

ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»  
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Утверждено:  
на заседании кафедры  
протокол № 7 от «18» февраля 2022 г.

Зав. кафедрой etCup- / Исмагилова А.С.

Согласовано:  
Председатель УМК института



/ Гильмутдинова Р.А.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

Б1.В.01 Введение в специальность

Часть, формируемая участниками образовательных отношений

**программа специалитета**

Специальность

10.05.05 Безопасность информационных технологий в правоохранительной сфере

Специализация

Организация и технологии защиты информации (по отраслям)

Квалификация

Специалист по защите информации

Разработчик (составитель)  
профессор, д-р физ.-мат. наук, доцент  
(должность, ученая степень, ученое звание)

etCup- / Исмагилова А.С.  
(подпись, Фамилия И.О.)

Для приема: 2022 г.

Уфа 2022 г.

Составитель: Исмагилова Альбина Сабирьяновна, д.ф.-м.н., профессор кафедры управления информационной безопасностью

Рабочая программа дисциплины утверждена на заседании кафедры управления информационной безопасностью, протокол № 7 от «18» февраля 2022 г.

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры \_\_\_\_\_,  
протокол № \_\_\_\_ от « \_\_\_\_ » \_\_\_\_\_ 20 \_ г.

Заведующий кафедрой \_\_\_\_\_ / \_\_\_\_\_ Ф.И.О/

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры \_\_\_\_\_,  
протокол № \_\_\_\_ от « \_\_\_\_ » \_\_\_\_\_ 20 \_ г.

Заведующий кафедрой \_\_\_\_\_ / \_\_\_\_\_ Ф.И.О/

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры \_\_\_\_\_,  
протокол № \_\_\_\_ от « \_\_\_\_ » \_\_\_\_\_ 20 \_ г.

Заведующий кафедрой \_\_\_\_\_ / \_\_\_\_\_ Ф.И.О/

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры \_\_\_\_\_,  
протокол № \_\_\_\_ от « \_\_\_\_ » \_\_\_\_\_ 20 \_ г.

Заведующий кафедрой \_\_\_\_\_ / \_\_\_\_\_ Ф.И.О/

## СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций .....	5
2. Цель и место дисциплины в структуре образовательной программы .....	6
3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся).....	6
4. Фонд оценочных средств по дисциплине .....	7
4.1. Перечень компетенций и индикаторов достижения компетенций с указанием соотнесенных с ними запланированных результатов обучения по дисциплине. Описание критериев и шкал оценивания результатов обучения по дисциплине .....	7
4.2. Типовые контрольные задания или иные материалы, необходимые для оценивания результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине .....	11
5. Учебно-методическое и информационное обеспечение дисциплины .....	19
5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины .....	19
5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы .....	19
6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине .....	20

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

В результате освоения образовательной программы обучающийся должен овладеть следующими результатами обучения по дисциплине:

<b>Категория (группа) компетенций (при наличии ОПК)</b>	<b>Формируемая компетенция (с указанием кода)</b>	<b>Код и наименование индикатора достижения компетенции</b>	<b>Результаты обучения по дисциплине</b>
Самоорганизация и саморазвитие (в том числе здоровье-сбережение)	УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни.	УК-6.1. Знает основные способы оценки приоритетов.	Знать основы планирования профессиональной траектории с учетом особенностей как профессиональной, так и других видов деятельности.
		УК-6.2. Умеет рационально прогнозировать распределение имеющихся ресурсов при постановке задач.	Уметь расставлять приоритеты профессиональной деятельности и способы ее совершенствования на основе самооценки; планировать самостоятельную деятельность в решении профессиональных задач; подвергать критическому анализу проделанную работу; находить и творчески использовать имеющийся опыт в соответствии с задачами саморазвития.
		УК-6.3. Владеет навыками оценки ситуации и анализа приоритетов.	Владеть навыками выявления стимулов для саморазвития; навыками определения реалистических целей профессионального роста.
Организационно-управленческая	ПК-1. Способен формировать требования по защите информации и политики безопасности компьютерных систем и сетей.	ПК-1.1. Знает основные принципы, методы и этапы формирования требования по защите информации и политики безопасности	Знать типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа в компьютерную среду; виды угроз информационных систем и методы обеспечения информационной безопасности; принципы

