Негосударственное аккредитованное некоммерческое частное образовательное учреждение высшего образования
«Академия маркетинга и социально-информационных технологий – ИМСИТ»
г. Краснодар

Академический колледж

УТВЕРЖДАЮ
Проректор по учебной работе,
доцент Н. И. Севрюгина
28 марта 2022 г.

ПМ.01 Участие в планировании и организации работ по обеспечению защиты информации

рабочая программа профессионального модуля

для студентов специальности

10.02.01 Организация и технология защиты информации

Технический профиль

Квалификация выпускника -Техник по защите информации

г. Краснодар 2022

Рассмотрено
на заседании предметно цикловой комиссии
Протокол № 8 от 21 марта 2022г.
Председатель ПЦК А.А. Куценко
Зав. ИИО Академического колледжа
Ю.А. Худына

Принято
педагогическим советом
Академического колледжа
Протокол № 7
от 22 марта 2022 г.

Рабочая программа разработана на основе основной профессиональной образовательной программы среднего профессионального образования программы подготовки специалистов среднего звена, специальности 10.02.01 Организация и технология защиты информации, Федерального закона Российской Федерации от 29 декабря 2012 г. № 273- ФЗ Об образовании в Российской Федерации (редакция от 25.12.2018 г.) и требований ФГОС среднего профессионального образования (приказ от 28.07.2014 г. №805 Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.01 Организация и технология защиты информации (Зарегистрировано в Минюсте России 21.08.2014 г. № 33750) технического профиля профессионального образования.

Содержание программы реализуется в процессе освоения студентами основной профессиональной образовательной программы по специальности 10.02.01 Организация и технология защиты информации технического профиля (на базе основного общего образования) в соответствии с требованиями ФГОС СПО на 3 курсе (ах) в 5,6 семестре (ах).

Рецензенты:

Заместитель директора по учебно-методической работе ЧУ ПОО КТУИС г. Краснодар, Бондаренко Н. А.

Директор ООО «Вектор» г. Краснодар,
Бромберг Е. М.

Советник директора ООО «Аэро-тревел», г. Краснодар,
Коробенко Я.В.

СОДЕРЖАНИЕ

1 ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1 Область применения программы

Примерная программа учебной дисциплины «Обеспечение организации системы безопасности предприятия» является частью примерной основной профессиональной образовательной программы в соответствии с ФГОС по специальности 10.02.01 «Организация и технология защиты информации».

Примерная программа учебной дисциплины «Обеспечение организации системы безопасности предприятия» может быть использована для разработки программ в управления процессами и потоками.

1.2 Место дисциплины в структуре основной средне - специальной профессиональной образовательной программы

Дисциплина входит в цикл профессионального модуля.

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 7. Оценивать значимость документов, применяемых в профессиональной деятельности.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ОК 10. Применять математический аппарат для решения профессиональных задач.

ОК 11. Оценивать значимость документов, применяемых в профессиональной деятельности.

ОК 12. Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность.

Участие в планировании и организации работ по обеспечению защиты объекта.

ПК 1.1. Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации.

ПК 1.2. Участвовать в разработке программ и методик организации защиты информации на объекте.

ПК 1.3. Осуществлять планирование и организацию выполнения мероприятий по защите информации.

ПК 1.4. Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности.

ПК 1.5. Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации.

ПК 1.6. Обеспечивать технику безопасности при проведении организационно-технических мероприятий.

ПК 1.7. Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите.

ПК 1.8. Проводить контроль соблюдения персоналом требований режима защиты информации.

ПК 1.9. Участвовать в оценке качества защиты объекта.

1.3 Цели и задачи дисциплины

Целью дисциплины «Обеспечение организации системы безопасности предприятия» - сформировать понимание о принципах, силах, средствах и условиях организационной защиты информации.

Задачи дисциплины:

– ознакомить будущих специалистов с назначением и структурой организационной защиты информации;

–

–

–

–

–

–

1.4 Формирование личностных результатов воспитательной работы обучающихся

ЛР 1. Осознающий себя гражданином и защитником великой страны.

