Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кубанский государственный университет»
Институт географии, геологии, туризма и сервиса

УТВЕРЖДАЮ
Проректор по учебной работе,
качеству образования – первый
проректор
_____Хагуров Т.А.
подпись
«_____» _____2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.01 ИФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(код и наименование дисциплины в соответствии с учебным планом)

Направление подготовки *44.03.05 Педагогическое образование (с двумя профилями подготовки)*

(код и наименование направления подготовки/специальности)

Направленность (профиль) *География и Безопасность жизнедеятельности*

(наименование направленности (профиля))

Программа подготовки *Академическая*

(академическая / прикладная)

Форма обучения *Очная*

(очная, очно-заочная, заочная)

Квалификация (степень) выпускника *Бакалавр*

(бакалавр, магистр, специалист)

Краснодар 2018

Рабочая программа дисциплины «Информационная безопасность» составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки (профилю) 44.03.05 Педагогическое образование (с двумя профилями подготовки), академический бакалавриат.

Программу составили:
ст. преподаватель каф. геоинформатики
ФГБОУ ВО «КубГУ». С. Зырянова С.В. Зырянова

Заведующий кафедрой (разработчика) А.В. Погорелов

«2» марта 2018 г.

Рабочая программа дисциплины утверждена на заседании кафедры экономической, социальной и политической географии
протокол № 8 от «9» апреля 2018 г.
Заведующий кафедрой (выпускающей) _____ В.В. Миненкова

Рабочая программа дисциплины утверждена на заседании кафедры физической географии
протокол № 10 от «24» апреля 2018 г.
Заведующий кафедрой (выпускающей) _____ Ю.Я. Нагалевский

Рабочая программа дисциплины утверждена на заседании кафедры геоинформатики
протокол
№9 от «2» марта 2018 г.
Заведующий кафедрой (разработчика) _____ А.В. Погорелов

Утверждена на заседании учебно-методической комиссии факультета

«25» апреля 2018 г., протокол № 04-18.

Председатель УМК ИГГТиС А.В. Погорелов

Эксперт(ы):

1. Еремин А.А. к.ф.-м.н., научный сотрудник ИММИ ФГБОУ ВО «КубГУ»

2. Шестернин В.В., канд. геогр. наук, директор ООО "КУМЦ "Транспортная безопасность"

1 Цели и задачи изучения дисциплины

1.1 Цель дисциплины – знакомство бакалавров с тенденцией развития информационной безопасности, с моделями возможных угроз, терминологией и основными понятиями теории безопасности информации, а также с нормативными документами России по данному вопросу и правилами получения соответствующих лицензий.

1.2 Задачи дисциплины:

– получение студентами знаний по существующим угрозам безопасности информации, подбору и применению современных методов и способов защиты информации;

– формирование навыков, необходимых студентам для защиты информации, в том числе при администрировании локальных сетей.

1.3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Информационная безопасность» является дисциплиной по выбору вариативной части блока 1 дисциплин. Она дает понятие об основных тенденциях развития информационной безопасности.

Она частично опирается на знания, полученные в курсе «Безопасность жизнедеятельности» и «Информационные технологии в образовании».

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

Изучение учебной дисциплины «Интернет и информационные ресурсы» направлено на формирование у обучающихся следующих профессиональных компетенций

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1.	ОПК-4	готовностью к профессиональной деятельности в соответствии с нормативными правовыми актами в сфере образования	законодательные нормы взаимодействия участников образовательного процесса особенности взаимодействия с различными участниками и партнерами в условиях образовательного процесса, социальные и культурные требования к взаимодействию участников	ориентироваться на законодательные нормы в условиях взаимодействия участников образовательного процесса использовать на законодательные нормы в условиях взаимодействия участников образовательного процесса толерантно воспринимать социальные, этноконфессиональные и культурные различия, сохраняя нормативно-правовые	навыками построения нормативноправовой основы во взаимодействии участников образовательного процесса навыками построения нормативноправовой основы во взаимодействии социальных партнеров создавать и поддерживать нормативноправовое поле в условиях

			образовательного процесса.	основы во взаимодействии	взаимодействия участников образовательного процесса
2.	ПК-9	способностью проектировать индивидуальные образовательные маршруты обучающихся	теоретические основы проектирования индивидуальных образовательных маршрутов обучающихся.	проводить анализ индивидуальных образовательных потребностей личности; проектировать индивидуальные образовательные маршруты обучающихся.	различными приемами, методами, технологиями проектирования индивидуальных образовательных маршрутов обучающихся;

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

2 зачетных единицы (72 часов, из них – 36 часов аудиторной нагрузки: практических 36 ч.; контролируемая самостоятельная работа – 2 ч.; промежуточная аттестация (ИКР) – 0,2 ч.; 33,8 часов самостоятельной работы).

