Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет «Московский институт электронной техники»

УТВЕРЖДАЮ
Проректор по УР
_____ А.Г. Балашов
«__11__» ____апреля____ 2023 г.

ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«ОСОБЕННОСТИ ВЫЯВЛЕНИЯ ПРОТИВОПРАВНЫХ ДЕЯНИЙ В СЕТИ ИНТЕРНЕТ»

Москва 2023

1. Цель реализации программы

Цель программы:

формирование компетенции, позволяющей эффективно проводить поиск противоправного контента в сети «Интернет», взаимодействовать с правоохранительными органами и осуществлять профилактику киберправонарушений на предприятии.

2. Характеристика профессиональной деятельности и (или) квалификации

Область профессиональной деятельности: 09 Юриспруденция (в сферах: правоохранительной деятельности; публично-правовой деятельности в интересах национальной безопасности в части уголовно-правовых, гражданско-правовых, государственно-правовых отношений)

Виды экономической деятельности: деятельность профессиональная, научная и техническая

Укрупненная группа специальностей: 40.00.00 Юриспруденция

3. Требования к результатам обучения

Формируемая компетенция: способен осуществлять профессиональную деятельность в интересах национальной безопасности в части уголовно-правовых, гражданско-правовых, государственно-правовых отношений на основе правовой оценки выявленных правонарушений.

В результате освоения программы слушатель должен:

Знать: основные понятия уголовного права, уголовно-процессуального права, криминалистики, информационной безопасности, методы выявления противоправной информации в сети «Интернет».

Уметь: отграничить преступное поведение от непреступного, давать уголовно-правовую оценку действиям физических и юридических лиц в сети «Интернет».

Иметь опыт: выявления киберправонарушений в сети «Интернет».

4. Содержание программы
Учебный план
программы повышения квалификации
«Особенности выявления противоправных деяний в сети Интернет»

Категория слушателей – лица, имеющие высшее образование, лица, получающие высшее образование.

Срок обучения – 36 часов.

Форма обучения – очно-заочная.

№ п/п	Наименование разделов / модулей	Всего, час	В том числе			Образовательные технологии, в том числе ЭО и (или) ДОТ
			Аудиторных		Самостоятельная работа	
			Лекции	Практические и лабораторные занятия		
1.	Правовое регулирование в сети «Интернет»	18	6	6	6	ЭО; ДОТ
2.	Установление и фиксация признаков совершенных и готовящихся административных правонарушений и преступлений в сети «Интернет» и киберпространстве	18	6	6	6	ЭО; ДОТ
	Всего	36	12	12	12	
Итоговая аттестация		Зачет				

Учебно-тематический план
программы повышения квалификации
«Особенности выявления противоправных деяний в сети Интернет»

№ п/п	Наименование тем разделов / модулей	Всего, час	В том числе			Образовательные технологии, в том числе ЭО и (или) ДОТ
			Аудиторных		Самостоятельная работа	
			Лекции	Практические и лабораторные занятия		
1.	Правовое регулирование в сети «Интернет»	**18**	**6**	**6**	**6**	ЭО; ДОТ
1.1	Правомерное и неправомерное поведение. Понятие преступления и административного правонарушения. Отличия преступного поведения от непреступного.	6	2	2	2	ЭО; ДОТ
1.2	Киберпреступность и ее виды. Правоохранительные органы, выявляющие административные правонарушения и преступления в сети «Интернет»: классификация, полномочия.	6	2	2	2	ЭО; ДОТ
1.3	Законодательство, предусматривающее ответственность за неправомерное поведение в сети «Интернет». Экстремизм и терроризм как составы преступлений. Иные составы преступлений и административных правонарушений в сети «Интернет» и киберпространстве	6	2	2	2	ЭО; ДОТ
2.	Установление и фиксация признаков совершенных и	**18**	**6**	**6**	**6**	ЭО; ДОТ

