Министерство образования и науки Российской Федерации

федеральное государственное бюджетное образовательное учреждение высшего образования
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

Кафедра Информационных технологий и систем безопасности

Рабочая программа по дисциплине

ВВЕДЕНИЕ В СПЕЦИАЛЬНОСТЬ

Основная профессиональная образовательная программа
высшего образования программы специалитета по специальности

10.05.02 «Информационная безопасность телекоммуникационных систем»

Специализация:
Разработка защищенных телекоммуникационных систем

Квалификация:
Специалист

Форма обучения
Очная

Согласовано
Руководитель ОПОП
«Информационная безопасность телекоммуникационных систем»

_____ **Бурлов В.Г.**

Утверждаю
Председатель УМС _____ **И.И. Палкин**

Рекомендована решением
Учебно-методического совета
19 апреля 2018 г., протокол № 4

Рассмотрена и утверждена на заседании кафедры
17 апреля 2018 г., протокол № 5
Зав. кафедрой _____ **Бурлов В.Г.**

Авторы-разработчики:
_____ **Грызунов В.В.**

Санкт-Петербург 2018

1. Цели освоения дисциплины

Целью освоения дисциплины «Введение в специальность» является формирование знаний о сущности и социальной значимости будущей профессии, создание высокой мотивации к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства.

Основные задачи дисциплин – дать знания по вопросам::

- Правовые основы и организация современного высшего образования в области информационной безопасности;
- современное состояние радиоэлектронных систем передачи и обработки информации, в том числе систем телекоммуникаций;
- основные направления, методы и средства обеспечения безопасности информации в телекоммуникационных системах.

2.Место дисциплины в структуре ОПОП

Дисциплина «Введение в специальность» для направления подготовки 10.05.02 – информационная безопасность телекоммуникационных систем относится к базовым дисциплинам Б1 Дисциплины (Модули).

Для успешного усвоения данной дисциплины необходимо, чтобы обучаемые владели знаниями, умениями и навыками, сформированными в процессе обучения в средней школе по предметам:

- «Информатика»,
- «Алгебра»,
- «Физика»,
- «Русский язык»,
- «Обществознание».

Параллельно с дисциплиной «Введение в специальность» изучаются дисциплины:«Информатика и программирование», «Интернет-технологии», «Учебная практика «Ознакомительная».

Знания и умения, полученные обучаемыми по дисциплине «Введение в специальность», служат фундаментом для изучения следующих дисциплин:

- «Аппаратные средства вычислительной техники
- «Электроника и схемотехника»,
- «Основы информационной безопасности»,
- «Организационное и правовое обеспечение информационной безопасности»,
- «Техническая защита информации»,
- «Сети и системы передачи информации»,
- «Информационные технологии».

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих

компетенций:

Код компетенции	Компетенция
ОК-5	способность понимать социальную значимость своей будущей профессии, обладание высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдение нормы профессиональной этики

В результате освоения компетенций в рамках дисциплины «Введение в специальность» обучающийся должен:

Код компетенции	Компетенция
ОК-5	Знать: − основные определения в сфере информационной безопасности (ИБ); − требования к специалисту по ИБ; − способы представления информации и особенности её обработки в ЭВМ; − основные угрозы ИБ на разных уровнях информационно-вычислительной системы (ИВС); − возможности и ограничения существующих средств обеспечения ИБ по уровням иерархии ИВС; − методы проектирования защищённых ИВС; − тренды ИБ; − влияние моральных, юридических, политических и экономических факторов на ИБ в стране. Уметь: − описать в общих чертах знания, недостающие для решения задач по ИБ; − исследовать возможности и ограничения существующих средств обеспечения ИБ; − использовать стратегию и тактику ведения переговоров в сфере ИБ; − применять UML, IDEF0 для проектирования и/или анализа ИВС. Владеть навыками: − предположить влияние существующих и новых угроз на общее состояние защищаемой ИВС; − оценить сложность задач по ИБ.

Основные признаки проявленности формируемых компетенций в результате освоения дисциплины «Введение в специальность» сведены в таблице.

