МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

ДЕПАРТАМЕНТ ГОСУДАРСТВЕННОЙ СЛУЖБЫ И КАДРОВ

ПРИМЕРНАЯ РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Актуальные вопросы деятельности подразделений, специализирующихся на предотвращении, выявлении, раскрытии и расследовании преступлений, совершаемых с использованием информационно-коммуникационных технологий»

профессионально-специализированного цикла унифицированных программ профессиональной (первоначальной) подготовки по должности служащего «Полицейский»

Москва 2021

04.09.2021 21/11/14077

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

ДЕПАРТАМЕНТ ГОСУДАРСТВЕННОЙ СЛУЖБЫ И КАДРОВ

УТВЕРЖДАЮ
Начальник Департамента
государственной службы и кадров
МВД России
генерал-лейтенант внутренней службы

В.Л. Кубышко

«__» августа 2021 г.

ПРИМЕРНАЯ РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Актуальные вопросы деятельности подразделений, специализирующихся на предотвращении, выявлении, раскрытии и расследовании преступлений, совершаемых с использованием информационно-коммуникационных технологий»

профессионально-специализированного цикла унифицированных программ профессиональной (первоначальной) подготовки по должности служащего «Полицейский»

Москва 2021

Примерная рабочая программа учебной дисциплины «Актуальные вопросы деятельности подразделений, специализирующихся на предотвращении, выявлении, раскрытии и расследовании преступлений, совершаемых с использованием информационно-коммуникационных технологий» профессионально-специализированного цикла унифицированных программ профессиональной (первоначальной) подготовки по должности служащего «Полицейский». – ДГСК МВД России, 2021. – 36 с.

Примерная рабочая программа учебной дисциплины подготовлена авторским коллективом Всероссийского института повышения квалификации сотрудников МВД России.

Согласовано:

ГУЭБиПК МВД России, ГУУР МВД России, ГУНК МВД России, ГУПЭ МВД России, ГУТ МВД России, Следственный департамент МВД России, ДИТСиЗИ МВД России, УОД МВД России, БСТМ МВД России.

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

1. Место дисциплины в структуре основной профессиональной образовательной программы.

1.1. Цель изучения учебной дисциплины.

Подготовка обучающегося к правоприменительной, экспертно-консультационной, оперативно-служебной и организационно-управленческой деятельности в сфере регулирования отношений, складывающихся в процессе использования информационно-коммуникационных технологий.

1.2. Задачи учебной дисциплины:

способствовать успешному овладению обучающимся базовыми знаниями в сфере противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий;

способствовать приобретению обучающимся навыков по выявлению, предупреждению, пресечению, раскрытию и расследованию преступлений, совершаемых с использованием информационно-коммуникационных технологий;

сформировать у обучающегося компетенции, необходимые для организации взаимодействия участников уголовного судопроизводства и использования специальных знаний по соответствующим уголовным делам;

содействовать формированию у обучающегося высокого уровня правосознания и правовой культуры, обеспечивающих неукоснительное соблюдение норм действующего законодательства в сфере информационно-коммуникационных технологий.

2. Планируемые результаты освоения учебной дисциплины.

В результате освоения учебной дисциплины «Актуальные вопросы деятельности подразделений, специализирующихся на предотвращении, выявлении, раскрытии и расследовании преступлений, совершаемых с использованием информационно-коммуникационных технологий» обучающийся должен:

знать:

особенности правового регулирования общественных отношений в сфере информационно-коммуникационных технологий;

основные понятия информационной безопасности и защиты информации;

признаки составов правонарушений в сфере информационно-коммуникационных технологий;

современное состояние борьбы с преступлениями, совершаемыми с использованием информационно-коммуникационных технологий и международный опыт противодействия преступлениям в указанной сфере;

организацию профилактической работы в целях противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий;

общие положения оперативно-розыскной деятельности, как основы выявления и раскрытия преступлений, совершаемых с использованием информационно-коммуникационных технологий;

методики расследования преступлений, совершенных с использованием информационно-коммуникационных технологий;

порядок представления и использования результатов оперативно-розыскной деятельности, полученных при производстве оперативно-розыскных мероприятий в сфере информационных технологий;

процессуальный порядок и тактику производства следственных действий по уголовным делам данной категории;

технико-криминалистические средства, используемые для работы с электронными носителями информации;

уметь:

выявлять, предупреждать, пресекать и раскрывать преступления, совершаемые с использованием информационно-коммуникационных технологий;

работать с заявлениями (сообщениями) о преступлениях, совершаемых с использованием информационно-коммуникационных технологий, принимать различные процессуальные решения в пределах своих полномочий;

выдвигать версии по расследуемому преступлению, совершенному с использованием информационно-коммуникационных технологий;

профессионально мыслить в условиях конкретной следственной ситуации, принимать оптимальные решения при расследовании преступлений, совершенных с использованием информационно-коммуникационных технологий;

взаимодействовать с оперативными подразделениями, органами предварительного следствия и дознания, экспертно-криминалистическими подразделениями;

применять технико-криминалистические средства и методы раскрытия и расследования преступлений, совершенных с использованием информационно-коммуникационных технологий;

использовать тактические приемы при производстве следственных действий и проведении оперативно-розыскных мероприятий;

правильно ставить вопросы, подлежащие разрешению, при назначении судебных экспертиз и предварительных исследований электронных носителей информации, анализировать и правильно оценивать содержание заключений эксперта (специалиста);

квалифицировать преступления, совершаемые с использованием информационно-коммуникационных технологий;

владеть навыками:

организации выявления, предупреждения, пресечения, раскрытия и расследования преступлений, совершаемых с использованием информационно-коммуникационных технологий;

применения технико-криминалистических средств и методов обнаружения, фиксации и изъятия следов и вещественных доказательств;

производства следственных и иных процессуальных действий;

принятия процессуальных решений и составления процессуальных документов;

применения методики расследования преступлений, совершаемых с использованием информационно-коммуникационных технологий.

II. СОДЕРЖАТЕЛЬНЫЙ РАЗДЕЛ

2.1. Примерный учебный план

№ п/п	Наименование темы	Всего часов	В том числе:					
			Занятия лекционного типа	Занятия семинарского типа	Самостоятельная работа	промежуточная аттестация		
						Зачет	Консультация	Экзамен
1	2	3	4	5	6	7	8	9
21.10.	**Итого по дисциплине**	**178**	**68**	**62**	**38**	**2**	**2**	**6**
21.10.1.	**Общие положения противодействия преступлениям в сфере информационно-коммуникационных технологий**	**18**	**4**	**2**	**12**	**-**	**-**	**-**
21.10.1.1.	Правовое регулирование общественных отношений в сфере информации, информационных технологий и защиты информации	2	-	-	2	-	-	-
21.10.1.2.	Уголовно-правовая характеристика и квалификация преступлений, совершаемых с использованием информационно-коммуникационных технологий	4	-	2	2	-	-	-
21.10.1.3.	Криминалистическая и криминологическая характеристики преступлений, совершаемых с использованием информационно-коммуникационных технологий	4	2	-	2	-	-	-
21.10.1.4.	Современное состояние борьбы с преступлениями, совершаемыми с использованием информационно-коммуникационных технологий	2	-	-	2	-	-	-
21.10.1.5.	Организация профилактической работы по предупреждению преступлений, совершаемых с использованием информационно-коммуникационных технологий	4	2	-	2	-	-	-

