Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Кубанский государственный университет»

Факультет романо-германской филологии

УТВЕРЖДАЮ:
Проректор по учебной работе,
качеству образования – первый
проректор
_____Хагуров Т. А.

30 мая 2025 года

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ФТД.02 Информационная безопасность

Направление подготовки/специальность	45.03.02 Лингвистика
Направленность (профиль)/специализация	Переводоведение
Форма обучения	Очная
Квалификация (степень) выпускника	Бакалавр

Краснодар 2025

Рабочая программа дисциплины ФТД.02 «Информационная безопасность» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 45.03.02 Лингвистика (Профиль Переводоведение) для очной формы обучения

Программу составил:

О.В. Назарова, канд. пед. наук, доцент

Рабочая программа дисциплины «Информационная безопасность» утверждена на заседании кафедры информационных образовательных технологий (ИОТ) протокол № 14 от «13» мая 2025 г.

Заведующий кафедрой ИОТ Грушевский С.П.

Утверждена на заседании учебно-методической комиссии факультета математики и компьютерных наук протокол № 4 от «14» мая 2025 г.

Председатель УМК ФМиКН Шмалько С.П.

Рецензенты:

Добровольская Н.Ю., канд. пед. наук, доцент, доцент кафедры информационных технологий ФКТиПМ КубГУ

Барсукова В.Ю., канд. физ.-мат. наук, доцент, зав. кафедрой функционального анализа и алгебры ФМиКН КубГУ

1. **Цели и задачи дисциплины**

1.1 Цель изучения дисциплины

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 основных направлений обеспечения информационной безопасности, меры законодательного, административного, процедурного и программно-технического уровней при работе на вычислительной технике и в каналах связи;
- приобретение теоретических и практических навыков по использованию современных методов защиты информации в компьютерных системах;
- изучение способов 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;
- развитие навыков информационной культуры будущего бакалавра, необходимые для дальнейшего самообучения в условиях непрерывного развития и совершенствования информационных технологий.

1.3. Место дисциплины в структуре ООП ВО

Дисциплина «Информационная безопасность» относится к части «Факультативы» дисциплин учебного плана. В соответствии с рабочим учебным планом дисциплина изучается на 4 курсе очной формы обучения. Вид промежуточной аттестации: зачет.

Дисциплины, необходимые для освоения данной дисциплины.

Слушатели должны владеть математическими знаниями в рамках программы средней школы, а также знаниями в области педагогики, психологии, информатики.

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

Изучение данной учебной дисциплины направлено на формирование у обучающихся компетенций

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине

ОПК-7 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	
ИОПК-7.3. Знает принципы работы современных цифровых технологий, возможность их применения для цифровой безопасности, потенциальные риски и способы их нейтрализации	Демонстрирует базовые знания современных цифровых технологий, в том числе систем искусственного интеллекта
	Применяет имеющиеся знания для обеспечения информационной безопасности ИС для образовательных организаций

Результаты обучения по дисциплине достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.

Индикаторы достижения компетенций считаются сформированными при достижении соответствующих им результатов обучения.

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 2 зач.ед. (72 часа), их распределение по видам работ представлено в таблице ***(для студентов очной формы)***

Вид учебной работы		Всего часов	Семестры (часы)
			6
Контактная работа, в том числе:		**38,2**	**38,2**
Аудиторные занятия (всего):		**36**	**36**
Занятия лекционного типа		18	18
Лабораторные занятия			
Занятия семинарского типа (семинары, практические занятия)		18	18
Иная контактная работа:		**2,2**	**2,2**
Контроль самостоятельной работы (КСР)		2	2
Промежуточная аттестация (ИКР)		0,2	0,2
Самостоятельная работа, в том числе:		**33,8**	**33,8**
Подготовка к занятиям		33,8	33,8
Контроль:			
Подготовка к экзамену			
Общая трудоемкость	**час.**	**72**	**75**
	в том числе контактная работа	**22,2**	**22,2**
	зач. ед	**2**	**2**

2.2 Содержание дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 6 семестре ***(для студентов очной формы).***

