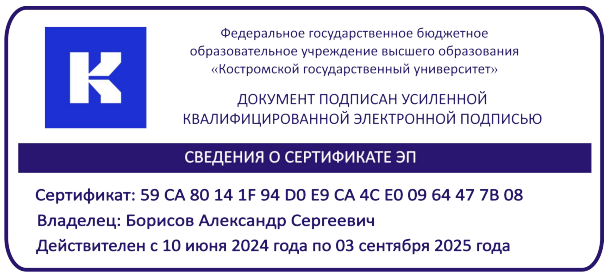
МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Костромской государственный университет»



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки 10.03.01 Информационная безопасность

Направленность «Организация и технология защиты информации»

Квалификация (степень) выпускника: Бакалавр

Кострома

Рабочая программа дисциплины «Организационное и правовое обеспечение информационной безопасности» разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования направления подготовки 10.03.01 Информационная безопасность утвержден 01.12.2016 г.

Разработал:  Виноградова Галина Леонидовна, к.т.н., доцент кафедры защиты информации

Рецензент:  Волков Антон Андреевич, к.т.н., доцент кафедры защиты информации

УТВЕРЖДЕНО:

На заседании кафедры защиты информации

Протокол заседания кафедры № 13 от 6 июля 2017 г.

Заведующий кафедрой защиты информации

 Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № 12 от 27 июня 2018 г.

Заведующий кафедрой защиты информации

 Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № _11_ от _30.05.2019_____ г.

Заведующий кафедрой защиты информации

 Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № _8_ от _6.04.2020_____ г.

Заведующий кафедрой защиты информации

 Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № _6_ от _22.01.2021_____ г.

Заведующий кафедрой защиты информации

 Щекочихин Олег Владимирович, к.т.н., доцент

1. Цели и задачи освоения дисциплины

Цель дисциплины: теоретическая и практическая подготовка бакалавра по основам правового регулирования общественных отношений, складывающихся в современной информационной сфере и обеспечение освоения практических навыков работы с нормативно-правовой базой. Формирование знаний по организационному обеспечению информационной безопасности и навыков по их определению для конкретных условий.

В результате изучения учебной дисциплины «Организационное и правовое обеспечение информационной безопасности» у обучаемых должны сформироваться профессиональные компетенции:

- способность использовать основы правовых знаний в различных сферах деятельности ОК-4;
- способность использовать нормативные правовые акты в профессиональной деятельности (ОПК-5);
- способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованию безопасности информации (ПК-5);
- способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8);
- способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9);
– способностью разработать комплекс мер по обеспечению информационной безопасности объекта и организовать его внедрение и последующее сопровождение (ПСК-2.3);
- способностью организовать контроль защищенности объекта в соответствии с нормативными документами (ПСК-2.4).

Задачи дисциплины:

- изучить понятийный аппарат, применяемый в организационном и правовом обеспечении информационной безопасности;
- изучить основные подходы к организационному и правовому обеспечению информационной безопасности;
- изучать нормативно-правовую базу по организационному и правовому обеспечению информационной безопасности;
- сформировать умение разрабатывать комплекс мер по обеспечению информационной безопасности объекта и организовать его внедрение;
- овладеть навыками организации и сопровождения аттестации объекта информатизации по требованию безопасности информации;
- овладеть навыками организации контроля защищенности объекта в соответствии с нормативными документами.

2. Перечень планируемых результатов обучения по дисциплине

В результате освоения дисциплины обучающийся должен:

знать

-основные нормативные правовые акты в области обеспечения информационной безопасности и защиты информации, а также нормативные методические документы федеральной службы безопасности Российской Федерации;
- правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны;
- правовые нормы и стандарты в области обеспечения защиты государственной тайны и сертификации средств защиты информации.

уметь

-пользоваться нормативными документами по защите информации.
- оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов по защите информации;
- осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по защите информации.
- составлять обзор по вопросам обеспечения информационной безопасности;
- организовать контроль защищенности объекта в соответствии с нормативными документами.

владеть

- навыками работы с нормативными правовыми актами;
- методами организации и управления деятельностью служб защиты информации на предприятии;
- навыками организации и обеспечения режима секретности.
- навыками участия в организации и сопровождении аттестации объекта информатизации по требованию безопасности информации;
- навыками разработки комплекса мер по обеспечению информационной безопасности объекта и организации его внедрения.