		компьютерных систем и сетей.	защиты информации и обеспечения информационной безопасности; об угрозах информационной безопасности и их источниках; архитектуру современных информационных технологий и их место в управлении предприятием.
		ПК-1.2. Умеет применять основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	Уметь осуществлять ведение базы данных и поддержку информационного обеспечения решения прикладных задач; выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в компьютерных системах и сетях.
		ПК-1.3. Владеет методикой формирования требований по защите информации и политики безопасности компьютерных систем и сетей.	Владеть основными положениями теории информационной безопасности компьютерных систем и сетей методами обеспечения безопасности передачи данных; методами обеспечения информационной безопасности; средствами защиты информации для обеспечения заданных свойств информационной безопасности.

## 2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Введение в специальность» относится к группе дисциплин части, формируемой участниками образовательных отношений образовательной программы.

Дисциплина изучается на 1 курсе в 1 семестре.

Целью изучения дисциплины является раскрытие сущности и значения понятий информационной безопасности и защиты информации, их места в системе национальной безопасности, определение теоретических, концептуальных, методологических и организационных основ обеспечения безопасности информации, классификация составляющих информационной безопасности и защиты информации, установление логической взаимосвязи входящих в них компонентов.

## 3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)

Содержание рабочей программы представлено в Приложении № 1.

#### 4. Фонд оценочных средств по дисциплине

##### 4.1. Перечень компетенций и индикаторов достижения компетенций с указанием соотнесенных с ними запланированных результатов обучения по дисциплине.

##### Описание критериев и шкал оценивания результатов обучения по дисциплине

УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни.

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
УК-6.1. Знает основные способы оценки приоритетов.	Знать основы планирования профессиональной траектории с учетом особенностей как профессиональной, так и других видов деятельности.	Не знает основы планирования профессиональной траектории и с учетом особенностей как профессиональной, так и других видов деятельности.	Знает некоторые основы планирования профессиональной траектории с учетом особенностей профессиональной деятельности.	Знает основы планирования профессиональной траектории с учетом особенностей профессиональной деятельности.	Знает основы планирования профессиональной траектории с учетом особенностей как профессиональной, так и других видов деятельности.
УК-6.2. Умеет рационально прогнозировать распределение имеющихся ресурсов при постановке задач.	Уметь расставлять приоритеты профессиональной деятельности и способы ее совершенствования на основе самооценки; планировать самостоятельную деятельность в решении профессиональных задач.	Не умеет расставлять приоритеты профессиональной деятельности и способы ее совершенствования на основе самооценки; планировать самостоятельную деятельность в решении профессиональных задач.	Умеет планировать самостоятельную деятельность в решении профессиональных задач.	Умеет планировать самостоятельную деятельность в решении профессиональных задач; находить и творчески использовать имеющийся опыт в соответствии с задачами саморазвития.	Умеет расставлять приоритеты профессиональной деятельности и способы ее совершенствования на основе самооценки; планировать самостоятельную деятельность в решении профессиональных задач.

	льных задач; подвергать критическому анализу проделанную работу; находить и творчески использовать имеющийся опыт в соответствии с задачами саморазвития;	льную деятельность в решении профессиональных задач; подвергать критическому анализу проделанную работу; находить и творчески использовать имеющийся опыт в соответствии с задачами саморазвития;			льных задач; подвергать критическому анализу проделанную работу; находить и творчески использовать имеющийся опыт в соответствии с задачами саморазвития;
УК-6.3. Владеет навыками оценки ситуации и анализа приоритетов.	Владеть навыками выявления стимулов для саморазвития; навыками определения реалистических целей профессионального роста.	Не владеет навыками выявления стимулов для саморазвития; навыками определения реалистических целей профессионального роста.	Владеет в некоторой степени навыками выявления стимулов для саморазвития.	Владеет навыками выявления стимулов для саморазвития.	Владеет навыками выявления стимулов для саморазвития; навыками определения реалистических целей профессионального роста.

