Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования «Северо-Осетинский государственный университет имени Коста Левановича Хетагурова»

УТВЕРЖДАЮ
Проректор по УР
_____ Л.М. Дигурова
«28» 05 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Комплексные системы защиты информации (ЭЦП, каналы связи)»

Направление подготовки 01.03.01 Математика

Профиль: "Кибербезопасность"

Форма обучения – очная

Владикавказ, 2019

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 01.03.01 Математика, утвержденным приказом Министерства образования и науки Российской Федерации от 10.01.2018 г. № 8, учебным планом подготовки бакалавриата по направлению подготовки 01.03.01 Математика, профиль: "Кибербезопасность", утвержденным Ученым советом ФГБОУ ВО «СОГУ» от 28.05.2019 г. № 10.

Составитель: Цуцаев А.О.

Рабочая программа обсуждена и утверждена на заседании кафедры прикладной математики (протокол №8 от 14.03.2019)

Одобрена советом факультета математики и информационных технологий (протокол №5 от 29.03.2019)

1. Структура и общая трудоемкость дисциплины

Общая трудоемкость дисциплины составляет 8 зачётных единиц. (288 час.).

	Очная Форма обучения
Курс	4
Семестр	7/8
Лекции	-
Практические занятия	-
Лабораторные занятия	34/40
Консультации	+/+
Итого аудиторных занятий	34/40
Самостоятельная работа	83/77
Курсовая работа	-
Зачет	+/-
Экзамен	27/27
Общее количество часов	288 час.

2. Цели освоения дисциплины

Целью преподавания дисциплины является формирование у студентов устойчивых основ знаний организации комплексных систем защиты информации на предприятии и методов ее управления, приобретения при этом необходимых умений и навыков.

3. Место дисциплины в структуре ОПОП:

Дисциплина «Комплексные системы защиты информации (ЭЦП, каналы связи)» относится к дисциплинам Блок 1. Дисциплины (модули). Часть, формируемая участниками образовательных отношений. Дисциплины по выбору. Б1.В.ДВ.02.02.

Для изучения дисциплины необходимы знания, полученные обучающимися в рамках школьного курса «Информатика и КТ», а также в результате освоения дисциплин: «Основы сетевых технологий (CISCO)», «Введение в криптографию», «Технические средства и методы защиты информации».

4. Требования к результатам освоения дисциплины

Компетенции обучающегося, формируемые в результате освоения дисциплины.

В результате изучения дисциплины обучающийся должен обладать следующими компетенциями (результатами освоения образовательной программы):

УК-1 -Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;

ПК-3 -Способен проводить научно-исследовательские и опытно-конструкторские разработки по отдельным разделам темы.

Взаимосвязь планируемых результатов обучения по дисциплине с формируемыми компетенциями ОПОП:

Компетенции		**Планируемые результаты обучения, соответствующие формируемым компетенциям ОПОП**		
Код	**Формулировка**	**Знать:**	**Уметь**	**Владеть:**

УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	порядок определения источников информации, порядок получения доступа к ним; методы описания и формализации полученной информации; способы верификации получаемой информации; принципы системного подхода; стратегию действий на основе системного подхода, используя обработанную полученную информацию.	использовать способы совершенствования деятельности; умеет использовать способы и приемы самооценки; использовать способы определения приоритетов деятельности	навыками критического анализа проблемных ситуаций;
ПК-3	Способен проводить научно-исследовательские и опытно-конструкторские разработки по отдельным разделам темы	основные методы зашиты информации. алгоритмы классических криптографических шифров и методы построения бизнес моделей. инструменты и методы защиты в бизнес-процессов	осуществлять поиск информации и последующую обработку; анализировать исходную документацию	навыками построения криптостойких систем зашиты информации и применения их при проектировании и реализации бизнес процессов

При проведении учебных занятий обеспечивается развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая при необходимости проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплин (модулей) в форме курсов, составленных на основе результатов научных исследований, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

