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
08 апреля 2024 г.

ОП. 02 Организационно-правовое обеспечение информационной безопасности

Рабочая программа учебной дисциплины

Для студентов специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

технический профиль

квалификация выпускника - Техник по защите информации

Краснодар, 2024

Рассмотрено
на заседании предметно цикловой комиссии
Протокол № 9 от 05 апреля 2024 г.
Председатель ПЦК Куценко А.А.
Зав отделением Борей Т.В.

Принято
педагогическим советом
Академического колледжа
Протокол № 9
от 05 апреля 2024 г.

Рабочая программа разработана на основе основной профессиональной образовательной программы среднего профессионального образования программы подготовки специалистов среднего звена, специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, 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 09.12.2016г. № 1553 Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем (Зарегистрировано в Минюсте России 26 декабря 2016 г. N 44938) технического профиля профессионального образования.

Содержание программы реализуется в процессе освоения студентами основной профессиональной образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем технического профиля (на базе среднего общего образования) в соответствии с требованиями ФГОС СПО на 1 курсе (ах) в 1 семестре (ах).

Рецензенты:

Ким Т. И./ Заместитель директора по учебно-методической работе ЧУ ПОО КТУИС г. Краснодар

Директор ООО «НТП» г. Краснодар, Поташкова Н.И.

Генеральный директор АО «Опытное конструкторское бюро «Икар» г. Краснодар,

А.Н. Качковский

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРИМЕРНОЙ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫОП.02 ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Место дисциплины в структуре примерной основной профессиональной образовательной программы:

Дисциплина *ОП.02 Организационно-правовое обеспечение информационной безопасности* входит в общепрофессиональный цикл, является дисциплиной, закладывающей базу для последующего изучения профессиональных модулей: *ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении, ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами, ПМ.03 Защита информации техническими средствами.*

1.2. Цель и планируемые результаты освоения дисциплины

Код ПК, ОК	Умения	Знания
ОК 01, ОК 02, ОК 03, ОК 04, ОК 06, ОК 9 ПК 1.4, ПК 2.1, ПК 2.4, ПК 3.2, ПК 3.5	– осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей техника по защите информации; – применять нормативные правовые акты и нормативные методические документы в области защиты информации; – контролировать соблюдение персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники; – оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты	– основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области; – правовые основы организации защиты информации, содержащей сведения, составляющие государственную тайну и информации конфиденциального характера, задачи органов защиты государственной тайны; – нормативные документы в области обеспечения защиты информации ограниченного доступа; – организацию ремонтного обслуживания аппаратуры и средств защиты информации; – принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности в организации; – правовое положение субъектов правоотношений в сфере профессиональной деятельности (включая предпринимательскую деятельность); – нормативные методические документы, регламентирующие порядок выполнения мероприятий по защите информации, обрабатываемой в автоматизированной

	информации; – защищать свои права в соответствии с трудовым законодательством	(информационной) системе; – законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.

2.СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем в часах**
Обязательная учебная нагрузка	84
в том числе:	
теоретическое обучение	48
практические занятия (если предусмотрено)	32
Самостоятельная работа[31]	4
Вариативная часть	10
Промежуточная аттестация[32]	

2.2. Тематический план и содержание учебной дисциплины «Организационно-правовое обеспечение информационной безопасности»

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов	Осваиваемые элементы компетенций
1	2	3	4
Введение	**Содержание учебного материала**	**2**	ОК 02, ОК 03, ОК 06
	Основные правовые понятия. Источники права. Основы государственного устройства РФ.	2	
Раздел 1 Правовое обеспечение информационной безопасности		**42**	
Тема 1.1 Введение в правовое обеспечение информационной безопасности	**Содержание учебного материала**	**4**	ОК 02, ОК 03, ОК 06, ОК 09
	Информационная безопасность государства. Нормативные правовые акты Российской Федерации в области информации, информационных технологий и защиты информации. Конституционные права граждан на информацию и возможности их ограничения	4	
Тема 1.2 Государственная система защиты информации в Российской Федерации, ее организационная структура и функции	**Содержание учебного материала**	**4**	ОК 02, ОК 03, ОК 06,
	Государственная система защиты информации в Российской Федерации, ее организационная структура и функции. Федеральная служба безопасности Российской Федерации, ее задачи и функции в области защиты информации и информационной безопасности. Федеральная служба по техническому и экспортному контролю, ее задачи, полномочия и права в области защиты информации	4	

