

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Сыров Игорь Анатольевич  
Должность: Директор  
Дата подписания: 30.10.2023 11:44:22  
Уникальный программный ключ:  
b683afe664d7e9f64175886cf9626a196149ad36

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

Факультет  
Кафедра

*Экономический*  
*Бухгалтерского учета и аудита*

**Рабочая программа дисциплины (модуля)**

дисциплина ***Б1.В.14 Информационная безопасность экономических систем***

часть, формируемая участниками образовательных отношений

Специальность

***38.05.01***  
код

***Экономическая безопасность***  
наименование специальности

Программа

***Экономико-правовое обеспечение экономической безопасности***

Форма обучения

***Заочная***

Для поступивших на обучение в  
***2023 г.***

Разработчик (составитель)  
***кандидат педагогических наук, доцент***  
***Рафикова В. М.***  
ученая степень, должность, ФИО

<b>1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций .....</b>	<b>3</b>
<b>2. Цели и 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>9</b>
6.1. Перечень учебной литературы, необходимой для освоения дисциплины (модуля)	9
6.2. Перечень электронных библиотечных систем, современных профессиональных баз данных и информационных справочных систем .....	10
6.3. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства .....	10
<b>7. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю) .....</b>	<b>11</b>

**1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций**

<b>Формируемая компетенция (с указанием кода)</b>	<b>Код и наименование индикатора достижения компетенции</b>	<b>Результаты обучения по дисциплине (модулю)</b>
ПК-1. Способен разработать интегрированную систему управления рисками	ПК-1.1. Применяет современные информационные системы и технологии управления рисками	<p>Обучающийся должен:</p> <p><b>Знать</b></p> <ul style="list-style-type: none"> <li>-источники возникновения информационных угроз;</li> <li>-каналы утечки информации;</li> <li>-направления и средства защиты информации;</li> <li>-принципы национальной безопасности.</li> </ul> <p><b>Уметь</b></p> <ul style="list-style-type: none"> <li>- применять правовые, организационные, технические и программные средства защиты информации;</li> <li>- выявлять потенциальные каналы утечки информации и определять их характеристики;</li> <li>- разрабатывать и обосновывать варианты эффективных управленческих решений в области управления рисками.</li> </ul> <p><b>Владеть</b></p> <ul style="list-style-type: none"> <li>- навыками противодействия утечке компьютерной информации;</li> <li>- навыками использования электронной цифровой подписи;</li> <li>- навыками проведения аудита локальной политики безопасности, аудита доступа к объектам</li> <li>- навыками профессиональной аргументации при разборе стандартных ситуаций в сфере управления рисками.</li> </ul>
	ПК-1.2. Использует программное обеспечение для работы с информацией	<p>Обучающийся должен:</p> <p><b>Знать</b></p> <ul style="list-style-type: none"> <li>- основные функциональные возможности современных программных средств.</li> </ul> <p><b>Уметь</b></p> <ul style="list-style-type: none"> <li>- использовать основные функциональные возможности</li> </ul>

		современных программных средств. Владеть - навыками использования основных функциональных возможностей современных программных средств поддержки профессиональной деятельности
	ПК-1.3. Осуществляет мониторинг наиболее критичных рисков, их динамики и вырабатывает рекомендации по дальнейшему развитию системы управления рисками	Обучающийся должен: Знать - порядок проведения мониторинга информационной безопасности объектов и систем Уметь - проводить мониторинг информационной безопасности объектов Владеть - навыками проведения мониторинга информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности

## 2. Цели и место дисциплины (модуля) в структуре образовательной программы

Цели изучения дисциплины:

Ознакомление обучающихся с основными направлениями деятельности по обеспечению информационной безопасности и защите информации, рассмотрение аспектов нормативно-правовой базы, регламентирующей данную деятельность, задач по сохранности информационных ресурсов, средств и механизмов, методов их применения.