ПК-1. Способен формировать требования по защите информации и политики безопасности компьютерных систем и сетей.

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
ПК-1.1. Знает основные	Знать типовые программно-	Не знает типовые программно-	Знает виды угроз информации	Знает типовые программно-	Знает типовые программно-

<p>принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.</p>	<p>аппаратные средства и системы защиты информации от несанкционированного доступа в компьютерную среду; виды угроз информационных систем и методы обеспечения информационной безопасности; принципы защиты информации и обеспечения информационной безопасности; об угрозах информационной безопасности и их источниках; архитектуру современных информационных технологий и их место в управлении предприятием.</p>	<p>о-аппаратные средства и системы защиты информации от несанкционированного доступа в компьютерную среду; виды угроз информационных систем и методы обеспечения информационной безопасности; принципы защиты информации и обеспечения информационной безопасности; об угрозах информационной безопасности и их источниках; архитектур современных информационных технологий и их место в управлении</p>	<p>нных систем и методы обеспечения информационной безопасности; принципы защиты информации и обеспечения информационной безопасности.</p>	<p>аппаратные средства и системы защиты информации от несанкционированного доступа в компьютерную среду; виды угроз информационных систем и методы обеспечения информационной безопасности; принципы защиты информации и обеспечения информационной безопасности.</p>	<p>аппаратные средства и системы защиты информации от несанкционированного доступа в компьютерную среду; виды угроз информационных систем и методы обеспечения информационной безопасности; принципы защиты информации и обеспечения информационной безопасности; об угрозах информационной безопасности и их источниках; архитектуру современных информационных технологий и их место в управлении предприятием.</p>
---	---	--	--	---	---



		предприят и ем.			
ПК-1.2. Умеет применять основные принципы, методы и этапы формировани я требования по защите информации и политики безопасности компьютерны х систем и сетей.	Уметь осуществлят ь ведение базы данных и поддержку информацио нного обеспечения решения прикладных задач; выявлять угрозы информацио нной безопасност и, обосновыват ь организац ио нно □ технич еские мероприятия по защите информации в компьютерн ых системах и сетях.	Не умеет осуществл ять ведение базы данных и поддержку информаци онного обеспечен ия решения прикладны х задач; выявлять угрозы информаци онной безопаснос ти, обосновыв ать организац ио нно □ техн ические мероприят ия по защите информаци и в компьютер ных системах и сетях.	Умеет выявлять угрозы информаци онной безопасност и.	Умеет выявлять угрозы информаци онной безопасност и, обосновыват ь организац ио нно □ технич еские мероприятия по защите информации в компьютерн ых системах и сетях.	Умеет осуществлят ь ведение базы данных и поддержку информацио нного обеспечения решения прикладных задач; выявлять угрозы информацио нной безопасност и, обосновыват ь организац ио нно □ технич еские мероприятия по защите информации в компьютерн ых системах и сетях.
ПК-1.3. Владеет методикой формировани я требований по защите информации и политики безопасности компьютерны х систем и сетей.	Владеть основными положениям и теории информацио нной безопасности компьютерн ых систем и сетей, методами обеспечения безопасности передачи данных; методами	Не владеет основными положения ми теории информаци онной безопаснос ти компьютер ных систем и сетей, методами обеспечени я безопаснос ти	Владеет основными положениям и теории информацио нной безопасности компьютерн ых систем и сетей.	Владеет основными положениям и теории информацио нной безопасности компьютерн ых систем и сетей, методами обеспечения безопасности передачи данных; методами	Владеет основными положениям и теории информацио нной безопасности компьютерн ых систем и сетей, методами обеспечения безопасности передачи данных; методами

	обеспечения информации безопасности ; средствами защиты информации для обеспечения заданных свойств информационной безопасности .	передачи данных; методами обеспечения информации безопасности; средствами защиты информации для обеспечения заданных свойств информационной безопасности.		обеспечения информации безопасности .	обеспечения информации безопасности ; средствами защиты информации для обеспечения заданных свойств информационной безопасности .
--	---	---	--	---------------------------------------	---

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины (для экзамена: текущий контроль – максимум 40 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания:

от 45 до 59 баллов – «удовлетворительно»;

от 60 до 79 баллов – «хорошо»;

от 80 баллов – «отлично».

