

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
филиал федерального государственного бюджетного образовательного учреждения
высшего образования «Мурманский арктический государственный университет»
в г. Апатиты

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.08 Защита информации

(название дисциплины (модуля) в соответствии с учебным планом)

**основной профессиональной образовательной программы
по направлению подготовки**

**09.03.02 Информационные системы и технологии
направленность (профиль): «Программно-аппаратные комплексы»**

(код и наименование направления подготовки
с указанием направленности (профиля) (наименования магистерской программы))

высшее образование – бакалавриат

уровень профессионального образования: высшее образование – бакалавриат / высшее образование –
специалитет, магистратура / высшее образование – подготовка кадров высшей квалификации

бакалавр

квалификация

очная

форма обучения

2019

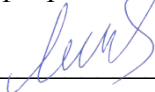
год набора

Составитель:

Федоров А.М., канд. техн. наук,
доцент кафедры информатики и
вычислительной техники

Утверждено на заседании кафедры
информатики и вычислительной техники
(протокол № 13 от «06» июня 2019 г.)

Зав. кафедрой



Яковлев С.Ю.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ) - обзор современных проблем в сфере информационной безопасности в информационных системах, а также обзор направлений развития программы информационной безопасности России.

В результате изучения дисциплины обучающийся должен:

знать:

- принципы построения и архитектуру вычислительных систем;
- виды контента информационных ресурсов предприятия и Интернет-ресурсов;
- основы безопасности жизнедеятельности в области профессиональной деятельности;
- методы и средства обеспечения информационной безопасности компьютерных систем;
- базовые понятия и определения, используемые в сфере информационной безопасности;
- основные угрозы безопасности информации и возможные способы их реализации, а также методы и средства противодействия этим угрозам.

уметь:

- ставить и решать схемотехнические задачи, связанные с выбором системы элементов при заданных требованиях к параметрам (временным, мощностным, габаритным, надежностным);
- проектировать, внедрять и организации эксплуатацию ИС и ИКТ; моделировать, анализировать и совершенствовать бизнес-процессы разрабатывать конкретные предложения по результатам исследований, готовить справочно-аналитические материалы для принятия управленческих решений;
- применять на практике собственные и классические алгоритмы криптографической защиты данных.

владеть:

- методами проектирования, разработки и реализации технического решения в области создания систем управления контентом Интернет-ресурсов и систем управления контентом предприятия;
- основными методами защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий;
- иметь представление о моделях безопасности ИС.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В результате освоении содержания дисциплины «Защита информации» обучающийся должен обладать следующими компетенциями:

- способность применять системный подход и математические методы в формализации решения прикладных задач, моделировать прикладные (бизнес) процессы и предметную область автоматизации организации (ПК-2);
- способность эксплуатировать и сопровождать информационные системы и сервисы, осуществлять ведение информационных хранилищ для решения прикладных задач профессиональной деятельности (ПК-3).

3. УКАЗАНИЕ МЕСТА ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Данная дисциплина относится к формируемой участниками образовательных отношений блока Б1 дисциплин основной образовательной программы бакалавриата по направлению подготовки 09.03.02 Информационные системы и технологии направленность (профиль) Программно-аппаратные комплексы.

Для освоения данной дисциплины обучающиеся используют знания, умения, навыки, способы деятельности и установки, которые они получили в процессе изучения дисциплин: «Информатика», «Программирование», «Управление данными», «Информационные технологии», «Операционные системы», «Мультимедиа технологии»

В свою очередь, «Защита информации» представляет собой методологическую базу для усвоения обучающимися содержания дисциплин: «Технологии обработки информации», «Методы и средства проектирование информационных систем и технологий», а также для подготовки и защиты выпускной квалификационной работы.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ С УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ИЛИ АСТРОНОМИЧЕСКИХ ЧАСОВ, ВЫДЕЛЕННЫХ НА КОНТАКТНУЮ РАБОТУ ОБУЧАЮЩИХСЯ С ПРЕПОДАВАТЕЛЕМ (ПО ВИДАМ УЧЕБНЫХ ЗАНЯТИЙ) И НА САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ

Общая трудоемкость дисциплины составляет 4 зачетные единицы или 144 часа.
(из расчета 1 ЗЕТ= 36 часов).

Курс	Семестр	Трудоемкость в ЗЕТ	Общая трудоемкость (час.)	Контактная работа			Всего контактных часов	Из них в интерактивной форме	Кол-во часов на СРС	Курсовые работы	Кол-во часов на контроль	Форма контроля
				ЛК	ПР	ЛБ						
4	7	4	144	32	-	32	64	10	44	-	36	экзамен
Итого:		4	144	32	-	32	64	10	44	-	36	экзамен

В интерактивной форме часы используются в виде: обратной связи.

