Министерство образования, науки и молодежной политики Нижегородской области

Государственное бюджетное профессиональное образовательное учреждение
«НИЖЕГОРОДСКИЙ ПРОМЫШЛЕННО-ТЕХНОЛОГИЧЕКИЙ ТЕХНИКУМ»

РАБОЧАЯ ПРОГРАММА

Учебной дисциплины

ОП.19 Основы информационной безопасности в органах внутренних дел

специальность
40.02.02 «Правоохранительная деятельность»

г. Нижний Новгород
2022г.

Рабочая программа учебной дисциплины ОП.19 Основы информационной безопасности в органах внутренних дел разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности среднего профессионального образования 40.02.02 Правоохранительная деятельность, утв. Приказом Министерства образования РФ от 12 мая 2014 г. № 509.

Организация-разработчик:
ГБПОУ «Нижегородский промышленно-технологический техникум»

Разработчик:
_____/_____преподаватель ГБПОУ «НПТТ»

Рабочая программа рассмотрена и одобрена цикловой комиссией

«____»_____2022 г. Протокол №_____

Председатель цикловой комиссии _____ / _____/

СОГЛАСОВАНО:
Зам. директора по НМР _____ / _____/

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП.19 Основы информационной безопасности в органах внутренних дел

1.1. Область применения рабочей программы

Рабочая программа учебной дисциплины ОП.19 Основы информационной безопасности в органах внутренних дел является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 40.02.02 Правоохранительная деятельность.

1.2. Место учебной дисциплины в структуре основной образовательной программы: дисциплина является общепрофессиональной дисциплиной и входит в вариативную часть циклов основной профессиональной образовательной программы.

1.3. Цели и задачи учебной дисциплины – требования к результатам освоения учебной дисциплины:

Цель учебной дисциплины: заключается в формировании у обучаемых понятийного аппарата, привитии знаний основных положений теории и методологии обеспечения информационной безопасности, а обеспечить профессиональную подготовку специалистов в сфере информационной деятельности ОВД.

Задачи дисциплины:

- знакомство обучающихся с современными знаниями в области информационной безопасности;
- привитие обучающимся простейших и необходимых знаний, навыков и умений при работе с электронно-вычислительными средствами в целях обеспечения информационной безопасности;
- овладение обучающимися методами безопасного использования телекоммуникационных систем, применяемыми на практике в ходе решения служебных задач.

В результате изучения дисциплины у обучаемых должны быть сформированы основные понятия, необходимые для обеспечения информационной безопасности, выработаны навыки использования средств закрытия компьютерной информации в служебной деятельности, постановки задач, создания моделей защиты информации в информационно-телекоммуникационных сетях (ИТКС). Обучающиеся должны изучить возможности средств защиты информации в вычислительных сетях, уметь практически применять их в ходе решения оперативно-служебных задач.

В результате изучения дисциплины обучаемые должны:

иметь представление:

- о понятийном аппарате, категориях информационной безопасности и научно-практической значимости их применения в деятельности правоохранительных органов;
- о системе органов защиты информации в России;
- о системе обеспечения информационной безопасности в правоохранительных органах России.

знать:

- сущность и содержание основных понятий в сферах информационной безопасности и зашиты информации;

- основные положения Концепции национальной безопасности России и Доктрины информационной безопасности России;

- главные положения законодательства России и ведомственных нормативных правовых актов в сфере информационных отношении:

- сущность и основные каналы утечки информации на объектах информатизации ОВД;

- основные методы и способы зашиты информационных процессов в компьютерных системах:

- основные методы и способы защиты информации в телекоммуникационных системах (Интернет, ЕИТКС ОВД).

уметь:

- практически оценивать риски, связанные с ситуациями несанкционированного доступа к информации, злоумышленной модификации информации и утраты служебной информации;

- предотвращать в служебной деятельности ситуации, связанные с информационными рисками;

- формулировать проблемы для их решения специалистами служб безопасности и защиты информации;

- использовать программно-аппаратные и технические средства защиты информации;

- применять программно-аппаратные средства при аутентификации электронных документов с использованием электронной цифровой подписи.

