МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯРОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

СОГЛАСОВАНО

Директор
Института дополнительного
профессионального образования
_____ М.Н. Большакова
2 сентября 2025 г.

УТВЕРЖДАЮ

Проректор по образовательной
деятельности
ФГАОУ ВО «Севастопольский
государственный университет»
_____ В.Р. Душко
1 сентября 2025 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«ПРОТИВОДЕЙСТВИЕ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ СОВРЕМЕННЫХ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ»

Севастополь – 2025

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. НОРМАТИВНАЯ БАЗА ПРОГРАММЫ

Дополнительная профессиональная программа повышения квалификации «Противодействие преступлениям, совершаемым с использованием современных информационно-коммуникационных технологий» разработана в соответствии со следующими нормативными документами:

Федеральный закон «Об образовании в Российской Федерации» от 29.12.2012 г. № 273-ФЗ;

- Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам: приказ Министерства науки и высшего образования Российской Федерации от 24 марта 2025 г. N 266.

- Постановление Правительства Российской Федерации от 11 октября 2023 № 1678 «Об утверждении Правил применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ» вступило в силу 1 сентября 2024 г.;

- Письмо Министерства образования и науки Российской Федерации «О направлении методических рекомендаций» от 10.02.2015 г. № 05-308 (вместе с Методическими рекомендациями по разработке основных профессиональных образовательных программ и дополнительных профессиональных программ с учетом соответствующих профессиональных стандартов», утв. 22.01.2015 г. № ДЛ-1/05вн);

- Инструкция по разработке дополнительных образовательных программ, дополнительных общеобразовательных программ и основных программ профессионального обучения, утвержденная приказом исполняющего обязанности ректора от 13.10.2021 №1850-п;

- Приказ Министерства труда и социальной защиты Российской Федерации от 29 сентября 2014 г. N 667н "О реестре профессиональных стандартов (перечне видов профессиональной деятельности)" с изменениями, внесенными приказом Министерства труда и социальной защиты Российской Федерации от 9 марта 2017 г. N 254н;

Образовательный стандарт:

- **ФГОС ВО по специальности 10.05.01 «Компьютерная безопасность»** (специалитет), утвержденный Приказом Министерства науки и высшего образования Российской Федерации от 26.11.2020 № 1459;

- **ФГОС ВО по направлению подготовки 40.03.01 «Юриспруденция»** (бакалавриат), утвержденный Приказом Министерства науки и высшего образования Российской Федерации от 13.08.2020 г. № 1011;
- **ФГОС ВО по направлению подготовки 40.05.01 «Правовое обеспечение национальной безопасности»** (специалитет), утвержденный Приказом Министерства науки и высшего образования Российской Федерации от 12.08.2020 № 970 (в качестве рекомендательного документа для смежных специальностей правоохранительной деятельности);

Профессиональный стандарт:

- **Профессиональный стандарт 06.032 «Специалист по безопасности компьютерных систем и сетей»**, утвержденный Приказом Министерства труда и социальной защиты Российской Федерации от 10.02.2022 № 52н (актуальная редакция);
- **Профессиональный стандарт 40.001 «Специалист в области обеспечения безопасности»** (для должностей в правоохранительных органах и службах безопасности), утвержденный Приказом Минтруда России от 11.04.2014 № 223н (с изменениями);
- **Квалификационные требования к должностям в органах внутренних дел Российской Федерации**, установленные нормативными правовыми актами МВД России.

Уровень квалификации: 6-7

1.2. ЦЕЛЬ РЕАЛИЗАЦИИ ПРОГРАММЫ

Дополнительная профессиональная программа повышения квалификации направлена на **формирование, совершенствование и актуализацию профессиональных компетенций**, необходимых для эффективного **выявления, предупреждения, раскрытия и расследования преступлений, совершаемых с использованием современных информационно-коммуникационных технологий (ИКТ).**

Конкретизация цели (для кого и зачем): Программа обеспечивает повышение профессионального уровня **в рамках имеющейся квалификации** следующих категорий слушателей:

- **Сотрудники правоохранительных органов**, в том числе:
  - Следственных и экспертно-криминалистических подразделений.
  - Подразделений дознания.
  - Оперативных подразделений (специально-технических мероприятий, уголовного розыска, по контролю за оборотом наркотиков, противодействия экстремизму, экономической безопасности и противодействия коррупции).

