1920

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Филиал федерального государственного бюджетного образовательного учреждения высшего образования
«Кубанский государственный университет» в г. Славянске-на-Кубани
Факультет математики, информатики, биологии и технологии
Кафедра математики, информатики, естественнонаучных и общетехнических дисциплин

УТВЕРЖДАЮ:
Проректор по учебной работе, качеству образования - первый проректор

_____ Т. А. Хагуров
«30» мая 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ФТД.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Специальность 44.05.01 Педагогика и психология девиантного поведения

Специализация Психолого-педагогическая профилактика девиантного поведения несовершеннолетних

Форма обучения: очная

Квалификация (степень) выпускника специалист

Краснодар 2025

Рабочая программа факультативной дисциплины «Информационная безопасность» составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО)- специалитет по специальности 44.05.01 Педагогика и психология девиантного поведения, утв. приказом Министерства образования и науки Российской Федерации от 15 апреля 2021 г. № 297, зарегистрировано в Минюсте России 24.05.2021 № 63580

Программу составил:

Поздняков С. А., доцент кафедры математики, информатики, естественнонаучных и общетехнических дисциплин
канд. тех. наук,

Рабочая программа факультативной дисциплины «Информационная безопасность» утверждена на заседании кафедры математики, информатики, естественнонаучных и общетехнических дисциплин
протокол № 9 от 06.05.2025 г.

Зав. кафедрой математики, информатики, естественнонаучных и общетехнических дисциплин Радченко С. А.,

Утверждена на заседании учебно-методической комиссии филиала,
протокол № 9 от 14.05.2025 г.

Председатель УМК филиала Поздняков С. А.

Рецензенты:

Пышная Л.Н., директор МАОУ СОШ № 18 имени Героя Советского Союза И. К.. Боронина, г. Славянска-на-Кубани МО Славянский район

Пушечкин Н.П., доцент, канд. физ.-мат. наук, доцент кафедры МИЕиОД, филиала КубГУ в г.Славянске-на-Кубани

Содержание

1 Цели и задачи изучения дисциплины

1.1 Цель освоения дисциплины

Целями освоения дисциплины «Информационная безопасность» являются:

– формирование у обучающихся системы знаний в области теории и практики информационной безопасности, а также практических навыков и способностей осуществления мероприятий по обеспечению информационной безопасности функционирования информационных систем в образовательных организациях.

1.2 Задачи дисциплины

Изучение дисциплины «Информационная безопасность» направлено на формирование у обучающихся следующих компетенций: ОПК-12

ОПК-12 – Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

В соответствие с этим ставятся следующие задачи дисциплины:

1. Изучить основные направления обеспечения информационной безопасности, меры законодательного, административного, процедурного и программно-технического уровней при работе на вычислительной технике и в каналах связи;

2. Приобрести теоретические знания и практические навыки по использованию современных методов защиты информации в компьютерных системах;

3. Изучить способы усовершенствования информационно-образовательной среды образовательной организации; безопасное использование интернет-ресурсов, ИКТ-технологий в творческом потенциале педагога для повышения качества образования и воспитания обучающихся, а также соблюдение правового законодательства в области информации;

4. Развить навыки информационной культуры учителя, необходимые для дальнейшего самообучения в условиях непрерывного развития и совершенствования информационных технологий.

1.3 Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность» относится к части «Факультативы» дисциплин учебного плана. Для освоения дисциплины обучающиеся должны владеть математическими знаниями, умениями, навыками, способами деятельности и установками, полученными и сформированными в рамках программы средней школы, а также знаниями в области педагогики, психологии, информатики, ей предшествует дисциплина «Анализ данных в профессиональной сфере».

В соответствии с рабочим учебным планом дисциплина изучается на 2 курсе, 4 семестре. Вид промежуточной аттестации: зачет.

1.4 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих общепрофессиональных компетенций (ОПК).

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине
ОПК-12 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	
ИОПК 12.5 Знание современных цифровых технологий, возможность их применения для цифровой без-	Знает основные принципы применения современных цифровых технологий, потенциальные риски и способы их нейтрализации в учебной и внеучеб-

опасности, потенциальные риски и способы их нейтрализации	ной деятельности
	Умеет применять современные цифровые технологий для цифровой безопасности в процессе реализации учебной и внеучебной деятельности
	Владеет современными информационными технологиями цифровой безопасности с учетом потенциальных рисков и способов их нейтрализации для решения задач профессиональной деятельности

2 Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 2 зач. ед. (72 ч.), их распределение по видам работ представлено в таблице

Вид учебной работы		Всего часов	Семестр (часы)
			4 семестр
Контактная работа			
Аудиторные занятия (всего):		**30**	**30**
Занятия лекционного типа		16	16
Лабораторные занятия		-	-
Занятия семинарского типа (семинары, практические занятия)		14	14
Иная контактная работа:			
Контроль самостоятельной работы		2	2
Промежуточная аттестация (ИКР)		0,2	0,2
Самостоятельная работа, в том числе:			
Курсовая работа (подготовка и написание)		-	-
Проработка учебного (теоретического) материала		36	36
Подготовка к текущему контролю		3,8	3,8
Контроль:			
Подготовка к экзамену/зачету		-	-
Общая трудоемкость	**Всего часов**	**72**	**72**
	в том числе контактная работа	**32,2**	**32,2**
	зач. ед	**2**	**2**

2.2 Структура дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.
4 семестр

№	Наименование разделов	Всего	Количество часов				
			Аудиторная работа			Внеаудиторная работа	КСР, ИКР, контроль
			ЛК	ПЗ	ЛР	СР	-
1	Нормативно-правовые документы в сфере информационной безопасности преподавателя в российском и мировом сообществе	9	2	2		5	
2	Программные средства защиты информации	9	2	2		5	

№	Наименование разделов	Всего	Количество часов				
			Аудиторная работа			Внеаудиторная работа	КСР, ИКР, контроль
			ЛК	ПЗ	ЛР	СР	-
3	Аппаратные средства защиты информации	9	2	2		5	
4	Информационная безопасность в социальных сетях	9	2	2		5	
5	Методы и технологии борьбы с компьютерными вирусами	9	2	2		5	
6	Информационная война и информационный терроризм	12	4	2		6	
7	Биометрия	9	2	2		5	
ИТОГО по разделам дисциплины		**66**	**16**	**14**	**-**	**36**	**-**
Контроль самостоятельной работы		2	-	-	-	-	2
Промежуточная аттестация (ИКР)		0,2	-	-	-	-	0,2
Подготовка к текущему контролю		3,8	-	-	-	3,8	-
Подготовка к зачету		-	-	-	-	-	-
Общая трудоемкость по дисциплине		**72**	**16**	**14**	**-**	**39,8**	**2,2**

Примечание: ЛК – лекции; ПЗ – практические занятия, семинары; ЛР – лабораторные работы; СР – самостоятельная работа студента; ИКР – иная контактная работа; КСР – контроль самостоятельной работы.