№ п/п	Наименование тем разделов / модулей	Всего, час	В том числе			Образовательные технологии, в том числе ЭО и (или) ДОТ
			Аудиторных		Самостоятельная работа	
			Лекции	Практические и лабораторные занятия		
	готовящихся административных правонарушений и преступлений в сети «Интернет» и киберпространстве					
2.1.	Мониторинг социальных сетей на предмет совершенных и готовящихся административных правонарушений и преступлений	6	2	2	2	ЭО; ДОТ
2.2.	Технические особенности фиксации цифровой информации, содержащей признаки совершенных и готовящихся административных правонарушений и преступлений	6	2	2	2	ЭО; ДОТ
2.3	Правовые и технические особенности взаимодействия с правоохранительными органами при установлении и фиксации признаков совершенных и готовящихся административных правонарушений и преступлений в сети «Интернет» и киберпространстве	6	2	2	2	ЭО; ДОТ
	Консультации					
	Всего	36	12	12	12	
Итоговая аттестация		Зачет				

Календарный учебный график

Календарный учебный график составляется в форме расписания занятий при наборе группы и прилагается к программе повышения квалификации.

Учебная программа повышения квалификации «Особенности выявления противоправных деяний в сети Интернет»

Модуль 1. Правовое регулирование в сети «Интернет» (18 часов).

Тема 1.1. Правомерное и неправомерное поведение.

Понятие преступления и административного правонарушения. Отличия преступного поведения от непреступного.

Понятие преступления. Понятие административного правонарушения. Состав преступления.

Тема 1.2. Киберпреступность и ее виды. Правоохранительные органы, выявляющие административные правонарушения и преступления в сети «Интернет»: классификация, полномочия.

Понятие киберпреступления. Мошенничество, кражи, совершенные с помощью ИКТ. Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства. Следователи Федеральной службы безопасности. Следователи Следственного комитета.

Тема 1.3. Законодательство, предусматривающее ответственность за неправомерное поведение в сети «Интернет».

Экстремизм и терроризм как составы преступлений. Иные составы преступлений и административных правонарушений в сети «Интернет» и киберпространстве.

Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ. Федеральный закон "О противодействии экстремистской деятельности" от 25.07.2002 N 114-ФЗ. Федеральный закон "О противодействии терроризму" от 06.03.2006 N 35-ФЗ. "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ. "Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 N 195-ФЗ.

Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации. Организация экстремистского сообщества.

Практические занятия

Номер темы	Краткое содержание	Кол-во часов
1.1.	Отличия преступного поведения от непреступного. Понятие преступления. Понятие административного правонарушения. Состав преступления.	2
1.2.	Понятие киберпреступления. Мошенничество, кражи, совершенные с	2

	помощью ИКТ. Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства. Следователи Федеральной службы безопасности. Следователи Следственного комитета.	
1.3.	Экстремизм и терроризм как составы преступлений. Иные составы преступлений и административных правонарушений в сети «Интернет» и киберпространстве.	2

Самостоятельная работа слушателей

Номер темы	Вид СРС	Кол-во часов
1.1.	Проработка лекционного и дополнительного материала в ОРИОКС по теме 1.1, выполнение практического задания по модулю 1.	2
1.2.	Проработка лекционного и дополнительного материала в ОРИОКС по теме 1.2, выполнение практического задания по модулю 1.	2
1.3.	Проработка лекционного и дополнительного материала в ОРИОКС по теме 1.3, выполнение практического задания по модулю 1.	2

Модуль 2. Установление и фиксация признаков совершенных и готовящихся административных правонарушений и преступлений в сети «Интернет» и киберпространстве (18 часов).

Тема 2.1. Мониторинг социальных сетей на предмет совершенных и готовящихся административных правонарушений и преступлений.

Понятие и виды социальных сетей. Ресурсы министерства юстиции Российской Федерации в сети «Интернет». Применение автоматизированных средства поиска противоправного контента. Технологии поиска противоправного контента через открытые источники (OSINT).

Тема 2.2. Технические особенности фиксации цифровой информации, содержащей признаки совершенных и готовящихся административных правонарушений и преступлений.

Сбор, хранение, передача цифровых следов совершенных и готовящихся киберправонарушений.

Тема 2.3. Правовые и технические особенности взаимодействия с правоохранительными органами при установлении и фиксации признаков совершенных и готовящихся административных правонарушений и преступлений в сети «Интернет» и киберпространстве.

