МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГЛАВНОЕ УПРАВЛЕНИЕ ПО РАБОТЕ С ЛИЧНЫМ СОСТАВОМ

ПРИМЕРНАЯ ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА

Повышение квалификации сотрудников территориальных органов МВД России, участвующих в противодействии несанкционированному доступу к базам данных банка с целью хищения денежных средств, совершенного с использованием IT-технологий

Москва 2022

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГЛАВНОЕ УПРАВЛЕНИЕ ПО РАБОТЕ С ЛИЧНЫМ СОСТАВОМ

УТВЕРЖДАЮ
Врио начальника
Главного управления по работе
с личным составом МВД России

генерал-лейтенант внутренней службы
В.Л. Кубышко

«____» июня 2022 г.

ПРИМЕРНАЯ ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА

Повышение квалификации сотрудников территориальных органов
МВД России, участвующих в противодействии несанкционированному доступу
к базам данных банка с целью хищения денежных средств, совершенного
с использованием IT-технологий

Москва 2022

Примерная дополнительная профессиональная программа «Повышение квалификации сотрудников территориальных органов МВД России, участвующих в противодействии несанкционированному доступу к базам данных банка с целью хищения денежных средств, совершенного с использованием IT-технологий». – М: ГУРЛС МВД России, 2022. – 21 с.

Примерная дополнительная профессиональная программа разработана авторским коллективом Уральского юридического института МВД России.

Рецензенты:
Санкт-Петербургский университет МВД России;
Барнаульский юридический институт МВД России;
Воронежский институт МВД России.

Согласовано:
ГУУР МВД России;
Следственный департамент МВД России;
БСТМ МВД России.

Разрешается размножать и направлять в органы, организации, подразделения МВД России в необходимом количестве.

Подлежит реализации в организациях, осуществляющих образовательную деятельность, находящихся в ведении МВД России[1] и имеющих лицензию на осуществление образовательной деятельности по дополнительным профессиональным программам.

[1] Далее – «образовательная организация».

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Нормативные правовые акты, использованные для разработки примерной дополнительной профессиональной программы «Повышение квалификации сотрудников территориальных органов МВД России, участвующих в противодействии несанкционированному доступу к базам данных банка с целью хищения денежных средств, совершенного с использованием IT-технологий»[1]:

Федеральный закон от 30 ноября 2011 г. № 342-ФЗ «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации»;

Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;

приказ Минобрнауки России от 1 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;

приказ МВД России от 23 августа 2017 г. № 816 «Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»;

приказ МВД России от 5 мая 2018 г. № 275 «Об утверждении Порядка организации подготовки кадров для замещения должностей в органах внутренних дел Российской Федерации».

1.2. Цель реализации программы

Удовлетворение образовательных и профессиональных потребностей, профессиональное развитие сотрудника органов внутренних дел Российской Федерации[2], специализирующегося на противодействии несанкционированному доступу к базам данных банка с целью хищения денежных средств, совершенного с использованием IT-технологий, обеспечение соответствия его квалификации меняющимся условиям профессиональной служебной деятельности и социальной среды.

1.3. Планируемые результаты освоения программы

Совершенствование компетенции, необходимой для профессиональной служебной деятельности и повышения профессионального уровня в рамках имеющейся квалификации сотрудника органов внутренних дел – способности решать профессиональные задачи по вопросам противодействия несанкционированному доступу к базам данных банка с целью хищения денежных средств, совершенного с использованием IT-технологий.

В результате повышения квалификации обучающийся должен:

Знать:

современные виды киберугроз, направленных на несанкционированный

---

[1] Далее – «программа».

[2] Далее – «органов внутренних дел».

доступ к базам данных банка с целью хищения денежных средств;

методы совершения киберпреступлений, в том числе способы совершения кибератак на средства хранения, обработки и передачи данных;

технические средства и методы противодействия несанкционированному доступу к базам данных банка с целью хищения денежных средств, совершенного с использованием IT-технологий;

особенности уголовно-правового противодействия преступлениям, связанным с несанкционированным доступом к базам данных банка с целью хищения денежных средств, совершенного с использованием IT-технологий;

уголовно-процессуальные и организационно-тактические особенности проведения следственных действий по делам о преступлениях, связанных с несанкционированным доступом к базам данных банка с целью хищения денежных средств, совершенного с использованием IT-технологий;

особенности организации оперативно-розыскной деятельности по раскрытию преступлений указанной категории.

