Межгосударственное образовательное учреждение высшего образования

«Белорусско-Российский университет»

|  |
| --- |
| УТВЕРЖДАЮ |
| Первый проректор Белорусско-Российского университета |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Ю.В. Машин |
| «\_\_\_»\_\_\_\_\_\_\_\_ 2021г. |
| Регистрационный № УД-\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/р |

**ЗАШИТа ИНФОРМАЦИИ**

(наименование дисциплины)

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Направление подготовки** 09.03.04 Программная инженерия

**Направленность (профиль)** Разработка программно-информационных систем

**Квалификация** Бакалавр

|  |  |
| --- | --- |
|  | **Форма обучения** |
| **Очная** |
| Курс | **3** |
| Семестр | 6 |
| Лекции, часы | 16 |
| Лабораторные занятия, часы | 34 |
| Экзамен, семестр | 6 |
| Контактная работа по учебным занятиям, часы | 50 |
| Самостоятельная работа, часы | 58 |
| Всего часов / зачетных единиц | 108/3 |

Кафедра-разработчик программы: Программное обеспечение информационных технологий

Составитель: В .В Кутузов, к.т.н., Е. А. Зайченко

Могилев, 2021

Рабочая программа составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 09.03.04 «Программная инженерия» (уровень бакалавриата), утвержденным приказом № \_920\_\_ от \_\_19.09.2017 г. и учебным планом, утвержденным Рег. № 090304-4 от 27.12.2019

Рассмотрена и рекомендована к утверждению кафедрой «Программное обеспечение информационных технологий»

«16» марта 2021 г., протокол № 7.

Зав. кафедрой ПОИТ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ В. В. Кутузов

Одобрена и рекомендована к утверждению Научно-методическим советом Белорусско-Российского университета

«16» июня 2021 г., протокол № 7.

Зам. председателя

Научно-методического совета \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ С.А. Сухоцкий

Рецензент:

\_\_Начальник управления информационных технологий ОАО «Лента» Миренков С. В.\_

(И.О. Фамилия, должность, ученая степень, ученое звание рецензента)

Рабочая программа согласована:

Ведущий библиотекарь \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Начальник учебно-методического

отдела \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ В.А. Кемова

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
   1. Цель учебной дисциплины

Цель учебной дисциплины - обучение студентов основным методам обеспечения информационной безопасности, средствам защиты информации, современным аппаратным и программным алгоритмам шифрования информации, построения надежных систем хранения информации, а также изучение перспективных направлений в развитии современных средств обеспечения информационной безопасности.

* 1. Планируемые результаты изучения дисциплины

В результате освоения учебной дисциплины студент должен

**знать**:

* основные понятия информационной безопасности;
* требования к системам защиты информации;
* принципы построения систем защиты информации;
* основные алгоритмы шифрования информации;
* методы проверки подлинности составляющих информационного процесса

**уметь**:

* проектировать структуру и выбирать составные компоненты систем защиты данных;
* применять методы и средства защиты компьютерной информации;
* оценивать надежность методов защиты компьютерной информации

**владеть**:

* навыками для оценки надежности методов защиты компьютерной информации;
* методологией проверки подлинности составляющих информационного процесса;
* технологией обеспечения информационной безопасности компьютерных систем
  1. Место учебной дисциплины в системе подготовки студента

Дисциплина относится к блоку 1 «Дисциплины (модули). Обязательная часть блока 1».

Перечень учебных дисциплин, изучаемых ранее, усвоение которых необходимо для изучения данной дисциплины:

* Технологии разработки программного обеспечения;
* ЭВМ и периферийные устройства.

Перечень учебных дисциплин (циклов дисциплин), которые будут опираться на данную дисциплину:

* Проектирование программного обеспечения (7 семестр);
* Современные системы программирования.
  1. Требования к освоению учебной дисциплины

Освоение данной учебной дисциплины должно обеспечивать формирование сле­дующих компетенций:

|  |  |
| --- | --- |
| Коды форми­руемых компе­тенций | Наименования формируемых компетенций |
| **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 |

1. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Вклад дисциплины в формирование результатов обучения выпускника (компетенций) и достижение обобщенных результатов обучения происходит путём освоения содержания обучения и достижения частных результатов обучения, описанных в данном разделе.

