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

Актуализировано:
на заседании кафедры
протокол № 10 от «7» июня 2018 г.
Зав. кафедрой / А.С. Исмагилова

Согласовано:
Председатель УМК института
/ Р.А. Гильмутдинова

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

Основы информационной безопасности
Б1.Б.13 базовая

программа бакалавриата

Направление подготовки
10.03.01 Информационная безопасность

Профиль подготовки
Организация и технология защиты информации

Квалификация
бакалавр

Разработчик (составитель)
профессор, д-р физ.-мат.
наук, доцент / Исмагилова А.С.

Для приема: 2017 г.

Уфа 2018 г

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

Рабочая программа дисциплины актуализирована на заседании кафедры управления информационной безопасностью, протокол № 10 от «7» июня 2018 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 планируемыми результатами освоения образовательной программы

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

| Результаты обучения | | Формируемая компетенция (с указанием кода) | Примечание |
|---|---|---|---|
| Знания | 1. Знать место и роль профессии в системе национальной безопасности РФ;<br>2. Знать социальные ценности общества и их связь с социальной значимостью своей будущей профессии;<br>3. Знать основные виды социальных организаций и способы взаимодействия в них;<br>4. Знать основные задачи своей профессии в соответствии с нормами морали, профессиональной этики и служебного этикета. | ОК-5Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики | |
| | 1. Знать понятие и методы саморазвития, самообучения и самовоспитания личности;<br>2. Знать компоненты образовательной деятельности (мотивационный, процессуальный, организационный, оценочный);<br>3. Знать типовые алгоритмы самообразования;<br>4. Знать требования к компетентности специалиста и его развитию, требования к повышению квалификации и мастерства в профессиональной среде. | ОК-8Способность к самоорганизации и самообразованию | |
| | 1. Знать средства | ОПК-7Способность определять | |

| | | | |
|---|---|---|---|
| | контроля контента;<br>2. Знать средства анализа защищенности и средства обнаружения атак для обеспечения безопасности в IP-сетях;<br>3. Знать средства защиты от несанкционированного доступа;<br>4. Знать применение межсетевых экранов. | 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 | |
| | 1. Знать политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации;<br>2. Знать общеметодологические принципы теории информационной безопасности;<br>3. Знать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации;<br>4. Знать состояние законодательной базы и стандарты в области информационной безопасности. | ПК-13 Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации | |
| Умения | 1. Уметь осознавать социальную значимость своей профессии;<br>2. Уметь находить баланс между интересами личности, общества и государства;<br>3. Уметь соблюдать нормы профессиональной этики. | ОК-5 Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики | |
| | 1. Уметь самостоятельно ставить самообразовательные задачи;<br>2. Уметь планировать и | ОК-8Способность к самоорганизации и самообразованию | |

| | | | |
|---|---|---|---|
| | реализовывать собственную образовательную траекторию;<br>3. Уметь анализировать и выбирать формы и методы повышения квалификации и мастерства в зависимости от собственных потребностей и образовательной траектории. | | |
| | 1. Уметь использовать базовые возможности информационных систем для решения задач фирмы;<br>2. Уметь внедрять компоненты систем предприятия, обеспечивающие информационную безопасность;<br>3. Уметь использовать системы электронного документооборота;<br>4. Уметь работать с информацией в глобальных компьютерных сетях. | ОПК-7 Способность 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 | |
| | 1. Уметь реализовывать на практике принципы политики безопасности;<br>2. Уметь использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности;<br>3. Уметь обосновывать организационно-технические мероприятия по защите информации;<br>4. Уметь использовать возможности и особенности организационных, аппаратных и | ПК-13 Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации | |

| | | | |
|---|---|---|---|
| | программных средств безопасности и защиты информации. | | |
| Владения (навыки / опыт деятельности) | 1. Владеть пониманием социологического аспекта профессионализации и высокой мотивацией к выполнению профессиональной деятельности;<br>2. Владеть навыками творческого мышления для выполнения профессиональных задач в области обеспечения безопасности информационных технологий и защиты интересов личности, общества и государства. | ОК-5 Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики | |
| | 1. Владеть методами самоанализа;<br>2. Владеть анализом и оценкой эффективности программы и результатов самообразования;<br>3. Владеть методами организации собственного обучения. | ОК-8Способность к самоорганизации и самообразованию | |
| | 1. Владеть методикой определения видов и форм информации, подверженной угрозам, анализировать угрозы информационно-вычислительным системам;<br>2. Владеть навыками работы с компьютером как средством защиты информации. | ОПК-7 Способность 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 | |
| | 1. Владеть навыками анализа, обработки и интерпретации результатов решения прикладных задач управления;<br>2. Владеть навыками формирования комплекса мер (правила, | ПК-13 Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации | |

| | | | |
|---|---|---|---|
| | процедуры, практические приемы и пр.) для управления информационной безопасностью;<br>3. Владеть навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации;<br>4. Владеть навыками выявления и устранения угроз информационной безопасности;<br>5. Владеть навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий;<br>6. Владеть навыками внедрения, адаптации и настройки средств защиты прикладных ИС. | | |

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

Дисциплина «Основы информационной безопасности» относится к группе дисциплин базовой части образовательной программы.

