, модели и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет;

методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях.

модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем, позволяющие получать оценки показателей информационной безопасности.

принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

Уметь

применять методы, аппаратно-программные средства и организационные меры защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида;

организовывать исследования и разрабатывать методы в области выявления и противодействия распространению ложной и вредоносной инфор-

мации;

применять методы, формализовывать модели и пользоваться средствами выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса;

строить модели, применять методы и средства обеспечения аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности, и расследования инцидентов информационной безопасности в автоматизированных информационных системах;

применять методы оценки защищенности информации и информационной безопасности объекта;

Владеть

методологиями и инструментами анализа рисков нарушения информационной безопасности и уязвимости процессов обработки, хранения и передачи информации в информационных системах любого вида и области применения;

средствами разработки безопасных программ, выявления дефектов безопасности в программном обеспечении, противодействия скрытым каналам передачи данных и выявления уязвимостей в компьютерных системах и сетях;

подходами к построению модели и применению методов формирования комплексов средств противодействия угрозам информационной безопасности для различного вида объектов защиты (систем, цепей поставки) вне зависимости от области их функционирования.

навыками организации мероприятий и механизмов формирования политики обеспечения информационной безопасности для объектов всех уровней иерархии системы управления.

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Методы и системы защиты информации, информационная безопасность» составляет 12 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры		
		3	4	5
Аудиторные занятия (всего)	54	18	18	18
В том числе:				
Лекции	54	18	18	18
Самостоятельная работа	342	90	90	162
Вид промежуточной аттестации (экзамен)	36			36
Общая трудоемкость: академические часы зач.ед.	432 12	108 3	108 3	216 6

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	СРС	Всего, час
1	Теория и методология обеспечения информационной безопасности и защиты информации.	Проблемы развития теории и практики обеспечения информационной безопасности. Основные понятия и определения в области информационной безопасности. Составляющие национальных интересов российской федерации в информационной сфере. Общее содержание защиты информации. Предмет и объект защиты информации. Угрозы информационной безопасности. Модель нарушителя. Системное обеспечение защиты информации.	10	56	66
2	Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса	Анализ уязвимостей системы. Базы уязвимостей. Типовые уязвимости. Оценка уязвимостей. Метрики. Банк данных угроз безопасности информации. Порядок оценки угроз безопасности информации. Определение негативных последствий от реализации (возникновения) угроз безопасности информации. Определение возможных объектов воздействия угроз безопасности информации. Оценка возможности реализации (возникновения) угроз безопасности информации и определение их актуальности: определение источников угроз безопасности информации; оценка способов реализации (возникновения) угроз безопасности информации; оценка актуальности угроз безопасности информации. Этапы моделирования угроз. Нарушители. Сценарии реализации угроз. Актуальность угроз. Уровень опасности угроз. Описание угрозы безопасности. Построение модели угроз в соответствии с методикой оценки угроз безопасности информации.	10	56	66
3	Методы, аппаратно-программные средства и организационные меры защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида	Средства защиты информации и их классификация. Средства защиты от несанкционированного доступа (СЗИ от НСД). Модуль доверенной загрузки. Межсетевые экраны (Файрволы, МЭ). Системы обнаружения вторжений (СОВ – IDS). Системы анализа уязвимостей (сканеры уязвимостей). Системы мониторинга безопасности (SIEM). Системы антивирусной защиты информации (САВЗ). Системы предотвращения утечек информации (DLP). Средства криптографической защиты информации (СКЗИ). Средства унифицированного управления угрозами (UTM). Признаки безопасности информации при соблюдении организационных мер: доступность сведений. целостность информации, конфиденциальность или недоступность данных для неавторизованных субъектов; авторство информации, или невозможность отрицания принадлежности действий или данных.	10	56	66
4	Методы, модели и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет	Понятия и терминология открытых систем. Задачи, свойства и состав открытых систем. Набор стандартов POSIX. Распределённые системы. Основные механизмы защиты информации в распределенных системах. Сетевые службы. Методы противодействия угрозам: правовые методы; экономические методы; организационные методы; инженерно-технические методы; технические методы; программно-аппаратные методы	8	58	66
5	Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях	Выявление сетевых атак путем анализа трафика. Основные типы систем обнаружения атак. Методы анализа и обнаружения атак: методы потенциальных функций, SVM, кластерный анализ, нейросети, аппарат нечёткой логики и т.д. Эксплуатация систем обнаружения атак.	8	58	66
6	Анализ рисков нарушения информационной безопасности и уязвимости процессов обработки, хранения и пере-	Стандарты в области управления рисками информационной безопасности. Понятие риска. Оценка риска. Количественное определение величины риска. Качественное определение величины риска. Активы организации как ключевые факторы риска. Подходы к управлению рисками. Анализ факторов	8	58	66