Общая трудоёмкость дисциплины составляет 2 зач.ед. (72 часов), их распределение по видам работ представлено в таблице 1 *(для студентов ОФО).*

Таблица 1 – Распределение трудоемкости дисциплины по видам работ

Вид учебной работы		Всего часов	Семестры
			4
Контактная работа, в том числе:		38,2	38,2
Аудиторные занятия (всего):		36	36
Занятия лекционного типа		-	-
Лабораторные занятия		-	-
Занятия семинарского типа (семинары, практические занятия)		36	36
Иная контактная работа:			
Контроль самостоятельной работы (КСР)		2	2
Промежуточная аттестация (ИКР)		0,2	0,2
Самостоятельная работа (всего):		33,8	33,8
Курсовая работа		-	-
Проработка учебного (теоретического) материала		10	10
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		20	20
Реферат		-	-
Подготовка к текущему контролю		3,8	3,8
Контроль:			
Подготовка к зачету		-	-
Общая трудоемкость	**час.**	72	72
	в том числе контактная работа	2,2	2,2
	зач. ед	2	2

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.
Разделы дисциплины, изучаемые в 4 семестре *(для студентов ОФО)*

№ раздела	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Самостоятельная работа
			Л	ПЗ	ЛР	
1	2	3	4	5	6	7
1.	Актуальность информационной безопасности в современных условиях.	4		2		2
2.	Понятие угрозы. Понятия о видах вирусов. Защита от «компьютерных вирусов.	16		8		8
3.	Современные методы защиты информации. Модели безопасности и их применение. Методы криптографии.	16		8		8
4.	Лицензирование и сертификация в ИБ.	8		4		4
5.	Концепция безопасности реляционных БД. Модели и механизмы обеспечения безопасности в СУБД. Критерии безопасности компьютерных систем «Оранжевая книга»	18		10		8
6.	Руководящие документы Гостехкомиссии	7,8		4		3,8
	Всего:			36		33,8

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа

Лекционные занятия – не предусмотрены.

2.3.2 Занятия семинарского типа

№	Наименование раздела	Тематика практических занятий (семинаров)	Форма текущего контроля
1	2	3	4
1.	Актуальность информационной безопасности в современных условиях.	Задачи и содержание курса, порядок его изучения. Материально-техническая и учебно-методическая база. Современное состояние защиты информации. Международные стандарты информационного обмена. Получение статистических знаний об атаках, которым подвергаются компьютерные системы и потерях банков. Изучение основных понятий и определений, используемых при изучении дисциплины	У

2.	Понятие угрозы. Понятия о видах вирусов. Защита от «компьютерных вирусов.	Понятие угрозы. Получение знаний о видах угроз, путей и каналов утечки информации, от кого они исходят и к чему приводят. Изучение видов атак и методов взлома интрасетей злоумышленниками. Три вида возможных нарушений информационной системы. Виды противников или «нарушителей». Информационная безопасность в условиях функционирования в России глобальных сетей. Понятия о видах вирусов. Получение знаний о существующих "компьютерных вирусах". Классификация "компьютерных вирусов". Угроза вирусов безопасности информации. Алгоритмы работы "компьютерных вирусов" и пути их внедрения в систему. Индивидуальные признаки, используемые для определения "ко Основные правила защиты от "компьютерных вирусов". Обзор антивирусных программ. Методика использования антивирусных программ. Восстановление пораженных "компьютерными вирусами" объектов.мпьютерных вирусов" различных классов.	У, ПР
3.	Современные методы защиты информации. Модели безопасности и их применение. Методы криптографии.	Рассматриваются методы защиты информации: ограничение доступа, разграничение доступа, разделение доступа, криптографическоепреобразование информации, контроль и учет доступа, законодательные меры, обеспечение информационной безопасности в Internet. Основные технологии построения защищенных ИС. Место информационной безопасности в национальной безопасности страны. Концепция информационной безопасности. Дискреционная и мандатная модели политики безопасности. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Традиционные и современные криптосистемы. Методы шифрования данных. Основные криптографические алгоритмы. Абонентское и пакетное шифрование. Взаимное подтверждение подлинности (аутентификация) абонентов и объектов сети. Обеспечение целостности информации на основе электронной цифровой подписи.	У, ПР
4.	Лицензирование и сертификация в ИБ.	Нормы и требования российского законодательства в области лицензирования и сертификации. Правила построения и функционирования системы лицензирования ФАПСИ. Порядок оформления и получения лицензий и сертификатов в области информационной безопасности. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.	У

