Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение   
высшего образования «Новосибирский национальный исследовательский  
государственный университет» (Новосибирский государственный университет, НГУ)

**Факультет информационных технологий**

СОГЛАСОВАНО

Декан ФИТ НГУ

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ М.М. Лаврентьев

«03» июля 2019 г.

РАБОЧАЯ ПРОГРАММА Дисциплины

**Защита информации**

Направление подготовки: 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

Направленность (профиль): Компьютерные науки и системотехника

Форма обучения: очная

Год обучения: 4, семестр: 7

|  |  |  |
| --- | --- | --- |
| **№** | **Вид деятельности** | **Семестр** |
| **7** |
| **1** | Лекции, час. | 32 |
| **2** | Практические занятия, час. |  |
| **3** | Лабораторные занятия, час. | 32 |
| **4** | Занятий в контактной форме без учета промежуточной аттестации, час, из них | 64 |
| **5** | в электронной форме, час. |  |
| **6** | из них аудиторных занятий, час. | 64 |
| **7** | из них в активной и интерактивной форме, час. | 26 |
| **8** | консультаций, час. |  |
| **9** | Самостоятельная работа, час. | 42 |
| **10** | в том числе на выполнение письменных работ, час |  |
| **11** | Форма аттестации (экзамен, зачет, дифференцированный зачет), час | ДЗ, 2 |
| **12** | Всего зачетных единиц[[1]](#footnote-1) | 3 |

Новосибирск 2019

Рабочая программа дисциплины составлена на основании федерального государственного образовательного стандарта (ФГОС) высшего образования - бакалавриат по направлению подготовки 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА.

Федеральный государственный образовательный стандарт (ФГОС) высшего образования - бакалавриат по направлению подготовки 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА введен в действие приказом Минобрнауки от 19.09.2017 № 929.

Место дисциплины в структуре учебного плана: Блок 1 Дисциплины (модули), обязательная часть, обязательная дисциплина.

Рабочая программа дисциплины утверждена решением Ученого совета факультета информационных технологий от 02.07.2019, протокол № 75.

Программу разработали:

доцент кафедры компьютерных систем ФИТ,

кандидат технических наук Т.М.Пестунова

Заведующий кафедрой компьютерных систем ФИТ,

кандидат технических наук Б.Н. Пищик

Ответственный за образовательную программу:

доцент кафедры систем информатики ФИТ,

кандидат физико-математических наук Д.С. Мигинский

**Аннотация к рабочей программе дисциплины**

**«Защита информации»**

Дисциплина «Защита информации» реализуется в рамках образовательной программы высшего образования – программы бакалавриата 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА, направленность (профиль): Компьютерные науки и системотехника по очной форме обучения на русском языке.

**Место в образовательной программе:** Дисциплина «Защита информации» развивает знания, умения и навыки, сформированные у обучающихся по результатам изучения следующих дисциплин: «Объектно-ориентированное программирование», «Введение в дискретную математику и математическую логику».

Дисциплина «Защита информации» является базовой для прохождения производственной практики и написания выпускной квалификационной работы.

Дисциплина «Защита информации» реализуется в 7 семестре в рамках базовой части дисциплин (модулей) Блока 1 и является обязательной дисциплиной.

Дисциплина «Защита информации» направлена на формирование компетенций:

**УК 2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений**

УК 2.3. Владеть: методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта, навыками работы с нормативно-правовой документацией

**ОПК 3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности**

ОПК 3.1. Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК 3.2. Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК 3.3. Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

**ОПК 9. Способен осваивать методики использования программных средств для решения практических задач**

ОПК 9.1. Знать: классификацию программных средств и возможности их применения для решения практических задач

**Перечень основных разделов (тем) дисциплины:**

Тема 1. Основные понятия и концептуальные основы информационной безопасности.

Тема 2. Правовое обеспечение защиты информации.

Тема 3. Методологические и организационные аспекты защиты информации.

Тема 4. Типовые подсистемы и сервисы безопасности в информационных системах и компьютерных сетях.

Тема 5. Введение в криптографические методы защиты информации

Тема 6. Математические модели управления доступом и информационными потоками в компьютерных системах

Тема 7. Стандарты безопасности информационных технологий

Тема 8. Понятие безопасного программирования.

При освоении дисциплины предусмотрены лекции, лабораторные занятия, самостоятельная работа.

На лекциях рассматриваются методологические основы информационной безопасности, типовые угрозы и уязвимости, правовое регулирование и организационное обеспечение защиты информации, формирование требований по защите информации для информационных систем, в том числе информационных систем персональных данных, государственных информационных систем, объектах критической информационной инфраструктуры. Изучаются базовые криптографические методы, принципы и свойства дискреционных, мандатных и ролевых систем управления доступом в компьютерных системах. Даётся обзор стандартов информационной безопасности, классов защищённости, профилей защиты и оценочных уровней доверия. Обсуждаются принципы безопасного программирования, вопросы разработки безопасного программного обеспечения и создания защищённых информационных систем.

На практических занятиях студенты выполняют лабораторные работы по исследованию уязвимостей, моделированию угроз, программной реализации алгоритмов защиты информации, администрированию средств защиты информации, а также докладывают результаты своей аналитической работы. В учебном процессе используются активные и интерактивные формы занятий*.* На практических занятиях проводятся обсуждения результатов выполненных заданий в формате собеседования и докладов-презентаций, а также ряда практически значимых вопросов по заданной тематике. На лекциях проводятся экспресс-опросы, совместный анализ практических примеров, иллюстрирующих теоретические положения.

Самостоятельная работа включает: изучение учебного и информационного материала по тематике дисциплины, подготовку докладов, презентаций и отчётных работ по результатам лабораторных работ и самостоятельной домашней работы, подготовку к текущей и промежуточной аттестации.

Общий объем дисциплины – 3 зачетных единиц (108 часов).

**Правила аттестации по дисциплине.** Текущий контроль по дисциплине «Защита информации» осуществляется в форме защиты результатов лабораторных и аналитических работ с оценкой по 5-балльной системе «неудовлетворительно», «удовлетворительно», «хорошо», «отлично». Выполнение на положительную оценку всех предусмотренных программой лабораторных работ является необходимым условием успешного прохождения 1 этапа промежуточной аттестации к дифференцированному зачёту.