Тема 1.3 Информация как объект правового регулирования	**Содержание учебного материала**	**8**	ОК 01, ОК 02, ОК 03, ОК 06, ОК 09 ПК 2.4
	Информация как объект правовых отношений. Субъекты и объекты правовых отношений в информационной сфере. Виды информации по законодательству Российской Федерации. Нормы законодательства Российской Федерации, определяющие защиту информации.	2	
	Практические занятия:	**6**	
	1. Работа с нормативными документами 2. Защита информации, содержащейся в информационных системах общего пользования		
Тема 1.4 Правовой режим защиты государственной тайны	**Содержание учебного материала**	**6**	ОК 01, ОК 02, ОК 03, ОК 06
	Государственная тайна как особый вид защищаемой информации. Законодательство Российской Федерации в области защиты государственной тайны. Основные понятия, используемые в Законе Российской Федерации «О государственной тайне», и их определения. Степени секретности сведений, составляющих государственную тайну. Отнесение сведений к государственной тайне. Засекречивание и рассекречивание. Документирование сведений, составляющих государственную тайну. Реквизиты носителей сведений, составляющих государственную тайну. Допуск к государственной тайне и доступ к сведениям, составляющим государственную тайну. Органы защиты государственной тайны в Российской Федерации. Ответственность за нарушения правового режима защиты государственной тайны	6	
Тема 1.5 Правовые	**Содержание учебного материала**	**10**	ОК 01,

режимы защиты конфиденциальной информации	Законодательство Российской Федерации в области защиты конфиденциальной информации. Виды конфиденциальной информации по законодательству Российской Федерации. Отнесение сведений к конфиденциальной информации. Нормативно-правовое содержание Федерального закона «О персональных данных». Документирование сведений конфиденциального характера. Защита конфиденциальной информации. Ответственность за нарушение режима защиты конфиденциальной информации.	4	ОК 02, ОК 03, ОК 06, ОК 09 ПК 2.4
	Практические занятия:	**6**	
	Разработка базового блока документов для обеспечения информационной безопасности ИСПДн: 1. Составление перечня ПДн, 2. Составление перечня защищаемых ресурсов ПДн, 3. Классификация ИСПДн.		
Раздел 2 Лицензирование и сертификация в области защиты информации		**24**	
Тема 2.1 Лицензирование деятельности в области защиты информации	**Содержание учебного материала**	**12**	ОК 01, ОК 02, ОК 03, ОК 09 ПК 2.4, ПК 3.2, ПК 3.5
	Основные понятия в области лицензирования и их определения. Нормативные правовые акты, регламентирующие лицензирование деятельности в области защиты информации. Виды деятельности в области защиты информации, подлежащие лицензированию. Участники лицензионных отношений в области защиты информации. Порядок получения лицензий на деятельность в области защиты информации.	6	
	Практические занятия:	**6**	
	Подготовка документов к получению лицензии		
Тема 2.2 Сертификация и аттестация по требованиям безопасности информации	**Содержание учебного материала**	**12**	ОК 1, ОК 2, ОК 3, ОК 9 ПК 2.4, ПК 3.2, ПК 3.5
	Аттестация объектов информатизации по требованиям безопасности информации. Основные понятия в области аттестации по требованиям безопасности информации и их определения. Системы сертификации средств защиты информации по требованиям безопасности информации	6	
	Практические занятия:	**6**	
	1. Подготовки документов к сертификации 2. Подготовка документов к аттестации объектов информатизации		