ЛР2.Проявляющий активную гражданскую позицию, демонстрирующий иверженность принципам честности, порядочности, открытости, экономической активности частвующий в студенческом и территориальном самоуправлении, в том числе на условиях бровольчества, продуктивно взаимодействующий и участвующий в деятельности щественных организаций.

ЛР3.Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, еспечения безопасности, права и свобод граждан России. Лояльный к установкам и оявлениям представителей субкультур, отличающий их от групп с деструктивным и зиантным поведением. Демонстрирующий неприятие и предупреждающий социально асное поведение окружающих.

ЛР4. Проявляющий и демонстрирующий уважение к людям труда, осознающий нность собственного труда. Стремящийся к формированию в сетевой среде личностно и офессионального конструктивного «цифрового следа».

ЛР5.Демонстрирующий приверженность к родной культуре, исторической памяти на нове любви к Родине, родному народу, малой родине, принятию традиционных ценностей огонационального народа России.

ЛР6. Проявляющий уважение к людям старшего поколения и готовность к участию в циальной поддержке и волонтерских движениях.

ЛР7. Осознающий приоритетную ценность личности человека; уважающий собственную ружую уникальность в различных ситуациях, во всех формах и видах деятельности.

ЛР8. Проявляющий и демонстрирующий уважение к представителям различных юкультурных, социальных, конфессиональных и иных групп. Сопричастность к сохранению, еумножению и трансляции культурных традиций и ценностей многонационального ссийского государства.

ЛР9. Соблюдающий и пропагандирующий правила здорового и безопасного образа зни, спорта; предупреждающий либо преодолевающий зависимости от алкоголя, табака, ихоактивных веществ, азартных игр и т.д. Сохраняющий психологическую устойчивость в гуативно сложных или стремительно меняющихся ситуациях.

ЛР10. Заботящийся о защите окружающей среды, собственной и чужой безопасности, в м числе цифровой.

ЛР11. Проявляющий уважение к эстетическим ценностям, обладающий основами етической культуры.

ЛР12. Принимающий семейные ценности, готовый к созданию семьи и воспитанию тей; демонстрирующий неприятие насилия в семье, ухода от родительской ответственности, каза от отношений со своими детьми и их финансового содержания.

1.5 Требования к уровню освоения содержания дисциплины

Дать студентам возможность приобрести знания по следующим направлениям:

– анализ эффективности системы организационной защиты информации и разработка направлений ее развития;

– умение разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации; организовывать работу с персоналом, обладающим конфиденциальной информацией;

– организация охраны персонала, территорий, зданий, помещений и продукции организаций;

– организация и проведение аналитической работы по предупреждению утечки конфиденциальной информации.

После изучения данного курса студенты должны приобрести знания по организационному обеспечению информационной безопасности и формированию практических навыков работы в реальных конкретных условиях.

Курс рассчитан на проведение лекционных занятий и практических занятий.

1.6 Количество часов на освоение программы учебной дисциплины

Максимальной учебной нагрузки студента 189 часов, в том числе:

- обязательной аудиторной учебной нагрузки студента 127 часов;
- практических занятий студента 43 часа;
- Курсовой проект (работа) 30 часов.

2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1 Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Всего часов	семестр	
		5	6
Общая трудоемкость дисциплины	189	96	63
Аудиторные занятия	127	64	63
Лекции	54	32	22
Практические занятия (ПЗ)	43	32	11
Семинары (С)			
Лабораторные работы (ЛР)			
и (или) другие виды аудиторных занятий			
Самостоятельная работа	62	32	30
Курсовой проект (работа)	30	30	
Реферат и (или) другие виды самостоятельной работы			
Вид промежуточного контроля (зачет, экзамен)			диф.зачет

2.2 Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Уровень освоения
5 семестр			