- **Сотрудники территориальных органов МВД России.**

1.3. ТРЕБОВАНИЯ К УРОВНЮ ПОДГОТОВКИ ПОСТУПАЮЩЕГО НА ОБУЧЕНИЕ

К освоению дополнительной профессиональной программы повышения квалификации допускаются лица, имеющие или получающие среднее профессиональное и (или) высшее образование.

Категория слушателей – сотрудники следственных и экспертно-криминалистических подразделений, подразделений дознания, специально-технических мероприятий, уголовного розыска, по контролю за оборотом наркотиков, противодействия экстремизму, экономической безопасности и противодействия коррупции территориальных органов МВД России, (далее - сотрудники территориальных подразделений МВД России) осуществляющих функции по противодействию преступлениям совершаемым с использованием современных информационно-коммуникационных технологий (далее - ИКТ)

1.4. ТРУДОЕМКОСТЬ ОБУЧЕНИЯ

Нормативная трудоемкость обучения по данной программе 42 академических часа, включая все виды учебной работы слушателя.

1.5. ФОРМА ОБУЧЕНИЯ

Форма обучения – заочная с применением дистанционных образовательных технологий.

1.6. РЕЖИМ ЗАНЯТИЙ

Учебная нагрузка устанавливается не более 8 академических часов в день, включая все виды учебной работы слушателя.

1.7. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

№	Профессиональные компетенции (ПК)	Знания (З)	Умения (У)	Владения / Навыки (В)
1	**ПК-1:** Способность применять знания в области материального и процессуального права, в том числе в	**З.1:** Правовые основы, классификацию и особенности квалификации преступлений в сфере компьютерной информации и высоких	**У.1:** Квалифицировать составы преступлений, совершаемых с использованием ИКТ. **У.2:** Применя	**В.1:** Навыкам и правового анализа ситуаций, связанных с киберпреступностью. **В.2:** Навыкам и применения процессуальн

№	Профессиональные компетенции (ПК)	Знания (З)	Умения (У)	Владения / Навыки (В)
	сфере квалификации преступлений, совершаемых с использованием ИКТ.	технологий (ст.ст. 272-274, 146, 159.6, 228.1, 282 УК РФ и др.). **З.2:** Требования федерального законодательства и ведомственных нормативных актов, регулирующих служебную деятельность и информационную безопасность (ФЗ «Об информации», «О персональных данных», «О связи», «Об оперативно-розыскной деятельности»).	ть нормы уголовного и уголовно-процессуального права при планировании и проведении процессуальных действий. **У.3:** Обеспечивать соблюдение правовых норм при работе с цифровыми доказательствами и информацией ограниченного доступа.	ых документов при расследовании преступлений в сфере ИКТ.
2	**ПК-2:** Способность выявлять, фиксировать, изымать и предварительно исследовать вещественные доказательства и цифровые следы на месте происшествия.	**З.3:** Механизмы следообразования в цифровой среде (виртуальные следы), классификацию следов при воздействии на информационные системы. **З.4:** Способы, технико-криминалистические средства и методики	**У.4:** Организовывать и проводить осмотр места происшествия с участием специалиста в области ИКТ. **У.5:** Применять технико-криминалистические средства и методы для	**В.3:** Практическими навыками работы с базовым комплексом технико-криминалистических средств для изъятия цифровых доказательств. **В.4:** Навыкам и составления