* 1. Содержание учебной дисциплины

|  |  |  |  |
| --- | --- | --- | --- |
| Номер тем | Наименование тем | Содержание | Коды формируемых компетенций |
|  | Основы информационной безопасности, методов и средств защиты информации | Основы информационной безопасности, методов и средств защиты информации. Методы и средства защиты информации. Рекомендуемая литература. Основные понятия и терминология  информационной безопасности. Цель и объект защиты информации. Задачи в сфере обеспечения информационной безопасности. Виды информации. Классификация видов информации. Информационные системы. Классификация. Нарушители информационной безопасности. Методы защиты информации. Классификация средства защиты информации. | ОПК-3 |
|  | Правовое и нормативное обеспечение защиты информации | Правовое и нормативное обеспечение защиты информации. Комплексный подход к обеспечению защиты объектов информационной безопасности. Классификация методов защиты информации. Законодательная база Республики Беларусь. Стандарты и рекомендации в области информационной безопасности, применяемых в рамках реализации цифровой повестки Евразийского экономического союза. Законодательная база Российской Федерации. Международное законодательство в области информационной безопасности. Стандарты ISO в области IT-безопасности | ОПК-3 |
|  | Защита персональных данных | Персональные данные. Термины и определения. Защита персональных данных. Законодательство по защите персональных данных. Обработка персональных данных. Операторы персональных данных. Утечки персональных данных. | ОПК-3 |
|  | Угрозы информационной безопасности | Уязвимости информации. Угрозы. Угрозы информационной безопасности. Задачи организационного обеспечения защиты информации. Классификация угроз информационной безопасности. Основные направления и методы реализации угроз. Типовые модели нарушителя для различных категорий лиц. Методики оценки и моделирования угроз. Базы и банки данных угроз безопасности информации | ОПК-3 |
|  | Управление рисками  Информационной безопасности | Управление рисками информационной безопасности. Риск ориентированный подход. Общая концепция управления рисками информационной безопасности. Карты рисков. Логика снижения уровня риска до приемлемого уровня. Классификации рисков. Ущерб от реализации атаки. Методологии риск-менеджмента. Методики оценки рисков информационной безопасности | ОПК-3 |
|  | Политика информационной безопасности в организациях | Политика информационной безопасности в организациях. Безопасность предприятия. Обеспечение безопасности организации и её персонала. Служба безопасности предприятия (организации). Функции службы безопасности. Пример структур служб безопасности. Электронные средства охраны, безопасности и контроля. Политика безопасности предприятия (организации). Рекомендуемые области разработки политики информационной безопасности | ОПК-3 |
|  | Критическая инфраструктура.  Критическая информационная инфраструктура | Критическая инфраструктура. Критическая информационная инфраструктура. Законодательство. История атак на критическую инфраструктуру. Атаки и меры защиты. | ОПК-3 |
|  | Идентификация, аутентификация и авторизация | Идентификация, аутентификация и авторизация. Общие сведения. Классификация средств идентификации и аутентификации с точки зрения применяемых технологий. Технологии аутентификации. Двухфакторная аутентификация. Протоколы аутентификации. Биометрическая аутентификация. Аутентификация с помощью одноразовых паролей. Аутентификация с использованием токенов. Применение криптографических алгоритмов при идентификации и аутентификации | ОПК-3 |
|  | Криптография | Криптография. Применение криптографических средств защиты информации. Шифры. Классификация криптографических алгоритмов. Примеры алгоритмов. Криптография с симметричными ключами. Криптография с асимметричными ключами. Средства криптографической защиты информации. Криптография на практике | ОПК-3 |
|  | Электронная цифровая подпись | Электронная цифровая подпись. Электронная цифровая подпись для аутентификации данных. Алгоритмы электронной цифровой подписи. Стандарты цифровой подписи. Практика применения электронной цифровой подписи. | ОПК-3 |
|  | Защита информации в операционных системах | Защита информации в операционных системах. Общие принципы безопасности операционных систем. Защита компьютерной информации в операционных системах Linux и Windows. Угрозы безопасности операционных систем. Средства защиты информации в операционных системах | ОПК-3 |
|  | Сетевые атаки и защита информации в компьютерных сетях | Сетевые атаки и защита информации в компьютерных сетях. Особенности обеспечения информационной безопасности в компьютерных сетях. Основы компьютерных сетей. Угрозы безопасности в компьютерных сетях. Классификация сетевых (удаленных) атак. Протоколы. Виды сетевых атак. DoS \DDoS Атаки. Программно-аппаратные средства защиты компьютерных систем. Межсетевые экраны (Firewall). VPN. Proxy. SSH туннели. Tor. Antivirus. Мониторинг ИТ-инфраструктуры. Программное обеспечение. Программно-аппаратные средства защиты компьютерных систем. | ОПК-3 |
|  | Защита internet ресурсов, сайтов | Защита internet ресурсов, сайтов. OWASP (Open Web Application Security Project) | ОПК-3 |