Дисциплина изучается на 1 курсе в1 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 с указанием этапов их формирования в процессе освоения образовательной программы. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

ОК-5Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области

обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики.

| Этап (уровень) освоения компетенции | Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций) | Критерии оценивания результатов защиты курсовой работы и экзамена | | | |
|---|---|---|---|---|---|
| | | 2 («Не удовлетво-рительно») | 3 («Удовлетворительно») | 4 («Хорошо») | 5 («Отлично») |
| Первый этап (уровень) | Знать:<br>- место и роль профессии в системе национальной безопасности РФ;<br>- социальные ценности общества и их связь с социальной значимостью своей будущей профессии;<br>- основные виды социальных организаций и способы взаимодействия в них;<br>- основные задачи своей профессии в соответствии с нормами морали, профессиональной этики и служебного этикета. | Не знает место и роль профессии в системе национальной безопасности РФ; социальные ценности общества и их связь с социальной значимостью своей будущей профессии; основные виды социальных организаций и способы взаимодействия в них; основные задачи своей профессии в соответствии с нормами морали, профессиональной этики и служебног | Знает место и роль профессии в системе национальной безопасности РФ. | Знает место и роль профессии в системе национальной безопасности РФ; социальные ценности общества и их связь с социальной значимостью своей будущей профессии; основные задачи своей профессии в соответствии с нормами морали, профессиональной этики и служебного этикета. | Знает место и роль профессии в системе национальной безопасности РФ; социальные ценности общества и их связь с социальной значимостью своей будущей профессии; основные виды социальных организаций и способы взаимодействия в них; основные задачи своей профессии в соответствии с нормами морали, профессиональной этики и служебного этикета. |

| | | | | | |
|---|---|---|---|---|---|
| | | о этикета. | | | |
| Второй этап (уровень) | Уметь:<br>- осознавать социальную значимость своей профессии;<br>- находить баланс между интересами личности, общества и государства;<br>- соблюдать нормы профессиональной этики. | Не умеет осознавать социальную значимость своей профессии; находить баланс между интересами личности, общества и государства; соблюдать нормы профессиональной этики. | Умеет осознавать социальную значимость своей профессии. | Умеет осознавать социальную значимость своей профессии; соблюдать нормы профессиональной этики. | Умеет осознавать социальную значимость своей профессии; находить баланс между интересами личности, общества и государства; соблюдать нормы профессиональной этики. |
| Третий этап (уровень) | Владеть:<br>- пониманием социологического аспекта профессионализации и высокой мотивацией к выполнению профессиональной деятельности;<br>- навыками творческого мышления для выполнения профессиональных задач в области обеспечения безопасности информационных технологий и защиты интересов личности, общества и государства | Не владеет пониманием социологического аспекта профессионализации и высокой мотивацией к выполнению профессиональной деятельности; навыками творческого мышления для выполнения профессиональных задач в области обеспечения безопаснос | Владеет некоторой мотивацией к выполнению профессиональной деятельности. | Владеет пониманием социологического аспекта профессионализации и высокой мотивацией к выполнению профессиональной деятельности. | Владеет пониманием социологического аспекта профессионализации и высокой мотивацией к выполнению профессиональной деятельности; навыками творческого мышления для выполнения профессиональных задач в области обеспечения безопасности информационных технологий |

| | | | | | |
|---|---|---|---|---|---|
| | | ти информационных технологий и защиты интересов личности, общества и государства | | | и защиты интересов личности, общества и государства |

ОК-8 Способность к самоорганизации и самообразованию.

| Этап (уровень) освоения компетенции | Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций) | Критерии оценивания результатов защиты курсовой работы и экзамена | | | |
|---|---|---|---|---|---|
| | | 2 («Не удовлетво-рительно») | 3 («Удовлетворительно») | 4 («Хорошо») | 5 («Отлично») |
| Первый этап (уровень) | Знать:<br>- понятие и методы саморазвития, самообучения и самовоспитания личности;<br>- компоненты образовательной деятельности (мотивационный, процессуальный, организационный, оценочный);<br>- типовые алгоритмы самообразования;<br>- требования к компетентности специалиста и его развитию, требования к повышению | Не знает понятие и методы саморазвития, самообучения и самовоспитания личности; компоненты образовательной деятельности; типовые алгоритмы самообразования; требования к компетентности специалиста и его развитию, требования к повышени | Знает понятие и методы саморазвития, самообучения и самовоспитания личности; компоненты образовательной деятельности. | Знает понятие и методы саморазвития, самообучения и самовоспитания личности; компоненты образовательной деятельности; типовые алгоритмы самообразования; требования к компетентности специалиста и его развитию. | Знает понятие и методы саморазвития, самообучения и самовоспитания личности; компоненты образовательной деятельности; типовые алгоритмы самообразования; требования к компетентности специалиста и его развитию, требования к повышению квалификации и |