**4.2. Типовые контрольные задания или иные материалы, необходимые для оценивания результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине**

<b>Код и наименование индикатора достижения компетенции</b>	<b>Результаты обучения по дисциплине</b>	<b>Оценочные средства</b>
УК-6.1. Знает основные способы оценки приоритетов.	Знать основы планирования профессиональной траектории с учетом особенностей как профессиональной, так и других видов деятельности.	Т, ПР
УК-6.2. Умеет рационально прогнозировать распределение имеющихся	Уметь расставлять приоритеты профессиональной деятельности и способы ее	

<p>ресурсов при постановке задач.</p>	<p>совершенствования на основе самооценки; планировать самостоятельную деятельность в решении профессиональных задач; подвергать критическому анализу проделанную работу; находить и творчески использовать имеющийся опыт в соответствии с задачами саморазвития;</p>	
<p>УК-6.3. Владеет навыками оценки ситуации и анализа приоритетов.</p>	<p>Владеть навыками выявления стимулов для саморазвития; навыками определения реалистических целей профессионального роста.</p>	
<p>ПК-1.1. Знает основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.</p>	<p>Знать типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа в компьютерную среду; виды угроз информационных систем и методы обеспечения информационной безопасности; принципы защиты информации и обеспечения информационной безопасности; об угрозах информационной безопасности и их источниках; архитектуру современных информационных технологий и их место в управлении предприятием.</p>	<p>Т, ПР</p>
<p>ПК-1.2. Умеет применять основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.</p>	<p>Уметь осуществлять ведение базы данных и поддержку информационного обеспечения решения прикладных задач; выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в компьютерных системах и сетях.</p>	

<p>ПК-1.3. Владеет методикой формирования требований по защите информации и политики безопасности компьютерных систем и сетей.</p>	<p>Владеть основными положениями теории информационной безопасности компьютерных систем и сетей, методами обеспечения безопасности передачи данных; методами обеспечения информационной безопасности; средствами защиты информации для обеспечения заданных свойств информационной безопасности.</p>	
--	--	--

Т - тестирование, ПР - практические работы

### Рейтинг-план дисциплины

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
<b>Модуль 1</b>				
Текущий контроль			0	20
Аудиторная работа (практические, лабораторные работы)	10	2	0	20
Рубежный контроль				15
Тест	15	1		15
<b>Всего</b>				<b>35</b>
<b>Модуль 2</b>				
Текущий контроль				20
Аудиторная работа (практические, лабораторные работы)	10	2	0	20
Рубежный контроль				15
Тест	15	1	0	15
<b>Всего</b>				<b>35</b>
<b>Поощрительные баллы</b>				
1. Студенческая олимпиада			0	4
2. Публикация статей, участие в конференции			0	6
<b>Всего</b>				<b>10</b>
<b>Посещаемость (баллы вычитаются из общей суммы набранных баллов)</b>				
1. Посещение лекционных занятий				-6
2. Посещение практических занятий				-10
<b>Итоговый контроль</b>				
Экзамен			0	30

## **Тестирование**

### **Модуль 1.**

1. Какие законы существуют в России в области компьютерного права?
  - 1) О государственной тайне
  - 2) об авторском праве и смежных правах
  - 3) о гражданском долге
  - 4) о правовой охране программ для ЭВМ и БД
  - 5) о правовой ответственности
  - 6) об информации, информатизации, защищенности информации
  
2. Какие существуют основные уровни обеспечения защиты информации?
  - 1) законодательный
  - 2) административный
  - 3) программно-технический
  - 4) физический
  - 5) вероятностный
  - 6) процедурный
  - 7) распределительный

### **Модуль 2.**

1. На современном этапе развития законодательного уровня информационной безопасности в России важнейшее значение имеют:
  - 1) меры ограничительной направленности
  - 2) направляющие и координирующие меры
  - 3) меры по обеспечению информационной независимости
  
2. Меры информационной безопасности направлены на защиту от:
  - 1) нанесения неприемлемого ущерба
  - 2) нанесения любого ущерба
  - 3) подглядывания в замочную скважину

## **Темы практических работ**

Для самостоятельного освоения и/или расширения знаний, умений, владений предусмотрены несколько практических заданий – представление докладов с последующим обсуждением.

