ЧАСТНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ДАГЕСТАНСКАЯ АКАДЕМИЯ ОБРАЗОВАНИЯ И КУЛЬТУРЫ»

УТВЕРЖДАЮ
Ректор ДАОК
Н. К. Мирзоева
«26» июня 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

Б.1.О.ДВ.03.02 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки: 38.03.02 - Менеджмент
Профиль: Менеджмент организации
Форма обучения: очная, очно-заочная, заочная

Дербент, 2023

При разработке рабочей программы учебной дисциплины использованы следующие нормативные правовые документы:

1. Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 38.03.02 Менеджмент (уровень бакалавриата), утвержденный приказом Министерства науки и высшего образования Российской Федерации № 970 от 12.08.2020 г. (зарегистрирован Минюстом Российской Федерации от 25.08.2020 № 59449);
2. Федеральный закон от 29 12. 2012г № 273-ФЗ «Об образовании в Российской Федерации».
3. Приказ Минобрнауки России от 06.04.2021 № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры».
4. Локальные и другие нормативные акты ДАОК.

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Целью изучения дисциплины «Основы информационной безопасности» является формирование у обучающихся способности осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач, осуществлять сбор, обработку и анализ данных, необходимых для решения поставленных управленческих задач, с использованием современного инструментария и интеллектуальных информационно-аналитических систем, понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

Цель изучения дисциплины «Основы информационной безопасности» достигается посредством решения в учебном процессе следующих **задач**:

- изучение основ риск-менеджмента в информационной безопасности;
- выявление угроз информации, исходящих от злоумышленников и вредоносных программ;
- использовать современный инструментарий и интеллектуальные информационно-аналитические системы защиты информации;
- изучение современных методов и средств защиты информации;
- умение собирать и анализировать информацию о источниках угроз, угрозах и уязвимостях информационных систем, с целью обеспечения их безопасности.

Воспитательной задачей является формирование российской гражданской идентичности, гражданской позиции активного и ответственного члена российского общества, осознающего свои конституционные права и обязанности, уважающего закон и правопорядок, обладающего чувством собственного достоинства, осознанно принимающего традиционные национальные и общечеловеческие гуманистические и демократические ценности.

МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Основы информационной безопасности» относится к дисциплинам по выбору обязательной части блока 1 «Дисциплины (модули)» основной профессиональной образовательной программы.

Дисциплина «Основы информационной безопасности» изучается в 4 семестре очной формы обучения, на 3 курсе заочной формы обучения, в 5 семестре очно-заочной формы обучения.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код и наименование компетенции	Наименование индикатора достижения компетенции	Планируемые результаты обучения, соотнесенные с индикаторами достижения компетенций
УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК 1.2. Применяет методы критического анализа и синтеза при работе с информацией, рассматривает и предлагает системные варианты для решения поставленных задач.	**Знать:** основные термины по проблематике информационной безопасности; **Уметь:** пользоваться нормативным и документами по защите информации; **Владеть:** навыками выявления и уничтожения компьютерных вирусов;

ОПК – 2. Способен осуществлять сбор, обработку и анализ данных, необходимых для решения поставленных управленческих задач, с использованием современного инструментария и интеллектуальных информационно-аналитических систем	ОПК 2.1. Определяет источники информации и осуществляет их поиск на основе поставленных целей для решения профессиональных задач.	**Знать**: значимость современного инструментария и интеллектуальных информационно-аналитических систем, применяемых в профессиональной деятельности; **Уметь:** анализировать и оценивать профессиональную информацию, обобщать, строить выводы, использовать данные поисковой системы при решении профессиональных задач и оформлении научных статей, отчетов, заключений; **Владеть:** методами формирования требований по защите информации;
ОПК-6. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.	ОПК 6.2. Осуществляет выбор общих или специализированных пакетов прикладных программ, используемых для выполнения конкретных профессиональных задач	**Знать:** современные инструментальные среды, программно-технические платформы и программные средства, в том числе отечественного производства, используемые для решения задач профессиональной деятельности, и принципы их работы; **Уметь:** создать информационную модель предметной области, учитывающую последовательность обработки данных и структуру взаимосвязи между ними; **Владеть:** навыками работы с программными комплексам и защиты информации;

В результате освоения дисциплины обучающийся должен:

знать:

- о моральном аспекте информационной безопасности;
- о социальной значимости своей будущей профессии;
- о значении информации в развитии современного общества;

уметь:

- осуществлять свою деятельность в различных сферах общественной жизни с уче-том принятых в обществе моральных норм;
- применять основные механизмы защиты информации на практике;
- применять достижения информационных технологий для защиты информации;

владеть:

- классификации информации;
- выделения объекта и предмета защиты в организации;
- основ построения модели нарушителя.