Уровень освоения компетенции	Результат обучения
	ОК-5: Знать, уметь, владеть
минимальный	плохо ориентируется в терминологии и содержании
	выделяет основные идеи, но не видит проблем
	допускает много ошибок

базовый	Способен выделить основные идеи текста, работает с критической литературой
	Способен показать основную идею в развитии
	Знает основные рабочие категории, однако не ориентируется в их специфике
продвинутый	Видит источники современных проблем в заданной области анализа, владеет подходами к их решению
	Выявляет основания заданной области анализа, понимает ее практическую ценность, однако испытывает затруднения в описании сложных объектов анализа
	Знает основное содержание современных научных идей в рабочей области анализа, способен их сопоставить

Соответствие уровней освоения компетенции планируемым результатам обучения и критериям их оценивания

Этап (уровень) освоения компетенции	Основные признаки проявленности компетенции (дескрипторное описание уровня)				
	1.	2.	3.	4.	5.
минимальный	не владеет	слабо ориентируется в терминологии и содержании	Способен выделить основные идеи текста, работает с критической литературой	Владеет основными навыками работы с источниками и критической литературой	Способен дать собственную критическую оценку изучаемого материала
	не умеет	не выделяет основные идеи	Способен показать основную идею в развитии	Способен представить ключевую проблему в ее связи с другими процессами	Может соотнести основные идеи с современными проблемами
	не знает	допускает грубые ошибки	Знает основные рабочие категории, однако не ориентируется в их специфике	Понимает специфику основных рабочих категорий	Способен выделить характерный авторский подход
базовый	не владеет	плохо ориентируется в терминологии и содержании	Владеет приемами поиска и систематизации, но не способен свободно изложить материал	Свободно излагает материал, однако не демонстрирует навыков сравнения основных идей и концепций	Способен сравнивать концепции, аргументированно излагает материал
	не умеет	выделяет основные идеи, но не видит проблем	Выделяет конкретную проблему, однако излишне упрощает ее	Способен выделить и сравнить концепции, но испытывает сложности с их практической привязкой	Аргументированно проводит сравнение концепций по заданной проблематике
	не знает	допускает много ошибок	Может изложить основные рабочие категории	Знает основные отличия концепций в заданной проблемной области	Способен выделить специфику концепций в заданной проблемной области
продвинутый	не владеет	ориентируется в терминологии и содержании	В общих чертах понимает основную идею, однако плохо связывает ее с существующей проблематикой	Видит источники современных проблем в заданной области анализа, владеет подходами к их решению	Способен грамотно обосновать собственную позицию Относительно решения современных проблем в заданной области
	не умеет	выделяет основные идеи, но не видит их в развитии	Может понять практическое назначение основной идеи, но затрудняется выявить ее основания	Выявляет основания заданной области анализа, понимает ее практическую ценность, однако испытывает затруднения в описании сложных объектов анализа	Свободно ориентируется в заданной области анализа. Понимает ее основания и умеет выделить практическое значение заданной области
	не знает	допускает ошибки при выделении рабочей области анализа	Способен изложить основное содержание современных научных идей в рабочей области анализа	Знает основное содержание современных научных идей в рабочей Области анализа, способен их сопоставить	Может дать критический анализ современным проблемам в заданной области анализа

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 часа.

Объем дисциплины (модуля) по видам учебных занятий в академических часах)[1]

Объём дисциплины	**Всего часов**
	Очная форма обучения
Общая трудоёмкость дисциплины	**72**
Контактная[2] работа обучающихся с преподавателям (по видам аудиторных учебных занятий) – всего[3]:	**36**
в том числе:	
лекции	**18**
практические занятия	**18**
семинарские занятия	
Самостоятельная работа (СРС) – всего:	**36**
в том числе:	
курсовая работа	
контрольная работа	
Вид промежуточной аттестации (зачет/экзамен)	**зачёт**

4.1. Структура дисциплины

Очная форма обучения

№ п/п	**Раздел и тема дисциплины**	**Семестр**	**Виды учебной работы, в т.ч. самостоятельная работа студентов, час.**			**Формы текущего контроля успеваемости**	**Занятия в активной и интерактивной форме, час.**	**Формируемые компетенции**
			Лекции	**Практич.**	**Самост. работа**			
1	Введение. Информационная безопасность в современном мире	**1**	2	2		По итогам дискусси и	4	ОК-5
2	Особенности информации с точки зрения её защиты	**1**	2	2		По итогам творческого задания	4	ОК-5

