**Федеральное государственное бюджетное образовательное учреждение высшего образования**
**«Омский государственный аграрный университет имени П.А. Столыпина»**

**Экономический факультет**

---

**ОПОП по направлению подготовки**
**09.03.02 Информационные системы и технологии**

# МЕТОДИЧЕСКИЕ УКАЗАНИЯ
# по освоению учебной дисциплины

# Б1.О.22 Безопасность информационных технологий и систем

**Направленность (профиль) «Информационные системы и технологии в бизнесе»**

| | |
|---|---|
| Обеспечивающая преподавание дисциплины кафедра | Кафедра экономики, бухгалтерского учета и финансового контроля |
| Разработчик, канд. экон. наук, доцент | В.В. Кузнецова |

Омск 2022

СОДЕРЖАНИЕ

## ВВЕДЕНИЕ

1. Настоящее издание является основным организационно-методическим документом учебно-методического комплекса по дисциплине в составе основной профессиональной образовательной программы высшего образования (ОПОП ВО). Оно предназначено стать для них методической основой по освоению данной дисциплины.

2. Содержательной основой для разработки настоящих методических указаний послужила Рабочая программа дисциплины, утвержденная в установленном порядке.

3. Методические аспекты развиты в учебно-методической литературе и других разработках, входящих в состав УМК по данной дисциплине.

4. Доступ обучающихся к электронной версии Методических указаний по изучению дисциплины, обеспечен в информационно-образовательной среде университета.

При этом в электронную версию могут быть внесены текущие изменения и дополнения, направленные на повышение качества настоящих методических указаний.

### Уважаемые обучающиеся!

Приступая к изучению новой для Вас учебной дисциплины, начните с вдумчивого прочтения разработанных для Вас кафедрой специальных методических указаний. Это поможет Вам вовремя понять и правильно оценить ее роль в Вашем образовании.

Ознакомившись с организационными требованиями кафедры по этой дисциплине и соизмерив с ними свои силы, Вы сможете сделать осознанный выбор собственной тактики и стратегии учебной деятельности, уберечь самих себя от неразумных решений по отношению к ней в начале семестра, а не тогда, когда уже станет поздно. Используя эти указания, Вы без дополнительных осложнений подойдете к промежуточной аттестации по этой дисциплине. Успешность аттестации зависит, прежде всего, от Вас. Ее залог – ритмичная, целенаправленная, вдумчивая учебная работа, в целях обеспечения которой и разработаны эти методические указания.

## 1. Место учебной дисциплины в подготовке выпускника

Учебная дисциплина относится к дисциплинам ОПОП университета, состав которых определяется вузом и требованиями ФГОС.

***Цель дисциплины*** – сформировать четкое представление и понимание теоретических и практических знаний о современных методах обеспечения информационной безопасности в информационных инфраструктурах государственных и частнопредпринимательских предприятий и организаций.

***В ходе освоения дисциплины обучающийся должен:***

решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

владеть:

– методами и средствами для решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности;

– методикой решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности;

– навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно исследовательской работе с учетом требований информационной безопасности;

знать:

– принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности;

– применять информационно- коммуникационных технологий и с учетом основных требований информационной безопасности для решения задач профессиональной деятельности;

– принципы, методы подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности;

уметь:

– использовать методы и средства для решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности;

– решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности;

– делать обзор, аннотации, составление рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

### 1.1. Перечень компетенций с указанием этапов их формирования в результате освоения учебной дисциплины:

| **Компетенции, в формировании которых задействована дисциплина** | | **Код и наименование индикатора достижений компетенции** | **Компоненты компетенций,** формируемые в рамках данной дисциплины (как ожидаемый результат ее освоения) | | |
|---|---|---|---|---|---|
| код | наименование | | знать и понимать | уметь делать (действовать) | владеть навыками (иметь навыки) |
| ***Общепрофессиональные компетенции*** | | | | | |
| ОПК-3 | Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | ИД-1$_{ОПК-3}$ Выбирает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности | Умеет использовать методы и средства для решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности | Владеет методами и средствами для решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности |

| Компетенции, в формировании которых задействована дисциплина | | Код и наименование индикатора достижений компетенции | Компоненты компетенций, формируемые в рамках данной дисциплины (как ожидаемый результат ее освоения) | | |
|---|---|---|---|---|---|
| код | наименование | | знать и понимать | уметь делать (действовать) | владеть навыками (иметь навыки) |
| ***Общепрофессиональные компетенции*** | | | | | |
| ОПК-3 | Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | ИД-2$_{ОПК-3}$ Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Знает как применять информационно-коммуникационные технологий и с учетом основных требований информационной безопасности решает задачи профессиональной деятельности | Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности | Владеет методикой решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности |
| | | ИД-3$_{ОПК-3}$ Участвует в подготовке обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности | Знает принципы, методы подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности | Умеет составлять обзор, писать аннотации, рефераты, научные доклады, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности | Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно исследовательской работе с учетом требований информационной безопасности |

**1.2. Описание показателей, критериев и шкал оценивания и этапов формирования компетенций в рамках дисциплины**

| Индекс и название компетенции | Код индикатора достижений компетенции | Индикаторы компетенции | Показатель оценивания – знания, умения, навыки (владения) | Уровни сформированности компетенций | | | | Формы и средства контроля формирования компетенций |
|---|---|---|---|---|---|---|---|---|
| | | | | компетенция не сформирована | минимальный | средний | высокий | |
| | | | | Оценки сформированности компетенций | | | | |
| | | | | 2 | 3 | 4 | 5 | |
| | | | | *Оценка «неудовлетворительно»* | *Оценка «удовлетворительно»* | *Оценка «хорошо»* | *Оценка «отлично»* | |
| | | | | Характеристика сформированности компетенции | | | | |
| | | | | Компетенция в полной мере не сформирована. Имеющихся знаний, умений и навыков недостаточно для решения практических (профессиональных) задач | Сформированность компетенции соответствует минимальным требованиям. Имеющихся знаний, умений, навыков в целом достаточно для решения практических (профессиональных) задач | Сформированность компетенции в целом соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в целом достаточно для решения стандартных практических (профессиональных) задач | Сформированность компетенции полностью соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в полной мере достаточно для решения сложных практических (профессиональных) задач | |
| Критерии оценивания | | | | | | | | |
| ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | ИД-1$_{ОПК-3}$ | Полнота знаний | Знает основные принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Не знает принципов, методов и средств решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Поверхностно ориентируется в методах и средствах решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Твёрдо знает основные принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Глубоко и прочно освоил применяемые принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Тестирование, реферат, проверка выполненных лабораторных работ, опрос |

| Индекс и название компетенции | Код индикатора достижений компетенции | Индикаторы компетенции | Показатель оценивания – знания, умения, навыки (владения) | Уровни сформированности компетенций | | | | Формы и средства контроля формирования компетенций |
|---|---|---|---|---|---|---|---|---|
| | | | | компетенция не сформирована | минимальный | средний | высокий | |
| | | | | Оценки сформированности компетенций | | | | |
| | | | | 2 | 3 | 4 | 5 | |
| | | | | *Оценка «неудовлетворительно»* | *Оценка «удовлетворительно»* | *Оценка «хорошо»* | *Оценка «отлично»* | |
| | | | | Характеристика сформированности компетенции | | | | |
| | | | | | | | | |
| Критерии оценивания | | | | | | | | |
| ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | ИД-1$_{ОПК-3}$ | Наличие умений | Умеет использовать основные принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Не умеет использовать основные принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Умеет самостоятельно применять принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Умеет правильно использует полученные знания при решении стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Имеет навыки применения методы и приемы информационной безопасности, использует информационно-коммуникационные технологии | Тестирование, реферат, проверка выполненных лабораторных работ, опрос |
| | | Наличие навыков (владение опытом) | Владения основными принципами, методами и средствами решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Не владеет основными принципами, методами и средствами решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Имеет поверхностные навыки применения основных принципов, методов и средств решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Имеет навыки применения методов и средств решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Уверенно владеет навыками применения методами и приемами информационной безопасности, использует информационно-коммуникационные технологии | |