иметь навыки:

- безопасного использования вычислительной техники при решении служебных задач;

- использования идентификации электронных документов:

- обеспечения сохранности различных носителей информации;

- самостоятельной работы с нормативной, учебно-методической и научной литературой.

Методологическими особенностями дисциплины являются ее междисциплинарный и прикладной характер.

В процессе освоения дисциплины у студентов должны формировать **общие компетенции (ОК):**

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 3. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 4. Принимать решения в стандартных и нестандартных ситуациях, в том числе ситуациях риска, и нести за них ответственность.

ОК 6. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 7. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 11. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

Процесс изучения дисциплины направлен на формирование следующих **профессиональных компетенций (ПК):**

ПК 1.2. Обеспечивать соблюдение законодательства субъектами права.

ПК 1.10. Использовать в профессиональной деятельности нормативные правовые акты и документы по обеспечению режима секретности в Российской Федерации.

ПК 1.11. Обеспечивать защиту сведений, составляющих государственную тайну, сведений конфиденциального характера и иных охраняемых законом тайн.

1.4. Личностные результаты реализации программы воспитания

Личностные результаты реализации программы воспитания *(дескрипторы)*	**Код личностных результатов реализации программы воспитания**
Осознающий себя гражданином и защитником великой страны	**ЛР 1**
Проявляющий активную гражданскую позицию, демонстрирующий приверженность принципам честности, порядочности, открытости, экономически активный и участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций	**ЛР 2**
Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих	**ЛР 3**
Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»	**ЛР 4**
Демонстрирующий приверженность к родной культуре, исторической памяти на основе любви к Родине, родному народу, малой родине, принятию традиционных ценностей многонационального народа России	**ЛР 5**
Проявляющий уважение к людям старшего поколения и готовность к участию в социальной поддержке и волонтерских движениях	**ЛР 6**
Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.	**ЛР 7**

Проявляющий и демонстрирующий уважение к представителям различных этнокультурных, социальных, конфессиональных и иных групп. Сопричастный к сохранению, преумножению и трансляции культурных традиций и ценностей многонационального российского государства	**ЛР 8**
Соблюдающий и пропагандирующий правила здорового и безопасного образа жизни, спорта; предупреждающий либо преодолевающий зависимости от алкоголя, табака, психоактивных веществ, азартных игр и т.д. Сохраняющий психологическую устойчивость в ситуативно сложных или стремительно меняющихся ситуациях	**ЛР 9**
Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой	**ЛР 10**
Проявляющий уважение к эстетическим ценностям, обладающий основами эстетической культуры	**ЛР 11**
Принимающий семейные ценности, готовый к созданию семьи и воспитанию детей; демонстрирующий неприятие насилия в семье, ухода от родительской ответственности, отказа от отношений со своими детьми и их финансового содержания	**ЛР 12**
Личностные результаты реализации программы воспитания, определенные отраслевыми требованиями к деловым качествам личности	
Демонстрирующий готовность и способность вести с другими людьми, достигать в нем взаимопонимания, находить общие цели и сотрудничать для их достижения в профессиональной деятельности	**ЛР 13**
Проявляющий сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности	**ЛР 14**
Проявляющий гражданское отношение к профессиональной деятельности как к возможности личного участия в решении общественных, государственных, общенациональных проблем	**ЛР 15**
Личностные результаты реализации программы воспитания, определенные ключевыми работодателями	
Осознанный выбор профессии и возможностей реализации собственных жизненных планов; отношение к профессиональной деятельности как возможности участия в решении личных, общественных, государственных, общенациональных проблем.	**ЛР 16**
Личностные результаты реализации программы воспитания, определенные субъектами образовательного процесса	
Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	**ЛР 17**

1.4. Количество часов на освоение рабочей программы учебной дисциплины

максимальной учебной нагрузки обучающегося – **96 часов**, в том числе,

- обязательной аудиторной учебной нагрузки обучающегося – **64 часа**;
- самостоятельной работы обучающегося – **32 часа**.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Максимальная учебная нагрузка (всего)	**96**
Обязательная аудиторная учебная нагрузка (всего)	**64**
в том числе:	
- практические занятия	**40**
Самостоятельная работа обучающегося (всего)	**32**
Промежуточная аттестация в форме ***экзамена***	

