МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Костромской государственный университет»

(КГУ)

УТВЕРЖДЕНО:

На заседании кафедры защиты информации

Протокол заседания № 10 от 15 мая 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Направленность/специализация: «Организация и технология защиты информации»

Квалификация выпускника: Бакалавр

Кострома 2023

Рабочая программа дисциплины «Организационное и правовое обеспечение информационной безопасности» разработана в соответствии с Федеральным государственным образовательным стандартом по направлению подготовки:

10.03.01	Информационная безопасность	ФГОС ВО - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность, утвержденный Минобранауки № 1427 от 17.11.2020
Разработал:	Виноградова Г. Л.	Доцент кафедры защиты информации, к. т. н.
Рецензент:	Щекочихин О.В.	Доцент кафедры защиты информации, к. т. н.

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.

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:

освоить компетенции:

Код и содержание индикаторов компетенции :

ОПК-5 - способность использовать нормативные правовые акты в профессиональной деятельности;

Код и содержание индикаторов компетенции:

ИК.ОПК5.1.Владеет способностью использовать нормативные правовые акты в профессиональной деятельности

ПСК-2.4 - способность организовать контроль защищенности объекта в соответствии с нормативными документами.

Код и содержание индикаторов компетенции:

ИК.ПСК2.4.1.Владеет способностью организовать контроль защищенности объекта в соответствии с нормативными документами.

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.

3. Место дисциплины в структуре ОП ВО

Дисциплина относится к обязательной части учебного плана. Изучается в 5 семестре обучения.

Изучение дисциплины основывается на ранее освоенных дисциплинах/практиках: «Теоретические основы информационных процессов», «Основы информационной безопасности».

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».

Компетенция ОПК-5 осваивается так же на следующих дисциплинах:

Б1.О.32	Организация и управление службой защиты информации на предприятии

4. Объем дисциплины

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

Виды учебной работы,	Очная форма	Очно-заочная	Заочная
Общая трудоемкость в зачетных единицах	3		

Общая трудоемкость в часах	108		
Аудиторные занятия в часах, в том числе:			
Лекции	34		
Практические занятия	-		
Лабораторные занятия	34		
Практическая подготовка			
Самостоятельная работа в часах	39,75		
Форма промежуточной аттестации	зачет		

4.2. Объем контактной работы на 1 обучающегося

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

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

5.1 Тематический план учебной дисциплины

№	Название раздела, темы	Всего з.е/час	Аудиторные занятия			Самостоятельная работа
			Лекц.	Практ.	Лаб.	
1	Раздел 1. Введение в организационное и правовое обеспечение информационной безопасности	5	2		2	3
1.1	Концептуальные основы информационной безопасности.	5	2		2	3
2	Раздел 2. Организационные основы защиты информации	58	18		18	22
2.1	Основные принципы, условия, подходы и требования к организационной защите информации. Основные силы и средства, используемые для организации защиты	6	2		2	2

	информации.					
2.2	Отнесение сведений к конфиденциальной информации. Засекречивание и рассекречивание сведений.	7	2		2	3
2.3	Организация допуска и доступа персонала к конфиденциальной информации.	6	2		2	2
2.4	Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации	7	2		2	3
2.5	Организация внутри объектового и пропускного режимов на предприятии.	6	2		2	2
2.6	Организация охраны предприятий	7	2		2	3
2.7	Организация защиты информации при проведении совещаний	6	2		2	2
2.8	Основы защиты информации при осуществлении международного сотрудничества и выезде персонала	7	2		2	3
2.9	Организация и проведение служебного расследования в случае разглашения сведений конфиденциального характера или утраты носителей сведений	6	2		2	2
3	Раздел 3. Правовая защита конфиденциальной информации	45	14		14	17
3.1	Уголовно-правовая защита сведений, составляющих коммерческую, налоговую или банковскую тайну.	7	2		2	3
3.2	Уголовно-правовая защита в сфере компьютерной информации.	6	2		2	2
3.3	Уголовно-правовая защита сведений, составляющих государственную тайну	6	2		2	2
3.4	Административно-правовая защита информации с ограниченным доступом	6	2		2	2
3.5	Гражданско-правовая защита	6	2		2	2