### **Модуль 1.**

Сущность безопасности информационных технологий в правоохранительной сфере и ее место в системе национальной безопасности

1. Становление и развитие, сущность и структура понятия «информационная безопасность в правоохранительной сфере».
2. Объекты информационной безопасности
3. Связь информационной безопасности с информатизацией общества.
4. Национальные интересы в информационной сфере как объект информационной безопасности.
5. Понятие и современная концепция национальной безопасности.
6. Место информационной безопасности в системе национальной безопасности.

### **Модуль 2.**

Современная доктрина информационной безопасности Российской Федерации

1. Понятие и назначение доктрины информационной безопасности.
2. Составляющие национальных интересов в информационной сфере, пути их достижения.
3. Виды и состав угроз информационной безопасности.

4. Принципы обеспечения информационной безопасности.

5. Особенности обеспечения информационной безопасности в различных сферах общественной жизни.

#### Критерии и методика оценивания докладов

10-8 баллов студент получает, если работа выполнена в полном объеме и изложена грамотным языком в правильной логической последовательности с точным использованием специализированной терминологии; если при этом показано уверенное владение материалом; подготовлен реферативный отчет и презентация.

7-5 баллов студент получает за работу, если она выполнена в полном объеме, но имеет некоторые недостатки. К примеру, в работе допущены один-два недочета при освещении основного содержания ответа и/или нет определенной логической последовательности, неточно используется специализированная терминология.

4-1 балл студент получает, если работа выполнена неполно, не показано общее понимание вопроса, имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, при знании теоретического материала выявлена недостаточная сформированность основных умений и навыков (пропорционально количеству недочетов, ошибок, пробелов в знаниях).

#### Устный опрос

Устный индивидуальный опрос проводится после изучения модуля с целью выяснения наиболее сложных вопросов, степени усвоения информации. Студент излагает содержание вопроса изученной темы.

#### Типовые вопросы для устного опроса

1. Прогресс информационных технологий и необходимость обеспечения информационной безопасности.
2. Основные понятия информационной безопасности.
3. Структура понятия информационная безопасность.
4. Система защиты информации и ее структура.
5. Профессиональные тайны, их виды.
6. Персональные данные и их защита.
7. Информационные угрозы, их виды и причины возникновения.
8. Информационные угрозы для государства.
9. Информационные угрозы для организации.
10. Информационные угрозы для личности (физического лица).

#### Критерии и методика оценивания ответов:

Студенту предлагается 5 вопросов из приведенного перечня в процессе изучения материала курса (т.о. студент может набрать до 5 баллов за устные ответы), в т.ч. за каждый вопрос устного опроса начисляется:

- 1 балл, если ответ на вопрос дан верно и достаточно полно;
- 0,5 балла за неполный ответ;
- 0 баллов если ответ на устный вопрос не дан или дан неверно.

#### Перечень вопросов для экзамена

1. Становление и развитие понятия «информационная безопасность».
2. Современные подходы к определению понятия «безопасности информационных технологий в правоохранительной сфере».
3. Программно-аппаратные средства обеспечения безопасности информационных технологий в правоохранительной сфере.
4. Сущность и структура понятия «информационная безопасность».
5. Объекты информационной безопасности в правоохранительной системе.
6. Связь информационной безопасности с информатизацией общества.