2.3 Содержание разделов дисциплины

2.3.1 Занятия лекционного типа

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
4 семестр			
1	Нормативно-правовые документы в сфере информационной безопасности преподавателя в российском и мировом сообществе	Концепция информационной безопасности. Лицензирование и сертификация в области защиты информации. Основные нормативные руководящие документы. Виды угроз информационной безопасности РФ	УП, Т
2	Программные средства защиты информации	Программы идентификации и аутентификации пользователей КС; программы разграничения доступа пользователей к ресурсам КС; программы шифрования информации; программы защиты информационных ресурсов (системного и прикладного программного обеспечения, баз данных, компьютерных средств обучения и т. п.) от несанкционированного изменения, использования и копирования	УП, Т
3	Аппаратные средства защиты информации	Аппаратные средства защиты информации: электрические, электронные, оптические, лазерные и другие устройства; специальные компьютеры, системы контроля сотрудников, защиты серверов и корпоративных сетей	УП, Т

4	Информационная безопасность в социальных сетях	Основные понятия сетевого этикета. Правила поведения в сети Интернет.	УП, Т
5	Методы и технологии борьбы с компьютерными вирусами	Методы обнаружения компьютерных вирусов. Технологии борьбы с компьютерными вирусами	УП, Т
6	Информационная война и информационный терроризм	Понятие «информационная война и информационный терроризм». Средства ведения информационных войн. Способы защиты	УП, Т
7	Биометрия	Биометрические характеристики. Биометрические технологии как средство обеспечения информационной безопасности	УП, Т

Примечание: УП – устный (письменный) опрос, Т – тестирование, К – коллоквиум, ПР – практическая работа.

2.3.2 Занятия семинарского типа

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
4 семестр			
1	Нормативно-правовые документы в сфере информационной безопасности преподавателя в российском и мировом сообществе	Государственная политика в сфере информатизации образования. Основные нормативные акты, регламентирующие государственную политику в сфере информатизации образования	Т, УП, ПР
2	Программные аппаратные средства защиты информации	Классификация программных аппаратных средств защиты информации, изучение их характеристик	Т, УП, ПР
3	Аппаратные средства защиты информации	Классификация аппаратных средств защиты информации, изучение их характеристик. Составление плана защиты информации организации, оценка видов угроз ОО.	Т, УП, ПР
4	Информационная безопасность в социальных сетях	Изучение основных понятий сетевого этикета. Правила поведения в сети Интернет.	Т, УП, ПР
5	Методы и технологии борьбы с компьютерными вирусами	Изучение методов обнаружения и технологий борьбы с компьютерными вирусам	Т, УП, ПР
6	Информационная война и информационный терроризм	Изучение способов защиты от информационных атак и информационного терроризма	Т, УП, ПР
7	Биометрия	Изучение биометрических характеристик. Правовые аспекты применения биометрических технологий	Т, УП, ПР

Примечание: УП – устный (письменный) опрос, Т – тестирование, К – коллоквиум, ПР – практическая работа.

2.3.3 Лабораторные занятия

Лабораторные занятия не предусмотрены учебным планом.

2.3.4 Примерная тематика курсовых работ

Курсовые работы не предусмотрены учебным планом.

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	Подготовка к лекционным и практическим (семинарским) занятиям	Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш. – 4-е изд. – Москва : РИОР : ИНФРА-М, 2024. – 336 с. – (Высшее образование). – URL: https://znanium.ru/catalog/product/2082642. – ISBN 978-5-369-01761-6. Городнова, А. А. Развитие информационного общества : учебник и практикум для вузов / А. А. Городнова. – 2-е изд. – Москва : Юрайт, 2024. – 294 с. – (Высшее образование). – URL: https://urait.ru/bcode/545422. – ISBN 978-5-534-18716-8. Мансуров, Г. З. Право цифровой безопасности : учебник / Г. З. Мансуров. – Москва : Директ-Медиа, 2022. – 148 с. – URL: https://biblioclub.ru/index.php?page=book&id=687364. – ISBN 978-5-4499-3061-3. Сидак, А. А. Информационная безопасность. Физические основы технических каналов утечки информации : учебное пособие / А. А. Сидак, В. В. Василенко, С. В. Рыженко ; Технологический университет имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова. – Москва : Директ-Медиа, 2022. – 128 с. – URL: https://biblioclub.ru/index.php?page=book&id=694670. – ISBN 978-5-4499-3327-0.
2	Выполнение самостоятельной работы	Козырь, Н. С. Гуманитарные аспекты информационной безопасности : учебное пособие для вузов / Н. С. Козырь, Н. В. Седых. – Москва : Юрайт, 2024. – 170 с. – (Высшее образование). – URL: https://urait.ru/bcode/544965. – ISBN 978-5-534-17153-2. Преступления в сфере высоких технологий и информационной безопасности : учебное пособие / В. Ф. Васюков, А. Г. Волеводз, М. М. Долгиева, В. Н. Чаплыгина ; Московский государственный институт международных отношений (Университет). – Москва : Прометей, 2023. – 1086 с. – URL: https://biblioclub.ru/index.php?page=book&id=701090. – ISBN 978-5-00172-447-6. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. – 3-е изд. – Москва : Юрайт, 2024. – 327 с. – (Высшее образование). – URL: https://urait.ru/bcode/542739. – ISBN 978-5-534-16772-6.
3	Подготовка к устному (письменному) опросу	Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш. – 4-е изд. – Москва : РИОР : ИНФРА-М, 2024. – 336 с. – (Высшее образование). – URL: https://znanium.ru/catalog/product/2082642. – ISBN 978-5-369-01761-6. Городнова, А. А. Развитие информационного общества : учебник и практикум для вузов / А. А. Городнова. – 2-е изд. – Москва : Юрайт, 2024. – 294 с. – (Высшее образование). – URL: https://urait.ru/bcode/545422. – ISBN 978-5-534-18716-8.

		Козырь, Н. С. Гуманитарные аспекты информационной безопасности : учебное пособие для вузов / Н. С. Козырь, Н. В. Седых. – Москва : Юрайт, 2024. – 170 с. – (Высшее образование). – URL: https://urait.ru/bcode/544965. – ISBN 978-5-534-17153-2. Мансуров, Г. З. Право цифровой безопасности : учебник / Г. З. Мансуров. – Москва : Директ-Медиа, 2022. – 148 с. – URL: https://biblioclub.ru/index.php?page=book&id=687364. – ISBN 978-5-4499-3061-3. Преступления в сфере высоких технологий и информационной безопасности : учебное пособие / В. Ф. Васюков, А. Г. Волеводз, М. М. Долгиева, В. Н. Чаплыгина ; Московский государственный институт международных отношений (Университет). – Москва : Прометей, 2023. – 1086 с. – URL: https://biblioclub.ru/index.php?page=book&id=701090. – ISBN 978-5-00172-447-6. Сидак, А. А. Информационная безопасность. Физические основы технических каналов утечки информации : учебное пособие / А. А. Сидак, В. В. Василенко, С. В. Рыженко ; Технологический университет имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова. – Москва : Директ-Медиа, 2022. – 128 с. – URL: https://biblioclub.ru/index.php?page=book&id=694670. – ISBN 978-5-4499-3327-0. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. – 3-е изд. – Москва : Юрайт, 2024. – 327 с. – (Высшее образование). – URL: https://urait.ru/bcode/542739. – ISBN 978-5-534-16772-6.
4	Подготовка к тестированию (текущей аттестации)	Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш. – 4-е изд. – Москва : РИОР : ИНФРА-М, 2024. – 336 с. – (Высшее образование). – URL: https://znanium.ru/catalog/product/2082642. – ISBN 978-5-369-01761-6. Городнова, А. А. Развитие информационного общества : учебник и практикум для вузов / А. А. Городнова. – 2-е изд. – Москва : Юрайт, 2024. – 294 с. – (Высшее образование). – URL: https://urait.ru/bcode/545422. – ISBN 978-5-534-18716-8. Козырь, Н. С. Гуманитарные аспекты информационной безопасности : учебное пособие для вузов / Н. С. Козырь, Н. В. Седых. – Москва : Юрайт, 2024. – 170 с. – (Высшее образование). – URL: https://urait.ru/bcode/544965. – ISBN 978-5-534-17153-2. Мансуров, Г. З. Право цифровой безопасности : учебник / Г. З. Мансуров. – Москва : Директ-Медиа, 2022. – 148 с. – URL: https://biblioclub.ru/index.php?page=book&id=687364. – ISBN 978-5-4499-3061-3. Преступления в сфере высоких технологий и информационной безопасности : учебное пособие / В. Ф. Васюков, А. Г. Волеводз, М. М. Долгиева, В. Н. Чаплыгина ; Московский государственный институт международных отношений (Университет). – Москва : Прометей, 2023. – 1086 с. – URL: https://biblioclub.ru/index.php?page=book&id=701090. – ISBN 978-5-00172-447-6. Сидак, А. А. Информационная безопасность. Физические основы технических каналов утечки информации : учебное пособие / А. А. Сидак,