| Индекс и название компетенции | Код индикатора достижений компетенции | Индикаторы компетенции | Показатель оценивания – знания, умения, навыки (владения) | Уровни сформированности компетенций | | | | Формы и средства контроля формирования компетенций |
|---|---|---|---|---|---|---|---|---|
| | | | | компетенция не сформирована | минимальный | средний | высокий | |
| | | | | Оценки сформированности компетенций | | | | |
| | | | | 2 | 3 | 4 | 5 | |
| | | | | *Оценка «неудовлетворительно»* | *Оценка «удовлетворительно»* | *Оценка «хорошо»* | *Оценка «отлично»* | |
| | | | | Характеристика сформированности компетенции | | | | |
| | | | | | | | | |
| Критерии оценивания | | | | | | | | |
| ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | ИД-2$_{ОПК-3}$ | Полнота знаний | Знает методики решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Не знает методики решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Поверхностно ориентируется в методиках решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Твердо знает методики решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | В совершенстве знает методики решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Тестирование, реферат, проверка выполненных лабораторных работ, опрос |
| | | Наличие умений | Умеет применять методики решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Не умеет применять методики решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Умеет применять методики решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Умеет самостоятельно применять методики решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Умеет грамотно и самостоятельно применять методики решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | |

| Индекс и название компетенции | Код индикатора достижений компетенции | Индикаторы компетенции | Показатель оценивания – знания, умения, навыки (владения) | Уровни сформированности компетенций | | | | Формы и средства контроля формирования компетенций |
|---|---|---|---|---|---|---|---|---|
| | | | | компетенция не сформирована | минимальный | средний | высокий | |
| | | | | Оценки сформированности компетенций | | | | |
| | | | | 2 | 3 | 4 | 5 | |
| | | | | *Оценка «неудовлетворительно»* | *Оценка «удовлетворительно»* | *Оценка «хорошо»* | *Оценка «отлично»* | |
| | | | | Характеристика сформированности компетенции | | | | |
| | | | | | | | | |
| Критерии оценивания | | | | | | | | |
| ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | ИД-2$_{ОПК-3}$ | Наличие навыков (владение опытом) | Владение методикой решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Не владеет методикой решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Имеет поверхностные навыки владения методикой решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Имеет навыки владения методикой решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | В совершенстве владеет навыками применения методик решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Тестирование, реферат, проверка выполненных лабораторных работ, опрос |
| | ИД-3$_{ОПК-3}$ | Полнота знаний | Знает принципы, методы подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности | Не знает принципы, методы подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности | Знает особенности принципов, методов подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности | Знает особенности принципов, методов подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности, но допускает небольшие ошибки. | В совершенстве знает особенности принципов, методов подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности | |

| Индекс и название компетенции | Код индикатора достижений компетенции | Индикаторы компетенции | Показатель оценивания – знания, умения, навыки (владения) | Уровни сформированности компетенций | | | | Формы и средства контроля формирования компетенций |
|---|---|---|---|---|---|---|---|---|
| | | | | компетенция не сформирована | минимальный | средний | высокий | |
| | | | | Оценки сформированности компетенций | | | | |
| | | | | 2 | 3 | 4 | 5 | |
| | | | | *Оценка «неудовлетворительно»* | *Оценка «удовлетворительно»* | *Оценка «хорошо»* | *Оценка «отлично»* | |
| | | | | Характеристика сформированности компетенции | | | | |
| | | | | | | | | |
| Критерии оценивания | | | | | | | | |
| ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | ИД-3$_{ОПК-3}$ | Наличие умений | Умеет проводить подготовку обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности | Не умеет проводить подготовку обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности | Не умеет участвовать в подготовке обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности | Умеет проводить подготовку обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности | Умеет грамотно проводить подготовку обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности | Тестирование, реферат, проверка выполненных лабораторных работ, опрос |
| | | Наличие навыков (владение опытом) | Владение методами и методиками проводить подготовку обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности | Не владеет методами и методиками проводить подготовку обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности | Имеет поверхностные навыки работы в проведении подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности | Имеет основные навыки в проведении подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности | В совершенстве владеет методиками работы в подготовке обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности | |

## 2. Структура учебной работы, содержание и трудоёмкость основных элементов дисциплины

### 2.1. Организационная структура, трудоемкость и план изучения дисциплины

Дисциплина обучающимися очной формы обучения изучается в четвертом семестре второго курса; обучающимися заочной формы обучения – на третьем курсе зимняя и летняя сессия.

*Очная форма обучения*: продолжительность четвертого семестра 17 1/6 недель.

*Заочная форма обучения*: продолжительность обучения, включая зимнюю и летнюю сессию 17 и 14 недель соответственно.

| Вид учебной работы | | Трудоемкость, час | | |
|---|---|---|---|---|
| | | семестр, курс* | | |
| | | очная | заочная форма | |
| | | 4 сем. | 3 курс (начитка) | 3 курс |
| **1. Аудиторные занятия, всего** | | 64 | 2 | 12 |
| – лекции | | 30 | 2 | 6 |
| – лабораторные работы | | 34 | - | 6 |
| **2. Внеаудиторная академическая работа** | | 80 | 34 | 92 |
| **2.1 Фиксированные виды внеаудиторных самостоятельных работ:** | | 10 | - | 10 |
| Выполнение и сдача индивидуального задания в виде** | | | - | |
| – реферата | | 10 | - | 10 |
| **2.2 Самостоятельное изучение тем/вопросов программы** | | - | 34 | - |
| **2.3 Самоподготовка к аудиторным занятиям** | | 50 | - | 50 |
| **2.4 Самоподготовка к участию и участие в контрольно-оценочных мероприятиях,** проводимых в рамках текущего контроля освоения дисциплины (*за исключением учтённых в пп. 2.1 – 2.2):* | | 20 | - | 32 |
| **3. Получение дифференцированного зачёта по итогам освоения дисциплины** | | + | - | 4 |
| **ОБЩАЯ трудоемкость дисциплины:** | **Часы** | **4** | **36** | **108** |
| | **Зачетные единицы** | **144** | **1** | **3** |

*Примечание:*
* – ***семестр*** – для очной и очно-заочной формы обучения, ***курс*** – для заочной формы обучения;
** – КР/КП, реферата/эссе/презентации, контрольной работы (для обучающихся заочной формы обучения), расчетно-графической (расчетно-аналитической) работы и др.;