4. ОБЪЕМ ДИСЦИПЛИНЫ В ЗАЧЕТНЫХ ЕДИНИЦАХ С УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ, ВЫДЕЛЕННЫХ НА КОНТАКТНУЮ РАБОТУ ОБУЧАЮЩИХСЯ С ПРЕПОДАВАТЕЛЕМ (ПО ВИДАМ УЧЕБНЫХ ЗАНЯТИЙ) И НА САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ

Очная форма обучения

Вид учебной работы	Всего часов	4 семестр
1.Контактная работа обучающихся с преподавателем:	**40.2**	**40.2**
Аудиторные занятия всего, в том числе:	36	36
Лекции	18	18
Лабораторные	-	
Практические занятия	18	18
Контактные часы на аттестацию (зачет)	0,2	0.2
Консультация	2	2
Контроль самостоятельной работы	2	2
2. Самостоятельная работа	**67.8**	**67.8**
Контроль		
ИТОГО:	**108**	**108**
Общая трудоемкость	**3**	**3**

Очно-заочная форма обучения

Вид учебной работы	Всего часов	5 семестр
1.Контактная работа обучающихся с преподавателем:	**36.2**	**36.2**
Аудиторные занятия всего, в том числе:	32	32
Лекции	16	16
Лабораторные	-	
Практические занятия	16	16
Контактные часы на аттестацию (зачет)	0,2	0.2
Консультация	2	2
Контроль самостоятельной работы	2	2
2. Самостоятельная работа	**71.8**	**71.8**
Контроль		
ИТОГО:	**108**	**108**
Общая трудоемкость	**3**	**3**

Заочная форма обучения

Вид учебной работы	Всего часов	3 курс
1.Контактная работа обучающихся с преподавателем:	**12.2**	**12.2**
Аудиторные занятия всего, в том числе:	8	8
Лекции	4	4
Лабораторные	-	
Практические занятия	4	4
Контактные часы на аттестацию (зачет)	0,2	0.2

Консультация	2	2
Контроль самостоятельной работы	2	2
2. Самостоятельная работа	**91.8**	**91.8**
Контроль	4	4
ИТОГО:	**108**	**108**
Общая трудоемкость	**3**	**3**

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Наименование раздела (темы) дисциплины	Содержание раздела (темы разделов)	Индекс компетенции
Тема 1. Компьютерные преступления и их классификация.	Основные понятия и определения. Виды информации. Классификация компьютерных преступлений. Способы совершения компьютерных преступлений. Злоумышленники. Причины уязвимости сети Internet.	УК-1.2
Тема 2. Угрозы информации	Основные свойства информации. Угрозы информационной безопасности. Удаленные атаки на интрасети.	ОПК-2.1
Тема 3. Вредоносные программы и защита от них	Признаки заражения компьютера вредоносными программами. Источники вредоносных программ. Методы обнаружения вредоносных программ. Антивирусные программы.	ОПК-6.2
Тема 4. Методы и средства защиты компьютерной информации.	Классификация мер безопасности компьютерных систем. Организационные методы, программно-технические методы и средства информационной безопасности.	ОПК-2.1 ОПК-6.2

6. СТРУКТУРА ДИСЦИПЛИНЫ С УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

Очная форма обучения

Наименование раздела (темы) дисциплины	Виды учебной деятельности, включая самостоятельную работу (в часах)			
	Л	ЛР	ПЗ	СРС
Тема 1. Компьютерные преступления и их классификация.	4	-	4	17
Тема 2. Угрозы информации	4	-	4	17
Тема 3. Вредоносные программы и защита от них.	4	-	6	17
Тема 4. Методы и средства защиты компьютерной информации.	6	-	4	16.8
Итого (часов)	18		18	67.8
Форма контроля	зачет			

Очно-заочная форма обучения

Наименование раздела (темы) дисциплины	Виды учебной деятельности, включая самостоятельную работу (в часах)			
	Л	ЛР	ПЗ	СРС
Тема 1. Компьютерные преступления и их классификация.	4	-	4	18
Тема 2. Угрозы информации	4	-	4	18
Тема 3. Вредоносные программы и защита от них.	4	-	4	18
Тема 4. Методы и средства защиты компьютерной информации.	4	-	4	17.8
Итого (часов)	16		16	71.8
Форма контроля	зачет			

Заочная форма обучения

Наименование раздела (темы) дисциплины	Виды учебной деятельности, включая самостоятельную работу (в часах)			
	Л	ЛР	ПЗ	СРС
Тема 1. Компьютерные преступления и их классификация.	1	-	1	23
Тема 2. Угрозы информации	1	-	1	23
Тема 3. Вредоносные программы и защита от них.	1	-	1	23
Тема 4. Методы и средства защиты компьютерной информации.	1	-	1	22.8
Итого (часов)	4		4	91.8
Форма контроля	зачет			

7. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Самостоятельная работа обучающихся направлена на углубленное изучение разделов и тем рабочей программы и предполагает изучение литературных источников, выполнение домашних заданий и проведение исследований разного характера. Работа основывается на анализе литературных источников и материалов, публикуемых в интернете, а также реальных речевых и языковых фактов, личных наблюдений. Также самостоятельная работа включает подготовку и анализ материалов по темам пропущенных занятий.

Самостоятельная работа по дисциплине включает следующие виды деятельности:

- работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы;
- поиск (подбор) и обзор литературы, электронных источников информации по индивидуально заданной проблеме курса, написание доклада, исследовательской работы по заданной проблеме;
- выполнение задания по пропущенной или плохо усвоенной теме;
- самостоятельный поиск информации в Интернете и других источниках;
- выполнение домашней контрольной работы (решение заданий, выполнение упражнений);
- изучение материала, вынесенного на самостоятельную проработку (отдельные темы, параграфы);
- написание рефератов;
- подготовка к тестированию;
- подготовка к практическим занятиям;
- подготовка к зачету.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1 Основная литература:

1. Зенков, А. В. Основы информационной безопасности : учебное пособие / А. В. Зенков. — Москва, Вологда : Инфра-Инженерия, 2022. — 104 с. — ISBN 978-5-9729-0864-6. —Режим доступа: https://www.iprbookshop.ru/124242.html— IPR SMART, по паролю

2. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. —Режим доступа: https://www.iprbookshop.ru/97562.html— IPR SMART, по паролю

3. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере : учебное пособие / А. Е. Фаронов. — 3-е изд. — Москва, Саратов : Интернет-Университет

Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 154 c. — ISBN 978-5-4497-0338-5. —Режим доступа: https://www.iprbookshop.ru/89453.html — IPR SMART, по паролю

4. Гультяева, Т. А. Основы информационной безопасности : учебное пособие / Т. А. Гультяева. — Новосибирск : Новосибирский государственный технический университет, 2018. — 79 c. — ISBN 978-5-7782-3640-0. —Режим доступа: https://www.iprbookshop.ru/91640.html— IPR SMART, по паролю

5. Основы информационной безопасности : учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В. Ю. Рогозин, И. Б. Галушкин, В. К. Новиков, С. Б. Вепрев. — Москва : ЮНИТИ-ДАНА, 2017. — 287 c. — ISBN 978-5-238-02857-6. —Режим доступа: https://www.iprbookshop.ru/72444.html— IPR SMART, по паролю

8.2.Дополнительная литература:

1. Нестеров С.А., Основы информационной безопасности : учебное пособие / Нестеров С.А.. — Санкт-Петербург : Санкт-Петербургский политехнический университет Петра Великого, 2014. — 322 c. — ISBN 978-5-7422-4331-1. —Режим доступа: https://www.iprbookshop.ru/43960.html— IPR SMART, по паролю

2. Добровольский, В. С. Управление интеллектуальной безопасностью: организационные и правовые основы информационной безопасности : учебное пособие / В. С. Добровольский. — Москва : Издательский Дом МИСиС, 2014. — 224 c. — ISBN 978-5-87623-789-7. —Режим доступа: для https://www.iprbookshop.ru/97872.html— IPR SMART, по паролю

3. Кожуханов, Н. М. Правовые основы информационной безопасности : учебное пособие / Н. М. Кожуханов, Е. С. Недосекова. — Москва : Российская таможенная академия, 2013. — 88 c. — ISBN 978-5-9590-0725-6. —Режим доступа: https://www.iprbookshop.ru/69749.html — IPR SMART, по паролю

4. Сычев, Ю. Н. Основы информационной безопасности : учебно-методический комплекс / Ю. Н. Сычев. — Москва : Евразийский открытый институт, 2012. — 342 c. — ISBN 978-5-374-00602-5. —Режим доступа: https://www.iprbookshop.ru/14642.html— IPR SMART, по паролю

5. Сычев, Ю. Н. Основы информационной безопасности : учебное пособие / Ю. Н. Сычев. — Москва : Евразийский открытый институт, 2010. — 328 c. — ISBN 978-5-374-00381-9. —Режим доступа: для https://www.iprbookshop.ru/10746.html— IPR SMART, по паролю

6. Голиков, А. М. Основы информационной безопасности : учебное пособие / А. М. Голиков. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2007. — 288 c. — ISBN 978-5-868889-467-1. —Режим доступа: https://www.iprbookshop.ru/13957.html — IPR SMART, по паролю

8.3.Лицензионное программное обеспечение

Microsoft Desctop School Windows//Sa Pack MVL (windows 10, windows 7) № 5 от 31 января 2019 г;

Microsoft Desktop School Office All languages/SA Pack (Microsoft Office 2010, Microsoft Office 2007) № 5 от 31 января 2019 г.;

Конвертация PDF в WORD https://www.ilovepdf.com/ru/pdf_to_word

Сжатие, оптимизация и изменение размера изображений http://www.imageoptimizer.net/Pages/Home.aspx

Скачивание видео с YouTube https://ru.savefrom.net/

Googletаблицы https://www.google.ru/intl/ru/sheets/about/

Яндекс Диск https://disk.yandex.ru/
GoogleChrome https://www.google.com/intl/ru_ru/chrome/
Яндекс Браузер https://browser.yandex

8.4.Современные профессиональные базы данных и информационные справочные системы

1. Государственная публичная научно-техническая библиотека России. – http://www.gpntb.ru/
2. Единая коллекция цифровых образовательных ресурсов. – http://window.edu.ru/
3. Электронно-библиотечная система «IPR SMART». – https://www.iprbookshop.ru/
4. Электронно-библиотечная система издательства «Лань». – https://e.lanbook.com/
5. Электронно-библиотечная система (ЭБС) «Юрайт». – https://urait.ru/
6. Федеральный центр информационно-образовательных ресурсов. – http://fcior.edu.ru/
7. http://www.gks.ru - Росстат – федеральная служба государственной статистики
8. http://www.iep.ru/ru/publikatcii/categories.html Федеральный образовательный портал. Экономика. Социология. Менеджмент
9. https://www.nalog.ru/rn39/program/- База программных средств налогового учета
10. https://rosmintrud.ru/opendata - База открытых данных Минтруда России
11. www.economy.gov.ru - Базы данных Министерства экономического развития и торговли России
12. http://www.fedsfm.ru/opendata - База открытых данных Росфинмониторинга
13. https://www.polpred.com - Электронная база данных "Polpred.com Обзор СМИ"

Информационные справочные системы:

1. Справочно-правовая система «Консультант Плюс» - Режим доступа: http://www.consultant.ru;
2. Информационно-правовой сервер «Гарант» http://www.garant.ru/