| | | | | | |
|---|---|---|---|---|---|
| | квалификации и мастерства в профессиональной среде | ю квалификации и мастерства в профессиональной среде. | | | мастерства в профессиональной среде. |
| Второй этап (уровень) | Уметь:<br>- самостоятельно ставить самообразовательные задачи;<br>- планировать и реализовывать собственную образовательную траекторию;<br>- анализировать и выбирать формы и методы повышения квалификации и мастерства в зависимости от собственных потребностей и образовательной траектории. | Не умеет самостоятельно ставить самообразовательные задачи; планировать и реализовывать собственную образовательную траекторию; анализировать и выбирать формы и методы повышения квалификации и мастерства в зависимости от собственных потребностей и образовательной траектории. | Умеет ставить самообразовательные задачи. | Умеет ставить самообразовательные задачи; планировать и реализовывать собственную образовательную траекторию; выбирать формы и методы повышения квалификации. | Умеет самостоятельно ставить самообразовательные задачи; планировать и реализовывать собственную образовательную траекторию; анализировать и выбирать формы и методы повышения квалификации и мастерства в зависимости от собственных потребностей и образовательной траектории. |
| Третий этап (уровень) | Владеть:<br>- методами самоанализа;<br>- анализом и оценкой эффективности программы и | Не владеет методами самоанализа; анализом и оценкой эффективности | Владеет анализом и оценкой эффективности программы и | Владеет анализом и оценкой эффективности программы и | Владеет методами самоанализа; анализом и оценкой эффективности |

| | | | | | |
|---|---|---|---|---|---|
| | результатов самообразования;<br>- методами организации собственного обучения. | программы и результатов самообразования; методами организации собственного обучения. | результатов самообразования. | результатов самообразования; методами организации собственного обучения. | программы и результатов самообразования; методами организации собственного обучения. |

ОПК-7Способность 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.

| Этап (уровень) освоения компетенции | Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций) | Критерии оценивания результатов защиты курсовой работы и экзамена | | | |
|---|---|---|---|---|---|
| | | 2 («Не удовлетво-рительно») | 3 («Удовлетворительно») | 4 («Хорошо») | 5 («Отлично») |
| Первый этап (уровень) | Знать:<br>- средства контроля контента;<br>- средства анализа защищенности и средства обнаружения атак для обеспечения безопасности в IP-сетях;<br>- средства защиты от несанкционированного доступа;<br>- применение межсетевых экранов. | Не знает средства контроля контента; средства анализа защищенности и средства обнаружения атак для обеспечения безопасности в IP-сетях; средства защиты от несанкционированного доступа; применение межсетевых экранов. | Знает средства анализа защищенности; применение межсетевых экранов. | Знает средства анализа защищенности; средства защиты от несанкционированного доступа; применение межсетевых экранов. | Знает средства контроля контента; средства анализа защищенности и средства обнаружения атак для обеспечения безопасности в IP-сетях; средства защиты от несанкционированного доступа; применение межсетевых экранов. |

| | | | | | |
|---|---|---|---|---|---|
| Второй этап (уровень) | Уметь:<br>- использовать базовые возможности информационных систем для решения задач фирмы;<br>- внедрять компоненты систем предприятия, обеспечивающие информационную безопасность;<br>- использовать системы электронного документооборота;<br>- работать с информацией в глобальных компьютерных сетях. | Не умеет использовать базовые возможности информационных систем для решения задач фирмы; внедрять компоненты систем предприятия, обеспечивающие информационную безопасность; использовать системы электронного документооборота; работать с информацией в глобальных компьютерных сетях. | Умеет использовать базовые возможности информационных систем для решения задач фирмы; работать с информацией в глобальных компьютерных сетях. | Умеет использовать базовые возможности информационных систем для решения задач фирмы; использовать системы электронного документооборота; работать с информацией в глобальных компьютерных сетях. | Умеет использовать базовые возможности информационных систем для решения задач фирмы; внедрять компоненты систем предприятия, обеспечивающие информационную безопасность; использовать системы электронного документооборота; работать с информацией в глобальных компьютерных сетях. |
| Третий этап (уровень) | Владеть:<br>- методикой определения видов и форм информации, подверженной угрозам, анализировать угрозы информационно-вычислительным системам;<br>- навыками работы с компьютером как средством | Не владеет методикой определения видов и форм информации, подверженной угрозам, анализировать угрозы информационно-вычислительным системам; | Владеет некоторыми навыками работы с компьютером как средством защиты информации. | Владеет методикой определения видов и форм информации, подверженной угрозам; навыками работы с компьютером как средством защиты информации. | Владеетметодикой определения видов и форм информации, подверженной угрозам, анализировать угрозы информационно-вычислительным системам;навыками |

| | | | | | |
|---|---|---|---|---|---|
| | защиты информации. | навыками работы с компьютером как средством защиты информации. | | | работы с компьютером как средством защиты информации. |

ПК-13Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.

| Этап (уровень) освоения компетенции | Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций) | Критерии оценивания результатов защиты курсовой работы и экзамена | | | |
|---|---|---|---|---|---|
| | | 2 («Не удовлетво-рительно») | 3 («Удовлетворительно») | 4 («Хорошо») | 5 («Отлично») |
| Первый этап (уровень) | Знать:<br>- политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации;<br>- общеметодологические принципы теории информационной безопасности;<br>- возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации; | Не знает политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации;<br>общеметодологические принципы теории информационной безопасности;<br>возможности и особенности организаци | Знает политики информационной безопасности и защиты информации;<br>общеметодологические принципы теории информационной безопасности. | Знает политики информационной безопасности и защиты информации, способы их организации и оптимизации;<br>общеметодологические принципы теории информационной безопасности;<br>состояние законодательной базы и стандарты в области информационной безопасности. | Знает политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации;<br>общеметодологические принципы теории информационной безопасности;<br>возможности и особенности организационных, аппаратных |