	служебной и коммерческой тайны					
3.6	Дисциплинарная ответственность за разглашение и (или) утрату конфиденциальных сведений	7	2		2	3
3.7	Материальная ответственность за разглашение и (или) утрату конфиденциальных сведений	7	2		2	3
	Зачет					0,25
	Итого:	3\108	34		34	**39,75**

5.2. Содержание:

Раздел 1. Введение в организационное и правовое обеспечение 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.

Раздел 2. Организационные основы 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.

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.

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.

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.

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.

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.
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.
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.

Законодательство РФ о разглашении сведений конфиденциального характера. Комиссия по ведению служебного расследования, задачи и функции. Этапы проведения служебного расследования.

Раздел 3. Правовая защита конфиденциальной информации

Законодательство РФ о защите конфиденциальных сведений. Коммерческая тайна. Налоговая тайна. Банковская тайна.
Понятие неправомерного доступа к компьютерной информации. Понятие охраняемой законом информации. Субъекты преступлений в сфере компьютерной информации. Законодательство РФ о защите в сфере компьютерной информации.
Субъекты преступлений в сфере защиты сведений, составляющих государственную тайну. Законодательство РФ о защите сведений, составляющих государственную тайну. Понятие государственной измены.
Административная ответственность за нарушение порядка обращения с информацией ограниченного распространения в Кодексе об административных правонарушениях.
Законодательство РФ о защита служебной и коммерческой тайны. Обязательные условия признания информации служебной или коммерческой тайной.
Законодательство РФ о дисциплинарной ответственности за разглашение и утрату конфиденциальных сведений. Признаки дисциплинарного проступка. Виды дисциплинарной ответственности. Процедура вынесения наказания за дисциплинарный проступок.
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

6.1. Самостоятельная работа обучающихся по дисциплине (модулю)

№ п/п	**Раздел (тема) дисциплины**	**Задание**	**Часы Очная форма**	**Часы очно-заочная,**	**Методические рекомендации по выполнению**	**Форма контроля**

				заочная	**задания**	
1	Раздел 1. Введение в организационное и правовое обеспечение информационной безопасности.	Изучение литературы и Интернет-источников	3	-	В качестве литературных источников предпочтительнее использовать [1] из списка дополнительной литературы и [4, 5] из списка основной литературы	Проверка
2	Раздел 2. Организационные основы защиты информации	Изучение литературы и Интернет-источников	22	-	В качестве литературных источников предпочтительнее использовать [1] из списка дополнительной литературы и [4, 5] из списка основной литературы	Тестирование
3	Раздел 3. Правовая защита конфиденциальной информации	Составление программ	17	-	Для подготовки к составлению программ рекомендуется пользоваться учебными пособиями [2] из списка основной литературы и [1] из списка дополнительной литературы	Контрольная
4	Зачет	Решение зачетных заданий	0,25	-	Для подготовки к составлению программ рекомендуется пользоваться учебными пособиями [2] из списка основной литературы и [2] из списка дополнительной литературы	Зачет

6.2. Тематика и задания для практических занятий

1. Изучение основных видов организационных средств обеспечения информационной безопасности.
2. Разработка структуры системы защиты информации объекта защиты. Выбрать и описать силы и средства, используемые для организации защиты информации.
3. Анализ грифов секретности. Работа с реквизитами носителей сведений, составляющих государственную тайну.
4. 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.
5. Оценка и анализ основных источников возможной утечки (разглашения) конфиденциальной информации на объекте защиты. Разработка подходов к работе с персоналом предприятия, допущенным к конфиденциальной информации на объекте защиты.
6. Определение целей, подходов и принципов организации внутри объектового режима предприятия.
7. Определение элементов системы организации пропускного режима, используемые силы и средства для выбранного объекта защиты.

