МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
"Казанский (Приволжский) федеральный университет"
Набережночелнинский институт (филиал)
Отделение информационных технологий и энергетических систем

УТВЕРЖДАЮ
Заместитель директора
по образовательной деятельности
НЧИ КФУ
_____ Н.Д. Ахметов
"31" августа 2020 г.

Программа дисциплины
Методы защиты информации

Направление подготовки: 01.03.02 - Прикладная математика и информатика
Профиль подготовки: отсутствует
Квалификация выпускника: бакалавр
Форма обучения: очная
Язык обучения: русский
Год начала обучения по образовательной программе: 2019

Содержание

Программу дисциплины разработали доцент, к. физ.-мат. н. (доцент) Товштейн М.Я.. (Кафедра системного анализа и информатики, Отделение информационных технологий и энергетических систем), MYTovshtejn@kpfu.ru; старший преподаватель, б/с Грудцына Л.Ю. (Кафедра системного анализа и информатики, Отделение информационных технологий и энергетических систем), LJGrudcyna@kpfu.ru.

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП ВО

Обучающийся, освоивший дисциплину (модуль), должен обладать следующими компетенциями:

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-4	Способен к разработке требований и проектированию программного обеспечения
ПК-6	Способен к обеспечению информационной безопасности на уровне баз данных

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

- роль информация как объекта защиты и возможные угрозы информационной безопасности, чтобы проектировать программное обеспечение и разрабатывать требования к нему;
- способы обеспечения информационной безопасности на уровне баз данных.

Должен уметь:

- ориентироваться в правовых и технических средствах защиты информации с учётом основных требований к проектированию программного обеспечения;
- реализовать криптографические методы защиты информации, обеспечивающие информационную безопасность на уровне баз данных.

Должен владеть навыками:

- ориентироваться в административно-организационных средствах защиты конфиденциальных данных для сохранения их при решении задач, возникающих при разработке требований к проектированию программного обеспечения;
- предотвращать приёмами криптографии несанкционированный доступ к информации на уровне баз данных, в сети Интернет и в других источниках.

2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1. Дисциплины (модули)" основной профессиональной образовательной программы 01.03.02 "Прикладная математика и информатика " и относится к вариативной части.
Осваивается на 4 курсе в 8 семестре.

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

Общая трудоемкость дисциплины составляет 3 зачетные единицы на 108 часов.

Контактная работа - 50 часов, в том числе лекции - 20 часов, практические занятия - 0 часов, лабораторные работы - 30 часов, контроль самостоятельной работы - 0 часов.

Самостоятельная работа - 58 часов.

Контроль (зачёт / экзамен) - 0 часов.

Форма промежуточного контроля дисциплины зачет в 8 семестре

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

4.1 Структура и тематический план контактной и самостоятельной работы по дисциплине (модулю)

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Информация как объект защиты.	8	2	0	0	4
2.	Тема 2. Правовые средства защиты информации от несанкционированного доступа	8	2	0	4	8
3.	Тема 3. Угрозы информационной безопасности предприятия.	8	2	0	2	2
4.	Тема 4. Административно - организационные средства защиты информации.	8	2	0	2	2
5.	Тема 5. Технические аспекты обеспечения защиты информации.	8	2	0	2	4
6.	Тема 6. Криптографические симметричные методы защиты информации.	8	4	0	10	18
7.	Тема 7. Криптографические асимметричные методы защиты информации.	8	6	0	10	20
	Итого		20	0	30	58

4.2 Содержание дисциплины (модуля)

Тема 1. Информация как объект защиты.

Различные определения понятия "информация": философские, техноцентрические, антропоцентрические. Особенности определения информации, данного в ФЗ "Об информации, информационных технологиях и о защите информации" от 6 июля 2016 г (в редакции ФЗ РФ от 03.04.2020 г. №105-ФЗ):"Информация - сведения (сообщения, данные) независимо от формы их представления". Способы поиска, хранения, обработки и анализа информации из различных источников с целью возможного применения методов её защиты .

Тема 2. Правовые средства защиты информации от несанкционированного доступа

Информационная безопасностью как защищенность информации и поддерживающей инфраструктуру от случайных или преднамеренных воздействий естественного или искусственного характера. Основные требования информационной безопасности. Виды государственных нормативных актов по защиты информации. Информация как объект правовых отношений.

Тема 3. Угрозы информационной безопасности предприятия.

Угроза как потенциальная возможность нарушить информационную безопасность. Атака -

попытка реализации угрозы. Потенциальные злоумышленники как источниками угрозы. Классификация средств защиты информации. Угрозы информационным ресурсам предприятия.

Роль морально-этических средств защиты информации. Технология работы с компьютером для поиска, хранения, обработки и анализа информации из различных источников с целью возможного применения методов защиты данных.

Тема 4. Административно - организационные средства защиты информации.

Организационные меры охраны конфиденциальных сведений на предприятиях малого бизнеса. Регламентация процессов функционирования систем, деятельность персонала по обеспечению безопасности. Меры, осуществляемые при проектировании, строительстве и оборудовании объектов обработки данных, а также мероприятия при подборе и постановки персонала, обслуживающего систему. Организация учёта, хранения, использования и уничтожение документов и носителя информации.

Организация разграничения доступа. Организация явного или скрытого контроля за работой пользователе

Тема 5. Технические аспекты обеспечения защиты информации.

Понятия идентификации и аутентификации. Принципы аутентификации: а) пользователь знает, б) пользователь имеет , в) пользователь есть. Каналы утечки информации. Краткие сведения о средствах съёма и защиты информации. Техническое оснащение рабочих мест и размещения технологического оборудования для предотвращения несанкционированного доступа к конфиденциальной информации

Тема 6. Криптографические симметричные методы защиты информации.

Методы закрытия данных симметричным ключом при работе с компьютером для поиска, хранения, обработки и анализа информации из различных источников 1) подстановка (замена), (2) простая перестановка, (3) вертикальная перестановка , (4) двойная перестановка, (5) гаммирование, (6) матричная алгебра как пример применения аналитического преобразования.