5.	Концепция безопасности реляционных БД. Модели и механизмы обеспечения безопасности в СУБД. Критерии безопасности компьютерных систем «Оранжевая книга»	Угрозы безопасности БД: общие и специфические. Требования безопасности БД. Защита от несанкционированного доступа (НСД). Защита от вывода. Целостность БД. Аудит. Задачи и средства администратора безопасности баз данных. Многоуровневая защита. Классификация моделей. Особенности применения моделей безопасности в СУБД Oracle и DB2. Механизмы обеспечения целостности СУБД. Метаданные и словарь данных. Доступ к словарю данных. Транзакции как средство изолированности пользователей. Правила согласования блокировок. Тупиковые ситуации, их распознавание и разрушение. Способы поддержания ссылочной целостности. Механизмы правил и событий. Механизмы обеспечения конфиденциальности в СУБД. Причины, виды, основные методы нарушения конфиденциальности. Получение несанкционированного доступа к конфиденциальной информации путем логических выводов. Методы защиты информации. Особенности применения криптографических методов. Средства идентификации и аутентификации. Средства управления доступом. Аудит и подотчетность. Рассмотрение критериев, с помощью которых оценивается защищенность вычислительных систем. Ознакомление со стандартом США "Оранжевая книга".	ПР
6.	Руководящие документы Гостехкомиссии	Изучение руководящих документов Гостехкомиссии Российской Федерации.	У

Примечание: У – устный опрос
КР – контрольная работа
ПР – практическая (расчетно-графическая) работа
Р – реферат

2.3.3 Лабораторные занятия

Лабораторные занятия – не предусмотрены.

2.3.4 Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) 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.	Актуальность информационной безопасности в современных условиях.	1. Написание и оформление рефератов. Учебно-методические указания по направлению подготовки 05.03.03 «Картография и геоинформатика», утвержденные на заседании кафедры геоинформатики протокол №10 от 2.06.2017 г.

		2. Составление презентаций. Методические указания по направлению подготовки 05.03.03 «Картография и геоинформатика» протокол №10 от 2.06.2017 г
2.	Понятие угрозы. Понятия о видах вирусов. Защита от «компьютерных вирусов.	1. Написание и оформление рефератов. Учебно-методические указания по направлению подготовки 05.03.03 «Картография и геоинформатика», утвержденные на заседании кафедры геоинформатики протокол №10 от 2.06.2017 г. 2. Составление презентаций. Методические указания по направлению подготовки 05.03.03 «Картография и геоинформатика» протокол №10 от 2.06.2017 г
3.	Современные методы защиты информации. Модели безопасности и их применение. Методы криптографии.	1. Написание и оформление рефератов. Учебно-методические указания по направлению подготовки 05.03.03 «Картография и геоинформатика», утвержденные на заседании кафедры геоинформатики протокол №10 от 2.06.2017 г. 2. Составление презентаций. Методические указания по направлению подготовки 05.03.03 «Картография и геоинформатика» протокол №10 от 2.06.2017 г
4.	Лицензирование и сертификация в ИБ.	1. Написание и оформление рефератов. Учебно-методические указания по направлению подготовки 05.03.03 «Картография и геоинформатика», утвержденные на заседании кафедры геоинформатики протокол №10 от 2.06.2017 г. 2. Составление презентаций. Методические указания по направлению подготовки 05.03.03 «Картография и геоинформатика» протокол №10 от 2.06.2017 г
5.	Концепция безопасности реляционных БД. Модели и механизмы обеспечения безопасности в СУБД. Критерии безопасности компьютерных систем «Оранжевая книга»	1. Написание и оформление рефератов. Учебно-методические указания по направлению подготовки 05.03.03 «Картография и геоинформатика», утвержденные на заседании кафедры геоинформатики протокол №10 от 2.06.2017 г. 2. Составление презентаций. Методические указания по направлению подготовки 05.03.03 «Картография и геоинформатика» протокол №10 от 2.06.2017 г
6.	Руководящие документы Гостехкомиссии	тоже

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,

– в форме аудиофайла,

– в печатной форме на языке Брайля.