№	Профессиональные компетенции (ПК)	Знания (З)	Умения (У)	Владения / Навыки (В)
		обнаружения, фиксации, изъятия материальных носителей информации и цифровых следов. **З.5:** Особенности осмотра места происшествия, обыска и выемки при расследовании компьютерных преступлений (работающего/неработающего оборудования, сетевой инфраструктуры).	обнаружения, фиксации и изъятия цифровых носителей информации. **У.6:** Обеспечивать сохранность и процессуальную чистоту изъятых электронных доказательств (правила опечатывания, упаковки, транспортировки, хранения).	протоколов следственных действий с отражением специфики работы с цифровыми объектами.
3	**ПК-3:** Способность применять методики судебно-экспертного исследования цифровой информации и формулировать задания для экспертов.	**З.6:** Основы судебной компьютерно-технической экспертизы: цели, задачи, объекты, пределы компетенции эксперта. **З.7:** Виды экспертиз, связанных с исследованием компьютерных средств, систем и сетей (компьютерно-	**У.7:** Определять необходимость и вид судебной экспертизы в зависимости от обстоятельств дела. **У.8:** Грамотно формулировать вопросы для эксперта в постановлени	**В.5:** Навыкам и анализа заключений судебных экспертов по компьютерным экспертизам. **В.6:** Навыкам и взаимодействия с экспертно-криминалистическими подразделениями для

№	Профессиональные компетенции (ПК)	Знания (З)	Умения (У)	Владения / Навыки (В)
		техническая, сетевой трафик, программное обеспечение, данные мобильных устройств). **З.8:** Особенности составления заключения эксперта и постановки вопросов при назначении компьютерных экспертиз.	и о назначении судебной экспертизы. **У.9:** Анализировать и оценивать заключение эксперта с точки зрения его полноты, обоснованности и значения для дела.	получения консультаций и назначения экспертиз.
4	**ПК-4:** Способность организовывать и проводить оперативно-розыскные мероприятия (ОРМ) в информационно-телекоммуникационной сети «Интернет».	**З.9:** Правовые основы, виды, тактику и особенности проведения ОРМ в сети «Интернет» для выявления преступлений (экстремизм, наркооборот, мошенничество и др.). **З.10:** Основы получения и фиксации оперативно-значимой информации из открытых и ограниченных интернет-источников.	**У.10:** Планировать и документально оформлять проведение ОРМ в сети «Интернет» в рамках предоставленных полномочий. **У.11:** Использовать базовые методы и средства поиска, сбора и первичного анализа информации в сети «Интернет».	**В.7:** Навыкам и безопасного и легитимного поиска информации в открытых источниках сети «Интернет» (OSINT-базовые). **В.8:** Навыкам и применения специализированного программного обеспечения для фиксации интернет-страниц и цифровых артефактов.

№	Профессиональные компетенции (ПК)	Знания (З)	Умения (У)	Владения / Навыки (В)
		З.11: Современные инструментальные средства и программно-аппаратные комплексы, используемые для ОРМ в киберпространстве.	**У.12:** Обеспечивать соблюдение законности при проведении ОРМ в цифровой среде.	
5	**ПК-5:** Способность применять базовые принципы и методы защиты информации и кибербезопасности в служебной деятельности.	**З.12:** Основные угрозы информационной безопасности, каналы утечки информации, способы несанкционированного доступа. **З.13:** Принципы криптографической защиты, аутентификации, использования электронной подписи и электронных ключей. **З.14:** Основы построения политики информационной безопасности, методы защиты при работе в сети «Интернет», с мобильными	**У.13:** Применять на практике основные методы и средства защиты информации (криптография, ЭП, настройки безопасности). **У.14:** Обеспечивать безопасность служебной информационной среды при использовании интернет-сервисов и удаленных подключений. **У.15:** Выявля	**В.9:** Навыками настройки базовых параметров безопасности персональных и служебных компьютерных систем (антивирус, межсетевой экран). **В.10:** Навыками безопасной работы с электронной почтой, съемными носителями и в публичных сетях. **В.11:** Навыками соблюдения режима информационной