7. Определение понятия «информационная безопасность».
8. Значение информационной безопасности и ее место в правоохранительной сфере.
9. Значение информационной безопасности для субъектов информационных отношений.
10. Национальные интересы в информационной сфере как объект информационной безопасности.
11. Национальные интересы и их содержание. Социальные интересы личности в информационной сфере.
12. Интересы общества в информационной сфере.
13. Интересы государства в информационной сфере.
14. Интересы сохранения национальной идентичности.
15. Безопасность национальных интересов в информационной сфере.
16. Соотношение национальных интересов и национальной безопасности.
17. Национальные интересы и безопасность России.
18. История развития представлений о национальной безопасности.
19. Современная концепция национальной безопасности.
20. Место информационной безопасности в системе национальной безопасности.
21. Понятие и назначение доктрины информационной безопасности.
22. Интересы личности, общества и государства в информационной сфере.
23. Составляющие национальных интересов в информационной сфере, пути их достижения.
24. Виды и состав угроз информационной безопасности.
25. Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению.
26. Принципы обеспечения информационной безопасности.
27. Общие методы обеспечения информационной безопасности.
28. Особенности обеспечения информационной безопасности в различных сферах общественной жизни.
29. Основные положения государственной политики обеспечения информационной безопасности, мероприятия по их реализации.
30. Организационная основа системы обеспечения информационной безопасности.
31. Существующие подходы к содержательной части понятия «защита информации».
32. Понятие уязвимости информации.
33. Виды уязвимости информации.
34. Формы и причины проявления уязвимости информации.
35. Несовершенство или нарушения организации работы с информацией или с носителем информации как причина проявления ее уязвимости.
36. Несовершенство системы защиты информации или нарушения в обеспечении информационной безопасности как причина проявления ее уязвимости.
37. Негативные социальные и психологические явления, происходящие в организации или ее структурном подразделении как причина проявления уязвимости информации.
38. Высокая ценность информации как причина проявления ее уязвимости.
39. Уязвимость и информационный риск.
40. Понятие, причины и условия утечки защищаемой информации.



## Образец экзаменационного билета

---

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Башкирский государственный университет»  
Институт истории и государственного управления

Направление

10.05.05 Безопасность информационных технологий в правоохранительной сфере

Дисциплина

«Введение в специальность»

### ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 5

1. Объекты информационной безопасности в правоохранительной системе.
2. Несовершенство или нарушения организации работы с информацией или с носителем информации как причина проявления ее уязвимости.

Зав. кафедрой управления информационной безопасностью

/А.С. Исмагилова /

---

Примерные критерии оценивания ответа на экзамене (только для тех, кто учится с использованием модульно-рейтинговой системы обучения и оценки успеваемости студентов):

Критерии оценки (в баллах):

- 25-30 баллов выставляется студенту, если студент дал полные, развернутые ответы на все теоретические вопросы билета, продемонстрировал знание функциональных возможностей, терминологии, основных элементов, умение применять теоретические знания при выполнении практических заданий. Студент без затруднений ответил на все дополнительные вопросы. Практическая часть работы выполнена полностью без неточностей и ошибок;

- 17-24 баллов выставляется студенту, если студент раскрыл в основном теоретические вопросы, однако допущены неточности в определении основных понятий. При ответе на дополнительные вопросы допущены небольшие неточности. При выполнении практической части работы допущены несущественные ошибки;

- 10-16 баллов выставляется студенту, если при ответе на теоретические вопросы студентом допущено несколько существенных ошибок в толковании основных понятий. Логика и полнота ответа страдают заметными изъянами. Заметны пробелы в знании основных методов. Теоретические вопросы в целом изложены достаточно, но с пропусками материала. Имеются принципиальные ошибки в логике построения ответа на вопрос. Студент не решил задачу или при решении допущены грубые ошибки;

- 0-10 баллов выставляется студенту, если он отказался от ответа или не смог ответить на вопросы билета, ответ на теоретические вопросы свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Обнаруживается отсутствие навыков применения теоретических знаний при выполнении практических заданий. Студент не смог ответить ни на один дополнительный вопрос.

