МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Красноярский государственный педагогический университет
им. В.П. Астафьева»

ПРЕДМЕТНАЯ ЧАСТЬ (ПО ПРОФИЛЮ ИНФОРМАТИКА)
Информационная безопасность и защита информации

рабочая программа дисциплины (модуля)

Квалификация **D8 Информатики и информационных технологий в образовании**

Форма обучения **очная**

44.03.05 Математика и информатика (о,2024).plx
44.03.05 Педагогическое образование (с двумя профилями подготовки)
Направленность (профиль): Математика и информатика
Выпускающая кафедра:
математики и методики обучения математике, информатики и информационных

Общая трудоемкость **2 ЗЕТ**

Часов по учебному плану 72
в том числе:
аудиторные занятия 38
самостоятельная работа 33,85
контактная работа во время промежуточной аттестации (ИКР) 0,15

Виды контроля в семестрах:
зачеты 10

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**10 (5.2)**		Итого	
Недель	10			
Вид занятий	УП	РП	УП	РП
Лекции	12	12	12	12
Лабораторные	26	26	26	26
Контактная работа (промежуточная аттестация) зачеты	0,15	0,15	0,15	0,15
В том числе в форме практ.подготовки	4	4	4	4
Итого ауд.	38	38	38	38
Контактная работа	38,15	38,15	38,15	38,15
Сам. работа	33,85	33,85	33,85	33,85
Итого	72	72	72	72

Программу составил(и):
кпн, Доцент, Ломаско Павел Сергеевич

Рабочая программа дисциплины
Информационная безопасность и защита информации

разработана в соответствии с ФГОС ВО:
Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки) (приказ Минобрнауки России от 22.02.2018 г. № 125)

составлена на основании учебного плана:
44.03.05 Педагогическое образование (с двумя профилями подготовки)
Направленность (профиль): Математика и информатика
Выпускающая кафедра:
математики и методики обучения математике; информатики и информационных технологий в образовании

Рабочая программа одобрена на заседании кафедры
D8 Информатики и информационных технологий в образовании

Протокол от 08.05.2024 г. № 9

Зав. кафедрой д-р пед. наук, проф. Пак Н.И.

Председатель НМСС(С) Аёшина Е.А.
Протокол от 15.05.2024 г. № 7

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
Формирование способности и готовности обучающихся к осуществлению учебной и будущей профессиональной деятельности с учетом рисков информационной безопасности и возможностей технологий защиты информации в контексте процессов интенсивной цифровизации сферы образования и с учетом реалий жизни в постиндустриальном обществе.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О.07.02
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Программное обеспечение систем и сетей
2.1.2	Информационные системы
2.1.3	Веб-технологии
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Выполнение и защита выпускной квалификационной работы
2.2.2	История информатики
2.2.3	Компьютерные технологии в принятии решений

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ПК-1: Способен осваивать и использовать теоретические знания и практические умения и навыки в предметной области при решении профессиональных задач	
ПК-1.1: Знает структуру, состав и дидактические единицы предметной области (преподаваемого предмета)	
Знать:	
Уровень 1	все виды угроз информационной безопасности
Уровень 2	основные виды угроз информационной безопасности
Уровень 3	некоторые виды угроз информационной безопасности
Уметь:	
Уровень 1	полностью самостоятельно оценивать степень риска и возможный ущерб при нарушении информационной безопасности на различных уровнях
Уровень 2	частично самостоятельно оценивать степень риска и возможный ущерб при нарушении информационной безопасности на различных уровнях
Уровень 3	только при посторонней помощи оценивать степень риска и возможный ущерб при нарушении информационной безопасности на различных уровнях
Владеть:	
Уровень 1	всеми методами минимизации рисков нарушения информационной безопасности на различных уровнях
Уровень 2	основными методами минимизации рисков нарушения информационной безопасности на различных уровнях
Уровень 3	некоторыми методами минимизации рисков нарушения информационной безопасности на различных уровнях
ПК-1.2: Умеет осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО	
Знать:	
Уровень 1	все темы и содержание, относящиеся к предметной области информационной безопасности и защиты информации
Уровень 2	основные темы и содержание, относящиеся к предметной области информационной безопасности и защиты информации
Уровень 3	некоторые темы и содержание, относящиеся к предметной области информационной безопасности и защиты информации
Уметь:	
Уровень 1	полностью самостоятельно осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО по направлению информационной безопасности и защиты информации
Уровень 2	в основном самостоятельно осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО по направлению информационной безопасности и защиты информации
Уровень 3	только при посторонней помощи осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО по направлению информационной безопасности и защиты информации
Владеть:	