№	Профессиональные компетенции (ПК)	Знания (З)	Умения (У)	Владения / Навыки (В)
		устройствами и при удаленном доступе (межсетевое экранирование). **З.15:** Требования по защите государственной и служебной тайны, обеспечению режима секретности при работе с цифровой информацией.	ть типовые признаки компрометации информационных систем и реагировать на них.	безопасности в повседневной служебной деятельности.
6	**ПК-6:** Способность анализировать оперативную и следственную ситуацию, выявлять причины и условия, способствующие совершению киберпреступлений, и разрабатывать предложения по их предупреждению.	**З.16:** Криминалистическую и криминологическую характеристику преступлений в сфере ИКТ, уровень и структуру киберпреступности, ее латентность. **З.17:** Основы виктимологической профилактики, формы и методы предупредительной деятельности органов внутренних дел в киберсфере, включая взаимодействие со СМИ и населением.	**У.16:** Проводить анализ расследуемого киберпреступления для выявления способа, средств совершения и криминальных связей. **У.17:** На основе обобщения экспертной и следственной практики выявлять системные причины и условия, способствующие	**В.12:** Навыками системного анализа преступлений в сфере ИКТ. **В.13:** Навыками подготовки информационно-аналитических материалов и предложений по совершенствованию предупредительной деятельности. **В.14:** Навыками консультирования граждан и

№	Профессиональные компетенции (ПК)	Знания (З)	Умения (У)	Владения / Навыки (В)
		З.18: Методы анализа данных, полученных в ходе расследования, для установления способа совершения преступления и выявления дополнительных источников информации.	совершению киберпреступлений. **У.18:** Разрабатывать практические рекомендации и информационные материалы для предупреждения киберпреступлений и повышения цифровой грамотности граждан.	представителей организаций по вопросам защиты от киберугроз.

2. СОДЕРЖАНИЕ ПРОГРАММЫ
2.1. УЧЕБНЫЙ ПЛАН
по дополнительной профессиональной программе повышения квалификации
«Противодействие преступлениям, совершаемым с использованием современных информационно-коммуникационных технологий»

Программа соответствует квалификационным требованиям:

- **ФГОС ВО по специальности 10.05.01 «Компьютерная безопасность»** (специалитет), утвержденный Приказом Министерства науки и высшего образования Российской Федерации от 26.11.2020 № 1459;
- **ФГОС ВО по направлению подготовки 40.03.01 «Юриспруденция»** (бакалавриат), утвержденный Приказом Министерства науки и высшего образования Российской Федерации от 13.08.2020 г. № 1011;
- **ФГОС ВО по направлению подготовки 40.05.01 «Правовое обеспечение национальной безопасности»** (специалитет), утвержденный Приказом Министерства науки и высшего образования Российской Федерации от 12.08.2020 № 970 (в качестве рекомендательного документа для смежных специальностей правоохранительной деятельности);
- **Профессиональный стандарт 06.032 «Специалист по безопасности компьютерных систем и сетей»**, утвержденный Приказом Министерства труда и социальной защиты Российской Федерации от 10.02.2022 № 52н (актуальная редакция);
- **Профессиональный стандарт 40.001 «Специалист в области обеспечения безопасности»** (для должностей в правоохранительных органах и службах безопасности), утвержденный Приказом Минтруда России от 11.04.2014 № 223н (с изменениями);
- **Квалификационные требования к должностям в органах внутренних дел Российской Федерации**, установленные нормативными правовыми актами МВД России.

Форма обучения – заочная с применением дистанционных образовательных технологий

Срок обучения – 42 академических часа, включая все виды учебной работы слушателя

Режим занятий – до 8 академических часов в день

Категория слушателей – сотрудники следственных и экспертно-криминалистических подразделений, подразделений дознания, специально-технических мероприятий, уголовного розыска, по контролю за оборотом наркотиков, противодействия экстремизму, экономической безопасности и противодействия коррупции территориальных органов МВД России, (далее - сотрудники территориальных подразделений МВД России) осуществляющих функции по противодействию преступлениям совершаемым с использованием современных информационно-коммуникационных технологий (далее - ИКТ)

№	Наименование разделов,	Кол-во часов (з.е.)	