Тема 1. Введение в дисциплину. Концепция информационной безопасности.	1. Основные концептуальные положения системы защиты информации. 2. Концептуальная модель информационной безопасности. 3. Угрозы конфиденциальной информации. 4. Действия, приводящие к неправомерному овладению конфиденциальной информацией.	6	1
	Практические занятия		
	Угрозы конфиденциальной информации.	2	3
Тема 2. Основные направления организационного обеспечения безопасности информационных ресурсов.	1. Правовая защита информации. 2. Организационная защита информации. 3. Инженерно-техническая защита информации. 4. Государственная политика информационной безопасности и организационная основа ее обеспечения. 5. Структура и общая характеристика информационного законодательства.	6	1
	Практические занятия		
	1. Государственная политика информационной безопасности и организационная основа ее обеспечения. 2. Структура и общая характеристика информационного законодательства.	4	2
Тема 3. Аналитическая работа органов защиты информации.	1. Понятие информационно-аналитической работы. 2. Направления аналитической работы. 3. Этапы аналитической работы. 4. Методы аналитической работы. 5. Система защиты конфиденциальной информации.	8	1
	Практические занятия		
	1. Основы политики государства в области правового обеспечения информационной безопасности. 2. Система защиты конфиденциальной информации.	4	2
Тема 4. Организационное обеспечение безопасности обработки конфиденциальных документов..	1. Защищенный документооборот. 2. Технологические системы защиты и обработки конфиденциальных документов. 3. Принципы учета конфиденциальных документов. 4. Учет поступивших пакетов и документов. 5. Распределение, рассмотрение и направление документов на исполнение. 6. Этапы подготовки конфиденциальных документов. 7. Учет, изготовление и издание документов. 8. Технология контроля исполнения документов и поручений.	9	1

	9. Порядок работы персонала с конфиденциальными документами и материалами. 10. Обработка изданных документов. 11. Назначение и порядок проведения проверки наличий документов, дел и носителей информации. 12. Порядок уничтожения документов, дел и носителей информации. 13. Особенности составления и ведения номенклатуры дел. 14. Формирование и ведение дел.		
	Практические занятия		
	1. Защищенный документооборот. 2. Принципы учета конфиденциальных документов. 3. Учет поступивших пакетов и документов. 4. Особенности учета грифованных документов.	4	3
	Самостоятельная работа		
Тема 5. Организационное обеспечение безопасности информации при работе с персоналом.	1. Персонал как основная опасность утраты конфиденциальной информации. 2. Методы получения ценной информации у персонала. 3. Особенности приема и перевода сотрудников на работу, связанную с владением конфиденциальной информацией. 4. Доступ персонала к конфиденциальным сведениям, документам и базам данных. 5. Особенности увольнения сотрудников, владеющих конфиденциальной информацией.	6	1
	Практические занятия		
	1. Персонал как основная опасность утраты конфиденциальной информации. 2. Методы получения ценной информации у персонала. 3. Особенности приема и перевода сотрудников на работу, связанную с владением конфиденциальной информацией.	5	3
	Самостоятельная работа		
Тема 6. Организационное обеспечение безопасности информации в особых условиях.	1. Организация организационной защиты информации при проведении переговоров. 2. Организация организационной защиты информации при проведении совещаний. 3. Особенности организационной защиты информации при проведении спасательной операции. 4. Организация организационной защиты информации при проведении переговоров с зарубежными партнерами.	6	1
	Практические занятия		

	1. Организация организационной защиты информации при проведении переговоров. 2. Организация организационной защиты информации при проведении совещаний. 3. Особенности организационной защиты информации при проведении спасательной операции. 4. Организация организационной защиты информации при проведении переговоров с зарубежными партнерами.	4	3
	Самостоятельная работа		
	Итого за семестр 5 семестр	**64**	
	6 семестр		
Тема 7. Ответственность за правонарушения в информационной сфере.	1. Понятие и виды юридической ответственности за нарушение норм по защите информации. 2. Уголовная ответственность за правонарушения в области защиты государственной тайны. 3. Уголовная ответственность за компьютерные преступления. 4. Административная ответственность за правонарушения в области информационной безопасности.	4	2
	Практические занятия		
	Гражданско-правовая ответственность за правонарушения в информационной сфере.	2	3
	Самостоятельная работа		
Тема 8. Организация доступа и допуска персонала и посетителей на объект.	1. Организация доступа персонала и посетителей на объект 2. Организация допуска персонала и посетителей на объект 3. Оформление допуска персоналу. 4. Ограничения на оформление допуска. 5. Ограничения после оформления допуска.	6	1
	Практические занятия		
	1. Организация доступа персонала и посетителей на объект 2. Организация допуска персонала и посетителей на объект 3. Оформление допуска персоналу. 4. Ограничения на оформление допуска. 5. Ограничения после оформления допуска.	3	3
	Самостоятельная работа		
Тема 9. Выделенные помещения на объекте.	1. Требования к выделенным помещениям. 2. Проведение специсследований и спецпроверки выделенных помещений.	4	1
	Практические занятия		
	1. Требования к выделенным помещениям. 2. Проведение специсследований и спецпроверки вы-	2	2

