ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

**«ЛЕНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**ИМЕНИ А.С. ПУШКИНА»**

УТВЕРЖДАЮ

Проректор по учебно-методической

работе

\_\_\_\_\_\_\_\_\_\_\_\_ С.Н.Большаков

РАБОЧАЯ ПРОГРАММА

дисциплины

**Б1.В.05.ДВ.03.02 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ**

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

Направленность (профиль) **Информатика и математика**

(год начала подготовки - 2022)

Санкт-Петербург

2022

**1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ**

Процесс изучения дисциплины направлен на формирование следующих компетенций:

| **Индекс компетенции** | **Содержание компетенции** **(или ее части)** | **Индикаторы компетенций (код и содержание)** |
| --- | --- | --- |
| ПК-3 | Способен применять предметные знания при реализации образовательного процесса | ИПК-3.1 Знает: основные понятия информационной безопасности; принципы классификации угроз информационной безопасности; принципы защиты информации; законодательные акты РФ в области информационной безопасности |
| ИПК-3.2 Умеет: анализировать возможные угрозы информационной безопасности организации; готовить предложения по предупреждению несанкционированного доступа к информационным ресурсам |
| ИПК-3.3 Владеет: навыками установки, настройки и использования средств для защиты от вредоносного ПО, средств шифрования и инструментов резервного копирования и восстановления информации; первичными навыками по подготовке информационных обзоров по проблеме информационной безопасности при использовании отечественных и зарубежных источников навыками использования электронной цифровой подписи |

**2. Место дисциплины в структуре ОП**

**Цель дисциплины**: раскрыть основы правового регулирования отношений в информационной сфере, конституционные гарантии прав граждан на получение информации и механизм их реализации, понятия и виды защищаемой информации по законодательству РФ, систему защиты государственной тайны, основы правового регулирования отношений в области интеллектуальной собственности и способы защиты этой собственности, понятие и виды компьютерных преступлений, а также приобретение обучаемыми знаний по организационному обеспечению защиты информации и формирование некоторых практических навыков работы, принципами, методами и средствами защиты информации в образовательном учреждении.

**Задачи дисциплины:**

* знакомство с основами информационной безопасности и защиты информации;
* изучение принципов криптографических преобразований, типовых программно-аппаратные средств и систем защиты информации от несанкционированного доступа;
* анализ угроз безопасности, приобретение навыков защиты информации; изучение методов и средств обеспечения защиты информации;
* знакомство с информационным законодательством Российской Федерации;
* знакомство с правилами лицензирования и сертификации в области защиты информации;
* знакомство с международным законодательством в области защиты информации;
* приобретение знаний о компьютерных преступлениях;
* знакомство с вопросами информационной безопасности в образовательном учреждении.

Дисциплина входит в блок **Б1** (**Дисциплины**) в **часть, формируемую участниками образовательных отношений**, в модуль **Документационное обеспечение управления и информационная безопасность** и является **дисциплиной по выбору (Б1.В.05.ДВ.03)** учебного плана направления 44.03.05 «Педагогическое образование» (Б1.В.05.ДВ.03.02). Дисциплина позволит сформировать у бакалавров представление об основных угрозах информационной безопасности и методах и средствах защиты информации.

Предшествующими для изучения учебной дисциплины являются дисциплины: Введение в информатику (Б1.В.02.ДВ.01.01), Информационные технологии в образовании (Б1.О.02.03), Программирование (Б1.О.08.04), «Операционные системы, сети и интернет-технологии» (Б1.В.02.ДВ.02.01), «Архитектура компьютера»( Б1.О.08.02).

После изучения дисциплины обучающиеся смогут использовать сформированные компетенции в процессе изучения дисциплин «Информатизация управления образовательным процессом» (Б1.В.ДВ.11.01), а также – в процессе самообразования. Также обучающиеся смогут использовать сформированные компетенции в процессе выполнения выпускной квалификационной работы (ВКР).