Уметь:

устанавливать способы несанкционированного доступа к базам данных банка с целью хищения денежных средств, совершенного с использованием IT-технологий;

правильно квалифицировать действия, содержащие признаки несанкционированного доступа к базам данных банка с целью хищения денежных средств, совершенного с использованием IT-технологий;

осуществлять необходимые следственные действия, оперативно-розыскные мероприятия и организовывать процесс расследования преступлений, связанных несанкционированным доступом к базам данных банка с целью хищения денежных средств, совершенного с использованием IT-технологий;

документировать обстоятельства совершения противоправных действий и ход расследования преступлений, связанных несанкционированным доступом к базам данных банка с целью хищения денежных средств, совершенного с использованием IT-технологий;

осуществлять взаимодействие подразделений, в том числе и в рамках международного сотрудничества, при расследовании преступлений, связанных с несанкционированным доступом к базам данных банка с целью хищения денежных средств, совершенного с использованием IT-технологий;

использовать специальные знания при расследовании преступлений, связанных с несанкционированным доступом к базам данных банка с целью хищения денежных средств, совершенного с использованием IT-технологий.

Владеть навыками:

определения способов совершения преступлений, связанных с несанкционированным доступом к базам данных банка с целью хищения денежных средств, совершенного с использованием IT-технологий;

оценки доказательств, достаточных для квалификации преступлений, связанных с несанкционированным доступом к базам данных банка с целью хищения денежных средств, совершенного с использованием IT-технологий;

определения юридических и фактических оснований для производства следственных и иных процессуальных действий, необходимых для получения доказательств по преступлениям, связанным с несанкционированным доступом к базам данных банка с целью хищения денежных средств, совершенного с использованием IT-технологий;

организации взаимодействия, в том числе и в рамках международного сотрудничества, при расследовании преступлений, связанных с несанкционированным доступом к базам данных банка с целью хищения денежных средств, совершенного с использованием IT-технологий;

использования специальных знаний при производстве следственных и процессуальных действий, оформлению и составлению процессуальных и организационно-распорядительных документов при расследовании преступлений, связанных с несанкционированным доступом к базам данных банка с целью хищения денежных средств, совершенного с использованием IT-технологий.

1.4. Нормативный срок освоения программы

Нормативный срок освоения программы – 8 учебных дней по очной форме обучения.

При применении дистанционных образовательных технологий[1] нормативный срок освоения программы увеличивается. Конкретный срок освоения программы определяется образовательной организацией самостоятельно в соответствии с трудоемкостью программы.

1.5. Трудоемкость программы

Трудоемкость программы в соответствии с примерным учебным планом и примерным календарным учебным графиком составляет 50 академических часов вне зависимости от формы обучения, а также применяемых образовательных технологий.

Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

Максимальный объем учебной нагрузки обучающегося при реализации:

по очной форме обучения – не более 54 академических часов в учебную неделю[2], включая все виды аудиторной и внеаудиторной (самостоятельной) учебной работы по ее освоению (объем аудиторной учебной нагрузки обучающегося в учебную неделю не более 46 академических часов, исключая самостоятельную работу);

с частичным применением ДОТ в дистанционный период – не более 6 академических часов контактной работы[3] в учебную неделю, в учебный период на базе образовательной организации – не более 54 академических

---

[1] Далее – «ДОТ».

[2] Учебная неделя включает в себя шесть учебных дней.

[3] Контактная работа может быть аудиторной, внеаудиторной, а также проводиться в электронной информационно-образовательной среде. Включает в себя: занятия лекционного и (или) семинарского типов и (или) групповые консультации, и (или) индивидуальную работу обучающегося и преподавателя. Количество часов самостоятельной работы обучающегося определяется образовательной организацией самостоятельно.

часов в учебную неделю, включая все виды аудиторной и внеаудиторной (самостоятельной) учебной работы по ее освоению (объем аудиторной учебной нагрузки обучающегося в учебную неделю не более 46 академических часов, исключая самостоятельную работу);

с применением исключительно ДОТ – не более 6 академических часов контактной работы в учебную неделю.

2. ПРИМЕРНЫЕ ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ

2.1. Примерные требования к условиям реализации программы

Обучение по программе может осуществляться по очной форме, с применением ДОТ.

К освоению программы допускается лицо:

имеющее среднее профессиональное и (или) высшее образование;

получающее среднее профессиональное и (или) высшее образование.

Образовательная деятельность по программе осуществляется на государственном языке Российской Федерации.

При формировании образовательной программы образовательная организация имеет право:

изменять соотношение реализации объемов учебных тем в календарном учебном графике между учебными неделями (учебными днями) в пределах максимального объема аудиторной учебной нагрузки обучающегося;

определять последовательность изучения учебных тем;

изменять соотношение занятий лекционного и семинарского типов в пределах 10% (до 50% для программ, реализуемых с применением ДОТ) от объема учебных тем;

вносить мотивированные изменения в формулировки отдельных учебных тем, перераспределять учебное время между отдельными учебными темами и по видам занятий в пределах трудоемкости, определенной программой для учебной темы;

дополнять содержание учебной темы с учетом изменений в нормативном правовом регулировании, задачах и функциях органов внутренних дел Российской Федерации и особенностей складывающейся оперативной обстановки по месту дислокации;

определять форму и виды занятий семинарского типа.