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ, СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ИЛИ АСТРОНОМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

№ п/п	Наименование раздела, темы	Контактная работа			Всего контактных часов	Из них в интерактивной форме	Кол-во часов на СРС	Кол-во часов на контроль
		ЛК	ПР	ЛБ				
1.	Понятие Информационной безопасности. Введение	2	-	2	4	-	5	-
2.	Законодательный уровень информационной безопасности	2	-	2	4	-	5	-
3.	Наиболее распространенные угрозы информационной безопасности	4	-	4	8	2	-	-
4.	Распространение объектно-ориентированного подхода на ИБ	2	-	2	4	1	5	-
5.	Административный уровень информационной безопасности	2	-	2	4	-	5	-

№ п/п	Наименование раздела, темы	Контактная работа			Всего контактных часов	Из них в интерактивной форме	Кол-во часов на СРС	Кол-во часов на контроль
		ЛК	ПР	ЛБ				
6.	Процедурный уровень информационной безопасности	2	-	2	4	-	-	-
7.	Основные программно-технические меры безопасности информации	2	-	2	4	2	5	-
8.	Основные программно-технические меры безопасности информации: идентификация и аутентификация; управление доступом	2	-	2	4	2	5	-
9.	Основные программно-технические меры безопасности информации: протоколирование, аудит, шифрование, контроль целостности, электронная цифровая подпись	2	-	2	4	-	-	-
10.	Основные программно-технические меры безопасности информации: Экранирование, Анализ защищенности	2	-	2	4	2	5	-
11.	Криптография: шифрование и обеспечение целостности	4	-	4	8	1	5	-
12.	Протоколирование и аудит, шифрование, контроль целостности	4	-	4	8	-	4	-
13.	Антивирусная защита компьютерных систем "	2	-	2	4	-	-	-
	Экзамен	-	-	-	-	-	-	36
	Итого:	32	-	32	64	10	44	36

Содержание дисциплины:

Тема	Содержание
Тема 1 "Понятие Информационной безопасности"	Базовые понятия и определения, используемые в сфере информационной безопасности. Роль справочно-аналитических материалов в принятии управленческих решений. Представление о моделях безопасности ИС.
Тема 2 "Законодательный уровень информационной безопасности"	Методы и средства обеспечения информационной безопасности компьютерных систем. Разработка макетов справочно-аналитических материалов для принятия управленческих решений на основе законодательного уровня ИБ. Основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий
Тема 3 "Наиболее распространенные угрозы информационной безопасности"	Основы безопасности жизнедеятельности в области профессиональной деятельности. Принципы проектирования, внедрения и эксплуатации в организации ИС и ИКТ. Методы проектирования, разработки и

Тема	Содержание
	реализации технического решения в области создания систем управления контентом Интернет-ресурсов и систем управления контентом предприятия.
Тема 4 "Распространение объектно-ориентированного подхода на ИБ"	Основные понятия объектно-ориентированного подхода. О необходимости объектно-ориентированного подхода к информационной безопасности. Применение объектно-ориентированного подхода к рассмотрению защищаемых систем.
Тема 5 Административный уровень информационной безопасности	Методы и средства обеспечения информационной безопасности компьютерных систем на административном уровне ИБ. Обзор справочно-аналитических материалов для принятия управленческих решений на административном уровне. Основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий
Тема 6 "Процедурный уровень информационной безопасности"	Методы и средства обеспечения информационной безопасности компьютерных систем на процедурном уровне. Проектирование, внедрение и эксплуатация в организации ИС и ИКТ на процедурном уровне.
Тема 7 "Основные программно-технические меры безопасности информации"	Основные угрозы безопасности информации и возможные способы их реализации, а также методы и средства противодействия этим угрозам. Постановка и решение схемотехнических задач, связанных с выбором системы элементов при заданных требованиях к параметрам (временным, мощностным, габаритным, надежностным). Знакомство с методами проектирования, разработки и реализации технического решения в области создания систем управления контентом Интернет-ресурсов и систем управления контентом предприятия.
Тема 8 "Основные программно-технические меры безопасности информации: идентификация и аутентификация; управление доступом" Анализ защищенности"	Основы безопасности жизнедеятельности в области профессиональной деятельности. Постановка и решение схемотехнических задачи, связанные с выбором системы элементов при заданных требованиях к параметрам (временным, мощностным, габаритным, надежностным). Принципы реализации и использования алгоритмов идентификации и аутентификации, управления доступом и процедур анализа защищенности.
Тема 9 "Основные программно-технические меры безопасности информации: протоколирование, аудит, шифрование, контроль целостности, электронная цифровая подпись"	Основные понятия. Описывается протоколирование и аудит, а также криптографические методы защиты. Показывается их место в общей архитектуре безопасности. Методы шифрования. Криптографического контроля целостности. Цифровые сертификаты.
Тема 10 "Основные программно-технические меры безопасности информации: Экранирование, Анализ защищенности"	Основные понятия программно-технического уровня информационной безопасности. Особенности современных информационных систем, существенные с точки зрения безопасности. Архитектурная безопасность.
Тема 11 "Криптография: шифрование и обеспечение целостности"	Основные угрозы безопасности информации и возможные способы их реализации, методы и средства противодействия этим угрозам. Применять на практике собственные и классические алгоритмы криптографической защиты данных. Методы проектирования, разработки и реализации технического решения в области создания систем