Промежуточная аттестация по дисциплине «Защита информации» проводится по завершению ее освоения в конце 7 семестра в форме дифференцированного зачёта, результаты которого оцениваются по шкале: «неудовлетворительно», «удовлетворительно», «хорошо», «отлично». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

Оценка за освоение дисциплины на дифференцированном зачёте выставляется на основе портфолио студента и письменного ответа на вопросы по билету. Портфолио включает: презентации и устные доклады по изучаемой тематике; отчёты о лабораторных работах. Вопросы билета составляются по тематике лекций, по его итогам студенты получают оценку за теорию по такой же шкале. Итоговая оценка определяется как среднее арифметическое баллов за портфолио и ответ по билету, в случае дробной части для округления в большую сторону преподаватель имеет право задать дополнительный вопрос.

Оценка «отлично» соответствует продвинутому уровню сформированности компетенции. Оценка «хорошо» соответствует базовому уровню сформированности компетенции. Оценка «удовлетворительно» соответствует пороговому уровню сформированности компетенции.

**Учебно-методическое обеспечение дисциплины.**

Учебно-методический комплекс по дисциплине «Защита информации» в электронной информационно-образовательной среде НГУ: <https://classroom.google.com/w/MTUzMjk4MTE1ODMy/t/all>

1. **Внешние требования к дисциплине**

Таблица 1.1

|  |
| --- |
| **Компетенция УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений** |
| У -2.3. Владеть: методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта, навыками работы с нормативно-правовой документацией |
| **Компетенция ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности** |
| ОПК-3.1. Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности |
| ОПК-3.2. Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности |
| ОПК-3.3. Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно- исследовательской работе с учетом требований информационной безопасности |
| **Компетенция ОПК-9. Способен осваивать методики использования программных средств для решения практических задач** |
| ОПК-9.1. Знать: классификацию программных средств и возможности их применения для решения практических задач |

1. **Требования к результатам освоения дисциплины**

Таблица 2.1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)** | | **Формы организации занятий** | | |
| **Лекции** | **Лабораторная** | **Самост. работа** |
| **УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений**  **УК-2.3.** Владеть: методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта, навыками работы с нормативно-правовой документацией | | | | |
| **1** | Иметь представление о современной проблематике информационной безопасности, как междисциплинарной предметной области, её роли в технологическом и социально-экономическом развитии общества, знать базовые понятия и определения. | + | + | + |
| **2** | Иметь представление об системе правового регулирования в области информационной безопасности в целом; знать сферу действия, основные положения и нормы соответствующих законов Российской Федерации и других базовых нормативно-правовых актов федерального уровня. | + | + | + |
| **3** | Знать методологические основы защиты информации: определение целей защиты информации, основные виды угроз безопасности информации и понятие модели угроз; принципы защиты информации, понятие и функции системы защиты информации, основные этапы создания системы защиты информации на основе оценки рисков. | + | + | + |
| **4** | Знать организационно-управленческие аспекты обеспечения информационной безопасности: понятие политики безопасности и её примерную структуру, задачи информационной безопасности во взаимосвязи с жизненным циклом информационных систем, типовые организационные меры по защиты информации. | + | + | + |
| **5** | Владеть навыками применения положений законодательства и требований нормативно-правовых документов по защите информации при проектировании, разработке, внедрении и эксплуатации информационных систем персональных данных, государственных информационных систем, объектов критической информационной инфраструктуры, а также при обеспечении личной информационной безопасности. | + | + | + |
| **ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно - коммуникационных технологий и с учетом основных требований ИБ**  **ОПК-3.1.** Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности | | | | |
| **6** | Иметь представление о принципах, моделях, методах и алгоритмах для решения задач защиты информации в компьютерных системах и сетях: знать формальные модели управления доступом в операционных системах и базах данных, основные принципы и примеры методов аутентификации, основные классы методов и примеры алгоритмов криптографической защиты информации, принципы и примеры алгоритмов стеганографии, принципы антивирусной защиты, обнаружения вторжений и мониторинга безопасности, принципы и примеры методов выявления уязвимостей и анализа защищённости. | + | + | + |
| **7.** | Знать суть понятия «безопасное программирование», угрозы информационной безопасности в процессе проектирования и разработки программного обеспечения, рекомендованные стандартом требования к организации процесса разработки безопасного ПО. | + | + | + |
|  | **ОПК-3.2.** Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности | | | |
| **8** | Уметь принимать участие в разработке программного обеспечения для решения задач защиты информации. | + | + | + |
| **9** | Уметь выявлять проблемы защиты информации при решении профессиональных задач, осуществлять обоснованный выбор необходимого системного и прикладного программного обеспечения, в контексте требований по защите информации. | + | + | + |
| **ОПК-3.3.** Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности | | | | |
| **10** | Владеть навыками освоения и применения для решения профессиональных задач средств защиты информации на примере доступных программных продуктов (встроенных сервисов безопасности операционных систем, средств криптографической защиты информации, средств анализа защищённости, обнаружения вторжений, VPN и др.) |  | + | + |
| **11** | Владеть профессиональной терминологией в области информационной безопасности и защиты информации, уметь правильно использовать её в письменных работах (при подготовке обзоров, рефератов, публикаций, докладов) и в устной речи. | + | + | + |
| **ОПК-9. Способен осваивать методики использования программных средств для решения практических задач**  **ОПК-9.1.** Знать: классификацию программных средств и возможности их применения для решения практических задач | | | | |
| **12** | Знать основные подсистемы и средства для решения задач защиты информации в автоматизированных (информационных) системах, их назначение и возможности. | + | + | + |
| **13** | Знать стандарты обеспечения безопасности информационных технологий, принципы разработки и возможности использования профилей защиты программного обеспечения. | + |  | + |
| **14** | Знать закреплённые нормативными документами принципы и методики классификации программного обеспечения информационных (автоматизированных) системы по классам (уровням) защищённости | + | + | + |
| **15** | Иметь представление о требованиях к мерам и средствам защиты информации в автоматизированных (информационных) системах различных классов (уровней) защищённости. | + | + | + |