освоить компетенции:

- способность использовать основы правовых знаний в различных сферах деятельности (ОК-4);
- способность использовать нормативные правовые акты в профессиональной деятельности (ОПК-5);
- способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованию безопасности информации (ПК-5);
- способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8);
- способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9);
– способностью разработать комплекс мер по обеспечению информационной безопасности объекта и организовать его внедрение и последующее сопровождение (ПСК-2.3);
- способностью организовать контроль защищенности объекта в соответствии с нормативными документами (ПСК-2.4).

3. Место дисциплины в структуре ОП ВО

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к циклу базовых дисциплин, при этом, в значительной степени отличается от других дисциплин сферой знаний и направленностью обучения. Именно эта дисциплина формирует у обучаемых способность применения подходов к организационному и правовому обеспечению информационной безопасности в практике конкретных организаций для повышения уровня защиты данных в информационных процессах и функциональных процессах объекта защиты.

Освоению дисциплины «Организационное и правовое обеспечение информационной безопасности» предшествуют обязательные дисциплины базовой части образовательной программы специальности, такие как: «Введение в специальность», «Защита и обработка конфиденциальных документов». Базируются на освоении дисциплины «Введение в специальность». Изучение дисциплины является основой для освоения последующих дисциплин/практик: «Основы управления информационной безопасностью», «Комплексные системы защиты информации на предприятии», «Информационный менеджмент», «Управление информационными ресурсами и проектами», «Организация и управление службой защиты информации на предприятии»

Знания, умения и навыки, полученные в ходе освоения дисциплины безусловно

будут использованы в дальнейшем в профессиональной деятельности.

Освоение данной дисциплины необходимо как предшествующее для прохождения производственной (преддипломной) практики, написания выпускной квалификационной работы.

Формирование профессиональных компетенций ОК-4, ОПК-5, ПК-5, ПК-8; ПК-9 и ПСК-2.3 и ПСК-2.4 происходит также на других профильных дисциплинах, раскрывая единство и взаимосвязь профильных дисциплин.

4. Объем дисциплины (модуля)

4.1. Объем дисциплины в зачетных единицах с указанием академических (астрономических) часов и виды учебной работы

Виды учебной работы,	Очная форма
Общая трудоемкость в зачетных единицах	4
Общая трудоемкость в часах	144
Аудиторные занятия в часах, в том числе:	68
Лекции	34
Практические занятия	-
Лабораторные занятия	34
Самостоятельная работа в часах	40
Форма промежуточной аттестации	6 Экзамен 1 з.е

4.2. Объем контактной работы на 1 обучающегося

Виды учебных занятий	Очная форма
Лекции	34
Практические занятия	-
Лабораторные занятий	34
Консультации	-
Зачет/зачеты	-
Экзамен/экзамены	0,25
Курсовые работы	–
Курсовые проекты	–
Всего	68,25

5.Содержание дисциплины (модуля), структурированное по темам (разделам), с указанием количества часов и видов занятий

5.1 Тематический план учебной дисциплины

№ п/п	Название раздела, темы	Всего з.е/час	Аудиторные занятия		Самостоятельная работа
			Лекции	Лабораторные	
Раздел 1. Введение в организационное и правовое обеспечение информационной безопасности					
1	Концептуальные основы информационной безопасности.	6	2	2	2
Раздел 2. Организационные основы защиты информации					

№ п/п	Название раздела, темы	Всего з.е/час	Аудиторные занятия		Самостоятельная работа
			Лекции	Лабораторные	
2	Основные принципы, условия, подходы и требования к организационной защите информации. Основные силы и средства, используемые для организации защиты информации.	8	2	2	2
3	Отнесение сведений к конфиденциальной информации. Засекречивание и рассекречивание сведений.	8	2	2	2
4	Организация допуска и доступа персонала к конфиденциальной информации.	10	2	2	2
5	Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации	10	2	2	4
6	Организация внутри объектового и пропускного режимов на предприятии.	8	2	2	2
7	Организация охраны предприятий	8	2	2	2
8	Организация защиты информации при проведении совещаний	10	2	2	4
9	Основы защиты информации при осуществлении международного сотрудничества и выезде персонала предприятия	8	2	2	2
10	Организация и проведение служебного расследования в случае разглашения сведений конфиденциального характера или утраты носителей сведений	10	2	2	4
Раздел 3. Правовая защита конфиденциальной информации					
11	Уголовно-правовая защита сведений, составляющих коммерческую, налоговую или банковскую тайну.	10	2	2	2
12	Уголовно-правовая защита в сфере компьютерной информации.	8	2	2	2
13	Уголовно-правовая защита сведений, составляющих государственную тайну.	8	2	2	2
14	Административно-правовая защита информации с ограниченным доступом.	8	2	2	2
15	Гражданско-правовая защита служебной и коммерческой тайны.	8	2	2	2
16	Дисциплинарная ответственность за разглашение и (или) утрату конфиденциальных сведений.	8	2	2	2
17	Материальная ответственность за разглашение и (или) утрату конфиденциальных сведений.	8	2	2	2