5. Содержание и учебно-методическая карта дисциплины

Таблица 5.1

Номер недели	Наименование тем (вопросов), изучаемых по данной дисциплине	Занятия			Самостоятельная работа студентов		Формы контроля	Баллы		Литература
		л	пр	лаб	Содержание	Часы		min	max	
1	Структура теории информационной безопасности.			2						**[1-7]**
2	Методология построения систем защиты АС.			2	Построение системы защиты АС.	20	Кейс-задача			**[1-7]**
3	Формальные политики безопасности.			2						**[1-7]**
4	Математические модели информационной безопасности.			2	Составление математической модели информационной безопасности.	10	Кейс-задача			**[1-7]**
5	Основные критерии защищенности АС.			2						**[1-7]**
6	Классы защищенности.			2						**[1-7]**
7	Основные этапы построения защищенной информационной системы.			2	Построение защищенной информационной системы	10	Кейс-задача			**[1-7]**
8	Контроль безопасности информационной системы.			2						**[1-7]**
9	Современные угрозы сетевой безопасности.			2	Разбор основных угроз сетевой безопасности и противодействия им	13	Кейс-задача			**[1-7]**
10	Обеспечение безопасности сетевых устройств.			2						**[1-7]**
11	Аутентификация, авторизация и учет.			2	Настройка систем аутентификации,	10	Кейс-задача			**[1-7]**

					авторизации и учета в виртуальной среде.					
12	Реализация технологий брандмауэра.			2						**[1-7]**
13	Внедрение системы предотвращения вторжений.			2						**[1-7]**
14	Обеспечение безопасности локальной сети (LAN).			2						**[1-7]**
15	Криптографические системы.			2	Обзор криптографические систем. Сравнение	10	реферат			**[1-7]**
16	Многофункциональное устройство обеспечения безопасности.			2						**[1-7]**
17	Управление безопасной сетью.			2	Настройка оборудования для организации безопасной сети.	10	Кейс-задача			**[1-7]**
1	Электронные документы.			4						**[1-7]**
2	Электронная подпись.			4	Криптографические методы защиты информации на основе ЭЦП.	10	Кейс-задача			**[1-7]**
3	Электронная цифровая подпись.			4	Создание электронной подписи.	12	Кейс-задача			**[1-7]**
4	Электронный сертификат.			4	Криптопровайдеры.	8	Кейс-задача			**[1-7]**
5	Электронные ключи eToken.			4	Электронные идентификаторы Рутокен.	10	Кейс-задача			**[1-7]**

6	Проблемы безопасности при применении электронных подписей.			4	Исследование проблем безопасности при применении электронных подписей.	7	Доклад			**[1-7]**
7	Компоненты PKI.									**[1-7]**
8	Принципы доверия PKI.				Эксплуатация PKI.	8	Кейс-задача			**[1-7]**
9	Проверка подлинности цифровых сертификатов в инфраструктуре Windows PKI.				Проверка подлинности цифровых сертификатов в инфраструктуре Windows PKI	12	Кейс-задача			**[1-7]**
10	Процедуры аннулирования сертификатов в Windows PKI.				Аннулированит сертификатов в Windows PKI.	10	Кейс-задача			**[1-7]**
	ИТОГО	0	0	74		160		**0**	**100**	

Примечания:

– Все виды учебной работы могут проводиться дистанционно на основании локальных нормативных актов.

– В целях реализации индивидуального подхода к обучению студентов, осуществляющих учебный процесс по индивидуальной траектории в рамках индивидуального рабочего плана, изучение данной дисциплины может осуществляться через индивидуальные консультации преподавателя очно, в часы консультаций, по электронной почте и с использованием платформ дистанционного обучения.

6. Образовательные технологии

В соответствии с государственными образовательными стандартами высшего образования реализация учебного процесса должна предусматривать проведение занятий в интерактивных и активных формах. Внедрение этих форм обучения – одно из важнейших направлений совершенствования подготовки студентов в современном вузе. Цель – повышение эффективности образовательного процесса, достижение всеми обучающимися высоких результатов обучения.

Интерактивные формы проведения занятий предполагают обучение в сотрудничестве. Все участники образовательного процесса (преподаватель и студенты) взаимодействуют друг с другом, обмениваются информацией, совместно решают проблемы, моделируют ситуации. Суть использования активных и интерактивных форм проведения состоит в погружении студентов в реальную атмосферу делового сотрудничества по разрешению проблем, оптимальную для выработки навыков и качеств будущего специалиста.

Для решения воспитательных и учебных задач преподавателем могут быть использованы следующие интерактивные формы обучения.

Традиционные лекции и практические (семинарские) занятия с использованием современных интерактивных технологий.

Лекция-диалог – содержание подается через серию вопросов, на которые студент должен отвечать непосредственно в ходе лекции.