**3. Содержание и структура учебной дисциплины**

Таблица 3.1

|  |  |  |  |
| --- | --- | --- | --- |
| **Темы лекций** | **Активные формы, час. (входит в общее кол-во часов)** | **Часы** | **Ссылки на результаты обучения** |
| **Семестр: 7** | | | |
| Тема 1. Основные понятия и концептуальные основы информационной безопасности. | 0 | 2 | **1, 3, 9** |
| Тема 2. Правовое обеспечение защиты информации. | 2 | 4 | **2, 5, 14** |
| Тема 3. Методологические и организационные аспекты защиты информации. | 2 | 4 | **3, 4, 9, 13** |
| Тема 4. Типовые подсистемы и средства обеспечения безопасности в информационных системах и компьютерных сетях. | 0 | 4 | **6, 9, 12** |
| Тема 5. Введение в криптографическую защиту информации и стеганографию | 2 | 6 | **6**, **8, 12** |
| Тема 6. Математические модели управления доступом и информационными потоками в компьютерных системах | 2 | 6 | **6, 8** |
| Тема 7. Стандарты безопасности информационных технологий. | 2 | 4 | **8, 12, 13, 15**, |
| Тема 8. Понятие безопасного программирования | 0 | 2 | **7, 8** |
| **Итого:** | **10** | **32** |  |

Таблица 3.2

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Темы лабораторных занятий** | **Активные формы, час.**  (входит в общее кол-во часов) | **Часы** | **Ссылки на результаты обучения** | **Учебная деятельность** |
| **Семестр: 7** | | | | |
| Тема 1. Основные понятия и концептуальные основы информационной безопасности. | 1 | 2 | **1, 3, 9** | Обучающиеся закрепляют основные понятия и принципы защиты информации на примерах, формируют тезаурус. Знакомятся с Интернет-ресурсами по угрозам, уязвимостям и средствам обеспечения информационной безопасности. Обсуждение в ходе группового опроса |
| Тема 2. Правовое обеспечение защиты информации. | 1 | 2 | **2, 5, 14** | Обучающиеся проводят анализ практических (модельных) примеров на применение положений законов и нормативно-правовых актов по защите информации; моделируют зависимости требований по защите информации от правового поля. Классифицируют информационные системы. |
| Тема 3. Методологические и организационные аспекты защиты информации. | 2 | 4 | **3, 4, 9, 11** | Обучающиеся выявляют угрозы и уязвимости web-систем для заданных ОС, СУБД и средств разработки web-приложения на основе анализа интернет-каталогов, выступают с краткими докладами, которые обсуждаются на занятии.  Выполняют анализ рисков и оценку актуальности угроз в информационных системах по стандартным методикам с разрабатывают модель угроз и выбирают необходимые меры защиты. |
| Тема 4. Типовые подсистемы и сервисы безопасности в информационных системах и компьютерных сетях. | 4 | 8 | **9, 12, 10, 11, 15** | Обучающиеся изучают базовые средства защиты информации в информационных системах: средства анализа защищённости (сетевые сканеры), сервисы безопасности в операционных системах и базах данных, осваивают на практике работу со средствами защиты от несанкционированного доступа к информации для решения задач аутентификации, управления доступом, аудита безопасности, обнаружения атак, антивирусной защиты. |
| Тема 5. Введение в криптографическую защиту информации и стеганографию | 6 | 12 | **6, 8, 10** | Обучающиеся решают задачи на основные понятия и методы шифрования, исследуют реализации криптоалгоритмов, методы стеганографического внедрения информации. Выполняют установку и администрирование программных средств криптографической защиты |
| Тема 8. Понятие безопасного программирования | 2 | 4 | **7, 8, 11** | Обучающиеся знакомятся с практическими аспектами применения принципов безопасного программирования и предотвращения уязвимостей при разработке ПО. Результаты представляется в форме эссе и обсуждаются на занятии. |
| **Итого:** | **16** | **32** |  |  |