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,

– в форме аудиофайла.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3. Образовательные технологии

В процессе преподавания дисциплины «Информационная безопасность» применяются следующие виды образовательных технологий:

– традиционные (практическое занятие);

– проблемного обучения (проблемная лекция, практическое занятие в форме практикума, практическое занятие на основе кейс-метода;

– проектного обучения (исследовательский проект, информационный проект);

– интерактивные (лекции «обратной связи» – лекция-провокация (изложение материала с заранее запланированными ошибками), лекциябеседа, лекция-дискуссия; семинары-дискуссии);

– информационно-коммуникационные (лекция-визуализация; практическое занятие в форме презентации – представление результатов проектной деятельности с использованием специализированных программных средств).

Удельный вес занятий, проводимых в интерактивных формах, приведён в таблице.

Семестр	Вид занятия (Л, ПР, ЛР)	Используемые интерактивные образовательные технологии	Количество часов
4	*ПР:* Актуальность информационной безопасности в современных условиях ПР: Классификация компьютерных вирусов и алгоритм их работы ПР: Анализ способов нарушений информационной безопасности ПР: Угрозы безопасности БД	Работа в малых группах, решение ситуационных задач с применением ПК	*2* *4* *4* *4*
Итого:			*14*
Л – лекция, ПР – практическая работа			

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

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 Фонд оценочных средств для проведения текущей аттестации

Текущий контроль осуществляется в ходе проведения практических занятий в виде устного опроса, выполнения практических работ. Перечень заданий к практическим занятиям приведен в фонде оценочных средств по дисциплине «Информационная безопасность».

4.2 Фонд оценочных средств для проведения промежуточной аттестации *Вопросы к зачету*

1. Актуальность и основные задачи защиты информации. Основные понятия информационной безопасности.
2. Асимметричные методы шифрования данных.
3. Основные угрозы безопасности данных и их классификация.
4. Симметричные методы шифрования данных.
5. Каналы утечки данных и их классификация.
6. Идентификация, аутентификация пользователей. Классификация методов идентификации пользователей.
7. Уязвимые места информационных систем.
8. Обеспечение доступности данных.
9. Основные методы защиты данных и их классификация.
10. Защита информации в системах управления базами данных.
11. Основные средства защиты данных и их классификация.
12. Основные подходы к оценке и принципы оценки безопасности ИТ, используемые в TCSEC, ITSEC, РД Гостехкомиссии России. Сходство и различия.
13. Формальные средства защиты информации.
14. Программно-технический аспект информационной безопасности.
15. Неформальные средства защиты информации.
16. Организационный аспект информационной безопасности.
17. Мероприятия по защите информации от несанкционированного доступа.
18. Управленческий аспект информационной безопасности.
19. Мероприятия по защите информации от потерь.

20. Законодательный аспект информационной безопасности.
21. Мероприятия по защите информации от вредоносных программ.
22. Вредоносные программы (вирусы) и их классификация.

Методические рекомендации для подготовки к зачету

Итоговым контролем уровня усвоения материала студентами является зачет. Зачет служит формой проверки качества усвоения студентами учебного материала практических занятий. Для эффективной подготовки к зачету процесс изучения материала курса предполагает достаточно интенсивную работу не только на занятиях, но и с различными текстами, нормативными документами и информационными ресурсами.

Особое внимание надо обратить на то, что подготовка к зачету требует обращения не только к учебникам, но и к информации, содержащейся в СМИ, а также в Интернете.

Критерии оценки ответа студента на зачете

Зачет является формой итоговой оценки качества освоения студентом образовательной программы по дисциплине. По результатам зачета студенту выставляется оценка «зачтено» или «не зачтено».

Зачет проводится в форме устного опроса с предварительной подготовкой студента в течении 15 минут. Каждый вопрос из тем изученных на практических занятиях, а также по вопросам тем для самостоятельной работы студентов. Экзаменатор вправе задавать дополнительные вопросы. Экзаменатор может проставить зачет без опроса и собеседования тем студентам, которые активно работали на практических (семинарских) занятиях.