№ раздела	Наименование разделов (темы)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Нормативно-правовые документы в сфере информационной безопасности преподавателя в российском и мировом сообществе	8	2	2		4
2.	Государственная и индивидуальная защита информации	8	2	2		4
3.	Программные средства защиты информации	8	2	2		4
4.	Аппаратные средства защиты информации	8	2	2		4
5.	Информационная безопасность в социальных сетях	8	2	2		4
6.	Методы и технологии борьбы с компьютерными вирусами	8	2	2		4
7.	Информационная война и информационный терроризм	8	2	2		4
8.	Биометрия	8	2	2		4
9.	Структура плана защиты информации организации	5,8	2	2		1,8
	ИТОГО по разделам дисциплины	69,8				
	Контроль самостоятельной работы (КСР)	2				
	Промежуточная аттестация (ИКР)	0,2				
	Подготовка к текущему контролю					
	Общая трудоемкость по дисциплине	72				

2.3 Содержание разделов дисциплины

Занятия лекционного типа

(для студентов очной формы)

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
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	Тесты для актуализации и проверки знаний, собеседование, онлайн-опрос
2.	Государственная и индивидуальная защита информации	Уровни информационной безопасности. Безопасность в Интернет	Тесты для актуализации и проверки знаний, собеседование, онлайн-опрос
3.	Программные средства защиты информации	Классификация программных аппаратных средств защиты информации, изучение их характеристик	Тесты для актуализации и проверки знаний, собеседование, онлайн-опрос
4.	Аппаратные средства защиты информации	Классификация аппаратных аппаратных средств защиты информации, изучение их характеристик. Составление плана защиты информации организации, оценка видов угроз ОО.	Тесты для актуализации и проверки знаний, собеседование, онлайн-опрос
5.	Информационная безопасность в социальных сетях	Изучение основных понятий сетевого этикета. Правила поведения в сети Интернет.	Тесты для актуализации и проверки знаний, собеседование, онлайн-опрос
6.	Методы и технологии борьбы с компьютерными вирусами	Изучение методов обнаружения и технологий борьбы с компьютерными вирусами	Тесты для актуализации и проверки знаний, собеседование, онлайн-опрос

7.	Информационная война и информационный терроризм	Изучение способов защиты от информационных атак и информационного терроризма	Тесты для актуализации и проверки знаний, собеседование, онлайн-опрос
8.	Биометрия	Изучение биометрических характеристик. Правовые аспекты применения биометрических технологий	Тесты для актуализации и проверки знаний, собеседование, онлайн-опрос
9.	Структура плана защиты информации организации	Этапы создания плана защиты информации. Структура плана защиты информации организации	Тесты для актуализации и проверки знаний, собеседование, онлайн-опрос

Практические работы (*для студентов очной формы)*

№	Наименование раздела	Тематика практических работ	Форма текущего контроля
1	2	3	4
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	Проверка домашней самостоятельной работы. Опрос. Контрольные тесты
2.	Государственная и индивидуальная защита информации	Уровни информационной безопасности. Безопасность в Интернет	Проверка домашней самостоятельной работы. Опрос. Контрольные тесты
3.	Программные аппаратные средства защиты информации	Классификация программных аппаратных средств защиты информации, изучение их характеристик	Проверка домашней самостоятельной работы. Опрос. Контрольные тесты
4.	Аппаратные средства защиты информации	Классификация аппаратных аппаратных средств защиты информации, изучение их характеристик. Составление плана	Проверка домашней самостоятельной работы. Опрос.

		защиты информации организации, оценка видов угроз ОО.	Контрольные тесты
5.	Информационная безопасность в социальных сетях	Изучение основных понятий сетевого этикета. Правила поведения в сети Интернет.	Проверка домашней самостоятельной работы. Опрос. Контрольные тесты
6.	Методы и технологии борьбы с компьютерными вирусами	Изучение методов обнаружения и технологий борьбы с компьютерными вирусами	Проверка домашней самостоятельной работы. Опрос. Контрольные тесты
7.	Информационная война и информационный терроризм	Изучение способов защиты от информационных атак и информационного терроризма	Проверка домашней самостоятельной работы. Опрос. Контрольные тесты
8.	Биометрия	Изучение биометрических характеристик. Правовые аспекты применения биометрических технологий	Проверка домашней самостоятельной работы. Опрос. Контрольные тесты
9.	Структура плана защиты информации организации	Составление плана защиты информации организации, оценка видов угроз	Проверка домашней самостоятельной работы. Опрос. Контрольные тесты

При изучении дисциплины могут применятся электронное обучение, дистанционные образовательные технологии в соответствии с ФГОС ВО.

Лабораторные работы

Лабораторные работы – не предусмотрены.