	дачи информации в информационных системах любого вида и области применения	риска. Оценка рисков информационной безопасности: идентификация активов, идентификация требований безопасности, определение ценности активов, анализ угроз и уязвимостей, определение величины риска. Обработка рисков информационной безопасности. способы обработки риска (принятие, уменьшение, передача, избежание). Инструментальные средства для управления рисками. обзор методов и инструментальных средств управления рисками (OCTAVE, CRAMM, RiskWatch, COBRA, RA2 the art of risk, vsRisk, Callio Secura 17799, Proteus Enterprise).			
Контроль					**36**
Итого			**54**	**342**	**432**

5.2 Перечень лабораторных работ

Не предусмотрено учебным планом

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение курсового проекта (работы) или контрольной работы.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе: «аттестован»; «не аттестован».

Критерии оценивания	Аттестован	Не аттестован
Активная работа на практических занятиях, отвечает на теоретические вопросы	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
Решение стандартных практических задач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
Решение прикладных задач в конкретной предметной области	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 5 семестре по системе: «отлично»; «хорошо»; «удовлетворительно»; «неудовлетворительно»

Критерии оценивания	**Отлично**	**Хорошо**	**Удовлетворительно**	**Неудовлетворительно**
Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1) Вопросы для собеседования.

Тема 1. Концепция информационной безопасности:

1. Критерии безопасности компьютерных систем.
2. Международные стандарты информационной безопасности.
3. Общие принципы построения защищенных информационных систем
4. Средства разработки ИС и правила их реализации.
5. Защищенные информационные технологии.

2) Тестирование

Тема 2. Угрозы информации.

Примеры вопросов тестов.

Задание 1. В каком году в России появились первые преступления с использованием компьютерной техники (были похищены 125,5 тыс. долл. США во Внешэкономбанке)?

1. 1988;
2. 1991;
3. 1994;
4. 1997;
5. 2002.

Задание 2. Сертификации подлежат:

1. средства криптографической защиты информации;
2. средства выявления закладных устройств и программных закладок;
3. защищенные технические средства обработки информации;
4. защищенные информационные системы и комплексы телекоммуникаций;
5. все вышеперечисленные средства.

Задание 3. В стандарте США «Оранжевой книге» фундаментальное требование, которое относится к группе Стратегия:

1. индивидуальные субъекты должны идентифицироваться;
2. контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность;
3. необходимо иметь явную и хорошо определенную систему обеспечения безопасности;
4. вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований;
5. гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взлома» и/или несанкционированного внесения изменений.

Задание 4. Естественные угрозы безопасности информации вызваны:

1. деятельностью человека;
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
3. воздействиями объективных физических процессов или стихийных природных явле-

ний, не зависящих от человека;
4. корыстными устремлениями злоумышленников;
5. ошибками при действиях персонала.