3	Иерархическая модель информационно-вычислительно системы (ИВС)	**1**	6	6		По итогам творческого задания	12	ОК-5
4	Планирование информационно-технических атак	**1**	2	2		По итогам творческого задания	4	ОК-5
5	Основные подходы и средства обеспечения информационной безопасности	**1**	2	2		По итогам деловой игры	4	ОК-5
6	Методы проектирования защищённых ИВС	**1**	2	2		По итогам решения кейса	4	ОК-5
7	Заключение. Тренды в информационной безопасности	**1**	2	2		По итогам творческого задания	4	ОК-5
	ИТОГО		**18**	**18**			**36**	

4.2. Содержание разделов дисциплины

4.2.1 Информационная безопасность в современном мире

Основные определения. Роль и место информационной безопасности в современном мире. Требования к специалисту по информационной безопасности на разных этапах развития телекоммуникационных систем.

4.2.2 Особенности информации с точки зрения её защиты

Представление информации и особенности её обработки в ЭВМ. Каналы утечки информации.

4.2.3 Иерархическая модель ИВС

Понятие иерархической модели ИВС. Угрозы на разных уровнях ИВС. Социальная инженерия. Основы сетей и телекоммуникаций.

4.2.4 Планирование информационно-технических атак

Понятие информационно-технической атаки и информационно-технического вторжения. Возможные цели и объекты атак. Средства планирования атак.

4.2.5 Основные подходы и средства обеспечения информационной безопасности

Инструментарий специалиста по информационной безопасности. Возможности и ограничения существующих средств обеспечения безопасности по уровням

иерархии
ИВС. Расследование инцидентов информационной безопасности.

4.2.6 Методы проектирования защищённых ИВС

Понятие защищённой ИВС. Основные способы проектирования ИВС. Применение методологии IDEF0 и UML для проектирования ИВС.

4.2.7 Тренды в информационной безопасности

Перспективы развития аппаратных и программных средств ИВС, средств планирования и реализации информационно-технических атак. Влияние моральных, юридических, политических и экономических факторов на информационную безопасность в стране.

4.3. Практические занятия, их содержание

№ п/п	№ раздела дисциплины	Тематика практических занятий	Форма проведения	Формируемые компетенции
1	1	Информационная безопасность в современном мире	Дискуссия	ОК-5
2	2	Синквейн на тему «Особенности информации с точки зрения её защиты»	Творческое задание	ОК-5
3	3	Изучение методов социальной инженерии	Творческое задание	ОК-5
4	3	Изучение методов социальной инженерии	Творческое задание	ОК-5
5	3	Дискуссия в форме эстафеты на тему «Иерархическая модель ИВС»	Дискуссия	ОК-5
6	4	Составление кроссворда на тему «Защита информации и информационно-технические атаки»	Творческое задание	ОК-5
7	5	Деловая игра «ФСБ проверяет банк»	Деловая игра	ОК-5
8	6	Применение IDEF0 и UML для проектирования ИВС	Кейс-задача	ОК-5
9	7	Брейн-ринг на тему «Информационная безопасность»	Творческое задание	ОК-5

5. Учебно-методическое обеспечение самостоятельной работы студентов и оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

5.1. Текущий контроль

Текущий контроль проводится путём проверки выполнения творческих заданий, деловой игры, дискуссий, кейс-задачи

5.2. Методические указания по организации самостоятельной работы

Во время самостоятельной работы студенты знакомятся с существующими методами и инструментами обеспечения информационной

безопасности в целом, методами социальной инженерии, возможными направлениями деятельности специалиста по информационной безопасности.

В перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине «Введение в специальность» входит дополнительная литература и видеофильмы для самостоятельного изучения.