№ п/п	Название раздела, темы	Всего з.е/час	Аудиторные занятия		Самостоятельная работа
			Лекции	Лабораторные	
Экзамен		1з.е.- 36 ч.			
Всего:		144	**34**	**34**	**40**

5.2. Содержание:

ТЕМА 1.. Концептуальные основы информационной безопасности. История возникновения органов защиты информации. Основные понятия информационной безопасности. Основные свойства информации в форме сведений. Информационная инфраструктура. Структура, сущность и содержание понятия "обеспечение информационной безопасности". Основные виды организационных средств обеспечения информационной безопасности.

ТЕМА 2. Основные принципы, условия, подходы и требования к организационной защите информации. Основные силы и средства, используемые для организации защиты информации. Основные принципы и условия организационной защиты информации. Основные направления защиты информации. Основные подходы и требования к организации системы защиты информации. Структура системы защиты информации. Основные силы и средства, используемые для организации защиты информации.

ТЕМА 3. Отнесение сведений к конфиденциальной информации. Засекречивание и рассекречивание сведений. Отнесение сведений к различным видам конфиденциальной информации. Законодательство РФ о категориях доступа к информации. Грифы секретности и реквизиты носителей сведений, составляющих государственную тайну. Грифы секретности и реквизиты носителей сведений, составляющих коммерческую тайну. Отнесение сведений к государственной тайне. Засекречивание сведений и их носителей. Структура перечня сведений, составляющих государственную тайну. Основания и порядок рассекречивания сведений и их носителей. Отнесение сведений к коммерческой тайне.

ТЕМА 4. Организация допуска и доступа персонала к конфиденциальной. Основные положения допуска персонала предприятия к конфиденциальной информации. Порядок оформления и переоформления допуска к государственной тайне. Формы допуска. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне и условия прекращения допуска. Организация доступа персонала предприятия к сведениям, составляющим государственную тайну.

ТЕМА 5. Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации. Основные источники возможной утечки (разглашения) конфиденциальной информации. Факторы и обстоятельства разглашения конфиденциальной информации персоналом предприятия. Методы работы с персоналом предприятия, допущенным к конфиденциальной информации. Функции работодателя по отношению к сотруднику предприятия в целях охраны конфиденциальности информации, составляющей коммерческую тайну.

ТЕМА 6. Организация внутри объектового и пропускного режимов на предприятии. Роль и место внутри объектового и пропускного режимов в общей системе защиты информации на предприятии**.** Основные цели, подходы и принципы организации внутри объектового режима. Силы и средства, используемые при организации внутри объектового режима. Цели и задачи пропускного режима. Основные элементы системы организации пропускного режима, используемые силы и средства.

ТЕМА 7. Организация охраны предприятий. Цели охраны предприятия. Основные задачи охраны. Система охраны предприятия. Основные обязанности сотрудников охраны. Права сотрудников подразделений охраны задач в пределах охраняемых объектов. Главные требования, предъявляемые к системе охраны.

ТЕМА 8. Организация защиты информации при проведении совещаний. Планирование мероприятий по защите информации при подготовке к проведению совещания. Организация допуска участников совещания к обсуждаемым вопросам. Подготовка места проведения совещания. Порядок проведения совещания и использования его материалов. Основы организации защиты информации в ходе издательской и рекламной деятельности предприятия. Организация подготовки материалов к открытому опубликованию.

ТЕМА 9. Основы защиты информации при осуществлении международного сотрудничества и выезде персонала. Порядок передачи различных видов конфиденциальной информации иностранным государствам. Организация подготовки к передаче сведений, составляющих государственную тайну, другим государствам. Ограничения прав гражданина, осведомленного в сведениях, составляющих государственную тайну, на выезд за границу. Работа должностных лиц предприятия по оформлению документов на выезд сотрудников в служебные командировки и по частным делам.