* 1. Учебно-методическая карта учебной дисциплины

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № недели | Лекции  (наименование тем) | Часы | Практические(семинарские) занятия | Часы | Лабораторные занятия | Часы | Самостоятельная работа, часы | Форма контроля знаний | Баллы (max) |
| Модуль 1 | | | | | | | | | |
| 1 | **Тема 1.** Системная методология информационной безопасности  **Тема 2.** Правовое и нормативное обеспечение защиты информации | 2 |  |  | Л.р. № 1. Хеширование информации | 2 | 3 | ЗЛР | 6 |
| 2 |  |  |  |  | Л.р. № 2. Шифрование данных в ОС Linux | 2 | 3 |  |  |
| 3 | **Тема 3.** Защита персональных данных **Тема 4.** Угрозы информационной безопасности | 2 |  |  | Л.р. № 2. Шифрование данных в ОС Linux | 2 | 2 | ЗЛР | 6 |
| 4 |  |  |  |  | Л.р. № 3. Разграничение прав доступа в ОС Linux | 2 | 2 |  |  |
| 5 | **Тема 5.** Управление рисками информационной безопасности. **Тема 6.** Политика информационной безопасности в организациях | 2 |  |  | Л.р. № 3. Разграничение прав доступа в ОС Linux | 2 | 2 | ЗЛР | 6 |
| 6 |  |  |  |  | Л.р. № 4. Возможности файловых подсистем Linux для защиты информации | 2 | 2 |  |  |
| 7 | **Тема 7.** Критическая инфраструктура. Критическая информационная инфраструктура | 2 |  |  | Л.р. № 4. Возможности файловых подсистем Linux для защиты информации | 2 | 2 | ЗЛР | 6 |
| 8 |  |  |  |  | Л.р. № 5. Обеспечение целостности и доступности данных с использованием Raid, LVM. | 2 | 2 | ЗЛР  ПКУ | 6  30 |
| Модуль 2 | | | | | | | | | |
| 9 | **Тема 8.** Идентификация, аутентификация и авторизация  **Тема 9** Криптография | 2 |  |  | Л.р. № 6. Изучение методов шифрования ОС Windows данных на дисках | 2 | 2 | ЗЛР | 6 |
| 10 |  |  |  |  | Л.р. № 7. Средства защиты данных в ОС Windows | 2 | 2 |  |  |
| 11 | **Тема 10.** Электронная цифровая подпись.  **Тема 11**. Защита информации в операционных системах | 2 |  |  | Л.р. № 7. Средства защиты данных в ОС Windows | 2 | 2 | ЗЛР | 8 |
| 12 |  |  |  |  | Л.р. № 8. Изучение методов аудита ОС Windows | 2 | 2 |  |  |
| 13 | **Тема 12.** Сетевые атаки и защита информации в компьютерных сетях | 2 |  |  | Л.р. № 8. Изучение методов аудита ОС Windows | 2 | 2 | ЗЛР | 8 |
| 14 |  |  |  |  | Л.р. № 9. Основы MS Crypto API | 2 | 2 |  |  |
| 15 | **Тема 13.** Защита internet ресурсов, сайтов | 2 |  |  | Л.р. № 9. Основы MS Crypto API | 2 | 2 | ЗЛР | 8 |
| 16 |  |  |  |  | Л.р. № 9. Основы MS Crypto API | 2 | 2 |  |  |
| 17 |  |  |  |  | Л.р. № 9. Основы MS Crypto API | 2 | 2 |  |  |
| 18-20 |  |  |  |  |  |  | 36 | ПА  (экзамен) | 40 |
| ИТОГО | | 16 |  |  |  | 34 | 58 |  | 100 |

Принятые обозначения:

Текущий контроль –

ЗЛР – защита лабораторной работы.