Задание 5. Хакер - это:
1. лицо, которое взламывает интрасеть в познавательных целях;
2. мошенник, рассылающий свои послания в надежде обмануть наивных и жадных;
3. лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов, разрушающих ПО;
4. плохой игрок в гольф, дилетант;
5. мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

Задание 6. Активный перехват информации это - перехват, который:
1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;
4. осуществляется путем использования оптической техники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

Задание 7. Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:
1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

Задание 8. По среде обитания классические вирусы разделяются:
1. на паразитические;
2. на компаньоны;
3. на файловые;
4. на ссылки;
5. на перезаписывающие.

Задание 9. Шифрование методом подстановки:
1. символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста;
2. символы шифруемого текста последовательно складываются символами некоторой специальной последовательности;
3. шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор;
4. символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов;
5. замена слов и предложений исходной информации шифрованными.

Задание 10. Метод защиты информации ограничение доступа заключается:
1. в контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления;

2. в создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями;
3. в разделении информации на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;
4. в том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;
5. в проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

Задание 11. Перехват, который неправомерно использует технологические отходы информационного процесса, называется:
1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

Задание 12. Спам, периодически проводящий рассылки не рекламных сообщений:
1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

Задание 13. Способ защиты информации, существующей в виде электромагнитного сигнала, зависит от ...
1. среды распространения электромагнитного сигнала;
2. длины волны сигнала;
3. наличия или отсутствия специальной линии связи;
4. типа линии связи;
5. форм воздействия на информацию или ее носитель;
6. предполагаемого способа нападения на информацию.

Задание 14. Попытка одного субъекта выдать себя за другого - это:
1. пассивная атака;
2. модификация потока данных»
3. фальсификация;
4. повторное использование;
5. отказ в обслуживании.

Задание 15. Антивирус просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок:
1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

7.2.2 Примерный перечень заданий для решения стандартных задач

1. Что понимается под маскирование неоднородностей
множество ресурсов, управляемых по одним и тем же правилам
скрытое местонахождение и принадлежность ресурсов в сообществе
ПО промежуточного уровня должно обеспечить стирание различий между программными обеспечениями промежуточного уровня виртуальных организаций

2.Что понимается под стандартизацией
федерация построена на открытых стандартах, протоколах и интерфейсах
множество ресурсов, управляемых по одним и тем же правилам
скрытое местонахождение и принадлежность ресурсов в сообществе

3. Что понимается под виртуализацией
федерация построена на открытых стандартах, протоколах и интерфейсах
ПО промежуточного уровня должно обеспечить стирание различий между программными обеспечениями
скрытое местонахождение и принадлежность ресурсов в сообществе

4. Современные вычислительные комплекса строятся по кластерной схеме, т.е. ....
архитектуры движутся в сторону параллельных систем
архитектуры движутся в сторону распределенных систем
архитектуры движутся в сторону сосредоточенных систем

5.Какие системы используют децентрализацию данных и управления
распределенные системы
Грид
службы WWW

6.Для чего Грид использует несколько уровней децентрализации данных
унификация в доступе к различным ресурсам
обеспечение интероперабельности систем управления ресурсами
адаптация к требованиям приложения

7.Что из перечисленного относится к архитектуре Грид
пользовательские интерфейсы
языки программирования
промежуточное программное обеспечение
инфраструктура сетей

8. К промежуточному программному обеспечению можно отнести...
доступ к памяти

среда решения задач
программные модели

9. Определите составляющие одного из слоев архитектуры Грид
языки программирования
неоднородные ресурсы
программные модели

10. Назовите задачи характерные для большинства моделей вычислений в Гриде
управление данными
управление ресурсами
формирование потоков работ

11. Какое приложение в Грид является географически распределенной базой знаний
Грид как коллекция научных данных
Грид как большой компьтер
семантический Грид

12. Что поддерживает семантический Грид
интеллектуальный информационный повод
извлечение знаний из "сырых" данных
принятие решений

13. Развитие и поддержки какой концепции требуют приложения в Грид
виртуальных ресурсов
ресурсов - данных
ресурсов- вычислительных мощностей