1. **Самостоятельная работа студентов**

Таблица 4.1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№** | **Виды самостоятельной работы** | **Ссылки на результаты обучения** | **Часы на выполнение** | **Часы на консультации** | |
| **Семестр: 7** | | | | | |
| 1 | Подготовка к практическим занятиям по теме 1. | **1, 3, 9** | 4 |  | |
| Обучающиеся повторяют материал лекции 1, для самоконтроля выполняют тест по терминологии (<https://classroom.google.com/w/MTUzMjk4MTE1ODMy/t/all>). При необходимости следует воспользоваться ГОСТ 50922-2006 «Защита информации. Основные термины и определения». ГОСТ 51275-2006 «Факторы, воздействующие на информацию», ГОСТ Р 53114-2008 «Обеспечение информационной безопасности организации»). Далее нужно познакомиться с материалами об актуальных угрозах и уязвимостях на специализированных сайтах по информационной безопасности: [https://www.kaspersky.ru](https://www.kaspersky.ru/) (в частности, отчёт <https://tproger.ru/news/kaspersky-lab-industrial-report> и др.), [https://securelist.ru](https://securelist.ru/), [https://www.drweb.ru](https://www.drweb.ru/), [https://www.securitylab.ru](https://www.securitylab.ru/), <https://safe-surf.ru/>, <https://www.ptsecurity.com/ru-ru/research>, и др. По результатам изучения материалов (с учётом своего личного опыта) составить и аргументировать свою версию Тор-10 угроз, актуальных для организаций (группы организаций, отобранных по какому-либо признаку) или пользователей информационных технологий на текущий момент. Защита работы производится на занятии в форме устного сообщения с последующим обсуждением. | | | | |
| 2 | Подготовка к практическим занятиям по теме 2. | **2, 5, 14, 15** | 4 |  | |
| Обучающиеся повторяют материал лекций по данной теме. Знакомятся с назначением, сферой действия, базовой терминологией и основными положениями Федеральных законов, приведённых в списке нормативно-правовых документов. Постановлений правительства в области обеспечения безопасности в информационных систем персональных данных, категорирования объектов критической информационной инфраструктуры и приказом ФСТЭК России об обеспечении безопасности государственных информационных систем. Изучают классификацию информационных систем персональных данных и государственных информационных систем, принципы категорирования объектов критической инфраструктуры. Сравнивают требования к защите информации в информационных системах разной архитектуры и разных классов (уровней) защищённости. | | | | |
| 3 | Подготовка к практическим занятиям по теме 3. | **3, 4, 9, 11** | 10 |  | |
| * + - 1. Изучить каталоги актуальных уязвимостей Open Web Application Security Project (OWASP), Web Application Security Consortium(WASC), ссылки на которые приведены в списке литературы (раздел «информационные источники»). Ознакомиться с соответствующими классификациями уязвимостей. Ответить на контрольные вопросы и дать описания распространённых типов атак. Выбрать вариант комплекса средств создания web-приложений (ОС, СУБД, средство разработки программного кода) из числа предложенных вариантов, определить для него известные уязвимости и возможные атаки. Подробное задание и методические рекомендации по подготовке отчётности и презентаций представлены в приложении к рабочей программе дисциплины: <https://classroom.google.com/w/MTUzMjk4MTE1ODMy/t/all>. На занятии результаты представляются в форме краткого сообщения (доклада с презентацией) с последующим общим обсуждением.       2. В соответствии с вариантом модельной информационной системы организации классифицировать её в соответствии с требованиями законодательства, построить проект модели угроз. Применив одну из изученных методик оценки рисков, определить актуальные угрозы. При формировании модели угроз рекомендуется использовать Базовую модель угроз безопасности в информационных системах персональных данных (доступна на сайте ФСТЭК России fstec.ru) и банк данных угроз bdu.fstec.ru. Отчётность оформляется в форме проекта модели угроз. Консультации и защита задания проводятся на занятиях.       3. Разработать одну из частных политик безопасности для изученной информационной системы (варианты определяется по согласованию с преподавателем). Разработанный проект документа представляется включается в отчёт | | | | |
| 4 | Подготовка к практическим занятиям по теме 4 | **10, 11, 12, 15** | 12 |  | |
| Обучающиеся изучают учебные материалы, техническую документацию, информационные источники на сайтах производителей средств защиты информации для подготовки к выполнению лабораторных работ, связанных с установкой и администрированием средств защиты информации:  - типовые сервисы безопасности, встроенные в операционные системы Windows и Linux доступных версий.  - типовые функции средств анализа уязвимостей (сканеров безопасности).  - типовые функции антивирусных систем, средств обнаружения вторжений и межсетевых экранов;  Методические указания к выполнению лабораторных работ размещаются и актуализируются на <https://classroom.google.com/w/MTUzMjk4MTE1ODMy/t/all>  Оформляют отчётность по итогам выполнения лабораторных работ. Отчёты о выполнении лабораторных работ защищаются индивидуально. | | | | |
| 5 | Подготовка к практическим занятиям по теме 5. | **6, 8, 10** | 8 | |  |
| Обучающиеся повторяют материал лекций, основные понятия и методы криптографии. Знакомятся с отечественными криптографическими стандартами, приведёнными в списке литературы. Для подготовки к лабораторной работе осуществляют выбор реализуемых криптографических средств защиты информации, анализируют особенности изученных криптоалгоритмов, формулирует концепцию их реализации на одном из языков программирования, готовят отчётность по лабораторной работе для защиты. Для подготовки к лабораторной работе выбирают программные средства внедрения цифровой информации и стегоанализа (напр., свободное ПО **OpenStego**), анализируют особенности алгоритмов стеганографии в контексте их программной реализации, готовятся отчётность о выполнении лабораторной работы для защиты.  Изучают принципы создания, особенности структуры и применения виртуальных частных сетей, в частности, методические материалы по установке, администрированию программных средств криптографической защиты информации, построения инфраструктуры открытых ключей с целью шифрования информации и формирования электронной подписи. Знакомятся со средствами построения VPN-сетей. Методические материалы размещаются и актуализируются на ресурсе <https://classroom.google.com/w/MTUzMjk4MTE1ODMy/t/all>. Для решения задач берётся программное обеспечение, ссылки на которое даны ниже в соответствующем разделе данной рабочей программы. Необходимая техническая документация берётся с сайтов производителей. | | | | |
| 6 | Подготовка к практическим занятиям по теме 8. | **7, 8, 11** | 4 | |  |
| Обучающиеся повторяют материал лекций, изучают РД Гостехкомиссии о классификации программного обеспечения по уровню контроля отсутствия недекларированных возможностей, требования к использованию методов безопасного программирования и анализу уязвимостей при разработке программного обеспечения защиты информации в ГОСТ Р 15408 -2013 (ч.3.), детализации анализа уязвимостей в соответствии с ГОСТ Р 58142-2018 (ч.1 и ч.2), угрозы безопасности при разработке программного обеспечения в соответствии с ГОСТ 58412—2019, общие требования к разработке безопасного программного обеспечения в соответствии с ГОСТ Р 56939-2016, требования к процессу создания автоматизированных систем в защищённом исполнении в соответствии с ГОСТ 51583-2000. Опираясь на нормативно-правовую документацию, материалы лекций и доступные интернет-ресурсы формируют свое понимание безопасного программирования, эссе по теме и подготавливаются к обсуждению его на занятиях. Методические материалы по теме размещены: <https://classroom.google.com/w/MTUzMjk4MTE1ODMy/t/all>. | | | | |
|  | **Итого:** |  | **42** |  | |

1. **Образовательные технологии**

В ходе учебного процесса по дисциплине проводятся лекционные и практические (лабораторные) занятия. Как правило, знания по вопросам, рассматриваемым на лекциях и изучаемые самостоятельно, закрепляются и углубляются на практических (лабораторных) занятиях, при этом уровень формирования компетенций повышается за счёт получения опыта практического применения изученных теоретических положений и методик, освоения программного инструментария для решения задач защиты информации и самостоятельной программной реализации некоторых алгоритмов защиты информации. По вопросам, вызывающим затруднения, проводятся консультации.

На лекциях излагаются основные концептуальные, нормативно-правовые, методологические и математические положения в соответствии с изучаемой тематикой. В целях закрепления новых понятий, подходов, методов проводятся экспресс-опросы с последующим анализом допущенных ошибок, совместный анализ проблем на примере приближённых к реалиям модельных ситуаций.

В ходе практических (лабораторных) занятий работа студентов выполняется в следующих формах:

- подготовка аналитических отчётов, докладов, презентаций по заданной тематике на основе изучения нормативно-правовых актов, учебной и научной литературы, поисковой работы в интернет с использованием профессиональных интернет-ресурсов по информационной безопасности;

- установка, конфигурирование и администрирование программного обеспечения для решения задач защиты информации (выполняется, как правило, на виртуальных машинах, доступных в компьютерных классах; виртуальные машины с изучаемыми средствами или непосредственно изучаемое программное обеспечение могут быть установлены также в ряде случаев и на личные ноутбуки обучающихся, что позволяет часть работы выполнять дома);

- разработка типовой документации, необходимой в процессе создания и эксплуатации систем информационной безопасности;

- программная реализация алгоритмов защиты информации;

- защита результатов выполненных работ в публичной (выступления с докладами и презентациями в форме конференций с последующим осуждением доложенных результатов всеми студентами) или индивидуальной (собеседования с преподавателем) формах.