ПКУ – промежуточный контроль успеваемости.

ПА – промежуточная аттестация

Итоговая оценка определяется как сумма текущего контроля и промежуточной аттестации и соответствует баллам:

Экзамен

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Оценка | Отлично | Хорошо | Удовлетворительно | Неудовлетворительно |
| Баллы | 87-100 | 65-86 | 51-64 | 0-50 |

1. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

При изучении дисциплины используется модульно-рейтинговая система оценки знаний. Применение форм и методов проведения занятий при изучении различных тем курса представлено в таблице.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№**  **п/п** | **Форма проведения занятия** *\** | **Вид аудиторных занятий** | | **Всего часов** |
| **Лекции** | **Лабораторные занятия** |
| 1 | Мультимедиа | Темы 1-13 |  | 16 |
| 3 | С использованием ЭВМ |  | Л.р. №№1 - Л.р. №9 | 34 |
|  | **ИТОГО** | 16 | 34 | 50 |

1. ОЦЕНОЧНЫЕ СРЕДСТВА

Используемые оценочные средства по учебной дисциплине представлены в таблице и хранятся на кафедре.

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Вид оценочных средств** | **Количество комплектов** |
| 1 | Вопросы к экзамену | 1 |
| 2 | Экзаменационные билеты | 1 |
| 3 | Вопросы для защиты лабораторных работа | 9 |

1. МЕТОДИКА И КРИТЕРИИ ОЦЕНКИ КОМПЕТЕНЦИЙ СТУДЕНТОВ
   1. Уровни сформированности компетенций

|  |  |  |  |
| --- | --- | --- | --- |
| **№**  **п/п** | **Уровни сформированности компетенции** | **Содержательное описание уровня** | **Результаты обучения** |
| 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. Способен применять принципы, методы и средства решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности | | | | |
| 1 | Пороговый уровень | Понимает способы и протоколы безопасной передачи данных в сети. Может оценить криптостойскость разрабатываемого программного обеспечения | Документирование алгоритмов по примерам лабораторных работ |
| 2 | Продвинутый уровень | Владеет теоретическими знаниями информационной безопасности. и умеет реализовывать их в виде про­граммного кода. | Способен решать стандартные задачи профессиональной деятельности на основе информационной культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. |
| 3 | Высокий  уровень | Способен использовать алгоритмы хеширования, электронной цифровой подписи и ассиметричного шифрования, осуществлять оценку криптоскойсти системы и модели­ровать атаку злоумышленника | Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Способность тестировать разрабатываемое программное обеспечение на наличие уязвимостей и устранять возможность атаки полным перебором |

* 1. Методика оценки знаний, умений и навыков студентов

|  |  |
| --- | --- |
| Результаты обучения | Оценочные средства\* |
| *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 | |
| Способен выполнять документирование алгоритмов по примерам лабораторных работ | Вопросы для защиты лабораторных работ. Вопросы к экзамену |
| Способен решать стандартные задачи профессиональной деятельности на основе информационной культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. | Вопросы для защиты лабораторных работ. Вопросы к экзамену |
| Способен тестировать разрабатываемое программное обеспечение на наличие уязвимостей и устранять возможность атаки полным перебором | Вопросы для защиты лабораторных работ. Вопросы к экзамену |

* 1. Критерии оценки лабораторных работ

Студент обязан самостоятельно в полном объеме выполнить лабораторные работы согласно рабочей программе.

Задание на работы выдает ведущий занятия преподаватель.

По результатам выполнения работ студент обязан оформить отчет по лабораторной работе в соответствии с действующими в Университете требованиями по оформлению отчета.

Отсутствие отчета является причиной недопуска к сдаче лабораторной работы.

Защита отчета проводится устно, путем ответов на контрольные вопросы к работе, решения задачи по теме лабораторной работы и демонстрации навыков, полученных при выполнении работы.

При защите лабораторной работы студент имеет право пользоваться собственноручно оформленным отчетом.

При отсутствии ответов на заданные преподавателем вопросы отчет не засчитывается и баллы не выставляются.

Правильные ответы оцениваются согласно оценочным уровням сформированности компетенций по изучаемой теме.

Каждая выполненная и защищенная работа оцениваются до 6-8 баллов, в зависимости от качества оформления и уровня знаний студента по тематике работы. Если по окончанию модуля лабораторная работа выполнена, но не защищена, то баллы по ней не начисляются, и она попадает в разряд задолженности.

