Федеральное государственное бюджетное образовательное учреждение высшего образования
«Алтайский государственный технический университет им. И.И. Ползунова»

**СОГЛАСОВАНО**

Декан ФИТ А.С. Авдеев

# Рабочая программа дисциплины

Код и наименование дисциплины: **Б1.В.8 «Комплексное обеспечение защиты информации объекта информатизации»**

Код и наименование направления подготовки (специальности): **10.03.01 Информационная безопасность**

Направленность (профиль, специализация): **Организация и технология защиты информации**

Статус дисциплины: **часть, формируемая участниками образовательных отношений (вариативная)**

Форма обучения: **очная**

| Статус | Должность | И.О. Фамилия |
|---|---|---|
| Разработал | старший преподаватель | А.В. Циклаков |
| Согласовал | Зав. кафедрой «ИВТиИБ» | А.Г. Якунин |
| | руководитель направленности (профиля) программы | Е.В. Шарлаев |

г. Барнаул

## 1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

| Код компетенции из УП и этап её формирования | Содержание компетенции | В результате изучения дисциплины обучающиеся должны: | | |
|---|---|---|---|---|
| | | знать | уметь | владеть |
| ПК-13 | способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации | принципы формирования комплекса мер по обеспечению информационной безопасности объекта информатизации организации, соответствующих требованиям правовых актов и стандартов | разрабатывать комплекс мер по обеспечению информационной безопасности, в том числе с учетом требований действующих правовых актов и стандартов | методами разработки комплекса мер по обеспечению информационной безопасности, в том числе с использованием соответствующих правовых актов и стандартов |
| ПК-15 | способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю | технологии защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспертному контролю; нормативные методические документы ФСБ России, ФСТЭК России в области защиты информации, в том числе документы по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации | организовать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспертному контролю, в том числе в области защиты государственной тайны | навыками подготовки документационного обеспечения для организации режима конфиденциальности информации, в том числе разработки локальных документов |
| ПК-4 | способностью участвовать в работах по реализации политики | принципы формирования | разрабатывать частные политики | навыками разработки политик |

| Код компетенции из УП и этап её формирования | Содержание компетенции | В результате изучения дисциплины обучающиеся должны: | | |
|---|---|---|---|---|
| | | знать | уметь | владеть |
| | информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты | политики информационной безопасности в информационных системах | информационной безопасности информационных систем; разрабатывать комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем | безопасности информационных систем |
| ПК-5 | способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации | организацию работы и нормативные правовые акты и стандарты по аттестации объектов информатизации | выбирать необходимые методики и документы по аттестации объектов информатизации | методиками проверки защищенности объектов информатизации на соответствие требованиям безопасности |
| ПСК2-1 | Способность проводить совместный анализ функционального процесса объекта защиты н его информационных составляющих с целью определения возможных источников информационных угроз, их вероятных целей и тактики | знать функциональные процессы объектов защиты и их информационных составляющих с целью определения возможных источников информационных угроз, их вероятных целей и тактики поведения, в том числе знать функциональные процессы информационных систем (государственных, персональных данных) и методики определения информационных угроз для них | проводить совместный анализ функционального процесса объекта защиты и его информационных составляющих с целью определения возможных источников информационных угроз и их вероятных целей | навыками определения возможных источников информационных угроз и их вероятных целей |
| ПСК2-2 | Способность формировать предложения по оптимизации функционального | способы оптимизации функционального процесса и его информационных | формировать предложения по оптимизации функционального | навыками формирования предложений по тактике защиты |

| Код компетенции из УП и этап её формирования | Содержание компетенции | В результате изучения дисциплины обучающиеся должны: | | |
|---|---|---|---|---|
| | | знать | уметь | владеть |
| | процесса объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объекта и локализации защищаемых элементов | составляющих для повышения их устойчивости к деструктивным воздействиям на информационные ресурсы; технологии безопасной архитектуры ОС, СУБД, вычислительных сетей; технологии защиты объекта (ИС – государственных, персональных данных, защищаемых помещений); технологии безопасной архитектуры ОС, СУБД, вычислительных сетей; технологии защиты объекта (ИС – государственных, персональных данных, защищаемых помещений) | процесса объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы, в том числе формировать предложения по тактике защиты объекта и локализации защищаемых элементов | объекта и локализации защищаемых элементов |
| ПСК2-3 | Способность разработать комплекс мер по обеспечению информационной безопасности объекта и организовать его внедрение и последующее сопровождение | технологии комплексного обеспечения защиты информации на объекте информатизации | применять технологии комплексного обеспечения защиты информации на объекте информатизации | методами разработки мер по обеспечению информационной безопасности объекта информатизации |
| ПСК2-4 | Способность организовать контроль защищенности объекта в соответствии с нормативными документами | методы контроля защищённости объекта информатизации в соответствии с нормативными документами, в том числе включая контроль защищенности вычислительной техники и выделенных (защищаемых) помещений | организовать контроль защищенности объекта в соответствии с нормативными документами, в том числе контроль защищенности вычислительной техники и выделенных (защищаемых) помещений | методами контроля защищенности объекта в соответствии с нормативными документами, в том числе включая контроль защищенности вычислительной техники и выделенных (защищаемых) помещений |