Тема 7. Криптографические асимметричные методы защиты информации

Недостатки симметричных методов шифрования и их устранение асимметричными методами. Протокол обмена сообщениями при асимметричном шифровании. Сочетание метода гаммирования с асимметричным методом шифрования для защиты канала связи между корреспондентами. Достоинства и недостатки ручной подписи. Назначение ЭЦП и сопоставление её с ручной подписью. Назначение дайджеста (слепка, контрольной суммы) сообщения. Роль дайджеста в защите информации. Назначение хеш-функции, реализующей дайджест сообщения. Алгоритм создания хеш-функции

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Самостоятельная работа обучающихся выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Самостоятельная работа подразделяется на самостоятельную работу на аудиторных занятиях и на внеаудиторную самостоятельную работу. Самостоятельная работа обучающихся включает как полностью самостоятельное освоение отдельных тем (разделов) дисциплины, так и проработку тем (разделов), осваиваемых во время аудиторной работы. Во время самостоятельной работы обучающиеся читают и конспектируют учебную, научную и справочную литературу, выполняют задания, направленные на закрепление знаний и отработку умений и навыков, готовятся к текущему и промежуточному контролю по дисциплине.

Организация самостоятельной работы обучающихся регламентируется нормативными документами, учебно-методической литературой и электронными образовательными ресурсами, включая:

Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры (утвержден приказом Министерства образования и

науки Российской Федерации от 5 апреля 2017 года №301)

Письмо Министерства образования Российской Федерации №14-55-996ин/15 от 27 ноября 2002 г. "Об активизации самостоятельной работы студентов высших учебных заведений"

Устав федерального государственного автономного образовательного учреждения "Казанский (Приволжский) федеральный университет"

Правила внутреннего распорядка федерального государственного автономного образовательного учреждения высшего профессионального образования "Казанский (Приволжский) федеральный университет"

Локальные нормативные акты Казанского (Приволжского) федерального университета

6. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств по дисциплине (модулю) включает оценочные материалы, направленные на проверку освоения компетенций, в том числе знаний, умений и навыков. Фонд оценочных средств включает оценочные средства текущего контроля и оценочные средства промежуточной аттестации.

В фонде оценочных средств содержится следующая информация:

– соответствие компетенций планируемым результатам обучения по дисциплине (модулю);

– индикаторы оценивания сформированности компетенций;

– механизм формирования оценки по дисциплине (модулю);

– описание порядка применения и процедуры оценивания для каждого оценочного средства;

– критерии оценивания для каждого оценочного средства;

– содержание оценочных средств, включая требования, предъявляемые к действиям обучающихся, демонстрируемым результатам, задания различных типов.

Фонд оценочных средств по дисциплине находится в Приложении 1 к программе дисциплины (модулю).

7. Перечень литературы, необходимой для освоения дисциплины (модуля)

Освоение дисциплины (модуля) предполагает изучение основной и дополнительной учебной литературы. Литература может быть доступна обучающимся в одном из двух вариантов (либо в обоих из них):

- в электронном виде - через электронные библиотечные системы на основании заключенных КФУ договоров с правообладателями и предоставленных доступов НЧИ КФУ;

- в печатном виде - в фонде библиотеки Набережночелнинского института (филиала) КФУ. Обучающиеся получают учебную литературу на абонементе по читательским билетам в соответствии с правилами пользования библиотекой.

Электронные издания доступны дистанционно из любой точки при введении обучающимся своего логина и пароля от личного кабинета в системе "Электронный университет". При использовании печатных изданий библиотечный фонд должен быть укомплектован ими из расчета не менее 0,25 экземпляра каждого из изданий, указанных в рабочей программе дисциплины, на одного обучающегося из числа лиц, одновременно осваивающих данную дисциплину.

Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля), находится в Приложении 2 к рабочей программе дисциплины. Он подлежит обновлению при изменении условий договоров КФУ с правообладателями электронных изданий и при изменении комплектования фондов библиотеки Набережночелнинского института (филиала) КФУ.

8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

Единое окно доступа к образовательным ресурсам - http://window.edu.ru
RSDN : сайт, посвященный разработке программного обеспечения - http://rsdn.ru/
Институт системного анализа РАН - http://www.isa.ru
Научная электронная библиотека - http://elibrary.ru
Общероссийский математический портал - http://www.mathnet.ru

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Вид работ	Методические рекомендации
лекции	Во время лекционных занятий студенту рекомендуется вести краткий конспект, фиксируя основные теоретические положения изучаемых разделов дисциплины. В качестве источников получения теоретических и справочных сведений лекции можно рассматривать как первичный, однако не единственный источник. Помимо лекций студент должен активно и самостоятельно работать с литературными источниками, источниками в сети Интернет. В случае применения дистанционных образовательных технологий работа представляется в платформе "Microsoft Teams".
отчёт по лабораторным работам	Рекомендуемая схема выполнения заданий к лабораторной работе по данной дисциплине включает следующие этапы: 1) Ознакомление с заданием. 2) Изучение необходимого теоретического материала. 3) Изучение примеров выполнения задания. 4) Выполнение задания в соответствии с теорией и примером. Лабораторные занятия проводятся с использованием интерактивных методов: работа в парах при передаче ключей шифрования, обсуждение конкретного метода защиты сообщения. Важно грамотно подготовиться к работе, прочитать рекомендованный материал из учебно-методической литературы. Выполненная на компьютере работа заканчивается оформлением письменного отчёта, который должен быть защищён к установленному сроку. Защита лабораторной работы заключается в проверке преподавателем задания согласно определенному варианту. В ходе защиты преподаватель задает студенту вопросы, касающиеся технологии выполнения задания, а также соответствующего лекционного материала. В процессе ответа студент должен продемонстрировать понимание сущности выполненных им действий и должен быть в состоянии описать практическую значимость полученных результатов. Неспособность студента грамотно ответить на поставленные вопросы является поводом для преподавателя усомниться в авторстве работы. В случае применения дистанционных образовательных технологий отчёты по лабораторным работам представляются в платформе "Microsoft Teams".
самостоятельная работа	Самостоятельная работа по дисциплине заключается в следующем: доработка лабораторных работ, изучение теоретического материала на основе конспектов лекций и рекомендованных учебников и учебных пособий, а также подготовка экзамену. Особенностью обучения бакалавров является высокий уровень самостоятельности в ходе образовательного процесса. Можно выделить два вида самостоятельной работы - аудиторная, под руководством преподавателя, и внеаудиторная. Аудиторная самостоятельная работа по дисциплине выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию. Внеаудиторная самостоятельная работа выполняется по заданию преподавателя, но без его непосредственного участия.