		В. В. Василенко, С. В. Рыженко ; Технологический университет имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова. – Москва : Директ-Медиа, 2022. – 128 с. – URL: https://biblioclub.ru/index.php?page=book&id=694670. – ISBN 978-5-4499-3327-0. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. – 3-е изд. – Москва : Юрайт, 2024. – 327 с. – (Высшее образование). – URL: https://urait.ru/bcode/542739. – ISBN 978-5-534-16772-6.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

для лиц с нарушениями зрения:

– в форме электронного документа,

для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа,

Данный перечень может быть дополнен и конкретизирован в зависимости от контингента обучающихся.

3 Образовательные технологии

С целью формирования и развития профессиональных навыков обучающихся, в соответствии с требованиями ФГОС ВО по направлению подготовки, для реализация компетентностного подхода программа предусматривает широкое использование в учебном процессе следующих форм учебной работы:

– активные формы (лекция, вводная лекция, обзорная лекция, заключительная лекция, презентация);

– интерактивные формы (практическое занятие, семинар, компьютерная симуляция);

– внеаудиторные формы (консультация, практикум, самостоятельная работа, подготовка реферата, написание курсовой работы);

– формы контроля знаний (опрос, практическая работа, тестирование, зачёт, экзамен).

3.1 Образовательные технологии при проведении лекций

Лекция – одна из основных форм организации учебного процесса, представляющая собой устное, монологическое, систематическое, последовательное изложение преподавателем учебного материала. Она предшествует всем другим формам организации учебного процесса, позволяет оперативно актуализировать учебный материал дисциплины. Для повышения эффективности лекций целесообразно воспользоваться следующими рекомендациями:

– четко и ясно структурировать занятие;

– рационально дозировать материал в каждом из разделов;

– использовать простой, доступный язык, образную речь с примерами и сравнениями;

– отказаться, насколько это возможно, от иностранных слов;

– использовать наглядные пособия, схемы, таблицы, модели, графики и т. п.;

– применять риторические и уточняющие понимание материала вопросы;

– обращаться к техническим средствам обучения.

№	Тема	Виды применяемых образовательных технологий	Кол. час
4 семестр			
1	Нормативно-правовые документы в сфере информационной безопасности преподавателя в российском и мировом сообществе	АВТ, РП, ТПС, ИСМ	2
2	Программные аппаратные средства защиты информации	АВТ, РП, ТПС, ИСМ	2
3	Аппаратные средства защиты информации	АВТ, РП, ТПС, ИСМ	2
4	Информационная безопасность в социальных сетях	АВТ, РП, ТПС, ИСМ	2
5	Методы и технологии борьбы с компьютерными вирусами	АВТ, РП, ТПС, ИСМ	2
6	Информационная война и информационный терроризм	АВТ, РП, ТПС, ИСМ	2
7	Биометрия	АВТ, РП, ТПС, ИСМ	4
		Итого по курсу	16
		в том числе интерактивное обучение*	-

Примечание: АВТ – аудиовизуальная технология (основная информационная технология обучения, осуществляемая с использованием носителей информации, предназначенных для восприятия человеком по двум каналам одновременно зрительному и слуховому при помощи соответствующих технических устройств, а также закономерностей, принципов и особенностей представления и восприятия аудиовизуальной информации); РП – репродуктивная технология; РМГ – работа в малых группах (в парах, ротационных тройках); ЛПО – лекции с проблемным изложением (проблемное обучение); ЭБ – эвристическая беседа; СПО – семинары в форме дискуссий, дебатов (проблемное обучение); ИСМ – использование средств мультимедиа (компьютерные классы); ТПС – технология полноценного сотрудничества.

3.2 Образовательные технологии при проведении практических занятий

Практическое (семинарское) занятие – основная интерактивная форма организации учебного процесса, дополняющая теоретический курс или лекционную часть учебной дисциплины и призванная помочь обучающимся освоиться в «пространстве» дисциплины; самостоятельно оперировать теоретическими знаниями на конкретном учебном материале. Для практического занятия в качестве темы выбирается обычно такая учебная задача, которая предполагает не существенные эвристические и аналитические напряжения и продвижения, а потребность обучающегося «потрогать» материал, опознать в конкретном то общее, о чем говорилось в лекции.

№	Тема	Виды применяемых образовательных технологий	Кол. час
4 семестр			

1	Нормативно-правовые документы в сфере информационной безопасности преподавателя в российском и мировом сообществе	ИСМ, РМГ, ТПС	2
2	Программные аппаратные средства защиты информации	ИСМ, РМГ, ТПС	2
3	Аппаратные средства защиты информации	ИСМ, РМГ, ТПС	2
4	Информационная безопасность в социальных сетях	ИСМ, РМГ, ТПС	2
5	Методы и технологии борьбы с компьютерными вирусами	ИСМ, РМГ, ТПС	2
6	Информационная война и информационный терроризм	ИСМ, РМГ, ТПС	2
7	Биометрия	ИСМ, РМГ, ТПС	2
		Итого по курсу	14
		в том числе интерактивное обучение*	-

4 Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «Вводный курс математики».
Оценочные средства включает контрольные материалы для проведения **текущего контроля** в формах вопросов для устного/письменного опроса (В), тестовых заданий (Т), заданий для практической работы (П), вопросов к коллоквиуму (К) и **промежуточной аттестации** в форме вопросов к зачету (З) или к экзамену (Э).
Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.
– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;
– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;
– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.
Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:
Для лиц с нарушениями зрения:
– в печатной форме увеличенным шрифтом,
– в форме электронного документа.
Для лиц с нарушениями слуха:
– в печатной форме,
– в форме электронного документа.
Для лиц с нарушениями опорно-двигательного аппарата:
– в печатной форме,
– в форме электронного документа.
Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

4.1 Структура оценочных средств для текущей и промежуточной аттестации

№ п/п	Код и наименование индикатора (в соответствии с п. 1.4)	Результаты обучения (в соответствии с п. 1.4)	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1	ИОПК 12.5 Знание современных цифровых технологий, возможность их применения для цифровой безопасности, потенциальные риски и способы их нейтрализации	Знает основные принципы применения современных цифровых технологий, потенциальные риски и способы их нейтрализации в учебной и внеучебной деятельности	Практические работы, устные (письменные) опросы, проверочные тесты, долговременная СРС	Вопросы на зачете
		Умеет применять современные цифровые технологий для цифровой безопасности в процессе реализации учебной и внеучебной деятельности	Практические работы, устные (письменные) опросы, проверочные тесты, долговременная СРС	Вопросы на зачете
		Владеет современными информационными технологиями цифровой безопасности с учетом потенциальных рисков и способов их нейтрализации для решения задач профессиональной деятельности	Практические работы, устные (письменные) опросы, проверочные тесты, долговременная СРС	Вопросы на зачете

4 СЕМЕСТР

№	Контролируемые разделы дисциплины*	Код контролируемой компетенции (или ее части)	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1	Нормативно-правовые документы в сфере информационной безопасности преподавателя в российском и мировом сообществе	ОПК-12	В, Т, П	з
2	Программные аппаратные средства защиты информации	ОПК-12	В, Т, П	з
3	Аппаратные средства защиты информации	ОПК-12	В, Т, П	з
4	Информационная безопасность в социальных сетях	ОПК-12	В, Т, П	з
5	Методы и технологии борьбы	ОПК-12	В, Т, П	з

	с компьютерными вирусами			
6	Информационная война и информационный терроризм	ОПК-12	В, Т, П	з
7	Биометрия	ОПК-12	В, Т, П	з

4.2 Показатели, критерии и шкала оценки сформированных компетенций

Продвинутый уровень – полная сформированность и устойчивость всех компетенций, охваченных компетентностной моделью.