При формировании и реализации программы образовательная организация обязана:

обеспечить эффективную самостоятельную работу обучающегося в сочетании с совершенствованием управления ею со стороны педагогических работников и учебно-вспомогательного персонала;

способствовать развитию воспитательного компонента образовательного процесса.

При организации образовательного процесса образовательная организация может применять сетевую форму реализации программы в порядке, установленном законодательством Российской Федерации.

Образовательная деятельность обучающегося по программе может предусматривать следующие виды учебных занятий: занятия лекционного типа; занятия семинарского типа (практические занятия, тактические (тактико-специальные) занятия (учения), практикумы, «круглые столы», деловые игры, выездные занятия в органы, организации, подразделения МВД России); групповые консультации и учебные работы, определенные примерным учебным планом программы, учебным планом образовательной программы образовательной организации.

С целью формирования и развития у обучающегося профессиональных умений и навыков реализация компетентностного подхода должна предусматривать широкое использование в образовательной деятельности образовательной организации активных и интерактивных форм проведения занятий (деловых и ролевых игр, компьютерных симуляций, анализа служебных ситуаций, тренингов) в сочетании с внеаудиторной работой.

В рамках аудиторных занятий могут быть предусмотрены встречи с представителями органов, организаций, подразделений МВД России, правоохранительных органов, государственных и общественных организаций.

Ответственность за реализацию программы в полном объеме в соответствии с примерным учебным планом, качество подготовки обучающегося несет образовательная организация.

2.2. Особенности порядка реализации программы с применением дистанционных образовательных технологий

Образовательная организация вправе осуществлять реализацию программы или ее частей с применением ДОТ.

При организации образовательной деятельности с применением ДОТ используется электронная информационно-образовательная среда[1], к которой предоставляется открытый доступ через информационно-телекоммуникационную сеть Интернет.

ЭИОС включает в себя электронные информационные ресурсы, электронные образовательные ресурсы, совокупность информационных технологий, телекоммуникационных технологий, соответствующих технологических средств, обеспечивающих освоение обучающимися программы в полном объеме независимо от его места нахождения.

При частичном применении ДОТ самостоятельное изучение программы сочетается с аудиторными занятиями, которые проводятся после прибытия обучающегося в образовательную организацию, включая итоговую аттестацию.

При применении исключительно ДОТ обучающийся изучает весь объем программы без отрыва от выполнения служебных (должностных) обязанностей по замещаемой должности.

---

[1] Далее – «ЭИОС».

2.3. Кадровое обеспечение реализации программы

Реализация программы обеспечивается педагогическими работниками и учебно-вспомогательным персоналом образовательной организации, а также лицами, привлекаемыми к реализации программы на условиях гражданско-правового договора.

Педагогическую деятельность по программе должны осуществлять лица, имеющие высшее образование и отвечающие квалификационным требованиям, указанным в квалификационных справочниках, и (или) профессиональным стандартам, а также прошедшие обучение по дополнительным профессиональным программам, в том числе не реже 1 раза в 3 года частично или полностью в форме стажировки в органах, организациях, подразделениях МВД России, а также в иных государственных органах и государственных организациях.

2.4. Примерное информационно-методическое обеспечение образовательного процесса при реализации программы

Учебно-материальная база образовательной организации должна соответствовать санитарно-гигиеническим и пожарно-техническим нормам, обеспечивать проведение всех видов теоретической и практической подготовки обучающегося, предусмотренных примерным учебным планом программы.

Обучающийся в образовательной организации должен обеспечиваться доступом к образовательной программе и методическим материалам образовательной организации, разработкам по ней, расписанию учебных занятий, к современным профессиональным базам данных, информационно-справочным и поисковым системам.

2.4.1. Библиотечно-информационное обеспечение образовательного процесса

Обучающемуся по программе должна быть предоставлена возможность пользоваться фондами библиотек образовательной организации, включая читальные залы, абонементы учебной, методической, научной, художественной литературы, информационно-библиотечные центры.

Библиотека(и) образовательной организации должна(ы) соответствовать требованиям Положения о порядке организации работы библиотек органов внутренних дел Российской Федерации, утвержденного приказом МВД России от 24 декабря 2008 г. № 1146, и Порядка организации работы по комплектованию библиотечного фонда образовательных организаций МВД России, утвержденного приказом МВД России от 14 октября 2019 г. № 703.