Уровень 1	всеми методами и средствами моделирования и анализа ситуаций нарушения информационной безопасности и прогнозирования возможных (негативных) последствий, в том числе во время осуществления учебного процесса в качестве преподавателя
Уровень 2	основными методами и средствами моделирования и анализа ситуаций нарушения информационной безопасности и прогнозирования возможных (негативных) последствий, в том числе во время осуществления учебного процесса в качестве преподавателя
Уровень 3	некоторыми методами и средствами моделирования и анализа ситуаций нарушения информационной безопасности и прогнозирования возможных (негативных) последствий, в том числе во время осуществления учебного процесса в качестве преподавателя

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Интеракт.	Пр. подгот.	Примечание
	Раздел 1. Основные понятия информационной безопасности							
1.1	Введение. Цели, задачи, направления информационной безопасности. /Лек/	10	2	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3			Прохождение входного тестирования
1.2	Становление предметной области. Определения и эволюция понятия «информационная безопасность». /Лаб/	10	2	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3			Выполнение заданий лабораторной работы
1.3	Базовые принципы и уровни обеспечения информационной безопасности. /Лаб/	10	2	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3			Выполнение заданий лабораторной работы
1.4	Изучение литературы и дополнительных источников по теме /Ср/	10	6	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3			Выполнение контрольной работы по теме
	Раздел 2. Правовые основы информационной безопасности и защиты персональных данных							
2.1	Законодательство о безопасности и защите информации, его структура и содержание. ГОСТы. /Лек/	10	2	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3			Выполнение контрольной работы по теме
2.2	Виды правонарушений в области защиты информации. /Лаб/	10	2	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3			Выполнение заданий лабораторной работы
2.3	Авторское право и интеллектуальная собственность. /Лаб/	10	2	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3			Выполнение заданий лабораторной работы
2.4	Типовые ситуации в образовательных организациях, связанные с правовой защитой информации /Лаб/	10	2	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3		2	Выполнение заданий лабораторной работы

2.5	Изучение литературы и дополнительных источников по теме /Ср/	10	6	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3			Выполнение контрольной работы по теме
	Раздел 3. Программные средства защиты информации							
3.1	Программные средства защиты информации. /Лек/	10	2	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3			Выполнение контрольной работы по теме
3.2	Компьютерные вирусы и антивирусная защита. /Лаб/	10	2	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3			Выполнение заданий лабораторной работы
3.3	Идентификация и аутентификация. Разграничение доступа. /Лаб/	10	2	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3			Выполнение заданий лабораторной работы
3.4	Межсетевые экраны и средства родительского контроля. /Лаб/	10	2	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3		2	Выполнение заданий лабораторной работы
3.5	Изучение литературы и дополнительных источников по теме /Ср/	10	6	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3			Выполнение контрольной работы по теме
	Раздел 4. Технические средства защиты и комплексное обеспечение информационной безопасности							
4.1	Технические средства защиты информации. /Лек/	10	2	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3			Выполнение контрольной работы по теме
4.2	Средства контроля доступа в информационных системах. /Лаб/	10	2	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3			Выполнение заданий лабораторной работы
4.3	Виды и назначение технических средств защиты информации. /Лаб/	10	2	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3			Выполнение заданий лабораторной работы
4.4	Политика информационной безопасности /Лек/	10	2	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3			Выполнение контрольной работы по теме

4.5	Основные этапы обеспечения защиты информации: определение политики и составляющих информационной безопасности, управление рисками, аудит информационной безопасности. /Лаб/	10	2	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3			Выполнение заданий лабораторной работы
4.6	Анализ и оценивание угроз информационной безопасности личности в цифровой образовательной среде. Интернет-зависимость. Влияние социальных сетей на адаптацию молодежи. /Лаб/	10	2	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3			Выполнение заданий лабораторной работы
4.7	Изучение литературы и дополнительных источников по теме /Ср/	10	12	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3			Выполнение контрольной работы по теме
	Раздел 5. Элементы криптографии							
5.1	Криптография, криптоанализ и стеганография. /Лек/	10	2	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3			Выполнение контрольной работы по теме
5.2	Симметричное и ассиметричное шифрование. Электронная подпись. /Лаб/	10	2	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3			Выполнение заданий лабораторной работы
5.3	Изучение литературы и дополнительных источников по теме /Ср/	10	3,85	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3			Выполнение контрольной работы по теме
	Раздел 6. Зачет							
6.1	Зачет /КРЗ/	10	0,15	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3			Вопросы к зачету