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Кабинет информатики и информационно-коммуникационных технологий №203 (1 корпус, 2 этаж)	Доска передвижная 21 компьютеров intel (r) cpu Принтер laser jet, локальная сеть, выход в Интернет 30 посадочных мест.
Помещение для самостоятельной работы обучающихся (ауд.7)	16 компьютеров intel (r) cpu Принтер laser jet, локальная сеть, выход в Интернет доступ к электронной информационно-образовательной среде 36 посадочных мест.
Помещение для хранения и профилактического обслуживания учебного оборудования (ауд.8)	Стеллажи, инвентарь, учебное оборудование

10.ОСОБЕННОСТИ ВЫПОЛНЕНИЯ ЗАДАНИЙ ОБУЧАЮЩИМИСЯ-ИНВАЛИДАМИ И ЛИЦАМИ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ (ПРИ НАЛИЧИИ)

Особые условия обучения и направления работы с инвалидами и лицами с ограниченными возможностями здоровья (далее обучающихся с ограниченными возможностями здоровья) определены на основании:

– Закона РФ от 29.12.2012г. № 273-ФЗ «Об образовании в Российской Федерации»;

– Закона РФ от 24.11.1995г. № 181-ФЗ «О социальной защите инвалидов в Российской Федерации»;

– Приказа Минобрнауки России от 06.04.2021 № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»;

– методических рекомендаций по организации образовательного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащенности образовательного процесса (утв. Минобрнауки России 08.04.2014 № АК-44/05вн).

Под специальными условиями для получения образования обучающихся с ограниченными возможностями здоровья понимаются условия обучения, воспитания и развития таких обучающихся, включающие в себя использование адаптированных образовательных программ и методов обучения и воспитания, специальных учебников, учебных пособий и дидактических материалов, специальных технических средств обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, проведение групповых и индивидуальных коррекционных занятий, обеспечение доступа в здания вуза и другие условия, без которых невозможно или затруднено освоение образовательных программ обучающимися с ограниченными возможностями здоровья.

В целях доступности изучения дисциплины инвалидами и обучающимися с ограниченными возможностями здоровья организацией обеспечивается:

1. Для инвалидов и лиц с ограниченными возможностями здоровья по зрению:

– наличие альтернативной версии официального сайта организации в сети «Интернет» для слабовидящих:

– размещение в доступных для обучающихся, являющихся слепыми или слабовидящими, местах и в адаптированной форме (с учетом их особых потребностей) справочной информации (информация должна быть выполнена крупным рельефно-контрастным шрифтом (на белом или желтом фоне) и продублирована шрифтом Брайля);

– присутствие ассистента. оказывающего обучающемуся необходимую помощь:

– обеспечение выпуска альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы);

– обеспечение доступа обучающегося, являющегося слепым и использующего собаку-поводыря. к зданию организации;

2. Для инвалидов и лиц с ограниченными возможностями здоровья по слуху:

– дублирование звуковой справочной информации визуальной (установка мониторов с возможностью трансляции субтитров (мониторы, их размеры и количество необходимо определять с учетом размеров помещения);

– обеспечение надлежащими звуковыми средствами воспроизведения информации:

3.Для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата. Материально- технические условия обеспечивают возможность беспрепятственного доступа обучающихся в помещения организации, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов, локальное понижение стоек-барьеров: наличие специальных кресел и других приспособлений).

Обучение лиц организовано как инклюзивно, так и в отдельных группах.

11.ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

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

Этапы формирования компетенций в процессе освоения ОПОП прямо связаны с местом дисциплин в образовательной программе. Каждый этап формирования компетенции характеризуется определенными знаниями, умениями и навыками и (или) опытом профессиональной деятельности, которые оцениваются в процессе текущего контроля успеваемости, промежуточной аттестации по дисциплине (практике) и в процессе государственной итоговой аттестации.

Оценочные материалы включают в себя контрольные задания и (или) вопросы, которые могут быть предложены обучающемуся в рамках текущего контроля успеваемости и промежуточной аттестации по дисциплине. Указанные планируемые задания и (или) вопросы позволяют оценить достижение обучающимися планируемых результатов обучения по дисциплине, установленных в соответствующей рабочей программе дисциплины, а также сформированность компетенций, установленных в соответствующей общей характеристике основной профессиональной образовательной программы.

На этапе текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине показателями оценивания уровня сформированности компетенций являются результаты устных и письменных опросов, написания рефератов, практических заданий, решения тестовых заданий.

Итоговая оценка сформированности компетенций определяется в период государственной итоговой аттестации.

Описание показателей и критериев оценивания компетенций

Показатели оценивания	Критерии оценивания компетенций	Шкала оценивания
Понимание смысла компетенции	Имеет базовые общие знания в рамках диапазона выделенных задач	Минимальный уровень
	Понимает факты, принципы, процессы, общие понятия в пределах области исследования. В большинстве случаев способен выявить достоверные источники информации, обработать, анализировать информацию.	Базовый уровень
	Имеет фактические и теоретические знания в пределах области исследования с пониманием границ применимости	Высокий уровень