Раздел 3 Организационное обеспечение информационной безопасности		**16**	
Тема 3.1 Допуск лиц и сотрудников к сведениям, составляющим государственную тайну и конфиденциальную информацию	**Содержание учебного материала**	**4**	ОК 01, ОК 02, ОК 03, ОК 04, ОК 06, ПК 2.4
	Особенности подбора персонала на должности, связанные с работой с конфиденциальной информацией. Должности, составляющие с точки зрения защиты информации «группы риска».	4	
	Понятие «допуск». Формы допусков, их назначение и классификация. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления, утверждения.		
	Работа по обучению персонала, допускаемому к конфиденциальной информации		
Тема 3.2 Организация пропускного и внутриобъектового режимов	**Содержание учебного материала**	**8**	ОК 01, ОК 02, ОК 03, ОК 04, ОК 06 ПК 2.4, ПК 3.5
	1. Понятие «охрана». Организация охраны территории, зданий, помещений и персонала. Цели и задачи охраны. Объекты охраны. Виды и способы охраны.	8	
	2. Понятие пропускного режима. Цели и задачи пропускного режима. Организация пропускного режима. Основные положения инструкции об организации пропускного режима и работе бюро пропусков. Понятие пропуска. Понятие внутриобъектового режима. Общие требования внутриобъектового режима		
	Требования к помещениям, в которых ведутся работы с конфиденциальной информацией, конфиденциальные переговоры.		
Тема 3.3 Организация ремонтного обслуживания аппаратуры и средств защиты	**Содержание учебного материала**	**4**	ОК 01, ОК 02, ОК 03, ПК 1.3, ПК 2.4 ПК 3.2
	Изъятие компьютерной техники и носителей информации. Инструкция изъятия компьютерной техники. Исследование компьютерной техники и носителей информации. Оформление результатов исследования	4	
Раздел 4 Основы трудового права			
Тема 4.1	**Содержание учебного материала**	**10**	ОК 02,

Законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.	Законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.	6	ОК 03, ОК 04, ОК 06, ОК 09
	Понятие, стороны и содержание трудового договора. Виды трудовых договоров. Заключения трудового договора. Испытательный срок. Правовые гарантии в области оплаты труда.		
	Практическое занятие:	**4**	
	Составление трудового договора сотрудника службы информационной безопасности		
Промежуточная аттестация по учебной дисциплине		**2**	
Всего:		**84**	

2.4 Оценочные средства и контрольные вопросы

1. Что включает в себя организационное обеспечение информационной безопасности?
2. Какие законы и нормативно-правовые акты регулируют область информационной безопасности?
3. Какие требования к защите информации установлены законодательством вашей страны?
4. Какие органы и учреждения отвечают за контроль и надзор в области информационной безопасности?
5. Что такое политика информационной безопасности и какие элементы она включает?
6. Каким образом формируется и утверждается политика информационной безопасности в организации?
7. Какие документы являются основой для организационного обеспечения информационной безопасности?
8. Какие меры предусмотрены для обеспечения конфиденциальности информации в организации?
9. Что такое регламенты и инструкции по обеспечению информационной безопасности?
10. Каким образом проводится обучение сотрудников по вопросам информационной безопасности?
11. Какие требования к хранению и обработке информации установлены действующим законодательством?
12. Каким образом организуется контроль за соблюдением правил информационной безопасности в организации?
13. Какие меры принимаются для предотвращения утечек конфиденциальной информации?
14. Что такое процедуры реагирования на инциденты информационной безопасности и как они должны быть организованы?
15. Какие меры предусмотрены для обеспечения целостности и доступности информации в организации?
16. Что такое аудит информационной безопасности и как он проводится в организации?
17. Какие меры принимаются для защиты от несанкционированного доступа к информации?
18. Каким образом определяются роли и ответственность сотрудников по вопросам информационной безопасности?
19. Что такое система управления информационной безопасностью (СУИБ) и как она внедряется в организации?
20. Каким образом организуется мониторинг и анализ угроз информационной безопасности?
21. Какие меры принимаются для обеспечения защиты от внутренних угроз информационной безопасности?
22. Что такое сертификация систем управления информационной безопасностью и какие стандарты применяются?
23. Каким образом происходит планирование и реализация мер по обеспечению информационной безопасности?
24. Какие меры предусмотрены для защиты от кибератак и вредоносных программ?
25. Что такое документирование процессов обеспечения информационной безопасности и как это осуществляется?
26. Каким образом осуществляется управление рисками в области информационной безопасности?
27. Какие меры принимаются для обеспечения соответствия требованиям законодательства в области информационной безопасности?
28. Что такое контрольные мероприятия по обеспечению информационной безопасности и как они проводятся?
29. Каким образом осуществляется анализ эффективности мер по обеспечению информационной безопасности?
30. Какие меры предусмотрены для обеспечения защиты персональных данных согласно законодательству?