	деленных помещений.		
	Самостоятельная работа		
Тема 10. Порядок засекречивания и рассекречивания сведений, документов и продукции	1. Перечень сведений, подлежащих засекречиванию. 2. Порядок засекречивания сведений и документов. 3. Порядок засекречивания продукции. 4. Требования, предъявляемые к засекреченным сведениям. 5. Требования, предъявляемые к засекреченной продукции. 6. Правила использования засекреченных сведений, документов и продукции. 7. Порядок рассекречивания сведений, документов и продукции.	8	1
	Практические занятия		
	1. Перечень сведений, подлежащих засекречиванию. 2. Порядок засекречивания сведений и документов. 3. Порядок засекречивания продукции. 4. Требования, предъявляемые к засекреченным сведениям.	4	3
	Самостоятельная работа		
	Итого за 6 семестр	**63**	
	Итого за год	**127**	

1. – ознакомительный (узнавание ранее изученных объектов, свойств);
2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)
3. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

3 КОНТРОЛЬНЫЕ ВОПРОСЫ ПО ДИСЦИПЛИНЕ

1. Введение в дисциплину.
2. Основные положения организационного обеспечения безопасности информации.
3. Объекты защиты и основные виды угроз интересам организации.
4. Базовые законы в области информационной деятельности и защиты информации .
5. Коммерческая тайна и ее защита.
6. Влияние организации офисной деятельности на реализацию защиты информации.
7. Сущность информационно-аналитической работы.
8. Методология информационно-аналитической работы.
9. Направления, этапы и методы аналитической работы.
10. Принципы информационно-аналитической работы.
11. Методология работы с открытыми источниками информации.
12. Организация защиты информации при осуществлении рекламной и публикационной деятельности.
13. Организация защиты информации при проведении совещаний.
14. Организация защиты информации при проведении переговоров.
15. Особенности защиты информации при проведении переговоров с зарубежными партнерами.
16. Правовое обеспечение защиты конфиденциальной информации.
17. Законодательные акты о государственной тайне и ее защите.
18. Организация допуска к сведениям, составляющим государственную тайну.
19. Порядок засекречивания и рассекречивания сведений, документов и продукции.
20. Ответственность за преступления в сфере компьютерной информации.
21. Методы и средства внешней защиты объекта.
22. Способы аутенфикации персонала.
23. Возможные каналы утраты информации.
24. Аудит выделенных помещений от несанкционированного получения информации.
25. Контроль функционирования системы организационной защиты информации.
26. Требования к выделенным помещениям.
27. Проведение специсследований и спецпроверки выделенных помещений.

28. Перечень сведений, подлежащих засекречиванию.

29. Порядок засекречивания сведений и документов.

30. Порядок засекречивания продукции.

31. Требования, предъявляемые к засекреченным сведениям.

32. Требования, предъявляемые к засекреченной продукции.

33. Правила использования засекреченных сведений, документов и продукции.

34. Порядок рассекречивания сведений, документов и продукции.

4 УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

Реализация учебной дисциплины требует наличия учебного компьютерной лаборатории. Оборудование компьютерной лаборатории:

- рабочее место студентов;
- рабочее место преподавателя;
- рабочая доска.

Технические средства обучения:

- компьютерная техника для обучающихся с наличием лицензионного программного обеспечения.

Программное обеспечение:

- Операционная система Microsoft Windows.
- Офисный пакет Microsoft Office Professional.
- Браузер для работы в Интернете Internet Explorer.
- Выход на сетевой диск S.