**3. Объем дисциплины и виды учебной работы**

Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 академических часа (1 зачетная единица соответствует 36 академическим часам).

**Очная форма обучения**

| **Вид учебной работы** | **Трудоемкость в акад.час** |
| --- | --- |
|  |  | **Практическая подготовка** |
| **Контактная работа (аудиторные занятия) (всего):** | **40** |
| В том числе: |  |
| Лекции | 14 | - |
| Лабораторные работы / Практические занятия (в т.ч. зачет) | 26/- | -/- |
| **Самостоятельная работа (всего)** | **32** |
| **Вид промежуточной аттестации (экзамен):** | - |
| контактная работа | - |
| самостоятельная работа по подготовке к экзамену | - |
| **Общая трудоемкость дисциплины (в час./з.е.)** | **72/2** |

**Заочная форма обучения**

| **Вид учебной работы** | **Трудоемкость в акад.час** |
| --- | --- |
|  |  | **Практическая подготовка** |
| **Контактная работа (аудиторные занятия) (всего):** | **14** |
| В том числе: |  |
| Лекции | 6 | - |
| Лабораторные работы / Практические занятия  | 8/- | -/- |
| **Самостоятельная работа (всего)** | **54** | **-** |
| **Вид промежуточной аттестации (зачет):** | **4** | **-** |
| контактная работа | 0,25 | **-** |
| самостоятельная работа по подготовке к зачету | 3,75 | **-** |
| **Вид промежуточной аттестации (экзамен):** | **-** |
| контактная работа | - |
| самостоятельная работа по подготовке к экзамену | - |
| **Общая трудоемкость дисциплины (в час./з.е.)** | **72/2** |

**4. Содержание дисциплины**

При проведении учебных занятий обеспечивается развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая при необходимости проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, составленных на основе результатов научных исследований, проводимых организацией, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

**4.1. Блоки (разделы) дисциплины**

|  |  |
| --- | --- |
| **№** | **Наименование блока (раздела) дисциплины** |
| 1 | Введение в информационную безопасность. Информация как объект правового регулирования |
| 2 | Организационно-правовое обеспечение информационной безопасности |
| 3 | Виды защищаемой информации. Правонарушения в области обеспечения информационной безопасности |
| 4 | Методы и средства защиты информации от угроз нарушения конфиденциальности, целостности, отказа доступа к информации |
| 5 | Основные виды угроз информационной безопасности в образовательном учреждении. Методы и средства информационной защиты |

**4.2. Примерная тематика курсовых работ (проектов)**

Выполнение курсовых проектов учебным планом не предусмотрено.

**4.3. Перечень занятий, проводимых в активной и интерактивной формах, обеспечивающих развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств. Практическая подготовка\***

| **№ п/п** | **Наименование блока (раздела) дисциплины** | **Занятия, проводимые в активной и интерактивной формах** | **Практическая подготовка\*** |
| --- | --- | --- | --- |
| **Форма проведения занятия**  | **Наименование видов занятий** |
| 1. | Введение в информационную безопасность. Информация как объект правового регулирования | лекционное занятие  | использование презентаций  |  |
| лабораторное занятие | решение ситуационных задач, работа в группах |  |
| 2. | Организационно-правовое обеспечение информационной безопасности | лекционное занятие | использование презентаций  |  |
| лабораторное занятие | решение ситуационных задач, работа в группах |  |
| 3. | Виды защищаемой информации. Правонарушения в области обеспечения информационной безопасности | лекционное занятие | использование презентаций  |  |
| лабораторное занятие | решение ситуационных задач, работа в группах |  |
| 4. | Методы и средства защиты информации от угроз нарушения конфиденциальности, целостности, отказа доступа к информации | лекционное занятие | использование презентаций  |  |
| лабораторное занятие | решение ситуационных задач, работа в группах |
| 5. | Основные виды угроз информационной безопасности в образовательном учреждении. Методы и средства информационной защиты | лекционное занятие | использование презентаций |  |
| лабораторное занятие | решение ситуационных задач, работа в группах |  |

**\***Практическая подготовка при реализации учебных предметов, курсов, дисциплин (модулей) организуется путем проведения практических занятий, практикумов, лабораторных работ и иных аналогичных видов учебной деятельности, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

**5. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине**

**5.1. Темы для творческой самостоятельной работы обучающегося**

Темы для творческой самостоятельной работы студента формулируются обучающимся самостоятельно, исходя из перечня тем занятий текущего семестра.