Освоение компетенции в рамках изучения дисциплины	Наличие основных умений, требуемых для выполнения простых задач. Способен применять только типичные, наиболее часто встречающиеся приемы по конкретной сформулированной (выделенной) задаче	Минимальный уровень
	Имеет диапазон практических умений, требуемых для решения определенных проблем в области исследования. В большинстве случаев способен выявить достоверные источники информации, обработать, анализировать информацию.	Базовый уровень
	Имеет широкий диапазон практических умений, требуемых для развития творческих решений, абстрагирования проблем. Способен выявлять проблемы и умеет находить способы решения, применяя современные методы и технологии.	Высокий уровень
Способность применять на практике знания, полученные в ходе изучения дисциплины	Способен работать при прямом наблюдении. Способен применять теоретические знания к решению конкретных задач.	Минимальный уровень
	Может взять на себя ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем. Затрудняется в решении сложных, неординарных проблем, не выделяет типичных ошибок и возможных сложностей при решении той или иной проблемы	Базовый уровень
	Способен контролировать работу, проводить оценку, совершенствовать действия работы. Умеет выбрать эффективный прием решения задач по возникающим проблемам.	Высокий уровень

1.2 Оценочные материалы для проведения текущего контроля

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач (контролируемый индикатор достижения УК 1.2. Применяет методы критического анализа и синтеза при работе с информацией, рассматривает и предлагает системные варианты для решения поставленных задач.);

ОПК – 2. Способен осуществлять сбор, обработку и анализ данных, необходимых для решения поставленных управленческих задач, с использованием современного инструментария и интеллектуальных информационно-аналитических систем (контролируемый индикатор достижения ОПК 2.1. Определяет источники информации и осуществляет их поиск на основе поставленных целей для решения профессиональных задач).

ОПК-6. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности (контролируемый индикатор достижения ОПК 6.2. Осуществляет выбор общих или специализированных пакетов прикладных программ, используемых для выполнения конкретных профессиональных задач).

Типовые задания, для оценки сформированности знаний

Результаты обучения
Знает инструментарий поиска критического анализа и синтеза информации, применяя системный

Результаты обучения
подход для решения поставленных задач; Знает значимость современного инструментария и интеллектуальных информационно-аналитических систем, применяемых в профессиональной деятельности; Знает современные инструментальные среды, программно-технические платформы и программные средства, в том числе отечественного производства, используемые для решения задач профессиональной деятельности, и принципы их работы;

Вопросы для устного опроса на практических занятиях

Тема 1. Компьютерные преступления и их классификация.

- Организация безопасного удаленного доступа к ЛВС предприятия.
- Построение защищенной виртуальной сети на базе специализированного программного обеспечения на предприятии.
- Автоматизация учета конфиденциальных документов на предприятии.
- Организация процессов мониторинга конфиденциального документооборота на предприятии.
- Автоматизация процесса проверок наличия конфиденциальных документов на предприятии.

Тема 2. Угрозы информации.

- Разработка комплексной системы защиты информации (КСЗИ) предприятия.
- Организация системы планирования и контроля функционирования КСЗИ на
- предприятии.
- Разработка основных направлений совершенствования КСЗИ предприятия.
- Организация подсистемы, обеспечивающей управление КСЗИ в условиях чрезвычайной ситуации на предприятии.
- Разработка методологии проектирования КСЗИ.
- Разработка моделей процессов защиты информации при проектировании КСЗИ

Тема 3. Вредоносные программы и защита от них.

- Разработка проекта программно-аппаратной защиты информации предприятия.
- Разработка методов расчета экономической эффективности программно-аппаратной защиты информации предприятия.
- Криптографические средства защиты информации на основе дискретных носителей.
- Разработка игровой (дискретной) модели программно-аппаратной защиты информации предприятия.
- Разработка изолированной программно-аппаратной среды в Windows, Linux и т.д.
- Обоснование и разработка требований и процедур по защите информации ограниченного доступа на предприятии.
- Анализ нормативно-правовой базы по защите информации в сети Интернет. Разработка требований по организационной защите конфиденциальной информации, передаваемой и получаемой по сети Интернет.

Тема 4 Методы и средства защиты компьютерной информации.

- Укажите основные отличия между современными и классическими блочными шифрами.
- Перечислите режимы работы ГОСТ 28147-89. Для чего служит каждый из данных режимов?
- Сравните DES и ГОСТ 28147-89.
- Сравните AES и ГОСТ 28147-89.
- Перечислите основные свойства хеш-функций.
- Чем хеширование отличается от выработки контрольных сумм?
- Чем хеширование отличается от выработки имитовставки?
- Укажите два подхода к построению функций хеширования

Критерии и шкала оценивания устного опроса

Оценка за ответ	Критерии
Отлично	выставляется обучающемуся, если: - теоретическое содержание курса освоено полностью, без пробелов; - исчерпывающее, последовательно, четко и логически излагает теоретический материал; - свободно справляется с решение задач, - использует в ответе дополнительный материал; - все задания, предусмотренные учебной программой выполнены; - анализирует полученные результаты; - проявляет самостоятельность при трактовке и обосновании выводов
Хорошо	выставляется обучающемуся, если: - теоретическое содержание курса освоено полностью; - необходимые практические компетенции в основном сформированы; - все предусмотренные программой обучения практические задания выполнены, но в них имеются ошибки и неточности; - при ответе на поставленный вопросы обучающийся не отвечает аргументировано и полно. - знает твердо лекционный материал, грамотно и по существу отвечает на основные понятия.
Удовлетворительно	выставляет обучающемуся, если: - теоретическое содержание курса освоено частично, но проблемы не носят существенного характера; - большинство предусмотренных учебной программой заданий выполнено, но допускаются не точности в определении формулировки; - наблюдается нарушение логической последовательности.
Неудовлетворительно	выставляет обучающемуся, если: - не знает значительной части программного материала; - допускает существенные ошибки; - так же не сформированы практические компетенции; - отказ от ответа или отсутствие ответа.