## 2. Место дисциплины в структуре образовательной программы

| | |
|---|---|
| Дисциплины (практики), предшествующие изучению дисциплины, результаты освоения которых необходимы для освоения данной дисциплины. | Криптографические методы защиты информации, Организационное и правовое обеспечение информационной безопасности, Основы информационной безопасности, Основы управления информационной безопасностью, Программно-аппаратные средства защиты информации, Техническая защита информации |
| Дисциплины (практики), для которых результаты освоения данной дисциплины будут необходимы, как входные знания, умения и владения для их изучения. | Выпускная квалификационная работа, Преддипломная практика, Проектно-технологическая практика |

## 3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающегося с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающегося

Общий объем дисциплины в з.е. /час: 4 / 144
Форма промежуточной аттестации: Экзамен

| Форма обучения | Виды занятий, их трудоемкость (час.) | | | | Объем контактной работы обучающегося с преподавателем (час) |
|---|---|---|---|---|---|
| | Лекции | Лабораторные работы | Практические занятия | Самостоятельная работа | |
| очная | 22 | 33 | 0 | 89 | 62 |

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

**Форма обучения: очная**
***Семестр: 8***

**Лекционные занятия (22ч.)**

**1. Комплексная система защиты информации. {беседа} (2ч.)[4,5,7]** Принципы организации и этапы разработки комплексной системы защиты информации. Методологические основы организации КСЗИ. Цели, задачи и принципы построения КСЗИ. Требования, предъявляемые к КСЗИ. Этапы разработки КСЗИ.

**2. Факторы, влияющие на организацию КСЗИ. {беседа} (2ч.)[4,5,7]** Факторы, влияющие на организацию комплексной системы защиты информации. Перечень факторов, влияющих на организацию КСЗИ. Факторы, определяющие

особенности защиты информации ограниченного доступа. Факторы, оказывающие влияние на построение КСЗИ.

**3. Состав защищаемой информации. {беседа} (2ч.)[4,5,6,7,8,12,13,14,15]** Определение и нормативное закрепление состава защищаемой информации. Нормативно-правовые аспекты определения состава защищаемой информации. Методика определения состава защищаемой информации и её нормативное закрепление.

**4. Объекты защиты информации. {беседа} (2ч.)[4,5,6,7,8,12,13,14,15]** Функциональный процесс и определение объектов защиты информации. Виды и типы объектов информатизации. Функциональный процесс и его информационные составляющие. Объекты защиты информации. Методика определения объектов комплексной защиты информации.

**5. Угрозы безопасности информации. {беседа} (2ч.)[4,5,6,7,8,10,11,12,13,14,15]** Анализ и оценка угроз безопасности информации для объекта информатизации. Цели и задачи оценки угроз безопасности информации. Основные методики анализа и оценки угроз безопасности информации. Источники, способы и результаты воздействия на информацию.

**6. Каналы и методы несанкционированного доступа к информации. {беседа} (2ч.)[4,5,6,7,8,10,11,12,13,14,15]** Определение потенциальных каналов и методов несанкционированного доступа к информации. Методика выявления каналов несанкционированного доступа к информации. Определение вероятных методов несанкционированного доступа к защищаемой информации. Определение вероятных методов НСД к ИСПДн и ГоИС.

**7. Модель нарушителя. {беседа} (2ч.)[4,5,6,7,8,10,11,12,13,14,15]** Определение возможностей несанкционированного доступа к защищаемой информации. Методика выявления нарушителей и состава интересующей их информации. Определение возможностей НСД к защищаемой информации внутренними нарушителями. Определение возможностей НСД к защищаемой информации внешними нарушителями. Модель нарушителя.

**8. Компоненты комплексной системы защиты информации. {беседа} (2ч.)[4,5,6,7,8,10,11,12,13,14,15]** Определение компонентов комплексной системы защиты информации. Компоненты КСЗИ. Методы определения компонентов КСЗИ. Синтез КСЗИ.