Вид работ	Методические рекомендации
	На аудиторных занятиях с участием преподавателя применяются следующие формы СРС: - текущие консультации; - разбор и проработка основных вопросов, освещённых на лекции, и способов решения задач по дисциплине. Внеаудиторная самостоятельная работа заключается в следующем: - проработка и усвоение теоретического материала на базе рекомендованной преподавателем учебной литературы (включая электронные библиотеки и др.); - подготовка к лабораторным занятиям (изучение образцов выполнения заданий, разобранных примеров решения некоторых задач и др.); - подготовка к защите выполненных лабораторных работ; - подготовка к письменному заданию; - подготовка к экзамену. При работе с литературой следует в первую очередь обращаться к основной литературе по дисциплине, причём работа с литературными источниками и источниками сети Интернет должна проводиться систематически. При этом желательно получить полное представление об интересующих вопросах, особенно, если возникли трудности в понимании какой-то темы Результатом такой работы должна быть систематизация и структурирование учебного материала Поэтому остается только найти элементы этих систем и выявить существующие между ними связи и отношения. Результатом самостоятельной работы должна быть систематизация и структурирование учебного материала по изучаемой теме, включение его в уже имеющуюся систему знаний. Поэтому остается только найти элементы этих систем и выявить существующие между ними связи и отношения. В случае применения дистанционных образовательных технологий работа представляется в платформе "Microsoft Teams".
письменное домашнее задание	Задание представляет собой перечень вопросов, на которые студент отвечает письменно. Ответы он находит в конспекте лекций, в рекомендованных литературных и /или интенет-источниках. Поощряется использование дополнительного материала, обоснование высказанного ответа и вообще — грамотное проявление творческого подхода. Сама работа оформляется на стандартном листе белой бумаги формата А4 на одной стороне (210х297 мм). Рекомендуемый шрифт -TimesNewRoman, межстрочный интервал полуторный, 14 кегль, в таблицах - 12, в подстрочных сносках - 10. Титульный лист заполняется по единому образцу. Надпись " Домашнее задание" печатается 18 шрифтом. Подчеркивание слов и выделение их курсивом не допускается. Поля сверху, снизу по 20 мм, справа - 20 мм, слева - 30 мм, отступ первой строки абзаца - 1,25, выравнивание по ширине. Объём работы составляет 10-20 страниц, включая титульный лист, оглавление, введение, список использованных источников. . В оглавлении, следующим за титульным листом, перечисляются разделы, части и параграфы с указанием номеров страниц. Названия параграфов (подзаголовки) выделяются полужирным шрифтом и выравниваются по центру. В конце заголовка (подзаголовка) точка не ставится. Размер заголовка - 16 пт., подзаголовка - 14 пт. Каждый параграф начинается с новой страницы. Расстояние между заголовком и подзаголовком, заголовком и последующим текстом, подзаголовком и предыдущим текстом отделяют двумя полуторными межстрочными интервалами (одной пустой строкой), а между подзаголовком и последующим текстом - одним полуторным

Вид работ	Методические рекомендации
	межстрочным интервалом (как строки последующего текста). Страницы должны иметь сквозную нумерацию арабскими цифрами по всему тексту. Номер страницы проставляют в центре нижнего поля страницы без точки в конце. Первой страницей письменной работы является титульный лист. Он не нумеруется. Размер шрифта, используемого для нумерации, должен быть меньше, чем у основного текста. В работе второй страницей является оглавление. Обоснование того или иного положения возможно с помощью цитат из научной, справочной и иной литературы. Необходимо учитывать правила включения в текст цитат и оформления сносок на используемые источники. В случае применения дистанционных образовательных технологий работа представляется в платформе "Microsoft Teams".
письменная работа	Работа выполняется письменно в аудитории и сдаётся преподавателю. Студенты получают задание по освещению вопросов, указанных в приложении 1. Оцениваются знания по теме работы, аналитические способности, умения и навыки, необходимые для выполнения заданий. На ответы даётся 60 минут В случае применения дистанционных образовательных технологий работа представляется в платформе "Microsoft Teams".
Зачёт	Бакалавр к этому времени уже знает, что зачёт - это заключительный этап работы в семестре по данной дисциплине. И понимает, что важнейшую роль для успешной его сдачи играют не только посещение занятий, но также и то, насколько внимательнен и активен он был на лекциях, при выполнении и защите лабораторные работ, при самостоятельной работе над учебно-методической литературой и интернет-источниками. Но решающую роль на этом этапе играет тот факт, насколько успешно прошла защита самостоятельно выполненных лабораторных работ. Именно это проявляется при ответе на вопросы, предоставленные студенту для подготовки к зачёту. Следует отметить, что неблагоприятное впечатление при ответе на билет вызывает чтение студентом написанного текста. Желателен свободный рассказ по существу с объяснением приготовленных примеров. Зачёт проводится в письменной форме по билетам. В билете 2 вопроса. Они включаются в билеты из списка в 30 вопросов, которые заранее известны студенту. Время, отводимое для подготовки к ответу, – 1 академический час. В случае применения дистанционных образовательных технологий используется платформа «Microsoft Teams». Билеты по сказанному студентом номеру преподаватель показывает на экране монитора. После некоторой подготовки студент отвечает на вопросы билета как при обычном очном экзамене в аудитории. Могут быть заданы преподавателем уточняющие вопросы по данному билету или по некоторым темам дисциплины.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем, представлен в Приложении 3 к рабочей программе дисциплины (модуля).

11. Описание материально-технической базы, необходимой для осуществления

образовательного процесса по дисциплине (модулю)

Материально-техническое обеспечение образовательного процесса по дисциплине (модулю) включает в себя следующие компоненты:

Помещения для самостоятельной работы обучающихся, укомплектованные специализированной мебелью и оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду КФУ.

Учебные аудитории – помещения для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные специальной мебелью и оборудованием:

- Меловая доска
- Ноутбук, проектор, экран
- Компьютеры

Рабочий кабинет – помещение для хранения и профилактического обслуживания учебного оборудования.