Кроме того, для обучающегося по программе должен быть организован доступ к полнотекстовым ресурсам электронно-библиотечной системы – электронной библиотеке с возможностью неограниченного доступа к изданиям по юридическим дисциплинам, общественным и гуманитарным наукам.

2.4.2. Информационно-справочные и поисковые системы

Для подготовки обучающегося к занятиям в образовательной организации должен быть оборудован доступ к сети Интернет, ИМТС МВД России и к сервисам Единой системы информационно-аналитического обеспечения деятельности МВД России, установлены автоматизированные рабочие места с возможностью доступа к справочной правовой системе и специализированной территориально распределенной автоматизированной системе «Юрист».

2.4.3. Программное обеспечение

Для обучающегося по программе и педагогических работников должны быть доступны:

операционные системы Astra Linux Special Edition и (или) Microsoft Windows;

пакеты офисных программ LibreOffice, Мой офис и (или) Microsoft Windows;

специализированное программное обеспечение, необходимое для реализации образовательной программы[1].

2.5. Примерные материально-технические условия реализации программы

В образовательной организации должен быть оборудован следующий специализированный аудиторный фонд[2]:

учебные аудитории, оборудованные техническими средствами с возможностью проведения занятий с применением дистанционных образовательных технологий (в случае применения ДОТ);

кабинеты: криминалистики; специальной техники;

специальные классы: информационных технологий (компьютерный класс).

---

[1] Перечень специализированного программного обеспечения определяется образовательной организацией самостоятельно исходя из особенностей реализации программы.

[2] Перечень специализированного аудиторного фонда определяется образовательной организацией самостоятельно исходя из особенностей реализации программы.

3. СОДЕРЖАНИЕ ПРОГРАММЫ

3.1. Примерный учебный план[1]

№ п/п	Наименование учебных тем	Всего часов	Из них:		Форма контроля
			Занятия лекционного типа	Занятия семинарского типа	
1.	Современные виды киберугроз, направленных на несанкционированный доступ к базам данных банка	4	4	-	-
2.	Вопросы квалификации преступлений, связанных с несанкционированным доступом к базам данных банка с целью хищения денежных средств, совершенного с использованием IT-технологий	8	4	4	-
Промежуточная аттестация		2	-	-	2
3.	Оперативно-розыскные мероприятия, проводимые в целях выявления преступлений, связанных с хищением денежных средств, совершенных с использованием IT-технологий путем несанкционированного доступа к базам данных банка	4	2	2	-
4.	Технические средства и системы связи органов внутренних дел Российской Федерации, используемые для установления лиц, причастных к хищению денежных средств, совершенных путем несанкционированного доступа к базам данных банка	4	2	2	-
5.	Особенности раскрытия и расследования преступлений, связанных с хищением денежных средств путем несанкционированного доступа к базам данных банка, совершенных с использованием IT-технологий	8	4	4	-
6.	Процессуальный порядок и технические особенности поиска, обнаружения, фиксации и изъятия электронно-цифровых следов при расследовании хищений денежных средств, совершенных путем несанкционированного доступа к базам данных банка	6	4	2	-
7.	Организация взаимодействия при расследовании дел о хищениях денежных средств, совершенных путем несанкционированного доступа к базам данных банка с использованием IT-технологий	6	4	2	-
Консультация перед итоговой аттестацией		2	-	-	2
Итоговая аттестация		6	-	-	6
Итого:		**50**	**24**	**16**	**10**

[1] При формировании образовательной программы с применением ДОТ образовательная организация самостоятельно определяет занятия, проводимые посредством ДОТ.

3.2. Примерный календарный учебный график

Вид учебного занятия / Учебный день	1	2	3	4	5	6	7	8
Занятия лекционного типа	6	2	4	4	2	4	2	-
Занятия семинарского типа	-	4	2	2	4	2	2	-
Промежуточная аттестация	-	-	2	-	-	-	-	-
Консультация перед итоговой аттестацией	-	-	-	-	-	-	2	-
Итоговая аттестация	-	-	-	-	-	-	-	6
Всего	**6**	**6**	**8**	**6**	**6**	**6**	**6**	**6**

3.3. Примерная рабочая программа учебных тем

Тема 1. Современные виды киберугроз, направленных на несанкционированный доступ к базам данных банка.

Современные киберугрозы. Методы совершения киберпреступлений. Уязвимости интернета вещей. Обеспечение кибербезопасности оконечных устройств (сетевые камеры видеонаблюдения, сетевые контроллеры, компьютеры, серверы, ноутбуки, смартфоны). Способы совершения кибератак на средства хранения, обработки и передачи данных. Банки и базы данных. Конфиденциальность информации. Доступность информации. Целостность информации. Несанкционированный доступ и модель нарушителя. Технический канал утечки информации. Виды технических каналов утечки информации. Угроза безопасности информации.