Онлайн-семинар – разновидность веб-конференции, проведение онлайн-встреч или презентаций через Интернет в режиме реального времени. Каждый из участников находится у своего компьютера (средства связи), а связь между ними поддерживается через Интернет посредством загружаемого приложения, установленного на компьютере каждого участника.

Видеоконференция – сеанс видеоконференцсвязи (ВКС) – это технология интерактивного взаимодействия двух и более участников образовательного процесса для обмена информацией в реальном режиме времени.

Видео-лекция – снятая на камеру сокращенная лекция, дополненная фотографиями и схемами, иллюстрирующая подаваемый в лекции материал.

Технология электронного обучения (реализуется при помощи электронной образовательной среды СОГУ при использовании ресурсов ЭБС, при проведении автоматизированного тестирования и т. д.).

Творческое задание составляет содержание (основу) любой интерактивной формы проведения занятия. Выполнение творческих заданий требует от студента воспроизведения полученной ранее информации в форме, определяемой преподавателем и требующей творческого подхода: 1) подборка примеров из практики; 2) подборка материала по определенной проблеме;

Публичная презентация проекта - самый эффективный способ донесения важной информации при публичных выступлениях. Слайд-презентации позволяют эффектно и наглядно представить содержание, выделить и проиллюстрировать сообщение.

Интерактивная лекция представляет собой выступление преподавателя перед аудиторий студентов с применением следующих интерактивных форм обучения: 1. управляемая дискуссия или беседа; 2. демонстрация слайдов или учебных фильмов; 3. мозговой штурм; 4. мотивационная речь и др.

Разработка проекта позволяет участникам мысленно выйти за пределы аудитории и составить проект своих действий по обсуждаемому вопросу Участники могут обратиться за консультацией, дополнительной литературой в специализированные учреждения, библиотеки и т.д.

Проблемное обучение - поиск ответов на вопросы по теме.

7. Учебно-методическое обеспечение самостоятельной работы

Самостоятельная работа обучающихся является одним из видов учебных занятий. Самостоятельная работа проводится с целью:

− систематизации и закрепления полученных теоретических знаний и практических умений обучающихся студентов;

− углубления и расширения теоретических знаний;

− формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу;

- формирования самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;

− развития исследовательских умений.

К видам самостоятельной работы при изучении данной дисциплины относится: написание докладов, эссе, подготовка презентаций, самостоятельное изучение литературы по теме и составление по ней конспектов, работа со справочными материалами (терминологическими и иными словарями, энциклопедиями) и т.д.

Темы и формы внеаудиторной самостоятельной работы, ее трудоёмкость содержатся в разделе 5, табл. 5.1.

Методические рекомендации по дисциплине прилагаются.

8. Оценочные средства для текущего контроля успеваемости, рубежной аттестации и промежуточной аттестации по итогам освоения дисциплины

Рабочая программа предусматривает проведение лабораторных занятий, а также следующие виды работ: самостоятельную работу студентов по подготовке устных сообщений, написанию докладов, подготовку презентаций и обсуждений по темам дисциплины - работу в активной и интерактивной формах.

Рабочая программа предполагает текущий и промежуточный контроль знаний.

Текущий контроль – это непрерывно осуществляемый мониторинг уровня усвоения знаний и формирования умений и навыков в течение семестра или учебного года. Текущий контроль знаний, умений и навыков студентов осуществляется в ходе учебных (аудиторных) занятий, проводимых по расписанию. Формами текущего контроля выступают опросы на занятиях с целью проверки наличия знаний, необходимых для усвоения нового материала или для выяснения степени усвоения изложенного материала.

Рубежный контроль осуществляется по окончании изучения материала модуля в заранее установленное время. Рубежный контроль проводится с целью определения качества усвоения материала учебного модуля в целом. В течение семестра такие контрольные мероприятия проводятся по графику.

Контрольные задания (демоверсии) для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

1. Методология построения систем защиты АС.
2. Формальные политики безопасности.
3. Основные критерии защищенности АС.
4. Основные этапы построения защищенной информационной системы.
5. Современные угрозы сетевой безопасности.
6. Внедрение системы предотвращения вторжений.
7. Криптографические системы.
8. Электронные документы.

9. Электронная подпись.
10. Электронная цифровая подпись.
11. Криптографические методы защиты информации на основе ЭЦП.
12. Электронный сертификат.
13. Создание электронной подписи.
14. Электронные ключи eToken.
15. Проблемы безопасности при применении электронных подписей.
16. Компоненты PKI.
17. Эксплуатация PKI.