1	2	3	4	5	6	7	8	9
21.10.1.6.	Международный опыт противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий	2	-	-	2	-	-	-
21.10.2.	**Оперативно-розыскная деятельность как основа выявления и раскрытия преступлений**	**48**	**26**	**8**	**14**	**-**	**-**	**-**
21.10.2.1.	Понятие и сущность оперативно-розыскной деятельности	2	2		-	-	-	-
21.10.2.2.	Задачи и принципы оперативно-розыскной деятельности	2	2	-	-	-	-	-
21.10.2.3.	Правовое регулирование оперативно-розыскной деятельности	2	2	-	-	-	-	-
21.10.2.4.	Соблюдение прав и свобод человека и гражданина при осуществлении оперативно-розыскной деятельности	4	-	2	2	-	-	-
21.10.2.5.	Государственные органы и должностные лица, осуществляющие оперативно-розыскную деятельность, их обязанности и права	4	-	2	2	-	-	-
21.10.2.6.	Лица, оказывающие конфиденциальное содействие (сотрудничество) органам внутренних дел	2	2	-	-	-	-	-
21.10.2.7.	Оперативно-розыскные мероприятия и их характеристика	6	2	2	2	-	-	-
21.10.2.8.	Оперативно-розыскные мероприятия, ограничивающие конституционные права граждан	2	2	-	-	-	-	-
21.10.2.9.	Основания и условия проведения оперативно-розыскных мероприятий	4	2	2	-	-	-	-
21.10.2.10.	Информационное обеспечение оперативно-розыскной деятельности	4	2	-	2	-	-	-
21.10.2.11.	Документирование оперативно-розыскной деятельности органов внутренних дел	2	2	-	-	-	-	-
21.10.2.12.	Использование результатов оперативно-розыскной деятельности	2	2	-	-	-	-	-

1	2	3	4	5	6	7	8	9
21.10.2.13.	Взаимодействие оперативных подразделений органов внутренних дел с другими субъектами оперативно-розыскной деятельности и иными государственными органами	4	2	-	2	-	-	-
21.10.2.14.	Взаимодействие оперативных подразделений с органами предварительного следствия и дознания	4	2	-	2	-	-	-
21.10.2.15.	Контроль и надзор за оперативно-розыскной деятельностью	4	2	-	2	-	-	-
21.10.3.	**Общие положения по расследованию преступлений, совершаемых с использованием информационно-коммуникационных технологий**	**24**	**10**	**12**	**-**	**2**	**-**	**-**
21.10.3.1.	Действия сотрудников органов внутренних дел при поступлении заявлений (сообщений) о преступлениях, совершенных с использованием информационно-коммуникационных технологий	4	2	2	-	-	-	-
21.10.3.2.	Особенности возбуждения уголовных дел по преступлениям, совершаемым с использованием информационно-коммуникационных технологий	4	2	2	-	-	-	-
21.10.3.3.	Электронный носитель информации как техническое средство, содержащее значимую для уголовного дела информацию	4	2	2	-	-	-	-
21.10.3.4.	Производство отдельных процессуальных действий по преступлениям, совершаемым с использованием информационно-коммуникационных технологий	4	2	2	-	-	-	-
21.10.3.5.	Участие специалиста при проведении отдельных оперативно-розыскных мероприятий и следственных действий по преступлениям, совершаемым с использованием информационно-коммуникационных технологий	2	2	-	-	-	-	-
21.10.3.6.	Порядок изъятия электронных носителей информации в рамках оперативно-розыскных мероприятий и следственных действий	2	-	2	-	-	-	-

1	2	3	4	5	6	7	8	9
21.10.3.7	Криминалистическое исследование электронных носителей информации, особенности подготовки и назначения судебных экспертиз по уголовным делам о преступлениях, совершаемых с использованием информационно-коммуникационных технологий	2	-	2	-	-	-	-
Зачет		**2**	-	-	-	**2**	-	-
21.10.4.	**Организация противодействия общеуголовным, экономическим и преступлениям террористической и экстремистской направленности, совершаемых с использованием информационно-коммуникационных технологий**	**30**	**10**	**16**	**4**	-	-	-
21.10.4.1.	Выявление и раскрытие преступлений общеуголовной направленности, совершаемых с использованием информационно-коммуникационных технологий	8	2	4	2	-	-	-
21.10.4.2.	Выявление, предупреждение, пресечение и раскрытие преступлений, совершаемых с использованием платежных карт	2	-	2	-	-	-	-
21.10.4.3.	Выявление и раскрытие преступлений экстремистской и террористической направленности, совершаемых с использованием информационно-коммуникационных технологий	8	2	4	2	-	-	-
21.10.4.4.	Понятие и сущность криптовалют и других виртуальных активов	4	2	2	-	-	-	-
21.10.4.5.	Порядок проведения доследственных проверок и принятия решений о возбуждении уголовных дел о преступлениях, связанных с использованием криптовалют и других виртуальных активов	4	2	2	-	-	-	-
21.10.4.6.	Квалификация преступлений, совершаемых с использованием криптовалют и других виртуальных активов	4	2	2	-	-	-	-

1	2	3	4	5	6	7	8	9
21.10.5.	**Организация противодействия преступлениям по линии незаконного оборота наркотиков, совершаемым с использованием информационно-коммуникационных технологий**	**24**	**10**	**10**	**4**	**-**	**-**	**-**
21.10.5.1.	Противодействие незаконному обороту наркотиков, совершаемому с использованием информационно-коммуникационных технологий	6	2	2	2	-	-	-
21.10.5.2.	Использование биллинговых данных при раскрытии и расследовании преступлений в сфере оборота наркотиков	4	2	2	-	-	-	-
21.10.5.3.	Тактика противодействия незаконным наркооперациям, совершаемым с использованием блокчейн-технологий	4	2	2	-	-	-	-
21.10.5.4.	Особенности раскрытия преступлений в сфере оборота наркотиков, совершаемых с использованием информационно-коммуникационных технологий	6	2	2	2	-	-	-
21.10.5.5.	Взаимодействие оперативных и экспертно-криминалистических подразделений при раскрытии и расследовании преступлений по линии незаконного оборота наркотиков, совершаемых с использованием информационно-коммуникационных технологий	4	2	2	-	-	-	-
21.10.6.	**Организация противодействия преступлениям в сфере коммуникаций и компьютерной информации**	**26**	**8**	**14**	**4**	**-**	**-**	**-**
21.10.6.1.	Особенности выявления и раскрытия преступлений в сфере коммуникаций и компьютерной информации	8	2	4	2	-	-	-
21.10.6.2.	Выявление и раскрытие преступлений, совершаемых в системе дистанционного банковского обслуживания	8	2	4	2	-	-	-
21.10.6.3.	Выявление фактов вовлечения несовершеннолетних в деструктивную деятельность посредством информационно-коммуникационных технологий	6	2	4	-	-	-	-

1	2	3	4	5	6	7	8	9
21.10.6.4.	Использование биометрических технологий и методов, способствующих раскрытию преступлений	4	2	2	-	-	-	-
Консультация перед экзаменом		2	-	-	-	-	2	-
Экзамен		**6**	-	-	-	-	-	**6**

2.2. Примерное содержание учебных разделов, тем

21.10.1. Общие положения противодействия преступлениям в сфере информационно-коммуникационных технологий

21.10.1.1. Правовое регулирование общественных отношений в сфере информации, информационных технологий и защиты информации.

Нормативные правовые акты, регулирующие общественные отношения в сфере информации, информационных технологий и защиты информации.

Цель и задачи государства в области защиты информации. Отрасли права, регламентирующие отношения, возникающие при формировании и использовании информационных ресурсов. Права и обязанности субъектов, участвующих в этих процессах. Понятие информации, информационной системы, электронного документа и других значимых категорий, закрепленных в нормативных правовых актах.

Технические и правовые аспекты Интернета как особой информационно-коммуникационной сети. Субъекты и объекты правоотношений в Интернете.