| | | | | | |
|---|---|---|---|---|---|
| | - состояние законодательной базы и стандарты в области информационной безопасности. | онных, аппаратных и программных средств безопасности и защиты информации; состояние законодательной базы и стандарты в области информационной безопасности. | | | и программных средств безопасности и защиты информации; состояние законодательной базы и стандарты в области информационной безопасности. |
| Второй этап (уровень) | Уметь: - реализовывать на практике принципы политики безопасности; - использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности; - обосновывать организационно-технические мероприятия по защите информации; - использовать возможности и особенности организационных, аппаратных и | Не умеет реализовывать на практике принципы политики безопасности; использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности; обосновывать организационно-технические мероприят | Умеет обосновывать организационно-технические мероприятия по защите информации. | Умеет реализовывать на практике принципы политики безопасности; обосновывать организационно-технические мероприятия по защите информации; использовать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты | Умеет реализовывать на практике принципы политики безопасности; использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности; обосновывать организационно-технические мероприятия по защите информации; |

| | | | | | |
|---|---|---|---|---|---|
| | программных средств безопасности и защиты информации. | ия по защите информации; использовать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации. | | информации. | использовать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации. |
| Третий этап (уровень) | Владеть:<br>- навыками анализа, обработки и интерпретации результатов решения прикладных задач управления;<br>- навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью;<br>- навыками организации комплекса мероприятий по защите информации в процессах автоматизиров | Не владеет навыками анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками формирования комплекса мер для управления информационной безопасностью; навыками организации комплекса мероприятий по защите информации в | Владеет навыками формирования мер для управления информационной безопасностью; навыками выявления и устранения угроз информационной безопасности. | Владеет навыками анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками формирования комплекса мер для управления информационной безопасностью; навыками выявления и устранения угроз информационной безопасности; навыками | Владеет навыками анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками формирования комплекса мер для управления информационной безопасностью; навыками организации комплекса мероприятий по защите информации в процессах автоматизированной |

| | | | | | |
|---|---|---|---|---|---|
| | анной обработки информации; - навыками выявления и устранения угроз информационной безопасности; - навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий; - навыками внедрения, адаптации и настройки средств защиты прикладных ИС. | процессах автоматизированной обработки информации; навыками выявления и устранения угроз информационной безопасности; навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий; навыками внедрения, адаптации и настройки средств защиты прикладных ИС. | | внедрения, адаптации и настройки средств защиты прикладных ИС. | обработки информации; навыками выявления и устранения угроз информационной безопасности; навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий; навыками внедрения, адаптации и настройки средств защиты прикладных ИС. |

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 оценки знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы.**

**Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций**

| Этапы освоения | Результаты обучения | Компетенция | Оценочные средства |
|---|---|---|---|
| 1-й этап Знания | 1. Знать место и роль профессии в системе национальной безопасности РФ;<br>2. Знать социальные ценности общества и их связь с социальной значимостью своей будущей профессии;<br>3. Знать основные виды социальных организаций и способы взаимодействия в них;<br>4. Знать основные задачи своей профессии в соответствии с нормами морали, профессиональной этики и служебного этикета. | ОК-5 Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики | Т, ПР, ЛР |
| | 1. Знать понятие и методы саморазвития, самообучения и самовоспитания личности;<br>2. Знать компоненты образовательной деятельности (мотивационный, процессуальный, организационный, оценочный);<br>3. Знать типовые алгоритмы самообразования;<br>4. Знать требования к компетентности специалиста и его развитию, требования к повышению квалификации и мастерства в профессиональной среде. | ОК-8 Способность к самоорганизации и самообразованию | Т, ПР, ЛР |
| | 1. Знать средства контроля контента;<br>2. Знать средства анализа защищенности и средства обнаружения атак для обеспечения безопасности в IP-сетях;<br>3. Знать средства защиты от несанкционированного доступа;<br>4. Знать применение межсетевых экранов. | ОПК-7 Способность 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 | Т, ПР, ЛР |
| | 1. Знать политики, стратегии и технологии информационной | ПК-13 Способность принимать участие в | Т, ПР, ЛР |

| | | | |
|---|---|---|---|
| | безопасности и защиты информации, способы их организации и оптимизации;<br>2. Знать общеметодологические принципы теории информационной безопасности;<br>3. Знать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации;<br>4. Знать состояние законодательной базы и стандарты в области информационной безопасности. | формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации | |
| 2-й этап Умения | 1. Уметь осознавать социальную значимость своей профессии;<br>2. Уметь находить баланс между интересами личности, общества и государства;<br>3. Уметь соблюдать нормы профессиональной этики. | ОК-5 Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики | Т, ПР, ЛР |
| | 1. Уметь самостоятельно ставить самообразовательные задачи;<br>2. Уметь планировать и реализовывать собственную образовательную траекторию;<br>3. Уметь анализировать и выбирать формы и методы повышения квалификации и мастерства в зависимости от собственных потребностей и образовательной траектории. | ОК-8 Способность к самоорганизации и самообразованию | Т, ПР, ЛР |
| | 1. Уметь использовать базовые возможности информационных систем для решения задач фирмы;<br>2. Уметь внедрять компоненты систем предприятия, обеспечивающие информационную безопасность;<br>3. Уметь использовать системы электронного документооборота; | ОПК-7 Способность 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 | Т, ПР, ЛР |