Критерии оценивания представлены в таблице 8.1.

Примеры тестовых заданий по дисциплине:

1. Шифрование – это…
   способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого
   совокупность тем или иным способом структурированных данных и комплексом аппаратно-программных средств
   удобная среда для вычисления конечного пользователя

2. Кодирование – это…
   преобразование обычного, понятного текста в код
   преобразование
   написание программы

3.Что требуется для восстановления зашифрованного текста
   Ключ
   Матрица
   вектор

4.Когда появилось шифрование
   четыре тысячи лет назад
   две тысячи лет назад
   пять тысяч лет назад

5.Первым известным применением шифра считается
   египетский текст
   русский
   нет правильного ответа

6.Какую секретную информацию хранит Windows
   пароли для доступа к сетевым ресурсам
   пароли для доступа в Интернет
   сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере

7.Алфавит – это…
   конечное множество используемых для кодирования информации знаков
   буквы текста
   нет правильного ответа

8.Текст – это…
упорядоченный набор из элементов алфавита
конечное множество используемых для кодирования информации знаков
все правильные

9.Шифрование – это…
преобразовательный процесс исходного текста в зашифрованный
упорядоченный набор из элементов алфавита
нет правильного ответа

10.Дешифрование – это…
на основе ключа шифрованный текст преобразуется в исходный
пароли для доступа к сетевым ресурсам
сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере

11.Криптографическая система представляет собой…
семейство T преобразований открытого текста, члены его семейства индексируются символом k
программу
систему

Методика формирования результирующей оценки

Таблица 8.1

Этап	**Форма контроля**	**Критерии оценивания (процент от максимального кол-ва баллов)**			
		86-100 %	**71–85%**	**60–70%**	**Менее 60%**
1. Текущий контроль (max 25 баллов за 1 модуль)					
		7-8 баллов	6–7 баллов	4–5 баллов	0–3 баллов
	Посещение занятий (max 8 б.)	Студент посетил более 85% занятий	Студент посетил 71–85% занятий	Студент посетил 56–70% занятий	Студент посетил менее 56% занятий
		9–10 баллов	7–8 баллов	6–7 баллов	0–5 баллов
	Текущая работа в течение модуля (мах 10б.)	Студент активно работает на занятиях, превосходно выполняет все задания преподавателя.	Студент активно работает на занятиях, хорошо выполняет задания преподавателя.	Студент недостаточно активно работает на занятиях, удовлетворительно выполняет задания преподавателя.	Студент недостаточно активно работает на занятиях, неудовлетворительно выполняет задания преподавателя.
		3/2 балла	2 балла	1 балл	0 баллов
	Доклад, презентация (мах 3б.) / опорный конспект (max 2б.)	Тема полностью раскрыта. Превосходное владение материалом. Высокий уровень самостоятельности, логичности, аргументированности. Превосходный стиль изложения.	Тема в основном раскрыта. Хорошее владение материалом. Средний уровень самостоятельности, логичности, аргументированности. Хороший стиль изложения.	Тема частично раскрыта. Удовлетворительное владение материалом. Низкий уровень самостоятельности, логичности, аргументированности. Удовлетворительный стиль изложения.	Тема не раскрыта. Неудовлетворительное владение материалом. Недостаточный уровень самостоятельности, логичности, аргументированности. Неудовлетворительный стиль изложения.

2. Рубежный контроль (25б. за 1 модуль)					
		22–25 баллов	18–21 балл	14–17 баллов	0–13 баллов
	Контрольная работа	Правильно выполнены все задания. Продемонстрирован высокий уровень владения материалом. Проявлены превосходные способности применять знания и умения к выполнению конкретных заданий.	Правильно выполнена большая часть заданий. Присутствуют незначительные ошибки. Продемонстрирован хороший уровень владения материалом. Проявлены средние способности применять знания и умения к выполнению конкретных заданий.	Задания выполнены более чем наполовину. Присутствуют серьезные ошибки. Продемонстрирован удовлетворительный уровень владения материалом. Проявлены низкие способности применять знания и умения к выполнению конкретных заданий.	Задания выполнены менее чем наполовину. Продемонстрирован неудовлетворительный уровень владения материалом. Проявлены недостаточные способности применять знания и умения к выполнению конкретных заданий.
3. Итоговый контроль по дисциплине					
		43–50 баллов	36–42 балла	28–35 баллов	0–27 баллов
	Экзамен/зачет	Дан полный, развернутый ответ на поставленный вопрос. Ответ формулируется в терминах науки, изложен литературным языком, логичен, доказателен, демонстрирует авторскую позицию студента.	Дан полный ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Но допущены незначительные ошибки, исправленные студентом с помощью «наводящих» вопросов преподавателя.	Дан недостаточно полный ответ. Студент не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи. Речевое оформление требует поправок, коррекции.	Не получены ответы по базовым вопросам дисциплины или дан неполный ответ и допущены грубые ошибки. Речь неграмотная. Уточняющие вопросы преподавателя не приводят к коррекции ответа студента не только на поставленный вопрос, но и на другие вопросы дисциплины.