В ходе реализации учебного процесса по дисциплине применяются такие формы проведения практических занятий, как дискуссии, обсуждение и защита результатов работы, а также применяются следующие интерактивные формы обучения (таблица 5.1).

Таблица 5.1

|  |  |  |
| --- | --- | --- |
| **1** | Технологии проблемного обучения | УК-2.3 ОПК-3.2, ОПК – 3.3, ОПК-9.1. |
| **Формируемые умения:** **5.** Владеть навыками применения положений законодательства и требований нормативно-правовых документов по защите информации при проектировании, разработке, внедрении и эксплуатации информационных систем персональных данных, государственных информационных систем, объектов критической информационной инфраструктуры, а также при обеспечении личной информационной безопасности. **1**. Иметь представление о современной проблематике и понятийном аппарате информационной безопасности, как междисциплинарной предметной области, её роли в технологическом и социально-экономическом развитии общества. **3.** Знать методологические основы защиты информации: определение целей защиты информации, основные виды угроз безопасности информации и понятие модели угроз; принципы защиты информации, понятие и функции системы защиты информации, основные этапы создания системы защиты информации на основе оценки рисков. **8**. Уметь принимать участие в разработке программного обеспечения для решения задач защиты информации. **9.** Уметь выявлять проблемы защиты информации при решении профессиональных задач, осуществлять обоснованный выбор необходимого системного и прикладного программного обеспечения, в контексте требований по защите информации. **11.** Владеть профессиональной терминологией в области информационной безопасности и защиты информации, уметь правильно использовать её в письменных работах (при подготовке обзоров, рефератов, эссе, публикаций, докладов) и в устной речи. **14.** Знать закреплённые нормативными документами принципы и методики классификации информационных (автоматизированных) системы по классам (уровням) защищённости | | |
| **Краткое описание применения:** активизация познавательной деятельности студента за счет ассоциации собственного опыта с предметом изучения: постановка самостоятельно или под руководством преподавателя проблемных задач из профессиональной деятельности ИТ-специалиста, в том числе на основе собственного жизненного опыта студентов, и активная самостоятельная деятельность обучающихся по их разрешению, сопровождающаяся обсуждением результатов. | | |
| **2** | Портфолио | УК-2.3. ОПК-3.1. ОПК-3.2. ОПК-3.3.  ОПК-9.1. |
| **Формируемые умения:** **5.** Владеть навыками применения положений законодательства и требований нормативно-правовых документов по защите информации при проектировании, разработке, внедрении и эксплуатации информационных систем персональных данных, государственных информационных систем, объектов критической информационной инфраструктуры, а также при обеспечении личной информационной безопасности. **3.** Знать методологические основы защиты информации: определение целей защиты информации, основные виды угроз безопасности информации и понятие модели угроз; принципы защиты информации, понятие и функции системы защиты информации, основные этапы создания системы защиты информации на основе оценки рисков. **4.** Знать организационно-управленческие аспекты обеспечения информационной безопасности: понятие политики безопасности и её примерную структуру, задачи информационной безопасности во взаимосвязи с жизненным циклом информационных систем, типовые организационные меры по защите информации. **7.** Знать суть понятия «безопасное программирование», угрозы информационной безопасности в процессе проектирования и разработки программного обеспечения, рекомендованные стандартом требования к организации процесса разработки безопасного ПО. **8.** Уметь принимать участие в разработке программного обеспечения для решения задач защиты информации. **10**. Владеть навыками освоения и применения для решения профессиональных задач средств защиты информации на примере доступных программных продуктов (встроенных сервисов безопасности ОС, средств криптографической защиты информации, средств анализа защищённости, обнаружения вторжений, VPN и др.) **11**. Владеть профессиональной терминологией в области информационной безопасности и защиты информации, уметь правильно использовать её в письменных работах (при подготовке обзоров, рефератов, эссе, публикаций, докладов) и в устной речи. **15.** Иметь представление о требованиях к мерам и средствам защиты информации в автоматизированных (информационных) системах различных классов (уровней) защищённости | | |
| **Краткое описание применения:** студенты ведут портфолио (коллекцию работ), которое учитывается при проведении аттестации по дисциплине. | | |
| **2** Индивидуальное обучение:ОПК 3.2. ОПК 3.3. | | |
| **Формируемые умения:** **8.** Уметь принимать участие в разработке программного обеспечения для решения задач защиты информации. **9.** Уметь выявлять проблемы защиты информации при решении профессиональных задач, осуществлять обоснованный выбор необходимого программного обеспечения, в контексте требований по защите информации. **10.** Владеть навыками освоения и применения для решения профессиональных задач средств защиты информации на примере доступных программных продуктов (встроенных сервисов безопасности ОС, средств криптографической защиты информации, средств анализа защищённости, обнаружения вторжений, VPN и др.) | | |
| **Краткое описание применения:** выстраивание студентом собственной образовательной траектории на основе формирования индивидуальной образовательной программы с учетом интересов студента за счёт предоставляемых возможностей выбора объектов, методов и инструментария при выполнении аналитических и практических работ по изучаемым тематикам с учетом интересов . | | |

Для организации и контроля самостоятельной работы студентов, а также проведения консультаций применяются информационно-коммуникационные технологии (таблица 5.2).

Таблица 5.2

|  |  |
| --- | --- |
| Информирование | <https://classroom.google.com/w/MTUzMjk4MTE1ODMy/t/all>,  официальные адреса групп студентов на \*@g.nsu.ru |
| Консультирование | [t.pestunova@g.nsu.ru](mailto:t.pestunova@g.nsu.ru), [ptm@ngs.ru](mailto:ptm@ngs.ru) (лекции)  a[.perov@g.nsu.ru](mailto:.perov@g.nsu.ru), [perov\_artem@inbox.ru](mailto:perov_artem@inbox.ru), (практика)  a[.balabanov@g.nsu.ru](mailto:.balabanov@g.nsu.ru), [baatob@gmail.com](mailto:baatob@gmail.com). (практика) |
| Контроль | Все задания, выносимые на контроль в рамках практических (лабораторных) занятий сдаются преподавателю в компьютерном классе во время занятий.  Отчётность, предоставляемая в рамках выполнения практических заданий, может предоставляться в электронном виде по адресам, указанным в строке «консультирование» |
| Размещение учебных материалов | <https://classroom.google.com/w/MTUzMjk4MTE1ODMy/t/all> |

**6. Правила аттестации студентов по учебной дисциплине**

По дисциплине «Защита информации» проводится текущая и промежуточная аттестация (итоговая по дисциплине).