21.10.1.2. Уголовно-правовая характеристика и квалификация преступлений, совершаемых с использованием информационно-коммуникационных технологий.

Особенности уголовно-правовой квалификации преступлений, совершаемых с использованием информационно-коммуникационных технологий[1]. Содержание и соотношение понятий: «преступления в сфере компьютерной информации», «преступления, совершаемые с использованием современных информационно-коммуникационных технологий», «компьютерные преступления», «киберпреступления», «преступления в сфере информационных технологий». Понятие компьютерной информации. Компьютерная информация как объект правовых отношений. Виды охраняемой законом компьютерной информации. Юридические признаки и свойства компьютерной информации.

Состав преступлений, совершаемых с использованием ИКТ.

21.10.1.3. Криминалистическая и криминологическая характеристики преступлений, совершаемых с использованием информационно-коммуникационных технологий.

Понятие и состав криминалистической характеристики преступлений, совершаемых с использованием компьютерной информации.

Криминалистический анализ интернета как особой информационно-коммуникационной сети: субъекты, объекты, техническое и правовое регулирование.

Наиболее распространенные способы совершения преступлений с использованием сети Интернет.

Типичные следы преступлений. Механизм следообразования при

---

[1] Далее – «ИКТ».

совершении преступлений в сфере компьютерной информации.

Криминологическая характеристика лиц, совершающих преступления с использованием компьютерной информации. Характерные особенности преступных групп, осуществляющих преступную деятельность в данной сфере.

21.10.1.4. Современное состояние борьбы с преступлениями, совершаемыми с использованием информационно-коммуникационных технологий.

Структура и динамика преступлений, совершаемых в сфере ИКТ. Показатели уголовно-правовой статистики преступлений, совершаемых в сфере ИКТ. Виды и формы преступности в сфере ИКТ.

Детерминанты преступности в сфере ИКТ в России.

21.10.1.5. Организация профилактической работы по предупреждению преступлений, совершаемых с использованием информационно-коммуникационных технологий.

Правовая основа, понятие, направления профилактики. Общее, специальное и индивидуальное предупреждение преступности в сфере ИКТ. Система субъектов профилактики преступности в сфере ИКТ. Государственные и общественные институты как субъекты предупреждения преступности в сфере ИКТ. Место органов внутренних дел в системе профилактической деятельности. Полномочия органов внутренних дел по профилактике преступлений, совершаемых с использованием ИКТ.

21.10.1.6. Международный опыт противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий.

Международное сотрудничество правоохранительных органов по противодействию преступлениям, совершаемым в сфере ИКТ. Международные организации, осуществляющие противодействие преступлениям в сфере ИКТ и сотрудничества по линии Интерпола.

Зарубежный опыт противодействия преступлениям в сфере ИКТ.

21.10.2.Оперативно-розыскная деятельность как основа выявления и раскрытия преступлений

21.10.2.1. Понятие и сущность оперативно-розыскной деятельности.

Место и роль оперативно-розыскной деятельности[1] в государственной системе мер борьбы с преступностью. Социально-историческая обусловленность возникновения и объективная необходимость существования ОРД на современном этапе.

Законодательное определение ОРД как особого вида правоохранительной деятельности. Цель ОРД.

---

[1] Далее – «ОРД».

21.10.2.2. Задачи и принципы оперативно-розыскной деятельности.

Задачи ОРД, закрепленные в Федеральном законе от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»[1]. Содержание задач ОРД и их сущность.

Принципы ОРД, закрепленные в Законе об ОРД, отражающие закономерности борьбы с преступностью. Система принципов ОРД и ее взаимосвязанная структура. Общие и специальные принципы. Связь и соотношение общих и специальных принципов ОРД.

21.10.2.3. Правовое регулирование оперативно-розыскной деятельности.

Понятие, сущность и необходимость правового регулирования ОРД. Система правового регулирования ОРД. Положения Конституции Российской Федерации в основе системы правого регулирования. Общепризнанные принципы и нормы международного права в системе правого регулирования.

Федеральные законы в правовом регулировании ОРД.

Общая характеристика Закона об ОРД. Связь и соотношение норм права, регулирующих ОРД, и ведомственных нормативных актов.

21.10.2.4. Соблюдение прав и свобод человека и гражданина при осуществлении оперативно-розыскной деятельности.

Защита прав и свобод человека и гражданина – конституционный принцип ОРД. Запреты, установленные для должностных лиц, осуществляющих ОРД.

Способы обжалования нарушений прав и свобод человека и гражданина при осуществлении ОРД.

Вопросы ОРД в решениях Европейского Суда по правам человека и определениях Конституционного Суда Российской Федерации.

21.10.2.5. Государственные органы и должностные лица, осуществляющие оперативно-розыскную деятельность, их обязанности и права.

Органы, осуществляющие ОРД, их общая характеристика и специфически функции. Обязанности сотрудников оперативных подразделений и их содержание.

Задачи, компетенции и объем полномочий органов и должностных лиц, осуществляющих ОРД. Взаимосвязь прав и обязанностей органов и должностных лиц, осуществляющих ОРД.

Оперативные подразделения, уполномоченные на осуществление ОРД в системе МВД России.

---

[1] Далее – «Закон об ОРД».

21.10.2.6. Лица, оказывающие конфиденциальное содействие (сотрудничество) органам внутренних дел.

Понятие конфиденциального содействия (сотрудничества) граждан оперативным подразделениям органов внутренних дел.

Сущность, социально-правовые и морально-этические основы конфиденциального содействия (сотрудничества) граждан оперативным подразделениям органов внутренних дел, его значение в борьбе с преступностью.

Виды и формы содействия (сотрудничества) граждан органам внутренних дел. Основания и порядок привлечения граждан к конфиденциальному содействию (сотрудничеству). Основания и порядок прекращения конфиденциального содействия (сотрудничества) граждан органам внутренних дел.

21.10.2.7. Оперативно-розыскные мероприятия и их характеристика.

Понятие оперативно-розыскного мероприятия[1]. Виды и классификация ОРМ.

ОРМ, осуществляемые по инициативе сотрудников оперативных подразделений, и порядок их проведения.

ОРМ, проводимые по постановлению с разрешения руководителя органа, осуществляющего ОРД, порядок их проведения.

ОРМ, осуществляемые по судебному решению, и порядок их проведения.

21.10.2.8. Оперативно-розыскные мероприятия, ограничивающие конституционные права граждан.

Виды и характеристика ОРМ, ограничивающих конституционные права граждан. Особенности подготовки и порядок проведения ОРМ, ограничивающих конституционные права граждан. Документальное оформление результатов ОРМ, ограничивающих конституционные права граждан, их использование и хранение.

21.10.2.9. Основания и условия проведения оперативно-розыскных мероприятий.

Сущность правовых оснований проведения ОРМ, определенных Законом об ОРД. Условия проведения ОРМ.

Правовые основания и условия проведения ОРМ, ограничивающих конституционные права граждан. Особенности проведения ОРМ, ограничивающих конституционные права граждан, в случаях, не терпящих отлагательства.

Рассмотрение материалов об ограничении прав граждан при проведении ОРМ как особый вид судебной деятельности. Порядок судебного рассмотрения материалов об ограничении конституционных прав граждан при проведении ОРМ.

---

[1] Далее – «ОРМ».

21.10.2.10. Информационное обеспечение оперативно-розыскной деятельности.

Сущность, задачи и правовые основания информационного обеспечения раскрытия и расследования преступлений. Понятие информационного обеспечения ОРД, его виды и формы. Роль и значение информационных систем органов внутренних дел в решении задач борьбы с преступностью. Современные информационные поисковые системы и порядок их использования в раскрытии преступлений.