Тематика рефератов

1. Виды угроз безопасности информации.
2. Основные параметры системы защиты информации.
3. Распространение сигналов в технических каналах утечки информации.
4. Физические процессы подавления опасных сигналов.
5. Физические основы побочных электромагнитных излучений и наводок.
6. Защита информации в компьютерных системах от утечки по каналам ПЭМИН.
7. Основы защиты информации от фотографической и оптико-электронной разведок.
8. Основы защиты информации от радиотехнической разведки.
9. Процессы подавления опасных сигналов.
10. Основные определения и классификация радиоэлектронных помех.
11. Методы и средства инженерной защиты и технической охраны объектов.
12. Классификация и характеристика охранных, пожарно-охранных и пожарных извещателей.
13. Технические средства несанкционированного доступа к информации.
14. Направления обеспечения безопасности.

15. Аттестация объектов, лицензирование деятельности по защите информации и сертификации ее средств.

16. Особенности инструментального контроля эффективности инженерно-технической

защиты информации.

17. Классификация средств вычислительной техники по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

18. Технические средства для тестирования и контроля систем обеспечения безопасности информации.

19. Принципы моделирования объектов защиты.

20. Стандартизация систем защиты информации.

Критерии оценивания выполнения реферата

Оценка	Критерии
Отлично	полностью раскрыта тема реферата; указаны точные названия и определения; правильно сформулированы понятия и категории; проанализированы и сделаны собственные выводы по выбранной теме; использовалась дополнительная литература и иные материалы и др.;
Хорошо	недостаточно полное, раскрытие темы; несущественные ошибки в определении понятий и категорий и т. п., кардинально не меняющих суть изложения; использование устаревшей литературы и других источников;
Удовлетворительно	реферат отражает общее направление изложения лекционного материала и материала современных учебников; наличие достаточного количества несущественных или одной-двух существенных ошибок в определении понятий и категорий и т. п.; использование устаревшей литературы и других источников; неспособность осветить проблематику дисциплины и др.;
Неудовлетворительно	тема реферата не раскрыта; большое количество существенных ошибок; отсутствие умений и навыков, обозначенных выше в качестве критериев выставления положительных оценок и др.

Тестовые задания

Тест № 1

1. Информация – это……

a. реквизит электронного документа, полученного в результате криптографического преобразования

b. данные, требующие защиты

c. сведения, независимо от формы их представления

2. Общедоступная информация – это …..

a. информация, доступ к которой не ограничен

b. информация, которая принадлежит общественной организации

c. информация, предназначенная для передачи по линиям связи, доступ к которой осуществляется с использованием средств вычислительной техники

3. Целостность информации – это …

a. документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации

b. состояние информации, характеризуемое способностью технических средств и информационных технологий обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия

c. устойчивость информации к несанкционированному или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации

4. Персональные данные – это…

a. любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)

b. любая информация, которая хранится на персональном компьютере

c. любые сведения

5. Несанкционированный доступ к информации- это …

a. передача персональных данных на территорию иностранного государства органу власти иностранного государства

b. доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами

c. действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных

6. ФЗ №149 "Об информации, информационных технологиях и о защите информации" регулирует отношения:

a. связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами

b. связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам

c. возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации; применении информационных технологий; обеспечении защиты информации.

7. Про какой руководящий документ идет речь:

«Настоящий руководящий документ устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в автоматизированных системах различных классов»

a. РД «Защита от несанкционированного доступа к информации. Термины и определения»

b. РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»

c. РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»

8. Согласно РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» устанавливается девять классов защищенности АС от НСД к информации. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. Какие АС в себя включает первая группа?

a. в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности

b. многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности

c. многопользовательские АС , в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС

9. Расшифруйте аббревиатуру «РД ФСТЭК»

_____

10. Область применения «ГОСТ Р ИСО/МЭК 15408-1-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»:

a. настоящий стандарт устанавливает основные понятия и принципы оценки безопасности ИТ, а также определяет общую модель оценки, которой посвящены различные части стандарта, предназначенного в целом для использования в качестве основы при оценке характеристик безопасности продуктов ИТ

b. настоящий стандарт устанавливает основные термины с соответствующими определениями, применяемые при проведении работ по стандартизации в области защиты информации

c. настоящий стандарт распространяется на испытания программных средств и их компонентов, цели которых - обнаружить в этих программных средствах и устранить из них компьютерные вирусы силами специальных предприятий (подразделений), и устанавливает общие требования к организации и проведению таких испытаний

Тест №2

1. Государственная тайна- это…

a. защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации

b. сведения о сферах деятельности государственных органов, доступ к которым ограничивается служебной необходимостью и разглашение или утрата которых может нанести ущерб государственным органам

c. режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду

2. Какие степени секретности бывают?

a. Важные, очень секретные, секретные

b. Особой важности, совершенно секретные, секретные

c. Совершенно важные, особо секретные, секретные

3. В соответствии со степенями секретности сведений, составляющих государственную тайну, устанавливаются три формы допуска первая, вторая, третья. Первая форма допуска:

a. для граждан, допускаемых к сведениям секретно

b. для граждан, допускаемых к сведениям совершенно секретно

c. для граждан, допускаемых к сведениям особой важности

4. Могут ли работать граждане, имеющие вторую форму допуска со сведениями «секретно»?_____

5. Перечислите не менее четырех органов безопасности РФ

1.