14. Эффективный пиоск в больших массивах данных требует распараллеливания...
процессов соединений
процессов вычислений
процессов ввода/вывода

15. Назовите важные процессы в исследованиях по распределенным системам
распределение
координация
интеграция

16. Какая из предложенных технологий позволяет строить приложения различной степени сложности и
гранулярности
язык моделирования Triad

компонентное программирование
функциональное программирование

17. Назовите основные этапы жизненного цикла приложения
спецификация
генерация кода
сопровождение

18. Какие сервисы инфраструктуры распределенных систем должна поддерживать технология
управление транзакциями
изменение обработки данных
создание "мостов" между Грид-системами

19. Что понимается под мобильным доступом к информации
возможность получения информации при перемещении пользователя
подключение к сети в любой географической точке
возможность подключения к сети и получения полной информации

20. Какое направление базируется на пользователе, находящемся в одном из углов решетки и имеющий возможность
использовать ресурсы, находящиеся в любых доступных в данный момент узлах решетки
Грид
мобильный компьютинг
тотальный компьтинг

7.2.3 Примерный перечень заданий для решения прикладных задач

Задание 1. Необходимо построить защищенное соединение между двумя компьютерами. Приведите отчет с результатами выполнения и описанием произведенных действий. Архитектура защищенного канала может быть:
сервер-клиент
клиент-клиент
Задание 2. Необходимо настроить защищенный обмен между двумя пользователями при помощи криптографических и стеганографических контейнеров. Приведите отчет с результатами выполнения и описанием произведенных действий.
Задание 3. Необходимо построить централизованную инфраструктуру открытых ключей. Удостоверяющим центром являетесь вы. Необходимо создать не менее двух пользователей, а также сформировать список отозванных сертификатов. Приведите отчет с результатами выполнения и описанием произведенных действий.
Задание 4. Даны некоторые ценные документы. Необходимо их подписать с помощью цифровой подписи и подготовить их для передачи предварительно

зашифровав. Приведите отчет с результатами выполнения и описанием произведенных действий.

Вариант № 5 Формирование групповой политики информационной безопасности: Active
Directory
Вопросы:
Сформируйте домен рабочей группы.
Сформируйте шаблон безопасности.
Вариант № 5 Программная виртуализация гостевой операционной системы на примере программного продукта Virtualbox
Вопросы:
Как монтировать раздел диска или CD-ROM?
Возможно ли внутри виртуальной машины запустить еще одну виртуальную машину?

1. Аудит информационной безопасности представляет собой:
проверку выполнения требований законодательства по защите сведений, составляющих коммерческую тайну
оценку мер по защите информационных ресурсов
проверку выполнения требований государственных стандартов в сфере информационной безопасности

2.Проведение комплексного внешнего аудита предприятия с последующей сертификацией демонстрирует его контрагентам:

способность предприятия выступать в качестве надежного партнера,
которому можно доверить конфиденциальные сведения
полное отсутствие уязвимостей в сетях, серверах и базах данных
достаточную страховую защиту от информационных рисков

3.Сертификация системы безопасности на соответствие требованиям стандарта ISO 17799 может быть осуществлена по результатам:

внешнего аудита
внутреннего аудита
инструментальной проверки защищенности

4. Аудит информационной безопасности подразделяется на:
текущий и итоговый
внешний и внутренний
объективный и субъективный

5. Услуги внешних аудиторов используются для:
снижения затрат на аудит

повышения объективности аудита
получения сертификатов на соответствие определенным стандартам

6. Инициирование аудита информационной безопасности на предприятии производится:
аудиторскими организациями
руководством предприятия
пользователями информационной системы предприятия

7. Инициаторами аудита информационной безопасности могут выступать:
государственные структуры
органы стандартизации
руководители предприятия