Текущий контроль по дисциплине «Защита информации» осуществляется в форме защиты результатов выполненных лабораторных работ и аналитических заданий на практических занятиях. Защита проводится индивидуально и заключается в презентации и защите докладов по основным разделам дисциплины, по итогам которых выставляется оценка по 4-балльной шкале «неудовлетворительно», «удовлетворительно», «хорошо», «отлично». Выполнение на положительную оценку всех предусмотренных программой лабораторных работ является необходимым условием успешного прохождения 1 этапа промежуточной аттестации к дифференцированному зачёту.

Промежуточная аттестация по дисциплине «Защита информации» проводится по завершению ее освоения в конце 7 семестра в форме дифференцированного зачёта. Результаты промежуточной аттестации по дисциплине оцениваются по 4-балльной шкале «неудовлетворительно», «удовлетворительно», «хорошо», «отлично». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

Оценка за освоение дисциплины в рамках дифференцированного зачёта выставляется по результатам оценивания портфолио работ студента и результатов контрольного задания по теоретическому (лекционному) материалу, выполняемого непосредственно в ходе проведения дифференцированного зачёта.

Портфолио включает в себя работы, выполненные в рамках лабораторных занятий и самостоятельной работы:

1) презентации и устные доклады на темы, соответствующие разделам дисциплины;

2) устные и (или) письменные отчёты о результатах лабораторных и аналитических работ.

За каждый артефакт портфолио выставляется оценка Oi по 5-балльной шкале, где i=1,2,.., Nпр , Nпр — количество оцениваемых артефактов портфолио по итогам практикума, исходя из следующих критериев.

«Отлично» (5 баллов): задание выполнено полностью и правильно, все выводы корректно убедительно аргументированы, грамотно изложены (в письменном и / или устном виде), аккуратно оформлены (для письменных артефактов и презентаций), студентом корректно используется профессиональная терминология, правильно формулируются понятия и категории предметной области дисциплины, студентом продемонстрирован высокий уровень владения материалом по теме задания на содержательном уровне, при подготовке используется актуальная литература и качественно подобранные интернет-источники. Для заданий в письменном виде допускаются отдельные незначительные погрешности оформления, не снижающие общего впечатления от выполненной работы.

«Хорошо» (4 балла): недостаточно полное раскрытие темы, отдельные ошибки при выполнении и объяснении процесса выполнения и полученных результатов, которые студент способен исправить самостоятельно или при небольшой подсказке преподавателя; несущественные ошибки в опреде­лении понятий и категорий, а также в аргументации решений и выводов, карди­нально не меняющих правильную суть изложе­ния; частичное использование неактуальных источников, незначительные погрешности грамотности изложения

«Удовлетворительно» (3 балла): общая правильная направленность действий в рамках выполнения задания, неполная и не всегда убедительная аргументация, наличие существенных ошибок и (или) множественных несущественных ошибок в определении понятий и в содержательной части работы, использование значительной части устаревшей учебной литературы и других источников, неполнота ответа, неспособность целостно осветить проблематику вопроса. Частично способен исправить ошибки при подсказке преподавателя.

«Неудовлетворительно» (0 баллов): недоведенное до конца выполнение задания, качественно неверный результат; большое количество существенных ошибок в процессе выполнения, неправильное (неубедительное) объяснение результатов или отсутствие такого объяснения; необоснованная и некачественная подборка литературы и информационных источников; слабое знание или незнание профессиональной терминологии, неспособность осветить пробле­матику вопроса, неспособность исправить ошибки даже при наводящей подсказке преподавателя.

В конце семестра определяется итоговый балл за портфолио (**Oпр)** как среднее арифметическое значение от количества баллов за каждый артефакт:

**Oпр =** (O1  + O2 + … + ONпр)/Nпр.

Контрольное занятие по теоретическому (лекционному) материалу на дифференцированном зачёте проводится по билетам в письменной форме по тематике лекций, по итогам студенты получают оценку за теорию, которая также нормируется в 5-балльную шкалу (**Oт**).

При аттестации по билетам студенту выдается билет с 6 вопросами, оценка определяется в зависимости количества правильных и полных ответов на поставленные вопросы в соответствии со следующими критериями.

«отлично» (5 баллов) — если не менее чем на 5 вопросов даны правильные аргументированные ответы (в правильном ответе допускается одна несущественная ошибка, которую студент смог самостоятельно исправить при указании на нее преподавателем), ответ на оставшийся вопрос может быть неполным, но с правильным общим направлением мысли;

«хорошо» (4 балла) — если студент ответил правильно на 4 вопроса, при ответе остальные вопросы допустил существенные ошибки при общем правильном направлении мысли, один вопрос может остаться без ответа;

«удовлетворительно» (3 балла) — если имеет место одна из двух ситуаций: а) студент смог правильно ответить на 3 вопроса, а на три других либо не ответил, либо допустил существенные ошибки; б) студент попытался ответить более, чем на 3 вопроса, не менее двух ответов правильные или почти правильные (с 1-2 несущественными ошибками), а остальные не доведены до конца, но при этом как минимум в ответах на два из них присутствует правильное общее направление мысли.

Итоговая оценка **O** за освоение дисциплины определяется как среднее арифметическое количества баллов за теорию и практику **O**= (**Oпр + Oт**) / 2. При возникновении дробной части для принятия решения об округлении в б***о***льшую сторону преподаватель имеет право задать дополнительный вопрос.

Оценка «отлично» соответствует продвинутому уровню сформированности компетенции.

Оценка «хорошо» соответствует базовому уровню сформированности компетенции.

Оценка «удовлетворительно» соответствует пороговому уровню сформированности компетенции.

В таблице 6.1 представлено соответствие форм аттестации заявляемым требованиям к результатам освоения дисциплины.