Классификация, виды и формы учетов. Возможности использования учетов в противодействии преступлениям, совершаемым с использованием ИКТ. Требования, предъявляемые к формированию учетов. Запросы на получение сведений из информационных баз данных.

21.10.2.11. Документирование оперативно-розыскной деятельности органов внутренних дел.

Правовая основа документирования оперативно-розыскной деятельности. Понятие, сущность, значение и содержание документирования.

Виды дел оперативного учета, основания и порядок их ведения.

21.10.2.12. Использование результатов оперативно-розыскной деятельности.

Понятие результатов ОРД. Основные направления использования результатов ОРД, закрепленные в Законе об ОРД.

Нормативно-правовые основания представления результатов ОРД в органы дознания, следователю или в суд.

Требования, предъявляемые к результатам ОРД, представляемым органу дознания, следователю или в суд.

Документальное оформление представления результатов ОРД.

21.10.2.13. Взаимодействие оперативных подразделений органов внутренних дел с другими субъектами оперативно-розыскной деятельности и иными государственными органами.

Нормативная основа взаимодействия. Понятие, виды и формы взаимодействия. Взаимодействие оперативных подразделений с иными службами и подразделениями органов внутренних дел.

Взаимодействие и сотрудничество оперативных подразделений с другими субъектами оперативно-розыскной деятельности, с государственными органами, уполномоченными на осуществление контрольной и надзорной деятельности в сфере ИКТ, и иными государственными органами.

Взаимодействие с подразделениями обеспечения безопасности банковских и иных финансовых подразделений, с операторами связи, провайдерами и другими организациями, оказывающими услуги в сфере ИКТ.

21.10.2.14. Взаимодействие оперативных подразделений с органами предварительного следствия и дознания.

Правовая основа совместной деятельности оперативных и следственных подразделений. Следственно-оперативные группы: понятие, виды и состав.

Деятельность сотрудников оперативных подразделений в составе следственно-оперативных групп и их полномочия, как членов следственно-оперативной группы.

21.10.2.15. Контроль и надзор за оперативно-розыскной деятельностью.

Цель, задачи и назначение контроля за ОРД. Субъекты контроля за ОРД, их права и сфера деятельности. Виды контроля за ОРД. Назначение и формы судебного контроля.

Понятие и сущность прокурорского надзора за ОРД. Предмет прокурорского надзора за ОРД. Организация и порядок его осуществления.

21.10.3. Общие положения по расследованию преступлений в сфере информационно-коммуникационных технологий

21.10.3.1. Действия сотрудников органов внутренних дел при поступлении заявлений (сообщений) о преступлениях, совершенных с использованием информационно-коммуникационных технологий.

Алгоритм действий сотрудников органов внутренних дел при поступлении заявлений (сообщений) о преступлениях, совершенных с использованием ИКТ. Порядок процессуальных и иных действий с заявителем (потерпевшим) на первоначальном этапе (перечень вопросов, которые необходимо осветить в ходе первоначального опроса; изъятие средства мобильной связи). Порядок изъятия информации, содержащей банковскую либо иную охраняемую законом тайну.

Обстоятельства, подлежащие установлению на этапе проверки заявлений (сообщений) о преступлениях, совершенных с использованием ИКТ.

21.10.3.2. Особенности возбуждения уголовных дел по преступлениям, совершаемым с использованием информационно-коммуникационных технологий.

Источники поступления сообщений о преступлениях, совершенных с использованием современных информационно-коммуникационных технологий.

Типичные поводы и основания для возбуждения уголовных дел о преступлениях, совершенных с использованием информационно-коммуникационных технологий. Обстоятельства, подлежащие установлению на стадии возбуждения уголовного дела.

Особенности планирования и создания следственно-оперативных групп по раскрытию и расследованию преступлений, совершенных с использованием ИКТ.

21.10.3.3. Электронный носитель информации как техническое средство, содержащее значимую для уголовного дела информацию.

Понятие электронного носителя информации. Технологии записи данных на электронные носители информации. Виды электронных носителей информации.

Электронные носители информации как вещественные доказательства: понятие и виды.

21.10.3.4. Производство отдельных процессуальных действий по преступлениям, совершаемым с использованием информационно-коммуникационных технологий.

Основные следственные действия, осуществляемые при расследовании преступлений, совершаемых с использованием ИКТ.

Осмотр места происшествия по рассматриваемой категории дел и этапы его проведения.

Круг субъектов, подлежащих допросу на начальном этапе расследования, и тактические особенности их допроса. Обстоятельства, подлежащие выяснению в ходе допроса различных категорий участников.

Тактика проведения обыска и выемки при расследовании преступлений в сфере компьютерной информации. Получение информации о соединениях между абонентами и (или) абонентскими устройствами.

21.10.3.5. Участие специалиста при проведении отдельных оперативно-розыскных мероприятий и следственных действий по преступлениям, совершаемым с использованием информационно-коммуникационных технологий.

Подготовка к проведению следственных действий с участием специалиста, порядок его привлечения, разъяснения прав и обязанностей. Использование специальных познаний и технических средств при проведении следственных действий по преступлениям, совершаемым с использованием ИКТ. Участие специалиста при проведении обыска (выемки) и осмотра предметов и документов.

21.10.3.6. Порядок изъятия электронных носителей информации в рамках оперативно-розыскных мероприятий и следственных действий.

Порядок изъятия электронных носителей и копирования информации, содержащейся на них в соответствии с требованиями уголовно-процессуального законодательства Российской Федерации и Закона об ОРД. Особенности изъятия различных видов электронных носителей информации.

Типичные научно-технические и технико-криминалистические средства, используемые при изъятии средств вычислительной техники и электронных носителей информации. Виды возможного противодействия изъятию электронных носителей информации и пути их пресечения.

Особенности фиксации в процессуальных документах хода и результатов изъятия электронных носителей, их упаковка, транспортировка и хранение.

21.10.3.7. Криминалистическое исследование электронных носителей информации, особенности подготовки и назначения судебных экспертиз по уголовным делам о преступлениях, совершаемых с использованием информационно-коммуникационных технологий.

Основы криминалистического исследования компьютерных устройств. Виды и задачи криминалистического исследования электронных носителей информации. Идентификационные и диагностические задачи судебных экспертиз электронных носителей. Следы совершения неправомерного доступа к компьютерной информации. Способы сокрытия следов преступлений в сфере компьютерной информации.

IP-адрес и доменная система имен в следовой картине компьютерных преступлений. MAC-адрес как уникальный идентификатор оборудования компьютерных сетей. Особенности отражения действий пользователя на сервере в лог-файлах. Меры предосторожности и обеспечения сохранности информации на электронных носителях.

Виды, понятие, цели и задачи судебных экспертиз электронных носителей информации. Подготовка материалов для назначения судебных экспертиз с целью исследования электронных носителей информации. Постановка вопросов при назначении судебных экспертиз. Заключение эксперта, его оценка и использование при расследовании преступлений.

21.10.4. Организация противодействия общеуголовным, экономическим и преступлениям террористической и экстремистской направленности, совершаемым с использованием информационно-коммуникационных технологий

21.10.4.1. Выявление и раскрытие преступлений общеуголовной направленности, совершаемых с использованием информационно-коммуникационных технологий.

Виды преступлений общеуголовной направленности, совершаемых с использованием ИКТ.

Действия сотрудников органов внутренних дел при раскрытии преступлений и расследовании уголовных дел, совершенных с использованием ИКТ в зависимости от способа хищения. Порядок и источники получения оперативно-значимой информации, способствующей установлению лица, причастного к совершенному преступлению.

21.10.4.2. Выявление, предупреждение, пресечение и раскрытие преступлений, совершаемых с использованием платежных карт.