Взаимодействие с прокуратурой, следственным комитетом, федеральной службой безопасности, органами исполнительной власти, Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Практические занятия

Номер темы	Краткое содержание	Кол-во часов
2.1.	Применение автоматизированных средства поиска противоправного контента. Технологии поиска противоправного контента через открытые источники (OSINT).	2
2.2.	Сбор, хранение, передача цифровых следов совершенных и готовящихся киберправонарушений.	2
2.3.	Взаимодействие с прокуратурой, следственным комитетом, федеральной службой безопасности, органами исполнительной власти, Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).	2

Самостоятельная работа слушателей

Номер темы	Вид СРС	Кол-во часов
2.1.	Проработка лекционного и дополнительного материала в ОРИОКС по теме 2.1, выполнение практического задания по модулю 2.	2
2.2.	Проработка лекционного и дополнительного материала в ОРИОКС по теме 2.2, выполнение практического задания по модулю 2.	2
2.3.	Проработка лекционного и дополнительного материала в ОРИОКС по теме 2.3, выполнение практического задания по модулю 2.	2

5. Материально-технические условия реализации программы

Для изучения дисциплины слушателю необходима компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду МИЭТ.

Необходимое программное обеспечение: Операционная система Microsoft Windows от 7 версии и выше, Microsoft Office Professional Plus или Open Office, браузер (Firefox, Google Chrome), Acrobat Reader DC.

6. Учебно-методическое обеспечение программы

6.1. Учебники и учебные пособия

1. Уголовно-процессуальное право. Актуальные проблемы теории и практики : Учеб. для бакалавриата, специалитета и магистратуры / А.А. Тарасов ; Под ред. В.А. Лазаревой, А.А. Тарасова. - 4-е изд., перераб. и доп. - М. : Юрайт, 2018. - 390 с. - (Бакалавр. Специалист. Магистр). - URL: https://urait.ru/bcode/426530 (дата обращения: 25.12.2020). - ISBN 978-5-534-08808-3 : 0-00. - Текст : электронный.

2. Основы теории электронных доказательств : Монография / Под ред. С.В. Зуева. - М. : Юрлитинформ, 2019. - 400 с. - ISBN 978-5-4396-1825-5 : 1400-00, 3000 экз.

3. Криминалистика : Учебник для бакалавров / Под ред. Л.В. Бертовского. - М. : Проспект : РГ-Пресс, 2018. - 960 с. - ISBN 978-5-9988-0671-1 : 1217-00. - Текст : непосредственный.

4. Информационное право : учебник для вузов / под редакцией Н. Н. Ковалевой. - Москва : Юрайт, 2020. - 353 с. - (Высшее образование). - URL: https://urait.ru/bcode/466887 (дата обращения: 03.08.2021). - ISBN 978-5-534-13786-6. - Текст : электронный.

Периодические издания

1. КРИМИНАЛИСТЪ : научно-практическое издание / ФГКОУ ВПО "Академия Генеральной прокуратуры Российской Федерации". - Санкт-Петербург : СПбЮИфУПРФ, 2008 - . - URL: http://www.procuror.spb.ru/kriminalist.html (дата обращения: 06.07.2021). - Режим доступа: свободный. - ISSN 2686-7753. - Текст : электронный.

2. ПРОБЕЛЫ В РОССИЙСКОМ ЗАКОНОДАТЕЛЬСТВЕ : научный журнал / Издательский дом "Юр-ВАК" (Москва). - Москва : Юр-ВАК, 2008 - . - На сайте журнала статьи доступны в полнотекстовом виде с 2013 г. после регистрации. - URL: https://urvak.ru/journals/probely-v-rossiyskom/ (дата обращения: 16.11.2020). - На сайте Научной электронной библиотеки eLIBRARY.RU доступ к полному тексту статей для зарегистрированных пользователей с 2008 г., последние два года - через систему заказа. - URL: https://www.elibrary.ru/title_about_new.asp?id=26718 (дата обращения: 23.03.2023). - ISSN 2072-3164.

6.2. Перечень профессиональных баз данных, информационных справочных систем

Лань: электронно-библиотечная система. – Санкт-Петербург, 2011. – URL: https://e.lanbook.com/ (дата обращения: 23.03.2023). – Режим доступа: для авторизованных пользователей МИЭТ.

eLIBRARY.RU: научная электронная библиотека: сайт. – Москва, 2000. – URL: https://elibrary.ru (дата обращения: 23.03.2023). – Режим доступа: для зарегистрированных пользователей.