ТЕМА 10. Организация и проведение служебного расследования в случае разглашения сведений конфиденциального характера или утраты носителей сведений. Законодательство РФ о разглашении сведений конфиденциального характера. Комиссия по ведению служебного расследования, задачи и функции. Этапы проведения служебного расследования.

ТЕМА 11. Уголовно-правовая защита сведений, составляющих коммерческую, налоговую или банковскую тайну. Законодательство РФ о защите конфиденциальных сведений. Коммерческая тайна. Налоговая тайна. Банковская тайна.

ТЕМА 12. Уголовно-правовая защита в сфере компьютерной информации. Понятие неправомерного доступа к компьютерной информации. Понятие охраняемой законом информации. Субъекты преступлений в сфере компьютерной информации. Законодательство РФ о защите в сфере компьютерной информации.

ТЕМА 13. Уголовно-правовая защита сведений, составляющих государственную тайну. Субъекты преступлений в сфере защиты сведений, составляющих государственную тайну. Законодательство РФ о защите сведений, составляющих государственную тайну. Понятие государственной измены.

ТЕМА 14. Административно-правовая защита информации с ограниченным доступом. Административная ответственность за нарушение порядка обращения с информацией ограниченного распространения в Кодексе об административных правонарушениях.

ТЕМА 15. Гражданско-правовая защита служебной и коммерческой тайны. Законодательство РФ о защита служебной и коммерческой тайны. Обязательные условия признания информации служебной или коммерческой тайной.

ТЕМА 16. Дисциплинарная ответственность за разглашение и (или) утрату конфиденциальных сведений. Законодательство РФ о дисциплинарной ответственности за

разглашение и утрату конфиденциальных сведений. Признаки дисциплинарного проступка. Виды дисциплинарной ответственности. Процедура вынесения наказания за дисциплинарный проступок.

ТЕМА 17. Материальная ответственность за разглашение и (или) утрату конфиденциальных сведений. Трудовой кодекс РФ о материальной ответственности. Условия наступления материальной ответственности. Процедура доказательства нанесения ущерба. Обстоятельства, исключающие ответственность работника за разглашение, уничтожение, утрату конфиденциальной информации. Порядок взыскания ущерба.

6. Методические материалы для обучающихся по освоению дисциплины

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторные занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы.

Обучающемуся важно помнить, что лекция эффективно помогает ему овладеть программным материалом благодаря расстановке преподавателем необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации. Кроме того, во время лекции имеет место прямой визуальный и эмоциональный контакт обучающегося с преподавателем, обеспечивающий более полную реализацию воспитательной компоненты обучения.

Самостоятельная работа преследует следующие цели:

- закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;
- формирование навыков осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности;
- совершенствование навыков оформления рабочей технической документации с учетом действующих нормативных и методических документов по организационному и правовому обеспечению информационной безопасности;
- совершенствование навыков разработки комплекса мер по обеспечению информационной безопасности объекта, организации его внедрения и последующего сопровождения;
- совершенствование навыков поиска публикаций и образовательных ресурсов, размещенных в сети Интернет;
- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем и учитываются при аттестации студента.

Предметом «Организационное и правовое обеспечение информационной безопасности» являются методические и законодательные материалы в области организационного и правового обеспечения защиты информации. Значимость методических и законодательных материалов в области организационного и правового обеспечения защиты информации и навыков работы с ними определяется тем, что вооружает специалиста по защите информации знаниями и данными о подходах к защите объектов. Знания методических и законодательных материалов позволяют правильно разрабатывать комплекс мер по обеспечению информационной безопасности объекта и организовать его внедрение, организовывать и сопровождать аттестацию объекта информатизации.