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся		Объем в часах	Уровень освоения	Личностные результаты реализации программы воспитания
1	2		3	4	5
Раздел 1. Защита информации в органах внутренних дел					**ЛР2, ЛР3, ЛР4, ЛР7, ЛР10, ЛР11, ЛР13, ЛР15**
Тема 1.1. Проблемы обеспечения информационной безопасности органов внутренних дел	**Содержание учебного материала:**				
	1	Понятие информации, информационной сферы, безопасности информации и информационной безопасности субъекта.	2	1	
		Информационная безопасность - важнейшая составляющая национальной безопасности Российской Федерации. Основные составляющие национальных интересов в информационной сфере; виды и источники угроз информационной безопасности страны. Принципы государственной политики обеспечения информационной безопасности Российской Федерации.	2		
Тема 1.2. Информационная сфера и информационная безопасность органов внутренних дел	**Содержание учебного материала:**				
	1	Важнейшие составляющие интересов в информационной сфере и основные угрозы информационной безопасности органов внутренних дел.	2	1	
		Предпосылки и актуальность обеспечения информационной безопасности органов внутренних дел. Обеспечение информационной безопасности как составляющая информационного противоборства организованной преступности			
	1	**Практические занятия:**			
		Устный опрос по теме			
		1. Понятие информации, информационной сферы, безопасности информации и информационной безопасности субъекта.	2		
		1.1. Состав организационно-правового обеспечения.			
		1.2. Основные Законы Российской Федерации по обеспечению	2		

	2 3	информационной безопасности. 2. Основные составляющие национальных интересов в информационной сфере. 2.1. Виды и источники угроз информационной безопасности страны. 2.2. Принципы государственной политики обеспечения информационной безопасности Российской Федерации. 3. Актуальность обеспечения информационной безопасности органов внутренних дел. 3.1. Нормативные документы, регламентирующие организационные мероприятий по обеспечению информационной безопасности. 3.2. Обеспечение информационной безопасности как составляющая информационного противоборства организованной преступности.	2 2 2 2	3	
Тема 1.3. Организационно-правовые основы зашиты информации в органах внутренних дел	**Содержание учебного материала:**				
	1 2	Правовые основы деятельности органов внутренних дел в сфере выявления, пресечения и раскрытия преступлений**,** в первую очередь - их оперативных подразделении. Федеральный закон «Об оперативно-розыскной деятельности». Основные угрозы информационной безопасности, возникающие в процессе деятельности оперативных подразделений органов внутренних дел.	2 2	1	
	1 2	**Практические занятия:** 1. Правовые основы деятельности органов внутренних дел в сфере выявления, пресечения и раскрытия преступлений. 1.1. Федеральные законы «Об информации, информационных технологиях и о защите информации», «Об оперативно-розыскной деятельности». 1.2. Нормативные документы МВД России, регламентирующие организационные мероприятий по обеспечению информационной безопасности 2. Основные угрозы информационной безопасности, возникающие в процессе деятельности органов внутренних дел. 2.1. Правовые основы реализации функций по добыванию, обработке и использованию оперативно-розыскной информации. 2.2. Сведения об оперативно-розыскной деятельности, подлежащие	2 2	 3	