12. Средства адаптации преподавания дисциплины к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья

При необходимости в образовательном процессе применяются следующие методы и технологии, облегчающие восприятие информации обучающимися инвалидами и лицами с ограниченными возможностями здоровья:

- создание текстовой версии любого нетекстового контента для его возможного преобразования в альтернативные формы, удобные для различных пользователей;

- создание контента, который можно представить в различных видах без потери данных или структуры, предусмотреть возможность масштабирования текста и изображений без потери качества, предусмотреть доступность управления контентом с клавиатуры;

- создание возможностей для обучающихся воспринимать одну и ту же информацию из разных источников - например, так, чтобы лица с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально;

- применение программных средств, обеспечивающих возможность освоения навыков и умений, формируемых дисциплиной, за счёт альтернативных способов, в том числе виртуальных лабораторий и симуляционных технологий;

- применение дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем, в том числе вебинаров, которые могут быть использованы для проведения виртуальных лекций с возможностью взаимодействия всех участников дистанционного обучения, проведения семинаров, выступления с докладами и защиты выполненных работ, проведения тренингов, организации коллективной работы;

- применение дистанционных образовательных технологий для организации форм текущего и промежуточного контроля;

- увеличение продолжительности сдачи обучающимся инвалидом или лицом с ограниченными возможностями здоровья форм промежуточной аттестации по отношению к установленной продолжительности их сдачи:

- продолжительности сдачи зачёта или экзамена, проводимого в письменной форме, - не более чем на 90 минут;

- продолжительности подготовки обучающегося к ответу на зачёте или экзамене, проводимом в устной форме, - не более чем на 20 минут;

- продолжительности выступления обучающегося при защите курсовой работы - не более чем на 15 минут.

Программа составлена в соответствии с требованиями ФГОС ВО и учебным планом по

направлению 01.03.02 "Прикладная математика и информатика".

Приложение №1
к рабочей программе дисциплины (модуля)
«Методы защиты информации»

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Казанский (Приволжский) федеральный университет»

Набережночелнинский институт (филиал)
Отделение информационных технологий и энергетических систем

Фонд оценочных средств по дисциплине (модулю)
Методы зашиты информации

Направление подготовки: 01.03.02 - Прикладная математика и информатика
Направленность (профиль) подготовки: отсутствует
Квалификация выпускника: бакалавр
Форма обучения: очная
Язык обучения: русский
Год начала обучения по образовательной программе: 2019

СОДЕРЖАНИЕ

1. **Соответствие компетенций планируемым результатам обучения по дисциплине (модулю)**

Код и наименование компетенции	Индикаторы достижения компетенций для данной дисциплины	Оценочные средства текущего контроля и промежуточной аттестации
ПК-4 Способен к разработке требований и проектированию программного обеспечения	Должен знать: роль информация как объекта защиты и возможные угрозы информационной безопасности, чтобы проектировать программное обеспечение и разрабатывать требования к нему. Должен уметь: ориентироваться в правовых и технических средствах защиты информации с учётом основных требований к проектированию программного обеспечения. Должен иметь навыки: ориентироваться в административно-организационных средствах защиты конфиденциальных данных для сохранения их при решении задач, возникающих при разработке требований к проектированию программного обеспечения.	**Текущий контроль:** 1. Письменное домашнее задание Тема 1. Информация как объект защиты. Тема 2. Правовые средства защиты информации от несанкционированного доступа. Тема 6. Технические аспекты обеспечения защиты 2. Письменная работа Тема 3. Угрозы информационной безопасности Тема 4. Административно-организационные средства защиты информации. **Промежуточная аттестация** - зачёт: контрольные вопросы
ПК-6 Способен к обеспечению информационной безопасности на уровне баз данных	Должен знать: способы обеспечения информационной безопасности на уровне баз данных. Должен уметь: реализовать криптографические методы защиты информации, обеспечивающие информационную безопасность на уровне баз данных. Должен владеть навыками: предотвращать приёмами криптографии несанкционированный доступ к информации на уровне баз данных, в сети Интернет и в других источниках.	**Текущий контроль:** 1. Отчёт по лабораторным работам Тема 5. Криптографические симметричные методы защиты информации (задания 1-9). Тема 7. Криптографические асимметричные методы защиты информации (задания 10-14). **Промежуточная аттестация** - зачёт: контрольные вопросы

2. Индикаторы оценивания сформированности компетенций

Компетенция	Зачтено			Не зачтено
	Высокий уровень (отлично) (86-100 баллов)	**Средний уровень (хорошо) (71-85 баллов)**	**Низкий уровень (удовлетворительно) (56-70 баллов)**	**Ниже порогового уровня (неудовлетворительно) (0-55 баллов**
ПК-4	Знает роль информация как объекта защиты и угрозы информационной безопасности, симметричные и асимметричные методы защиты сообщений, чтобы проектировать программное обеспечение и разрабатывать требования к нему Правильно и в срок выполняет все задания.	Знает роль информация как объекта защиты и угрозы информационной безопасности, чтобы проектировать программное обеспечение и разрабатывать требования к нему. Правильно, но с некоторыми опозданиями выполняет все задания.	Знает роль информация как объекта защиты и лишь некоторые угрозы информационной безопасности, чтобы проектировать программное обеспечение и разрабатывать требования к нему. После нескольких исправлений и с опозданием выполняет лишь некоторые задания.	Не знает роли информации как объекта защиты и лишь некоторые угрозы информационной безопасности, поэтому вряд ли сможет проектировать программное обеспечение и разрабатывать требования к нему. Не выполнены многие из заданий, причём не может грамотно объяснить полученные результаты.
	Умеет ориентироваться в правовых и технических средствах защиты информации с учётом основных требований к проектированию программного обеспечения. Проявляет отличные умения владеть материалом.	Умеет ориентироваться в правовых и технических средствах защиты информации с учётом основных требований к проектированию программного обеспечения.. Присутствуют незначительные ошибки при выполнении заданий. Проявляет хорошие умения владеть материалом.	Умеет с существенными пробелами ориентироватьс я в правовых и технических средствах защиты информации с учётом основных требований к проектировани ю программного обеспечения. Задания выполнены, но не все и не вовремя. Проявляет слабые умения владеть материалом.	Не умеет ориентироваться в правовых и технических средствах защиты информации и вряд ли сможет проектировать программное обеспечение и разрабатывать требования к нему. Проявляет неудовлетворител ьные умения владения материалом.