5 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДЛЯ ОБУЧАЮЩИХСЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Специфика получаемой направленности (профиля) образовательной программы предполагает возможность обучения следующих категорий инвалидов и лиц с ограниченными возможностями здоровья:

— с ограничением двигательных функций;

— с нарушениями слуха.

Организация образовательного процесса обеспечивает возможность беспрепятственного доступа обучающихся с ограниченными возможностями здоровья и (или) инвалидов в учебные аудитории и другие помещения, для этого имеются пандусы, поручни, лифты и расширенные дверные проемы.

В учебных аудиториях и лабораториях имеется возможность оборудовать места для студентов-инвалидов с различными видами нарушения здоровья, в том числе опорно-двигательного аппарата и слуха. Освещенность учебных мест устанавливается в соответствии с положениями СНиП 23-05-95 «Естественное и искусственное освещения». Все предметы, необходимые для учебного процесса, располагаются в зоне максимальной досягаемости вытянутых рук.

Помещения предусматривают учебные места для лиц с ограниченными возможностями здоровья и инвалидов, имеющих сердечно-сосудистые заболевания, они оборудованы солнцезащитными устройствами (жалюзи), в них имеется система климат-контроля.

По необходимости для инвалидов и лиц с ограниченными возможностями здоровья разрабатываются индивидуальные учебные планы и индивидуальные графики, обучающиеся обеспечиваются печатными и электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

6 УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

6.1 Основная литература

1. Гришина Н.В. Информационная безопасность предприятия: Учебное пособие / Гришина Н.В., - 2-е изд., доп - М.:Форум, НИЦ ИНФРА-М, 2019. - 240 с.

2. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / Шаньгин В. Ф. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2019. - 416 с.

3. Ищейнов В.Я. Основные положения информационной безопасности: Учебное пособие/В.Я.Ищейнов, М.В.Мецатунян - М.: Форум, НИЦ ИНФРА-М, 2020. - 208 с.:

4. Партыка Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2020. - 432 с.:

5. Васильков А.В. Безопасность и управление доступом в информационных системах: учебное пособие / Васильков А.В., Васильков И.А. - М.:Форум, НИЦ ИНФРА-М, 2019. - 368 с.

6.2 Дополнительная литература

Для преподавателя

1. Конституция РФ.

2. Гражданский кодекс РФ (Принят Государственной думой 21 октября 1994 г.)

3. Уголовный Кодекс РФ (Принят Государственной думой 24 мая 1996 г., одобрен Советом Федерации 5 июня 1996 г.).

4. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ.

5. Федеральный закон (ФЗ) «О безопасности» от 5 марта 1992 г. № 2446-1.

6. ФЗ «О государственной тайне» от 21 июля 1993 г. № 5485-1.

7. ФЗ «О коммерческой тайне» от 9 июля 2004 г. № 98-ФЗ.

8. ФЗ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ.

9. ФЗ «О экспортном контроле» от 22 июня 1999 г. № 126-ФЗ (редакция ФЗ от 30 декабря 2001г. № 196-ФЗ, от 29 июня 2004 г. № 58-ФЗ.

10. ФЗ «О персональных данных» от 27 июля 2006 г. № 152-ФЗ.

11. ФЗ «Об электронной цифровой подписи» от 10 января 2002 г. № 1-ФЗ.

12. ФЗ «Об оперативно-розыскной деятельности» от 12 августа 1995 г. № 144-ФЗ.

13. ФЗ «О средствах массовой информации» от 27 декабря 1991 г. №2124-.

14. ФЗ «О связи» от 18 июня 2003 г. № 126-ФЗ.

15. ФЗ «О почтовой связи» от 17 июля 1999 г. № 176-ФЗ.

16. ФЗ «О порядке выезда из РФ и въезда в РФ» от 15 августа 1996 г. №114-ФЗ.

17. Патентный закон РФ от 23 сентября 1992 г. № 3517-1.

18. ФЗ «Об авторском праве и смежных правах» от 9 июля 1993 г. № 5352-1 (редакция ФЗ № 72-ФЗ от 20 июля 2004 г.).