2.3.1 Примерная тематика курсовых работ

Курсовые работы – не предусмотрены.

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

№	Наименование раздела	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1.	Занятия лекционные и практические	1. Петров, С. В. Обеспечение безопасности образовательной организации : учебное пособие для вузов / С. В. Петров, П. А. Кисляков. — 3-е изд., испр. и доп. — Москва : Издательство Юрайт, 2024. — 189 с. — (Высшее образование). — ISBN 978-5534-14077-4. — Текст : электронный // Образовательная
		платформа Юрайт [сайт]. — URL: https://www.urait.ru/bcode/538236 (дата обращения: 30.05.2024). 2. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://www.urait.ru/bcode/544029 (дата обращения: 30.05.2024). 3. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://www.urait.ru/bcode/544290 (дата обращения: 30.05.2024).
2.	Выполнение самостоятельной работы обучающихся	1. Козырь, Н. С. Гуманитарные аспекты информационной безопасности : учебное пособие для вузов / Н. С. Козырь, Н. В. Седых. — Москва : Издательство Юрайт, 2024. — 170 с. — (Высшее образование). — ISBN 978-5-534-17153-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://www.urait.ru/bcode/544965 (дата обращения: 30.05.2024). 2. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2024. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://www.urait.ru/bcode/543351 (дата обращения: 30.05.2024). 3. Психологическая безопасность личности : учебник и практикум для вузов / А. И. Донцов, Ю. П. Зинченко, О. Ю. Зотова, Е. Б. Перелыгина. — Москва : Издательство Юрайт,

		2024. — 222 с. — (Высшее образование). — ISBN 978-5-53409996-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://www.urait.ru/bcode/541853 (дата обращения: 30.05.2024).

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 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.

3. Образовательные технологии

В ходе изучения дисциплины предусмотрено использование следующих образовательных технологий: лекции, лабораторные работы, проблемное обучение, модульная технология, подготовка письменных аналитических работ, самостоятельная работа студентов.

Компетентностный подход в рамках преподавания дисциплины реализуется в использовании интерактивных технологий и активных методов (проектных методик, разбора конкретных ситуаций, анализа педагогических задач, педагогического эксперимента, иных форм) в сочетании с внеаудиторной работой.

Информационные технологии, применяемые при изучении дисциплины: использование информационных ресурсов, доступных в информационно телекоммуникационной сети Интернет.

Адаптивные образовательные технологии, применяемые при изучении дисциплины – для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «Информационная безопасность».

Оценочные средства включает контрольные материалы для проведения **текущего контроля** в форме тестовых заданий, доклада-презентации по проблемным вопросам, разноуровневых заданий и **промежуточной аттестации** в форме вопросов и заданий к экзамену.

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-7.3. Знание современных цифровых технологий, возможность их применения для цифровой безопасности, потенциальные риски и способы их нейтрализации	Демонстрирует базовые знания современных цифровых технологий, в том числе систем искусственного интеллекта Применяет имеющиеся знания для обеспечения информационной безопасности ИС для образовательных организаций	Проверочные тесты, лабораторные работы, долговременная СРС	Вопросы на зачете

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

Вопросы для зачета

1. Необходимость защиты информации
2. Сохранность защищаемой информации: сущность и основные виды. Сущность понятия "защищаемая информация"
3. Разновидность защищаемой информации и ее носителей.
4. Компьютерные вирусы и их классификация

5. Характеристика антивирусного программного обеспечения
6. Способы ограничение доступа к информации
7. Методы взлома компьютерных систем. Атаки на уровне систем управления базами данных
8. Методы взлома компьютерных систем. Атаки на уровне операционной системы
9. Методы взлома компьютерных систем. Атаки на уровне сетевого программного обеспечения.
10. Методы взлома компьютерных систем. Защита системы от взлома.
11. Характеристика троянских программ. Возникновение троянских программ.
12. Характеристика троянских программ. Распознавание троянской программы.
13. Программные закладки и их классификация
14. Модели воздействия программных закладок на компьютеры
15. Защита системы от программных закладок. Разновидность ПЗ (имитаторы, фильтры и заместители).
16. Парольные взломщики. Защита системы от клавиатурных шпионов. Парольная защита операционных систем.
17. Взлом парольной защиты ОС UNIX
18. Взлом парольной защиты ОС Windows/Linux
19. Информационная безопасность компьютерной сети. Характеристика и назначение сканеров.
20. Информационная безопасность компьютерной сети. Защита от анализаторов протоколов.
21. Значение и современные методы шифрования информации в информационном обществе
22. Методологические основы технологии шифрования программными средствами.
23. Применение и проблемы стандартизации криптографических алгоритмов. 23. Средства безопасности ОС Windows/Linux. Понятия и термины защиты данных. Характеристики безопасности.
24. Средства безопасности ОС Windows/Linux. Применение шифрования с открытым и закрытым ключами.
25. Средства безопасности ОС Windows/Linux. Протокол аутентификации Kerberos. Основы применения протокола Kerberos.