	Владеет навыками применения всех методов защиты сообщений при использовании компьютерных и сетевых технологий. Продемонстрирован отличный уровень владения материалом.	Владеет навыками применения всех методов защиты сообщений при использовании компьютерных и сетевых технологий. Но неуверенно использует методы защиты канала от НСД. Проявлена хорошая теоретическая подготовка. Необходимые навыки в основном освоены.	Владеет немногими навыками применения методов защиты сообщений при использовании компьютерных и сетевых технологий. Но не может объяснить некоторые результаты. Проявлена удовлетворительная теоретическая подготовка.	Плохо владеет навыками применения методов защиты сообщений при использовании компьютерных технологий. Задания выполнены менее чем наполовину, или не к положенному сроку. Не может объяснить им же полученные результаты. Демонстрирует неудовлетворительный уровень владения материалом.
ПК-6	Знает все основные требования информационной безопасности, а также организационные средства защиты данных, чтобы соблюдать требования информационной безопасности;. Знает методы информационных технологий, поэтому правильно и в срок выполняет все задания. Демонстрирует отличный уровень знания материала.	Знает некоторые методы обеспечения информационной безопасности. Знает методы информационных технологий, поэтому правильно выполняет все задания, но защищает некоторые из них с опозданием. Демонстрирует хороший уровень знания материала.	Слабо знает методы обеспечения информационной безопасности и организационные средства защиты данных. Знает не все методы информационных технологий, поэтому выполняет не все задания и часто с нарушением срока их сдачи. Демонстрирует удовлетворительный уровень знания материала. .	Плохо знает методы информационных технологий и методы защиты данных даже симметричными ключами. Недостаточно самостоятельности в выполнении заданий по защите данных. Демонстрирует плохой уровень знания материала
	Умеет . ориентироваться в государственных	Умеет ориентироваться в правовых	Не умеет разбираться в правовых	Не умеет разбираться в правовых

	нормативных актах по защите информации, чтобы соблюдать основные требования информационной безопасности; Умеет применять различные методы информационных технологий, поэтому выполняет все задания правильно и в срок. Демонстрирует отличный уровень умения пользоваться известным материалом.	средствах защиты информации от несанкционированного доступа. Умеет использовать некоторые методы обеспечения информационной безопасность Умеет применять различные методы информационных технологий, поэтому выполняет все задания правильно, но не всегда к заданному сроку. Демонстрирует хороший уровень умения пользоваться известным материалом.	средствах защиты информации от несанкционированного доступа. Неумело пользуется методами защиты данных. Неуверенно применяет методы информационных технологи, поэтому выполняет лишь половину заданий правильно и всегда с опозданием. Демонстрирует удовлетворительный уровень умения пользоваться известным материалом.	средствах защиты информации от несанкционированного доступа. Плохо и неуверенно применяет методы информационных технологий, поэтому выполняет менее половины заданий правильно, часто не может пояснить полученный результат. Демонстрирует плохой уровень умения пользоваться известным материалом.
	Владеет навыками работы с компьютером и методами защиты конфиденциальных данных, обеспечивая их информационную безопасность. Владеет навыками применять различные методы информационных технологий, поэтому выполняет все задания правильно и в срок. Демонстрирует отличный уровень владения	Владеет навыками работы с компьютером и методами защиты информации. Неплохо освоены методы информационных технологий, предотвращающих утечку конфиденциальных данных. Но выполняет задания с ошибками, причём достаточно часто они выполняются с опозданием. Демонстрирует хороший уровень владения	Владеет навыками работы с компьютером. Однако не владеет приёмами криптографии, достаточными для соблюдения требований информационной безопасности Демонстрирует средний уровень владения материалом.	Владеет навыками работы с компьютером и некоторыми методами информационных технологий, но не владеет приёмами криптографии, достаточными для соблюдения требований информационной безопасности. Демонстрирует плохой уровень владения материалом.

	материалом.	материалом.		

3. Распределение оценок за формы текущего контроля и промежуточную аттестацию

Семестр 8

Текущий контроль:

Письменное домашнее задание (ПК-4) .... – 12 баллов

Письменная работа (ПК4) .. – 10 баллов

Отчёт по лабораторным работам (ПК-6) … – 28 баллов

Промежуточная аттестация - зачёт (ПК-4, ПК-6) --.50 баллов

Итого (12+10+28+50).....– 100 баллов

Зачёт проводится в письменной форме по билетам, составленным из списка с 30 вопросами.

В билете - 2 вопроса.

Максимальное количество баллов на 1 вопрос - 25

Максимальное количество баллов за ответы на билет - 50

Максимальное количество баллов на экзамене ..... -50

Учитывается полнота ответа, наличие примеров с объяснениями.

Общее количество баллов по дисциплине за текущий контроль и экзамен:

50+50=100 баллов.

Соответствие баллов и оценок:

56 и более - зачтено

55 баллов и менее - незачтено.

4. Оценочные средства, порядок их применения и критерии оценивания.

4.1. Оценочные средства текущего контроля

4.1.1. Письменное домашнее задание

4.1.1.1. Порядок проведения и процедура оценивания

Задание представляет собой перечень вопросов, на которые студент отвечает письменно. Ответы он находит в конспекте лекций, в рекомендованных литературных и /или интернет-источниках. Поощряется использование дополнительного материала, обоснование высказанного ответа и вообще — грамотное проявление творческого подхода.

Сама работа оформляется на персональном компьютере и должна быть напечатана на стандартном листе белой бумаги формата А4 на одной стороне (210х297 мм). Рекомендуемый шрифт -TimesNewRoman, межстрочный интервал полуторный, 14 кегль, в таблицах - 12, в подстрочных сносках - 10. Титульный лист заполняется по единому образцу. Надпись " Домашнее задание" печатается 18 шрифтом. Подчеркивание слов и выделение их курсивом не допускается.

Поля сверху, снизу по 20 мм, справа - 20 мм, слева - 30 мм, отступ первой строки абзаца - 1,25, выравнивание по ширине. Объём работы составляет 5-10 страниц, включая титульный лист, оглавление, введение, список использованных источников. Названия параграфов (подзаголовки) выделяются полужирным шрифтом и выравниваются по центру. В конце заголовка (подзаголовка) точка не ставится. Размер заголовка - 16 пт., подзаголовка - 14 пт.

Каждый параграф начинается с новой страницы. Расстояние между заголовком и подзаголовком, заголовком и последующим текстом, подзаголовком и предыдущим текстом отделяют двумя полуторными межстрочными интервалами (одной пустой строкой), а между подзаголовком и последующим текстом - одним полуторным междустрочным интервалом (как строки последующего текста). Страницы должны иметь сквозную нумерацию арабскими цифрами по всему тексту.

Номер страницы проставляют в центре нижнего поля страницы без точки в конце. Первой страницей письменной работы является титульный лист. Он не нумеруется. Размер шрифта, используемого для нумерации, должен быть меньше, чем у основного текста.

Обоснование того или иного положения возможно с помощью цитат из научной, справочной и иной литературы. Важно *понимать то, что цитируешь: за любое слово в вашей работе вы несёте ответственность.* Тупое копирование текста из источника не прибавляет вам знания, но умаляет уважение к вам. Необходимо указывать ссылку на источник цитаты, название которого находится в списке литературных и интернет-источников. Список этот помещается в самом конце изложения.