Базовый уровень – прочная сформированность и устойчивость компетенций, охваченных компетентностной моделью.

Пороговый уровень – достаточная (фрагментарная) сформированность компетенций, охваченных компетентностной моделью.

Код и наименование компетенций	**Соответствие уровней освоения компетенции планируемым результатам обучения и критериям их оценивания**		
	пороговый	**базовый**	**продвинутый**
	Оценка		
	Удовлетворительно /зачтено	Хорошо/зачтено	Отлично/зачтено
ОПК-12	- частично с пробелами освоены знания, умения, компетенции и теоретический материал; - многие учебные задания либо не выполнил, либо они оценены числом баллов близким к минимальному; - некоторые практические навыки не сформированы.	- практически полностью освоены знания, умения, компетенции и теоретический материал; - учебные задания не оценены максимальным числом баллов; - в основном сформированы практические навыки.	- освоены знания, умения, компетенции и теоретический материал без пробелов; - выполнены все задания, предусмотренные учебным планом на высоком качественном уровне; - практические навыки профессионального применения освоенных знаний сформированы.

Минимальный уровень (не зачтено) - не освоены знания, умения, компетенции и теоретический материал, учебные задания не выполнены, практические навыки не сформированы.

4.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерные вопросы для устного (письменного) опроса

Перечень компетенций (части компетенции), проверяемых оценочным средством: ОПК-12.

1. Понятие информационной безопасности. Понятие информационной безопасности электронной информационно-образовательной среде образовательной организации
2. Основные составляющие информационной безопасности
3. Понятия "Безопасная система", "Надежная система"
4. Основные определения и критерии классификации угроз безопасности информации
5. Случайные угрозы безопасности информации
6. Преднамеренные умышленные угрозы безопасности информации
7. Неформальная модель нарушителя
8. Компьютерные преступления
9. Компьютерное пиратство. Хакеры.
10. Руководящие документы Гостехкомиссии России в области информационной безопасности

11. Особенности современных информационных систем, существенные с точки зрения безопасности
12. Законодательный уровень информационной безопасности
13. Административный уровень информационной безопасности
14. Процедурный уровень информационной безопасности
15. Программно-технический уровень информационной безопасности
16. Сервисы информационной безопасности
17. Методы парольной защиты
18. Использование простого пароля для защиты информационных систем
19. Использование динамически изменяющегося пароля для защиты информационных систем
20. Идентификация/аутентификация с помощью биометрических данных. Основные понятия.
21. Способы хранения матрицы доступа: списки управления доступом.
22. Способы хранения матрицы доступа: перечни возможностей.
23. Система блочного шифрования DES
24. Система блочного шифрования ГОСТ 28147-89
25. Асимметричные системы шифрования
26. Типы компьютерных вирусов
27. Антивирусное программное обеспечение
28. Классификация межсетевых экранов
29. Туннелирование
30. Пути и проблемы практической реализации концепции комплексной защиты информации

Примерные тестовые задания для текущей аттестации

Перечень компетенций (части компетенции), проверяемых оценочным средством: ОПК-12.

1. Выберите определение термина «информационная безопасность» согласно ГОСТ Р ИСО/МЭК 17799-2005, ст.2.1:
1) защита конфиденциальности, целостности и доступности информации
2) защита информации от злоумышленников, взлома, утечки данных
3) защищенность информации от незаконного ознакомления, преобразования и уничтожения, а также защищенность информационных ресурсов от вредоносных воздействий
4) защищенность информации с учетом принципов конфиденциальности, целостности и фильтрации

2. Согласно Указа Президента РФ от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» под информационной сферой понимается:
1) совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений
2) правовые, организационные, технические и другие средства информации
3) совокупность объектов информатизации, информационных систем, сайтов в сети "Интернет" и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации
4) область создания и внедрения информационных технологий с целью развития отрасли информационных технологий и электронной промышленности
3. Под вредоносными воздействиями на информационные ресурсы понимаются:
1) попытки проникновения злоумышленников
2) ошибки персонала, стихийные бедствия

3) выход из строя аппаратных и программных средств
4) попытки проникновения злоумышленников, ошибки персонала, выход из строя аппаратных и программных средств, стихийные бедствия и т.п.
4. Понятие «угроза» в рамках информационной безопасности – это…
1) передача информации третьим лицам без согласия ее обладателя
2) возможное происшествие (преднамеренное или нет), которое способно оказать нежелательное воздействие на активы и ресурсы, связанные с вычислительной системой
3) обеспечение доступа к информации любым пользователям
4) осуществлено преднамеренное изменение информации субъектом, не имеющими на него право
5. Конфиденциальность информации – это ...
1) обеспечение доступа к информации только авторизованным пользователям
2) требование не передавать такую информацию третьим лицам без согласия ее обладателя
3) состояние информации, при котором отсутствует любое ее изменение
4) защита от нежелательного воздействия на активы и ресурсы, связанные с вычислительной системой
6. Сколько различных типов угроз, и соответственно, свойства информации принято выделять?
1) 2
2) 3
3) 4
4) 5
7. Целостность информации - это...
1) обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости
2) защита от нежелательного воздействия на активы и ресурсы, связанные с вычислительной системой
3) состояние информации, при котором отсутствует любое ее изменение
4) защищенность информации от незаконного ознакомления, преобразования и уничтожения
8. Три свойства информации – это...
1) конфиденциальность, целостность, безопасность
2) авторизация, целостность, безопасность
3) конфиденциальность, целостность, доступность
4) конфиденциальность, авторизация, целостность
9. Доступность информации – это...
1) обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости
2) защита от нежелательного воздействия на активы и ресурсы, связанные с вычислительной системой
3) состояние информации, при котором отсутствует любое ее изменение
4) защищенность информации от незаконного ознакомления, преобразования и уничтожения
10. Что не относится к видам защиты информации согласно ГОСТ Р 50922-2006
1) правовая защита информации
2) криптографическая защита информации
3) технологическая защита информации
4) физическая защита информации
11. Разработка законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением – это…
1) правовая защита информации