2.

3.

4.

6. Что означает допуск к сведениям составляющим государствую тайну?

a. процедура оформления права граждан на доступ к сведениям, составляющим

государственную тайну, а предприятий, учреждений и организаций - на проведение работ с использованием таких сведений

b. санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну

c. совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их осителей,

а также мероприятий, проводимых в этих целях

7. Укажите верную последовательность действий при оформлении допуска к государственной тайне

a. Отправка всех подготовленных документов и письменного обоснования о допуске в орган безопасности

b. Разработка номенклатуры должностей в режимно -секретном подразделении

c. Подготовка личных документов гражданина, на которого оформляется допуск

d. Знакомство гражданина с нормативной базой в области ГТ

8. Где проставляется отметка о допуске к ГТ

a. В анкете

b. В карточке

c. Нигде, в устной форме извещается гражданин

9. Какие документы необходимо подготовить гражданину, желающему получить допуск к ГТ

a. Документ удостоверяющий личность, медицинскую справку об отсутствии противопоказаний для работы.

b. Документ удостоверяющий личность, медицинскую справку об отсутствии противопоказаний для работы, все документы указанные в анкете, анкету

c. Документ удостоверяющий личность, медицинскую справку об отсутствии противопоказаний для работы, все документы указанные в анкете

10. Государственная тайна- это…

a. защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации

b. сведения о сферах деятельности государственных органов, доступ к которым ограничивается служебной необходимостью и разглашение или утрата которых может нанести ущерб государственным органам

c. режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду

Критерии оценивания образовательных достижений для тестовых заданий

Оценка	Коэффициент К (%)	Критерии оценки
Отлично	Свыше 80% правильных ответов	глубокое познание в освоенном материале
Хорошо	Свыше 70% правильных ответов	материал освоен полностью, без существенных ошибок
Удовлетворительно	Свыше 50% правильных ответов	материал освоен не полностью, имеются значительные пробелы в знаниях
Неудовлетворительно	Менее 50% правильных ответов	материал не освоен, знания обучающегося ниже базового

		уровня

11.3. Оценочные материалы для проведения промежуточной аттестации

Типовые задания, направленные на формирование профессиональных умений.

Результаты обучения
Умеет осуществлять поиск необходимой для решения поставленной задачи информации, критически оценивая надежность различных источников информации;
Умеет применить на практике аналитический инструментарий для постановки и решения управленческих задач с применением информационно-аналитических систем технологий;
Умеет создать информационную модель предметной области, учитывающую последовательность обработки данных и структуру взаимосвязи между ними;

Типовые задания для подготовки к зачету

1. Дать определение информационной безопасности.
2. Какие виды компьютерных преступлений существуют?
3. Какие виды злоумышленников существуют?
4. В чем отличие злоумышленника от нарушителя?
5. Что входить в программно-аппаратные меры по защите информации?
6. Как на территории РФ законодательно регулируются вопросы по защите информации?
7. Цель защиты информации?
8. Что включает в себя экономическая безопасность компании?
9. Что такое кадровая безопасность?
10. Что входить в организационные меры по защите информации?
11. Методология построения и оценки СЗИ.
12. Дайте определение угрозы, актива, атаки, уязвимости. Обоснуйте их взаимосвязь.
13. Основные этапы атаки.
14. Определение нарушителя безопасности информации.
15. Инсайдер, работающий в интересах лица, находящегося вне информационной системы к какому типу нарушителей, относится?
16. Как описывается угроза безопасности информации в информационной системе?
17. Что содержит модель нарушителя безопасности информации?
18. Перечислите синонимы уязвимости, встречающиеся в нормативно-технических документах.
19. Назовите причины появления уязвимостей.
20. Какие существуют уровни (степени) опасности уязвимости?
21. Перечислить известные виды вредоносного программного обеспечения, дать краткое описание.
22. Описать способы заражения компьютера компьютерными вирусами?
23. Что такое программные и аппаратные закладки?
24. Классификация компьютерных вредоносных программ.
25. Методы обнаружения известных и неизвестных вирусов.
26. Профилактика заражению компьютеров вирусами.
27. Что такое сетевой червь, способы заражения и методы распространения?
28. Что такое программная уязвимость? Кем и как они могут быть использованы?
29. Как устроены и работают антивирусные программы? Какие существуют современные методы выявления вредоносных программ?
30. Что такое троянская программа, в чем отличие от программ шпионов?
31. Инженерно-техническое обеспечение компьютерной безопасности.

32. Что такое резервное копирование информации? Где и как применяется?
33. Организационное обеспечение компьютерной безопасности.
34. Политики компьютерной безопасности, инструкции, структуры политик.
35. Методы обеспечения безопасности операционных систем.
36. Безопасное использование и защита электронной почты.
37. Что такое межсетевой экран, принципы обеспечения безопасности с помощью МЭ?
38. Криптографические методы защиты компьютерной информации, плюсы и минусы.
39. Защиты информации в сети Интернет.
40. Что такое активный аудит информационной безопасности? Как, где и кем применяется?