Отдельные вопросы квалификации мошенничества с использованием платежных карт. Особенности возбуждения и расследования уголовных дел о преступлениях, связанных с мошенническими действиями, совершенными с использованием платежных карт.

Действия сотрудников органов внутренних дел по раскрытию преступлений, совершенных с использованием платежных карт на

первоначальном этапе.

21.10.4.3. Выявление и раскрытие преступлений экстремистской и террористической направленности, совершаемых с использованием информационно-коммуникационных технологий.

Виды преступлений, террористической и экстремистской направленности совершаемых с использованием ИКТ.

Уголовно-правовая и криминалистическая характеристика преступлений экстремистской и террористической направленности, совершаемых с использованием ИКТ. Выявление и документирование преступлений экстремистской и террористической направленности, совершаемых с использованием ИКТ.

Мониторинг информационных ресурсов сети Интернет.

Методы работы в сетевом информационном пространстве, направленные на противодействие преступлениям экстремистской направленности.

21.10.4.4. Понятие и сущность криптовалют и других виртуальных активов.

Понятийный аппарат электронных финансовых расчетов. Электронные средства платежа, электронные денежные средства. Безналичный денежный оборот, неперсонифицированные платежные продукты, криптовалюта и другие виртуальные активы.

Механизм эмиссии и функционирования криптовалют и других виртуальных активов, объем рынка. Майнинг, публичный блокчейн, мультиподпись, система распределенного реестра. Операторы информационных систем, криптобиржи.

Нормативно-правовое регулирование криптовалют и других виртуальных активов в Российской Федерации. Цифровые права, имущественные права. Российская ассоциация криптовалют и блокчейна.

Международный опыт нормативно-правового регулирования криптовалют и других виртуальных активов.

21.10.4.5. Порядок проведения доследственных проверок и принятия решений о возбуждении уголовных дел о преступлениях, связанных с использованием криптовалют и других виртуальных активов.

Средства и методы процессуальных проверок сообщений о преступлениях, связанных с использованием криптовалют и других виртуальных активов. Способы собирания доказательственной информации на стадии возбуждения уголовных дел о преступлениях, связанных с использованием криптовалют и других виртуальных активов. Особенности проверки и процессуального закрепления информации о преступлениях.

Организация и тактика производства проверочных действий по сообщениям о преступлениях, связанных с использованием криптовалют и других виртуальных активов. Обстоятельства, исключающие производство по уголовным делам. Основания отказов в возбуждении уголовных дел о

преступлениях, связанных с использованием криптовалют и других виртуальных активов.

21.10.4.6. Квалификация преступлений, совершаемых с использованием криптовалют и других виртуальных активов.

Квалификация мошенничеств и иных хищений криптовалют и других виртуальных активов; преступлений против собственности, совершаемых с использованием криптовалют и других виртуальных активов.

Квалификация легализации (отмывания) денежных средств или иного имущества, полученных преступным путем, с использованием криптовалют и других виртуальных активов; уголовно-правовая оценка деятельности по финансированию террористической или экстремистской деятельности с использованием криптовалют и других виртуальных активов.

21.10.5. Организация противодействия преступлениям по линии незаконного оборота наркотиков, совершаемых с использованием информационно-коммуникационных технологий

21.10.5.1. Противодействие незаконному обороту наркотиков, совершаемому с использованием информационно-коммуникационных технологий.

Субъекты деятельности по борьбе с незаконным оборотом наркотиков.

Динамика:

выявления преступлений всех видов, в том числе с использованием информационно-коммуникационных технологий, связанных с незаконным оборотом наркотиков;

выявления лиц, совершивших преступления в сфере незаконного оборота наркотиков;

выявления преступлений в сфере незаконного оборота наркотиков, совершенных группами лиц;

количества наркотиков изъятых из незаконного оборота правоохранительными органами России.

Участие органов внутренних дел в проведении ежегодных межведомственных комплексных широкомасштабных оперативно-профилактических операций.

Пресечение деятельности организованных преступных группировок, осуществлявшей поставки наркотиков в Россию с использованием сети «Интернет».

21.10.5.2. Использование биллинговых данных при раскрытии и расследовании преступлений в сфере оборота наркотиков.

Технические возможности использования биллинговых данных при раскрытии и расследовании уголовных дел, связанных с незаконным оборотом наркотиков.

Правовая база для использования в раскрытии тяжких и особо тяжких преступлений системы технических средств по обеспечению ОРМ.

Понятие и принципы функционирования базовой станции.

21.10.5.3.Тактика противодействия незаконным наркооперациям, совершаемым с использованием блокчейн-технологий.

Потоки денежных средств от наркопотребителей к организаторам.

Финансирование незаконной деятельности.

Состав преступных сообществ. Использование криптовалют в сетевом сбыте наркотиков. Использование электронных средств платежа в сетевом сбыте наркотиков.

Механизмы расчетов, наиболее часто используемые за наркотические средства и легализации доходов.

21.10.5.4. Особенности раскрытия преступлений в сфере оборота наркотиков, совершаемых с использованием информационно-коммуникационных технологий.

Уголовно-правовая и криминалистическая характеристика преступлений, совершаемых с использованием ИКТ.

Виды преступлений, совершаемых с использованием ИКТ. Современные способы их выявления и раскрытия.

Своевременное получение необходимой информации как один из основных элементов в ходе раскрытия преступлений в сфере незаконного оборота наркотиков.

21.10.5.5. Взаимодействие оперативных и экспертно-криминалистических подразделений при раскрытии и расследовании преступлений по линии незаконного оборота наркотиков, совершаемых с использованием информационно-коммуникационных технологий.

Правовые основы взаимодействия оперативных и экспертно-криминалистических подразделений при раскрытии и расследовании наркопреступлений, совершаемых с использованием ИКТ. Применение экспертно-криминалистических средств и методов при проведении отдельных видов следственных действий и ОРМ. Особенности назначения криминалистических исследований (экспертиз) при раскрытии и расследовании преступлений, совершаемых с использованием ИКТ.

Тактика назначения судебных экспертиз при расследовании преступлений, связанных с незаконным оборотом наркотиков.

21.10.6. Организация противодействия преступлениям в сфере коммуникаций и компьютерной информации

21.10.6.1. Особенности выявления и раскрытия преступлений в сфере коммуникаций и компьютерной информации.

Виды преступлений, относящихся к категории «компьютерные преступления» и совершаемых в телекоммуникационных сетях.

Основные понятия и определения, используемые в ходе раскрытия преступлений, совершаемых в информационно-телекоммуникационных сетях. Сообщение и сигнал. Модель, системы передачи сигналов. Обобщенная модель системы передачи сигналов. Телекоммуникационная система. Особенности развития телекоммуникационных систем.

Уголовно-правовая и криминалистическая характеристика преступлений, совершаемых в сфере коммуникаций и компьютерной информации. Вредоносные программы и компьютерные вирусы. Выявление и раскрытие преступлений, связанных с вредоносными компьютерными программами.

Особенности взаимодействия оперативных подразделений с подразделениями «К» при раскрытии преступлений в сфере коммуникаций и компьютерной информации.

21.10.6.2. Выявление и раскрытие преступлений, совершаемых в системе дистанционного банковского обслуживания.

Основные понятия системы дистанционного банковского обслуживания[1]. Способы совершения хищений денежных средств в системе ДБО.

Действия сотрудников органов внутренних дел по раскрытию хищений денежных средств в системе ДБО. Способы установления лица, причастного к хищению, с использованием сети Интернет. Источники получения оперативно-значимой информации о лице, причастном к совершению преступления (абонентский номер, учетные записи, электронный кошелек, банковский терминал и др.).