2) криптографическая защита информации
3) техническая защита информации
4) физическая защита информации
12. Защита информации с помощью ее криптографического преобразования – это…
1) правовая защита информации
2) криптографическая защита информации
3) техническая защита информации
4) физическая защита информации
13. Обеспечение безопасности информации некриптографическими методами, с применением технических, программных и программно-технических средств – это…
1) правовая защита информации
2) криптографическая защита информации
3) техническая защита информации
4) физическая защита информации
14. Применение организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты – это…
1) правовая защита информации
2) криптографическая защита информации
3) техническая защита информации
4) физическая защита информации
15. К основным целям защиты информации не относится:
1) Соблюдение конфиденциальности информации ограниченного доступа, реализация конституционного права граждан на доступ к информации
2) Предотвращение несанкционированного доступа к информации и (или) передачи её лицам, не имеющим права на доступ к такой информации
3) Недопущение воздействия на технологические объекты, в результате которого нарушается их функционирование
4) Предотвращение несанкционированных действий по уничтожению, модификации, копированию, блокированию и предоставлению информации, а также иных неправомерных действий в отношении такой информации
16. К основным видам информационных атак на мобильные телефоны не относится:
1) установка вредоносных приложения и посещение веб-сайтов
2) мошенническая смс-атака
3) DDoS-атака
4) утечки данных
17. DDos-атака – это…
1) Отправка большого количества запросов на веб-ресурс, в результате чего может произойти прекращение работы ресурса – «отказ в обслуживании»
2) Атака вредоносной программы, которая маскируется под легальное ПО. С их помощью злоумышленники пытаются получить доступ к системе пользователя
3) Использование сети из большого количества компьютеров, зараженных вредоносным программным обеспечением для различных вредоносных действий без ведома пользователей
4) Атака с целью получение ценных данных пользователей, которые могут быть проданы или использованы для вредоносных целей, таких как вымогательство, похищение денег или личных данных
18. Фишинг – это…
1) Отправка большого количества запросов на веб-ресурс, в результате чего может произойти прекращение работы ресурса – «отказ в обслуживании»
2) Атака вредоносной программы, которая маскируется под легальное ПО. С их помощью злоумышленники пытаются получить доступ к системе пользователя

3) Использование сети из большого количества компьютеров, зараженных вредоносным программным обеспечением для различных вредоносных действий без ведома пользователей
4) Атака с целью получение ценных данных пользователей, которые могут быть проданы или использованы для вредоносных целей, таких как вымогательство, похищение денег или личных данных
19. Троян – это…
1) Отправка большого количества запросов на веб-ресурс, в результате чего может произойти прекращение работы ресурса – «отказ в обслуживании»
2) Атака вредоносной программы, которая маскируется под легальное ПО. С их помощью злоумышленники пытаются получить доступ к системе пользователя
3) Использование сети из большого количества компьютеров, зараженных вредоносным программным обеспечением для различных вредоносных действий без ведома пользователей
4) Атака с целью получение ценных данных пользователей, которые могут быть проданы или использованы для вредоносных целей, таких как вымогательство, похищение денег или личных данных
20. Ботнет – это…
1) Отправка большого количества запросов на веб-ресурс, в результате чего может произойти прекращение работы ресурса – «отказ в обслуживании»
2) Атака вредоносной программы, которая маскируется под легальное ПО. С их помощью злоумышленники пытаются получить доступ к системе пользователя
3) Использование сети из большого количества компьютеров, зараженных вредоносным программным обеспечением для различных вредоносных действий без ведома пользователей
4) Атака с целью получение ценных данных пользователей, которые могут быть проданы или использованы для вредоносных целей, таких как вымогательство, похищение денег или личных данных
21. К правовым методам, обеспечивающим информационную безопасность, относятся:
1) Разработка аппаратных средств обеспечения правовых данных
2) Разработка и установка во всех компьютерных правовых сетях журналов учета действий
3) Разработка и конкретизация правовых нормативных актов обеспечения безопасности 4) Конкретизация правовых нормативных актов безопасности аппаратных средств
22. Основными источниками угроз информационной безопасности являются все указанное в списке:
1) Хищение жестких дисков, подключение к сети, инсайдерство
2) Хищение данных, подкуп системных администраторов, нарушение регламента работы
3) Перехват данных, хищение данных, изменение архитектуры системы
4) Многоплатформенная реализация системы, разграничение доступа к потокам данных
23. Что не относится к одному из основных видов рисков на примере социальной сети «ВКонтакте»:
1) Пропаганда нездорового образа жизни
2) Пропаганда развития навыков создания и распространения медиатекстов с соблюдением нравственных и правовых норм
3) Пропаганда, представляющая собой угрозу для здоровья
4) Пропаганда разжигания конфликтов между несколькими различными социальными группами
24. Медиакультура – это…
1) культура производства, передачи и восприятия информации
2) умение искать информацию и проверять ее достоверность
3) полнота и точность передачи информации
4) умение обрабатывать информацию с помощью разных технологий

25. В роли потребителя медиакультуры необходимо…
1) уметь оценивать и создавать медиатексты
2) уметь искать информацию и проверять ее достоверность
3) оперативно передавать информацию
4) уметь обрабатывать информацию с помощью разных технологий

4.4 Зачетно-экзаменационные материалы для промежуточной аттестации

Примерные вопросы на зачет

1. Виды защиты информации
2. Основные цели защиты информации
3. Примеры информационных атак
4. Доктрина информационной безопасности РФ
5. Нормативное регулирование в сфере обеспечения информационной безопасности обучающихся
6. Информационная безопасность несовершеннолетних: правовые и социальные аспекты
7. Методы обеспечения информационной безопасности
8. Средства обеспечения информационной безопасности
9. Формальные средства защиты информации
10. Аппаратные или технические средства защиты информации
11. Применение технических средств защиты информации
12. Программные средства защиты информации
13. Программно-аппаратные средства защиты информации
14. Средства уничтожения информации
15. Защита от несанкционированного доступа
16. Методы и средства технологий защиты от угроз информационной безопасности
17. Криптографические методы защиты информации
18. Неформальные средства защиты информации
19. Безопасный интернет
20. Конфиденциальность, целостности и доступности информации
21. Морально-этические средства защиты информации
22. Правила поведения в Интернете (сетевой этикет)
23. Виды зависимости, в том числе от Интернета и цифровых устройств
24. Авторизация, идентификация
25. Однофакторная аутентификация, двухфакторная аутентификация
26. Электронная подпись
27. Информационная война
28. Информационный терроризм
29. Иллюзии соцсетей
30. Биометрия

4.5 Рейтинговая система оценки текущей успеваемости студентов

№	Наименование раздела	Виды оцениваемых работ	Максимальное кол-во баллов
1	2	3	4
4 семестр			
1	Нормативно-правовые документы в сфере информационной без-	Практическая работа Самостоятельная работа	4 4

	опасности преподавателя в российском и мировом сообществе		
2	Программные аппаратные средства защиты информации	Практическая работа Самостоятельная работа	4 4
3	Аппаратные средства защиты информации	Практическая работа Самостоятельная работа	4 4
4	Информационная безопасность в социальных сетях	Практическая работа Самостоятельная работа	4 4
5	Методы и технологии борьбы с компьютерными вирусами	Практическая работа Самостоятельная работа	4 4
6	Информационная война и информационный терроризм	Практическая работа Самостоятельная работа	6 6
7	Биометрия	Практическая работа Самостоятельная работа	4 4
	Внутрисеместровая аттестация	Компьютерное тестирование	40
		ВСЕГО	100