| | | | |
|---|---|---|---|
| | 4. Уметь работать с информацией в глобальных компьютерных сетях. | защиты | |
| | 1. Уметь реализовывать на практике принципы политики безопасности;<br>2. Уметь использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности;<br>3. Уметь обосновывать организационно-технические мероприятия по защите информации;<br>4. Уметь использовать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации. | ПК-13 Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации | Т, ПР, ЛР |
| 3-й этап владение навыками | 1. Владеть пониманием социологического аспекта профессионализации и высокой мотивацией к выполнению профессиональной деятельности;<br>2. Владеть навыками творческого мышления для выполнения профессиональных задач в области обеспечения безопасности информационных технологий и защиты интересов личности, общества и государства. | ОК-5 Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики | Т, ПР, ЛР |
| | 1. Владеть методами самоанализа;<br>2. Владеть анализом и оценкой эффективности программы и результатов самообразования;<br>3. Владеть методами организации собственного обучения. | ОК-8 Способность к самоорганизации и самообразованию | Т, ПР, ЛР |
| | 1. Владеть методикой определения видов и форм информации, подверженной угрозам, анализировать угрозы информационно-вычислительным системам;<br>2. Владеть навыками работы с компьютером как средством | ОПК-7 Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания | Т, ПР, ЛР |

| | | | |
|---|---|---|---|
| | защиты информации. | информационных процессов и особенностей функционирования объекта защиты | |
| | 1. Владеть навыками анализа, обработки и интерпретации результатов решения прикладных задач управления;<br>2. Владеть навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью;<br>3. Владеть навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации;<br>4. Владеть навыками выявления и устранения угроз информационной безопасности;<br>5. Владеть навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий;<br>6. Владеть навыками внедрения, адаптации и настройки средств защиты прикладных ИС. | ПК-13 Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации | Т, ПР, ЛР |

Т - тестирование, ПР - практические работы, ЛР - лабораторные работы

### 4.3. Рейтинг-план дисциплины

Рейтинг-план дисциплины представлен в приложении 2.

### Примерные вопросы для экзамена

1. История развития информационной безопасности.
2. Современные направления развития информационной безопасности.
3. Структура государственной системы защиты информации.
4. Законодательство в области ИБ.
5. Защита государственной тайны в РФ.
6. Защита коммерческой тайны в РФ.
7. Классификация и содержание возможных угроз информации.
8. Причины и условия утечки защищаемой информации.
9. Понятие и особенности защищаемой информации.
10. Классификация защищаемой информации.
11. Методы защиты информации.
12. Правовые принципы защиты информации.
13. Организационные принципы защиты информации.
14. Способы защиты информации.
15. Понятие средства защиты информации и их классификация.

16. Технические средства защиты информации.
17. Построение систем защиты от угроз нарушения конфиденциальности информации.
18. Идентификация и аутентификация.
19. Особенности парольных систем аутентификации.
20. Криптографические методы защиты информации.
21. Построение систем защиты от угроз нарушения целостности.
22. Цифровые подписи.
23. Построение систем защиты от угроз нарушения доступности.
24. Руководящие документы Гостехкомиссии России.
25. Стандарт ГОСТ Р ИСО/МЭК 15408-2012.
26. Общие сведения о стандартах в информационной безопасности.
27. Системный подход на информационную безопасность.
28. Объектно-ориентированный подход на информационную безопасность.
29. Политики безопасности.
30. Административный уровень информационной безопасности.
31. Протоколирование и аудит.
32. Управление доступом.
33. Межсетевые экраны.
34. Туннелирование.
35. Анализ защищенности.
36. Обеспечение отказоустойчивости.
37. Лицензирование в сфере ИБ.
38. Сертификация в области защиты информации.
39. Методы борьбы с компьютерными вирусами.
40. Похищение документов, содержащих защищаемые сведения: характеристика и специфика.

**Образец экзаменационного билета**

---

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Башкирский государственный университет»
Институт истории и государственного управления

Направление
10.03.01Информационнаябезопасность

Дисциплина
«Основы информационной безопасности»

**ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 5**

1. Современные направления развития информационной безопасности.
2. Лицензирование в сфере ИБ.

Зав. кафедрой управления информационной безопасностью /А.С. Исмагилова /

---

Перевод оценки из 100-балльной в пятибалльную производится следующим образом:
- отлично – от 80 до 110 баллов (включая 10 поощрительных баллов);
- хорошо – от 60 до 79 баллов;
- удовлетворительно – от 45 до 59 баллов;
- неудовлетворительно – менее 45 баллов.

Критерии оценивания результатов экзамена: При выставлении баллов именно за экзамен (до 30 баллов в дополнение к баллам, полученным за другие виды отчетности) действует такой критерий оценки:

25-30 баллов

Студент дал полные, развернутые ответы на теоретический вопрос билета и правильно выполнил практическое задание, продемонстрировал знание функциональных возможностей, терминологии, умение применять теоретические знания. Студент без затруднений ответил на дополнительные вопросы.

17-24 баллов

Студент раскрыл в основном теоретический вопрос, однако допущены неточности в определении основных понятий. При ответе на дополнительные вопросы допущены небольшие неточности.

10-16 баллов

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. Теоретические вопросы в целом изложены достаточно, но с пропусками материала. Имеются принципиальные ошибки в логике построения ответа на вопрос.

1-10 баллов

Ответ на теоретический вопрос свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Студент не смог ответить ни на один дополнительный вопрос.

**Тестирование в Moodle**

Модуль 1.