В случае применения дистанционных образовательных технологий работа представляется в платформе "Microsoft Teams".

4.1.1.2. Критерии оценивания

Всего 6 вопросов. Каждый подробный ответ с примерами на вопрос стоит 2 балла, максимальная оценка за всю работу - 12 баллов.

Учитываются: а) главное - *наличие примеров*. Ответ без поясняющих примеров (даже при цитировании источников) штрафуется удалением одного балла; б) полнота ответов с возможным привлечением дополнительных источников, в) наличие в тексте грамотно оформленных ссылок на бумажные и интернет-источники, использованные при написании работы.

4.1.1.3. Содержание оценочного средства

ВОПРОСЫ ДЛЯ ОСВЕЩЕНИЯ В ПИСЬМЕННОМ ДОМАШНЕМ ЗАДАНИИ:

Тема 1. *Информация как объект защиты*.

1. Как понятие «информация» определено в ФЗ «Об информации, информационных технологиях и о защите информации»? На кого оно ориентировано? Может ли в соответствием с этим определением обмениваться информацией, например, котёнок и клубок ниток, которым котёнок играет, или волк с овцой? Почему?
2. Какие элементы полезно имеют в виду при определении понятия «информация»? Поясните на примерах, обмениваются ли информацией животные, неживые объекты с неживыми объектами или с живыми, люди с животными и между собой? Если да, то в соответствии с каким определением?

Тема 2. *Правовые средства защиты информации от несанкционированного доступа*

3. На какую информацию не может быть ограничен доступ и какие способы несанкционированного доступа вам известны? Каким воздействиям может быть подвернута информация? Какие условия способствуют и приводят к неправомерному овладению конфиденциальной информацией?
4. Что составляет коммерческую тайну в соответствии с ФЗ «О коммерческой тайне» №98 от 2004 ? Какие требования информационной безопасности реализует персонал предприятия и, в частности, студент на производственной практике, чтобы не допустить утечки конфиденциальных данных?

Тема 3 *«Технические аспекты обеспечения защиты информации»* должна осветить следующий примерный перечень вопросов:

5. Какие средства инженерно-технической защиты информации вам известны и каким требованиям должны удовлетворять средства охраны помещений, предназначенных для работы с конфиденциальной информацией
6. Каким требованиям должны удовлетворять техническое оснащение рабочих мест и размещения технологического оборудования для предотвращения несанкционированного доступа к конфиденциальной информации?

4.1.2. Письменная работа

4.1.2.1. Порядок проведения и процедура оценивания

Работа выполняется письменно в аудитории и сдаётся преподавателю. Студенты

получают задание по освещению вопросов, указанных в разделе 4.1.2.3. Оцениваются знания по теме работы, аналитические способности, умения и навыки, необходимые для выполнения заданий. На ответы даётся 60 минут.

В случае применения дистанционных образовательных технологий работа представляется в платформе "Microsoft Teams".

4.1.2.2. Критерии оценивания

Предоставляются для обсуждения 10 вопросов.

Каждый подробный ответ на вопрос стоит 1 балл.

Максимальное количество баллов — 10.

Учитываются: а) самостоятельность в ответах на вопросы, б) наличие примеров с подробными объяснениями на основании приведённого определения понятия, в) способность защитить написанные ответы устно, без чтения написанного текста (невыполнение этого условия штрафуется удалением двух баллов).

Ответ без поясняющих соображений и примеров стоит 0 баллов.

4.1.2.3. Содержание оценочного средства

Тема 3 *«Угрозы информационной безопасности предприятия»* должна осветить следующий примерный перечень вопросов с использованием примеров:

1. Какие три группы угроз информации, их источники и следствия реализации можно отметить? Какие меры противодействия угрозам вам известны?
2. Что такое идентификация и аутентификация в социальной системе и какие три принципа аутентификации вам известны?

Тема 4 *«Административно-организационные средства защиты информации»* должна осветить следующий примерный перечень вопросов:

3. Что относится к коммерческой тайне?
4. Какими принципами следует руководствоваться администрации предприятия при организации защиты конфиденциальной информации?
5. Какие основные обязанности администрации и руководителей подразделений должны быть предусмотрены в Уставе предприятия для защиты конфиденциальной информации?
6. Какое отношение к защите информации имеют обеспечение дисциплины труда кадров, порядок подбора, приёма, подготовки и увольнения сотрудников, а также должностные инструкции сотрудников?
7. На какую информацию не может быть ограничен доступ и какие способы несанкционированного доступа вам известны?
8. Какие условия способствуют утечке информации и что приводит к неправомерному овладению конфиденциальной информацией?
9. Какое отношение к защите информации имеют обеспечение дисциплины труда кадров, порядок подбора, приёма, подготовки и увольнения сотрудников?
10. Как администрация применяет морально-этические нормы поведения для предотвращения утечки конфиденциальной информациеии?

4.1.3. Отчёт по лабораторным работам

4.1.3.1. Порядок проведения и процедура оценивания

Лабораторные занятия проводятся с использованием интерактивных методов: работа в парах при передаче ключей шифрования, обсуждение конкретного метода защиты сообщения. Важно грамотно подготовиться к работе, суметь организовать поиск, хранение, обработку и анализ информации из различных источников, т.е. прочитать записанную лекцию, обращая внимание на наиболее важные моменты, прочитать рекомендованный материал из учебно-методической литературы. Полезно также познакомиться с соответствующими статьями, содержащимися в Интернете. Выполненная на компьютере работа заканчивается оформлением письменного отчёта, который должен быть защищён к установленному сроку.

В случае применения дистанционных образовательных технологий работа представляется в платформе "Microsoft Teams".

4.1.3.2 Критерии оценивания

По темам 5 и 7 выполнятся лабораторные работы, в которых практически отрабатываются методы криптографического закрытия компьютерных сообщений.

Всего требуется выполнить 14 заданий, перечень которых приведён в следующем разделе под номерами 1 - 14.

Каждый подробный отчёт по заданию стоит 1 балл.

За сданный к заданному сроку отчёт (и ответы на вопросы) добавляется 1 балл.

Максимальная оценка за все сданные вовремя отчёты ..... .(2x14=) -- 28 баллов

За защиту работы после намеченного преподавателем срока и/или отсутствие правильных ответов на вопросы по заданию вычитается 1 балл за каждое задание.