	3	засекречиванию в системе органов внутренних дел. 2.3. Правовая защита сотрудников оперативных подразделений органов внутренних дел от негативных информационно-психологических воздействии. Решение ситуационных задач по теме.	2		
	1	**Практические занятия:** - Проведение анализа современных нормативных актов по обеспечению безопасности информации. - Разработка организационных мероприятий по обеспечению информационной безопасности в информационной системе. Разработка должностной инструкции сотрудника подразделения информационной безопасности.	2	1	
	2 3 4	**Практические занятие:** *1. Понятие и виды каналов утечки информации*. 1.1. Классификация каналов утечки информации. 1.2. Условия и факторы, способствующие утечке информации 1.3. Основные каналы утечки информации объектов информатизации ОВД *2. Основные угрозы безопасности информации*. 2.1. Каналы утечки информации. 2.2. Характеристика средств несанкционированного получения информации. 2.3. Технологии применения средств несанкционированного получения информации. *3. Основные направления инженерно-технической защиты информации*. 3.1. Способы блокирования каналов утечки информации. 3.2. Основные этапы проведения специальных проверок объектов информатизации. Решение ситуационных задач по теме.	2 2 2	3	
Тема 1.4. Сведения об оперативно-розыскной деятельности, в системе органов внутренних дел.	**Содержание учебного материала:**				
	1	Сведения об оперативно-розыскной деятельности, подлежащие засекречиванию в системе органов внутренних дел. Правовые основы реализации функций по добыванию, обработке и использованию оперативно-розыскной информации.	2 2	1	

		Обеспечение безопасности ведомственной информации, информационных ресурсов, средств и систем информатизации. Правовая защита сотрудников оперативных подразделений органов внутренних дел от негативных информационно-психологических воздействии.			
	1	**Практическое занятие:** Решение ситуационных задач по теме.	2	3	
Тема 1.5. Защита информационных процессов и информации в компьютерных системах	**Содержание учебного материала:**		**2**		
	1	Уязвимость компьютерных систем. Понятие несанкционированного доступа (НСД), Классы и виды НСД. Модели угроз и нарушителя. Понятие «идентификации пользователя». Задача идентификации пользователя. Использование идентификации в защите информационных процессов. Методы и средства зашиты данных от НСД. Понятие атрибутов доступа к файлам. Организация доступа к файлам в различных операционных системах (ОС). Защита сетевого файлового ресурса на примерах организации доступа в различных ОС. Способы фиксации фактов доступа. Журналы доступа. Выявление следов несанкционированного доступа к файлам. Понятие доступа к данным со стороны процесса; отличия от доступа со стороны пользователя. Понятие и примеры скрытого доступа. Надежность систем ограничения доступа.	2 2	1	
Тема 1.6. Аппаратные и программно-аппаратные средства криптозащиты данных.	**Содержание учебного материала:**		**4**		
	1	Аппаратные и программно-аппаратные средства криптозащиты данных. Защищаемые компоненты компьютера: отчуждаемые и неотчуждаемые. Контроль процесса начальной загрузки компьютера, взаимодействие аппаратной и программной частей. Преимущества и недостатки программных и аппаратных средств. Несанкционированное копирование программ как тип НСД. Юридические аспекты несанкционированного копирования программ. Способы защиты от копирования. Вирусы как особый класс разрушающих программных воздействий. Защита от разрушающих программных воздействий. Необходимые и	2 2	1	

		достаточные условия предотвращения разрушающего воздействия. Понятие изолированной программной среды.			
	1	**Практические занятия:** - Исследование шифров перестановки. - Исследование шифров простой замены. Исследование шифров сложной замены.	2		
	2	**Практические занятия:** Решение ситуационных задач по теме. 1. Восстановление зараженных файлов 2. Профилактика проникновения «троянских программ» 3. Настройка безопасности почтового клиента Outlook Express 4. Настройка параметров аутентификации Windows 2000 (XP) 5. Шифрующая файловая система EFS и управление сертификатами в Windows 2000 (XP)	2	3	
Тема 1.7. Защита информации в телекоммуникационных системах (Интернет, ЕИТКС ОВД)	**Содержание учебного материала:**		**4**		
	1	Угрозы безопасности современных информационно-вычислительных и телекоммуникационных систем. Классификация угроз безопасности. Методы и средства воздействия на безопасность сетей. Модели угроз и нарушителя. Сравнительный анализ методов воздействия и противодействия в сети Internet. Направления по защите от враждебных воздействий на безопасность сетей. Особенности построения защиты информации в телекоммуникационных системах. Современные технические и программные средства сетевой зашиты компьютерной информации. Использование методов стеганографии в процессе передачи информации между различными подразделениями. Идентификация электронных документов в процессе их передачи между различными подразделениями. Аутентификация электронных документов с использованием электронной цифровой подписи в процессе их передачи между различными подразделениями.	2	1	
	1	**Практическое занятие:** 1. Назначение прав пользователей произвольном управлении			