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (ОЦЕНОЧНЫЕ СРЕДСТВА) для текущего контроля успеваемости, промежуточной аттестации

5.1. Контрольные вопросы и задания

Пример контрольного задания № 1

1. Создайте в тетради или текстовом процессоре таблицу Вижинера размерностью 7×3 и алфавитом А={Н, А, Д, О, В, Р}. Зашифруйте слово ДВОР с помощью ключа ДНО.
2. С помощью этой же таблицы зашифруйте произвольное слово (не более 6 букв) с ключом РОВ. Напишите получившуюся шифрограмму. Расшифруйте шифрограмму ОРНВТ.
3. С помощью этой же таблицы зашифруйте произвольное слово (не более 6 букв) с произвольным ключом (не более 4 букв). Какой метод для подбора ключа бы будете использовать?
4. Создайте в тетради или текстовом процессоре квадрат Бьюфорта размерностью 5×5 и алфавитом А={А, Е, О, П, Р}. Расшифруйте шифрограмму ЕААР с помощью ключа ПА.
5. С помощью этого же квадрата расшифруйте шифрограмму ЕАЕАПН, если известно, что размерность ключа от 3 до 6 символов.
6. Зашифруйте с помощью этого же квадрата произвольное слово не более чем из 5 символов и ключом ПЕРО с количеством раундов = 2.
7. Используя интерфейс, аналогичный программе «Квадрат Полибия» напишите алгоритм шифрования текстовых файлов (UTF-8) методом Вижинера или Бьюфорта

Пример контрольного задания № 2

1. Зашифруйте при помощи шифра A1Z26 файл с текстом: «Шифрование может быть симметричным и асимметричным» (кодировка ANSI) в файл Primer1_C.txt, напишите, что получилось в результате.
2. Расшифруйте файл Photo1_C.jpg методом XOR в файл Result.jpg, если известно, что ключ – это символ ASCII и лежит в пределах от «%» до «<« .
3. Создайте произвольное изображение (включите в него текст с любым посланием) с помощью MS Paint, сохраните его как Ваша_фамилия.jpg. Зашифруйте данный файл методом XOR с произвольным потоковым ключом длины

64. Отправьте ключ.

5.2. Темы письменных работ

Примерная тематика заданий для индивидуальных работ:
1. Изучение ФЗ №152-ФЗ «О персональных данных» и ФЗ «О защите детей от
2. информации, причиняющей вред их развитию»
3. Составление каталога интернет-ресурсов, полезных для воспитания, образования и
4. развития детей.
5. Сравнение функций родительского контроля в составе антивирусных программ
6. Планирование мероприятий по защите персональных данных в образовательной
7. организации.
8. Разработка политики информационной безопасности в образовательной организации.

Примерная тематика индивидуальных проектных заданий.
1. Биометрические системы идентификации
2. Безопасность и конфиденциальность в Интернете
3. Понятие о персональных данных
4. Информация, составляющая коммерческую тайну
5. Объекты информационной безопасности в предметной области
6. Информационная среда иллюзии или реальности
7. Случайные и целенаправленные угрозы нарушения сохранности информации
8. Понятие дезинформации
9. Риски информационной безопасности
10. Информационное оружие
11. Информационные войны
12. Технические средства промышленного шпионажа
13. Классы безопасности
14. Аудит информационной безопасности
15. История хакерства
16. Хакерство в России
17. Правовые механизмы защиты информации на разных уровнях
18. Понятие и применение электронной цифровой подписи
19. Манипуляции сознанием
20. Программы родительского контроля
21. Средства антивирусной защиты мобильных устройств

5.3. Оценочные материалы (оценочные средства)