5. Перечень учебной литературы, информационных ресурсов и технологий

5.1. Учебная литература

1. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш. – 4-е изд. – Москва : РИОР : ИНФРА-М, 2024. – 336 с. – (Высшее образование). – URL: https://znanium.ru/catalog/product/2082642. – ISBN 978-5-369-01761-6.
2. Городнова, А. А. Развитие информационного общества : учебник и практикум для вузов / А. А. Городнова. – 2-е изд. – Москва : Юрайт, 2024. – 294 с. – (Высшее образование). – URL: https://urait.ru/bcode/545422. – ISBN 978-5-534-18716-8.
3. Информатика для гуманитариев : учебник и практикум для вузов / Г. Е. Кедрова [и др.] ; под редакцией Г. Е. Кедровой. – 3-е изд. – Москва : Юрайт, 2024. – 662 с. – (Высшее образование). – URL: https://urait.ru/bcode/536415. – ISBN 978-5-534-16197-7.
4. Киселев, Г. М. Информационные технологии в педагогическом образовании : учебник / Г. М. Киселев, Р. В. Бочкова. – 6-е изд. – Москва : Дашков и К°, 2024. – 300 с. – (Учебные издания для бакалавров). – URL: https://biblioclub.ru/index.php?page=book&id=711130. – ISBN 978-5-394-05582-9.
5. Козырь, Н. С. Гуманитарные аспекты информационной безопасности : учебное пособие для вузов / Н. С. Козырь, Н. В. Седых. – Москва : Юрайт, 2024. – 170 с. – (Высшее образование). – URL: https://urait.ru/bcode/544965. – ISBN 978-5-534-17153-2.
6. Мансуров, Г. З. Право цифровой безопасности : учебник / Г. З. Мансуров. – Москва : Директ-Медиа, 2022. – 148 с. – URL: https://biblioclub.ru/index.php?page=book&id=687364. – ISBN 978-5-4499-3061-3.
7. Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. – 3-е изд. – Санкт-Петербург : Лань, 2024. – 324 с. – URL: https://e.lanbook.com/book/370967. – ISBN 978-5-507-49077-6.
8. Преступления в сфере высоких технологий и информационной безопасности : учебное пособие / В. Ф. Васюков, А. Г. Волеводз, М. М. Долгиева, В. Н. Чаплыгина ; Московский государственный институт международных отношений (Университет). –

Москва : Прометей, 2023. – 1086 с. – URL: https://biblioclub.ru/index.php?page=book&id=701090. – ISBN 978-5-00172-447-6.
9. Сидак, А. А. Информационная безопасность. Физические основы технических каналов утечки информации : учебное пособие / А. А. Сидак, В. В. Василенко, С. В. Рыженко ; Технологический университет имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова. – Москва : Директ-Медиа, 2022. – 128 с. – URL: https://biblioclub.ru/index.php?page=book&id=694670. – ISBN 978-5-4499-3327-0.
10. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. – 3-е изд. – Москва : Юрайт, 2024. – 327 с. – (Высшее образование). – URL: https://urait.ru/bcode/542739. – ISBN 978-5-534-16772-6.

Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья используются специальные сервисы в электронно-библиотечных системах (ЭБС), доступ к которым организует Научная библиотека КубГУ.

5.2. Периодические издания

1. Безопасность информационных технологий. – URL: https://elibrary.ru/title_about_new.asp?id=8429.
2. БИТ. Бизнес & информационные технологии. – URL : https://dlib.eastview.com/browse/publication/66752.
3. Вестник информационной безопасности. – URL: https://dlib.eastview.com/browse/publication/84979.
4. Инфокоммуникационные технологии. – URL : https://www.elibrary.ru/title_about_new.asp?id=9585.
5. Информатизация в цифровой экономике. – URL: https://elibrary.ru/title_about_new.asp?id=77953.
6. Информатика в школе. - URL: https://dlib.eastview.com/browse/publication/18988.
7. Информатика и образование. – URL: http://dlib.eastview.com/browse/publication/18946.
8. Информатика. – URL: https://elibrary.ru/title_about_new.asp?id=64817.
9. Информационно-коммуникационные технологии в педагогическом образовании. – URL: https://www.elibrary.ru/title_about_new.asp?id=48910.
10. Информационно-управляющие системы. – URL: https://dlib.eastview.com/browse/publication/71235.
11. Информационные ресурсы России. – URL: https://dlib.eastview.com/browse/publication/114926.
12. Открытые системы. СУБД. – URL: http://dlib.eastview.com/browse/publication/64072.
13. Прикладная информатика. – URL: https://dlib.eastview.com/browse/publication/66410.
14. Программные продукты и системы. – URL: http://dlib.eastview.com/browse/publication/64086.
15. Проектирование и технология электронных средств. – URL: https://www.elibrary.ru/title_about.asp?id=9013.
16. Системный администратор. – URL: https://dlib.eastview.com/browse/publication/66751
17. Системный анализ и прикладная информатика. – URL: https://e.lanbook.com/journal/2420#journal_name

5.3. Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

5.3.1. Электронно-библиотечные системы (ЭБС)

1. ЭБС «Университетская библиотека онлайн» [учебные, научные издания, первоисточники, художественные произведения различных издательств; журналы; коллекция

медиа-материалов: аудиокниги, аудиофайлы, видеокурсы, экспресс-подготовка к экзаменам, презентации, тесты, карты, онлайн-энциклопедии, словари]. – URL: http://www.biblioclub.ru/.

2. ЭБС «ZNANIUM» [учебные, научные, справочные, научно-популярные издания различных издательств, журналы]. – URL: https://znanium.ru/.

3. ЭБС «Лань» [учебные, научные издания, первоисточники, художественные произведения различных издательств; журналы]. – URL: http://e.lanbook.com/.

4. Образовательная платформа «Юрайт» [учебники и учебные пособия издательства «Юрайт», медиа-материалы, тесты]. – URL: https://urait.ru/.

5. ЭБС «BOOK.ru» [учебная литература, журналы]. – URL: https://www.book.ru.

6. ЭБ ОИЦ «Академия» [учебные издания по общеобразовательным дисциплинам СПО для первого курса, включенных в ФПУ]. – URL: https://academia-moscow.ru/elibrary/.

5.3.2. Профессиональные базы данных

1. Виртуальный читальный зал Российской государственной библиотеки (РГБ). – URL: https://ldiss.rsl.ru/.

2. Национальная электронная библиотека (НЭБ) [включает Электронную библиотеку диссертаций РГБ] : [федеральная государственная информационная система Министерства культуры РФ]. – URL: https://rusneb.ru/ (полный доступ к объектам НЭБ – в локальной сети с компьютеров библиотеки филиала).

3. Научная электронная библиотека «eLIBRARY.RU» [российские научные журналы, труды конференций; Российская национальная база данных научного цитирования (РИНЦ)]. – URL: http://www.elibrary.ru/.

4. Универсальные базы данных «ИВИС» [российские научные журналы по вопросам педагогики и образования, экономики и финансов, информационным технологиям, экономике и предпринимательству, общественным и гуманитарным наукам, индивидуальные издания, Вестники МГУ, СПбГУ, статистические издания России и стран СНГ]. – URL: https://eivis.ru/basic/details.

5. Полнотекстовая коллекция журналов на платформе РЦНИ. Национальная платформа периодических научных изданий. – URL: https://journals.rcsi.science/.

6. Общероссийский портал «Math-Net.Ru» : информационная система доступа к научной информации по математике, физике, информационным технологиям и смежным наукам / Математический институт имени В. А. Стеклова РАН. – URL: http://www.mathnet.ru/.

7. Президентская библиотека им. Б.Н. Ельцина. – URL: https://www.prlib.ru/.

8. Журналы издательства Wiley: [полнотекстовая коллекция электронных журналов по: химии, физике, математике, социальным и гуманитарным наукам, психологии, бизнесу, экономике и юриспруденции]. – URL: https://onlinelibrary.wiley.com/.

9. Полнотекстовая коллекция книг eBook Collections издательства SAGE Publications: [включает монографии и справочники по различным областям знаний: бизнес, психология, криминология и уголовное право, образование, география, науки о Земле и окружающей среде, здравоохранение и социальная помощь, СМИ и коммуникация, культурология, политика и международные отношения, социология и др.]. – URL: https://sk.sagepub.com/books/discipline.

10. Ресурсы Springer Nature: [Полнотекстовая коллекция книг (монографий) издательств Springer Nature по различным отраслям знаний]. – URL: https://link.springer.com/, https://www.nature.com/.

5.3.3. Информационные справочные системы

1. КонсультантПлюс : справочная правовая система (доступ – в локальной сети с компьютеров библиотеки филиала).