5.3. Промежуточный контроль: зачёт

Перечень вопросов к зачету

1. Понятие информации. Особенности информации с точки зрения её защиты.
2. Роль и место ИБ в современном мире.
3. Возможные направления деятельности специалиста по ИБ.
4. Требования к специалисту по ИБ.
5. Понятие утечки информации. Структура типового канала утечки информации.
6. Информационный сигнал. Природа, математическая модель.
7. Аналоговый сигнал.
8. Цифровой сигнал.
9. Способы модуляции сигнала.
10. Каналы утечки информации технических средств обработки, хранения и передачи информации
11. Электрические и электромагнитные каналы утечки информации.
12. Каналы утечки речевой и видовой информации.
13. Каналы утечки информации на программном уровне ИВС
14. Иерархическая модель. Структура, сферы применения.
15. Угрозы и средства защиты информации на аппаратном уровне иерархической модели. Возможности и ограничения средств защиты информации уровня.
16. Угрозы и средства защиты информации на программном уровне иерархической модели. Возможности и ограничения средств защиты информации уровня.
17. Угрозы и средства защиты информации на уровне персонала иерархической модели. Возможности и ограничения средств защиты информации уровня.
18. Защита информации на обеспечивающем уровне иерархической модели ИВС. Уголовная ответственность в сфере информационной безопасности. Возможности и ограничения средств защиты информации уровня.
19. Классификация методов защиты информации. Комплексные методы защиты информации.
20. Социальная инженерия. Пирамида нейрологических уровней.
21. Социальная инженерия. Фокусы языка: намерение, разделение, иерархия критериев.
22. Социальная инженерия. Фокусы языка: объединение, другой результат, противоположный пример.
23. Социальная инженерия. Фокусы языка аналогия, изменение размеров фрейма, метамодель.
24. Социальная инженерия. Фокусы языка: метафрейм, стратегия реальности,

переопределение.

25. Социальная инженерия. Фокусы языка: применение к себе, последствия.
26. Информационно-технические атаки и вторжения. Объекты атак.
27. Типовые этапы и сценарии информационно-технических атак.
28. Дерево атаки, назначение, структуру, сфера использования.
29. Блок-схема алгоритма, диаграмма Ганта и Activity diagram (UML).
30. Цели проектирования
31. Способы проектирования ИВС. IDEF0.
32. Способы проектирования ИВС. UML.
33. Этапы синтеза ИВС.
34. Компоненты успеха IT-проекта.
35. SMART при постановке цели IT-проекта.
36. Классический и экспресс варианты внедрения IT-системы.
37. Сетевая топология. Общая шина. Особенности работы с точки зрения ИБ.
38. Сетевая топология. Звезда. Особенности работы с точки зрения ИБ.
39. Сетевая топология. Кольцо. Особенности работы с точки зрения ИБ.
40. Сетевая топология. Иерархическая топология. Особенности работы с точки зрения ИБ.
41. Понятие протокола и интерфейса.
42. Модель OSI. Назначение, состав.
43. Перспективы развития аппаратных и программных средств ИБ.
44. Интеллектуальные технологии в сфере ИБ.

Критерии оценивания:

- оценка «***зачтено***»: в целом ориентируется в предметной области, умеет анализировать и делать выводы;
- оценка «***не зачтено***»: плохо ориентируется в предметной области, не умеет анализировать или делать выводы.

6. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1.
2. ГОСТ 19.701-90 «Схемы алгоритмов программ, данных и систем».
3. ГОСТ 34.601-90. Автоматизированные системы. Стадии создания.
4. Грушо А.А., Применко Э.А., Тимонина Е.Е. Теоретические основы компьютерной безопасности, 2009. https://vk.com/doc-135429705_467778411
5. Грызунов В.В. Аналитическая модель целостной информационной системы // Доклады ТУСУР.– 2009.– № 1(19), ч.1.– С.226-230. https://vk.com/doc- 135429705_440206638
6. Миноженко А., Евдокимов Д. «Анализ безопасности мобильных банковских приложений 2012». https://vk.com/doc-135429705_485404364

7. Муха Ю.П., Авдеюк О.А., Королёва И.Ю. Алгебраическая теория синтеза сложных систем: Монография/ВолгГТУ, Волгоград, 2003. – 320 с.

8. ФГОС ВПО по направлению подготовки «10.05.02 Информационная безопасность телекоммуникационных систем».