Тема 2. Вопросы квалификации преступлений, связанных с несанкционированным доступом к базам данных банка с целью хищения денежных средств, совершенного с использованием IT-технологий.

Виды преступлений против собственности, совершаемых с использованием IT-технологий.

Особенности квалификации кражи, совершенной с банковского счета, а равно в отношении электронных денежных средств.

Особенности квалификации мошенничества с использованием электронных средств платежа. Отличие мошенничества с использованием электронных средств платежа от кражи, совершенной с банковского счета, а равно в отношении электронных денежных средств.

Особенности квалификации мошенничества в сфере компьютерной информации. Отличие мошенничества в сфере компьютерной информации от смежных составов преступлений.

Особенности квалификации неправомерного доступа к компьютерной информации.

Особенности квалификации создания, использования и распространения вредоносных компьютерных программ.

Особенности квалификации нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации

и информационно-телекоммуникационных сетей.

Особенности квалификации неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации.

Тема 3. Оперативно-розыскные мероприятия, проводимые в целях выявления преступлений, связанных с хищением денежных средств, совершенных с использованием IT-технологий путем несанкционированного доступа к базам данных банка.

Понятие и сущность оперативно-розыскных мероприятий. Сущность и содержание снятия информации с технических каналов связи и получения компьютерной информации.

Оперативно-розыскная характеристика преступлений, связанных с хищением денежных средств, совершенных с использованием IT-технологий путем несанкционированного доступа к базам данных банка. Цифровые платформы оперативно-розыскного противодействия информационно-телекоммуникационной преступности.

Тема 4. Технические средства и системы связи органов внутренних дел Российской Федерации, используемые для установления лиц, причастных к хищению денежных средств, совершенных путем несанкционированного доступа к базам данных банка.

Оперативно-розыскное обеспечение коллективной безопасности в условиях информационного общества. Цифровое обеспечение организации работы оперативных подразделений. Технический контроль оперативными подразделениями несанкционированного доступа к базам данных банков.

Розыскная и идентификационная деятельность оперативных подразделений в условиях цифровизации общества. Использование IT-технологий и билинговой информации для установления лиц, причастных к хищению денежных средств, совершенных путем несанкционированного доступа к базам данных банка.

Информационно-аналитическое обеспечение оперативно-розыскной деятельности органов внутренних дел Российской Федерации.

Тема 5. Особенности раскрытия и расследования преступлений, связанных с хищением денежных средств путем несанкционированного доступа к базам данных банка, совершенных с использованием IT-технологий.

Общая характеристика предмета и пределов доказывания при производстве по уголовным делам о хищениях денежных средств, совершенных с использованием IT-технологий путем несанкционированного доступа к базам данных банка.

Криминалистическая характеристика преступлений, связанных с хищением денежных средств путем несанкционированного доступа к базам данных банка, совершенных с использованием IT-технологий. Криминалистически значимая информация о способе совершаемых

преступлений с использованием информационно-телекоммуникационных технологий. Личность преступника и его связь с потерпевшим. Механизм следообразования.

Установление события хищения денежных средств, совершенных с использованием IT-технологий путем несанкционированного доступа к базам данных банка.

Организационно-тактические особенности проведения отдельных следственных действий при расследовании преступлений, связанных с хищением денежных средств путем несанкционированного доступа к базам данных банка, совершенных с использованием IT-технологий. Тактика назначения и производства судебных экспертиз.

Значение заключений и показаний эксперта, специалиста в установлении обстоятельств, имеющих значение при расследовании уголовных дел о хищениях денежных средств, совершенных с использованием IT-технологий путем несанкционированного доступа к базам данных банка.

Значение информации о вкладах и счетах граждан в банках и иных кредитных организациях в установлении обстоятельств, имеющих значение при расследовании уголовных дел о хищениях денежных средств, совершенных с использованием IT-технологий путем несанкционированного доступа к базам данных банка.

Тема 6. Процессуальный порядок и технические особенности поиска, обнаружения, фиксации и изъятия электронно-цифровых следов при расследовании хищений денежных средств, совершенных путем несанкционированного доступа к базам данных банка.

Понятие электронной информации в уголовно-процессуальном доказывании.

Электронные носители информации в уголовно-процессуальном доказывании: понятие, значение, особенности хранения.

Участие специалиста в следственных и иных процессуальных действиях, направленных на обнаружение и изъятие электронных носителей информации, копирование данных и фиксацию доказательственной информации на сетевых ресурсах. Особенности проведения криминалистических исследований электронных носителей информации, компьютерной техники и иных видов цифровых следов при расследовании хищений денежных средств, совершенных путем несанкционированного доступа к базам данных банка.