п/п	дисциплин (модулей)	Всего	Аудиторные			Дистанционные			СР	Форма аттестации
			ЛК	ЛБ	ПР	ЛК	ЛБ	ПР		
1	Понятие юридической ответственности за правонарушения в области компьютерной безопасности	7				6			1	
2	Криминалистическая и криминологическая характеристика компьютерных преступлений	10				2		4	4	
3	Проведение ОРМ при обнаружении компьютерных инцидентов	3				2			1	
4	Характеристика инструментальных модулей, необходимых для обнаружения следов компьютерных преступлений	3				2			1	
5	Судебно-экспертное исследование компьютерных средств и систем	3				2			1	
6	Предотвращение компьютерных преступлений в сфере высоких технологий	14						8	6	
8	**Итоговая аттестация**	2						2		Зачет
	Итого	42				14		14	14	

2.2. УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН

по дополнительной профессиональной программе повышения квалификации

«Противодействие преступлениям, совершаемым с использованием современных информационно-коммуникационных технологий»

- **ФГОС ВО по специальности 10.05.01 «Компьютерная безопасность»** (специалитет), утвержденный Приказом Министерства науки и высшего образования Российской Федерации от 26.11.2020 № 1459;
- **ФГОС ВО по направлению подготовки 40.03.01 «Юриспруденция»** (бакалавриат), утвержденный Приказом Министерства науки и высшего образования Российской Федерации от 13.08.2020 г. № 1011;
- **ФГОС ВО по направлению подготовки 40.05.01 «Правовое обеспечение национальной безопасности»** (специалитет), утвержденный Приказом Министерства науки и высшего образования Российской Федерации от 12.08.2020 № 970 (в качестве рекомендательного документа для смежных специальностей правоохранительной деятельности);
- **Профессиональный стандарт 06.032 «Специалист по безопасности компьютерных систем и сетей»**, утвержденный Приказом Министерства труда и социальной защиты Российской Федерации от 10.02.2022 № 52н (актуальная редакция);
- **Профессиональный стандарт 40.001 «Специалист в области обеспечения безопасности»** (для должностей в правоохранительных органах и службах безопасности), утвержденный Приказом Минтруда России от 11.04.2014 № 223н (с изменениями);
- **Квалификационные требования к должностям в органах внутренних дел Российской Федерации**, установленные нормативными правовыми актами МВД России.

Форма обучения – заочная с применением дистанционных образовательных технологий

Срок обучения – 42 академических часа, включая все виды учебной работы слушателя

Режим занятий – до 8 академических часов в день

Категория слушателей – сотрудники следственных и экспертно-криминалистических подразделений, подразделений дознания, специально-технических мероприятий, уголовного розыска, по контролю за оборотом наркотиков, противодействия экстремизму, экономической безопасности и противодействия коррупции территориальных органов МВД России, (далее - сотрудники территориальных подразделений МВД России) осуществляющих функции по противодействию преступлениям совершаемым с использованием современных информационно-коммуникационных технологий (далее - ИКТ)

№ п/п	Наименование разделов, дисциплин (модулей)	Кол-во часов (з.е.)							Форма аттестации
		Всего	Аудиторные			Дистанционные			СР	
			ЛК	ЛБ	ПР	ЛК	ЛБ	ПР		
1	**Понятие юридической ответственности за правонарушения в области компьютерной безопасности**	**7**				**6**			**1**	
1.1	Международные и зарубежные уголовно-правовые классификации преступлений в сфере высоких технологий. Становление отечественного уголовно-правового и уголовно-процессуального регулирования в сфере высоких технологий и компьютерной информации. Современное состояние преступности в сфере компьютерной информации	7				6			**1**	
2	**Криминалистическая и криминологическая характеристика компьютерных преступлений**	**10**				**2**		**4**	**4**	
2.1	Криминалистическая классификация преступлений в сфере высоких технологий. Понятие криминалистической характеристики преступлений в сфере высоких технологий и её особенности	6				2		**2**	**2**	
2.2	Способы совершения преступлений в сфере высоких технологий.	4						**2**	**2**	
3	**Проведение ОРМ при обнаружении компьютерных инцидентов**	**3**				**2**			**1**	

3.1	Виды и особенности проведения следственных осмотров при расследовании преступлений в сфере высоких технологий. Особенности проведения допроса и проверки показаний на месте. Особенности следственного эксперимента при расследовании преступлений в сфере высоких технологий. Специальные средства криминалистической техники, используемые при проведении отдельных следственных действий	3				**2**			**1**	
4	**Характеристика инструментальных модулей, необходимых для обнаружения следов компьютерных преступлений**	**3**				**2**			**1**	
4.1	Понятие виртуальных следов и их основные свойства. Механизм следообразования при совершении преступлений в сфере компьютерной информации.	3				2			**1**	
5	**Судебно-экспертное исследование компьютерных средств и систем**	**3**				**2**			**1**	
5.1	Понятие и сущность специальных знаний сведущих лиц при расследовании преступлений в сфере высоких технологий. Функции специалиста в области информационных средств и технологий, привлеченного к участию в	3				**2**			**1**	