### *2.2.* Укрупнённая содержательная структура учебной дисциплины и общая схема её реализации в учебном процессе

| | Номер и наименование раздела дисциплины. Укрупненные темы раздела | Трудоемкость раздела и ее распределение по видам учебной работы, час. | | | | | | | Формы текущего контроля успеваемости и промежуточной аттестации | №№ компетенций, на формирование которых ориентирован раздел |
|---|---|---|---|---|---|---|---|---|---|---|
| | | общая | Аудиторная работа | | | | ВАРС | | | |
| | | | всего | лекции | занятия | | всего | Фиксированные виды | | |
| | | | | | практические (всех форм) | лабораторные | | | | |
| **Очная форма обучения** | | | | | | | | | | |
| 1 | Основные понятия теории информационной безопасности | 12 | 4 | 2 | - | 2 | 8 | 10 | Проверка выполненных лабораторных заданий на лабораторных занятиях, опрос, в том числе по самостоятельно изученным вопросам, оценка подготовленного реферата, тестирование | ИД-1$_{ОПК-3}$ ИД-2$_{ОПК-3}$ ИД-2$_{ОПК-3}$ |
| 2 | Информация как объект защиты | 12 | 4 | 2 | - | 2 | 8 | | | |
| 3 | Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности | 14 | 6 | 2 | - | 4 | 8 | | | |
| 4 | Угрозы информационной безопасности | 16 | 6 | 2 | - | 4 | 10 | | | |
| 5 | Построение систем защиты от угрозы нарушения конфиденциальности | 22 | 14 | 6 | - | 8 | 8 | | | |
| 6 | Построение системы защиты от угрозы нарушения целостности информации и отказа доступа | 22 | 14 | 6 | - | 8 | 8 | | | |
| 7 | Политика и модели безопасности | 18 | 8 | 4 | - | 4 | 10 | | | |
| 8 | Обзор международных стандартов информационной безопасности | 16 | 6 | 4 | - | 2 | 10 | | | |
| 9 | Информационные войны и информационное противоборство | 12 | 2 | 2 | - | - | 10 | | | |
| | Промежуточная аттестация | × | × | × | × | × | × | × | Зачет с оценкой | |
| | Итого по дисциплине | 144 | 64 | 30 | x | 34 | 80 | 10 | - | |

| | Номер и наименование раздела дисциплины. Укрупненные темы раздела | Трудоемкость раздела и ее распределение по видам учебной работы, час. | | | | | | | Формы текущего контроля успеваемости и промежуточной аттестации | №№ компетенций, на формирование которых ориентирован раздел |
|---|---|---|---|---|---|---|---|---|---|---|
| | | общая | Аудиторная работа | | | | ВАРС | | | |
| | | | всего | лекции | занятия | | всего | Фиксированные виды | | |
| | | | | | практические (всех форм) | лабораторные | | | | |
| **Заочная форма обучения** | | | | | | | | | | |
| 1 | Основные понятия теории информационной безопасности | 14,5 | 0,5 | 0,5 | - | - | 14 | 10 | Проверка выполненных лабораторных заданий на лабораторных занятиях, опрос, в том числе по самостоятельно изученным вопросам, оценка подготовленного реферата, тестирование | ИД-1$_{ОПК-3}$ ИД-2$_{ОПК-3}$ ИД-2$_{ОПК-3}$ |
| 2 | Информация как объект защиты | 11 | 1 | 1 | - | - | 10 | | | |
| 3 | Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности | 11 | 1 | 1 | - | - | 10 | | | |
| 4 | Угрозы информационной безопасности | 16,5 | 0,5 | 0,5 | - | - | 16 | | | |
| 5 | Построение систем защиты от угрозы нарушения конфиденциальности | 17 | 3 | 1 | - | 2 | 14 | | | |
| 6 | Построение системы защиты от угрозы нарушения целостности информации и отказа доступа | 19 | 5 | 1 | - | 4 | 14 | | | |
| 7 | Политика и модели безопасности | 19 | 1 | 1 | - | - | 18 | | | |
| 8 | Обзор международных стандартов информационной безопасности | 15 | 1 | 1 | - | - | 14 | | | |
| 9 | Информационные войны и информационное противоборство | 17 | 1 | 1 | - | - | 16 | | | |
| | Промежуточная аттестация | 4 | × | × | × | × | × | × | Зачет с оценкой | |
| | Итого по дисциплине | 144 | 14 | 8 | x | 6 | 126 | 10 | 4 | |

## 3. Общие организационные требования к учебной работе обучающегося

### 3.1. Организация занятий и требования к учебной работе обучающегося

Организация занятий по дисциплине носит циклический характер. По всем разделам предусмотрена взаимоувязанная цепочка учебных работ: лекция – самостоятельная работа обучающихся (аудиторная и внеаудиторная). На занятиях студенческая группа получает задания и рекомендации.

Для своевременной помощи обучающимся при изучении дисциплины кафедрой организуются индивидуальные и групповые консультации, устанавливается время приема выполненных работ.

Учитывая статус дисциплины к её изучению предъявляются следующие организационные требования:

– обязательное посещение обучающимся всех видов аудиторных занятий;

– ведение конспекта в ходе лекционных занятий;

– качественная самостоятельная подготовка к лабораторным занятиям, активная работа на них;

– активная, ритмичная самостоятельная аудиторная и внеаудиторная работа обучающегося; своевременная сдача преподавателю отчетных документов по аудиторным и внеаудиторным видам работ;

– в случае наличия пропущенных обучающимся занятиям, необходимо получить консультацию по подготовке и оформлению отдельных видов заданий.

Для успешного освоения дисциплины, обучающемуся предлагаются учебно-информационные источники в виде учебной, учебно-методической литературы по всем разделам.

## 4. Лекционные занятия

Для изучающих дисциплину читаются лекции в соответствии с планом, представленным в таблице ниже.

| № раздела | № лекции | Тема лекции. Основные вопросы темы | Трудоемкость по разделу, час. | | Применяемые интерактивные формы обучения |
|---|---|---|---|---|---|
| | | | очная форма | заочная форма | |
| 1 | 1 | Тема: *Основные понятия теории информационной безопасности*<br>1. История становления информационной безопасности<br>2. Предметная область теории информационной безопасности<br>3. Систематизация понятий в области защиты информации<br>4. Основные термины и определения правовых понятий в области информационных отношений и защиты информации<br>5. Понятия предметной области «Защита информации»<br>6. Основные принципы построения систем защиты<br>7. Концепция комплексной защиты информации<br>8. Задачи защиты информации<br>9. Средства реализации комплексной защиты информации | 2 | 0,5 | Лекция-дискуссия |
| 2 | 2 | Тема: Информация как объект защиты<br>1. Понятие об информации как объекте защиты<br>2. Уровни предоставления информации<br>3. Основные свойства защищаемой информации<br>4. Виды и формы представления информации. Информационные ресурсы<br>5. Структура и шкала ценности информации. Классификация информационных ресурсов<br>6. Правовой режим информационных ресурсов | 2 | 1 | Лекция-дискуссия |
| 3 | 3 | Тема: *Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности*<br>1. Информационная безопасность и ее место в системе национальной безопасности Российской Федерации<br>2. Органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность | 2 | 1 | - |
| 4 | 4 | Тема: *Угрозы информационной безопасности*<br>1. Анализ уязвимостей системы<br>2. Классификация угроз информационной безопасности<br>3. Основные направления и методы реализации угроз<br>4. Неформальная модель нарушителя<br>5. Оценка уязвимости системы | 2 | 0,5 | - |
| 5 | 5-7 | Тема: *Построение системы защиты от угрозы нарушения конфиденциальности*<br>1. Определение и основные способы несанкционированного доступа<br>2. Методы защиты от НСД<br>3. Организационные методы защиты от НСД.<br>4. Инженерно-технические методы защиты от НСД. Построение системы защиты от угрозы утечки по техническим каналам<br>5. Идентификация и аутентификация<br>6. Основные направления и цели использования криптографических методов<br>7. Защита от угрозы нарушения конфиденциальности на уровне содержания информации | 6 | 1 | - |