**5.2. Темы конспектов**

1. Виды нормативно-правовых актов, их иерархия;
2. Федеральное законодательство в вопросах информационной безопасности.
3. Ответственность за правонарушения в области информационной безопасности и ее виды.
4. Государственная система защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам.
5. Понятие угрозы. Виды угроз.
6. Модели безопасности и их применение.
7. Методы и принципы обеспечения информационной безопасности.
8. Методы реализации угроз информационной безопасности
9. Понятие политики безопасности.
10. Сущность и содержание основных типов политик безопасности.
11. Программно-апппаратные средства защиты от несанкционированного доступа к компьютерным криптографическим системам.
12. Организационные, технологические, правовые методы защиты от несанкционированного доступа к информации.
13. Организационные методы защиты от несанкционированного доступа к информации.
14. Технологические методы защиты от несанкционированного доступа к информации.
15. Правовые методы защиты от несанкционированного доступа к информации.
16. Парольные системы.
17. Криптографические методы защиты.
18. Электронная цифровая подпись.

**5.3. Вопросы для подготовки к устным собеседованиям (опросам)**

1. Понятие информации.
2. Информация как основной объект информационного права.
3. Специфические особенности и юридические свойства информации.
4. Информационные отношения как основной объект правового регулирования.
5. Законодательный уровень информационной безопасности РФ: обзор правовых актов общего, административного и программно-технического назначения.
6. Порядок совершения гражданско-правовых сделок, связанных с использованием информации, обеспечение безопасности.
7. Правонарушения в области обеспечения информационной безопасности
8. Основные положения Федерального закона от 27.11.2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации».
9. Кодекс Российской Федерации об административных правонарушениях, в сфере информационной безопасности, составление протоколов об указанных административных правонарушениях.
10. Положение «О государственной системе защиты информации. в российской федерации от иностранных технических. разведок и от ее утечки по техническим каналам». от 15 сентября 1993 г. № 912-51.
11. Что такое информационная безопасность?
12. Что понимают под доступностью информационных ресурсов?
13. Что понимают под целостностью информационных ресурсов?
14. Что понимают под конфиденциальностью информационных ресурсов?
15. Что такое защита информации?
16. Что такое угроза информационной безопасности? Чем угроза отличается от атаки?
17. Приведите известные Вам варианты классификации угроз информационной безопасности.
18. Приведите примеры законодательных и морально-этических мер противодействия угрозам информационной безопасности.
19. Приведите примеры административных мер противодействия угрозам информационной безопасности.
20. Приведите примеры физических и технических мер противодействия угрозам информационной безопасности.
21. Чем шифрование отличается от кодирования? Приведите примеры шифра и кода. Что такое ключ?
22. Что такое симметричное шифрование? Каковы достоинства и недостатки симметричного шифрования? Приведите примеры симметричных алгоритмов шифрования.
23. Что такое асимметричное шифрование? Каковы достоинства и недостатки асимметричного шифрования? Приведите примеры асимметричных алгоритмов шифрования.
24. Что собой представляет дискреционная модель управления доступом?
25. Что собой представляет мандатная модель управления доступом?
26. Что собой представляет ролевая модель управления доступом?
27. Что такое идентификация, аутентификация и авторизация?
28. Кратко охарактеризуйте основные классы аутентифицирующей информации.
29. Какие методы взлома парольной защиты Вы знаете?
30. Перечислите пути снижения уязвимости парольной защиты от взлома базы паролей.
31. Чем (с точки зрения защиты информации) может быть полезен менеджер паролей?
32. Перечислите основные методы и средства защиты доступности информационных ресурсов.
33. Что такое помехоустойчивое кодирование? Приведите примеры обнаруживающих и корректирующих кодов.