Профилактика хищений денежных средств в системе ДБО.

21.10.6.3. Выявление фактов вовлечения несовершеннолетних в деструктивную деятельность посредством информационно-коммуникационных технологий.

Характеристика современных тенденций вовлечения несовершеннолетних в деструктивную деятельность посредством ИКТ, включая сеть Интернет. Коллективные и индивидуальные формы вовлечения.

Меры противодействия технологиям вовлечения несовершеннолетних в деструктивную деятельность посредством ИКТ, включая сеть Интернет (классификация и содержание данных мер).

---

[1] Далее – «ДБО».

21.10.6.4. Использование биометрических технологий и методов, способствующих раскрытию преступлений.

Возможности и состав Федеральной информационной системы биометрических учетов: идентификация человека по отпечаткам или следам рук; идентификация по лицу; поиск по радужной оболочке глаза; идентификация (поиск) по голосу; поиск по изображению татуировок и их фрагментам; поиск по генетической информации.

Информационные системы биометрической идентификации, используемые органами внутренних дел в борьбе с преступностью.

2.3. Примерный перечень рекомендуемой литературы, необходимой для освоения учебной дисциплины

2.3.1. Нормативные правовые акты:

1. Конституция Российской Федерации (принята всенародным голосованием 2 декабря 1993 г.) [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

2. Окинавская Хартия глобального информационного общества от 22 июля 2000 г. [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

3. Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (Душанбе, 28 сентября 2018 г.) [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

4. Конвенция о преступности в сфере компьютерной информации (Будапешт, 23 ноября 2001 г.) [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

5. Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации относительно введения уголовной ответственности за правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных систем (Страсбург, 28 января 2003 г.) [Электронный ресурс] // Доступ из справочной правовой системы «Консультант Плюс».

6. Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

7. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

8. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

9. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

10. Федеральный закон от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

11. Федеральный закон от 17 января 1992 г. № 2202-1 «О прокуратуре Российской Федерации» [Электронный ресурс] // Доступ из справочно-правовой системы «КонсультантПлюс».

12. Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

13. Федеральный закон от 8 января 1998 г. № 3-ФЗ «О наркотических средствах и психотропных веществах» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

14. Федеральный закон от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

15. Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

16. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

17. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

18. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

19. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

20. Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

21. Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции» [Электронный ресурс] // Доступ из справочно-правовой системы «КонсультантПлюс».

22. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

23. Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

24. Указ Президента Российской Федерации от 12 апреля 2021 г. № 213 «Об утверждении основ государственной политики Российской Федерации в области международной информационной безопасности» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

25. Постановление Правительства Российской Федерации от 27 августа 2005 г. № 538 «Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

26. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

27. Постановление Пленума Верховного Суда Российской Федерации от 27 декабря 2002 г. № 29 «О судебной практике по делам о краже, грабеже и разбое» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

28. Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

29. Приказ Генпрокуратуры России от 15 февраля 2011 г. № 33 «Об организации прокурорского надзора за исполнением законов при осуществлении оперативно-розыскной деятельности» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

30. Приказ МВД России, Минюста России, МЧС России, Минфина России, Минобороны России, ФСБ России, ФСКН России, ФСО России, СВР России, ФТС России, ФМС России, ГФС России, СК России, Генпрокуратуры России от 12 февраля 2014 г. № 89дсп/ 19дсп/ 73дсп/ 1дсп/ 113дсп/ 108дсп/ 75дсп/ 93дсп/ 19дсп/ 324дсп/ 133дсп/ 63дсп/ 14дсп,/ 95дсп «Об утверждении Наставления по ведению, использованию централизованных оперативно-справочных, криминалистических и розыскных учетов органов внутренних дел Российской Федерации» // Текст документа официально опубликован не был.

31. Приказ МВД России от 17 января 2006 г. № 19 «О деятельности органов внутренних дел по предупреждению преступлений» [Электронный ресурс] // Доступ из СТРАС «Юрист».

32. Приказ МВД России от 19 июня 2012 г. № 608 «О некоторых вопросах организации оперативно-розыскной деятельности в системе МВД России» [Электронный ресурс] // Доступ из СТРАС «Юрист».

33. Приказ МВД России от 4 апреля 2013 г. № 001 «Об утверждении Наставления об основах организации и тактики оперативно-розыскной деятельности органов внутренних дел Российской Федерации» // Текст документа официально опубликован не был.

34. Приказ МВД России, Минобороны России, ФСБ России, ФСО России, ФТС России, СВР России, ФСИН России, ФСКН России, СК России от 27 сентября 2013 г. № 776/ 703/ 509/ 42/ 535/ 398/ 68 «Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд» [Электронный ресурс] // Доступ из СТРАС «Юрист».

35. Приказ МВД России от 28 мая 2014 г. № 446 «Об утверждении Перечня должностных лиц органов внутренних дел Российской Федерации, правомочных получать в кредитных организациях на основании судебных

решений справки по операциям и счетам юридических лиц и индивидуальных предпринимателей, по операциям, счетам и вкладам физических лиц» [Электронный ресурс] // Доступ из СТРАС «Юрист».

36. Приказ МВД России от 29 апреля 2015 г. № 495дсп «Об утверждении Инструкции по организации совместной оперативно-служебной деятельности подразделений органов внутренних дел Российской Федерации при раскрытии преступлений и расследовании уголовных дел» // Текст документа официально опубликован не был.

37. Приказ МВД России от 3 апреля 2018 г. № 196 «О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений» [Электронный ресурс] // Доступ из СТРАС «Юрист».

2.3.2. Основная литература:

1. Алескеров В.И., Колокольчикова О.Н. Раскрытие преступлений в сфере телекоммуникаций и компьютерной информации: учебно-практическое пособие. – Домодедово: ВИПК МВД России, 2018.

2. Алескеров В.И., Колокольчикова О.Н., Федоткин А.И. Выявление и раскрытие преступлений экстремистской направленности, совершаемых с использованием сферы телекоммуникаций и компьютерной информации: учебно-методическое пособие. – Домодедово: ВИПК МВД России, 2018.

3. Деятельность органов внутренних дел по борьбе с преступлениями, совершёнными с использованием информационных, телекоммуникационных и высоких технологий: учебное пособие [А.В. Аносов и др.]. – М.: Академия управления МВД России, 2019.

4. Использование информации, содержащейся на электронных носителях, в уголовно-процессуальном доказывании: учебное пособие / под ред. Ю.В. Гаврилина, А.В. Победкина. – М.: Академия управления МВД России, 2021.

5. Основы оперативно-розыскной деятельности: учебное пособие / под ред. М.С. Десятова. – Омск: Омская академия МВД России, 2017.

6. Теория оперативно-розыскной деятельности: учебник / под ред. К.К. Горяинова, В.С. Овчинского. – М.: Норма: ИНФРА-М, 2021.

7. Халиков А.Н. Оперативно-розыскная деятельность: учебное пособие. – М.: РИОР ИНФРА-М, 2017.

2.3.3. Дополнительная литература:

1. Авдеев В.Г. Использование результатов оперативно-розыскной деятельности в уголовном процессе: монография / В.Г. Авдеев, А.В. Герасимов. – Калининград: КФ СПбУ МВД России, 2015.

2. Актуальные вопросы информационного противоборства по результатам оценки информационной обстановки, контент анализа средства массовой информации и сети «Интернет»: аналитическая справка. – М.: ВНИИ МВД России, 2020.

3. Архипова Н.А. Использование возможностей средств сотовой связи в раскрытии и расследовании преступлений: учебное пособие / Н.А. Архипова, А.В. Шебалин, Ю.Л. Бойко. – М.: ДГСК МВД России, 2017.