| № | | Тема лекции. Основные вопросы темы | Трудоемкость по разделу, час. | | Применяемые интерактивные формы обучения |
|---|---|---|---|---|---|
| раздела | лекции | | очная форма | заочная форма | |
| 6 | 8-10 | Тема: *Построение систем защиты от угрозы нарушения целостности информации и отказа доступа*<br>1. Защита целостности информации при хранении<br>2. Защита целостности информации при обработке<br>3. Защита целостности информации при транспортировке<br>4. Защита от угрозы нарушения целостности информации на уровне содержания<br>5. Построение систем защиты от угрозы отказа доступа к информации<br>6. Защита семантического анализа и актуальности информации | 6 | 1 | - |
| 7 | 11-12 | Тема: Политика и модели безопасности<br>1. Политика безопасности<br>2.Субъективно-объектные модели разграничения доступа<br>3.Аксиомы политики безопасности<br>4.Политика и модели дискреционного доступа<br>5.Парольные системы разграничения доступа<br>6.Политика и модели мандатного доступа<br>7.Теоретико-информационные модели<br>8.Политика и модели тематического разграничения доступа<br>9.Ролевая модель безопасности | 4 | 1 | - |
| 8 | 13-14 | Тема: Обзор международных стандартов информационной безопасности<br>1.Роль стандартов информационной безопасности<br>2.Критерии безопасности компьютерных систем министерства обороны США (Оранжевая книга), TCSEC<br>3.Европейские критерии безопасности информационных технологий (ITSEC)<br>4.Федеральные критерии безопасности информационных технологий США<br>5.Единые критерии безопасности информационных технологий<br>6.Группа международных стандартов 270000 | 4 | 1 | - |
| 9 | 15 | Тема: Информационные войны и информационное противоборство<br>1.Определение и основные виды информационных войн<br>2.Информационно-техническая война<br>3.Информационно-психологическая война | 2 | 1 | - |
| Общая трудоемкость лекционного курса | | | | | x |

| Всего лекций по дисциплине: | час. | Из них в интерактивной форме: | час. |
|---|---|---|---|
| – очная форма обучения | 30 | – очная форма обучения | 4 |
| – заочная форма обучения | 8 | – заочная форма обучения | 1,5 |

## 5. Лабораторные занятия по дисциплине и подготовка к ним

Лабораторные занятия по курсу проводятся в соответствии с планом, представленным в таблице ниже.

**Примерный тематический план лабораторных занятий по разделам дисциплины**

| № | | | Тема лабораторной работы | Трудоемкость ЛР, час | | Связь с ВАРС | | Применяемые интерактивные формы обучения* |
|---|---|---|---|---|---|---|---|---|
| раздела | ЛЗ* | ЛР* | | очная форма | заочная форма | предусмотрена самоподготовка к занятию +/- | Защита отчета о ЛР во внеаудиторное время +/- | |
| 5 | 1-7 | 1 | Основные программно-технические меры | 14 | 2 | + | - | - |
| 6 | 8-11 | 2 | Основные составляющие информационной безопасности. Важность и сложность проблемы информационной безопасности | 8 | 4 | + | - | - |
| 7 | 12-15 | 3 | Экранирование, анализ защищенности | 8 | - | + | - | Практико-ориентированные задачи |
| 8 | 16-17 | 4 | Туннелирование и управление | 4 | - | + | - | |
| Итого ЛР | | | Общая трудоемкость ЛР | 34 | 6 | x | | |

Подготовка обучающихся к лабораторным занятиям осуществляется с учетом общей структуры учебного процесса. На лабораторных занятиях осуществляется входной и текущий аудиторный контроль в виде опроса, по основным понятиям дисциплины.

Для осуществления работы по подготовке к занятиям, необходимо ознакомиться с методическими указаниями по дисциплине, внимательно ознакомиться с литературой и электронными ресурсами, с рекомендациями по подготовке.

## 6. Общие методические рекомендации по изучению отдельных разделов дисциплины

При изучении конкретного раздела дисциплины, из числа вынесенных на лекционные и лабораторные занятия, обучающемуся следует учитывать изложенные ниже рекомендации. Обратите на них особое внимание при подготовке к аттестации.

Работа по теме прежде всего предполагает ее изучение по учебнику или пособию. Следует обратить внимание на то, что в любой теории, есть либо неубедительные, либо чересчур абстрактные, либо сомнительные положения. Поэтому необходимо вырабатывать самостоятельные суждения, дополняя их аргументацией, что и следует демонстрировать на семинарах. Для выработки самостоятельного суждения важным является умение работать с научной литературой. Поэтому работа по теме кроме ее изучения по учебнику, пособию предполагает также поиск по теме научных статей в научных журналах. Таким журналом является Информационные технологии. Выбор статьи, относящейся к теме, лучше делать по последним в году номерам, где приводится перечень статей, опубликованных за год.

### Раздел 1. Основные понятия теории информационной безопасности

*Краткое содержание*

История становления информационной безопасности. Предметная область теории информационной безопасности. Систематизация понятий в области защиты информации. Основные термины и определения правовых понятий в области информационных отношений и защиты информации. Понятия предметной области «Защита информации». Основные принципы построения систем защиты. Концепция Средства реализации комплексной защиты информации комплексной защиты информации. Задачи защиты информации.

*Вопросы для самоконтроля*

1. Дайте определение понятию информационная безопасность.
2. Перечислите основные составляющие информационной безопасности.
3. Какое значение имеют составляющие информационной безопасности для субъектов информационных отношений?
4. Каковы интересы РФ в информационной сфере?
5. Определите источники угроз информационной безопасности РФ и постройте их классификацию.
6. Перечислите основные методы обеспечения информационной безопасности РФ.
7. Какие основные проблемы международного сотрудничества стоят на повестке дня сегодня?
8. Перечислите основные документы в области международной информационной безопасности.

### Раздел 2. Информация как объект защиты

*Краткое содержание*

Понятие об информации как объекте защиты. Уровни предоставления информации. Основные свойства защищаемой информации. Виды и формы представления информации. Информационные ресурсы. Структура и шкала ценности информации. Классификация информационных ресурсов. Правовой режим информационных ресурсов.

*Вопросы для самоконтроля*

1.Что такое информация?
2.Что такое коммерческая тайна?
3.Какие сведения не могут составлять коммерческую тайну?
4.Что такое государственная тайна?
5.Какие сведения не подлежат отнесению к государственной тайне?
6.Как осуществляется допуск к государственной тайне?
7.Какие основные нормативно-правовые акты регулируют защиту информации и государственной тайны?
8.Какие существуют виды ответственности за разглашение государственной тайны?

**Раздел 3. Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности**

*Краткое содержание*

Информационная безопасность и ее место в системе национальной безопасности Российской Федерации. Органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность.

*Вопросы для самоконтроля*

1. Что такое государственная информационная политика?
2. В чем заключается Концепция государственной информационной политики?
3. Что такое информационное пространство?
4. Охарактеризуйте понятие информационное общество.

**Раздел 4. Угрозы информационной безопасности**

*Краткое содержание*

Анализ уязвимостей системы. Классификация угроз информационной безопасности. Основные направления и методы реализации угроз. Неформальная модель нарушителя. Оценка уязвимости системы.

*Вопросы для самоконтроля*

1.Какие технологии информационной защиты необходимо использовать чтобы обеспечить надежную защиту ресурсов информационной системы?

2. Что такое доступность, целостность и конфиденциальность?

3. Что такое угроза безопасности информации, ущерб безопасности, источник угрозы безопасности, уязвимость, атака?

4. Что такое защита информации, объект защиты, эффективность защиты информации, цель защиты информации, защита информации от утечки?

5. Что такое санкционированный и несанкционированный доступ к информации, права доступа?

**Раздел 5. Построение систем защиты от угрозы нарушения конфиденциальности**

*Краткое содержание*

Определение и основные способы несанкционированного доступа. Краткое содержание Методы защиты от НСД. Организационные методы защиты от НСД. Инженерно-технические методы защиты от НСД. Построение системы защиты от угрозы утечки по техническим каналам. Идентификация и аутентификация. Основные направления и цели использования криптографических методов. Защита от угрозы нарушения конфиденциальности на уровне содержания информации.