Основы экспертного исследования компьютеров и мобильных устройств. Уровни извлечения данных из компьютеров и мобильных устройств (ручное извлечение данных, извлечение данных на логическом уровне, извлечение данных на физическом уровне, извлечение данных из интегральных схем памяти, микроуровень). Специальные программно-аппаратные комплексы и программные продукты, используемые для извлечения криминалистически значимой информации. Верификация результатов технико-криминалистического исследования компьютеров и мобильных устройств.

Тема 7. Организация взаимодействия при расследовании дел о хищениях денежных средств, совершенных путем несанкционированного доступа к базам данных банка с использованием IT-технологий.

Понятие, задачи, принципы взаимодействия следователя, дознавателя с органом дознания в процессе раскрытия и расследования уголовного дела.

Основные формы и задачи взаимодействия следователя, дознавателя с органом дознания на этапе проверки сообщений о хищениях денежных средств, совершенных с использованием IT-технологий путем несанкционированного доступа к базам данных банка.

Взаимодействие следователя, дознавателя с организациями и учреждениями (сотовые операторы, банки, операторы систем электронных платежей, интернет-провайдеры и т.д.), у которых в процессе расследования запрашивается или изымается необходимая информация по уголовному делу.

Виды, задачи и принципы работы следственно-оперативных групп, создаваемых для раскрытия и расследования хищений денежных средств, совершенных с использованием IT-технологий путем несанкционированного доступа к базам данных банка.

3.4. Рекомендуемая литература

Нормативные правовые акты:

1. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г.) [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

2. Гражданский кодекс Российской Федерации (часть первая от 30 ноября 1994 г. № 51-ФЗ, часть вторая от 26 января 1996 г. № 14-ФЗ, часть третья от 26 ноября 2001 г. № 146-ФЗ) [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

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

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

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

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

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

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

«КонсультантПлюс».

9. 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».

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

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

12. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

13. Указ Президента Российской Федерации от 2 июля 2021 г. № 400 «О стратегии национальной безопасности Российской Федерации» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

14. Приказ МВД России от 29 июня 2005 г. № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации» (вместе с Инструкцией по организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации, Перечнем родов (видов) судебных экспертиз, производимых в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации) [Электронный ресурс] // Доступ из специализированной территориально распределенной автоматизированной системы «Юрист».

15. Приказ МВД России от 17 января 2006 г. № 19 «О деятельности органов внутренних дел по предупреждению преступлений» [Электронный ресурс] // Доступ из специализированной территориально распределенной автоматизированной системы «Юрист».

16. Приказ МВД России от 24 декабря 2015 г. № 1228 «Об утверждении правил организации доступа к информационно-телекоммуникационной сети «Интернет» в органах внутренних дел Российской Федерации» [Электронный ресурс] // Доступ из специализированной территориально распределенной автоматизированной системы «Юрист».

17. 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 специализированной территориально распределенной автоматизированной системы «Юрист».

Акты судебных органов:

1. 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 «Консультант Плюс».

2. Постановление Пленума Верховного Суда Российской Федерации от 1 июня 2017 г. № 19 «О практике рассмотрения судами ходатайств о производстве следственных действий, связанных с ограничением конституционных прав граждан» [Электронный ресурс] // Доступ из справочной правовой системы «Консультант Плюс».

3. 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 «Консультант Плюс».

4. Определение Верховного Суда Российской Федерации от 29 сентября 2020 г. по делу № 12-УДП-5-К6 (по вопросам квалификации хищений чужого имущества, связанных с использованием принадлежащей другому лицу кредитной, расчетной или иной платежной карты) [Электронный ресурс] // Доступ из справочной правовой системы «Консультант Плюс».

5. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России) // Доступ из справочной правовой системы «Консультант Плюс».

Основная литература:

1. Использование информации, содержащейся на электронных носителях, в уголовно-процессуальном доказывании: учебное пособие / Балашова А.А., Васюков В.Ф., Гаврилин Ю.В. [и др.]; под ред. Ю.В. Гаврилина и А.В. Победкина. – Москва: Академия управления МВД России, 2021. – 140 с.

2. Использование современных технологий в доказывании по уголовным делам (отечественный и зарубежный опыт): учебное пособие / Р.А. Исмагилов, Р.М. Исаева. – Уфа: Уфимский ЮИ МВД России, 2021. – 88 с.

3. Практикум по особенностям квалификации отдельных видов преступлений: учебник / М. Н. Косарев [и др.]. – Москва: ДГСК МВД России, 2019. – 392 с.

4. Противодействие преступлениям в сфере информационных технологий: учебник / [В.В. Гончар и др.]. – М.: Московский университет МВД России имени В.Я. Кикотя, 2021. – 332 с.

5. Расследование преступлений в сфере компьютерной информации, совершаемых против собственности: учебное пособие / А.В. Пузарин и др. – М.: Московский университет МВД России имени В.Я. Кикотя, 2020. – 185 с.