**9. Концепция комплексной системы защиты информации. {беседа} (2ч.)[4,5,6,7,8,10,11,12]** Определение условий функционирования и разработка концепции комплексной системы защиты информации. Основные условия функционирования КСЗИ определяемые при её создании или модернизации. Содержание концепции построения КСЗИ. Основные положения концепции относительно объектов, целей, задач защиты и угроз безопасности информации. Основные положения концепции по обеспечению безопасности информации.

**10. Создание комплексной системы защиты информации. {беседа} (2ч.)[4,5,7]** Технологическое и организационное построение КСЗИ. Общее содержание работ по организации КСЗИ. Характеристика основных стадий создания КСЗИ. Назначение и структура задания на проектирование, технического задания,

технического проекта.

**11. Функциональная модель КСЗИ. Аттестация объекта информатизации. {беседа} (2ч.)[4,5,7,13,14,15]** Разработка модели КСЗИ и аттестация объекта информатизации. Понятие модели объекта, основные виды моделей и их характеристики. Модель как инструмент количественного и качественного анализа КСЗИ. Функциональная модель КСЗИ. Организационная модель КСЗИ. Информационная модель КСЗИ. Организация аттестации объекта информатизации.

**Лабораторные работы (33ч.)**

**1. Состав защищаемой информации. {работа в малых группах} (8ч.)[1,3,4,5,6,7,15]** Определение и нормативное закрепление состава защищаемой информации организации.

**2. Объекты защиты. {работа в малых группах} (8ч.)[1,3,4,5,6,7,8,10,11,12,15]** Анализ функционального процесса и определение объектов защиты при проектировании КСЗИ

**3. Угрозы безопасности информации. {работа в малых группах} (8ч.)[1,3,4,5,6,7,8,10,11,12,13,15]** Разработка модели угроз безопасности объектам информатизации организации.

**4. Концепция КСЗИ. {работа в малых группах} (9ч.)[1,3,4,5,6,7,8,10,11,12,13,14,15]** Разработка элементов концепции КСЗИ объекта информатизации и политики информационной безопасности организации.

**Самостоятельная работа (89ч.)**

**1. Подготовка к текущим занятиям, самостоятельное изучение материала. {разработка проекта} (12ч.)[1,4,5,6,7,8,10,11,12,13,14,15]**

**2. Подготовка к текущему контролю успеваемости. {использование общественных ресурсов} (12ч.)[2,4,5,6,7,8,10,11,12]**

**3. Выполнение курсовой работы и подготовка к защите. {разработка проекта} (20ч.)[3,4,5,7]** Курсовая работа посвящена разработке комплекса мер по обеспечению информационной безопасности типового объекта информатизации (типовой объект задается преподавателем по вариантам), включая разработку модели угроз, разработку комплекса мер по обеспечению ИБ, разработку политики безопасности и разработку проектов локальных документов.

**4. Подготовка к промежуточной аттестации (экзамен). {использование общественных ресурсов} (45ч.)[4,5,6,7,8,10,11,12,13,14,15]**

## 5. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

Для каждого обучающегося обеспечен индивидуальный неограниченный доступ к электронно-библиотечным системам: Лань, Университетская библиотека он-лайн, электронной библиотеке АлтГТУ и к электронной информационно-образовательной среде:

1. Методические рекомендации к выполнению лабораторных работ по дисциплине «Информационная безопасность предприятия» / Ю.Н. Загинайлов, О.С. Лесковец, Алт. гос. тех. ун-т им. И.И. Ползунова. – Барнаул: АлтГТУ. – 2015. -74 с. [электронный ресурс]: -режим доступа: http://elib.altstu.ru/eum/download/ivtib/uploads/zaginaylov-yu-n-ivtiib-54c1f980e1ae4.pdf

2. Загинайлов Ю.Н. Методические рекомендации по выполнению курсовых работ по дисциплине «Информационная безопасность предприятия (организации)» / Ю.Н. Загинайлов; Алт. гос. тех. ун-т им. .И. Ползунова. – Барнаул: АлтГТУ. – 2015. -47 с. http://new.elib.altstu.ru/eum/download/ivtib/uploads/zaginaylov-yu-n-ivtiib-54c8f89fcbea6.pdf

3. Загинайлов Ю.Н. Информационная безопасность в терминах и определениях законодательства и стандартов защиты информации: учебно-справочное пособие /Ю.Н.Загинайлов, Е.В. Урминский.- Алт. гос. тех. ун-т им. И.И. Ползунова. – Барнаул, 2010. - 204с. [электронный ресурс]: -режим доступа: http://new.elib.altstu.ru/eum/download/vsib/zaginajlov-stib.pdf

## 6. Перечень учебной литературы

6.1. Основная литература

4. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 253 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557