Студенты, получившие в ходе текущего и рубежного контроля 56-100 баллов, автоматически получают «Зачет» или соответствующую шкале экзаменационную оценку. Результирующая оценка складывается по соответствующей БРС формуле.

Вопросы для подготовки к зачёту/экзамену:

1. Структура теории информационной безопасности.
2. Методология построения систем защиты АС.
3. Формальные политики безопасности.
4. Математические модели информационной безопасности.
5. Основные критерии защищенности АС.
6. Классы защищенности.
7. Основные этапы построения защищенной информационной системы.
8. Контроль безопасности информационной системы.
9. Современные угрозы сетевой безопасности.
10. Обеспечение безопасности сетевых устройств.

11. Аутентификация, авторизация и учет.
12. Реализация технологий брандмауэра.
13. Внедрение системы предотвращения вторжений.
14. Обеспечение безопасности локальной сети (LAN).
15. Криптографические системы.
16. Многофункциональное устройство обеспечения безопасности.
17. Управление безопасной сетью.
18. Электронные документы.
19. Электронная подпись.
20. Электронная цифровая подпись.
21. Криптографические методы защиты информации на основе ЭЦП.
22. Электронный сертификат.
23. Криптопровайдеры.
24. Создание электронной подписи.
25. Электронные ключи eToken.
26. Электронные идентификаторы Рутокен.
27. Проблемы безопасности при применении электронных подписей.
28. Компоненты PKI.
29. Принципы доверия PKI.
30. Эксплуатация PKI.
31. Проверка подлинности цифровых сертификатов в инфраструктуре Windows PKI.
32. Процедуры аннулирования сертификатов в Windows PKI.

Показатели и критерии оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Уровень сформированности компетенций			
«Минимальный уровень не достигнут» (менее 60 баллов)	**«Минимальный уровень» (60-70 баллов)**	**«Средний уровень» (71-85 баллов)**	**«Высокий уровень» (86-100 баллов)**
Компетенции не сформированы. Знания отсутствуют, умения и навыки не сформированы.	*Компетенции сформированы.* Сформированы базовые структуры знаний. Умения фрагментарны и носят репродуктивный характер. Демонстрируется низкий уровень самостоятельности практического навыка.	*Компетенции сформированы.* Знания обширные, системные. Умения носят репродуктивный характер, применяются к решению типовых заданий. Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка.	*Компетенции сформированы.* Знания твердые, аргументированные, всесторонние. Умения успешно применяются к решению как типовых, так и нестандартных творческих заданий. Демонстрируется высокий уровень самостоятельности, высокая адаптивность практического навыка
Описание критериев оценивания			
Обучающийся демонстрирует:	Обучающийся демонстрирует:	Обучающийся демонстрирует:	Обучающийся демонстрирует:

- существенные пробелы в знаниях учебного материала; - допускаются принципиальные ошибки при ответе на основные вопросы, отсутствует знание и понимание основных понятий и категорий; -непонимание сущности дополнительных вопросов в рамках заданий; - отсутствие умения выполнять практические задания, предусмотренные программой дисциплины; - отсутствие готовности (способности) к дискуссии и низкую степень контактности.	- знания теоретического материала; - неполные ответы на основные вопросы, ошибки в ответе, недостаточное понимание сущности излагаемых вопросов; - неуверенные и неточные ответы на дополнительные вопросы; - недостаточное владение литературой, рекомендованной программой дисциплины; - умение без грубых ошибок решать практические задания, которые следует выполнить.	- знание и понимание основных вопросов контролируемого объема программного материала; - твердые знания теоретического материала. -способность устанавливать и объяснять связь практики и теории, выявлять противоречия, проблемы и тенденции развития; - правильные и конкретные, без грубых ошибок, ответы на поставленные вопросы; - умение решать практические задания, которые следует выполнить; - владение основной литературой, рекомендованной программой дисциплины; - наличие собственной обоснованной позиции по обсуждаемым вопросам. Возможны незначительные оговорки и неточности в раскрытии отдельных положений вопросов, присутствует неуверенность в ответах.	- глубокие, всесторонние и аргументированные знания программного материала; - полное понимание сущности и взаимосвязи рассматриваемых процессов и явлений, точное знание основных понятий в рамках обсуждаемых заданий; - способность устанавливать и объяснять связь практики и теории; - логически последовательные, содержательные, конкретные и исчерпывающие ответы на все задания, а также дополнительные вопросы экзаменатора; - умение решать практические задания; - свободное использование в ответах на вопросы материалов рекомендованной основной и дополнительной литературы.
Оценка «неудовлетворительно» /не зачтено	**Оценка «удовлетворительно» / «зачтено»**	**Оценка «хорошо» / «зачтено»**	**Оценка «отлично» / «зачтено»**

9. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Ельчанинова, Н.Б. Правовые основы защиты информации с ограниченным доступом : учебное пособие / Н.Б. Ельчанинова ; Министерство науки и высшего образования РФ, Южный федеральный университет, Инженерно-технологическая академия. –

Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2017. – 77 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=499598 – Библиогр. в кн. – ISBN 978-5-9275-2501-0. – Текст : электронный.

2. Лапонина, О.Р. Межсетевые экраны : учебное пособие / О.Р. Лапонина. – 2-е изд., исправ. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 466 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=429093 – Текст : электронный.
3. Мэйволд, Э. Безопасность сетей / Э. Мэйволд. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 572 с. : схем., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=429035 – Текст : электронный.
4. Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 369 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=428820 – Текст : электронный.
5. *Внуков, А. А.* Защита информации в банковских системах : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2017. — 246 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01679-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/400283 .

б) дополнительная литература:

6. Голиков, А.М. Защита информации от утечки по техническим каналам : учебное пособие : [16+] / А.М. Голиков ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 256 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=480636 – Библиогр.: с. 213. – Текст : электронный.
7. Пилиди, В.С. Математические основы защиты информации : учебное пособие : [16+] / В.С. Пилиди ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2019. – 309 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=577894 – Библиогр.: с. 301. – ISBN 978-5-9275-3363-3. – Текст : электронный.

в) электронные библиотечные системы, с которыми у СОГУ имеется действующий договор, современные профессиональные базы, информационные справочные системы:

– eLIBRARY.RU [Электронный ресурс]: научная электронная библиотека. – URL: http://www.elibrary.ru.

– База данных «ЭБС elibrary»: http://elibrary.ru

– Издательство «Юрайт» [Электронный ресурс]: электронно-библиотечная система. – URL: http://biblio-online.ru.

- Университетская библиотека online [Электронный ресурс]: электронно-библиотечная система. – URL: http://www.biblioclub.ru.

10. Материально-техническое обеспечение дисциплины

Занятия по дисциплине проводятся в аудиториях, обеспеченных компьютерами, имеющими доступ к сети Интернет, интерактивными досками и мультимедийным оборудованием.

Лицензионное программное обеспечение:

1. Windows 10 Pro for Workstations, (№ 4100072800 Microsoft Products (MPSA) от 04.2016г);
2. Office Standard 2016 (№ 4100072800 Microsoft Products (MPSA) от 04.2016г);
3. Система поиска текстовых заимствований «Антиплагиат ВУЗ»;
4. CiscoWebex- Система проведения вебинаров (ООО Айстекдоговор № Д83-2020 от 10.08.2020-10.08.2021 г.).

Перечень ПО в свободном доступе:

1. Kaspersky Free;
2. WinRar;
3. Google Chrome;
4. Yandex Browser;
5. OperaBrowser;
6. Cisco Packet Tracer.

11. Лист обновления/актуализации

1. Рабочая программа

пересмотрена и актуализирована на заседании кафедры прикладной математики протокол № 7 от 19.03.2020г.;

одобрена на заседании совета факультета математики и информационных технологий, протокол № 5 от 27.03.2020 г.