Дисциплина Информационная безопасность экономических систем реализуется в рамках части, формируемой участниками образовательных отношений. Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин: Экономическая информатика, Информационные технологии и программные средства в экономике.

Дисциплина изучается на 3, 4 курсах в 6, 7 семестрах

## 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 144 акад. ч.

<b>Объем дисциплины</b>	<b>Всего часов</b>
-------------------------	--------------------

	<b>Заочная форма обучения</b>
Общая трудоемкость дисциплины	144
Учебных часов на контактную работу с преподавателем:	
лекций	6
практических (семинарских)	10
другие формы контактной работы (ФКР)	0,2
Учебных часов на контроль (включая часы подготовки):	7,8
дифференцированный зачет	
Учебных часов на самостоятельную работу обучающихся (СР)	120

<b>Формы контроля</b>	<b>Семестры</b>
дифференцированный зачет	7

#### 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>Основы информационной безопасности</b>	<b>1</b>	<b>2</b>	<b>0</b>	<b>24</b>
1.1	Понятие информационной безопасности. Основные составляющие	1	0	0	12
1.2	Наиболее распространенные угрозы информационной безопасности и её составляющие	0	2	0	12
<b>2</b>	<b>Уровни информационной безопасности</b>	<b>2</b>	<b>2</b>	<b>0</b>	<b>36</b>
2.1	Законодательный уровень информационной безопасности	1	0	0	12
2.2	Административный уровень информационной безопасности	1	0	0	12
2.3	Процедурный уровень информационной безопасности	0	2	0	12
<b>3</b>	<b>Программно-технические меры по обеспечению информационной безопасности</b>	<b>3</b>	<b>6</b>	<b>0</b>	<b>60</b>
3.1	Основные характеристики программно-технических мер	1	0	0	12
3.2	Идентификация и аутентификация	1	0	0	12
3.3	Протоколирование и аудит, шифрование, контроль целостности	0	2	0	12

3.4	Экранирование, анализ защищенности	0	2	0	12
3.5	Обеспечение высокой доступности	1	2	0	12
	<b>Итого</b>	<b>6</b>	<b>10</b>	<b>0</b>	<b>120</b>

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

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
<b>1</b>	<b>Основы информационной безопасности</b>	
1.2	Наиболее распространенные угрозы информационной безопасности и её составляющие	<ol style="list-style-type: none"> <li>1. Перечислите виды угроз безопасности информации.</li> <li>2. Каковы источники угроз безопасности информации?</li> <li>3. Каковы проблемы защиты электронной информации?</li> <li>4. Что такое компьютерное преступление?</li> <li>5. Дайте классификацию компьютерным преступлениям.</li> <li>6. Правовое обеспечение защиты информации.</li> <li>7. Опишите механизмы преступлений с использованием пластиковых карт.</li> <li>8. Опишите мошенничество на Интернет-аукционах.</li> <li>9. Компьютерные вирусы и средства защиты от них.</li> <li>10. Троянские программы, использование троянских программ для совершения компьютерных преступлений.</li> <li>11. Что такое информационная атака?</li> <li>12. Что такое информационная война?</li> <li>13. Что такое электронный терроризм?</li> </ol>
<b>2</b>	<b>Уровни информационной безопасности</b>	
2.3	Процедурный уровень информационной безопасности	<ol style="list-style-type: none"> <li>1. Управление персоналом</li> <li>2. Поддержание работоспособности</li> <li>3. Планирование восстановительных работ</li> <li>4. Физическая защита</li> <li>5. Реагирование на нарушение безопасного режима</li> </ol>
<b>3</b>	<b>Программно-технические меры по обеспечению информационной безопасности</b>	
3.3	Протоколирование и аудит, шифрование, контроль целостности	<ol style="list-style-type: none"> <li>1. Протоколирование и аудит. Основные понятия.</li> <li>2. Активный аудит. Основные понятия.</li> <li>3. Функциональные компоненты и архитектура.</li> </ol>