8. Разработка системы охраны выбранного предприятия.. Определение главных требований, предъявляемых к системе охраны объекта защиты.
9. Разработка плана мероприятий по защите информации при подготовке к проведению совещания.
10. Разработка подходов к организации защиты информации в ходе издательской и рекламной деятельности предприятия.
11. Разработка плана организации подготовки к передаче сведений, составляющих государственную тайну, другим государствам. Оформление документов на выезд сотрудников в служебные командировки и по частным делам.
12. Разработка плана мероприятий по защите коммерческой тайны на объекте защиты
13. Организация комиссии по ведению служебного расследования. Проведение служебного расследования по разглашению сведений конфиденциального характера.
14. Оценка субъектов преступлений по компьютерной информации на выбранном объекте защите. Разработка плана мероприятий по защите от преступлений по компьютерной информации на выбранном объекте защите.
15. Оценка субъектов преступлений по компьютерной информации на выбранном объекте защите. Разработка плана мероприятий по защите от преступлений по компьютерной информации на выбранном объекте защите.
16. Оценка субъектов преступлений в сфере защиты сведений на выбранном объекте защите. Разработка плана мероприятий по защите от преступлений защиты сведений на выбранном объекте защите.
17. Оценка субъектов преступлений в сфере защиты информации с ограниченным доступом на выбранном объекте защите.
18. Разработка плана мероприятий по защите информации с ограниченным доступом на выбранном объекте защиты.
19. Оценка условий признания информации служебной и коммерческой тайной на выбранном объекте защиты.
20. Оценка признаков дисциплинарного проступка на выбранном объекте защиты. Выбрать вид дисциплинарной ответственности. Разработка процедуры вынесения наказания за дисциплинарный проступок.

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

Темы докладов на практических занятиях

1. Концептуальные основы информационной безопасности..
2. Основные принципы, условия, подходы и требования к организационной защите информации. Основные силы и средства, используемые для организации защиты информации.
3. Отнесение сведений к конфиденциальной информации. Засекречивание и рассекречивание сведений.
4. Организация допуска и доступа персонала к конфиденциальной.
5. Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации.
6. Организация внутри объектового и пропускного режимов на предприятии.
7. Организация охраны предприятий.
8. Организация защиты информации при проведении совещаний.
9. Основы защиты информации при осуществлении международного сотрудничества и выезде персонала.
10. Организация и проведение служебного расследования в случае разглашения сведений конфиденциального характера или утраты носителей сведений.
11. Уголовно-правовая защита сведений, составляющих коммерческую, налоговую или банковскую тайну.
12. Уголовно-правовая защита в сфере компьютерной информации
13. Уголовно-правовая защита сведений, составляющих государственную тайну..
14. Административно-правовая защита информации с ограниченным доступом.
15. Гражданско-правовая защита служебной и коммерческой тайны.
16. Дисциплинарная ответственность за разглашение и (или) утрату конфиденциальных сведений.
17. Материальная ответственность за разглашение и (или) утрату конфиденциальных сведений

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

а) основная:

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.
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

Информация о курсе дисциплины в СДО:
Элемент «Лекции»*;*
Элемент «Практические занятия», «Лабораторные занятия»*;*
Элемент «Самостоятельная работа»;
Информационно-образовательные ресурсы:

1. Библиотека ГОСТов. Все ГОСТы, [Электронный ресурс], URL:http://vsegost.com/

Электронные библиотечные системы:

1. ЭБС Университетская библиотека онлайн - http://biblioclub.ru
2. ЭБС «Лань» https://e.lanbook.com
3. ЭБС «ZNANIUM.COM» http://znanium.com
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

Лекционные занятия проводятся в аудиториях с требуемым числом посадочных мест, оборудованные мультимедиа.

Практические занятия проводятся в компьютерных классах.

Лицензионное программное обеспечение:

Не требуется

Свободно распространяемое программное обеспечение:

Офисный пакет