7. Оценка качества освоения программы

Итоговая аттестация осуществляется в форме зачета, который состоит из итогового теста по освоенным модулям. Общее количество баллов за тестирование составляет 10 баллов (примерный перечень вопросов приведен в Приложении № 1).

Показатель оценки	Критерий оценивания достижения показателя	Условия начисления баллов по критерию	Количество баллов

Показатель оценки	Критерий оценивания достижения показателя	Условия начисления баллов по критерию	Количество баллов
Выполненное тестовое задание, предполагающее выбор верного ответа из ряда предложенных.	Соответствие ответов на вопросы теста эталону правильного ответа.	1 балл за правильный ответ 0 баллов на неправильный ответ	0-10
		Суммарный балл по показателю:	**0 - 10**

Слушатель считается аттестованным, если по итогам выполнения заданий набрал 7 и более баллов.

8. Составители программы

Директор Института ВП СГН,
д-р юрид. наук, профессор — Л.В. Бертовский

зам. директора Института ВП СГН
канд. юрид. наук — Г.С. Девяткин

Согласовано:

Директор ДРОП — Н. Ю. Соколова

Приложение № 1

Примерный вариант тестирования

1. Какая ответственность предусмотрена за взлом и получение доступа к странице Вконтакте?

А) Уголовная

Б) Административная

В) Гражданско-правовая

Г) Дисциплинарная

2. Киберпреступление это:

А) общественно-опасное деяние, совершенное в информационно-телекоммуникационной сети «Интернет»

Б) «Телефонное» мошенничество

В) Несанкционированное получение доступа к переписке пользователя ВКонтакте

Г) все вышеуказанные варианты верны

3. Что образует состав преступления?

А) объект, субъект, объективная сторона, субъективная сторона

Б) Объект и субъект преступления

В) Вариативная и обязательная сторона

Г) Вина и деяние

4. Какие функции выполняет Роскомнадзор?

А) возбуждение уголовных дел

Б) надзор в сфере связи, информационных технологий и СМИ, а также надзор по защите персональных данных согласно закону и деятельность по организации радиочастотной службы

В) предоставление доступа к сети «Интернет»

Г) предоставление доменных имен для физических и юридических лиц

5. Какие персональные данные ограничены для свободного распространения?

А) сведения о наличии социальной страницы ВКонтакте

Б) сведения о наличии аккаунта в Госуслугах

В) сведения о судимости лица

Г) сведения о наличии задолженности у ФССП

6. Какие функции предусмотрены у прокуратуры при обнаружении ресурса в сети «Интернет», содержащего признаки экстремистского

А) обращение в суд с целью признания ресурса экстремистским

Б) самостоятельная блокировка ресурса

В) блокировка ресурса с привлечением экспертной организации

7. Какие критерии предусмотрены для отнесения ресурса в сети «Интернет» к социальной сети?

А) доступ в течение суток имеют более 500 тысяч пользователей, находящихся на территории России

Б) возможность он-лайн общения хотя бы двух пользователей

В) наличие сайта и пользовательского соглашения с указанием «социальная сеть»

Г) Наличие специального сертификата

8. Какое средний размер похищенных средств за один эпизод «телефонного мошенничества» зафиксирован в России в 2022 году?

А) 132 000 рублей

Б) 500 000 рублей

В) 1 200 000 рублей

Г) 72 000 рублей

9. Что включает в себя технология OSINT?

А) сбор информации о физическом лице или организации из открытых источников и ее последующий анализ

Б) незаконный способ получения сведений закрытого характера о физическом лице

В) база данных о физическом лице

Г) номер телефона, ИНН и СНИЛС физического лица

10. Каким образом возможно зафиксировать цифровые следы удаленного диалога в мессенджере?

А) установить специальное приложение для поиска удаленных диалогов

Б) переустановить мессенджер и получить доступ к удаленным диалогам

В) обратиться к провайдеру и уполномоченному лицу от мессенджера с ходатайством о предоставлении удаленного диалога

Г) все вышеуказанные варианты верны