		4. Шифрование. 5. Контроль целостности.
3.4	Экранирование, анализ защищенности	1. Понятие межсетевого экранирования 2. Типы межсетевых экранов, краткая характеристика. 3. Технология виртуальных частных сетей (VPN)
3.5	Обеспечение высокой доступности	1. Основные понятия: • заданный уровень доступности • эффективности • время недоступности 2. Основные меры обеспечения высокой доступности • Структуризация системы • Высокая отказоустойчивость (резервирование, тиражирование); • Обслуживаемость информационной системы.

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
<b>1</b>	<b>Основы информационной безопасности</b>	
1.1	Понятие информационной безопасности. Основные составляющие	Информационная безопасность. Защита информации, субъект информационных отношений, неприемлемый ущерб. Доступность, целостность, конфиденциальность. Компьютерное преступление, жизненный цикл информационных систем.
<b>2</b>	<b>Уровни информационной безопасности</b>	
2.1	Законодательный уровень информационной безопасности	Российское законодательство в области информационной безопасности. Стандарты и спецификации в области информационной безопасности.
2.2	Административный уровень информационной безопасности	Основные понятия, политика безопасности. Жизненный цикл информационной системы. Синхронизация программы безопасности с жизненным циклом систем. Управление рисками
<b>3</b>	<b>Программно-технические меры по обеспечению информационной безопасности</b>	
3.1	Основные характеристики программно-технических мер	Основные понятия программно-технического уровня. Архитектурная безопасность. Экранирование. Анализ защищённости. Отказоустойчивость. Безопасное восстановление.
3.2	Идентификация и аутентификация	Основные понятия. Парольная аутентификация. Одноразовые пароли. Идентификация/аутентификация с помощью биометрических данных. Управление доступом. Ролевое управление доступом.
3.5	Обеспечение высокой доступности	Эффективность услуг. Время недоступности. Основы мер обеспечения высокой доступности. Отказоустойчивость и

		зона риска. Обеспечение отказоустойчивости. Обеспечение обслуживаемости. Туннелирование.
--	--	---

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

Самостоятельная работа студентов подразумевает подготовку докладов, самоконтроль, подготовку к тестированию, работу с нормативно-правовыми актами и информационными ресурсами. Для самостоятельной работы студентов подготовлены задания для самостоятельной работы, список литературы.

1. Информационные ресурсы, подлежащие защите в сфере финансовой деятельности.
2. Классификация угроз информационной безопасности и их сравнительный анализ.
3. Информационная безопасность в современных условиях хозяйствования. Общегосударственные цели, задачи и методы обеспечения информационной безопасности.
4. Понятия о видах вирусов. Классификация вирусов и угрозы для информационной инфраструктуры хозяйствующих субъектов.
5. Вида возможных нарушений информационной безопасности в сфере финансовой деятельности.
6. Отечественные и международные стандарты обеспечения информационной безопасности.
7. Особенности современной нормативно-правовой и методологической базы обеспечения информационной безопасности.
8. Основные нормативные руководящие документы, касающиеся конфиденциальной информации и государственной тайны, нормативно-справочные документы по обеспечению информационной безопасности применяемые в финансовой деятельности.
9. Общие критерии оценки безопасности информационных систем и технологий ГОСТ 15408, как основа определения требований к обеспечению информационной безопасности.
10. Место информационной безопасности экономических систем в национальной безопасности страны.
11. Цели и задачи обеспечения национальной безопасности. Система целеполагания в структуре государственного и муниципального управления при обеспечении информационной безопасности.
12. Основные положения концепции информационной безопасности. Сравнительная таблица.
13. Государственные информационные ресурсы, подлежащие защите в сфере финансовой деятельности.
14. Взаимосвязь государственных и коммерческих информационных ресурсов (конфиденциальной информации и государственной тайны).
15. Модели безопасности, и их применение.
16. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Оценка системы защиты информации.
17. Оценка эффективности средств и механизмов обеспечения информационной безопасности.
18. Методы анализа способов нарушений информационной безопасности.
19. Программно-аппаратные комплексы криптографической защиты, их характеристики и особенности применения. Сравнительная таблица.
20. Нормативно-правовая база криптографической защиты.
21. ЭЦП и особенности работы в системах государственного и муниципального управления.