Задания для промежуточной аттестации – перечень примерных вопросов для устного собеседования на зачете.
1. Назовите и охарактеризуйте основные понятия предметной области информационной безопасности. Приведите примеры, раскрывающие понятия: воздействия, угрозы, уязвимости, риски, атаки.
2. Опишите текущую ситуацию в цифровом обществе с позиции кибербезопасности. Укажите, каковы наиболее часто встречающиеся инциденты кибербезопасности в нашей стране и мире. Дайте определение кибертерроризму. Назовите и приведите примеры угроз кибербезопасности.
3. На примере объектов персональной защиты раскройте понятие информационных ценностей и покажите, как определить ценность информационных активов. Определите понятие и виды ущерба. Перечислите основные группы информационных ценностей.
4. Перечислите и раскройте смысл составляющих информационной безопасности. Опишите типовые ситуации, нарушающие данные составляющие и дайте название каждому типу.
5. Опишите основные виды средств формальной и неформальной защиты информации, приведите конкретные примеры на каждый вид. Приведите схему, показывающую, что защита информации должна быть комплексной и системной.
6. Приведите не менее 4 примеров основных инцидентов, связанных с информационной безопасностью и защитой информации персональных ценностей. Предложите меры по их предотвращению и устранению последствий.
7. Дайте определение общему понятию атаки и назовите ее ключевые признаки. Приведите 3-4 примера известных вам атак, связанных с кибербезопасностью.
8. Перечислите и охарактеризуйте основные фазы жизненного цикла атаки: общую схему любой атаки и фазы таргетированной атаки. Приведите примеры таргетированной и нетаргетированной атаки.
9. Назовите и охарактеризуйте основные виды кибератак. Приведите по 1-2 примера на каждый вид. Предложите контрмеры для избегания таких случаев и устранения последствий каждого вида атак.
10. Дайте определение консольным атакам. Приведите примеры 4-5 возможных инцидентов, связанных с консольными атаками на настольные ПК, ноутбуки, смартфоны и планшеты.
11. Перечислите и поясните 4-5 основных возможных инцидентов при атаках на браузеры, сервисы быстрых сообщений и электронной почты. Как определить фальсификацию сообщений электронной почты и социальный «спуффинг»?
12. Приведите примеры использования социальной инженерии при реализации сетевых атак: «маскарад» и использование беспечных пользователей. Предложите контрмеры для избегания и устранения последствий каждого вида атак.
13. Дайте определение и приведите примеры атак: сетевого спуффинга, сниффинга, фладинга, боминга. Охарактеризуйте следующие типы злоумышленников: хакер, кардер, пранкер, кибербуллер, крэкер, шпион, вандал, спаммер.