4.1.3.3 Содержание оценочного средства

Ниже представлен перечень заданий, в каждом из которых (1) представляется информация в криптографически защищённом формате с использованием информационных, компьютерных и сетевых технологий и (2) применяются методы информационных технологий, предотвращающие утечку конфиденциальных данных приёмами криптографии, достаточными для соблюдения основных требований информационной безопасности.

Тема 5. *Криптографические симметричные методы защиты информации.*

Все задания предполагают выполнение следующих действий:

1) изучить краткие теоретические сведения,
2) разобрать предоставленные примеры шифрования и расшифрования,
3) составить в роли Отправителя (Алисы) сообщение, ключ шифрования и создать шифрограмму определённым методом,
4) переслать по сети криптограмму в адрес Получателя (Боба), сообщив ему метод закрытия сообщения и ключ,
5) получить от Боба его криптограмму и ключ,
6) расшифровать криптограмму Боба,
7) разработать программу шифрования и расшифрования,
8) оформить по известному шаблону отчёт, указав фамилию и имя Боба,
9) подготовиться к защите отчёта по имеющимся контрольным вопросам,
10) защитить отчёт к указанному сроку.

ПЕРЕЧЕНЬ ЗАДАНИЙ

1. Применить шифры атбаш, Цезаря и Гронсфельда.
2. Применить шифры Полибия и тюремный.
3. Применить шифры Тритемия и Абеля
4. Применить шиф Виженера.
5. Применить шифр одноразового блокнота.
6. Применить шифр гаммирования в русском алфавите.
7. Применить шифр гаммирования в двоичном и десятичном алфавите.
8. Применить шифры простой, вертикальной и двойной перестановки.
9. Применить шифрование с помощью алгебры матриц.

Тема 7. *Криптографические асимметричные методы защиты информации***.**

ПЕРЕЧЕНЬ ЗАДАНИЙ

10. Получить открытый и закрытый ключи, проверить протокол обмена сообщениями по сети при асимметричном шифровании (шок).
11. Создать защищённый канал связи использованием одноразового блокнота в качестве сеансового ключа.
12. Создать электронную цифровую подпись и выполнить аутентификацию сообщения с её помощью.
13. Создать дайджест и хеш-код сообщения для повышения скорости передачи сообщений.

14. Реализовать протокол обмена сообщениями с применением дайджеста.

4.2. Оценочные средства промежуточной аттестации - зачёт

4.2.1. Письменный ответ на вопросы билета

4.2.1.1. Порядок проведения и процедура оценивания

Бакалавр к этому времени уже знает, что зачёт - это заключительный этап работы в семестре по данной дисциплине. И понимает, что важнейшую роль для успешной его сдачи играют не только посещение занятий, но также и то, насколько внимателен и активен он был на лекциях, при выполнении и защите лабораторные работ, при самостоятельной работе над учебно-методической литературой и интернет-источниками. Но решающую роль на этом этапе играет тот факт, насколько успешно прошла защита самостоятельно выполненных лабораторных работ. Именно это проявляется при ответе на вопросы, предоставленные студенту для подготовки к зачёту.

Следует отметить, что неблагоприятное впечатление при ответе на билет вызывает чтение студентом написанного текста. Желателен свободный рассказ по существу с объяснением приготовленных примеров.

Зачёт проводится в письменной форме по билетам. В билете 2 вопроса.

Они включаются в билеты из списка в 30 вопросов, которые заранее известны студенту. Время, отводимое для подготовки к ответу, – 1 академический час.

В случае применения дистанционных образовательных технологий используется платформа «Microsoft Teams» Билеты по сказанному студентом номеру преподаватель показывает на экране монитора. После некоторой подготовки студент отвечает на вопросы билета как при обычном очном экзамене в аудитории. Могут быть заданы преподавателем уточняющие вопросы по данному билету или по некоторым темам дисциплины.

4.2.1.2. Критерии оценивания

Максимальное количество баллов на 1 вопрос …..... - 25

Максимальное количество баллов за ответы на билет - 50

Максимальное количество баллов на экзамене ..... - 50

Учитывается полнота ответа, наличие примеров, то есть владение материалом, его системное освоение, способность применять нужные знания, навыки и умения решать практические задания. Оценка снижается за неумение объяснить приведённый пример.

Баллы в интервале *86-100%* от максимальных ставятся, если студент:

– полностью ответил на все вопросы билета и дополнительные вопросы, при ответе использовал примеры практического применения рассматриваемого теоретического материала, ответ четкий и хорошо структурированный, освоен понятийный аппарат.

Баллы в интервале *71-85%* от максимальных ставятся, если студент:

– частично ответил на два вопроса, однако испытывал затруднение с приведением практических примеров применения рассматриваемого теоретического материала, ответил не на все дополнительные вопросы, ответ структурирован, освоен понятийный аппарат

Баллы в интервале *56-70%* от максимальных ставятся, если студент:

– раскрыл вопросы лишь частично, при ответе на билет читает написанный текст, не смог привести практические примеры применения рассматриваемого теоретического материала, частично ответил на некоторые из дополнительных вопросов, допускает несущественные ошибки при использовании понятийного аппарата.

Баллы в интервале *0-55%* от максимальных ставятся, если студент:

– не ответил на вопросы или же ответы не соответствовали заданным вопросам, не дал адекватного ответа на дополнительные вопросы, допускает грубые ошибки при использовании понятийного аппарата или не использует понятийный аппарат предметной области вовсе.

Баллы от 56 и выше — зачёт, ниже 56 — незачёт.

4.2.1.3. Оценочные средства.

ВОПРОСЫ К ЗАЧЁТУ:

1. Определение *информации*, данное в ФЗ «Об информации, информационных технологиях

и о защите информации». На какую информацию не может быть ограничен доступ?