1. Критерии оценки экзамена

**5.4.1.** К сдаче экзамена допускаются студенты, получив за семестр в сумме не менее 36 баллов. На экзамене студент может набрать от 0 до 40 баллов. Студенты сдают экзамен в комбинированной форме. Количество баллов, набранных студентом, рассчитывается как сумма баллов, полученных за четыре компонента экзамена: письменный ответ на первый теоретический вопрос (от 0 до 10 баллов); письменный ответ на второй теоретический вопрос (от 0 до 10 баллов), решение задачи в письменном виде (от 0 до 10 баллов) и устные ответы на дополнительные вопросы (от 0 до 10 баллов).

**5.4.2. Оценка ответа на теоретический вопрос**

**10 баллов – десять:**

– систематизированные, глубокие и полные знания по всем разделам учебной программы, а также по основным вопросам, выходящим за ее пределы;

– точное использование научной терминологии (в том числе – на иностранном языке), стилистически грамотное, логически правильное изложение ответа на вопросы;

– безупречное владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке и решении научных и профессиональных задач;

– выраженная способность самостоятельно и творчески решать сложные проблемы в нестандартной ситуации;

– полное и глубокое усвоение основной и дополнительной литературы, рекомендованной учебной программой дисциплины;

– умение ориентироваться в теориях, концепциях и направлениях по изучаемой дисциплине и давать им критическую оценку, использовать научные достижения других дисциплин.

**9 баллов – девять:**

– систематизированные, глубокие и полные знания по всем разделам учебной программы;

– точное использование научной терминологии (в том числе на иностранном языке), стилистически грамотное, логически правильное изложение ответа на вопросы;

– владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке и решении научных и профессиональных задач;

– способность самостоятельно и творчески решать сложные проблемы в нестандартной ситуации в рамках учебной программы;

– полное усвоение основной и дополнительной литературы, рекомендованной учебной программой дисциплины;

– умение ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им критическую оценку.

**8 баллов – восемь:**

– систематизированные, глубокие и полные знания по всем поставленным вопросам в объеме учебной программы;

– использование научной терминологии, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы;

– владение инструментарием учебной дисциплины (методами комплексного анализа, техникой информационных технологий), умение его использовать в постановке и решении научных и профессиональных задач;

– способность самостоятельно решать сложные проблемы в рамках учебной программы;

– усвоение основной и дополнительной литературы, рекомендованной учебной программой;

– умение ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им критическую оценку.

**7 баллов – семь:**

– систематизированные, глубокие и полные знания по всем разделам учебной программы;

– использование научной терминологии (в том числе на иностранном языке), лингвистически и логически правильное изложение ответа на вопросы, умение делать обоснованные выводы;

– владение инструментарием учебной дисциплины, умение его использовать в постановке и решении научных и профессиональных задач;

– усвоение основной и дополнительной литературы, рекомендованной учебной программой дисциплины;

– умение ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им критическую оценку.

**6 баллов – шесть:**

– достаточно полные и систематизированные знания в объеме учебной программы;

– использование необходимой научной терминологии, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы;

– владение инструментарием учебной дисциплины, умение его использовать в решении учебных и профессиональных задач;

– способность самостоятельно применять типовые решения в рамках учебной программы;

– усвоение основной литературы, рекомендованной учебной программой дисциплины;

– умение ориентироваться в базовых теориях, концепциях и направлениях по изучаемой дисциплине и давать им сравнительную оценку.

**5 баллов – пять:**

– достаточные знания в объеме учебной программы;

– использование научной терминологии, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать выводы;

– владение инструментарием учебной дисциплины, умение его использовать в решении учебных и профессиональных задач;

– способность самостоятельно применять типовые решения в рамках учебной программы;

– усвоение основной литературы, рекомендованной учебной программой дисциплины;

– умение ориентироваться в базовых теориях, концепциях и направлениях по изучаемой дисциплине и давать им сравнительную оценку.

**4 балла – четыре, зачтено:**

– достаточный объем знаний в рамках образовательного стандарта;

– усвоение основной литературы, рекомендованной учебной программой дисциплины;

– использование научной терминологии, стилистическое и логическое изложение ответа на вопросы, умение делать выводы без существенных ошибок;

– владение инструментарием учебной дисциплины, умение его использовать в решении стандартных (типовых) задач;

– умение под руководством преподавателя решать стандартные (типовые) задачи;

– умение ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им оценку.