Типовые практические задания, направленные на формирование профессиональных навыков, владений

Результаты обучения
Владеет навыками находить рациональные идеи для решения поставленных задач в сфере стратегического планирования;
Владеет аналитическим инструментарием для постановки и решения типовых задач управления с применением информационных технологий;
Владеет навыками применения современных информационно-коммуникационных и интеллектуальных технологий, инструментальных сред, программно-технических платформ и программных средств, в том числе отечественного производства, для решения задач профессиональной деятельности;

Типовые практические задания для подготовки к зачету

Задание 1.

Используя основные положения части 4, главы 70 Гражданского кодекса РФ, решить ситуационную задачу. Гражданин Смирнов А.В. создал инструментальное программное средство для работы с трехмерной компьютерной графикой под названием «Albert 3D» и зарегистрировал на него свои права. 15.09.2019 этот гражданин заключил договор с компанией «MosTechnology» и передал свои имущественные права на распространение своего программного продукта сроком на один год. После заключения договора компания «MosTechnology» распространила версию программы «Albert 3D» с предварительной модификацией данного программного продукта без ведома автора

Вопрос: Имеет ли место в данной ситуации нарушение авторского права гражданина Смирнова? Ответ: согласно статьи №….

Задание 2.

Используя статьи УК РФ, ответьте на вопросы после ознакомления с ситуацией. Ситуация: А.Н. Иванов, сотрудник одного из филиалов ИТ-банка, внедрил в компьютерную банковскую систему вирус, уничтожающий исполняемые файлы (расширение .exe). В результате внедрения этого вируса было уничтожено 40 % банковских программных приложений, что принесло банку материальный ущерб в размере 780000 рублей.

Вопросы: – Какая статья УК РФ была нарушена? – Что послужило предметом преступления? – Какие неправомерные информационные действия были совершены А.Н. Ивановым?

Задание 3.

Вы – начальник отдела по вопросам информационной безопасности в некоторой некрупной организации (20-30 человек). Вам необходимо разработать требования к хранению, использованию и утилизации информации для вашей организации.

Цель: обеспечение информационной безопасности при хранении, обработке, передаче и уничтожении информации.

Задание 4.

Проработайте требования для специалистов по подбору кадров вашей организации с целью внесения пунктов об информационной безопасности в трудовой договор новых сотрудников.

Цель: уведомление новых сотрудников о строгом выполнении требований по обеспечению информационной безопасности и ответственности за их нарушение.

Критерии оценивания практических заданий

	Критерии оценивания
Решения практического задания	«5» (отлично) – выставляется за полное, безошибочное выполнение задания
	«4» (хорошо) –в целом задание выполнено, имеются отдельные неточности или недостаточно полные ответы, не содержащие ошибок.
	«3» (удовлетворительно) – допущены отдельные ошибки при выполнении задания.
	«2» (неудовлетворительно) – отсутствуют ответы на большинство вопросов задачи, задание не выполнено или выполнено не верно.

Критерии и шкала оценивания ответов на зачете

Шкала оценивания	Показатели
Зачтено	Достаточный объем знаний в рамках изучения дисциплины В ответе используется научная терминология. Стилистическое и логическое изложение ответа на вопрос правильное Умеет делать выводы без существенных ошибок Владеет инструментарием изучаемой дисциплины, умеет его использовать в решении стандартных (типовых) задач. Ориентируется в основных теориях, концепциях и направлениях по изучаемой дисциплине. Активен на практических (лабораторных) занятиях, допустимый уровень культуры исполнения заданий.
Не зачтено	Не достаточно полный объем знаний в рамках изучения дисциплины В ответе не используется научная терминология. Изложение ответа на вопрос с существенными стилистическими и логическими ошибками. Не умеет делать выводы по результатам изучения дисциплины Слабое владение инструментарием изучаемой дисциплины, не компетентность в решении стандартных (типовых) задач. Не умеет ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине. Пассивность на практических (лабораторных) занятиях, низкий уровень культуры исполнения заданий. Не сформированы компетенции, умения и навыки. Отказ от ответа или отсутствие ответа.

ЛИСТ ДОПОЛНЕНИЙ И ИЗМЕНЕНИЙ
рабочей программы дисциплины

Рабочая программа дисциплины рассмотрена на заседании кафедры (протокол от___________ №___) и одобрена на заседании Ученого совета (протокол от ____________ №____) для исполнения в 20__-20__ учебном году
Внесены дополнения (изменения): ____
____
____
____
Заведующий кафедрой

____
(подпись, инициалы и фамилия)

Рабочая программа дисциплины рассмотрена на заседании кафедры (протокол от___________ №___) и одобрена на заседании Ученого совета (протокол от ____________ №____) для исполнения в 20__-20__ учебном году
Внесены дополнения (изменения): ____
____
____
____
Заведующий кафедрой

____
(подпись, инициалы и фамилия)

Рабочая программа дисциплины рассмотрена на заседании кафедры (протокол от___________ №___) и одобрена на заседании Ученого совета (протокол от ____________ №____) для исполнения в 20__-20__ учебном году
Внесены дополнения (изменения): ____
____
____
____
Заведующий кафедрой

____
(подпись, инициалы и фамилия)

Рабочая программа дисциплины рассмотрена на заседании кафедры (протокол от___________ №___) и одобрена на заседании Ученого совета (протокол от ____________ №____) для исполнения в 20__-20__ учебном году
Внесены дополнения (изменения): ____
____
____
Заведующий кафедрой

____
(подпись, инициалы и фамилия)