2. Определение *информации*, по которому можно объяснить, обмениваются ли информацией животные, неживые объекты с неживыми объектами и т.п.
3. Сопоставление понятий: информация документированная, общедоступная, конфиденциальная. На какую информацию может быть ограничен доступ и в какой мере?
4. Условия, способствующие неправомерному овладению конфиденциальной информацией. Какие действия приводят к неправомерному овладению конфиденциальной информацией?
5. Воздействия, которым может быть подвернута информация. Приведите примеры таких воздействий. Три группы угроз информации, источники и следствия реализации этих угроз.
6. Меры противодействия угрозам информации. Охарактеризуйте их и приведите примеры.
7. Идентификация и аутентификация в социальной системе и в компьютерной сфере. Какие три принципа аутентификации вам известны.
8. Требования к инженерным и техническим средствам охраны помещений, предназначенных для работы с конфиденциальной информацией.
9. Требования к техническому оснащению рабочих мест и размещению технологического оборудования для предотвращения НСД к конфиденциальной информации.
10. Права на доступ к информации. Сопоставление понятий "информация документированная" и "общедоступная информация".
11. Характеристика групп угроз информации. Правовые и морально-этические меры защиты информации.
12. Несанкционированный доступ к информации. Условия, способствующие неправомерному овладению конфиденциальной информацией , и действия, приводящие к НСД
13. Источники и следствия реализации угроз информации. Воздействия, которым может быть подвернута информация..
14. Виды "тайн", защищаемые законами РФ. Три степени государственной тайны, установленные ФЗ "О государственной тайне". Сведения, относящиеся конфиденциальной/коммерческой информации.
15. Определение коммерческой тайны в ФЗ "О коммерческой тайне". Организационные меры, предпринимаемые работодателем для защиты конфиденциальной информации.
16. Определение понятий *шифр, ключ шифрования*. Протокол шифрования симметричным ключом.
17. Определение «моноалфавитной замены». Шифр Гронсфельда – модификация шифра Цезаря.
18. Шифр Тритемия - модификация шифра Полибия как пример моноалфавитной замены симметричного шифрования.
19. Шифр Виженера как пример многоалфавитной, или сложной замены.
20. Гаммирование конечной гаммой на основе русского алфавита. Преимущество метода гаммирования перед другими методами шифрования.
21. Гаммирование в двоичном алфавите как частный случай многоалфавитной замены.
22. Гаммирование десятичными числами для ручного шифрования/расшифрования.
23. Простая перестановка и её преимущество перед шифрами моноалфавитной замены.
24. Вертикальная перестановка. Преимущество шифров перестановки перед шифрами подстановки.
25. Аналитический метод шифрования и сравнение его с шифрами подстановки.
26. Недостатки симметричных методов шифрования и их устранение асимметричными методами. Протокол обмена сообщениями при асимметричном шифровании.
27. Сочетание метода гаммирования с асимметричным методом шифрования для защиты канала связи между корреспондентами.

28. Достоинства и недостатки ручной подписи. Назначение ЭЦП и сопоставление её с ручной подписью.
29. Назначение дайджеста (слепка, контрольной суммы) сообщения. Роль дайджеста в защите информации.
30. Назначение хеш-функции, реализующей дайджест сообщения. Алгоритм создания хеш-функции.

Приложение 2
к рабочей программе дисциплины (модуля)
Методы защиты информации

Перечень литературы, необходимой для освоения дисциплины (модуля)

Направление подготовки: 01.03.02 "Прикладная математика и информатика"
Профиль подготовки: отсутствует
Квалификация выпускника: бакалавр
Форма обучения: очная
Язык обучения: русский
Год начала обучения по образовательной программе: 2019

Основная литература:

1. Баранова Е. К. Основы информатики и защиты информации : учебное пособие / Е. К. Баранова. - Москва : ИЦ РИОР : НИЦ ИНФРА-М, 2018. - 183 с. - (Высшее образование. Бакалавриат). - ISBN 978-5-369-01169-0. - URL: https://znanium.com/catalog/product/959916 (дата обращения: 25.08.2020). - Текст : электронный.

2. Никифоров С. Н. Методы защиты информации. Шифрование данных : учебное пособие / С. Н. Никифоров. - 2-е изд., стер. - Санкт-Петербург : Лань, 2019. - 160 с. - ISBN 978-5-8114-4042-9. - URL: https://e.lanbook.com/book/114699 (дата обращения: 25.08.2020). - Текст : электронный.

3. Шаньгин В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В. Ф. Шаньгин. - Москва : ИД 'ФОРУМ' : ИНФРА-М, 2019. - 592 с. - (Высшее образование. Бакалавриат). - ISBN 978-5-8199-0730-6. - URL: https://znanium.com/catalog/product/996789 (дата обращения: 25.08.2020). - Текст : электронный.

Дополнительная литература:

1. Васильев В. И. Интеллектуальные системы защиты информации : учебное пособие/ В. И. Васильев. - 2-е изд., испр. и доп. - Москва : Машиностроение, 2013. - 172 с. - ISBN 978-5-94275-667-3. - URL : https://www.studentlibrary.ru/book/ISBN9785942756673.html (дата обращения: 25.08.2020). - Текст : электронный

2. Башлы П. Н. Информационная безопасность и защита информации : учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва : РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2. - URL: https://znanium.com/catalog/product/405000 (дата обращения: 25.08.2020). - Текст : электронный.

3. Никифоров С. Н. Методы защиты информации. Защищенные сети : учебное пособие / С. Н. Никифоров. - Санкт-Петербург : Лань, 2018. - 96 с. - ISBN 978-5-8114-3099-4. - URL: https://e.lanbook.com/book/110935 (дата обращения: 25.08.2020). - Текст : электронный.

Приложение 3
к рабочей программе дисциплины (модуля)
Методы защиты информации

Перечень информационных технологий, используемых для освоения дисциплины (модуля), включая перечень программного обеспечения и информационных справочных систем

Направление подготовки: 01.03.02 "Прикладная математика и информатика

Профиль подготовки: отсутствует

Квалификация выпускника: бакалавр

Форма обучения: очная

Язык обучения: русский

Год начала обучения по образовательной программе: 2019

Освоение дисциплины (модуля) предполагает использование следующего программного обеспечения и информационно-справочных систем:

Операционная система Microsoft Windows 7

Пакет офисного программного обеспечения Microsoft Office

Браузер Mozilla Firefox

Браузер Google Chrome

Adobe Acrobat Reader

Антивирус Касперского

Qt Creator

Mathworks Matlab R2014b

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен обучающимся. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, учебно-методические комплексы, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего образования (ФГОС ВО) нового поколения.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань" , доступ к которой предоставлен обучающимся. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям по максимальному количеству профильных направлений с соблюдением всех авторских и смежных прав.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "Консультант студента", доступ к которой предоставлен обучающимся. Многопрофильный образовательный ресурс "Консультант студента" является электронной библиотечной системой (ЭБС), предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Полностью соответствует требованиям федеральных

государственных образовательных стандартов высшего образования к комплектованию библиотек, в том числе электронных, в части формирования фондов основной и дополнительной литературы.