## 5. Учебно-методическое и информационное обеспечение дисциплины

### 5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

#### Основная литература:

1. Технологии защиты информации в компьютерных сетях / Н.А.Руденков, А.В.Пролетарский, Е.В.Смирнова, А.М.Суровов. - 2-е изд., испр. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с.: ил.; То же [Электронный ресурс]. - <http://biblioclub.ru/index.php?page=book&id=428820>
2. Прохорова О.В. Информационная безопасность и защита информации : учебник / О.В.Прохорова. - Самара: Самарский государственный архитектурно-строительный университет, 2014. - 113 с.: - ISBN 978-5-9585-0603-3. То же [Электронный ресурс]. - <http://biblioclub.ru/index.php?page=book&id=438331>

#### Дополнительная литература:

3. Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] / А.А. Бирюков. - Электрон. дан. – М.: ДМК Пресс, 2017. - 434 с. - Режим доступа: <https://e.lanbook.com/book/93278>
4. Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс]: учебник / А.А. Бирюков. - Электрон. дан. – М.: ДМК Пресс, 2012. - 474 с. - Режим доступа: <https://e.lanbook.com/book/39990>
5. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю.Н.Загинайлов. - М., Берлин: Директ-Медиа, 2015. - 253 с. ISBN 978-5-4475-3946-7. То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=276557>

### 5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы

1. Справочная правовая система «КонсультантПлюс» – <http://www.consultant-plus.ru>.
2. Электронная библиотечная система «Университетская библиотека онлайн» – <https://biblioclub.ru>.
3. Электронная библиотечная система издательства «Лань» – <https://e.lanbook.com/>
4. Электронный каталог Библиотеки БашГУ – <http://www.bashlib.ru/catalogi/>
5. [www.fstec.ru](http://www.fstec.ru) – сайт ФСТЭК России
6. [www.fsb.ru](http://www.fsb.ru) – сайт ФСБ России
7. <http://window.edu.ru/> – Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам»;
8. <http://univertv.ru/video/matematika/> – Открытый образовательный видеопортал UniverTV.ru. Образовательные фильмы на различные темы. Лекции в ведущих российских и зарубежных вузах. Научная конференция или научно-популярная лекция по интересующему вопросу);
9. [www.newlibrary.ru](http://www.newlibrary.ru) – Новая электронная библиотека;
10. [www.edu.ru](http://www.edu.ru) – Федеральный портал российского образования;
11. [www.elibrary.ru](http://www.elibrary.ru) – Научная электронная библиотека;
12. [www.nehudlit.ru](http://www.nehudlit.ru) – Электронная библиотека учебных материалов.
13. Windows 8 Russian Russian OLP NL Academic Edition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные.
14. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.

15. Система централизованного тестирования БашГУ (Moodle).GNU General Public License.

### 6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
1	2	3
1. учебная аудитория для проведения занятий лекционного типа: аудитория № 403 (гуманитарный корпус), аудитория № 405 (гуманитарный корпус), аудитория № 413 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 515 (гуманитарный корпус), аудитория № 516 (гуманитарный корпус).	Лекционные занятия	<p>Аудитория № 403</p> <p>Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия.</p> <p>Аудитория № 405</p> <p>Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром PrometheanActivBoard 387 RPOMOUNTEST -1 шт., Ком-ер встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H – 1 шт. , Мультимедиа-проектор PanasonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт. , Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт.</p>
2. учебная аудитория для проведения занятий семинарского типа: аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус).	Практические (семинарские) занятия	<p>Аудитория № 413</p> <p>Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт.</p> <p>Аудитория № 415</p> <p>Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт.</p> <p>Аудитория № 416</p> <p>Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт.</p> <p>Аудитория № 418</p> <p>Учебная мебель, доска, Экран настенный Lumien Master Piktura 153*203 Matte White Fiber Clas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт.</p> <p>Аудитория № 419</p> <p>Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт.</p>
3. учебная аудитория	Консультации	