	процессуальных действиях.									
6	**Предотвращение компьютерных преступлений в сфере высоких технологий**	**14**						**8**	**6**	
6.1	Криптографическая защита информации.	2						1	1	
6.2	Электронные ключи. Аутентификация с использованием электронных ключей. Формирование и использование электронной подписи.	2						1	1	
6.3	Политика безопасности при использовании интернет-сервисов.	3						2	1	
6.4	Методы обеспечения информационной безопасности при работе в сети Интернет.	2						1	1	
6.5	Обеспечение информационной безопасности при удаленном подключении к интернет-сервисам. Защита мобильных устройств.	2						1	1	
6.6	Межсетевое экранирование. Настройка персонального межсетевого экрана	3						2	1	
8	**Итоговая аттестация**	**2**						**2**		**Зачет**
	Итого	**42**				**14**		**14**	**14**	

2. https://znanium.com/catalog/product/2127013 (дата обращения: 06.12.2025). – Режим доступа: по подписке.

3. Симаков, А. А. Защита информации в компьютерных системах : учебное пособие / А. А. Симаков, А. В. Кургузов. — Омск : Омская академия МВД России, 2022. — 108 с. — ISBN 978-5-88651-802-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/138415.html (дата обращения: 06.12.2025). — Режим доступа: для авторизир. пользователей

4. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. — Москва : Ай Пи Ар Медиа, 2025. — 263 с. — ISBN 978-5-4497-4085-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/147936.html (дата обращения: 06.12.2025). — Режим доступа: для авторизир. пользователей

3.2. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», ИСПОЛЬЗУЕМЫХ В УЧЕБНОМ ПРОЦЕССЕ

Перечень, электронных образовательных ресурсов, условия доступа к учебной литературе, профильным периодическим изданиям, к сетям Интернет.

Таблица 3.2 – Описание информационных ресурсов необходимых для освоения дисциплины

№	Адрес сайта и его описание	Перечень материалов представленных на сайте
1.	https://lib.sevsu.ru/xmlui/	Репозиторий eSevSUIR (Electronic Sevastopol State University Institutional Repository)
2.	https://e.lanbook.com/	ЭБС Лань
	http://new.znanium.com/	ЭБС Znanium
	https://urait.ru/	ЭБС Юрайт
	http://www.iprbookshop.ru/	ЭБС IPRBook
3.	http://www.garant.ru	Информационно-правовой портал ГАРАНТ
4.	http://www.consultant.ru/	Информационно-правовой портал КонсультантПлюс

3.3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММЫ

Доступная обучающимся и работникам СевГУ Электронная информационно-образовательная среда СевГУ включает в себя личные кабинеты обучающихся (https://lk.sevsu.ru), Информационную систему электронного обучения и дистанционных образовательных технологий (https://do.sevsu.ru/), официальный сайт СевГУ (https://www.sevsu.ru), сайт библиотеки СевГУ (https://lib.sevsu.ru/) и другие ресурсы.

3.4. КАДРОВОЕ ОБЕСПЕЧЕНИЕ

Дополнительной профессиональная программа повышения квалификации «Противодействие преступлениям, совершаемым с использованием современных информационно-коммуникационных технологий»

№ п/п	Дисциплина (модуль), предмет	Характеристика педагогических работников							
		Фамилия, имя, отчество, должность	Образование (наименование образовательного учреждения, наименование специальности, программы обучения)	Ученая степень, ученое (почетное) звание	Стаж работы			Основное место работы, должность	Условия привлечения к педагогической деятельности
					Всего	в т. ч. педагогической работы			
						всего	в т. ч. по указанному предмету		
1	Раздел 1-5	Ожиганова Марина Ивановна	АНО ДПО ЦПК «АИС», Информационная безопасность (профессиональная переподготовка), 2016 г. СНУЯЭиП, квалификация Научный сотрудник в области вычисления компьютерных систем эколого-экономического мониторинга (магистратура), 2009 г.	к.т.н., доцент	33	20	16	СевГУ, заведующий кафедрой «Информационная безопасность»	Штатный сотрудник