Дополнительная литература:

1. Бердникова О.П. Особенности первоначального и последующего этапов расследования мошенничества в сфере компьютерной информации: учебное пособие / О.П. Бердникова, Р.А. Дерюгин – Екатеринбург: Уральский юридический институт МВД России, 2019. – 56 с.

2. Вехов В.Б. IT-справочник следователя / под. ред. докт. юрид. наук С.В. Зуева. – М.: Юрлитинформ, 2019. – 232 с.

3. Вехов В.Б. Цифровая криминалистика: учебник для вузов / В.Б. Вехов [и др.]; под редакцией В. Б. Вехова, С. В. Зуева. – Москва: Издательство Юрайт, 2021. – 417 с.

4. Гизатуллин М.Г. Основы информационной безопасности в органах внутренних дел: учебное пособие / М.Г. Гизатуллин, И.Ф. Файсханов. – Екатеринбург: Уральский юридический институт МВД России, 2020. – 51 с.

5. Гулевич Д.С. Сети связи следующего поколения: учебное пособие / Д.С. Гулевич. – 3-е изд. – Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. – 212 с. // Цифровой образовательный ресурс IPR SMART: [сайт]. – URL:https://www.iprbookshop.ru/102063.html.

6. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие: в 2 ч. / [А.В. Аносов и др.]. – М.: Академия управления МВД России, 2019. – Ч. 1. – 208 с.

7. Использование искусственного интеллекта при выявлении, раскрытии, расследовании преступлений и рассмотрении уголовных дел в суде: монография / под. ред. докт. юрид. наук С.В. Зуева, канд. юрид. наук Д.В. Бахтеева. – М.: Юрлитинформ, 2022. – 216 с.

8. Концептуальные основы частной теории электронной цифровой криминалистики (частной теории собирания, исследования и использования электронной цифровой информации и информационно-технологических устройств): монография / А.Б. Смушкин; под общ. ред. В.Б. Вехова. – Москва: РУСАЙНС, 2022. – 222 с.

9. Кузьмин И.А. Раскрытие мошенничеств, совершенных с использованием информационно-коммуникационных технологий: учебное пособие / И.А. Кузьмин; Восточно-Сибирский институт МВД России. – Иркутск: ВСИ МВД России, 2021. – 80 с.

10. Международный опыт противодействия преступной деятельности с использованием криптовалюты: учебно-практическое пособие / Т.В. Пинкевич, Е.С. Смольянинов – Москва: Академия управления МВД России, 2021. – 108 с.

11. Методика расследования преступлений против собственности, совершаемых с использованием компьютерных и телекоммуникационных технологий: методические рекомендации / Т.В. Валькова, В.Э. Шунк, В.В. Долгаев; СПб: Изд-во СПб ун-та МВД России. 2020. – 56 с.

12. Методические рекомендации по расследованию преступлений в сфере компьютерной информации: учебное пособие / [И.Г. Чекунов и др.]. – М.:

Московский университет МВД России имени В.Я. Кикотя, 2019. – 176 с.

13. О научных подходах к проблеме использования информационно-телекоммуникационных технологий в преступных целях: научно-практическое пособие. – Москва: Академия управления МВД России, 2021. – 72 с.

14. Основы информационных технологий: учебное пособие/ С.В. Назаров, С.Н. Белоусова, И.А. Бессонова [и др.]. – 3-е изд. – Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. – 530 с. // Цифровой образовательный ресурс IPR SMART: [сайт]. – URL: http://www.iprbookshop.ru/89454.html.

15. Основы теории электронных доказательств: монография / под. ред. докт. юрид. наук С.В. Зуева. – М.: Юрлитинформ, 2019. – 400 с.

16. Особенности квалификации и расследования хищений электронных денежных средств, в том числе совершенных посредством использования информационно-телекоммуникационных сетей: учебное пособие / А.Ю. Ушаков, А.Г. Саакян, Р.С. Поздышев, М.А. Степанова. – Нижний Новгород: Нижегородская академия МВД России, 2022. – 55 с.

17. Особенности расследования преступлений, совершенных с использованием сети Интернет: учебно-практическое пособие / М.М. Душенко, О.А. Науменко. – Краснодар: Краснодарский университет МВД России, 2020. – 58 с.

18. Особенности реализации компьютерных экспертиз в системе МВД России: учебное пособие / В.Л. Акапьев, А.А. Гуржий, А.А. Дрога [и др.]. – Белгород: Бел ЮИ МВД России имени И.Д. Путилина, 2019. – 99 с.

19. Процессуальные и организационно-тактические особенности фиксации доказательственной информации, хранящейся на ресурсах сети Интернет: учебно-методическое пособие / А.И. Гайдин. – Москва: ДГСК МВД России, 2019. – 80 с.