2.5 Фонд оценочных средств

1. Каковы характерные черты компьютерных вирусов?
2. Дайте определение программного вируса.
3. Какой вид вирусов наиболее распространяемый в распределенных вычислительных сетях? Почему?
4. Перечислите классификационные признаки компьютерных вирусов.
5. В чем особенности резидентных вирусов?
6. Перечислите деструктивные возможности компьютерных вирусов.
7. Поясните самошифрование и полиморфичность как свойства компьютерных вирусов.
8. Перечислите виды « вирусоподобных» программ.
9. Поясните механизм функционирования «троянской программы» (логической бомбы).
10. поясните понятия «сканирование на лету» и « сканирование по запросу».
11. Перечислите виды антивирусных программ.
12. Охарактеризуйте антивирусные сканеры.
13. В чем особенности эвристических сканеров?
14. Какие факторы определяют качество антивирусной программы?
15. Перечислите наиболее распространенные пути заражения компьютеров вирусами.
16. Перечислите основные правила защиты от компьютерных вирусов, получаемых не из вычислительных сетей.
17. Характерные черты макровируса.
18. Как проверить систему на наличие макровируса?
19. Является ли наличие скрытых листов в Excel признаком заражения макровирусом?

20. Принципом, предполагающим вложение средств в системы защиты таким образом, чтобы получить максимальную отдачу, является:
1. Принцип системности
2. Принцип гибкости управления
3. Принцип комплексности
4. Принцип разумной достаточности

21. Установите соответствие между принципами защиты информации и описаниями
Принцип защиты информации:
1. Принцип комплексности
2. Принцип разумной достаточности
3. Принцип гибкости управления и применения
4. Механизм простоты применения Описание:
A. Предполагает строить систему из разнородных средств, перекрывающих все существующие каналы реализации угрозы безопасности и не содержащих слабых мест на стыке отдельных компонентов.
B. Предполагает необходимость учета всех взаимосвязанных взаимодействий.
C. При проектировании системы защита может получиться либо избыточной либо недостаточной.
D. Вложение средств в системы защиты должно быть построено таким образом, чтобы получить максимальную отдачу.
E. Все механизмы защиты должны быть интуитивно понятны и просты в использовании.

22. Какой показатель, согласно руководящим документам ГосТехКомиссии РФ, не является показателем защищенности?
1. Маркировка документов.
2. Идентификация и аутентификация.
3. Надежное восстановление.
4. Смена пароля.

23 Что не является причиной случайных воздействий на информационную систему?
1. Отказы и сбои аппаратуры.
2. Ошибки персонала.
3. Помехи в линиях связи из-за воздействия внешней среды.
4. Подбор пароля.

24 Что является основными путями проникновения вирусов в компьютер?
1. Съемные диски.
2. Компьютерные сети.
3. Линии связи.
4. Клавиатура.

25 Какой уровень безопасности операционных систем связан с управлением доступом к ресурсам ОС?
1. Внешний уровень.
2. Сетевой уровень.
3. Системный уровень.
4. Уровень приложений.

26 Что является основополагающим документом по информационной безопасности в РФ?
1. Конституция РФ.
2. Уголовный кодекс.
3. Закон о средствах массовой информации.
4. Закон об информационной безопасности.

27 Что из перечисленного не является функцией управления криптографическими ключами?
1. Генерация.
2. Хранение.
3. Распределение.
4. Изучение.

28 Защищённостью чего характеризуется информационная безопасность?
1. Пользователя информационной системы.
2. Информации и поддерживающей ее инфраструктуры.
3. Источника информации.
4. Носителя информации.