Преподаватель принимает зачет только при наличии ведомости и надлежащим образом оформленной зачетной книжки. Результат зачета объявляется студенту непосредственно после его сдачи, затем выставляется в экзаменационную ведомость и зачетную книжку студента. Если в процессе зачета студент использовал недопустимые дополнительные материалы (шпаргалки), то экзаменатор имеет право изъять шпаргалку и поставить оценку «незачтено».

Основные средства защиты данных и их классификация

Оценка **«зачтено»** ставится студенту, ответ которого содержит глубокое знание материала курса, знание концептуально-понятийного аппарата всего курса, знание литературы по курсу или ответ которого демонстрирует знания материала по программе, содержит в целом правильное, но не всегда точное и аргументированное изложение материала.

Оценка **«не зачтено»** ставится студенту, имеющему существенные пробелы в знании основного материала по программе, допустившему принципиальные ошибки при изложении материала, а также не давшему ответа на вопрос.

Каналы утечки данных и их классификация

В процессе подготовки и проведения практических занятий студенты закрепляют полученные ранее теоретические знания, приобретают навыки их практического применения, опыт рациональной организации учебной работы, готовятся к сдаче зачета. Важной задачей является также развитие навыков самостоятельного изложения студентами своих мыслей по вопросам курса.

В начале семестра студенты получают сводную информацию о формах проведения занятий и формах контроля знаний. Тогда же студентам предоставляется список тем практических заданий.

Поскольку активность студента на практических занятиях является предметом внутрисеместрового контроля его продвижения в освоении курса, подготовка к таким занятиям требует от студента ответственного отношения.

При подготовке к занятию студенты в первую очередь должны использовать материал занятий и соответствующих литературных источников. Самоконтроль качества подготовки к

каждому занятию студенты осуществляют, проверяя свои знания и отвечая на вопросы для самопроверки по соответствующей теме.

Входной контроль осуществляется преподавателем в виде проверки и актуализации знаний студентов по соответствующей теме.

Выходной контроль осуществляется преподавателем проверкой качества и полноты выполнения задания.

Типовой план практических занятий:

1. Изложение преподавателем темы занятия, его целей и задач.
2. Выдача преподавателем задания студентам, необходимые пояснения.
3. Выполнение задания студентами под наблюдением преподавателя. Обсуждение результатов. Резюме преподавателя.
4. Общее подведение итогов занятия преподавателем и выдача домашнего задания.

Коллоквиум

Форма проверки и оценивания знаний учащихся в системе образования, представляет собой проводимый по инициативе преподавателя промежуточный контроль знаний по определенным разделам для оценки текущего уровня знаний студентов, а также для повышения знаний студентов.

Общие правила выполнения письменных работ

Академическая этика, соблюдение авторских прав. На первом занятии студенты должны быть проинформированы о необходимости соблюдения норм академической этики и авторских прав в ходе обучения. В частности, предоставляются сведения:

- общая информация об авторских правах;
- правила цитирования;
- правила оформления ссылок

Все имеющиеся в тексте сноски тщательно выверяются и снабжаются «адресами». Недопустимо включать в свою работу выдержки из работ других авторов без указания на это, пересказывать чужую работу близко к тексту без отсылки к ней, использовать чужие идеи без указания первоисточников (это касается и информации, найденной в Интернете). Все случаи плагиата должны быть исключены.

Список использованной литературы должен включать все источники информации, изученные и проработанные студентом в процессе выполнения работы, и должен быть составлен в соответствии с ГОСТ Р 7.0.5-2008 «Библиографическая ссылка. общие требования и правила».

Составление презентаций в Microsoft PowerPoint

Презентация дает возможность наглядно представить инновационные идеи, разработки и планы. Учебная презентация представляет собой результат самостоятельной работы студентов, с помощью которой они наглядно демонстрируют материалы публичного выступления перед аудиторией. Компьютерная презентация – это файл с необходимыми материалами, который состоит из последовательности слайдов. Каждый слайд содержит законченную по смыслу информацию, так как она не переносится на следующий слайд автоматически в отличие от текстового документа. Студенту – автору презентации, необходимо уметь распределять материал в пределах страницы и грамотно размещать отдельные объекты. В этом ему поможет целый набор готовых объектов (пиктограмм, геометрических фигур, текстовых окон и т.д.). Бесспорным достоинством презентации является возможность при необходимости быстро вернуться к любому из ранее просмотренных слайдов или буквально на ходу изменить последовательность изложения материала. Презентация помогает самому выступающему не забыть главное и точнее расставить акценты. Одной из основных программ для создания презентаций в мировой практике является программа PowerPoint компании Microsoft. Для визуального восприятия текст на слайдах презентации должен быть не менее 18 пт, а для заголовков – не менее 24 пт. Макет презентации должен быть оформлен в строгой цветовой гамме. Фон не должен быть слишком ярким или пестрым. Текст должен хорошо читаться. Одни и те же элементы на разных слайдах должен быть одного цвета. Пространство слайда (экрана) должно быть максимально