**5.4. Вопросы для подготовки к коллоквиумам**

Проведение коллоквиумов не предполагается

**5.5. Темы рефератов**

1. Внутренние угрозы информационной безопасности
2. Недостатки каналов связи различной физической природы при обеспечении информационной безопасности
3. Технические каналы утечки информации
4. Угрозы целостности и конфиденциальности информации в компьютерных сетях
5. Методы защиты информации в телекоммуникационных сетях
6. Методы защиты информации и программного обеспечения в локальных компьютерных сетях
7. Компьютерные вирусы и метолы борьбы с ними
8. Способы повышения устойчивости паролирования в компьютерных сетях
9. Правовые основы информационной безопасности
10. Правовое обеспечение ограничения информационного доступа
11. Государственная информационная политика
12. Система защиты государственной тайны
13. Сертификация и лицензирование средств защиты информации
14. Правовая защита авторских и смежных прав
15. Криптографические методы защиты информации и основные направления их обеспечения
16. Особенности расследования компьютерных преступлений
17. Средства и методы физической защиты объекта
18. Применение межсетевых экранов для защиты компьютерных сетей
19. Синхронное и асинхронное шифрование
20. Расследование компьютерных преступлений в РФ и за рубежом
21. Основные виды угроз информационной безопасности в образовательном учреждении

**6. Оценочные средства для текущего контроля УСПЕВАЕМОСТИ**

**6.1. Текущий контроль**

|  |  |  |
| --- | --- | --- |
| **№****пп** | **№ и наименование блока (раздела) дисциплины** | **Форма текущего контроля** |
| 1 | Введение в информационную безопасность. Информация как объект правового регулирования | Устное собеседование |
| 2 | Организационно-правовое обеспечение информационной безопасности | Устное собеседование  |
| 3 | Виды защищаемой информации. Правонарушения в области обеспечения информационной безопасности | Устное собеседование |
| 4 | Методы и средства защиты информации от угроз нарушения конфиденциальности, целостности, отказа доступа к информации | Устное собеседование  |
| 5 | Основные виды угроз информационной безопасности в образовательном учреждении. Методы и средства информационной защиты | Устное собеседование |

**6.2. Примеры оценочных средств для текущего контроля по дисциплине**

**Темы конспектов**

Представлены в разделе 5.1.

**Вопросы для сдачи коллоквиумов**

Представлены в разделе 5.3.

**Вопросы для проведения устных опросов**

Представлены в разделе 5.2.

**Темы рефератов**

Представлены в разделе 5.4.

**Задания для лабораторных занятий**

**Тема «Организация поиска нормативных документов в СПС Консультант Плюс»**

**Задание 1.** Найдите Федеральный закон Российской Федерации от 27 июля

2006 г. № 149-ФЗ «Об информации, информационных технологиях и о

защите информации».

Сохраните в текстовом файле с названием Задача1:

- реквизиты закона,

- статьи, содержащие термин «информация» и другие понятия, связанные с термином «информация».

**Задание 2.** Найдите Закон «О безопасности» 1992 г.

Сохраните в текстовом файле с названием Задача4:

- реквизиты закона,

- статьи, содержащие понятие «безопасность», «информационная безопасность».