5. Загинайлов Ю.Н. Информационная безопасность предприятия (организации): курс визуальных лекций / Ю.Н. Загинайлов; Алт.гос.техн.ун-т им. И.И.Ползунова.- Баранаул: Изд-во АлтГТУ.-2016- 90с. [Электронный ресурс]. http://new.elib.altstu.ru/eum/download/ivtib/uploads/zaginaylov-yu-n-ivtiib-58622503493eb.pdf

6. Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - СПб : Издательство Политехнического университета, 2014. - 322 с. : схем., табл., ил. - ISBN 978-5-7422-4331-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=363040

6.2. Дополнительная литература

7. Грибунин В.Г. Комплексная система защиты информации на предприятии: учебник для студ. высш. учеб. заведений./ В.Г.Грибунин, В.В.

Чудовский.- М.: Издательский центр «Академия», 2008.-320с. ( 25 экз. Гриф УМО)

8. Малюк, А.А. Теория защиты информации [Электронный ресурс] / А.А. Малюк. — Электрон. дан. — Москва : Горячая линия-Телеком, 2015. — 184 с. — Режим доступа: https://e.lanbook.com/book/111077

10. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. [электронный ресурс]/Изд-во "ДМК Пресс", 2012. 592 с. – доступ из ЭБС «Лань» - Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=3032 - Загл. с экр

11. Технические методы и средства защиты информации [электронный ресурс]/Под ред. А.П. Зайцева. - М.:2012 г.- доступ из ЭБС «Лань» - Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5154 - Загл. с экр

12. Лапина, М.А. Информационное право : учебное пособие / М.А. Лапина, А.Г. Ревин, В.И. Лапин ; под ред. И.Ш. Килясханова. - М. : Юнити-Дана, 2015. - 336 с. - (Высшее профессиональное образование: Юриспруденция). - Библиогр. в кн. - ISBN 5-238-00798-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=118624

## 7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

13. Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК) России [электронный ресурс]:- режим доступа: http://www.fstec.ru

14. Официальный сайт федерального агентства по техническому регулированию и метрологии [электронный ресурс]: режим доступа: http://protect.gost.ru//

15. Правовая справочная система «Гарант» [электронный ресурс]: -режим доступа: 1. Ауд.94 ПК АлтГТУ. (Платформа F1 Гарант); 2. http://www.garant.ru

## 8. Фонд оценочных материалов для проведения текущего контроля успеваемости и промежуточной аттестации

Содержание промежуточной аттестации раскрывается в комплекте контролирующих материалов, предназначенных для проверки соответствия уровня подготовки по дисциплине требованиям ФГОС, которые хранятся на кафедре-разработчике РПД в печатном виде и в ЭИОС.

Фонд оценочных материалов (ФОМ) по дисциплине представлен в приложении А.

## 9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

Для успешного освоения дисциплины используются ресурсы электронной информационно-

образовательной среды, образовательные интернет-порталы, глобальная компьютерная сеть Интернет. В процессе изучения дисциплины происходит интерактивное взаимодействие обучающегося с преподавателем через личный кабинет студента.

| №пп | Используемое программное обеспечение |
|---|---|
| 1 | Windows |
| 2 | Гарант |
| 3 | Microsoft Office |
| 4 | LibreOffice |
| 5 | Антивирус Kaspersky |

| №пп | Используемые профессиональные базы данных и информационные справочные системы |
|---|---|
| 1 | Бесплатная электронная библиотека онлайн "Единое окно к образовательным ресурсам" для студентов и преподавателей; каталог ссылок на образовательные интернет-ресурсы (http://Window.edu.ru) |
| 2 | Национальная электронная библиотека (НЭБ) — свободный доступ читателей к фондам российских библиотек. Содержит коллекции оцифрованных документов (как открытого доступа, так и ограниченных авторским правом), а также каталог изданий, хранящихся в библиотеках России. (http://нэб.рф/) |

## 10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

| Наименование специальных помещений и помещений для самостоятельной работы |
|---|
| учебные аудитории для проведения занятий лекционного типа |
| учебные аудитории для проведения занятий семинарского типа |
| учебные аудитории для проведения курсового проектирования (выполнения курсовых работ) |
| учебные аудитории для проведения групповых и индивидуальных консультаций |
| учебные аудитории для проведения текущего контроля и промежуточной аттестации |
| помещения для самостоятельной работы |

Материально-техническое обеспечение и организация образовательного процесса по дисциплине для инвалидов и лиц с ограниченными возможностями здоровья осуществляется в соответствии с «Положением об обучении инвалидов и лиц с ограниченными возможностями здоровья».