20. Райфельд М.А. Системы и сети мобильной связи: учебное пособие / М.А. Райфельд, А.А. Спектор. – Новосибирск: Новосибирский государственный технический университет, 2019. – 96 с. // Цифровой образовательный ресурс IPR SMART: [сайт]. – URL:https://www.iprbookshop.ru/99218.html.

21. Расследование преступлений, совершаемых с использованием компьютерных и телекоммуникационных технологий: учебное пособие / Т.В. Валькова, В.В. Долгаев, С.В. Смелова. – Санкт-Петербург: Изд-во СПб ун-та МВД России, 2021. – 132 с.

22. Расследование хищений денежных средств с банковских счетов граждан, совершенных с использованием систем дистанционного банковского обслуживания: учебно-практическое пособие / В.Н. Чаплыгина [и др.]; – Орел: ОрЮИ МВД России им. В.В. Лукьянова, 2019. – 36 с.

23. Решетняк О.А. Расследование хищений чужого имущества, совершенных с использованием информационно-телекоммуникационных технологий: учебное пособие / О.А. Решетняк, С.А. Ковалев; – Волгоград: ВА МВД России, 2021. – 58 с.

24. Скрипник Д.А. Общие вопросы технической защиты информации: учебное пособие / Д.А. Скрипник. – 3-е изд. – Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. – 424 с.// Цифровой образовательный ресурс IPR SMART: [сайт]. – URL: http://www.iprbookshop.ru/89451.html.

25. Способы получения доказательств и информации в связи с обнаружением (возможностью обнаружения) электронных носителей: учебное пособие / В.Ф. Васюков, Б.Я. Гаврилов, А.А. Кузнецов [и др.]; под общ. ред. Б.Я. Гаврилова. – М.: Проспект, 2017. – 160 с.

26. Щетинина Н.В., Харламова А.А., Кокорин Д.Л. Квалификация преступлений против собственности. Екатеринбург: Уральский юридический институт МВД России, 2018. – 104 с.

27. Электронные носители информации в криминалистике: монография / под. ред. докт. юрид. наук О.С. Кучина. – М.: Юрлитинформ, 2017. – 304 с.

3.5. Примерный перечень ресурсов информационно-телекоммуникационной сети Интернет, необходимых для освоения программы

1. URL:http://www.consultant.ru – Официальный сайт компании «Консультант Плюс».
2. URL:http://www. garant.ru – Информационно-правовой портал «Гарант».
3. URL:http://www.gov.ru – Сервер органов государственной власти Российской Федерации «Официальная Россия».
4. URL:http://www.sudrf.ru – Государственная автоматизированная система Российской Федерации «Правосудие».
5. URL:http://www.iprbookshop.ru – Цифровой образовательный ресурс IPR SMART.
6. URL:http://www.crimlib. info – Электронный справочник следователя.
7. URL:http://www.sudact.ru – Суд Акт: Судебные и нормативные акты Российской Федерации.

4. ФОРМЫ АТТЕСТАЦИИ

Контроль успеваемости обучающегося – важнейшая форма контроля образовательной деятельности, включающая в себя целенаправленный систематический мониторинг освоения обучающимся программы в целях:

получения необходимой информации о выполнении обучающимся программы;

оценки уровня знаний, умений и приобретенной (усовершенствованной) обучающимся компетенции;

стимулирования самостоятельной работы обучающегося.

В ходе реализации программы предусматриваются текущий контроль успеваемости, промежуточная и итоговая аттестации.

Форма проведения промежуточной и итоговой аттестаций устанавливается образовательной организацией самостоятельно в образовательной программе.

Итоговая аттестация для обучающегося организуется в соответствии с требованиями, установленными Федеральным законом от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации», приказом Минобрнауки России от 1 июля 2013 г. № 499 «Об утверждении Порядка организации осуществления образовательной деятельности по дополнительным профессиональным программам».

Консультация перед итоговой аттестацией проводится в последний учебный день, предшествующий итоговой аттестации.

Итоговая аттестация проводится в сроки, предусмотренные учебным планом, календарным учебным графиком программы и расписанием учебных занятий.

Лицу, успешно освоившему программу и прошедшему итоговую аттестацию, на основании распорядительного акта образовательной организации выдается документ о квалификации – удостоверение о повышении квалификации установленного образца.

Лицу, не прошедшему итоговую аттестацию или получившему на итоговой аттестации оценку «неудовлетворительно», а также лицу, освоившему часть программы и (или) исключенному из числа обучающихся образовательной организации в ходе освоения программы, на основании распорядительного акта образовательной организации выдается справка об обучении или о периоде обучения установленного образца.