Тема	Содержание
	управления контентом Интернет-ресурсов и систем управления контентом предприятия с использованием криптографических систем защиты.
Тема 12 «Протоколирование и аудит, шифрование, контроль целостности»	Основные угрозы безопасности информации и возможные способы их реализации, а также методы и средства противодействия этим угрозам в рамках реализации процедур протоколирования и аудита, контроля целостности (в т.ч. с использованием элементов шифрования).
Тема 13 " Антивирусная защита компьютерных систем "	Принципы организации антивирусной защиты информационных систем. Типология вирусов. Достоинства и недостатки эвристических алгоритмов поиска вирусов.

6. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Основная литература:

1. Прохорова, О.В. Информационная безопасность и защита информации: учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». - Самара : Самарский государственный архитектурно-строительный университет, 2014. - 113 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-9585-0603-3 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=438331>

Дополнительная литература:

1. Галатенко, В.А. Основы информационной безопасности: Курс лекций: учебное пособие / В.А. Галатенко ; под ред. В.Б. Бетелина. - Изд. 3-е. - Москва : Интернет-Университет Информационных Технологий, 2006. - 208 с. - (Основы информационных технологий). - ISBN 5-9556-0052-3 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=233063>

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

В образовательном процессе используются:

- учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (мебель аудиторная (столы, стулья, доска аудиторная), комплект мультимедийного оборудования, включающий мультимедиапроектор, экран, переносной ноутбук для демонстрации презентаций; учебно-наглядные пособия; обеспечивающие тематические иллюстрации);

- помещения для самостоятельной работы (оснащены компьютерными столами, стульями, доской аудиторной, компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета);

- помещения для хранения и профилактического обслуживания учебного оборудования (оснащены наборами инструментов, оборудованием, расходными материалами для монтажа, ремонта и обслуживания информационно-телекоммуникационной сети филиала и вычислительной техники);

- лаборатория информационных технологий (оснащена компьютерными столами, стульями, мультимедийным проектором, экраном проекционным, компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета).

7.1. ПЕРЕЧЕНЬ ЛИЦЕНЗИОННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

1. Microsoft Windows;
2. MicrosoftOffice / LibreOffice;
3. Microsoft Visual Studio – средство разработки программных приложений;
4. среда программирования: Borland C++ 3.1;
5. среда программирования: dev-c++;
6. среда программирования: Code::Blocks.

7.2. ЭЛЕКТРОННО-БИБЛИОТЕЧНЫЕ СИСТЕМЫ

1. ЭБС «Издательство Лань»[Электронный ресурс]: электронная библиотечная система / ООО «Издательство Лань». – Режим доступа: <https://e.lanbook.com/>;
2. ЭБС «Электронная библиотечная система ЮРАЙТ» [Электронный ресурс]: электронная библиотечная система / ООО «Электронное издательство ЮРАЙТ». – Режим доступа: <https://biblio-online.ru/>;
3. ЭБС «Университетская библиотека онлайн»[Электронный ресурс]: электронно-периодическое издание; программный комплекс для организации онлайн-доступа к лицензионным материалам / ООО «НексМедиа». – Режим доступа: <https://biblioclub.ru/>.

7.3. СОВРЕМЕННЫЕ ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ

1. Электронная база данных SCOPUS.
2. Электронная база данных РИНЦ.

7.4. ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

1. Справочно-правовая информационная система Консультант Плюс <http://www.consultant.ru/>
2. Электронный справочник "Информо" для высших учебных заведений <http://www.informio.ru/>

8. ИНЫЕ СВЕДЕНИЯ И МАТЕРИАЛЫ НА УСМОТРЕНИЕ ВЕДУЩЕЙ КАФЕДРЫ

Не предусмотрено.

9. ОБЕСПЕЧЕНИЕ ОБРАЗОВАНИЯ ДЛЯ ЛИЦ С ОВЗ

Для обеспечения образования инвалидов и лиц с ограниченными возможностями здоровья реализация дисциплины может осуществляться в адаптированном виде, с учетом специфики освоения и дидактических требований, исходя из индивидуальных возможностей и по личному заявлению обучающегося.