*Вопросы для самоконтроля*

1.Каким образом следует выбирать меры защиты конфиденциальности информации?

2.Дайте определение идентификации и аутентификации пользователя. В чем разница между этими понятиями?

3.Перечислите основные способы аутентификации. Какой, на Ваш взгляд, является наиболее эффективным?

4.Какие основные методы контроля доступа используются в известных вам информационных системах? В чем их достоинства и недостатки?

5.Почему аутентификация с использованием пароля считается в настоящее время ненадежной?

6.Каковы методы аутентификации с использованием предметов заданного типа? Назовите те, которые получили распространение в последнее время.

7.Дайте определение шифра и сформулируйте основные требования к нему.

8.Поясните, что понимается под совершенным шифром.

9.Почему большинство современных шифрограмм могут быть однозначно дешифрованы?

## Раздел 6. Построение систем защиты от угрозы нарушения целостности информации и отказа доступа

*Краткое содержание*

Защита целостности информации при хранении. Защита целостности информации при обработке. Защита целостности информации при транспортировке. Защита от угрозы нарушения целостности информации на уровне содержания. Построение систем защиты от угрозы отказа доступа к информации. Защита семантического анализа и актуальности информации.

*Вопросы для самоконтроля*

1.Как контролировать целостность сообщений при высоком уровне помех в каналах связи?
2.Как организован обмен документами, заверенными цифровой подписью?
3.Какими принципами нужно руководствоваться для сохранения целостности данных при их обработке?
4.Почему проблемы контроля целостности данных относятся к проблемам информационной безопасности?
5.Что означает контроль целостности данных на уровне содержания? Приведите примеры.
6.Как обеспечить целостность данных при их хранении?
7.Что такое надежность и чем отличается надежность аппаратуры от надежности программного обеспечения?
8.Следует ли различать защиту от случайных угроз и от действий злоумышленника при обеспечении беспрепятственного доступа к информации? Обоснуйте свой ответ.
9.Как защитить программное обеспечение от изучения логики его работы?
10.Как изменяется надежность аппаратуры с течением времени?
11.Каковы способы повышения надежности аппаратуры и линий связи?

## Раздел 7. Политика модели безопасности

*Краткое содержание*

Политика безопасности. Субъективно-объектные модели разграничения доступа. Аксиомы политики безопасности. Политика и модели дискреционного доступа. Парольные системы разграничения доступа. Политика и модели мандатного доступа. Теоретико-информационные модели. Политика и модели тематического разграничения доступа. Ролевая модель безопасности.

*Вопросы для самоконтроля*

1. Охарактеризуйте объективные геополитические факторы национальной безопасности.
2. Охарактеризуйте субъективные геополитические факторы национальной безопасности.
3. В чем состоит сущность общей геополитической модели системы национальной безопасности?
3. В чем состоит сущность структурно-функциональной модели обеспечения национальной безопасности?

## Раздел 8. Обзор международных стандартов информационной безопасности

*Краткое содержание*

Роль стандартов информационной безопасности. Критерии безопасности компьютерных систем министерства обороны США (Оранжевая книга), TCSEC. Европейские критерии безопасности информационных технологий (ITSEC). Федеральные критерии безопасности информационных технологий США. Единые критерии безопасности информационных технологий. Группа международных стандартов 270000.

*Вопросы для самоконтроля*

1.Цели применения стандартов информационной безопасности.
2.Охарактеризуйте основные положения Оранжевой книги.
3.Почему в современных стандартах отказываются от единых шкал, характеризующих уровень безопасности?
4.Каковы основные положения Европейских критериев безопасности информационных технологий?
5.Чем отличаются «информационная система» и «продукт информационных технологий»?
6.Для чего вводятся критерии адекватности?

7.Что такое Профиль защиты?

8.В чем особенности Канадских критериев безопасности компьютерных систем?

9.Опишите структуру Общих критериев безопасности информационных технологий.

10.Опишите технологию применения Общих критериев безопасности информационных технологий.

11.Каковы тенденции развития международной нормативной базы в области информационной безопасности?

### Раздел 9. Информационные войны и информационное противоборство

*Краткое содержание*

Определение и основные виды информационных войн. Информационно-техническая война. Информационно-психологическая война.

*Вопросы для самоконтроля*

1. Какова структура современного геополитического противоборства?
2. Охарактеризуйте цивилизационные аспекты современного геополитического противоборства.
3. Охарактеризуйте формационные аспекты современного геополитического противоборства.
4. Охарактеризуйте информационный компонент геополитического противоборства.

**Шкала и критерии оценивания**
**для опроса**

– «зачтено» Тема раздела раскрыта. Продемонстрировано владение материалом. Использованы надлежащие источники в нужном количестве.

– «не зачтено» Тема раздела не раскрыта. Продемонстрировано неудовлетворительное владение материалом. Использованные источники недостаточны.

| **Шкала и критерии оценивания для тестирований** | |
|---|---|
| **Отлично** | Более 81% тестовых заданий решены верно |
| **Хорошо** | От 70 до 79% тестовых заданий решены верно |
| **Удовлетворительно** | От 61 до 69% тестовых заданий решены верно |
| **Неудовлетворительно** | Менее 61% тестовых заданий решены верно |

## 7. Общие методические рекомендации по оформлению и выполнению отдельных видов ВАРС

### 7.1. Рекомендации по написанию рефератов

**Учебные цели, на достижение которых ориентировано выполнение реферата:** контроль усвояемости учебного материала студентом и проверка его навыков самостоятельной работы с источниками.

**Учебные задачи, которые должны быть решены обучающимся в рамках выполнения реферата:**

– детальное рассмотрение наиболее актуальных проблем;

– формирование и отработка навыков исследования, накопление опыта работы с научной литературой, подбора и анализа фактического материала;

– совершенствование в изложении своих мыслей, критики, самостоятельного построения структуры работы, постановки задач, раскрытие основных вопросов, умение сформулировать логические выводы и предложения.

**ПРИМЕРНАЯ ТЕМАТИКА**
**рефератов**

1. Информационное право и информационная безопасность.
2. Концепция информационной безопасности.
3. Анализ законодательных актов об охране информационных ресурсов открытого доступа.
4. Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.
5. Соотношение понятий: информационные ресурсы, информационные системы и информационная безопасность.
6. Информационная безопасность (по материалам зарубежных источников и литературы).
7. Правовые основы защиты конфиденциальной информации.
8. Экономические основы защиты конфиденциальной информации.
9. Организационные основы защиты конфиденциальной информации.
10. Структура, содержание и методика составления перечня сведений, относящихся к предпринимательской тайне.
11. Составление инструкции по обработке и хранению конфиденциальных документов.
12. Направления и методы защиты документов на бумажных носителях.
13. Направления и методы защиты машиночитаемых документов.
14. Архивное хранение конфиденциальных документов.
15. Направления и методы защиты аудио- и визуальных документов.
16. Порядок подбора персонала для работы с конфиденциальной информацией.
17. Методика тестирования и проведения собеседования с претендентами на должность, связанную с секретами организации.
18. Назначение, структура и методика построения разрешительной системы доступа персонала к секретам организации.
19. Порядок проведения переговоров и совещаний по конфиденциальным вопросам.
20. Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний.
21. Порядок работы с посетителями фирмы, организационные и технические методы защиты секретов фирмы. 22. Порядок защиты информации в рекламной и выставочной деятельности.
23. Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.
24. Анализ источников, каналов распространения и каналов утечки информации (на примере конкретной организации).
25. Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.
26. Основы технологии обработки и хранения конфиденциальных документов (по зарубежной литературе).
27. Назначение, виды, структура и технология функционирования системы защиты информации.
28. Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.
29. Аналитическая работа по выявлению каналов утечки информации организации.
30. Анализ функций секретаря-референта небольшой фирмы в области защиты информации.
31. Направления и методы защиты профессиональной тайны.
32. Направления и методы защиты служебной тайны.
33. Направления и методы защиты персональных данных о гражданах.
34. Методы защиты личной и семейной тайны.