1. Годом принятия Конституции Российской Федерации является
а) 1993
б) 1992
в) 1991
г) 1994

2. ФСТЭК
а) Федеральная служба по техническому и экспортному контролю
б) Федеральная служба технического и эксплуатационного контроля
в) Федеральная служба по техническому и экспертному контролю
г) Федеральная служба технологического и экспертного контроля

3. Предоставление информации - это
а) действия, направленные на получение информации определенным кругом лиц или передачу
б) действия, направленные на распространение сведений в средствах массовой информации
в) действия, направленные на получение информации неопределенным кругом лиц или передачу
г) действия, направленные на получение информации как определенным так и неопределенным

Модуль 2.

1. Требования к системе защиты информации, обрабатываемой в государственных информационных системах (ГИС) определяются в зависимости от
а) класса защищенности ИС
б) угроз безопасности информации

в) уровня квалификации обслуживающего ГИС персонала
г) уровня квалификации сотрудников

2. Информация в зависимости от категории доступа к ней подразделяется на
а) ограниченного доступа
б) общедоступную
в) широкого доступа
г) особо конфиденциальную

**Темы практических работ**

Модуль 1.

1. Научные и законодательные определения информации. Соотношение понятий «информация», «документированная информация», «информационные ресурсы», «документ».
2. Сущность и понятие информационной безопасности. Связь информационной безопасности с информатизацией общества.
3. Понятие и назначение доктрины информационной безопасности. Основные положения доктрины информационной безопасности Российской Федерации и их реализация.
4. Сущность и понятие защиты информации. Уязвимость информации. Цели защиты информации.
5. Законодательная база защиты документированной информации в РФ.
6. Подзаконные нормативно-правовые акты в сфере защиты информации.
7. Понятие и виды конфиденциальной информации в современном российском законодательстве.
8. Государственная тайна, ее нормативное регулирование.
9. Правовой режим персональных данных. Общая характеристика Федерального закона «О персональных данных».
10. Понятие коммерческой тайны. Общая характеристика Федерального закона «О коммерческой тайне».
11. Понятие и разновидности служебной и профессиональной тайн.
12. Перечень конфиденциальных сведений и Перечень конфиденциальных документов, методика их формирования.
13. Служба конфиденциального делопроизводства, ее статус в структуре организации. Квалификационные характеристики и требования к сотрудникам службы КД.
14. Цели и задачи, права и обязанности, нормативно-методическая база службы КД.
15. Анализ угроз несанкционированного получения документированной информации, хищения или уничтожения документов, их фальсификации или подмены. Предполагаемые рубежи и уровни защиты документопотоков.

Модуль 2.

1. Понятие «защищенный документооборот», его цели и задачи.
2. Гриф ограничения доступа к документу: понятие, назначение, виды.
3. Избирательность и разрешительная система доступа к конфиденциальным документам.
4. Прием и регистрация конфиденциальных документов.
5. Принципы и этапы документирования конфиденциальных сведений.
6. Учетные формы: виды, правила оформления и ведения.
7. Составление, учет и уничтожение проектов конфиденциальных документов.
8. Особенности оформления реквизитов конфиденциальных документов.
9. Правила издания, копирования и тиражирования конфиденциальных документов.
10. Экспедиционная обработка исходящих конфиденциальных документов.
11. Организация и контроль исполнения конфиденциальных документов. Правила работы исполнителя.

12. Экспертиза ценности конфиденциальных документов.
13. Номенклатура конфиденциальных дел. Установление сроков конфиденциальности при составлении номенклатуры дел.
14. Правила формирования и оформления конфиденциальных дел.
15. Учет выдачи дел во временное пользование.
16. Подготовка конфиденциальных дел и документов для архивного хранения.

**Темы лабораторных работ**

Модуль 1.

1. Понятие и виды конфиденциальной информации в современном российском законодательстве.
2. Государственная тайна.
3. Правовой режим персональных данных. Общая характеристика Федерального закона «О персональных данных».
4. Понятие коммерческой тайны. Общая характеристика Федерального закона «О коммерческой тайне».
5. Понятие и разновидности служебной и профессиональной тайн.
6. Гражданско-правовая, административная и дисциплинарная ответственность за правонарушения в информационной сфере.

Модуль 2.

1. Служба конфиденциального делопроизводства (КД), ее статус в структуре организации.
2. Квалификационные характеристики и требования к сотрудникам службы КД.
3. Цели и задачи, права и обязанности, нормативно-методическая база службы КД.
4. Анализ угроз несанкционированного получения документированной информации, хищения или уничтожения документов, их фальсификации или подмены. Предполагаемые рубежи и уровни защиты документопотоков.
5. Экспертиза ценности конфиденциальных документов.
6. Номенклатура конфиденциальных дел. Установление сроков конфиденциальности при составлении номенклатуры дел.
7. Правила формирования и оформления конфиденциальных дел.

**Примерные темы курсовых работ**

1. История и современные направления защиты информации.
2. Источники угроз защищаемой информации.
3. Организационно-правовые формы засекречивания информации: перечневая форма и система первоначального засекречивания.
4. Классификация защищаемой информации по принадлежности, содержанию и степени секретности.
5. Правовые основы защиты коммерческой тайны за рубежом и в России.
6. Правовые основы защиты коммерческой тайны за рубежом и в России.
7. Ответственность за нарушение законодательства о коммерческой тайне.
8. Организация защиты от несанкционированного доступа конфиденциальной информации, обрабатываемой средствами вычислительной техники.
9. Организация защиты конфиденциальной информации от утечки по техническим каналам.
10. Защита информации, составляющей профессиональную тайну.
11. Защита информации, составляющей банковскую тайну.
12. Защита сведений, составляющих личную тайну.
13. Защита информации об оперативно-розыскной деятельности.
14. Основные концептуальные положения системы защиты информации.
15. Основные положения концепции информационной безопасности.

