

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Сыров Игорь Анатольевич  
Должность: Директор  
Дата подписания: 22.08.2025 10:48:50  
Уникальный программный ключ:  
b683afe664d7e9f64175886cf9626a196149ad36

СТЕРЛИТАМАКСКИЙ ФИЛИАЛ  
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО  
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ  
«УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»

Факультет Математики и информационных технологий  
Кафедра Математического моделирования

**Рабочая программа дисциплины (модуля)**

дисциплина Программно-аппаратные средства защиты информации

**Блок Б1, базовая часть, Б1.Б.29**

цикл дисциплины и его часть (базовая, вариативная, дисциплина по выбору)

Направление

**10.03.01**

**Информационная безопасность**

код

наименование направления

Программа

**Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)**

Форма обучения

**Очная**

Для поступивших на обучение в  
**2020 г.**

Разработчик (составитель)  
кандидат физико-математических наук, доцент  
**Беляева М. Б.**  
ученая степень, должность, ФИО

<b>1. Перечень планируемых результатов обучения по дисциплине (модулю) .....</b>	<b>3</b>
1.1. Перечень планируемых результатов освоения образовательной программы .....	3
1.2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы .	3
<b>2. Место дисциплины (модуля) в структуре образовательной программы .....</b>	<b>4</b>
<b>3. 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 .....</b>	<b>4</b>
<b>4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий.....</b>	<b>5</b>
4.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах) .....	5
4.2. Содержание дисциплины, структурированное по разделам (темам) .....	6
<b>5. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине (модулю).....</b>	<b>8</b>
<b>6. Учебно-методическое и информационное обеспечение дисциплины (модуля) .....</b>	<b>8</b>
6.1. Перечень учебной литературы, необходимой для освоения дисциплины .....	8
6.2. Перечень электронных библиотечных систем, современных профессиональных баз данных и информационных справочных систем .....	9
6.3. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства .....	9
<b>7. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю) .....</b>	<b>9</b>

## 1. Перечень планируемых результатов обучения по дисциплине (модулю)

### 1.1. Перечень планируемых результатов освоения образовательной программы

Выпускник, освоивший программу высшего образования, в рамках изучаемой дисциплины, должен обладать компетенциями, соответствующими видам профессиональной деятельности, на которые ориентирована программа:

Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)

Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)

### 1.2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Формируемая компетенция (с указанием кода)	Этапы формирования компетенции	Планируемые результаты обучения по дисциплине (модулю)
Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)	1 этап: Знания	Обучающийся должен знать: - место и роль систем управления версиями в процессе разработки программного обеспечения; - принципы использования современных систем управления версиями.
	2 этап: Умения	Обучающийся должен уметь: - основные тенденции развития рынка программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем управления организацией; - условия создания и эксплуатации программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем управления коммерческой организацией; - безопасные сетевые технологии, в которых используются программно-аппаратные средств обеспечения информационной безопасности; принципы функционирования и обеспечения защиты программно-аппаратных средств информационной

		безопасности;
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: методами установки и настройки программных, программно-аппаратных и технических средств защиты информации.
Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)	1 этап: Знания	Обучающийся должен знать: информации в развитии современного общества, применять информационные технологии для поиска и обработки информации
	2 этап: Умения	Обучающийся должен уметь: использовать современные системы управления версиями в процессе работы над индивидуальным и командным проектами.
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: - навыками работы в системе Git. Должен демонстрировать способность и готовность: - использовать полученные знания и навыки в дальнейшей учебной и профессиональной деятельности.

## 2. Место дисциплины (модуля) в структуре образовательной программы

Данная учебная дисциплина включена в раздел "Б1.В.ДВ.4 Дисциплины (модули)" основной профессиональной образовательной программы 10.03.01 "Информационная безопасность (Безопасность компьютерных систем)" и относится к дисциплинам по выбору.

Дисциплина изучается на 3 курсе в 6 семестре

## 3. 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 (объем) дисциплины составляет 4 зач. ед., 144 акад. ч.

Объем дисциплины	Всего часов
	Очная форма обучения
Общая трудоемкость дисциплины	144
Учебных часов на контактную работу с преподавателем:	
лекций	12
практических (семинарских)	18

лабораторных	18
другие формы контактной работы (ФКР)	1,2
Учебных часов на контроль (включая часы подготовки):	34,8
курсовая работа	
экзамен	
Учебных часов на самостоятельную работу обучающихся (СР):	60
курсовая работа	

Формы контроля	Семестры
курсовая работа	6
экзамен	6

**4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий**

**4.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах)**

№ п/п	Наименование раздела / темы дисциплины	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
		Контактная работа с преподавателем			СР
		Лек	Пр/Сем	Лаб	
<b>1</b>	<b>Основные принципы создания и применения программно-аппаратных средств обеспечения информационной безопасности.</b>	<b>8</b>	<b>12</b>	<b>12</b>	<b>39</b>
1.1	Введение. Основные понятия.	2	2	2	10
1.2	Стандарты и спецификации в области ИБ. Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности.	2	4	5	9
1.3	Категории и модели информационной безопасности	2	4	3	10
1.4	Идентификация и аутентификация пользователей. Понятие несанкционированного доступа.	2	2	2	10
<b>2</b>	<b>Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности, взаимодействие с общесистемными компонентами вычислительных систем</b>	<b>4</b>	<b>6</b>	<b>6</b>	<b>21</b>
2.1	Программно-аппаратные средства шифрования.	2	2	2	12
2.2	Защита компонентов ПЭВМ. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим	2	4	4	9