26. Средства безопасности ОС Windows/Linux. Характеристика протоколов обмена сообщениями.
27. Аутентификация протокола Kerberos в доменах ОС Windows/Linux.
28. Средства безопасности ОС Windows/Linux. Применение EPS в ОС Windows/Linux.
29. Средства безопасности ОС Windows/Linux. Шифрование файлов и каталогов. Копирование, перемещение, переименование и уничтожение зашифрованных файлов и папок.
30. Средства безопасности ОС Windows/Linux. Архивация и восстановление зашифрованных файлов на другом компьютере
31. Средства безопасности ОС Windows/Linux. Восстановление данных, зашифрованных с помощью неизвестного личного ключа.
32. Протокол безопасности IP в ОС Windows/Linux. Характеристика средств безопасности протокола IP.
33. Архитектура протокола безопасности IP в ОС Windows/Linux.
34. Администрирование безопасности в ОС Windows/Linux.
35. Использование сертификатов для обеспечения безопасности в ОС Windows/Linux. Хранилища сертификатов безопасности.
36. Планирование мероприятий по защите информации
37. Применение средства криптографической защиты информации Pretty good Privacy (PGP).

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.

Критерии оценивания результатов обучения

Оценка	Критерии оценивания по зачету
Высокий уровень (зачтено)	заслуживает студент, освоивший знания, умения, компетенции и теоретический материал без пробелов; выполнивший все задания, предусмотренные учебным планом на высоком качественном уровне; практические навыки профессионального применения освоенных знаний сформированы.
Средний уровень (зачтено)	заслуживает студент, практически полностью освоивший знания, умения, компетенции и теоретический материал, учебные задания не оценены максимальным числом баллов, в основном сформировал практические навыки.
Пороговый уровень (зачтено)	заслуживает студент, частично с пробелами освоивший 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.
Минимальный уровень (не зачтено)	заслуживает студент, не освоивший знания, умения, компетенции и теоретический материал, учебные задания не выполнил, практические навыки не сформированы.

5. Перечень учебной литературы, информационных ресурсов и технологий

5.1 Учебная литература

Основная литература

1. Петров, С. В. Обеспечение безопасности образовательной организации: учебное пособие для вузов / С. В. Петров, П. А. Кисляков. — 3-е изд., испр. и доп. — Москва : Издательство Юрайт, 2024. — 189 с. — (Высшее образование). — ISBN

978-5-534-14077-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://www.urait.ru/bcode/538236 (дата обращения: 30.05.2024).

2. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://www.urait.ru/bcode/544029 (дата обращения: 30.05.2024).
3. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 107 с. — (Высшее образование). — ISBN 978-5-53416388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://www.urait.ru/bcode/544290 (дата обращения: 30.05.2024).

Дополнительная литература

1. Козырь, Н. С. Гуманитарные аспекты информационной безопасности : учебное пособие для вузов / Н. С. Козырь, Н. В. Седых. — Москва : Издательство Юрайт, 2024. — 170 с. — (Высшее образование). — ISBN 978-5-534-17153-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://www.urait.ru/bcode/544965 (дата обращения: 30.05.2024).
2. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2024. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://www.urait.ru/bcode/543351 (дата обращения: 30.05.2024).
3. Психологическая безопасность личности : учебник и практикум для вузов / А. И. Донцов, Ю. П. Зинченко, О. Ю. Зотова, Е. Б. Перелыгина. — Москва : Издательство Юрайт, 2024. — 222 с. — (Высшее образование). — ISBN 978-5-534-09996-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://www.urait.ru/bcode/541853 (дата обращения: 30.05.2024).