16. Угрозы конфиденциальной информации.
17. Действия, приводящие к неправомерному овладению защищаемой информацией.
18. Правовая защита информации.
19. Организационная защита информации.
20. Виды инженерно-технических средств защиты информации и их характеристика.
21. Сущность и понятие информационной безопасности, характеристика ее составляющих.
22. Значение информационной безопасности для субъектов информационных отношений.
23. Место информационной безопасности в системе национальной безопасности.
24. Современная концепция информационной безопасности.
25. Понятие и сущность защиты информации, ее место в системе информационной безопасности.
26. Цели и концептуальные основы защиты информации.
27. Критерии, условия и принципы отнесения информации к защищаемой.
28. Носители защищаемой информации.
29. Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности.
30. Понятие и структура угроз защищаемой информации.
31. Источники, виды и методы дестабилизирующего воздействия на защищаемую информацию.
32. Причины, обстоятельства и условия, вызывающие дестабилизирующее воздействие на защищаемую информацию.
33. Виды уязвимости информации и формы ее проявления.
34. Каналы и методы несанкционированного доступа к конфиденциальной информации.
35. Направления, виды и особенности деятельности спецслужб по несанкционированному доступу к конфиденциальной информации.
36. Методологические подходы к защите информации и принципы ее организации.
37. Классификация методов и средств защиты информации.
38. Кадровое и ресурсное обеспечение защиты информации.

**Критерии оценивания курсовой работы**

Оценка «отлично»:

работа выполнена в полном объеме и изложена грамотным языком в определенной логической последовательности с точным использованием специализированной терминологии; показано уверенное владение прикладными программами.

Оценка «хорошо»:

работа выполнена в полном объеме,но имеет один из недостатков:в работе допущены один-два недочета при освещении основного содержания ответа;нет определенной логической последовательности, неточно используется специализированная терминология;

Оценка «удовлетворительно»:

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.

## 5. Учебно-методическое и информационное обеспечение дисциплины

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

**Основная литература:**

1. Аверченков, В.И. История развития системы государственной безопасности России: учебное пособие / В.И. Аверченков, В.В. Ерохин, О.М. Голембиовская. - 3-е изд., стер. -

Москва: Издательство «Флинта», 2016. - 192 с. - Библиогр. в кн. - ISBN 978-5-9765-1259-7; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93267
2. Малюк, А.А. Защита информации в информационном обществе: учебное пособие / А.А. Малюк. - Москва: Горячая линия-Телеком, 2015. - 229 с.: ил., схем., табл. - Библиогр. в кн. - ISBN 978-5-9912-0481-1; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=457170

**Дополнительная литература:**

3. Малюк, А.А. Теория защиты информации / А.А. Малюк. - Москва: Горячая линия - Телеком, 2012. - 184 с.: ил. - Библиогр. в кн. - ISBN 978-5-9912-0246-6; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=253553.
4. Вирен, Г. Современные медиа: приемы информационных войн: учебное пособие / Г. Вирен. - Москва: Аспект Пресс, 2017. - 127 с. - Библиогр. в кн. - ISBN 978-5-7567-0824-0; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=457409

### 5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины

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 –сайт ФСТЭК России
6. 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 – Новая электронная библиотека;
10. www. edu.ru – Федеральный портал российского образования;
11. www.elibrary.ru – Научная электронная библиотека;
12. www.nehudlit.ru – Электронная библиотека учебных материалов.
13. 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.
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. *учебная аудитория для проведения занятий*** | Лекции, практические | **Аудитория № 403** Учебная мебель, доска, Мультимедийный- | 1. Windo |

| | | | |
|---|---|---|---|
| ***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).<br>**2.** ***учебная аудитория для проведения лабораторных работ:*** компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус), Лаборатория систем и сетей передачи данных, сетей и систем передачи информации, программно-аппаратных средств обеспечения информационной безопасности аудитория №507 (гуманитарный корпус).<br>**3.** ***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).<br>**4.** ***учебная аудитория для курсового проектирования (выполнения курсовых работ):***аудитория №613 (гуманитарный корпус). | занятия, лабораторные занятия, курсовое проектирование (выполнение курсовых работ), групповые и индивидуальные консультации, текущий контроль, промежуточная аттестация | проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия.<br>**Аудитория № 405**<br>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.<br>**Аудитория № 413**<br>Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт APAPT MA1225 – 1 шт.<br>**Аудитория № 415**<br>Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт APAPT MA1225 – 1 шт.<br>**Аудитория № 416**<br>Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт.<br>**Аудитория № 418**<br>Учебная мебель, доска, Экран настенный Lumien Master Pikture 153*203 Matte White Fiber Clas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт.<br>**Аудитория № 419**<br>Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт.<br>**Аудитория № 515**<br>Учебная мебель, доска, терминал видео конференц-связи 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 | ws 8 Russian Russian OLP NL AcademicEditio n и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные.<br>2. Micros oft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.<br>3. Систе ма централизован ного тестирования БашГУ (Moodle).GNU General Public License. |