4. Баркалов Ю.М. Специальные знания, используемые при исследовании компьютерной информации: учебное пособие / Ю.М. Баркалов. – Воронеж: ВИ МВД России 2017.

5. Бураева Л.А. Производство следственных действий при расследовании уголовных дел о преступлениях, совершаемых с использованием платежных карт: учебно-методическое пособие / Л.А. Бураева. – Краснодар: КрУ МВД России, 2015.

6. Быков В.М. Преступления в сфере компьютерной информации: криминологические, уголовно-правовые и криминалистические проблемы: монография / В.М. Быков, В.Н. Черкасов. – М.: Юрлитинформ, 2015.

7. Васюков В.Ф. Способы получения доказательственной информации в связи с обнаружением (возможностью обнаружения) электронных носителей: учебное пособие / В.Ф. Васюков, Б.Я. Гаврилов, А.А. Кузнецов / под общ. ред. Б.Я. Гаврилова. – М.: Проспект, 2017.

8. Вовлечение несовершеннолетних в деструктивную деятельность посредством информационно телекоммуникационных технологий, включая сеть «Интернет», современные тенденции и способы противодействия: научно-практическое пособие. – М.: ВНИИ МВД России, 2019.

9. Гайдин А.И. Особенности тактики производства следственных действий при расследовании мошенничеств с использованием мобильных средств сотовой связи: учебно-методическое пособие / А.И. Гайдин, В.А. Мещеряков, О.А. Никулина, Е.А. Пидусов. – Воронеж: Воронежский институт МВД России, 2018.

10. Гайдин А.И. Процессуальные и организационно-тактические особенности фиксации доказательственной информации, хранящейся на ресурсах сети Интернет: учебно-методическое пособие / А.И. Гайдин. – Воронеж: Воронежский институт МВД России, 2018.

11. Гилязов Р.Р. Методика организации раскрытия и расследования преступлений, связанных с телефонным мошенничеством: методические рекомендации / Р.Р. Гилязов, И.Х. Еркеев. – М.: ДГСК МВД России, 2015.

12. Грибунов О.П. Расследование преступлений в сфере компьютерной информации и высоких технологий: учебное пособие / О.П. Грибунов, М.В. Старичков. – М.: ДГСК МВД России, 2017.

13. Земцова С.И. Методика расследования незаконного сбыта синтетических наркотических средств, совершенного с использованием интернет-магазинов: учебное пособие / С.И. Земцова, О.А. Суров, П.В. Галушин. – Красноярск: СибЮИ МВД России, 2019.

14. Информатика и информационные технологии: учебное пособие / Ю.Д. Романова и др. / под ред. Ю.Д. Романовой. – М.: Эксмо, 2010.

15. Использование результатов оперативно-розыскной деятельности в уголовном процессе: учебно-методическое пособие / Т.В. Астишина, Г.П. Афонькин, А.В. Кузьмин, Е.В. Маркелова. – М.: ДГСК МВД России, 2017.

16. Киберпреступность: криминологический, уголовно-правовой, уголовно-процессуальный и криминалистический анализ / науч. ред. И.Г. Смирнова. – М.: Юрилитинформ, 2016.

17. Комментарий к Федеральному закону «Об оперативно-розыскной деятельности». С приложением решений Конституционного Суда Российской Федерации и обзоров практики Европейского Суда по правам человека / отв. ред. В.С. Овчинский. – М.: Норма: ИНФРА-М, 2018.

18. Маринин С.А. Правовые и организационно-тактические основы выявления, документирования и раскрытия преступлений, совершаемых в сфере незаконного игорного бизнеса с использованием компьютерной техники и интернета: монография / С.А. Маринин. – Нижний Новгород: Нижегородская академия МВД России, 2015.

19. Мешалкин С.Н., Горностаева И.В., Федоткин А.И. Выявление, предупреждение, раскрытие и расследование преступлений экстремистской направленности, совершаемых в сети Интернет: учебно-методическое пособие. – Домодедово: ВИПК МВД России, 2016.

20. Овчинский В.С. Криминология цифрового мира: учебник. – М.: Норма: Инфра-М, 2018.

21. Основы борьбы с киберпреступностью и кибертерроризмом: хрестоматия / сост. В.С. Овчинский. – М.: Норма, 2017.

22. Пинкевич Т.В., Смольянинов Е.С. Международный опыт противодействия преступной деятельности с использованием криптовалюты: учебно-практическое пособие. – М.: Академия управления МВД России, 2021.

23. Расследование хищений денежных средств, совершенных с использованием информационных банковских технологий: учебное пособие / Ю.В. Гаврилин, Г.З. Гаспарян. – М.: Академия управления МВД России, 2021.

24. Репин А.В. Обнаружение, фиксация и изъятие следов при расследовании преступлений в сфере незаконного оборота наркотиков: учеб. пособие / А.В. Репин, Е.В. Попельницкий, Е.Б. Мельников. – Красноярск: СибЮИ МВД России, 2018.

25. Русскевич Е.А. Уголовное право и «цифровая преступность»: проблемы и решения: монография. – М.: Инфра-М, 2020.

26. Тактика производства следственных действий при расследовании преступлений в сфере незаконного оборота наркотиков: учебное пособие / Е.Е. Космодемьянская, С.И., Земцова, М.Н. Минисламов и др. – Красноярск: СибЮИ МВД России, 2016.

27. Тактика следственных действий, направленных на отыскание, обнаружение, изъятие и исследование электронных носителей и информации на них: учебное пособие. – Омск: Омская академия МВД России, 2015.

28. Улейчик В.В. Расследование мошеннических действий, совершенных с использованием платежных карт: методические рекомендации / В.В. Улейчик, В.А. Рязанцев. – М.: ВНИИ МВД России, 2019.

29. Фирсов О.В. Правовые основы оперативно-розыскных мероприятий: учебное пособие / Фирсов О.В. – М.: Норма: ИНФРА-М, 2016.

30. Чашин А.Н. Борьба с правонарушениями в сети Интернет. – М.: Дело и сервис, 2016.

31. IT-справочник следователя / под ред. С.В. Зуева. – М.: Юрлитинформ, 2019.

2.4. Примерный перечень ресурсов информационно-телекоммуникационной сети Интернет, рекомендуемых для освоения учебной дисциплины

1. URL:http://www.consultant.ru/ – Справочная правовая система «КонсультантПлюс».

2. URL: http:\ www.stras-yrist.ru/ – Специализированная территориально распределенная автоматизированная система СТРАС «Юрист».

3. URL:http://ndki.narod.ru/Liblary – Федеральный правовой портал «Компьютерные преступления: квалификация, расследование, профилактика».

4. URL:http://www.crime-research.ru – Центр исследования компьютерной преступности.

5. URL:http://www.securitylab.ru – Сайт с материалами об обеспечении информационной безопасности.

6. URL:http://procuror.spb.ru – Журнал «КриминалистЪ».

7. URL:http://cyberleninka.ru – Электронная библиотека.

8. URL:http://kriminalisty.ru – Сообщество криминалистов и экспертов.

9. URL:http://www.iprbookshop.ru – электронно-библиотечная система IPRbooks.

10. URL:http://prilab.ru – Информационный ресурс ФГБУ «Президентская библиотека имени Б.Н. Ельцина»

2.5. Примерный перечень материально-технической базы, необходимой для осуществления образовательного процесса

1. Мультимедийное оборудование (проектор, экран, ноутбук (АРМ), колонки).

2. Аудитории для проведения учебных занятий лекционного и семинарского типа.

3. Компьютерный класс.