		доступом в Windows 2000 (XP) 2. Настройка параметров регистрации и аудита в Windows 2000 [XP] 3. Управление шаблонами безопасности в Windows 2000 (XP) 4. Настройка и использование межсетевого экрана в Windows 2000 (XP) 5. Создание VPN-подключения средствами Windows 2000 (XP) Решение ситуационных задач.	2	3	
	1	- Шифрование данных в стандарте DES. - Шифрование данных в ГОСТ 28147-89. Режим простой замены. - Шифрование данных в ГОСТ 28147-89. Режим гаммирования. - Шифрование данных в ГОСТ 28147-89. Режим гаммирования с обратной связью. - Шифрование данных в ГОСТ 28147-89. Режим выработки имитовставки. Программирование алгоритма шифрования данных в ГОСТ 28147-89.	2 2	1	
	2	- Создание сертификатов, удостоверяющих подлинность пользователя. Аутентификация данных. Постановка электронной цифровой подписи. Аутентификация данных.		2,3	
Самостоятельная работа обучающихся: составление презентаций, рефератов, сообщений. **Примерная тематика презентаций, рефератов, сообщений:** 1. Правовые аспекты регулирования отношений в сфере информационной безопасности. 2. Обзор Руководящих документов ФСТЭК по защите информации в АС и СВТ. 3. Перспективы использования средств идентификации и аутентификации в вычислительных сетях. 4. Зарубежный опыт организационного обеспечения защиты информации. 5. Показатели защищенности от неправомерного доступа к компьютерной информации. 6. Классификация автоматизированных систем. 7. Средства обнаружения и лечения компьютера от вредоносных программ (вирусов). 8. Аппаратные и программные средства защиты от неправомерного доступа в вычислительных сетях. 9. Порядок проведения работ по обеспечению защиты служебных локальных вычислительных сетей. 10. Методы и средства защиты информации при работе с удаленными базами данных. 11. Возможные каналы утечки, искажения и порчи информации, циркулирующей в сети. 12. Защитные преобразования, шифрование и дешифрование для обеспечения достоверности и целостности информации передаваемой по каналам связи. 13. Обеспечение информационной безопасности в телекоммуникационных системах.		**32**	3	

14. Модель угроз и принципы обеспечения безопасности программного обеспечения. 15. Подходы к защите разрабатываемых программ от автоматической генерации инструментальными средствами программных закладок. 16. Методы идентификации программ и их характеристик. 17. Обеспечение эксплуатационной безопасности программного обеспечения. 18. Способы защиты программного обеспечения от внедрения на этапе его эксплуатации и сопровождения программных закладок. 19. Основные подходы к защите программ от неправомерного копирования. 20. Сертификационные испытания программных средств. 21. Роль автоматизированных информационных систем в деятельности правоохранительных органов. 22. Современные информационные технологии, применяемые в сфере обеспечения информационной безопасности в вычислительных сетях. 23. Законодательная база борьбы с преступлениями в сфере информационных технологий. 24. Электронный документооборот и электронная цифровая подпись. 25. Государственная политика в сфере обеспечения информационной безопасности. 26. Актуальные вопросы борьбы со спамом в вычислительных сетях. 27. Методы защита персональных данных при обработке информации в вычислительных сетях. 28. Политика информационной безопасности в Российской Федерации. 29. Сравнительный анализ стандартов информационной безопасности. 30. Дискреционная модель безопасности. 31. Мандатная модель безопасности. 32. Криптографические методы защиты информации. 33. Антивирусные пакеты как средство защиты информационных систем. 34. Криптографические пакеты как средство защиты информационных систем. 35. Средства защиты электронной почты.				
Промежуточная аттестация	**Экзамен**	**-**	**-**	
Всего:		**96**	**-**	

Для характеристики уровня освоения учебного материала используются следующие обозначения:

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. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к материально-техническому обеспечению

Реализация рабочей программы учебной дисциплины требует наличие учебного кабинета.