29 Что из перечисленного является составляющей информационной безопасности?
1. Нарушение целостности информации.
2. Проверка прав доступа к информации.
3. Доступность информации;.
4. Выявление нарушителей.

30 Что является важнейшими аспектами информационной безопасности?
1. Системность, комплексность и непрерывность защиты.
2. Идентификация, аутентификация и доступность.
3. Доступность, целостность и конфиденциальность.
4. Криптография, шифрование и целостность.

31 Что из перечисленного не является идентификатором при аутентификации?
1. Пароль.
2. Особенности поведения пользователя.
3. Персональный идентификатор.
4. Секретный ключ.

32 Что используется для контроля целостности передаваемых по сетям данных?
1. Аутентификация данных.
2. Электронная цифровая подпись.
3. Аудит событий.
4. Межсетевое экранирование.

33 Что из перечисленного не является функцией управления криптографическими ключами?
1. Генерация.
2. Хранение.
3. Распределение.
4. Изучение.

34 Защищённостью чего характеризуется информационная безопасность?
1. Пользователя информационной системы.
2. Информации и поддерживающей ее инфраструктуры.
3. Источника информации.
4. Носителя информации.

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Для реализации программы учебной дисциплины должны быть предусмотрены следующие специальные помещения:

Кабинет нормативного правового обеспечения информационной безопасности 18 столов, 36 стульев, преподавательское место - 1 шт., доска учебная - 1 шт., персональный компьютер - 1 шт., многофункциональное устройство - 1 шт., мультимедийный проектор - 1 шт., проекционный экран - 1 шт., соответствующее программное обеспечение, наглядные пособия.

Оборудование лаборатории информационных технологий: рабочие места на базе вычислительной техники по одному рабочему месту на обучающегося, подключенными к локальной вычислительной сети и сети «Интернет»; программное обеспечение сетевого оборудования; мультимедийное оборудование; программное обеспечение (справочная правовая система).

3.2. Информационное обеспечение реализации программы

3.2.1. Основные печатные источники:

1.Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 357 с. — (Профессиональное образование).

3.2.2. Дополнительные печатные источники:

1. учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование).
2. учебное пособие для СПО / Е. М. Самойлова, М. В. Виноградов. — Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2023. — 135 с.
3. Организационно-правовое обеспечение информационной безопасности: учеб. Пособие для студентов вузов / под ред. А. А. Стрельцова. –М.: Изд. Центр «Академия»

3.2.3. Электронные источники:

1. Электронная юстиция http://pravoinfo.su/magistratura_chapter2.html
2. Сайт Совета Безопасности РФ http://www.scrf.gov.ru/
3. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
4. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
5. Справочно-правовая система «Консультант Плюс» www.consultant.ru
6. Справочно-правовая система «Гарант» » www.garant.ru
7. Федеральный портал «Российское образование www.edu.ru
8. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
9. Российский биометрический портал www.biometrics.ru

10. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
11. Сайт Научной электронной библиотеки www.elibrary.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения	Критерии оценки	Формы и методы оценки
Знания: – основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области; – правовые основы организации защиты информации, содержащей сведения, составляющие государственную тайну и информации конфиденциального характера, задачи органов защиты государственной тайны; – нормативные документы в области обеспечения защиты информации ограниченного доступа; – организацию ремонтного обслуживания аппаратуры и средств защиты информации; – принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности в организации; – правовое положение субъектов правоотношений в сфере профессиональной деятельности (включая предпринимательскую деятельность); – нормативные методические документы, регламентирующие порядок выполнения мероприятий по защите информации, обрабатываемой в	Оценка устных ответов обучающихся. Оценка контрольных работ.	Устное и письменное выполнение индивидуальных практических работ, решение тестовых заданий.

автоматизированной (информационной) системе; – законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.		
Умения: – осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей техника по защите информации; – применять нормативные правовые акты и нормативные методические документы в области защиты информации; – контролировать соблюдение персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники; – оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации; – защищать свои права в соответствии с трудовым законодательством;	Выполнение практических работ в соответствии с заданием	Оценка результатов выполнения практических работ. Экспертное наблюдение за выполнением работ.