	носителям.				
	<b>Итого</b>	<b>12</b>	<b>18</b>	<b>18</b>	<b>60</b>

#### 4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
<b>1</b>	<b>Основные принципы создания и применения программно-аппаратных средств обеспечения информационной безопасности.</b>	
1.1	Введение. Основные понятия.	Основные понятия в области обеспечения безопасности информации
1.2	Стандарты и спецификации в области ИБ. Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности.	Технические средства защиты информации от несанкционированного доступа
1.3	Категории и модели информационной безопасности	Категории и модели информационной безопасности
1.4	Идентификация и аутентификация пользователей. Понятие несанкционированного доступа.	Понятие несанкционированного доступа. Тип:
<b>2</b>	<b>Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности, взаимодействие с общесистемными компонентами вычислительных систем</b>	
2.1	Программно-аппаратные средства шифрования.	Основные виды программно-аппаратных средств защиты информации.
2.2	Защита компонентов ПЭВМ. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.	способность определять информационные ресурсы

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
<b>1</b>	<b>Основные принципы создания и применения программно-аппаратных средств обеспечения информационной безопасности.</b>	
1.1	Введение. Основные понятия.	Управление учетными записями пользователей и создание групп Упражнение
1.2	Стандарты и спецификации в области ИБ. Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности.	Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности.
1.3	Категории и модели информационной безопасности	Управление разрешениями в файловой системе NTFS

		Упражнение
1.4	Идентификация и аутентификация пользователей. Понятие несанкционированного доступа.	. Управление локальными политиками безопасности Упражнение
<b>2</b>	<b>Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности, взаимодействие с общесистемными компонентами вычислительных систем</b>	
2.1	Программно-аппаратные средства шифрования.	Создание и изменение шаблона политики безопасности Упражнение
2.2	Защита компонентов ПЭВМ. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.	Анализ шаблона политики безопасности Упражнение

#### Курс лабораторных занятий

№	Наименование раздела / темы дисциплины	Содержание
<b>1</b>	<b>Основные принципы создания и применения программно-аппаратных средств обеспечения информационной безопасности.</b>	
1.1	Введение. Основные понятия.	Построение системы резервного копирования в ОС семейства Windows Установка и настройка ПО VipNet
1.2	Стандарты и спецификации в области ИБ. Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности.	Использование инструментальных средств анализа защищённости. Установка и использование сканера Nessus.
1.3	Категории и модели информационной безопасности	Обзор средств разграничения доступа на активном оборудовании
1.4	Идентификация и аутентификация пользователей. Понятие несанкционированного доступа.	Использование средств разграничения доступа на нескольких коммутаторах
<b>2</b>	<b>Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности, взаимодействие с общесистемными компонентами вычислительных систем</b>	
2.1	Программно-аппаратные средства шифрования.	Создание и удаление виртуальных сетей на коммутаторе Catalyst 2950
2.2	Защита компонентов ПЭВМ. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.	Использование инструментальных средств анализа защищённости. Установка и использование сканера Nessus.

## **5. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине (модулю)**

Самостоятельная работа включает в себя подготовку рефератов, докладов, составление библиографического списка за определенный временной период, подготовки проблемных вопросов, самостоятельное изучение отдельных аспектов содержания дисциплины, подготовка презентаций, инновационных проектов и пр. Наиболее эффективному усвоению теоретических знаний, получению практических умений и навыков по дисциплине способствуют различные формы индивидуальной учебной деятельности студентов магистратуры: конспектирование учебной и научной литературы, работа с понятиями, решение педагогических ситуаций и задач, сбор и анализ практического материала, выполнение вопросов и заданий для самостоятельной работы, учебно-исследовательских заданий, подготовка сообщений и рефератов по предлагаемым темам.

Типовые вопросы для самостоятельного изучения

1. Виды безопасности в различных сферах жизнедеятельности личности, общества и государства
2. Проблемы региональной информационной безопасности
3. Основные понятия информационной безопасности
4. Виды защищаемой информации и защита интеллектуальной собственности
5. Угрозы информационной безопасности Российской Федерации в различных сферах
6. Методы информационного противоборства и применение информационного оружия
7. Компьютерная система как объект информационной войны
8. Программно-аппаратные средства обеспечения информационной безопасности
9. Механизмы защиты информации компьютерных систем
10. Формальные модели обеспечения информационной безопасности
11. Стандарты по управлению информационной безопасностью ISO/IEC 27000
12. Защита автоматизированных систем и средств вычислительной техники от внешнего электромагнитного воздействия.