6.1. Самостоятельная работа обучающихся по дисциплине (модулю)

№ п/п	Раздел (тема)	Задание	Методические рекомендации по выполнению задания	Форма контроля

	дисциплины			
1	**2**	**3**	**4**	**5**
1.	Тема № 1	Усвоить	1. Изучить структуру, сущность и содержание понятия "обеспечение информационной безопасности». 2. Изучить основные виды организационных средств обеспечения информационной безопасности.	Контрольный опрос
2.	Тема № 2	Усвоить	1. Изучить основные принципы и услови организационной защиты информации. 2. Изучить основные подходы и требования к организации системы защиты информации. 3. Изучить основные силы и средства, используемые для организации защиты информации.	Контрольный опрос
3.	Тема № 3	Приобрес-ти навык	1.Изучить подходы к отнесению сведений к различным видам конфиденциальной информации. 2.Изучить положения Законодательство РФ о категориях доступа к информации. 3. Исследовать подходы к засекречиванию сведений и их носителей. 4. Изучить структуру перечня сведений, составляющих государственную тайну.	Проверка выполнения практического задания
4.	Тема № 4	Усвоить	1. Изучить основные положения допуска персонала предприятия к конфиденциальной информации. 2. Изучить порядок оформления и переоформления допуска к государственной тайне. Формы допуска. 3. Изучить этапы к организации доступа персонала предприятия к сведениям, со-ставляющим государственную тайну.	Контрольный опрос
5.	Тема № 5	Приобрес-ти навык	1. Изучить основные источники возможной утечки (разглашения) конфиденциальной информации. 2. Изучить методы работы с персоналом предприятия, допущенным к конфиденциальной информации. 3. Изучить факторы и обстоятельства разглашения конфиденциальной информации персоналом предприятия	Проверка выполнения практического задания
6	Тема № 6	Приобрес-ти навык	1.Изучить основные цели, подходы и принципы организации внутри объектового режима.. 2.Изучить цели и задачи пропускного режима. 3. Изучить основные элементы системы организации пропускного режима, используемые силы и средства.	Проверка выполнения практическог о задания

7	Тема № 7	Усвоить	1. Изучить цели и задачи охраны предприятия. 2. Изучить систему охраны предприятия. 3. Изучить права сотрудников подразделений охраны задач в пределах охраняемых объектов. 4. Изучить основные обязанности сотрудников охраны.	Контрольный опрос
8	Тема № 8		1. Изучить методы планирования мероприятий по защите информации при подготовке к проведению совещания 2. Изучить подходы к организации допуска участников совещания к обсуждаемым вопросам. 3. Изучить основы организации защиты информации в ходе издательской и рекламной деятельности предприятия.	Проверка выполнения практического задания
9	Тема № 9		1. Изучить порядок передачи различных видов конфиденциальной информации иностранным государствам. 2. Изучить подходы к организации подготовки к передаче сведений, составляющих государственную тайну. 3. Изучить ограничения прав гражданина, осведомленного в сведениях, составляющих государственную тайну, на выезд за границу.	Контрольный опрос
10	Тема № 10		1. Изучить положения Законодательства РФ о разглашении сведений конфиденциального характера. 2. Изучить этапы проведения служебного расследования. 3. Изучить задачи и функции комиссии по ведению служебного расследования.	Проверка выполнения практического задания
11	Тема № 11		1. Изучить положения Законодательства РФ о защите конфиденциальных сведений. 2. Изучить особенности коммерческой тайны, налоговой тайна, банковской тайны.	Проверка выполнения практического задания
12	Тема № 12		1. Изучить положения неправомерного доступа к компьютерной информации. 2. Изучить субъекты преступлений в сфере компьютерной информации. 3. Изучить положения Законодательства РФ о защите в сфере компьютерной информации.	Контрольный опрос
13	Тема № 13		1. Изучить субъекты преступлений в сфере защиты сведений, составляющих государственную тайну. 2. Изучить положения Законодательства РФ о защите сведений, составляющих государственную тайну.	Контрольный опрос

14	Тема № 14		1. Изучить положения административной ответственности за нарушение порядка обращения с информацией ограниченного распространения	Проверка выполнения практического задания
15	Тема № 15		1. Изучить положения Законодательства РФ о защита служебной и коммерческой тайны. 2. Изучить обязательные условия признания информации служебной или коммерческой тайной.	Проверка выполнения практического задания
16	Тема № 16		1. Изучить положения Законодательства РФ о дисциплинарной ответственности за разглашение и утрату конфиденциальных сведений. 2. Изучить признаки и виды дисциплинарного проступка.. 3. Изучить этапы процедуры вынесения наказания за дисциплинарный проступок.	Контрольный опрос
17	Тема № 17		1. Изучить положения Трудового кодекса РФ о материальной ответственности. 2. Изучить условия наступления материальной ответственности. 3. Изучить этапы процедуры доказательства нанесения ущерба.	Проверка выполнения практического задания

6.2. Тематика и задания для практических занятий

Формой отчетности по данной дисциплине является зачет. Необходимые условия допуска к зачету :

- Наличие полного конспекта лекций
- Сдача всех практических работ с положительным результатом

Занятие 1.