**3 балла – три, незачтено:**

– недостаточно полный объем знаний в рамках образовательного стандарта;

– знание части основной литературы, рекомендованной учебной программой дисциплины;

– использование научной терминологии, изложение ответа на вопросы с существенными лингвистическими и логическими ошибками;

– слабое владение инструментарием учебной дисциплины, некомпетентность в решении стандартных (типовых) задач;

– неумение ориентироваться в основных теориях, концепциях и направлениях изучаемой дисциплины.

**2 балла – два, незачтено:**

– фрагментарные знания в рамках образовательного стандарта:

– знания отдельных литературных источников, рекомендованных учебной программой дисциплины;

– неумение использовать научную терминологию дисциплины, наличие в ответе грубых стилистических и логических ошибок.

**1 балл – один, незачтено:**

– Отсутствие знаний и компетенций в рамках образовательного стандарта или отказ от ответа.

1. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ И ВЫПОЛНЕ­НИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Самостоятельная работа студентов (СРС) направлена на закрепление и углубление освоения учебного материала, развитие практических умений. СРС включает следующие виды самостоятельной работы студентов:

Перечень контрольных вопросов и заданий для самостоятельной работы студентов хранится на кафедре.

Виды самостоятельной работы

* проработка тем (вопросов), вынесенных на самостоятельное изучение;
* конспектирование учебной литературы;
* подготовка докладов;
* подготовка презентаций;
* подготовка рефератов.

Для СРС рекомендуется использовать источники, приведенные в п. 7.

1. УЧЕБНО- МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ
   1. Основная литература

|  |  |  |  |
| --- | --- | --- | --- |
| №  п/п | Библиографическое описание | Гриф*\*\*\** | Количество  экземпляров |
| 1 | Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации: учеб. пособие / А.П. Жук и др. - 3-е изд., - Москва: РИОР:ИНФРА-М, 2021. – 400 с [Электронный ресурс, режим доступа [http://www.znanium.com]](http://www.znanium.com]/). | Рек. УМО по образованию в области информационных технологий и систем связи в качестве учебного пособия для студентов высших учебных заведений» | znanium.com |
| 2 | Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2021. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1013711 (дата обращения: 18.04.2021). | Рек. Межрегиональным учебно-методическим советом профессионального образования в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению подготовки 10.03.01 «Информационная безопасность» (квалификация «бакалавр») | znanium.com |

* 1. Дополнительная литература

|  |  |  |  |
| --- | --- | --- | --- |
| №  п/п | Библиографическое описание | Гриф | Количество  экземпляров |
| 1 | Герман, О. Н. Теоретико-числовые методы в крип­тографии : учебник для студентов вузов / О. Н. Герман, Ю. В. Нестеренко. - М. : Академия, 2012. - 272с | Учебник создан в соответствии с ФГОС по направлениям подготовки "Информационная безопасность" и "Математика" | 2 |
| 2 | Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189326 (дата обращения: 18.04.2021). | Допущено Учебно-методическим объединением по образованию в области прикладной информатики в качестве учебного пособия для студентов, обучающихся по направлению «Прикладная информатика» | znanium.com |
| 3 | Информационная безопасность сетей и систем: пособие / В. И. Аверченков  [и др.]. – Могилев: Белорус.-Рос. ун-т, 2020. – 212 с. | Рекомендовано УМО по образованию в области информатики и радиоэлектроники в качестве пособия для специальности 1 -53 01 02 “Автоматизированные системы обработки информации” Президиума Совета УМО по образованию в области информатики и радиоэлектроники) | 50 |
| 4 | Мельников, В. П. Информационная безопасность и защита информации : учеб. пособие для вузов / В.  П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - 6-е изд., стер. - М. : Академия, 2012. - 336с | Рек. МО и науки РФ в качестве учеб. пособия для студентов вузов | 1 |
| 5 | Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. — 3-е изд., испр. и доп. — Москва : ИНФРА-М, 2021. — 327 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1035570. - ISBN 978-5-16-015471-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189342 (дата обращения: 15.05.2021). – Режим доступа: по подписке. |  | znanium.com |

1. Перечень ресурсов сети Интернет по изучаемой дисциплине

<http://moodle.bru.by> – Образовательный портал Белорусско-Российского университета;