35. Построение и функционирование защищенного документооборота.
36. Защита секретов в дореволюционной России.
37. Методика инструктирования и обучения персонала правилами защиты секретов организации.

### Этапы работы над рефератом

**Выбор темы**. Очень важно правильно выбрать тему. Выбор темы не должен носить формальный характер, а иметь практическое и теоретическое обоснование.

Автор реферата должен осознанно выбрать тему с учетом его познавательных интересов. Если интересующая тема отсутствует в рекомендательном списке, то по согласованию с преподавателем обучающемуся предоставляется право самостоятельно предложить тему реферата, раскрывающую содержание изучаемой дисциплины. Тема не должна быть слишком общей и глобальной, так как небольшой объем работы (до 20 страниц) не позволит раскрыть ее.

При выборе темы необходимо учитывать полноту ее освещения в имеющейся научной литературе. Для этого можно воспользоваться тематическими каталогами библиотек и библиографическими указателями литературы, периодическими изданиями, либо справочно-библиографическими ссылками изданий посвященных данной теме.

После выбора темы составляется список изданной по теме (проблеме) литературы, опубликованных статей, необходимых справочных источников.

Знакомство с любой научной проблематикой следует начинать с освоения имеющейся основной научной литературы. При этом следует сразу же составлять библиографические выходные данные (автор, название, место и год издания, издательство, страницы) используемых источников. Названия работ иностранных авторов приводятся только на языке оригинала.

Начинать знакомство с избранной темой лучше всего с чтения обобщающих работ по данной проблеме, постепенно переходя к узкоспециальной литературе.

На основе анализа прочитанного и просмотренного материала по данной теме следует составить тезисы по основным смысловым блокам, с пометками, собственными суждениями и оценками. Предварительно подобранный в литературных источниках материал может превышать необходимый объем реферата, но его можно использовать для составления плана реферата.

**Составление плана**. Автор по предварительному согласованию с преподавателем может самостоятельно составить план реферата, с учетом замысла работы, либо взять за основу рекомендуемый план, приведенный в данных методических указаниях по соответствующей теме. Правильно построенный план помогает систематизировать материал и обеспечить последовательность его изложения.

Наиболее традиционной является следующая структура реферата:

Титульный лист.
Оглавление (план, содержание).
Введение.
Глава 1 (полное наименование главы).
1.1. (полное название параграфа, пункта);
1.2. (полное название параграфа, пункта).
Глава 2 (полное наименование главы).
2.1. (полное название параграфа, пункта);
2.2. (полное название параграфа, пункта).
Заключение (или выводы).
Список использованной литературы.
Приложения (по усмотрению автора).

} Основная часть

***Титульный лист*** заполняется по единой форме (Приложение 1).

***Оглавление*** (план, содержание) включает названия всех разделов (пунктов плана) реферата и номера страниц, указывающие начало этих разделов в тексте реферата.

***Введение.*** В этой части реферата обосновывается актуальность выбранной темы, формулируются цели работы и основные вопросы, которые предполагается раскрыть в реферате, указываются используемые материалы и дается их краткая характеристика с точки зрения полноты освещения избранной темы. Объем введения не должен превышать 1-1,5 страницы.

***Основная часть*** реферата может быть представлена одной или несколькими главами, которые могут включать 2-3 параграфа (подпункта, раздела).

Здесь достаточно полно и логично излагаются главные положения в используемых источниках, раскрываются все пункты плана с сохранением связи между ними и последовательности перехода от одного к другому.

Автор должен следить за тем, чтобы изложение материала точно соответствовало цели и названию главы (параграфа). Материал в реферате рекомендуется излагать своими словами, не допуская дословного переписывания из литературных источников. В тексте обязательны ссылки на пер-

воисточники, т.е. на тех авторов, у которых взят данный материал в виде мысли, идеи, вывода, числовых данных, таблиц, графиков, иллюстраций и пр.

Работа должна быть написана грамотным литературным языком. Сокращение слов в тексте не допускается, кроме общеизвестных сокращений и аббревиатуры. Каждый раздел рекомендуется заканчивать кратким выводом.

***Заключение*** (выводы). В этой части обобщается изложенный в основной части материал, формулируются общие выводы, указывается, что нового лично для себя вынес автор реферата из работы над ним. Выводы делаются с учетом опубликованных в литературе различных точек зрения по проблеме рассматриваемой в реферате, сопоставления их и личного мнения автора реферата. Заключение по объему не должно превышать 1,5-2 страниц.

***Приложения*** могут включать графики, таблицы, расчеты. Они должны иметь внутреннюю (собственную) нумерацию страниц.

***Библиография*** (список литературы) здесь указывается реально использованная для написания реферата литература, периодические издания и электронные источники информации. Список составляется согласно правилам библиографического описания.

**Процедура оценивания**

При аттестации бакалавра по итогам его работы над рефератом, руководителем используются критерии оценки качества **процесса подготовки реферата, к**ритерии оценки **содержания реферата, к**ритерии оценки **оформления реферата, критерии оценки участия обучающегося в контрольно-оценочном мероприятии.**

*1. Критерии оценки содержания реферата:* степень раскрытия темы; самостоятельность и качество анализа теоретических положений; глубина проработки, обоснованность методологической и методической программы исследования; качество анализа объекта и предмета исследования; проработка литературы при написании реферата.

*2 Критерии оценки оформления реферата:* логика и стиль изложения; структура и содержание введения и заключения; объем и качество выполнения иллюстративного материала; качество ссылок и списка литературы; общий уровень грамотности изложения.

*3. Критерии оценки качества подготовки реферата:* способность работать самостоятельно; способность творчески и инициативно решать задачи; способность рационально планировать этапы и время выполнения реферата, диагностировать и анализировать причины появления проблем при выполнении реферата, находить оптимальные способы их решения; дисциплинированность, соблюдение плана, графика подготовки диссертации; способность вести дискуссию, выстраивать аргументацию с использованием результатов исследований, демонстрация широты кругозора;

*4. Критерии оценки участия бакалавра в контрольно-оценочном мероприятии:* способность и умение публичного выступления с докладом; способность грамотно отвечать на вопросы;

**7.1.1. Шкала и критерии оценивания**

– «зачтено» Тема раскрыта. Продемонстрировано владение материалом. Использованы надлежащие источники в нужном количестве. Структура работы соответствует поставленным задачам. Степень самостоятельности работы высокая.

– «не зачтено» Тема не раскрыта. Продемонстрировано неудовлетворительное владение материалом. Использованные источники недостаточны. Структура работы не соответствует поставленным задачам. Работа несамостоятельна.

Оценка по реферату расписывается преподавателем в оценочном листе (приложение 2).

### 7.2. Рекомендации по самостоятельному изучению тем

**ВОПРОСЫ**
**для самостоятельного изучения темы**
**«Основные понятия теории информационной безопасности»**

1. История становления информационной безопасности.
2. Основные термины и определения правовых понятий в области информационных отношений и защиты информации.
3. Предметная область теории информационной безопасности.

**ВОПРОСЫ**
**для самостоятельного изучения темы**
**«Информация как объект защиты»**

1. Понятие об информации как объекте защиты.
2. Уровни предоставления информации.