2	Раздел 6	Егорова Анастасия Олеговна	РГЭУ (РИНХ), направление подготовки 10.06.01 Информационная безопасность (аспирантура), 2024 г		9,5	8,5	8,5	СевГУ, старший преподаватель кафедры «Информационная безопасность»	Штатный сотрудник

Для реализации программы возможно привлечение других преподавателей Севастопольского государственного университета, а также внешних приглашенных специалистов-практиков.

- Слушатели, успешно прошедшие итоговую аттестацию, получают **удостоверение о повышении квалификации** установленного образца.

5. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК ПРОГРАММЫ

День	Дата	Наименование разделов, модулей, тем	Виды учебной работы и формы контроля	Ак. Чч	Преподаватель
1	[Дата]	**Раздел 1. Правовые и криминологические основы**		**8**	Ожиганова М.И.
		Раздел 1. Понятие юридической ответственности в области компьютерной безопасности	Лекция	4	
			Самостоятельная работа: изучение нормативной базы	2	
		Раздел 2. Криминалистическая и криминологическая характеристика компьютерных преступлений	Лекция	2	
2	[Дата]	**Продолжение Раздел 1.**		**8**	Ожиганова М.И.

День	Дата	Наименование разделов, модулей, тем	Виды учебной работы и формы контроля	Ак. Чч	Преподаватель
		Раздел 2. (Практикум). Способы совершения и квалификация киберпреступлений	Практическое занятие (разбор кейсов, задач)	4	Ожиганова М.И.
			Самостоятельная работа: решение задач по квалификации	4	
3	[Дата]	**Раздел 2. Тактика и методика расследования**		**8**	Ожиганова М.И.
		Раздел 3. Проведение ОРМ и следственных действий при обнаружении компьютерных инцидентов	Лекция с элементами демонстрации	4	
		Раздел 4. Характеристика инструментальных модулей для обнаружения цифровых следов	Лекция	2	

День	Дата	Наименование разделов, модулей, тем	Виды учебной работы и формы контроля	Ак. Чч	Преподаватель
			Самостоятельная работа: конспектирование, подготовка к практикуму	2	
4	[Дата]	**Раздел 3. Специальные познания и экспертиза**		**8**	Ожиганова М.И.
		Раздел 5. Судебно-экспертное исследование компьютерных средств и систем	Лекция-семинар с приглашенным экспертом (при наличии)	4	
		Практикум по Разделам 2 и 3. Решение ситуационных задач по тактике осмотра и назначению экспертиз	Практическое занятие	2	
			Самостоятельная работа: подготовка проекта постановления о назначении экспертизы	2	

День	Дата	Наименование разделов, модулей, тем	Виды учебной работы и формы контроля	Ак. Чч	Преподаватель
5	[Дата]	**Раздел 4. Технологии защиты и предупреждения**		**8**	Егорова А.О.
		Раздел 6. Предотвращение компьютерных преступлений в сфере высоких технологий	Практические занятия в компьютерном классе: • Криптография и ЭЦП (2 ч.) • Политика безопасности и МЭ (4 ч.)	6	
			Самостоятельная работа: подготовка памятки по информационной безопасности	2	
6	[Дата]	**ИТОГОВАЯ АТТЕСТАЦИЯ**		**2**	Аттестационная комиссия
		Консультация перед аттестацией	Консультация	1	Руководитель программы
		Итоговая аттестация (дифференцированный зачет)	Компьютерное тестирование и решение комплексного кейса	1	

День	Дата	Наименование разделов, модулей, тем	Виды учебной работы и формы контроля	Ак. Чч	Преподаватель
		Итого по программе:		**42**	

6. СОСТАВИТЕЛЬ ПРОГРАММЫ

Ожиганова Марина Ивановна, кандидат технических наук, доцент, заведующая кафедрой «Информационная безопасность» Института информационных технологий СевГУ.