5.3.4. Ресурсы свободного доступа

1. Официальный интернет-портал правовой информации. Государственная система правовой информации. – URL: http://pravo.gov.ru/

2. КонсультантПлюс : некоммерческая интернет-версия справочной правовой системы. – URL: https://www.consultant.ru/cons/cgi/online.cgi?req=home&utm_csource=online&utm_cmedium=button.

3. Министерство науки и высшего образования Российской Федерации (Минобрнауки России) - официальный сайт. – URL: https://www.minobrnauki.gov.ru

4. Министерство просвещения Российской Федерации - официальный сайт. – URL: https://edu.gov.ru

5. Портал «Культура.РФ» : гуманитарный просветительский проект, посвященный культуре России [кино, музеи, музыка, театры, архитектура, литература, персоны, традиции, лекции-онлайн] : сайт / Министерство культуры РФ. – URL: https://www.culture.ru/.

6. Справочно-информационный портал «Грамота.ру» / Министерство цифрового развития, связи и массовых коммуникаций РФ. – URL: http://www.gramota.ru/.

7. Лекториум [раздел «Медиатека» – открытый видеоархив лекций на русском языке]: образовательная платформа : сайт. – URL: https://www.lektorium.tv/medialibrary.

8. Научная электронная библиотека «КиберЛенинка» [российские научные журналы]. – URL: http://cyberleninka.ru/.

9. Большая российская энциклопедия: [электронная версия] / Министерство культуры РФ. – URL: https://bigenc.ru/.

10. Лингвистический проект «СЛОВАРИ.РУ» / Институт русского языка им. В. В. Виноградова РАН. – URL: http://slovari.ru/start.aspx?s=0&p=3050.

5.3.5. Собственные электронные образовательные и информационные ресурсы:

1. База информационных потребностей [КубГУ и филиалов] (разделы: Научные публикации преподавателей и обучающихся; Информация об участии преподавателей и обучающихся в научных конференциях; Темы выпускных квалификационных работ студентов). – URL: https://infoneeds.kubsu.ru/infoneeds/.

2. Электронная библиотека информационных ресурсов филиала [КубГУ в г. Славянске-на-Кубани]. – URL: http://sgpi.ru/bip.php.

3. Поступления литературы в библиотеки филиалов : [электронный каталог библиотек филиалов КубГУ]. – URL: http://megapro.kubsu.ru/MegaPro/UserEntry?Action=ToDb&idb=1.

4. Электронная библиотека трудов учёных КубГУ. – URL: http://megapro.kubsu.ru/MegaPro/UserEntry?Action=ToDb&idb=6.

6 Методические указания для обучающихся по освоению дисциплины

6.1. Общие рекомендации по самостоятельной работе обучающихся

Лекционные занятия проводятся по основным разделам дисциплины «Информационная безопасность». Они дополняются практическими работами, в ходе которых студенты выполняют задания по всем предлагаемым темам. Для подготовки к лекциям необходимо изучить основную и дополнительную литературу по заявленной теме и обратить внимание на те вопросы, которые предлагаются к рассмотрению в конце каждой темы.

При изучении дисциплины студенты часть материала должны проработать самостоятельно. Роль самостоятельной работы велика.

Планирование самостоятельной работы студентов по дисциплине необходимо проводить в соответствии с уровнем подготовки студентов к изучаемой дисциплине. Самостоятельная работа студентов распадается на два самостоятельных направления: на изучение и освоение теоретического лекционного материала, и на освоение методики решения практических задач.

При всех формах самостоятельной работы студент может получить разъяснения по непонятным вопросам у преподавателя на индивидуальных консультациях в соответствии с графиком консультаций. Студент может также обратиться к рекомендуемым преподавателем учебникам и учебным пособиям, в которых теоретические вопросы изложены более широко и подробно, чем на лекциях и с достаточным обоснованием. Консультация – активная форма учебной деятельности в педвузе. Консультацию предваряет самостоятельное изучение студентом литературы по определенной теме. Качество консультации зависит от степени подготовки студентов и остроты поставленных перед преподавателем вопросов.

Основной частью самостоятельной работы студента является его систематическая подготовка к практическим занятиям. Студенты должны быть нацелены на важность качественной подготовки к таким занятиям. При подготовке к практическим занятиям студенты должны освоить вначале теоретический материал по новой теме занятия, с тем чтобы использовать эти знания при выполнении практических работ. Если некоторые задания вызвали затруднения при выполнении, попросить объяснить преподавателя на очередном практическом занятии или консультации.

Для работы на практических занятиях, самостоятельной работы во внеаудиторное время, а также для подготовки к зачету рекомендуется использовать методические рекомендации к практическим занятиям. При подготовке к тестированию необходимо повторить материал, рассмотренный на практических занятиях, убедиться в знании терминов, определений и т. д.

Ряд тем и вопросов курса отведены для самостоятельной проработки студентами. При этом у лектора появляется возможность расширить круг изучаемых проблем, дать на самостоятельную проработку новые интересные вопросы. Студент должен разобраться в рекомендуемой литературе и письменно изложить кратко и доступно для себя основное содержание материала. Преподаватель проверяет качество усвоения самостоятельно проработанных вопросов на практических занятиях. Затем корректирует изложение материала и нагрузку на студентов.

Таким образом, использование всех рекомендуемых видов самостоятельной работы дает возможность значительно активизировать работу студентов над материалом курса и повысить уровень их усвоения.

На самостоятельную работу студентов по курсу «Информационная безопасность» отводится около половины времени от общей трудоемкости курса. Сопровождение самостоятельной работы студентов может быть организовано в следующих формах:

- подготовка заданий для домашней контрольной работы с обязательной ее защитой студентами;
- составление индивидуальных планов самостоятельной работы конкретным студентам с указанием темы и видов заданий, форм и сроков представления результатов, критерием оценки самостоятельной работы;
- консультации (индивидуальные и групповые);
- промежуточный контроль хода выполнения заданий строится на основе различных способов взаимодействия со студентами.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

6.2 Организация процедуры промежуточной аттестации

Промежуточная аттестация в семестре осуществляется в форме зачета и организуется в соответствии с утвержденным рабочим учебным планом, рабочей программой дисциплины и расписанием. Студенты очной формы обучения обязаны сдать зачет до начала экзаменационной сессии. Зачет проводится во время последних аудиторных занятий или в дополнительно назначенное время. Не сдача до начала сессии зачета не является основанием для не допуска к экзаменам. Не сдача зачета является академической задолженностью. Повторная сдача (пересдача) зачета возможна только после окончания экзаменационной сессии в соответствии с утвержденным деканом расписанием пересдач. Форм проведения зачета – устная, письменная и др. – устанавливаются преподавателем и доводятся до сведения студентов в начале семестра.

Зачет может быть получен по результатам выполнения практических заданий и/или выступлений студентов на семинарских и практических занятиях. По результатам сдачи зачета выставляется «зачтено» / «не зачтено». «Не зачтено» выставляется только в экзаменационную ведомость. Зачетная ведомость выдается преподавателю в день зачета и возвращается им за три дня до начала экзаменационной сессии. Преподаватель обязан указывать в зачетной книжке студента количество зачетных единиц трудоемкости (ЗЕТ), отводимых учебным планом на изучение данной дисциплины.

Студент обязан явиться к началу зачета в соответствии с расписанием и предъявить преподавателю зачетную книжку. При отсутствии зачетной книжки у студента экзаменатор не имеет права принимать у него зачет. Такой студент считается не явившимся на зачет. В исключительных случаях, на основании распоряжения декана (директора института, филиала) преподаватель может допустить студента к зачету при наличии документа, удостоверяющего личность. В целях объективного оценивания знаний во время проведения зачетов не допускается наличие у студентов посторонних предметов и технических устройств. Студенты, нарушающие правила поведения при проведении зачетов, могут быть незамедлительно удалены из аудитории, к ним могут быть применены меры дисциплинарного воздействия.