19. ФЗ «О правовой охране программ для ЭВМ и баз данных» от 23 сентября 1992 г. № 3523-1 (редакция ФЗ от 24 декабря 2002 г. № 177-ФЗ, от 2 ноября 2004 г. № 127-ФЗ).

20. ФЗ «О лицензировании отдельных видов деятельности» от 8 августа 2001 г. № 128-ФЗ.

21. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Положение о Федеральной службе по техническому и экспортному контролю РФ».

22. Указ Президента Российской Федерации от 11 августа 2003 г. № 960 «Положение о Федеральной службе безопасности Российской Федерации».

23. Указ Президента РФ от 7 августа 2004 г. № 101 «Вопросы Федеральной службы охраны Российской Федерации» (редакция - Указы Президента РФ от 28 декабря 2004 г. № 1627, от 22 марта 2005 г. № 329).

24. Указ Президента Российской Федерации от 3 апреля 1995 г, № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а таи же предоставления услуг в области шифрования информации».

25. Постановление Правительства Российской Федерации от 23 сентября 2002 г. № 691 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами».

26. Постановление Правительства РФ от 15 апреля 1996 г. № 333 «Положение о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» (редакция - Постановления Правительства РФ (от 23 апреля 1996 . № 509 «О внесении дополнений в некоторые решения Правительства РФ», от 30 апреля 1997 г. № 513 и от 29 июля 1998 г. № 854).

27. Постановление Правительства Российской Федерации № 290 от 30 апреля 2002 г. «О лицензировании деятельности по технической защите конфиденциальной информации».

28. Постановление Правительства Российской Федерации от 26 января 2006 г. № 45 «Об организации лицензирования отдельных видов деятельности».

29. Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации».

7 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Умения:	
- правильно применять в повседневной деятельности порядок засекречивания и рассекречивания сведений, документов и продукции;	Экспертная оценка работ студентов с использованием интерактивных технологий.
- проводить анализ методов организационной защиты информации; - ориентироваться в организации аналитической работы по предупреждению утечки конфиденциальной информации; направлениям и методам работы с персоналом, обладающим конфиденциальной информацией.	Экспертная оценка работ студентов с использованием интерактивных технологий.
Знания:	
- назначение и структура организационной защиты информации;	Экспертная оценка работ студентов с использованием интерактивных технологий.
- о порядке допуска и доступа к конфиденциальной информации и документам; организации внутриобъектового и пропускного режимов на предприятиях; организации подготовки и проведении совещаний и заседаний по конфиденциальным вопросам; организации охраны предприятий; защиты информации при публикаторской и рекламной деятельности.	Экспертная оценка работ студентов с использованием интерактивных технологий.

КОНКРЕТИЗАЦИЯ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Знать: место и роль службы защиты информации в системе защиты информации, задачи и функции службы, структура и штаты службы информационной безопасности.	Задачи и функции службы информационной безопасности предприятия, обеспечение безопасности персонала, обеспечение защиты конфиденциальной информации, обеспечение внешней деятельности предприятия.
Уметь: применять методы организации и управления службами защиты информации	Разработать инструкции отдела службы безопасности предприятия, привести пример угрозы информационной безопасности предприятия
Владеть: методами организации и управления службами защиты информации	Для того чтобы указать должностные инструкции отдела службы безопасности необходимо придерживаться нормативным документом.
Знать: организационные основы и принципы деятельности службы, подбор, расстановка и обучение сотрудников службы, организация труда сотрудников службы, принципы, методы и технология управления службой.	Создание комплексной системы информационной безопасности выделенного объекта, разработать должностную инструкцию сотрудников службы безопасности, указать их права и обязанности, разработать план работы службы информационной безопасно по защите информации от неправомерного доступа.