Таблица 6.1

|  |  |  |  |
| --- | --- | --- | --- |
| **Коды компетенций ФГОС** | **Результаты обучения** | **Формы аттестации** | |
| **Портфолио** | **Дифференци-рованный зачет** |
| **УК-2** | **УК 2.3.** Владеть методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта, навыками работы с нормативно-правовой документацией | **+** | **+** |
| **ОПК-3** | **ОПК 3.1.** Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности | **+** | **+** |
| **ОПК 3.2.** Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности | **+** |  |
| **ОПК 3.3.** Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности | **+** |  |
| **ОПК 9** | **ОПК 9.1.** Знать: классификацию программных средств и возможности их применения для решения практических задач | **+** | **+** |

Требования к структуре и содержанию портфолио, оценочные средства, а также критерии оценки сформированности компетенций и освоения дисциплины в целом, представлены в Фонде оценочных средств, являющемся приложением 1 к настоящей рабочей программе дисциплины.

**7. Литература**

1. Нестеров, С.А. Основы информационной безопасности : учебное пособие (бакалавриат) / С.А. Нестеров .— 4-е изд., стереот. — Москва : Лань, 2018 .— 324 с. ; [Электронный ресурс]. - URL: <https://e.lanbook.com/book/103908#authors>

2. Ковалев, Д.В. Информационная безопасность : учебное пособие / Д.В. Ковалев, Е.А. Богданова ; Министерство образования и науки РФ, Южный федеральный университет. - Ростов-на-Дону : Издательство Южного федерального университета, 2016. - 74 с. : схем., табл., ил. - Библиогр. в кн. - ISBN 978-5-9275-2364-1 ; То же [Электронный ресурс]. - URL: [http://biblioclub.ru/index.php?page=book&id=493175](https://mail.ngs.ru/Redirect/biblioclub.ru/index.php?page=book&id=493175)

3. Скрипник, Д.А. Общие вопросы технической защиты информации / Д.А. Скрипник. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: [http://biblioclub.ru/index.php?page=book&id=429070](https://mail.ngs.ru/Redirect/biblioclub.ru/index.php?page=book&id=429070)

4. Спицын, В.Г. Информационная безопасность вычислительной техники : учебное пособие / В.Г. Спицын ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). - Томск : Эль Контент, 2011. - 148 с. : ил.,табл., схем. - ISBN 978-5-4332-0020-3 ; То же [Электронный ресурс]. - URL: [http://biblioclub.ru/index.php?page=book&id=208694](https://mail.ngs.ru/Redirect/biblioclub.ru/index.php?page=book&id=208694)

5. Лапонина, О.Р. Криптографические основы безопасности / О.Р. Лапонина. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 244 с. : ил. - (Основы информационных технологий). - Библиогр. в кн. - ISBN 5-9556-00020-5 ; То же [Электронный ресурс]. - URL: [http://biblioclub.ru/index.php?page=book&id=429092](https://mail.ngs.ru/Redirect/biblioclub.ru/index.php?page=book&id=429092)

6. Лапонина, О.Р. Межсетевые экраны : учебное пособие / О.Р. Лапонина. - 2-е изд., исправ. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 466 с. : ил. ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=429093>

7.Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - Москва ; Берлин : Директ-Медиа, 2015. - 253 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=276557>

7.Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - Москва ; Берлин : Директ-Медиа, 2015. - 253 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557

8. Тушко, Т.А. Информатика : учебное пособие / Т.А. Тушко, Т.М. Пестунова ; Сибирский федеральный университет. – Красноярск : Сибирский федеральный университет (СФУ), 2017. – 204 с. : ил. - Библиогр. в кн. – ISBN 978-5-7638-3604-2 ; – URL: <https://biblioclub.ru/index.php?page=book&id=497738>

*Интернет-ресурсы*

Таблица 7.1

|  |  |  |
| --- | --- | --- |
| № п/п | Наименование Интернет-ресурса | Краткое описание |
| 1 | Безопасность информационных технологий / - [Электронный ресурс] / Режим доступа: <https://bit.mephi.ru/index.php/bit/index> |  |
| 2 | Вестник УрФО. Безопасность в информационной сфере/ - [Электронный ресурс] / Режим доступа: [http://www.info-secur.ru](http://www.info-secur.ru/) |
| 3 | Category:OWASP Top Ten Project [Электронный ресурс] / Режим доступа: <https://www.owasp.org/index.php/Top_10_2013-Top_10> – Загл. с экрана | Открытый проект по анализу уязвимостей (с 2013 года). |
| 4 | The WASC Threat Classification v2.0 ENG - [Электронный ресурс] / Режим доступа: <http://projects.webappsec.org/w/page/13246978/Threat%20Classification> - Загл. с экрана | Ресурс по классификации угроз безопасности Web- приложений, поддержи-ваемый консорциумом “The Web Application” Security Consortium |
| 5 | CVE. Common Vulnerabilities and Exposures. - [Электронный ресурс] / Режим доступа: <http://cve.mitre.org/> - Загл. с экрана | База стандартных идентификаторов для общеизвестных ИТ-уязвимостей |
| 6 | Банк данных угроз безопасности информации - [Электронный ресурс] / Режим доступа: <http://bdu.fstec.ru/> - Загл. с экрана | Банк данных угроз безопасности информации в ИС, уязвимостей программного обеспечения и аппаратных платформ. Официальный ресурс ФСТЭК России. |
| 7 | ФСТЭК России. Федеральная служба по техническому и экспортному контролю Российской федерации - [Электронный ресурс] / Режим доступа: <https://fstec.ru/> - Загл. с экрана | Официальный сайт ФСТЭК России. |
| 8 | Федеральная безопасности Российской федерации - [Электронный ресурс] / Режим доступа: <http://www.fsb.ru/> - Загл. с экрана | Официальный сайт ФСБ России. |
| 9 | Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. - [Электронный ресурс] / Режим доступа: <https://rkn.gov.ru/> -Загл. с экрана | Официальный сайт . Роскомнадзора |
| 10 | Управление Роскомнадзора по Сибирскому федеральному округу. - [Электронный ресурс] / Режим доступа: [http://54.rkn.gov.ru](http://54.rkn.gov.ru/) - Загл. с экрана | Официальный сайт территор. управл. Роскомнадзора |
| 11 | Росстандарт. - [Электронный ресурс] / Режим доступа: <https://www.gost.ru/portal/gost/> - Загл. с экрана | Официальный сайт Федер. агентства по техническому регулированию. |
| 12 | IB-BANK.RU. Отраслевой портал. - [Электронный ресурс] / Режим доступа : https://ib-bank.ru/ - Загл. с экрана | Отраслевой портал по ИБ в финансовой сфере |
| 13 | BIS Journal − Информационная безопасность банков / - [Электронный ресурс] / Режим доступа: <https://journal.ib-bank.ru/journal> - Загл. с экрана | Электронный журнал по ИБ в банковской сфере |
| 14 | SecurityLab.ru by Positive Technology− Информационная безопасность банков / - [Электронный ресурс] / Режим доступа https://www.securitylab.ru/ - Загл. с экрана | Информац. порталы о событиях в сфере защиты информации, интернет-права, уязвимостях, угрозах, инцидентах и методах защиты информации. |
| 15 | Kaspersky Lab. Secure List. - [Электронный ресурс] / Режим доступа [https://securelist.ru](https://securelist.ru/), - Загл. с экрана |
| 16 | Безопасность пользователей в сети Интернет - [Электронный ресурс] / Режим доступа: <https://safe-surf.ru/> - Загл. с экрана |
| 17 | AM. Anti-malware. - [Электронный ресурс] / Режим доступа <https://www.anti-malware.ru/security> - Загл. с экрана |
| 18 | Positive Technology. - [Электронный ресурс]\* / Режим доступа <https://www.ptsecurity.com/ru-ru/> - Загл. с экрана | Информация о сертифицированных. средствах защиты информации на сайтах производителей.  \*Примечание: также статьи и аналитика по информационной безопасности, материалы вебинаров. |
| 19 | Kaspersky Lab. Secure List. - [Электронный ресурс] / Режим доступа : [https://www.kaspersky.ru](https://www.kaspersky.ru/) - Загл. с экрана |
| 20 | Dr. Web. Антивирус - [Электронный ресурс] / Режим доступа : [https://www.drweb.ru](https://www.drweb.ru/) - Загл. с экрана |
| 21 | Infotecs. - [Электронный ресурс]\* / Режим доступа : https://infotecs.ru/ - Загл. с экрана |
| 22 | РУСБИТЕХ. - [Электронный ресурс] / Режим доступа <http://rusbitech.ru/> - Загл. с экрана |
| 23 | Директор по безопасности - [Электронный ресурс] / Режим доступа: <http://www.s-director.ru/magazine/latestnumber.html> | Специализированное издание по корпоративной безопасности |
| 24 | Информационная безопасность - [Электронный ресурс] / Режим доступа: <http://www.itsec.ru/> | Периодическое информационно-справочное издание для ИТ- и ИБ-директоров |
| 25 | Лаборатория пен-теста.- [Электронный ресурс] / Режим доступа: https://habr.com/ru/company/pentestit/blog/332902/ | Интерактивый виртуальный полигон для практического знакомства с активными методами анализа уязвимостей |