9. Цвиркун А.Д. Основы синтеза структуры сложных систем/ Институт проблем управления. – М.: Наука, 1982. – 200 с. https://vk.com/doc-135429705_485388608

б) дополнительная литература:

1. Пелехатый М. М., Чекчурин Ю. А. Сертификационный курс НЛП-Практик, — М.: Твои книги, 2014. — 272 с. https://vk.com/doc-135429705_440046735

в) программное обеспечение и Интернет-ресурсы:

1. Архитектура и стратегия информационной безопасности Cisco. http://www.justogroup.ru/dokumentacija/cisco/informacionnaja-bezopasnost/arhitektura_i_strategiya_informacionnoy_bezopasnosti_cisco.pdf

2. Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак http://proceedings.spiiras.nw.ru/ojs/index.php/sp/article/viewFile/3267/1883

3. Коллер Р. «Метод конструирования машин, приборов и аппаратов», 1976, электронный ресурс http://www.metodolog.ru/instruments.html#KOLER дата обращения 31.07.2017, режим доступа свободный

4. Лекция 16: Анализ защищенности информационной системы на основе выявления уязвимостей и обнаружения вторжений http://www.intuit.ru/studies/courses/600/456/lecture/10220?page=3

5. Лукацкий А. Новые подходы к обеспечению информационной безопасности сети. http://compress.ru/article.aspx?id=11178

6. Медведовский И.Д, Семьянов П.В., Платонов В.В. Атака через Интернет. http://citforum.ru/internet/attack/toc.shtml

7. Технические каналы утечки информации. http://www.intuit.ru/studies/courses/2291/591/lecture/12696.

Программное обеспечение:

- windows 7
- office 2007
- dr Web
- UMLet, yEd GNU General Public License
- MS Visio - yEd GNU General Public License

Интернет-ресурсы

- https://biblio-online.ru – ЭБС Юрайт
- http://znanium.com – ЭБС Знаниум
- http://www.prospektnauki.ru – ЭБС Проспект науки
- http://elib.rshu.ru ЭБС ГидроМетеоОнлайн
- https://нэб.рф - Национальная электронная библиотека

7. Методические указания для обучающихся по освоению дисциплины

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. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии
Практические и семинарские занятия	Закрепление знаний на практике. Уяснить задачу на занятие, поставленную преподавателем, активно принимать участие в её решении. При возникновении трудностей сначала попытаться решить с другими студентами, в случае неуспеха, обратиться к преподавателю
Самостоятельная работа	Изучение конспекта лекций, дополнительной литературы. Акцент делать на вопросы, не вошедшие в конспект лекций, на контекст применения изучаемого материала
Подготовка к зачёту	При подготовке к экзамену необходимо ориентироваться на конспекты лекций, рекомендуемую литературу и др.
Текущий контроль	Проверка текущего уровня усвоения материала. Точно и в срок выполнять практические задания

8. Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Тема (раздел) дисциплины	Образовательные и информационные технологии	Перечень программного обеспечения и информационных справочных систем
Введение. Информационная безопасность в современном мире	Чтение лекций с использованием слайд-презентаций, интерактивное взаимодействие педагога и студента; использование деятельностного подхода; сочетание средств эмоционального и рационального воздействия; сочетание индивидуального и коллективного обучения	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web
Особенности информации с точки зрения её защиты	Чтение лекций с использованием слайд-презентаций, интерактивное взаимодействие педагога и студента; использование деятельностного подхода; сочетание средств эмоционального и рационального воздействия; сочетание индивидуального и коллективного обучения	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web UMLet, yEd GNU MS Visio - yEd
Иерархическая модель информационно-вычислительно системы (ИВС)	Чтение лекций с использованием слайд-презентаций, интерактивное взаимодействие педагога и студента; использование деятельностного подхода; сочетание средств эмоционального и рационального воздействия; сочетание индивидуального и коллективного обучения	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web UMLet, yEd GNU MS Visio - yEd
Планирование информационно-технических атак	Чтение лекций с использованием слайд-презентаций, интерактивное взаимодействие педагога и студента; использование деятельностного подхода; сочетание средств эмоционального и рационального воздействия; сочетание индивидуального и коллективного обучения,	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web UMLet, yEd GNU MS Visio - yEd

	творческое задание	
Основные подходы и средства обеспечения информационной безопасности	Чтение лекций с использованием слайд-презентаций, интерактивное взаимодействие педагога и студента; использование деятельностного подхода; сочетание средств эмоционального и рационального воздействия; сочетание индивидуального и коллективного обучения	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web UMLet, yEd GNU MS Visio - yEd
Методы проектирования защищённых ИВС	Чтение лекций с использованием слайд-презентаций, интерактивное взаимодействие педагога и студента; использование деятельностного подхода; сочетание средств эмоционального и рационального воздействия; сочетание индивидуального и коллективного обучения, решение кейса	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web UMLet, yEd GNU MS Visio - yEd
Заключение. Тренды в информационной безопасности	Чтение лекций с использованием слайд-презентаций, интерактивное взаимодействие педагога и студента; использование деятельностного подхода; сочетание средств эмоционального и рационального воздействия; сочетание индивидуального и коллективного обучения	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web