При индивидуальном графике сдачи экзаменов и зачетов (досрочная сдача экзаменационной сессии, ликвидация академических задолженностей и т.д.) студенту выдается в деканате индивидуальная ведомость с указанием сроков проведения экзаменов и зачетов. При наличии у студента нескольких задолженностей экзаменационный лист выдается на пересдачу только одной дисциплины. Выдача последующих экзаменационных листов возможна после представления в деканат ранее выданного. Срок действия экзаменационного листа – 5 дней с момента его выдачи.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:
для лиц с нарушениями зрения:
– в печатной форме увеличенным шрифтом,
– в форме электронного документа;
для лиц с нарушениями слуха:
– в печатной форме,
– в форме электронного документа;
для лиц с нарушениями опорно-двигательного аппарата:
– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

Критерии оценки по промежуточной аттестации

Зачет проводится в устной форме. Экзаменатор имеет право задавать студентам дополнительные вопросы по всей учебной программе дисциплины. Время проведения зачета устанавливается нормами времени. Результат сдачи зачета заносится преподавателем в зачетно-экзаменационную ведомость и зачетную книжку.

Критерии оценивания:

«зачтено» выставляется студенту, обнаружившему всестороннее систематическое знание учебно-программного материала в сфере профессиональной деятельности, освоившему основную литературу и знакомому с дополнительной литературой, рекомендованной программой, студентам, усвоившим взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявившему творческие способности в понимании и использовании учебно-программного материала. Также оценка «зачтено» выставляется студенту, обнаружившему знание основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справляющемуся с выполнением практических заданий и учебных (контрольных) нормативов на контрольных работах, зачетах, предусмотренных программой, студентам, обладающим необходимыми знаниями, но допустившим неточности при выполнении контрольных нормативов;

«не зачтено» выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, не может точно выполнять тестовые задания, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания на практике.

Обучающиеся обязаны сдать экзамен в соответствии с расписанием и учебным планом. Экзамен по дисциплине преследует цель оценить сформированность требуемых компетенций, работу обучающегося за курс, получение теоретических знаний, их прочность, развитие творческого мышления, приобретение навыков самостоятельной работы, умение применять полученные знания для решения практических задач.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

7. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

По всем видам учебной деятельности в рамках дисциплины используются аудитории, кабинеты и лаборатории, оснащенные необходимым специализированным и лабораторным оборудованием.

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения
Учебные аудитории для проведения занятий лекционного типа	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер	1. Apache OpenOffice. The Free and Open Productivity Suite. Apache OpenOffice 4.1.3 released – свободное программное обеспечение, бессрочное, с неограниченным количеством лицензий, правообладатель: SUN/Oracle. 2. Условия предоставления услуг Google Chrome. Исходный код предоставляется бесплатно, бессрочно с неограниченным количеством лицензионных соглашений, правообладатель – «Google». 3. Licenses. LibreOffice is Free Software [свободное программное обеспечение LibreOffice], бессрочное, с неограниченным кол-вом лицензий, правообладатель – «The Document Foundation».

		4. 7-Zip. License for use and distribution [7-Zip. Лицензия на использование и распространение]. Свободное программное обеспечение, бессрочное, с неограниченным кол-вом лицензий, правообладатель – Igor Pavlov. 5. Лицензия. Программа FreeCommander, бесплатная, свободного использования, бессрочная, правообладатель – Marek Jasinski. 6. Mozilla Firefox – бесплатная программа на условиях Публичной лицензии, бессрочной для неограниченного количества пользователей, разработчики – участники проекта mozilla.org.
Учебные аудитории для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер	1. Apache OpenOffice. The Free and Open Productivity Suite. Apache OpenOffice 4.1.3 released – свободное программное обеспечение, бессрочное, с неограниченным количеством лицензий, правообладатель: SUN/Oracle. 2. Условия предоставления услуг Google Chrome. Исходный код предоставляется бесплатно, бессрочно с неограниченным количеством лицензионных соглашений, правообладатель – «Google». 3. Licenses. LibreOffice is Free Software [свободное программное обеспечение LibreOffice], бессрочное, с неограниченным кол-вом лицензий, правообладатель – «The Document Foundation». 4. 7-Zip. License for use and distribution [7-Zip. Лицензия на использование и распространение]. Свободное программное обеспечение, бессрочное, с неограниченным кол-вом лицензий, правообладатель – Igor Pavlov. 5. Лицензия. Программа FreeCommander, бесплатная, свободного использования, бессрочная, правообладатель – Marek Jasinski. 6. Mozilla Firefox – бесплатная программа на условиях Публичной лицензии, бессрочной для неограниченного количества пользователей, разработчики – участники проекта mozilla.org.

Для самостоятельной работы обучающихся предусмотрены помещения, укомплектованные специализированной мебелью, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Наименование помещений для самостоятельной работы обучающихся	Оснащенность помещений для самостоятельной работы обучающихся	Перечень лицензионного программного обеспечения
Помещение для самостоятельной работы обучающихся (353560, Краснодарский край, г. Славянск-на-Кубани, ул. Кубанская, 200, Электронный зал библиотеки, читальный зал № 2, № А-1)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	1. Apache OpenOffice. The Free and Open Productivity Suite. Apache OpenOffice 4.1.3 released – свободное программное обеспечение, бессрочное, с неограниченным количеством лицензий, правообладатель: SUN/Oracle. 2. Условия предоставления услуг Google Chrome. Исходный код предоставляется бесплатно, бессрочно с неограниченным количеством лицензионных соглашений, правообладатель – «Google». 3. Licenses. LibreOffice is Free Software [свободное программное обеспечение LibreOffice], бессрочное, с неограниченным кол-вом лицензий, правообладатель – «The Document Foundation». 4. 7-Zip. License for use and distribution [7-Zip. Лицензия на использование и распространение]. Свободное программное обеспечение, бессрочное, с неограниченным кол-вом лицензий, правообладатель – Igor Pavlov. 5. Лицензия. Программа FreeCommander, бесплатная, свободного использования, бессрочная, правообладатель – Marek Jasinski. 6. Mozilla Firefox – бесплатная программа на услови-

		ях Публичной лицензии, бессрочной для неограниченного количества пользователей, разработчики – участники проекта mozilla.org.
Помещение для самостоятельной работы обучающихся (353563, Краснодарский край, г. Славянск-на-Кубани, ул. Коммунистическая, дом № 2, Читальный зал библиотеки, № 2)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение)	1. Apache OpenOffice. The Free and Open Productivity Suite. Apache OpenOffice 4.1.3 released – свободное программное обеспечение, бессрочное, с неограниченным количеством лицензий, правообладатель: SUN/Oracle. 2. Условия предоставления услуг Google Chrome. Исходный код предоставляется бесплатно, бессрочно с неограниченным количеством лицензионных соглашений, правообладатель – «Google». 3. Licenses. LibreOffice is Free Software [свободное программное обеспечение LibreOffice], бессрочное, с неограниченным кол-вом лицензий, правообладатель – «The Document Foundation». 4. 7-Zip. License for use and distribution [7-Zip. Лицензия на использование и распространение]. Свободное программное обеспечение, бессрочное, с неограниченным кол-вом лицензий, правообладатель – Igor Pavlov. 5. Лицензия. Программа FreeCommander, бесплатная, свободного использования, бессрочная, правообладатель – Marek Jasinski. 6. Mozilla Firefox – бесплатная программа на условиях Публичной лицензии, бессрочной для неограниченного количества пользователей, разработчики – участники проекта mozilla.org.