**Тема «Организация полнотекстного поиска. Работа со списком в СПС Консультант»**

**Задача 1**. Список документов (1-5штук)сохраните в текстовом файле с названием Задача 1.

Подобрать документы по тематике «**шифровальные (криптографические) средства».**

**Задача 2**. Список документов (1-5штук)сохраните в текстовом файле с названием Задача 2.

Подобрать документы по тематике «**доступ к информации».**

**Задача 3**. Список документов (1-5штук)сохраните в текстовом файле с названием Задача 3.

Подобрать документы по тематике «**технические средства защиты информации».**

**Тема «Работа со списком и текстом найденных документов. Справочная информация в СПС Консультант Плюс»**

**Задача 1.**

Найдите Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Поставить закладки на любые три статьи, содержащие термины «информация» и другие понятия, связанные с термином «информация».

**Задача 2.**

Создайте папку с именем Нормативный правовой акт и включите в нее документы, содержащие понятие «нормативный правовой акт».

**Тема «Использование классических криптоалгоритмов подстановки и перестановки для защиты текстовой информации»**

**1.** Для одноалфавитного метода с фиксированным смешением определить установленное в программе смещение. Для этого следует:

* просмотреть предварительно созданный с помощью редактора свой текстовый файл;
* выполнить для этого файла шифрование;
* построить гистограммы исходного и зашифрованного текстов;
* описать гистограммы (в чем похожи, чем отличаются) и определить, каким смещением было выполнено шифрование;
* расшифровать зашифрованный текст:

**2.**Для одноалфавитного метода с задаваемым смещением (шифр Цезаря) следует:

* выполнить шифрование с произвольным смещением для своего исходного текста;
* построить гистограммы исходного и зашифрованного текстов, определить смещение для нескольких символов;
* расшифровать текст.

**3.**Создайте небольшой файл длиной в несколько слов с известным вам текстом, зашифруйте его, постройте гистограммы (опишите их; ответьте, можно ли извлечь из них полезную дешифрации информацию). Сравните исходный и зашифрованный тексты и определите закон перестановки символов. Дешифруйте файл.

**4.** Для инверсного кодирования (по дополнению до 255):

* выполните шифрование для своего произвольного файла;
* постройте гистограммы исходного и зашифрованного текстов, опишите гистограммы и определите смещение для нескольких символов;
* дешифруйте зашифрованный текст.

**Тема «Исследование различных методов защиты текстовой информации и их стойкости на основе подбора ключей»**

**1.**Выполнить настройку программы: выбрать метод шифрования, ввести ключи для всех методов, ввести вероятное слово, осуществить все остальные системные настройки.

**2.**Для метода замены (одноалфавитного метода):

* убрать данный алгоритм в списке доступных методов шифрования и установить необходимое смещение;
* открыть произвольный файл;
* просмотреть содержимое исходного файла;
* исполнить для этого файла шифрование (при необходимости можно задать имя зашифрованного файла);
* просмотреть в редакторе зашифрованный файл;
* ввести вероятное слово;
* ввести вероятную длину ключа (кроме метода замены);
* подобрать ключ;
* выполнить расшифрование со всеми найденными ключами;
* найти в каком-либо из расшифрованных файлов правильно расшифрованное ключевое слово;
* расшифровать файл исходным ключом;
* проверить результат.

**3.**Для метода перестановки:

* выбрать метод перестановки;
* в открывшемся окне ввода ключа перестановки символов указать сначала длину этого ключа, а затем из появившихся кнопок составить необходимую комбинацию для ключа, нажимая на кнопки в заданном порядке; при этом уже использованные кнопки становятся недоступными для предотвращения их повторного ввода;
* далее действия полностью соответствуют изложенным в п.2.

**4.**Для метода гаммирования:

* выбрать метод;
* ввести ключ;
* полностью повторить п.2.

**5.**Для таблицы Виженера все действия повторяются из п.4 (метод гаммирования). В отчете для каждого метода шифрования описывается последовательность выполняемых действий, указываются имена всех использованных файлов, исходные и найденные ключи, описывается процесс дешифрования.

**Тема «Стандарт симметричного шифрования AES Rijndael»**

**1.**Изучить на примере обычных текстовых файлов способы шиф­рования и расшифрования с помощью алгоритма Rijndael. Подробно рассмотреть действие всех цикловых преобразований как при шифровании, так и расшифровании. Исходный текст для шифрования может быть подготовлен заранее и сохранен в файле \*.txt.