9. Особенности освоения дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Обучение обучающихся с ограниченными возможностями здоровья при необходимости осуществляется на основе адаптированной рабочей программы с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

При определении формы проведения занятий с обучающимся-инвалидом учитываются рекомендации, содержащиеся в индивидуальной программе реабилитации инвалида, относительно рекомендованных условий и видов труда.

При необходимости для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья создаются специальные рабочие места с учетом нарушенных функций и ограничений жизнедеятельности.

10. Материально-техническое обеспечение дисциплины

Учебная аудитории для проведения занятий лекционного типа – укомплектована специализированной (учебной) мебелью, набором демонстрационного оборудования и учебно-наглядными пособиями, обеспечивающими тематические иллюстрации, соответствующие рабочим учебным программам дисциплин (модулей).

Учебная аудитории для проведения занятий практического типа - компьютерный класс с ЛВС связанной с интернетом и мультимедиа. На компьютерах установлен браузер, StarUML, а также MS Visio..

Учебная аудитория для групповых и индивидуальных консультаций - укомплектована специализированной (учебной) мебелью, техническими средствами обучения, служащими для представления учебной информации.

Учебная аудитория для текущего контроля и промежуточной аттестации - укомплектована специализированной (учебной) мебелью, техническими средствами обучения, служащими для представления учебной информации.

Помещение для самостоятельной работы – укомплектовано специализированной (учебной) мебелью, оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечено доступом в электронную информационно-образовательную среду организации

Лаборатория – компьютерный класс с ЛВС связанной с интернетом и мультимедиа. На компьютерах установлен браузер, StarUML, а также MS Visio.

Рассмотрено и рекомендовано к использованию в учебном процессе на 2019/2020 учебный год с изменениями (смотри лист изменений)

Протокол заседания кафедры ИТиСБ от 07.05.2019 №5

Лист Изменений

Изменения, внесенные протоколом заседания кафедры ИТиСБ от 07.05.2019 №5

1. Дисциплина перенесена на 3 семестр.

2. Изменены аудиторные часы в соответствии с таблицей 1 и таблицей 2

Таблица 1 Объем дисциплины по видам учебных занятий в академических часах)

Объём дисциплины	**Всего часов**
	Очная форма обучения
Общая трудоёмкость дисциплины	**72**
Контактная[2] работа обучающихся с преподавателям (по видам аудиторных учебных занятий) – всего[3]:	**28**
в том числе:	
лекции	**14**
практические занятия	**14**
семинарские занятия	
Самостоятельная работа (СРС) – всего:	**44**
в том числе:	
курсовая работа	
контрольная работа	
Вид промежуточной аттестации (зачет/экзамен)	**зачёт**

Таблица 2

№ п/п	**Раздел и тема дисциплины**	**Семестр**	**Виды учебной работы, в т.ч. самостоятельная работа студентов, час.**			**Формы текущего контроля успеваемости**	**Занятия в активной и интерактивной форме, час.**	**Формируемые компетенции**
			Лекции	**Практич.**	**Самост. работа**			
1	Введение. Информационная безопасность в современном мире	**1**	2	2		По итогам дискусси и	4	ОК-5

2	Особенности информации с точки зрения её защиты	**1**	2	2		По итогам творческого задания	4	ОК-5
3	Иерархическая модель информационно-вычислительно системы (ИВС)	**1**	2	2		По итогам творческого задания	4	ОК-5
4	Планирование информационно-технических атак	**1**	2	2		По итогам творческого задания	4	ОК-5
5	Основные подходы и средства обеспечения информационной безопасности	**1**	2	2		По итогам деловой игры	4	ОК-5
6	Методы проектирования защищённых ИВС	**1**	2	2		По итогам решения кейса	4	ОК-5
7	Заключение. Тренды в информационной безопасности	**1**	2	2		По итогам творческого задания	4	ОК-5
	ИТОГО		**14**	**14**			**28**	