Оборудование учебного кабинета:

Комплект учебной мебели для обучающихся для обучающихся рабочее место учителя, доска,

ПК учителя HP Pavilion TG01-1019ur MT Ryzen 5 4600G/8Gb;

ПК ученика HP Pavilion TG01-1016ur MT Ryzen 5 4600G/8Gb;

Монитор Liyama 23/8"G-MASTER G2440HSU-B1;

Монитор Liyama 27"Prolie XB2783HSU-B3;

Телевизор LG 60UN71006LB.60.Uitra HD4K;

МФУ лазерный XEROX DocuCentre SC2020, A3;

Коммутатор ZYXEL GS1900-24-EU0101F.

3.2. Информационное обеспечение обучения

Основная литература:

1. Суворова, Г. М. Основы информационной безопасности : учебное пособие для СПО / Г. М. Суворова. — Саратов : Профобразование, 2021. — 135 c. — ISBN 978-5-4488-1294-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS.

Дополнительная литература:

2. Гультяева, Т. А. Основы информационной безопасности : учебное пособие / Т. А. Гультяева. — Новосибирск : Новосибирский государственный технический университет, 2018. — 79 с. — ISBN 978-5-7782-3640-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART.

3. Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : учебное пособие / О. Р. Лапонина ; под редакцией В. А. Сухомлина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 605 c. — ISBN 978-5-4497-0684-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART.

Интернет-ресурсы:

www.fcior.edu.ru (Федеральный центр информационно-образовательных ресурсов — ФЦИОР).

www. school-collection.edu.ru (Единая коллекция цифровых образовательных ресурсов).

http://ru.iite.unesco.org/publications (Открытая электронная библиотека «ИИТО ЮНЕСКО» по ИКТ в образовании).

www.megabook.ru (Мегаэнциклопедия Кирилла и Мефодия, разделы «Наука / Математика. Кибернетика» и «Техника / Компьютеры и Интернет»).

www.ict. edu. ru (портал «Информационно-коммуникационные технологии в образовании»).

www.digital-edu.ru (Справочник образовательных ресурсов «Портал цифрового образования»).

www.window. edu. ru (Единое окно доступа к образовательным ресурсам Российской Федерации).

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения текущего контроля и промежуточной аттестации.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
В результате освоения дисциплины обучающийся должен уметь:	**Формы контроля обучения:**
- практически оценивать риски, связанные с ситуациями несанкционированного доступа к информации, злоумышленной модификации информации и утраты служебной информации; - предотвращать в служебной деятельности ситуации, связанные с информационными рисками; - формулировать проблемы для их решения специалистами служб безопасности и защиты информации; - использовать программно-аппаратные и технические средства защиты информации; - применять программно-аппаратные средства при аутентификации электронных документов с использованием электронной цифровой подписи.	Текущий контроль: устный опрос, письменное тестирование; самостоятельная работа, практические задания, активность на занятиях. Промежуточный контроль: - экзамен.
В результате освоения дисциплины обучающийся должен знать:	
- сущность и содержание основных понятий в сферах информационной безопасности и зашиты информации; - основные положения Концепции национальной безопасности России и Доктрины информационной безопасности России; - главные положения законодательства России и ведомственных нормативных правовых актов в сфере информационных отношении: - сущность и основные каналы утечки информации на объектах информатизации ОВД; - основные методы и способы зашиты информационных процессов в компьютерных системах: - основные методы и способы защиты информации в телекоммуникационных системах (Интернет, ЕИТКС ОВД).	Текущий контроль: устный опрос, письменное тестирование; самостоятельная работа, практические задания, активность на занятиях. Промежуточный контроль: - экзамен.

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся сформированность профессиональных компетенций.