5.2. Периодическая литература

5.3. Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы Электронно-библиотечные системы (ЭБС):

1. ЭБС «ЮРАЙТ» https://urait.ru/
2. ЭБС «УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА ОНЛАЙН» www.biblioclub.ru
3. ЭБС «BOOK.ru» https://www.book.ru
4. ЭБС «ZNANIUM.COM» www.znanium.com
5. ЭБС «ЛАНЬ» https://e.lanbook.com

Профессиональные базы данных:

1. Журналы издательства Wiley https://onlinelibrary.wiley.com/
2. Научная электронная библиотека (НЭБ) http://www.elibrary.ru/
3. Полнотекстовые архивы ведущих западных научных журналов на Российской платформе научных журналов НЭИКОН http://archive.neicon.ru
4. Национальная электронная библиотека (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ) https://rusneb.ru/
5. Президентская библиотека им. Б.Н. Ельцина https://www.prlib.ru/
6. "Лекториум ТВ" http://www.lektorium.tv/
7. Университетская информационная система РОССИЯ http://uisrussia.msu.ru

Информационные справочные системы:

1. Консультант Плюс - справочная правовая система (доступ по локальной сети с компьютеров библиотеки)

Ресурсы свободного доступа:

1. КиберЛенинка (http://cyberleninka.ru/);
2. Министерство науки и высшего образования Российской Федерации https://www.minobrnauki.gov.ru/;
3. Федеральный портал "Российское образование" http://www.edu.ru/;
4. Информационная система "Единое окно доступа к образовательным ресурсам" http://window.edu.ru/;
5. Единая коллекция цифровых образовательных ресурсов http://schoolcollection.edu.ru/ .
6. Федеральный центр информационно-образовательных ресурсов (http://fcior.edu.ru/);

7. Проект Государственного института русского языка имени А.С. Пушкина "Об- разование на русском" https://pushkininstitute.ru/;

8. Справочно-информационный портал "Русский язык" http://gramota.ru/;

9. Служба тематических толковых словарей http://www.glossary.ru/;

10. Словари и энциклопедии http://dic.academic.ru/;

11. Образовательный портал "Учеба" http://www.ucheba.com/;

12. Законопроект "Об образовании в Российской Федерации". Вопросы и ответы http://xn--273--84d1f.xn--p1ai/voprosy_i_otvety

Собственные электронные образовательные и информационные ресурсы КубГУ:

1. Среда модульного динамического обучения http://moodle.kubsu.ru

2. База учебных планов, учебно-методических комплексов, публикаций и конференций http://mschool.kubsu.ru/

3. Библиотека информационных ресурсов кафедры информационных образовательных технологий http://mschool.kubsu.ru;

4. Электронный архив документов КубГУ http://docspace.kubsu.ru/

5. Электронные образовательные ресурсы кафедры информационных систем и технологий в образовании КубГУ и научно-методического журнала "ШКОЛЬНЫЕ ГОДЫ" http://icdau.kubsu.ru/

6. Методические указания для обучающихся по освоению дисциплины

Лекционные занятия проводятся по основным разделам дисциплины «Информационная безопасность». Они дополняются лабораторными 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. После изучения определенных разделов проводится аттестация в форме теста. Тесты оцениваются в баллах, сумма которых дает рейтинг каждого обучающегося. В баллах оцениваются не только знания и навыки обучающихся, но и их творческие возможности: активность, неординарность решений поставленных проблем, умение сформулировать и решить научную проблему.

Самостоятельная работа студентов предполагает систематический характер. Студентам рекомендуется чтение после прослушивания лекций соответствующих разделов

тех или иных учебников. Выполнение домашних заданий, домашних контрольных работ и индивидуальных работ.

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.

7. Материально-техническое обеспечение по дисциплине (модулю)

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

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.

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	Лекционные занятия	Лекционная аудитория, оснащенная презентационной техникой (интерактивная доска, компьютер/ноутбук) и соответствующим программным обеспечением (ПО) Power Point 303н
2.	Практические занятия	Компьютерный класс с необходимым программным обеспечение, локальной сетью и выходом в Интернет для проведения лабораторных работ 301н, 114н

3.	Групповые (индивидуальные) консультации	Аудитория, консультации в дистанционной форме 301н, 302н, 303н, 308н, 309н, 316н, 318н, 320н
4.	Текущий контроль, промежуточная аттестация	Аудитория 301н, 302н, 303н, 308н, 309н, 316н, 320н
5.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», обеспеченный доступом в электронную информационно-образовательную среду университета 301н, 302н, 303н, 308н, 309н, 316н, 320н