3. Виды и формы представления информации. Информационные ресурсы.

**ВОПРОСЫ**
**для самостоятельного изучения темы**
**«Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности»**

1. Информационная безопасность и ее место в системе национальной безопасности Российской Федерации.
2. Органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность.

**ВОПРОСЫ**
**для самостоятельного изучения темы**
**«Угрозы информационной безопасности»**

1. Анализ уязвимостей системы.
2. Классификация угроз информационной безопасности.
3. Основные направления и методы реализации угроз.

**ВОПРОСЫ**
**для самостоятельного изучения темы**
**«Построение систем защиты от угрозы нарушения конфиденциальности»**

1. Определение и основные способы несанкционированного доступа.
2. Методы защиты от НСД.
3. Основные направления и цели использования криптографических методов.

**ВОПРОСЫ**
**для самостоятельного изучения темы**
**«Построение системы защиты от угрозы нарушения целостности информации и отказа доступа»**

1. Защита целостности информации при хранении.
2. Защита целостности информации при обработке.
3. Защита целостности информации при транспортировке.

**ВОПРОСЫ**
**для самостоятельного изучения темы**
**«Политика и модели безопасности»**

1. Политика безопасности.
2. Субъективно-объектные модели разграничения доступа.
3. Аксиомы политики безопасности.

**ВОПРОСЫ**
**для самостоятельного изучения темы**
**«Обзор международных стандартов информационной безопасности»**

1. Роль стандартов информационной безопасности.
2. Единые критерии безопасности информационных технологий.
3. Группа международных стандартов.

**ВОПРОСЫ**
**для самостоятельного изучения темы**
**«Информационные войны и информационное противоборство»**

1. Определение и основные виды информационных войн.
2. Информационно-техническая война.
3. Информационно-психологическая война.

**Общий алгоритм самостоятельного изучения темы**

| |
|---|
| 1. Ознакомиться с рекомендованной учебной литературой и электронными ресурсами по теме (ориентируясь на вопросы для самоконтроля) |
| 2. На этой основе составить развёрнутый план изложения темы |
| 3. Провести самоконтроль освоения темы по вопросам, выданным преподавателем |
| 4. Подготовиться к предусмотренному контрольно-оценочному мероприятию по результатам самостоятельного изучения темы – тестирование |
| 5. Принять участие в указанном мероприятии, пройти тестирование по разделу на аудиторном занятии и заключительное тестирование в установленное для внеаудиторной работы время |

### 7.2.1. ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ самостоятельного изучения темы

- оценка «отлично» выставляется обучающемуся, если получено более 81% правильных ответов.
- оценка «хорошо» - получено от 71 до 80% правильных ответов.
- оценка «удовлетворительно» - получено от 61 до 70% правильных ответов.
- оценка «неудовлетворительно» - получено менее 61% правильных ответов.

## 8. Текущий (внутрисеместровый) контроль хода и результатов учебной работы

В течение семестра, проводится текущий контроль успеваемости по дисциплине, к которому обучающийся должен быть подготовлен.

Отсутствие пропусков аудиторных занятий, активная работа на практических занятиях, общее выполнение графика учебной работы являются основанием для получения положительной оценки по текущему контролю.

В качестве текущего контроля может быть использован тестовый контроль. Тест состоит из небольшого количества элементарных вопросов по основным разделам дисциплины: неправильные решения разбираются на следующем занятии; частота тестирования определяется преподавателем.

### 8.1. ВОПРОСЫ для самоподготовки к лабораторным занятиям

В процессе подготовки к семинарскому занятию обучающийся изучает представленные ниже вопросы по темам. На занятии обучающийся демонстрирует свои знания по изученным вопросам в форме устного ответа. Для усвоения материала по теме занятия обучающийся выполняет лабораторные задания.

**Тема. Построение системы защиты и угрозы нарушения**

1. В чем отличие идентификации от аутентификации..
2. Основные направления и цели использования криптографических методов?
3. Посторение систем защиты от угрозы утечки по техническим каналам.

**Тема. Построение системы защиты от угрозы нарушения целостности информации и отказа доступа**

1. Основные понятия программно-технического уровня информационной безопасности.
2. Архитектурная безопасность – три принципа, содержащихся в приведенном утверждении.
3. Международные стандарты информационного обмена.
4. Безопасность в сетях Internet и Intranet.

**Тема. Политика и модели безопасности**

1. Модели анализа безопасности программного обеспечения.
2. Элементы политики безопасности.
3. Политка верхнего уровня, среднего уровня.
4. Мероприятия по управлению рисками.

**Тема. Международные стандарты информационной безопасности**

1 .«Оранжевая книга» как оценочный стандарт.
2. Шесть классов безопасности и их основные характеристики.
3. Сетевые механизмы безопасности.
4. Администрирование средств безопасности.
5. Руководящие документы Гостехкомиссии России.

#### 8.1.1. Шкала и критерии оценивания самоподготовки по темам лабораторных занятий

- оценка «зачтено» выставляется обучающемуся, если все вопросы темы раскрыты, во время дискуссии высказывается собственная точка зрения на обсуждаемую проблему, демонстрируется способность аргументировать доказываемые положения и выводы.

- оценка «не зачтено» выставляется, если обучающийся не способен доказать и аргументировать собственную точку зрения по изученной теме, не способен ссылаться на мнения ведущих специалистов по обсуждаемой проблеме.

## 9. Промежуточная (семестровая) аттестация по курсу

| **9.1. Нормативная база проведения промежуточной аттестации обучающихся по результатам изучения дисциплины**: | |
|---|---|
| Действующее «Положение о текущем контроле успеваемости, промежуточной аттестации обучающихся по программам высшего образования (бакалавриат, специалитет, магистратура) и среднего профессионального образования в ФГБОУ ВО Омский ГАУ» | |
| **9.2. Основные характеристики промежуточной аттестации обучающихся по итогам изучения дисциплины** | |
| **Цель промежуточной аттестации –** | установление уровня достижения каждым обучающимся целей и задач обучения по данной дисциплине, изложенным в п.2.2 настоящей программы |
| **Форма промежуточной аттестации –** | Дифференцированный зачет |
| **Место процедуры получения зачёта в графике учебного процесса** | 1) участие обучающегося в процедуре получения зачёта осуществляется за счёт учебного времени (трудоёмкости), отведённого на изучение дисциплины |
| | 2) процедура проводится в рамках ВАРО, на последней неделе семестра |
| **Основные условия получения обучающимся зачёта:** | 1) обучающийся выполнил все виды учебной работы (включая самостоятельную) и отчитался об их выполнении в сроки, установленные графиком учебного процесса по дисциплине;<br>2) прошёл заключительное тестирование |

**ПРОЦЕДУРА ПРОВЕДЕНИЯ**
**зачета**

1) обучающийся выполнил все виды учебной работы (включая самостоятельную) и отчитался об их выполнении в сроки, установленные графиком учебного процесса по дисциплине;

2) прошёл заключительное тестирование.

### 9.3. Заключительное тестирование по итогам изучения дисциплины

По итогам изучения дисциплины, обучающиеся проходят заключительное тестирование. Тестирование является формой контроля, направленной на проверку владения терминологическим аппаратом, современными информационными технологиями и конкретными знаниями в области фундаментальных и прикладных дисциплин.

#### 9.3.1. Подготовка к заключительному тестированию по итогам изучения дисциплины

Тестирование осуществляется по всем темам и разделам дисциплины, включая темы, выносимые на самостоятельное изучение.

Процедура тестирования ограничена во времени и предполагает максимальное сосредоточение обучающегося на выполнении теста, содержащего несколько тестовых заданий.

Тестирование проводится в письменной форме (на бумажном носителе). Тест включает в себя 30 вопросов. Время, отводимое на выполнение теста - 30 минут.