<http://e.biblio.bru.by/> – Электронная библиотека Белорусско-Российского университета;

<https://znanium.com/> – Электронно-библиотечная система Znanium;

<https://stepik.org/catalog> – Российская образовательная платформа и конструктор бесплатных открытых онлайн-курсов и уроков;

<https://openedu.ru> – Открытое образование

<https://habr.com/ru/> – Хабр. Публикации по ИТ тематикам;

1. **Перечень наглядных и других пособий, методических рекомендаций по про­ведению учебных занятий, а также методических материалов к используемым в об­разовательном процессе техническим средствам**
2. Методические рекомендации

Защита информации. Методические рекомендации к лабораторным работам для студентов направлений подготовки 09.03.04 «Программная инженерия» и 09.03.01 «Информатика и вычислительная техника». – Могилёв, 2021 (электронный вариант).

1. Информационные технологии

Мультимедийные презентации

Тема 1. Основы информационной безопасности, методов и средств защиты информации

Тема 2. Правовое и нормативное обеспечение защиты информации

Тема 3. Защита персональных данных

Тема 4. Угрозы информационной безопасности

Тема 5. Управление рисками информационной безопасности

Тема 6. Политика информационной безопасности в организациях

Тема 7. Критическая инфраструктура. Критическая информационная инфраструктура

Тема 8. Идентификация, аутентификация и авторизация

Тема 9. Криптография

Тема 10. Электронная цифровая подпись

Тема 11. Защита информации в операционных системах

Тема 12. Сетевые атаки и защита информации в компьютерных сетях

Тема 13. Защита internet ресурсов, сайтов

1. Перечень программного обеспечения, используемого в образовательном процессе
2. Виртуальная машина Hyper-V (свободно распространяемое ПО).
3. Microsoft Office (лицензионное ПО)

.

**8 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ**

Материально-техническое обеспечение дисциплины содержится в паспорте лаборатории а. 517/2 , рег. № паспорта лаборатории № ПУЛ - 4 517/2-20; в паспорте лаборатории а. 518/2 , рег. № паспорта лаборатории № ПУЛ - 4 518/2-20.

ЗАЩИТА ИНФОРМАЦИИ

(наименование дисциплины)

АННОТАЦИЯ

К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

**Направление подготовки** 09.03.04 Программная инженерия

**Направленность (профиль)** Разработка программно-информационных систем

**Квалификация** Бакалавр

|  |  |
| --- | --- |
|  | **Форма обучения** |
| **Очная** |
| Курс | 3 |
| Семестр | 6 |
| Лекции, часы | 16 |
| Лабораторные занятия, часы | 34 |
| Экзамен, семестр | 6 |
| Контактная работа по учебным занятиям, часы | 50 |
| Самостоятельная работа, часы | 58 |
| Всего часов / зачетных единиц | 108/3 |

1 Цель учебной дисциплины

Цель учебной дисциплины - обучение студентов основным методам обеспечения информационной безопасности, средствам защиты информации, современным аппаратным и программным алгоритмам шифрования информации, построения надежных систем хранения информации, а также изучение перспективных направлений в развитии современных средств обеспечения информационной безопасности.

1. Планируемые результаты изучения дисциплины

В результате освоения учебной дисциплины студент должен

**знать**:

* основные понятия информационной безопасности;
* требования к системам защиты информации;
* принципы построения систем защиты информации;
* основные алгоритмы шифрования информации;
* методы проверки подлинности составляющих информационного процесса

**уметь**:

* проектировать структуру и выбирать составные компоненты систем защиты дан­ных;
* применять методы и средства защиты компьютерной информации;
* оценивать надежность методов защиты компьютерной информации

**владеть**:

* навыками для оценки надежности методов защиты компьютерной информации;
* методологией проверки подлинности составляющих информационного процесса;
* технологией обеспечения информационной безопасности компьютерных систем

1. Требования к освоению учебной дисциплины

Освоение данной учебной дисциплины должно обеспечивать формирование сле­дующих компетенций:

|  |  |
| --- | --- |
| Коды форми­руемых компе­тенций | Наименования формируемых компетенций |
| **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 |

1. Образовательные технологии

Мультимедиа, С использованием ЭВМ и сеть бесшовного wi-fi и системы идентификации пользователей.