14. Охарактеризуйте атаки на средства аутентификации, используя слова: «стойкость паролей», «брутфорс», «атака по словарю». Приведите примеры консольных и сетевых атак на пароли.
15. Опишите, каковы целевые назначения систем защиты информации и каковы минимальные требования к обеспечению информационной безопасности. Охарактеризуйте каждый уровень защиты информации с позиции системного подхода.
16. Дайте определение политике информационной безопасности организации. Приведите основные характеристики и принципы по ее реализации с точки зрения различных уровней: организационного, программного, технического.
17. Раскройте через примеры основные способы защиты информационных объектов: препятствие, управление, маскировка, регламентация, побуждение и принуждение. Приведите схему, раскрывающую модель комплексной системы защиты информации.
18. Перечислите и дайте определение основным механизмам защиты информации. Приведите примеры реализации каждого механизма.
19. Опишите особенности построения моделей комплексной защиты информации через модель угроз и модель нарушителя. Приведите примеры угроз и потенциальных инцидентов.
20. Приведите основные виды программных угроз информационной безопасности. Охарактеризуйте каждый вид с позиции возможных инцидентов и ущерба от них. Опишите основные виды вредоносного программного обеспечения.
21. Охарактеризуйте основные методы оценки рисков информационной безопасности и пути их применения. Перечислите и поясните основные стратегии управления рисками. Опишите, как должно осуществляться реагирование на реализацию рисков в системах защиты информации.
22. Дайте определение криптологии как области знаний. Перечислите и охарактеризуйте основные составляющие. Приведите примеры, раскрывающие применение в защите информации ее основных разделов.
23. Приведите в ретроспективе процесс развития стеганографии с древних времен до современного этапа. Проиллюстрируйте применение современной стеганографии для защиты информации.
24. Раскройте определение криптоанализа и его роли при построении систем защиты информации. Перечислите и поясните на примерах основные методы криптоанализа.
25. Раскройте определение криптографии и ее роли при построении систем защиты информации. Приведите в ретроспективе процесс развития криптографии с древних времен до современного этапа и возможные перспективы в будущем.
26. Приведите схему, раскрывающую основные виды криптоалгоритмов. Укажите определение криптосистемы и основных понятий, с ней связанных. Объясните, для чего применяются бесключевые криптоалгоритмы.
27. Перечислите и опишите функциональные возможности средств для осуществления родительского и/или педагогического контроля для цифровых устройств (компьютеров, смартфонов, планшетов, смартТВ, цифровых приставок и т.п.).
28. Опишите принцип работы симметричного шифрования. Продемонстрируйте процесс шифрования и расшифрования при помощи любого известного вам метода (шифра).
29. Раскройте основные направления и особенности применения симметричных криптосистем, приведите примеры и их названия. Объясните, в чем основной недостаток применения симметричных шифров на текущем этапе развития цифрового общества.
30. Опишите различия потоковых и блочных шифров. Поясните их на примере простого шифрования. Объясните, какой вклад внес в развитие криптографии Хорст Фейстель и в чем его суть.
31. Объясните, каким образом определяется стойкость криптоалгоритма. Укажите, какой вклад в данную область внес Огюст Керкгоффс и какие шифры сегодня считаются абсолютно стойкими и достаточно стойкими.
32. Опишите принцип работы асимметричного шифрования. Раскройте основные направления и особенности применения асимметричных криптосистем, приведите примеры и их названия.
33. Объясните, в чем суть проблемы распределения ключей шифрования. Приведите пример такой проблемы между двумя сторонами, возможные варианты ее решения. Укажите, какой способ решения предложили Уитфилд Диффи и Мартин Хеллман.
34. Раскройте суть правового обеспечения информационной безопасности через понятие информационного права, основные объекты защиты. Приведите основные законы РФ, связанные с областью информационной безопасности.
35. Перечислите и поясните, в чем заключаются особенности обеспечения информационной безопасности в образовательных организациях. Приведите примеры основных видов мер по защите информации в сфере образования.
36. На примерах поясните, какие риски, связанные с информационной безопасностью и защитой информации, существуют для педагогических работников. Предложите основные меры по их минимизации.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Адрес
Л1.1	Прохорова О. В.	Информационная безопасность и защита информации: учебник	Самара: Самарский государственный архитектурно-строительный университет, 2014	https://biblioclub.ru/index.php?page=book&id=438331
Л1.2	Ищейнов В. Я.	Информационная безопасность и защита информации: теория и практика: учебное пособие	Москва, Берлин: Директ-Медиа, 2020	https://biblioclub.ru/index.php?page=book&id=571485

	Авторы, составители	Заглавие	Издательство, год	Адрес
Л1.3	Трушин В. А., Котов Ю. А., Левин Л. С., Донской К. А.	Введение в информационную безопасность и защиту информации: учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2017	https://biblioclub.ru/index.php?page=book&id=575113

6.3.1 Перечень программного обеспечения

1. Microsoft® Windows® 8.1 Professional (OEM лицензия, контракт № 20А/2015 от 05.10.2015);
2. Kaspersky Endpoint Security – Лиц сертификат №1B08-190415-050007-883-951;
3. 7-Zip - (Свободная лицензия GPL);
4. Adobe Acrobat Reader – (Свободная лицензия);
5. Google Chrome – (Свободная лицензия);
6. Mozilla Firefox – (Свободная лицензия);
7. LibreOffice – (Свободная лицензия GPL);
8. XnView – (Свободная лицензия);
9. Java – (Свободная лицензия);
10. VLC – (Свободная лицензия);

6.3.2 Перечень профессиональных баз данных и информационных справочных систем

Elibrary.ru: электронная библиотечная система : база данных содержит сведения об отечественных книгах и периодических изданиях по науке, технологии, медицине и образованию. Адрес: http://elibrary.ru Режим доступа: Свободный доступ;
Электронно-библиотечная система «Университетская библиотека онлайн». Адрес: https://biblioclub.ru Режим доступа: Индивидуальный неограниченный доступ;
Электронно-библиотечная система издательства «ЛАНЬ». Адрес: e.lanbook.com Режим доступа: Индивидуальный неограниченный доступ;
Образовательная платформа «Юрайт». Адрес: https://urait.ru Режим доступа: Индивидуальный неограниченный доступ;
ИС Антиплагиат: система обнаружения заимствований. Адрес: https://krasspu.antiplagiat.ru Режим доступа: Индивидуальный неограниченный доступ;
Консультант Плюс /Электронный ресурс/:справочно – правововая система. Адрес: Научная библиотека Режим доступа: Локальная сеть вуза;