Тема: Концептуальные основы информационной безопасности..

Обсуждаемые вопросы: История возникновения органов защиты информации. Основные понятия информационной безопасности. Основные свойства информации в форме сведений. Информационная инфраструктура. Структура, сущность и содержание понятия "обеспечение информационной безопасности". Основные виды организационных средств обеспечения информационной безопасности.

.

Задание. Изучить основные виды организационных средств обеспечения информационной безопасности.

.

Занятие 2.

Тема: Основные принципы, условия, подходы и требования к организационной защите информации. Основные силы и средства, используемые для организации защиты информации.

Обсуждаемые вопросы: Основные принципы и условия организационной защиты информации. Основные направления защиты информации. Основные подходы и требования к организации системы защиты информации. Структура системы защиты информации. Основные силы и средства, используемые для организации защиты информации.

Задание. Разработать структуру системы защиты информации объекта защиты. Выбрать и описать силы и средства, используемые для организации защиты информации.

Занятие 3.

Тема: Отнесение сведений к конфиденциальной информации. Засекречивание и рассекречивание сведений.

Обсуждаемые вопросы: Отнесение сведений к различным видам конфиденциальной информации. Законодательство РФ о категориях доступа к информации. Грифы секретности и реквизиты носителей сведений, составляющих государственную тайну. Грифы секретности и реквизиты носителей сведений, составляющих коммерческую тайну. Отнесение сведений к государственной тайне. Засекречивание сведений и их носителей. Структура перечня сведений, составляющих государственную тайну. Основания и порядок рассекречивания сведений и их носителей. Отнесение сведений к коммерческой тайне.

Задание. Проанализировать грифы секретности. Работа с реквизитами носителей сведений, составляющих государственную тайну.

Занятие 4.

Тема: Организация допуска и доступа персонала к конфиденциальной.

Обсуждаемые вопросы: Основные положения допуска персонала предприятия к конфиденциальной информации. Порядок оформления и переоформления допуска к государственной тайне. Формы допуска. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне и условия прекращения допуска. Организация доступа персонала предприятия к сведениям, составляющим государственную тайну.

Задание. Оформление и переоформление документов допуска к государственной тайне. Оформление документов формы допуска. Разработка мероприятий по организации доступа персонала предприятия к сведениям, составляющим государственную тайну на объекте защиты.

Занятие 5.

Тема: Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации.

Обсуждаемые вопросы: Основные источники возможной утечки (разглашения) конфиденциальной информации. Факторы и обстоятельства разглашения конфиденциальной информации персоналом предприятия. Методы работы с персоналом предприятия, допущенным к конфиденциальной информации. Функции работодателя по отношению к сотруднику предприятия в целях охраны конфиденциальности информации, составляющей коммерческую тайну.

Задание. Оценить и проанализировать основные источники возможной утечки (разглашения) конфиденциальной информации на объекте защиты. Разработать подходы к работе с персоналом предприятия, допущенным к конфиденциальной информации на объекте защиты.

Занятие 6.

Тема: Организация внутри объектового и пропускного режимов на предприятии.

Обсуждаемые вопросы: Роль и место внутри объектового и пропускного режимов в общей системе защиты информации на предприятии**.** Основные цели, подходы и принципы организации внутри объектового режима. Силы и средства, используемые при организации внутри объектового режима. Цели и задачи пропускного режима. Основные элементы системы организации пропускного режима, используемые силы и средства.

Задание. Определить цели, подходы и принципы организации внутри объектового режима предприятия. Определить элементы системы организации пропускного режима, используемые силы и средства для выбранного объекта защиты.

Занятие 7.

Тема: Организация охраны предприятий.
Обсуждаемые вопросы: Цели охраны предприятия. Основные задачи охраны. Система охраны предприятия. Основные обязанности сотрудников охраны. Права сотрудников подразделений охраны задач в пределах охраняемых объектов. Главные требования, предъявляемые к системе охраны.
Задание. Разработать систему охраны выбранного предприятия.. Определить главные требования, предъявляемые к системе охраны объекта защиты.