| | | | |
|---|---|---|---|
| **5.** ***учебная аудитория 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).<br>**6.** ***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), компьютерный класс аудитория № 420 (гуманитарный корпус).<br>**7.** ***помещения для самостоятельной работы:*** читальный зал библиотеки аудитория 402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус).<br>**8.*помещение для хранения и профилактического*** | | 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром.<br>**Аудитория № 516**<br>Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран.<br>**Аудитория № 509**<br>Учебная мебель, доска, мобильное мультимедийное оборудование.<br>**Аудитория № 608**<br>Учебная мебель, доска, мобильное мультимедийное оборудование.<br>**Аудитория № 609**<br>Учебная мебель, доска, мобильное мультимедийное оборудование.<br>**Аудитория № 610**<br>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.<br>**Аудитория № 613**<br>Учебная мебель, доска, моноблок стационарный – 15 шт.<br>**Компьютерный класс аудитория № 420**<br>Учебная мебель, моноблоки стационарные 15 шт.<br>**Компьютерный класс аудитория № 404**<br>Учебная мебель, компьютеры -15 штук.<br>**Аудитория 402 читальный зал библиотеки**<br>Учебная мебель, доска, компьютеры в комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура, мышь, стеллажи, шкафы картотечные, комбинированные.<br>**Лаборатория систем и сетей передачи данных, сетей и систем передачи информации, программно-аппаратных средств обеспечения информационной безопасности № 507**<br>Учебная мебель, учебно-наглядные пособия, аудиторная доска трехсекционная, плакаты с тематикой технические средства обработки информации, стенд "Устройство ПК".<br>**Аудитория № 523**<br>Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт. | |

| | | | |
|---|---|---|---|
| ***обслуживания учебного оборудования:***аудитория № 523 (гуманитарный корпус). | | | |

**Приложение 1**

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

**Содержание рабочей программы**
дисциплины **Основы информационной безопасности**
на 1 семестр ОФО

| Вид работы | Объем дисциплины |
|---|---|
| Общая трудоемкость дисциплины (ЗЕТ / часов) | 5ЗЕТ / 180часов |
| Учебных часов на контактную работу с преподавателем: | 57,2 |
| лекций | 18 |
| практических/ семинарских | 18 |
| лабораторных | 18 |
| других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР) | 3,2 |
| Учебных часов на самостоятельную работу обучающихся (СР) | 88 |
| Учебных часов на подготовку к экзамену | 34,8 |

Форма контроля:
экзамен 1 семестр
В том числе:
курсовая работа 1 семестр, контактных часов – 2, часов на самостоятельную работу – 20

| № | Тема и содержание | Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах) | | | | Основная и дополнительная литература, рекомендуемая студентам (номера из списка) | Задания по самостоятельной работе студентов | Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.) |
|---|---|---|---|---|---|---|---|---|
| | | ЛК | ПР | ЛР | СРС | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 1 | Информационные угрозы<br>Понятие информационных угроз. Понятие информации. | 2 | 2 | | 4 | 1 - 4 | Самостоятельное изучение рекомендуемых источников и материалов | Т, ПР, ЛР |
| 2 | Информационные войны. Информационные угрозы безопасности РФ. | 2 | 2 | 2 | 5 | 1 - 4 | Самостоятельное изучение рекомендуемых источников и материалов | Т, ПР, ЛР |
| 3 | Виды противников. Хакеры. Виды возможных нарушений информационной системы. | 2 | 2 | 2 | 5 | 1 - 4 | Самостоятельное изучение рекомендуемых источников и материалов | Т, ПР, ЛР |
| 4 | Общая классификация информационных угроз. | 2 | 2 | 2 | 5 | 1 - 4 | Самостоятельное изучение рекомендуемых источников и материалов | Т, ПР, ЛР |
| 5 | Причины уязвимостей компьютерных сетей. | 2 | 2 | 2 | 5 | 1 - 4 | Самостоятельное изучение | Т, ПР, ЛР |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | рекомендуемых источников и материалов | |
| 6 | Правовое регулирование защиты информации Доктрина ИБ. | 2 | 2 | 2 | 9 | 1 - 4 | Самостоятельное изучение рекомендуемых источников и материалов | Т, ПР, ЛР |
| 7 | Анализ статей УК, других нормативных актов | 2 | 2 | 4 | 8 | 1 - 4 | Самостоятельное изучение рекомендуемых источников и материалов | Т, ПР, ЛР |
| 8 | Нормативные документы, регулирующие информационную деятельность в РФ и мире. | 2 | 2 | 2 | 8 | 1 - 4 | Самостоятельное изучение рекомендуемых источников и материалов | Т, ПР, ЛР |
| 9 | Стандарты ИБ. | 2 | 2 | 2 | 9 | 1 - 4 | Самостоятельное изучение рекомендуемых источников и материалов | Т, ПР, ЛР |
| | Всего | 18 | 18 | 18 | 88 | | | |
| 3 | Курсовая работа | | | | 20 | 1 - 4 | Изучение терминологического фундамента, приобретение навыков проведения анализа угроз информационной безопасности, выполнение основных | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | этапов решения задач информационной безопасности, изучение методов и средств обеспечения информационной безопасности, а также методов нарушения конфиденциальности, целостности и доступности информации. | |

Т - тестирование, ПР - практические работы, ЛР - лабораторные работы

Приложение 2

**Рейтинг-план дисциплины**
Основы информационной безопасности

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