**8. Учебно-методическое и программное обеспечение дисциплины**

**8.1. Учебно-методическое обеспечение**

Пестунова Т.М. Защита информации [Электронный ресурс] : электронный учебно-методический комплекс / Т.М.Пестунова ; Новосиб. гос. ун-т. - Новосибирск [2018] - Режим доступа: <https://classroom.google.com/w/MTUzMjk4MTE1ODMy/t/all> - Загл. с экрана.

**8.2. Программное обеспечение**

Для обеспечения реализации дисциплины используются:

- стандартный комплект программного обеспечения (ПО), включающий регулярно обновляемое лицензионное ПО Windows и MS Office;

- Файловый архиватор 7-Zip v16.04;

- Офисный пакет **LibreOffice v6.х;**

- Браузеры: Google Chrome, Internet Explorer, Mozilla Firefox;

- Программа просмотра электронных публикаций в формате PDF**: Adobe Acrobat Reader DC v15.020.**

Перечень специализированного программного обеспечения для изучения дисциплины представлен в таблице 8.1. В случае появления в течение семестра возможности использования в учебном процессе нового программного обеспечения (например, в результате заключения соответствующих договоров с производителями), оно также может рассматриваться в процессе изучения курса. Порядок доступа к нему доводится до студентов в рабочем порядке.

Таблица 8.1

Специализированное программное обеспечение

|  |  |  |
| --- | --- | --- |
| **№** | **Наименование ПО** | **Назначение** |
| 1 | Microsoft Visual Studio Professional 2019 | Среда разработки приложений |
| 2 | Eclipse 2019 | Среда разработки приложений |
| 3 | OpenVPN v2.3.11 | Технологии виртуальной частной сети |
| 4 | **Oracle VM VirtualBox 6.0.10** | Программный продукт виртуализации для операционных систем |
| 5 | 7-Zip v16.04 | Средство свободной файловой архивации с высокой степенью сжатия данных |
| 6 | **LibreOffice v6.x** | [Офисный пакет](https://ru.wikipedia.org/wiki/%D0%9E%D1%84%D0%B8%D1%81%D0%BD%D1%8B%D0%B9_%D0%BF%D0%B0%D0%BA%D0%B5%D1%82) |
| 7 | **Gpg4win Vanilla** | Средство криптографической защиты и шифрования файлов |

\***Примечание:** программное обеспечения со свободными лицензиями. Скачивается студентами самостоятельно, устанавливается на виртуальные машины с использованием доступного в классах программного обеспечения для виртуализации (Oracle VM VirtualBox 6.0.10), после чего запускается в любом компьютерном классе.

**9. Профессиональные базы данных и информационные справочные системы**

1. Электронная библиотека диссертаций Российской государственной библиотеки (ЭБД РГБ)
2. Лицензионные материалы на сайте eLibrary.ru
3. Правовая БД «Консультант Плюс»
4. Правовая БД «Гарант»

**10. Материально-техническое обеспечение**

Таблица 10.1

|  |  |  |
| --- | --- | --- |
| **№** | **Наименование** | **Назначение** |
| 1 | Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления) | Для проведения лекционных занятий |
| 2 | Компьютерный класс (с выходом в Internet) | Для проведения лабораторных занятий и организации самостоятельной работы обучающихся |

Материально-техническое обеспечение образовательного процесса по дисциплине для обучающихся из числа лиц с ограниченными возможностями здоровья осуществляется согласно «Порядку организации и осуществления образовательной деятельности по образовательным программам для инвалидов и лиц с ограниченными возможностями здоровья в Новосибирском государственном университете».

**Лист актуализации рабочей программы дисциплины  
«Защита информации»**

|  |  |  |  |
| --- | --- | --- | --- |
| № | Характеристика внесенных изменений (с указанием пунктов документа) | Дата и №  протокола Ученого совета ФИТ | Подпись  ответственного |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. С учетом выделенных часов на промежуточную аттестацию [↑](#footnote-ref-1)