#### Основная учебная литература

1. Зенков, А. В. Информационная безопасность и защита информации: учебное пособие для вузов / А. В. Зенков. — Москва: Издательство Юрайт, 2022. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — URL : <https://urait.ru/bcode/497002> (дата обращения 21.05.2023)
2. Суворова, Г. М. Информационная безопасность: учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2022. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — URL : <https://urait.ru/bcode/496741>(дата обращения 21.05.2023)

#### Дополнительная учебная литература

1. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва: Издательство Юрайт, 2022. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — URL : <https://urait.ru/bcode/498844> (дата обращения 21.05.2023)
2. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2022. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — URL : <https://urait.ru/bcode/489745> (дата обращения 21.05.2023)
3. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2022. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — URL : <https://urait.ru/bcode/490421> (дата обращения 21.05.2023)

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

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

#### **Основная учебная литература:**

1. Суворова, Г. М. Информационная безопасность: учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2022. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — URL : <https://urait.ru/bcode/496741>(дата обращения 21.05.2023)
2. Зенков, А. В. Информационная безопасность и защита информации: учебное пособие для вузов / А. В. Зенков. — Москва: Издательство Юрайт, 2022. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — URL : <https://urait.ru/bcode/497002> (дата обращения 21.05.2023)

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

1. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2022. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — URL : <https://urait.ru/bcode/490421> (дата обращения 21.05.2023)
2. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2022. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — URL : <https://urait.ru/bcode/489745> (дата обращения 21.05.2023)

3. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва: Издательство Юрайт, 2022. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — URL : <https://urait.ru/bcode/498844> (дата обращения 21.05.2023)

### 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.consultant.ru">www.consultant.ru</a>	официальный сайт ЗАО «Консультант Плюс».
2	<a href="http://www.garant.ru">www.garant.ru</a>	официальный сайт ООО «НПП Гарант-Сервис».
3	<a href="http://www.kodeks.ru">www.kodeks.ru</a>	официальный сайт информационно-правового консорциума «Кодекс».

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

Наименование программного обеспечения
Office Standart 2010 RUS OLP NL Acdmc / 200 / Лицензионный договор №04297 от 9.04.2012
Windows XP / Лицензионное соглашение MSDN. Государственный контракт №9 от 18.03.2008 г. ЗАО «СофтЛайн»

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

<b>Тип учебной аудитории</b>	<b>Оснащенность учебной аудитории</b>
Читальный зал: помещение для самостоятельной работы	Учебная мебель, учебно-наглядные пособия, компьютеры с доступом к сети «Интернет» и ЭИОС Филиала
Учебная аудитория для проведения занятий семинарского типа, учебная аудитория для проведения практических работ, учебная аудитория для проведения групповых и индивидуальных консультаций, учебная аудитория текущего контроля и промежуточной аттестации; аудитория, оборудованная для проведения занятий по информационным технологиям; компьютерный класс с доступом к сети "Интернет" и электронной информационно-образовательной среде СФ УУНиТ. Учебная аудитория курсового проектирования (выполнения курсовых работ)	учебная мебель, доска, мультимедиа-проектор, экран настенный, компьютеры
Учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий семинарского типа, учебная аудитория для проведения практических работ, учебная аудитория для проведения групповых и индивидуальных консультаций, учебная аудитория текущего контроля и промежуточной аттестации	учебная мебель, доска, мультимедиа-проектор, экран настенный, учебно-наглядные пособия