III. РАЗДЕЛ ОЦЕНОЧНЫХ МАТЕРИАЛОВ (ФОНД ОЦЕНОЧНЫХ СРЕДСТВ)

Примерный перечень вопросов для подготовки к экзамену

1. Правовое регулирование общественных отношений в сфере информации, информационных технологий и защиты информации. Основные понятия: информация, информационные технологии, информационные системы, информационно-телекоммуникационная сеть.
2. Современное состояние борьбы с преступлениями, совершаемыми с использованием ИКТ. Структура и динамика преступлений, совершаемых в данной сфере.
3. Организация профилактической работы по предупреждению преступлений, совершаемых с использованием ИКТ.
4. Зарубежный опыт противодействия преступлениям в сфере ИКТ.
5. Оперативно-розыскная деятельность как особый вид правоохранительной деятельности.
6. Федеральный закон «Об оперативно-розыскной деятельности» и его структура.
7. Понятие ОРД и ее сущность.
8. Задачи ОРД.
9. Принципы ОРД: понятие, система и значение.
10. Органы, осуществляющие ОРД, их значение.
11. Оперативные подразделения в системе МВД России.
12. Правовая основа ОРД.
13. Соблюдение прав и свобод человека и гражданина при осуществлении ОРД.
14. Соблюдение конституционного права на неприкосновенность жилища при осуществлении ОРД. Понятие «жилище».
15. Права органов, осуществляющих ОРД.
16. Обязанности органов, осуществляющих ОРД.
17. Порядок представления результатов ОРД органу дознания, следователю или в суд.
18. ОРМ: понятие, виды.
19. ОРМ, не требующие санкционирования и их краткая характеристика.
20. ОРМ ведомственного санкционирования и их краткая характеристика.
21. ОРМ судебного санкционирования и их краткая характеристика.
22. Общие правила оформления ОРМ и возможности использования результатов в уголовном процессе.
23. Основания проведения ОРМ, предусмотренные Законом об ОРД.
24. Условия проведения ОРМ, предусмотренные Законом об ОРД.
25. Правовые условия ограничения конституционных прав граждан.
26. Информационное обеспечение ОРД и его значение в раскрытии преступлений.
27. Понятие и сущность документирования ОРД.

28. Правовые основания взаимодействия оперативных и следственных подразделений в соответствии с уголовно-процессуальным и оперативно-розыскным законодательством.

29. Основные формы и методы взаимодействия оперативных подразделений органов внутренних дел.

30. Контроль за ОРД. Основные виды и формы.

31. Ведомственный контроль за ОРД. Основные формы и методы его осуществления.

32. Прокурорский надзор за ОРД. Правовая основа, предмет, задачи, акты прокурорского реагирования.

33. Основные задачи и направления деятельности оперативных подразделений правоохранительных органов в сфере противодействия терроризму и экстремизму.

34. Алгоритм действия сотрудников органов внутренних дел при выявлении фактов, содержащих признаки составов преступлений террористического и экстремистского характера.

35. Уголовно-правовая и криминологическая характеристика преступлений, совершаемых с использованием ИКТ.

36. Криминалистическая характеристика преступлений, совершаемых с использованием ИКТ.

37. Виды преступлений, совершаемых с использованием ИКТ.

38. Современные способы выявления преступлений, совершаемых с использованием ИКТ и их раскрытия.

39. Правовые основы взаимодействия между оперативными и экспертно-криминалистическими подразделениями при раскрытии и расследовании наркопреступлений, совершаемыми с применением ИКТ.

40. Применение экспертно-криминалистических средств и методов при проведении следственных действий и ОРМ отдельных видов.

41. Особенности назначения криминалистических исследований (экспертиз) при раскрытии и расследовании преступлений, совершаемых с применением современных ИКТ.

42. Осуществление ОРМ и следственных действий по преступлениям, связанным с неправомерным доступом к компьютерной информации.

43. Осуществление ОРМ и следственных действий по преступлениям, связанным с неправомерным использованием электронных платежных карт.

44. Понятие электронных средств платежа, электронных денежных средств, криптовалюты и других виртуальных активов.

45. Понятие майнинга, публичного блокчейна, системы распределенного реестра, криптобиржи.

46. Нормативно-правовое регулирование криптовалют и других виртуальных активов в Российской Федерации.

47. Порядок проведения и осмотра места происшествия по делам о преступлениях, совершенных с использованием ИКТ.

48. Осмотр и предварительное исследование электронных носителей информации.

49. Действия сотрудников органов внутренних дел при поступлении заявлений (сообщений) о преступлениях, совершенных с использованием ИКТ.

50. Понятие и виды компьютерных преступлений.

51. Взаимодействие следователя (дознавателя) с органом дознания и иными контролирующими органами при расследовании неправомерного доступа к компьютерной информации на первоначальном этапе.

52. Виды и особенности тактики осмотров по делам о преступлениях, совершенных с использованием ИКТ.

53. Виды мошенничеств, совершаемых с использованием сети Интернет и особенности их расследования.

54. Возможности комплексного экспертного исследования по делам о преступлениях, совершенных с использованием ИКТ.

55. Возможности судебных экспертиз при расследовании преступлений, совершенных с использованием ИКТ.

56. Действия следователя (дознавателя) по установлению и устранению причин и условий, способствующих совершению преступлений с использованием ИКТ.

57. Получение образцов для сравнительного исследования при расследовании преступлений, совершенных с использованием ИКТ.

58. Использование результатов оперативно-розыскной деятельности при расследовании преступлений, совершенных с использованием ИКТ.

59. Компьютерная информация как объект правовых отношений. Виды охраняемой законом компьютерной информации.

60. Криминалистическая характеристика неправомерного доступа к компьютерной информации.

61. Криминалистическая характеристика создания, использования и распространения вредоносных программ.

62. Обстоятельства, подлежащие установлению и доказыванию по делам о преступлениях, совершенных с использованием ИКТ.

63. Информация о преступнике, которую можно получить при осмотре места происшествия по делам о преступлениях, совершенных с использованием ИКТ.

64. Особенности возбуждения уголовного дела по материалам оперативно-розыскной деятельности о преступлениях, совершенных с использованием ИКТ.

65. Особенности доказывания при расследовании преступлений, совершенных с использованием ИКТ.

66. Особенности проведения следственных действий и ОРМ при раскрытии и расследовании сетевых компьютерных преступлений.

67. Особенности расследования краж и мошенничества, совершенных с использованием поддельных банковских карт.

68. Особенности расследования преступлений, совершенных с использованием ИКТ.

69. Особенности осмотра электронных носителей информации.

70. Тактика изъятия электронных носителей информации при производстве следственных действий и ОРМ.

71. Тактика использования помощи специалистов при производстве следственных действий ОРМ о преступлениях, совершенных с использованием ИКТ.

72. Типичные следственные ситуации и действия следователя на первоначальном этапе расследования преступлений, совершенных с использованием ИКТ.

73. Организация ОРМ по раскрытию преступлений, связанных с незаконным оборотом наркотических средств.

74. Особенности взаимодействия оперативных подразделений системы МВД России в сфере противодействия незаконному обороту наркотических средств.

75. Особенности выявления преступлений, связанных с незаконным оборотом наркотиков, совершенных с использованием ИКТ.

76. Особенности пресечения деятельности организованных преступных группировок, осуществлявшей поставки наркотиков в Россию с использованием сети «Интернет».

77. Технические возможности использования биллинговых данных при раскрытии и расследовании уголовных дел, связанных с незаконным оборотом наркотиков.

78. Использование электронных средств платежа и криптовалют в сетевом сбыте наркотиков.

79. Источники получения значимой информации о лице, причастном к совершению хищений денежных средств в системе дистанционного банковского обслуживания.

80. Возможности и состав Федеральной информационной системы биометрических учетов.