## **6. Учебно-методическое и информационное обеспечение дисциплины (модуля)**

### **6.1. Перечень учебной литературы, необходимой для освоения дисциплины**

#### **Основная учебная литература:**

1. Казарин О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов: Издательство Юрайт, 2018//ЭБС Университетская библиотека Online <https://biblioonline.ru/book/E458AFCD-826E-4A1F-9BAB68BB83EA616F>

#### **Дополнительная учебная литература:**

1. Грибунин В. Г., Чудовский В. В. Комплексная система защиты информации на предприятии: учеб. пособие для вузов М.: Академия, 2009.-185с.
2. Хорев П. Б. Методы и средства защиты информации в компьютерных системах: учеб. пособие для вузов М.: Академия, 2005.- 385с.
3. Ярочкин В.И., Бузанова Я.В. Аудит безопасности фирмы: теория и практика: учеб. пособие для вузов Королев: Парадигма, 2005.-265с.

## 6.2. Перечень электронных библиотечных систем, современных профессиональных баз данных и информационных справочных систем

№ п/п	Наименование документа с указанием реквизитов
1	Договор на доступ к ЭБС ZNANIUM.COM между БашГУ в лице директора СФ БашГУ и ООО «Знаниум» № 3/22-эбс от 05.07.2022
2	Договор на доступ к ЭБС «ЭБС ЮРАЙТ» (полная коллекция) между БашГУ в лице директора СФ БашГУ и ООО «Электронное издательство ЮРАЙТ» № 1/22-эбс от 04.03.2022
3	Договор на доступ к ЭБС «Университетская библиотека онлайн» между БашГУ и «Нексмедиа» № 223-950 от 05.09.2022
4	Договор на доступ к ЭБС «Лань» между БашГУ и издательством «Лань» № 223-948 от 05.09.2022
5	Договор на доступ к ЭБС «Лань» между БашГУ и издательством «Лань» № 223-949 от 05.09.2022
6	Соглашение о сотрудничестве между БашГУ и издательством «Лань» № 5 от 05.09.2022
7	ЭБС «ЭБ БашГУ», бессрочный договор между БашГУ и ООО «Открытые библиотечные системы» № 095 от 01.09.2014 г.
8	Договор на БД диссертаций между БашГУ и РГБ № 223-796 от 27.07.2022
9	Договор о подключении к НЭБ и о предоставлении доступа к объектам НЭБ между БашГУ в лице директора СФ БашГУ с ФГБУ «РГБ» № 101/НЭБ/1438-П от 11.06.2019
10	Договор на доступ к ЭБС «ЭБС ЮРАЙТ» (полная коллекция) между УУНиТ в лице директора СФ УУНиТ и ООО «Электронное издательство ЮРАЙТ» № 1/23-эбс от 03.03.2023

## Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет»)

№ п/п	Адрес (URL)	Описание страницы
1	<a href="http://www.scopus.com">http://www.scopus.com</a>	Электронная база данных «Scopus»

## 6.3. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

Наименование программного обеспечения
AcademicEdition Networked Volume Licenses RAD Studio XE5 Professional Concurrent App / Плавающая – 60 шт. Бессрочная / ООО «Фермомобайл» / № 04182 от 03.12.2013
Visual Studio Community 2019 v.16.3 / OLP. Бессрочная / <a href="https://visualstudio.microsoft.com/ru/vs/community/">https://visualstudio.microsoft.com/ru/vs/community/</a>
Windows 10 Education N / Бессрочная / Microsoft Imagine. Подписка №8001361124 от 04.10.2017 г.
Office Standart 2010 RUS OLP NL Acdmc / 200, Бессрочная / ООО «Компания Фермо» / № Ф-04211 от 12.03.2021
Kaspersky Endpoint Security / 950 / ООО «Смартлайн»/ №44/013 от 06.12.2021

## 7. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)

Тип учебной аудитории	Оснащенность учебной аудитории
Читальный зал: помещение для	учебная мебель, учебно-наглядные

самостоятельной работы	пособия, компьютеры
Лаборатория программно-аппаратных средств обеспечения информационной безопасности. Помещение для проведения учебных занятий семинарского типа, групповых и индивидуальных консультаций.	компьютеры; учебно-наглядные пособия; антивирусные программные комплексы; аппаратные средства аутентификации пользователя; программно-аппаратные комплексы защиты информации; стенды для изучения проводных и беспроводных компьютерных сетей; аппаратно-программные средства управления доступом к данным, шифрования.
Учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий семинарского типа, учебная аудитория текущего контроля и промежуточной аттестации, учебная аудитория групповых и индивидуальных консультаций	Доска, учебная мебель, компьютеры, проектор, экран, учебно-наглядные пособия.
Учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий семинарского типа, учебная аудитория текущего контроля и промежуточной аттестации, учебная аудитория групповых и индивидуальных консультаций, учебная аудитория курсового проектирования (выполнения курсовых работ)	Доска, учебная мебель, компьютеры, проектор, экран, учебно-наглядные пособия.