Результаты обучения (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 1.2 Обеспечивать соблюдение законодательства субъектами права.	Демонстрирует правильность формирования профессиональных навыков по выявлению нарушений соблюдения законодательства Российской Федерации субъектами права; осуществляет отбор, и систематизацию законоположений, относящихся к ситуациям, нуждающимся в правовой оценке и регулировании; решает ситуации, связанные с соблюдением законодательства Российской Федерации субъектами права.	Текущий контроль в форме: - фронтального опроса; - практических занятий; - тестового задания по темам; - решение ситуационных задач по теме. Промежуточный контроль: - экзамен.
ПК 1.10. Использовать в профессиональной деятельности нормативные правовые акты и документы по обеспечению режима секретности в Российской Федерации.	Демонстрирует знание основных законов и нормативных правовых актов, регламентирующих деятельность органов внутренних дел, регламентирующих обеспечение режима секретности. Умеет правильно составлять и оформлять служебные документы, в том числе секретные, содержащие сведения ограниченного пользования.	Текущий контроль в форме: - фронтального опроса; - практических занятий; - тестового задания по темам; - решение ситуационных задач по теме. Промежуточный контроль: - экзамен.
ПК 1.11. Обеспечивать защиту сведений, составляющих государственную тайну, сведений конфиденциального характера и иных охраняемых законом тайн.	Демонстрирует знание основных законов и нормативных правовых актов, регламентирующих деятельность органов внутренних дел, регламентирующих защиту сведений составляющих государственную тайну,	Текущий контроль в форме: - фронтального опроса; - практических занятий; - тестового задания по темам; - решение ситуационных задач по теме.

	служебную тайну. Умеет правильно составлять и оформлять служебные документы, в том числе секретные, содержащие сведения ограниченного пользования; а также выполнять служебные обязанности в строгом соответствии с требованиями режима секретности.	Промежуточный контроль: - экзамен.

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

Результаты обучения (освоенные общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.	Демонстрирует устойчивый интерес к будущей профессии; владеет приемами совершенствования профессиональных знаний и профессионального опыта.	Практическое занятие. Проверка правильности выполнения практической работы. Своевременное выполнение самостоятельной работы, проверка результатов работы.
ОК 3. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	Знает наиболее эффективное обоснование выбора и наиболее актуальные методы, и способы решения профессиональных задач в области информационной безопасности; Умеет наиболее эффективно организовать свою учебно-практическую деятельность в разрешении тех или иных правовых ситуаций, при выполнении поставленных задач.	Практическое занятие. Проверка правильности выполнения практической работы. Своевременное выполнение самостоятельной работы, проверка результатов работы.
ОК 4. Принимать решения в стандартных и нестандартных ситуациях, в том числе ситуациях риска, и нести за них ответственность.	Знает теоретическое обоснование и алгоритм действий, при принятии решений в ситуациях пограничных с чрезвычайными и ситуациями риска, в том числе в области информационной	Практическое занятие. Проверка правильности выполнения практической работы. Своевременное выполнение самостоятельной работы, проверка результатов работы.

	безопасности; Умеет правильно организовать деятельность по защите информации, соотносить свои возможности и как следствие понимать всю полноту ответственности.	
ОК 6. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.	Знает систему источников права и систему нормативно-правовых актов РФ в области информационной безопасности; Умеет ориентироваться в источниках права, умеет находить нужные нормы права в системе законодательства, для разрешения правовых ситуаций в области информационной безопасности.	Практическое занятие. Проверка правильности выполнения практической работы. Своевременное выполнение самостоятельной работы, проверка результатов работы.
ОК 7. Использовать информационно-коммуникационные технологии в профессиональной деятельности.	Знает алгоритм работы с информационно-правовыми системами; Умеет демонстрировать навыки использования информационно- правовых систем (технологий) в профессиональной деятельности, а также эффективно использовать технологии защиты информации в органах внутренних дел.	Практическое занятие. Проверка правильности выполнения практической работы. Своевременное выполнение самостоятельной работы, проверка результатов работы.
ОК 11. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.	Знает значение и роль повышения квалификации сотрудников системы правоохранительных органов, в том числе в области информационной безопасности. квалификации; Умеет организовать работу по самообразованию.	Практическое занятие. Проверка правильности выполнения практической работы. Своевременное выполнение самостоятельной работы, проверка результатов работы.