использовано, за счет, например, увеличения масштаба рисунка. Кроме того, по возможности необходимо занимать верхние площади слайда (экрана), поскольку нижняя часть экрана плохо просматривается с последних рядов. Каждый слайд должен содержать заголовок. В конце заголовков точка не ставится. В заголовках должен быть отражен вывод из представленной на слайде информации. Оформление заголовков заглавными буквами можно использовать только в случае их краткости. На слайде следует помещать не более 5-6 строк и не более 5-7 слов в предложении. Текст на слайдах должен хорошо читаться. При добавлении рисунков, схем, диаграмм, снимков экрана (скриншотов) необходимо проверить текст этих элементов на наличие ошибок. Необходимо проверять правильность написания названий улиц, фамилий авторов методик и т.д

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья имеются издания в электронном виде в электроннобиблиотечных системах

5.1 Основная литература:

1. Нестеров, С.А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / С.А. Нестеров. — Электрон. дан. — Санкт-Петербург : Лань, 2018. — 324 с. — Режим доступа: https://e.lanbook.com/book/103908. — Загл. с экрана.

5.2 Дополнительная литература:

1. Чусавитина, Г.Н. Подготовка будущих учителей к обеспечению информационной безопасности [Электронный ресурс] : монография / Г.Н. Чусавитина, Л.В. Курзаева, Л.З. Давлеткиреева, М.О. Чусавитин. — Электрон. дан. — Москва : ФЛИНТА, 2014. — 188 с. — Режим доступа: https://e.lanbook.com/book/70429. — Загл. с экрана.

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

https://e.lanbook.com

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

Самостоятельная работа студентов осуществляется в целях подготовки к практическим занятиям (согласно тематическому плану, см. ФОС) и к зачету (см. перечень вопросов к зачету).

В освоении дисциплины инвалидами и лицами с ограниченными возможностямиздоровья 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 доровья.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю) (при необходимости)

8.1. Перечень информационных технологий

Использование электронных презентаций при проведении занятий семинарского типа.

8.2. Перечень необходимого программного обеспечения

Для освоения учебной дисциплины «Информационная безопасность» в процессе обучения будут использоваться следующие ПО:

лицензионные программы общего назначения, такие как Microsoft Windows 7, пакет Microsoft Officce Professional (Word, Excel, PowerPoint,
Access), программы демонстрации видео материалов (Windows Media Player), программы для демонстрации и создания презентаций (Microsoft Power
Point).

8.3. Перечень необходимых информационных справочных систем

Каждый обучающийся обеспечен доступом к электронным библиотечным системам:

1. Электронная библиотечная система издательства “Лань” (www.e.lanbook.com)
2. Электронная библиотечная система “Университетская Библиотека онлайн” (www.biblioclub.ru)
3. Электронная библиотечная система “ZNANIUM.COM” (www.znanium.com)
4. Электронная библиотечная система eLIBRARY.RU (http://www.elibrary.ru)
5. Science Direct (Elsevir) (www.sciencedirect.com)
6. Scopus (www.scopus.com)
7. Единая интернет- библиотека лекций “Лекториум” (www.lektorium.tv)

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)

Для проведения занятий по дисциплине, предусмотренной учебным планом подготовки аспирантов, имеется необходимая материальнотехническая база, соответствующая действующим санитарным и противопожарным правилам и нормам:

№ п/п	Вид занятий	Наименование оборудованных учебных кабинетов для проведения занятий лекционного типа, практических занятий, лабораторных занятий, практик, помещений для самостоятельной работы	Фактический адрес учебных кабинетов (№ аудитории)
1	Практические занятия	Мультимедийная лаборатория с выходом в ИНТЕРНЕТ: 13 рабочих станций с графикой Aquarius EltE50S45 (Intel P-2800, 4 GB, HDD 256 GB) + монитор Aquarius TF1910W, 24 стула, 10 компьютерных столов, 1 стол для сервера	206