8. Цели аудита информационной безопасности могут включать в себя:
выявление лиц, нарушающих требования информационной безопасности
сертификацию на соответствие общепризнанным требованиям и стандартам
установление степени защищенности информационных ресурсов

9. К целям аудита информационной безопасности относятся:
проверка достижения поставленных целей в сфере информационной безопасности
выявление фактов нарушения информационной безопасности
привлечение к ответственности лиц, виновных в краже и утрате конфиденциальных данных

10. Заключительной стадией аудита является:
внесение изменений в действующие политики безопасности
проведение аттестации сотрудников департамента информационной безопасности
формирование аудиторского заключения

11. Для поддержки разработки политик безопасности используются:
автоматизированные сканеры уязвимостей
электронные справочные системы
средства управления паролями

12. Оценка рисков по методологии CRAMM является:
основным результатом аудита информационной безопасности
основой для выработки системы контрмер
показателем эффективности вложений в средства информационной безопасности

7.2.4 Примерный перечень вопросов для подготовки к зачету

Не предусмотрено учебным планом

7.2.5 Примерный перечень заданий для подготовки к экзамену

Не предусмотрено учебным планом

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Аттестация проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 6 до 10 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.)

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Теория и методология обеспечения информационной безопасности и защиты информации.		Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
2			Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
3	Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса		Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
4	Методы, аппаратно-программные средства и организационные меры защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида		Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
5	Методы, модели и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в от-		Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….

	крытых компьютерных сетях, включая Интернет		
6	Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях		Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-58114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401

Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — Текст : электронный // Лань : электроо-библиотечная система. — URL:https://e4anbook.com2/book/165837 .

Диогенес, Ю. Кибербезопасность. стратегия атак и обороны / Ю. Диогенес, Э. Озкайя ; перевод с английского Д. А. Беликова. — Москва : ДМК Пресс, 2020. — 326 с. — ISBN 978-5-97060-709-1. — Текст : электронный // Лань: электронно-библиотечная система.URL: https://e.lanbook.com/book/131717

Мельников В.П., под ред., Куприянов А.И. Информационная безопасность: Учебник / — Электрон. дан. — Москва : КноРус, 2021 .— 267 с. Internet access .— URL:https://www.book.ru/book/939292

Прохорова, О. В., Информационная безопасность и защита информации

[Электронный ресурс]: учебник / Прохорова О. В. — 2-е изд., стер. — Санкт-Петербург: Лань, 2021 .— 124 с.—URL:https://e.lanbook.com/book/158939

Грибунин, В. Г. Комплексная система защиты информации на предприятии: учебное пособие для вузов / В. Г. Грибунин, В. В. Чудовский. - М.: Академия, 2009. - 411 с

Аверченков В. И. Организационная защита информации: учебное пособие для вузов 3-е изд., стер. - М.: Флинта, 2011. 224 с.

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

Шаблоны типовых документов по информационной безопасности http://securitypolicy.ru/%D1%88%D0%B0%D0%B1%D0%BB%D0%BE%D0%BD%D1%8B

Государственный реестр сертифицированных средств защиты информации

https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591 -gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001 -01bi00

Банк данных угроз безопасности информации

https://bdu.fstec.ru/vul

Международные, национальные (государственные) и отраслевые стандарты в области информационной безопасности (защиты информации), а также информационных технологий и непрерывности бизнеса

http://www.iso27000.ru/

Управление рискми ИБ

https://www.securityvision.ru/blog/upravlenie-riskami-informatsionnoy-bezopasnosti-chast-1-osnovnye-ponyatiya-i-metodologiya-otsenki-ri/

Электронная образовательная система ВГТУ https: //old. education. cchgeu. ru/

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Методы и системы защиты информации, информационная безопасность» читаются лекции.

Основой изучения дисциплины являются лекции, на которых излага-

ются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед три дня эффективнее всего использовать для повторения и систематизации материала.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Перечень вносимых изменений	Дата внесения изменений	Подпись заведующего кафедрой, ответственной за реализацию ОПОП