ТЕХНОЛОГИИ ФОРМИРОВАНИЯ ОК

Название ОК ПК	**Технология формирования ОК (на учебных занятиях)**
ОК 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.	Технология «публичная презентация проекта» (представление содержания, выделение и иллюстрация сообщения)
ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	Технология развития критического мышления (групповое обсуждение проблемных вопросов, выполнение творческих заданий, учебная дискуссия)
ОК. 3. Принимать решения в стандартных ситуациях и нести за них ответственность.	Технология электронных образовательных ресурсов (умение ориентироваться в специальной юридической литературе – работа с нормативно-правовыми актами)
ОК. 4 Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.	Технология электронных образовательных ресурсов (работа с информационно-справочная правовая система «КОНСУЛЬТАНТ-ПЛЮС».
ОК. 5 Владеть информационной культурой, анализировать и оценивать информацию с использованием информационно-коммуникационных технологий.	Обучение коллективной мыслительной и практической работе, формирование умений и навыков социального взаимодействия и общения, навыков индивидуального и совместного принятия решений; воспитание ответственного отношения к делу, уважения к социальным ценностям и установкам коллектива и общества в целом.
ОК. 6 Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.	Технология «Анализ конкретных ситуаций» (выявление проблемы; поиск причин возникновения проблемы; анализ проблемы с использованием теоретических конструкций; анализ положительных и отрицательных последствий решения проблемы; обоснование лучшего варианта решения проблемы).

8. ЛИСТ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ, ВНЕСЕННЫХ В РАБОЧУЮ ПРОГРАММУ

№ изменения, дата внесения изменения; № страницы с изменением;	
БЫЛО	**СТАЛО**
Основание: Подпись лица внесшего изменения	

9. Оценка освоения достижений личностных результатов воспитательной работы

Оценка достижения обучающимися личностных результатов (далее – ЛР) проводиться в рамках контрольных и оценочных процедур, предусмотренных данной Программой.

Способы контроля результатов и критерии результативности реализации воспитательной работы обучающихся академического колледжа.

Вид контроля	Результат контроля
Входной контроль	диагностика способностей и интересов обучающихся (тестирование, анкетирование, социометрия, опрос).
Текущий контроль	педагогическое наблюдение в процессе проведения мероприятий, педагогический анализ творческих работ, мероприятий обучающихся, формирование и анализ портфолио обучающегося; исполнение текущей отчетности
Итоговый контроль	анализ деятельности

Комплекс критериев оценки личностных результатов обучающихся:

– демонстрация интереса к будущей профессии;

– оценка собственного продвижения, личностного развития;

– положительная динамика в организации собственной учебной деятельности по результатам самооценки, самоанализа и коррекции ее результатов;

– ответственность за результат учебной деятельности и подготовки к профессиональной деятельности;

– проявление высокопрофессиональной трудовой активности;

– участие в исследовательской и проектной работе;

– участие в конкурсах профессионального мастерства, олимпиадах по профессии, викторинах, в предметных неделях;

– соблюдение этических норм общения при взаимодействии с обучающимися, преподавателями, руководителями практик;

– конструктивное взаимодействие в учебном коллективе;

– демонстрация навыков межличностного делового общения, социального имиджа;

– готовность к общению и взаимодействию с людьми самого разного статуса, этнической, религиозной принадлежности и в многообразных обстоятельствах;

– сформированность гражданской позиции; участие в волонтерском движении;

– проявление мировоззренческих установок на готовность молодых людей к работе на благо Отечества;

– проявление правовой активности и навыков правомерного поведения, уважения к Закону;

– отсутствие фактов проявления идеологии терроризма и экстремизма среди обучающихся;

– отсутствие социальных конфликтов среди обучающихся, основанных на межличностной, межрелигиозной почве;

– участие в реализации просветительских программ, поисковых, военно-исторических, краеведческих отрядах и молодежных объединениях;

– добровольческие инициативы по поддержки инвалидов и престарелых граждан;

– проявление экологической культуры, бережного отношения к родной земле, природным богатствам России и мира;

– демонстрация умений и навыков разумного природопользования, нетерпимого отношения к действиям, приносящим вред экологии;

– демонстрация навыков здорового образа жизни и высокий уровень культуры здоровья обучающихся;

– проявление культуры потребления информации, умений и навыков пользования компьютерной техникой, навыков отбора и критического анализа информации, умения ориентироваться в информационном пространстве;

– участие в конкурсах профессионального мастерства и в командных проектах;

проявление экономической и финансовой культуры, экономической грамотности а также собственной адекватной позиции по отношению к социально-экономической действительности.