Занятие 8.
Тема: Организация защиты информации при проведении совещаний.
Обсуждаемые вопросы: Планирование мероприятий по защите информации при подготовке к проведению совещания. Организация допуска участников совещания к обсуждаемым вопросам. Подготовка места проведения совещания. Порядок проведения совещания и использования его материалов. Основы организации защиты информации в ходе издательской и рекламной деятельности предприятия. Организация подготовки материалов к открытому опубликованию
Задание. Разработать план мероприятий по защите информации при подготовке к проведению совещания. Разработать подходы к организации защиты информации в ходе издательской и рекламной деятельности предприятия.
Занятие 9.
Тема: Основы защиты информации при осуществлении международного сотрудничества и выезде персонала.
Обсуждаемые вопросы: Порядок передачи различных видов конфиденциальной информации иностранным государствам. Организация подготовки к передаче сведений, составляющих государственную тайну, другим государствам. Ограничения прав гражданина, осведомленного в сведениях, составляющих государственную тайну, на выезд за границу. Работа должностных лиц предприятия по оформлению документов на выезд сотрудников в служебные командировки и по частным делам.

Задание. Разработать план организации подготовки к передаче сведений, составляющих государственную тайну, другим государствам. Оформить документы на выезд сотрудников в служебные командировки и по частным делам.
Занятие 10.
Тема: Организация и проведение служебного расследования в случае разглашения сведений конфиденциального характера или утраты носителей сведений.
Обсуждаемые вопросы: Законодательство РФ о разглашении сведений конфиденциального характера. Комиссия по ведению служебного расследования, задачи и функции. Этапы проведения служебного расследования
Задание. Деловая игра: Организовать комиссию по ведению служебного расследования. Провести служебное расследование по разглашению сведений конфиденциального характера.
Занятие 11.
Тема: Уголовно-правовая защита сведений, составляющих коммерческую, налоговую или банковскую тайну.
Обсуждаемые вопросы: Законодательство РФ о защите конфиденциальных сведений. Коммерческая тайна. Налоговая тайна. Банковская тайна.

Задание. Разработать план мероприятий по защите коммерческой тайны на объекте защиты.
Занятие 12.
Тема: Уголовно-правовая защита в сфере компьютерной информации

Обсуждаемые вопросы: Понятие неправомерного доступа к компьютерной информации. Понятие охраняемой законом информации. Субъекты преступлений в сфере компьютерной информации. Законодательство РФ о защите в сфере компьютерной информации.

Задание. Оценить субъекты преступлений по компьютерной информации на выбранном объекте защите. Разработать план мероприятий по защите от преступлений по компьютерной информации на выбранном объекте защите.

Занятие 13.

Тема: Уголовно-правовая защита сведений, составляющих государственную тайну..

Обсуждаемые вопросы: Субъекты преступлений в сфере защиты сведений, составляющих государственную тайну. Законодательство РФ о защите сведений, составляющих государственную тайну. Понятие государственной измены.

Задание. Оценить субъекты преступлений в сфере защиты сведений на выбранном объекте защите. Разработать план мероприятий по защите от преступлений защиты сведений на выбранном объекте защите.

Занятие 14.

Тема: Административно-правовая защита информации с ограниченным доступом.

Обсуждаемые вопросы: Административная ответственность за нарушение порядка обращения с информацией ограниченного распространения в Кодексе об административных правонарушениях.

Задание. Оценить субъекты преступлений в сфере защиты информации с ограниченным доступом на выбранном объекте защите. Разработать план мероприятий по защите информации с ограниченным доступом на выбранном объекте защиты.

Занятие 15.

Тема: Гражданско-правовая защита служебной и коммерческой тайны.

Обсуждаемые вопросы: Законодательство РФ о защита служебной и коммерческой тайны. Обязательные условия признания информации служебной или коммерческой тайной.

Задание. Оценка условий признания информации служебной и коммерческой тайной на выбранном объекте защиты.

Занятие 16.

Тема: Дисциплинарная ответственность за разглашение и (или) утрату конфиденциальных сведений.

Обсуждаемые вопросы: Законодательство РФ о дисциплинарной ответственности за разглашение и утрату конфиденциальных сведений. Признаки дисциплинарного проступка. Виды дисциплинарной ответственности. Процедура вынесения наказания за дисциплинарный проступок.