**Бланк теста**

*Образец*

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Омский государственный аграрный университет имени П.А. Столыпина»

**Тестирование по итогам освоения дисциплины**
**«Безопасность информационных технологий и систем»**

**Для обучающихся направления подготовки 09.03.02 Информационные системы и технологии**

**ФИО**_____**группа**_____
**Дата**_____

Уважаемые обучающиеся!

Прежде чем приступить к выполнению заданий внимательно ознакомьтесь с инструкцией:

1. Отвечая на вопрос с выбором правильного ответа, правильный, на ваш взгляд, ответ (ответы) обведите в кружок.
2. В заданиях открытой формы впишите ответ в пропуск.
3. В заданиях на соответствие заполните таблицу.
4. В заданиях на правильную последовательность впишите порядковый номер в квадрат.
4. Время на выполнение теста – 30 минут
5. За каждый верный ответ Вы получаете 1 балл, за неверный – 0 баллов.

Желаем удачи!

**Примерные тестовые задания**

**1) Специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензируемых требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю называется:**
a) дипломом
b) лицензией
c) патентом

**2) Потенциально уязвимы с точки зрения нарушения целостности не только данные, но и:**
a) аппаратные средства
b) программы
c) сети.

**3) Самыми опасными источниками внутренних угроз являются:**
a) некомпетентные руководители
b) обиженные сотрудники
c) любобытные администраторы

**4) Спектр интересов, связанных с использованием информационных систем, можно разделить на следующие категории:**
**Обеспечение доступности, целостности, конфиденциальности информационных ресурсов и**
_____
a) информационных услуг
b) поддерживающей инфраструктуры
c) сведения о технических каналах утечки информации

**5) Под определение средств защиты информации, данное в Законе «О государственной тайне», подпадают:**
а)средства выявления злоумышленной активности
б)средства обеспечения отказоустойчивости
в)средства контроля эффективности защиты информации

**9.3.2 ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ**

ответов на тестовые вопросы тестирования по итогам освоения дисциплины

- оценка «отлично» выставляется обучающемуся, если получено более 81% правильных ответов.
- оценка «хорошо» - получено от 71 до 80% правильных ответов.
- оценка «удовлетворительно» - получено от 61 до 70% правильных ответов.
- оценка «неудовлетворительно» - получено менее 61% правильных ответов.

## 10. Информационное и методическое обеспечение учебного процесса по дисциплине

В соответствии с действующими государственными требованиями для реализации учебного процесса по дисциплине обеспечивающей кафедрой разрабатывается и постоянно совершенствуется учебно-методический комплекс (УМКД), соответствующий данной рабочей программе и прилагаемый к ней. При разработке УМКД кафедра руководствуется установленными университетом требованиями к его структуре, содержанию и оформлению. В состав УМКД входят перечисленные ниже и другие источники учебной и учебно-методической информации, средства наглядности.

Электронная версия актуального УМКД, адаптированная для обучающихся, выставляется в информационно-образовательной среде университета.

**ПЕРЕЧЕНЬ**
**литературы, рекомендуемой для изучения дисциплины**
**Б1.О.22 Безопасность информационных технологий и систем**

| Автор, наименование, выходные данные | Доступ |
|---|---|
| Арзуманян, А. Б. Международные стандарты правовой защиты информации и информационных технологий : учебное пособие / А. Б. Арзуманян ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2020. – 140 с. – ISBN 978-5-9275-3546-0. – Текст : электронный. – URL: https://znanium.com/catalog/product/1308349. – Режим доступа: по подписке. | http://znanium.com |
| Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш. – 4-е изд., перераб. и доп. – Москва : РИОР : ИНФРА-М, 2022. – 336 с. – DOI: https://doi.org/10.29039/1761-6. – ISBN 978-5-369-01761-6. – Текст : электронный. – URL: https://znanium.com/catalog/product/1861657. – Режим доступа: по подписке. | http://znanium.com |
| Баранова, Е. К. Информационная безопасность. История специальных методов криптографической деятельности : учебное пособие / Е. К. Баранова, А. В. Бабаш, Д. А. Ларин. – Москва : РИОР : ИНФРА-М, 2022. – 236 с. – ISBN 978-5-369-01788-3. – Текст : электронный. - URL:https://znanium.com/catalog/product/1843171. – Режим доступа: по подписке. | http://znanium.com |
| Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем : учебное пособие / Е.В. Глинская, Н.В. Чичварин. – Москва : ИНФРА-М, 2021. – 118 с. + Доп. материалы. – DOI 10.12737/13571. – ISBN 978-5-16-010961-9. – Текст : электронный. – URL: https://znanium.com/catalog/product/1178152. – Режим доступа: по подписке. | http://znanium.com |
| Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. – Москва : ИНФРА-М, 2022. – 180 с. – DOI 10.12737/monography_5d412ff13c0b88.75804464. – ISBN 978-5-16-015149-6. – Текст : электронный. – URL: https://znanium.com/catalog/product/1862651. – Режим доступа: по подписке. | http://znanium.com |
| Мартишин, С. А. Основы теории надежности информационных систем : учебное пособие / С. А. Мартишин, В. Л. Симонов, М. В. Храпченко. – Москва : ФОРУМ : ИНФРА-М, 2020. – 255 с. – ISBN 978-5-8199-0757-3. – Текст : электронный. – URL: https://znanium.com/catalog/product/1062374. – Режим доступа по подписке. | http://znanium.com |
| Организационно-техническое и правовое обеспечение информационной безопасности Российской Федерации : учебник / сост. И. Г. Дровникова, А. В. Калач, И. И. Лившиц [и др]. – Воронеж: Научная книга, 2022. – 304 с. – ISBN 978-5-4446-1743-4. – Текст : электронный. – URL: https://znanium.com/catalog/product/1999941. – Режим доступа: по подписке. | http://znanium.com |
| Информационные технологии. – Москва : Новые технологии, 1995. – Выходит ежемесячно. – ISSN 1684-6400. – Текст: непосредственный. | НСХБ |

**ПРИЛОЖЕНИЕ 1**

**Форма титульного листа реферата**

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Омский государственный аграрный университет имени П.А. Столыпина»

Экономический факультет

Кафедра экономики, бухгалтерского учета и финансового контроля

Направление – 09.03.02 Информационные системы и технологии

Реферат

по дисциплине Безопасность информационных технологий и систем

на тему: _____

Выполнил(а): ст. ____группы

*ФИО*_____

Проверил(а): *уч. степень*, *должность*

*ФИО*_____

Омск – _____г.

**ПРИЛОЖЕНИЕ 2**

**Результаты проверки реферата**

| № п/п | Оцениваемая компонента реферата и/или работы над ним | Оценочное заключение преподавателя по данной компоненте | | | |
|---|---|---|---|---|---|
| | | Она сформирована на уровне | | | |
| | | высоком | среднем | минимально приемлемом | ниже приемлемого |
| 1 | Соблюдение срока сдачи работы | | | | |
| 2 | *Оценка содержания реферата* | | | | |
| 3 | *Оценка оформления реферата* | | | | |
| 4 | *Оценка качества подготовки реферата* | | | | |
| 5 | *Оценка выступления с докладом и ответов на вопросы* | | | | |
| 6 | Степень самостоятельности обучающегося при подготовке реферата | | | | |

Общие выводы и замечания по реферату

| | | |
|---|---|---|
| **Реферат принят с оценкой:** | _____ *(оценка)* | _____ *(дата)* |
| Ведущий преподаватель дисциплины | _____ *(подпись)* | _____ И.О. Фамилия |
| Обучающийся | _____ *(подпись)* | _____ И.О. Фамилия |