<p>для проведения групповых и индивидуальных консультаций: аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус).</p>		<p>Аудитория № 515 Учебная мебель, доска, терминал видео конференции LifeSize Icon 600-камера, интер-ая система со встроенным короткофокусным проектором Promethean ActivBoard 387 RPO MOUNT EST, профес-сиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса HDMI CMPRO 4H4H, интер-ая напольная кафедра докладчика, ком-ер встраиваемый в кафедру IN-TEL Core i3-4150/DDR3 4 Gb/HDD 1TB/DVD-RW/Therm altake VL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром.</p> <p>Аудитория № 516 Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран.</p> <p>Аудитория № 509 Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p>Аудитория № 608 Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p>Аудитория № 609 Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p>Аудитория № 610 Учебная мебель, доска, учебно-наглядные пособия, LED Телевизор TCLL55P6 USBLACK – 1 шт., кронштейн для телевизора NBP 5 – 1 шт., Кабель HDMI (m)-HDH(m)ver14,10м.</p>
<p>4. учебная аудитория для текущего контроля и промежуточной аттестации: аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус),</p>	<p>Текущий контроль и промежуточная аттестация</p>	<p>Аудитория № 613 Учебная мебель, доска, моноблок стационарный – 15 шт.</p> <p>Компьютерный класс аудитория № 420 Учебная мебель, моноблоки стационарные 15 шт.</p> <p>Компьютерный класс аудитория № 404 Учебная мебель, компьютеры -15 штук.</p> <p>Аудитория 402 читальный зал библиотеки Учебная мебель, доска, компьютеры в комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура, мышь, стеллажи, шкафы картотечные, комбинированные</p> <ol style="list-style-type: none"> <li>1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные.</li> <li>2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.</li> <li>3. Система централизованного тестирования БашГУ (Moodle). GNU General Public License.</li> <li>4. Правовая система «КонсультантПлюс». Договор №28826 от 09.01.2019 г. Лицензии бессрочные.</li> </ol>

компьютерный класс аудитория № 420 (гуманитарный корпус).		
5. помещения для самостоятельной работы: аудитория № 613 (гуманитарный корпус), читальный зал библиотеки аудитория 402 (гуманитарный корпус).	Самостоятельная работа студентов	

МИНОБРНАУКИ РОССИИ  
 ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»  
 ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Содержание рабочей программы  
 дисциплины **Введение в специальность**  
 на 1 семестр ОФО

<b>Вид работы</b>	<b>Объем дисциплины</b>
Общая трудоемкость дисциплины (ЗЕТ / часов)	4 ЗЕТ / 144 часа
Учебных часов на контактную работу с преподавателем:	55,2
лекций	18
практических/ семинарских	36
лабораторных	
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	1,2
Учебных часов на самостоятельную работу обучающихся (СР)	34,8
Учебных часов на подготовку к экзамену/зачету/дифференцированному зачету (Контроль)	54

Форма контроля:  
 экзамен 1 семестр

№	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Основная и дополнитель ная литература, рекомендуе мая студентам (номера из списка)	Задания по самостоятельно й работе студентов	Форма текущего контроля успеваемос ти (коллоквиу мы, контрольн ые работы, компьютер ные тесты и т.п.)
		ЛК	ПР	ЛР	СРС			
1	2	4	5	6	7	8	9	10
1	<p>Модуль 1. Сущность безопасности информационных технологий в правоохранительной сфере и ее место в системе национальной безопасности:</p> <p>Становление и развитие, сущность и структура понятия «информационные технологии и безопасность».</p> <p>Объекты информационной безопасности.</p> <p>Связь информационной безопасности с информатизацией общества.</p> <p>Национальные интересы в информационной сфере как объект информационной безопасности.</p> <p>Понятие и современная концепция безопасности информационных технологий в правоохранительной сфере.</p>	10	18	-	18	1-5	Самостоятельное изучение рекомендуемых источников и материалов, подготовка к практическому занятию и тестированию.	ПЗ, СР

	Обеспечение информационной безопасности в правоохранительной сфере.							
2	<p>Модуль 2. Современная доктрина информационной безопасности Российской Федерации:</p> <p>Составляющие национальных интересов в информационной сфере, пути их достижения.</p> <p>Виды и состав угроз информационной безопасности.</p> <p>Принципы обеспечения информационной безопасности.</p> <p>Особенности обеспечения информационной безопасности в различных сферах общественной жизни.</p> <p>Сущность уязвимости и утечки информации.</p>	8	18	-	16,8	1-5	Самостоятельное изучение рекомендуемых источников и материалов, подготовка к практическому занятию и тестированию.	ПЗ, СР
	Итого	18	36	-	18			

Т - тестирование, ПР - практические работы