Задание. Оценить признаки дисциплинарного проступка на выбранном объекте защиты. Выбрать вид дисциплинарной ответственности. Разработать процедуру вынесения наказания за дисциплинарный проступок.

Занятие 17.

Тема: Материальная ответственность за разглашение и (или) утрату конфиденциальных сведений

Обсуждаемые вопросы: Трудовой кодекс РФ о материальной ответственности. Условия наступления материальной ответственности. Процедура доказательства нанесения ущерба. Обстоятельства, исключающие ответственность работника за разглашение, уничтожение, утрату конфиденциальной информации. Порядок взыскания ущерба.

.

Задание. Оценить условия наступления материальной ответственности на объекте защиты. Составить доказательства нанесения ущерба на объекте защиты. разработать порядок взыскания ущерба по объекту защиты.

7. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины (модуля)

а) основная

1. Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 239 с. : ил. — (Высшее образование: Бакалавриат). http://znanium.com/catalog.php?bookinfo=612572
2. Информационная безопасность и защита информации: Учебное пособие. / Баранова Е.К., Бабаш А.В. — 3-е изд., перераб. и доп. — М.: РИОР: ИНФРА-М, 2017. — 322 с. — (Высшее образование). — ww.dx.doi.org/10.12737/11380. http://znanium.com/catalog.php?bookinfo=763644
3. Обеспечение информационной безопасности машиностроительных предприятий : В 2-х ч.: учебник для вузов . Ч.1 / С. А. Клейменов [и др.]. - Старый Оскол : ТНТ, 2011. - 360 с.: рис. - УМО. - СД. - обязат. - ISBN 978-5-94178-282-6 : 582.48.
4.
Галатенко, В. А. Основы информационной безопасности : курс лекций : учеб. пособие / В. А. Галатенко ; под ред. В. Б. Петелина. - Изд. 3-е. - М. : ИНТУИТ, 2006. - 208 с. - (Серия "Основы информационных технологий"). - Библиогр.: с. 200-205. - ISBN 5-9556-0052-3 : 200.00.
Рекомендовано

б) дополнительная

1. Золотарев, В. В. Управление информационной безопасностью. Ч. 1. Анализ информационных рисков [Электронный ресурс] : учеб. пособие/ В. В. Золотарев, Е. А. Данилова. - Красноярск :Сиб. гос. аэрокосмич. ун-т, 2010. - 144 с.
http://znanium.com/catalog.php?bookinfo=463037
2. Жукова, М. Н. Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности [Электронный ресурс] : учеб. пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с.
http://znanium.com/catalog.php?bookinfo=463061
3. Городов, О. А. Информационное право : учебник для бакалавров / Городов Олег Александрович. - Москва : Проспект, 2014. - 256 с. - ОПД. - осн. - ISBN 978-5-392-12269-1 : 275.00.
4. Организационно-правовое обеспечение информационной безопасности : учеб. пособие для вузов / А. А. Стрельцов [и др.] ; под ред. А.А. Стрельцова. - Москва : Академия, 2008. - 256 с. - (Высш. проф. образование. Информац. безопасность). - УМО спец. 090102 - Компьютерная безопасность; 090105 - Комплексное обеспечение информационной безопасности автоматизир. систем; 090106 - Информационная безопасность телекоммуникационных систем. - ЕН. - ISBN 978-5-7695-4240-4
5. Мельников, Владимир Павлович.
Информационная безопасность и защита информации : учеб. пособие для вузов спец. 230201 "Информац. системы и технологии" / Мельников Владимир Павлович, С. А. Клейменов, А. М. Петраков ; под ред. Клейменова С.А. - 3-е изд., стер. - Москва : Академия, 2008. - 336 с. - (Высш. проф. образов. Информат. и выч. техн.). - УМО. - ЕН, ОПД, СД. - ISBN 978-5-7695-4884-0 : 165.66.

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

Информационно-образовательные ресурсы:
1. www.atlas.Krasnodar.ru -КФ НТЦ «Атлас»: защита информации.
Электронные библиотечные системы:

1. Университетская библиотека онлайн http://biblioclub.ru
2. «Лань» http://e.lanbook.com/
3. ЭБС «Znanium»
4. Справочно-информационная система (СИС) «Гарант».
5. Справочно-информационная система «Консультант».
6.Электронно-библиотечная система (ЭБС) «Инфра-М».

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

Мультимедийный комплекс, включающий электронную доску, ноутбук и проектор.