**Тема «Генерация простых чисел, используемых в асимметричных системах шифрования»**

**1.** Проверить на простоту два произвольных числа разрядностью не менее 5.

**2.** Найти в заданном интервале все простые числа. Предварительно вычислить количество простых чисел.

**3.** Известно, что в заданном интервале имеются числа Кармайкла. Найти их.

**Тема «Электронная цифровая подпись»**

**1.** Ознакомиться с основными направлениями работ в рамках федеральной целевой программы «Электронная Россия», а также со сведениями о порядке использования и действующих алгоритмах постановки электронной цифровой подписи.

**2.** Сгенерировать и переслать участникам обмена ключи для шифрования исходного документа и ключи для подписания документа.

**3.** Зашифровать исходное сообщение и подписать его на секретном ключе отправителя.

**4.** Переслать зашифрованное и подписанное сообщение получателю. Выполнить проверку правильности ЭЦП и восстановить исходный текст сообщения.

**Тема «Шифрование методом скользящей перестановки»**

**1.**Открыть данные для шифрования.

**2.** Произвести шифрование информации с использованием шифра скользящей перестановки, сохранить шифротекст в файле.

**Тема «Корректирующие коды. Коды Хемминга»**

**1.** Построить самокорректирующийся код Хэмминга для слов длины 4.

**2.** Обнаружить и исправить ошибку при передаче кодовых слов  из кода Хэмминга :



**3.**

**3.1.**Закодировать с помощью кода Хэмминга предложенный алфавит: **Кириллица А .. М**. Описать в тетради процесс получения кода одной любой буквы (на выбор).

**3.2.**В каждую строку таблицы с закодированной информацией внести одиночную ошибку, зафиксировать в кодовой таблице результат декодирования. Описать в тетради процесс декодирования кода с одной ошибкой любой буквы (на выбор).

**3.3.**В последние две строки таблицы с закодированной информацией внести двойные ошибки, зафиксировать в кодовой таблице результат декодирования.

**3.4.**Проанализировать полученные результаты и сформулировать аргументированные выводы.

**3.5.**Описать полученный код Хэмминга:

* количество контрольных и информационных разрядов и их номера;
* минимальное кодовое расстояние;
* оценить корректирующую способность полученного кода.

**3.6.**Составить из предложенного алфавита слово длиной не менее пяти символов и закодировать его с помощью полученного кода Хэмминга. Подсчитать длину исходного текста (кодировка ASCII) и закодированного текста (код Хэмминга).

**3.7.**Оценить результаты обнаружения и исправления одиночных и обнаружения двойных ошибок. Сделать выводы о корректирующей способности исследуемого кода.

**Тема «Методы сжатия по Шеннону и Хаффмену»**

**1.** Выполните следующие задания:

* число символов алфавита *k*=*т+2 (т —* номер варианта). Составьте такое исходное сообщение, чтобы:
	+ символы алфавита встречались в сообщении с равными вероятностями,
	+ символы алфавита встречались в сообщении с разными вероятностями;
* введите произвольный связный текст на русском языке. Это может быть пословица, стихотворение или произвольный текст. Используя результаты работы программы, проанализируйте алфавит введенного сообщения: подсчитайте количество символов алфавита, значение энтропии *H*, среднее количество символов на знак *L* при целочисленном кодировании.

**2.**Сообщение состоит из последовательности двух букв *А* и *В*, вероятности появления каждой из которых не зависят от того, какая была передана раньше, и равны 0,8 и 0,2 соответственно. Произведите кодирование по методу Шеннона: а) отдельных букв;
б) блоков, состоящих из двухбуквенных сочетаний; в) блоков, состоящих из трехбуквенных сочетаний. Сравните полученные коды по их эффективности.