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Перечень учебных аудиторий и помещений закрепляется ежегодным приказом «О закреплении аудиторий и помещений в Федеральном государственном бюджетном образовательном учреждении высшего образования «Красноярский государственный педагогический университет им. В.П. Астафьева на текущий год» с обновлением перечня программного обеспечения и оборудования в соответствии с требованиями ФГОС ВО, в том числе:
1. Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля успеваемости и промежуточной аттестации
2. Помещения для самостоятельной работы обучающихся
3. Помещения для хранения и профилактического обслуживания учебного оборудования
4. Перечень лабораторий.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Преподавание учебной дисциплины «Информационная безопасность и защита информации» предусматривает использование не только традиционных форм обучения (чтение лекций, проведение групповых практических занятий), но и использование новых информационных и образовательных технологий.
Преподавателями будут максимально использоваться те формы обучения, которые потребуют от вас активности, самостоятельности и ответственности.
При изучении лекционного материала вам необходимо будет использовать как выложенные в электронном курсе опорные презентации и сопроводительные материалы, так и дополнительные статьи из периодических изданий и зарубежных источников. Освоение данной дисциплины требует также активного использования возможностей Интернет-ресурсов, что позволяет значительно обогатить используемый в практике материал, а также способствует развитию вашей профессиональной компетентности в области использования возможностей информационных систем в будущей деятельности.
В ходе занятий необходимо быть готовыми использовать новые информационные технологии, в частности, использовать средства мультимедийных аудиторий. Лекционный материал будет сопровождаться использованием в ходе занятий средств повышения наглядности представляемых материалов (наглядных пособий, аудиовизуальных средств обучения, интерактивных заданий и упражнений), чтобы сформировать у вас понимание, умения и навыки их применения в практической деятельности.
Особое внимание необходимо уделять изучению понятийного аппарата дисциплины. Лекции ориентированы на систематизированное представление знаний, раскрытие сущности наиболее трудных для освоения учебных вопросов (материалов). При посещении лекции нужно учитывать, что затем будет проводиться практическое, следует делать краткие записи в виде конспекта, задавать преподавателю вопросы относительно дальнейшего применения лекционного материала на практических занятиях и промежуточной аттестации (контрольной работе, тестировании, зачете, экзамене) по каждой теме.
Практические занятия проводятся в виде: группового обсуждения студентами проблем по предлагаемым темам в рамках

определенного раздела изучаемой дисциплины; анализа, проведения, обработки и интерпретации результатов изучения различных информационных источников; изучения характеристик и возможностей средств различных научных отраслей; практической отработки навыков применения теоретических знаний на практике; обсуждения выполненных в ходе занятия работ (заданий).

В качестве текущего контроля успеваемости на занятиях используются проблемные практические задания, которые потребуют от вас решения конкретных задач и проблем, моделирования поведения в ситуациях, принятия решений и активных действий согласно собственному плану. При текущем контроле преподаватель будет в первую очередь обращать внимание на проявление у вас признаков информационной культуры, сформированность исследовательских навыков, способность аргументировать свою позицию, развитие навыков обоснования выполненных действий, способность действовать самостоятельно.

Преподаватель в течение всего семестра будет оценивать вашу активность и качество выполнения всех заданий, при этом активно помогая тем, кто испытывает определенные затруднения при изучении материалов учебной дисциплины, при помощи консультаций, дополнительных пояснений или специальных дополнительных материалов и заданий.

Итоговой формой контроля работы по дисциплине является зачет. Критериями допуска к зачету являются:

а) успешное выполнение и сдача не менее 75% промежуточных заданий в текущем семестре;

б) успешное прохождение итогового тестирования по дисциплине (на положительную оценку в 61% и более баллов);

в) успешная защита кейсового задания;

г) наличие посещаемости большей части (60% и более) очных занятий и/или активности в электронном курсе (изучение не менее 70% ресурсов).

К итоговому тестированию необходимо будет подготовиться, опираясь на список заданий и лекции. В качестве источников для ответов на тестовые задания можно использовать рекомендованные данной программой учебники и учебные пособия, материалы занятий, ресурсы электронного курса, а также самостоятельно обнаруженные цифровые ресурсы образовательного характера.