**7. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ**

| **№ п/п** | **Наименование** | **Авторы** | **Место издания** | **Год издания** | Наличие |
| --- | --- | --- | --- | --- | --- |
| Печат-ные изда-ния | ЭБС (адрес в сети Интернет) |
| 1. | Основы информационной безопасности: учебное пособие | Гультяева Т.А. | Новосибирск: Новосибирский государственный технический университет | 2018 |  | <http://biblioclub.ru> |
| 2. | Информационная безопасность: учебно-методическое пособие | Моргунов А.В. | Новосибирск: Новосибирский государственный технический университет | 2019 |  | <http://biblioclub.ru> |
| 3. | Преступления в сфере информационной безопасности: учебное пособие для вузов | Корабельников С. М.  | М.: Издательство Юрайт | 2022 |  | <https://urait.ru/bcode/496492> |
| 4. | Основы защиты информации: учебное пособие | Гультяева Т.А. | Новосибирск: Новосибирский государственный технический университет | 2018 |  | <http://biblioclub.ru> |
| 5. | Криптографические методы защиты информации: стандартные шифры. Шифры с открытым ключом: учебное пособие | Котов Ю.А. | Новосибирск: Новосибирский государственный технический университет | 2017 |  | <http://biblioclub.ru> |
| 6. | Информационная безопасность и защита информации: учебное пособие для вузов | Зенков А. В.  | М.: Издательство Юрайт | 2022 |  | <https://urait.ru/bcode/497002> |
| 7. | Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов | Полякова Т.А., Стрельцова А.А.  | М.: Издательство Юрайт | 2022 |  | <https://urait.ru/bcode/498844> |
| 8. | Информационная безопасность: учебное пособие для вузов | Суворова Г. М.  | М.: Издательство Юрайт | 2022 |  | <https://urait.ru/bcode/496741> |
| 8. | Информационная безопасность человека: учебное пособие для вузов | Чернова Е. В.  | М.: Издательство Юрайт | 2022 |  | <https://urait.ru/bcode/495922> |

**8. Ресурсы информационно-телекоммуникационной сети «Интернет»:**

1. «НЭБ». Национальная электронная библиотека. – Режим доступа: [http://нэб.рф/](http://www.biblioclub.ru/)

2. «eLibrary». Научная электронная библиотека. – Режим доступа: [https://elibrary.ru](https://elibrary.ru/)

3. «КиберЛенинка». Научная электронная библиотека. – Режим доступа: <https://cyberleninka.ru/>

4. ЭБС «Университетская библиотека онлайн». – Режим доступа: [http://www.biblioclub.ru/](http://www.knigafund.ru/)

5. Российская государственная библиотека. – Режим доступа: <http://www.rsl.ru/>

**9. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ИСПОЛЬЗУЕМЫЕ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ:**

В ходе осуществления образовательного процесса используются следующие информационные технологии:

- средства визуального отображения и представления информации (LibreOffice) для создания визуальных презентаций как преподавателем (при проведении занятий) так и обучаемым при подготовке докладов для семинарского занятия.

- средства телекоммуникационного общения (электронная почта и т.п.) преподавателя и обучаемого.

- использование обучаемым возможностей информационно-телекоммуникационной сети «Интернет» при осуществлении самостоятельной работы.

**9.1. Требования к программному обеспечению учебного процесса**

Для успешного освоения дисциплины, обучающийся использует следующие программные средства:

* Windows 10 x64
* MicrosoftOffice 2016
* LibreOffice
* Firefox
* GIMP

**9.2. Информационно-справочные системы (при необходимости):**

Не используются

**10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий.

Для изучения дисциплины используется следующее оборудование: аудитория, укомплектованная мебелью для обучающихся и преподавателя, доской, ПК с выходом в интернет, мультимедийным проектором и экраном.

Для самостоятельной работы обучающихся используется аудитория, укомплектованная специализированной мебелью и техническими средствами (ПК с выходом в интернет и обеспечением доступа в электронно-информационно-образовательную среду организации).