**МИНИCTEPCTBO НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ**

**РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Федеральное государственное автономное образовательное учреждение высшего образования**

**«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»**

«УТВЕРЖДАЮ»

и.о. проректора по учебной работе,

заместитель проректора

Мезенцева О.С.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

«\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_2020 г.

**Паспорт дополнительной профессиональной программы**

**повышения квалификации**

**«Противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий»**

|  |  |  |
| --- | --- | --- |
| Объём занятий: | Всего: | - 72 часа |
|  | в.т.ч.: лекций | - 26 часов |
|  | практические занятия | - 24 часов |
|  | самостоятельная работа | - 20 часа |
|  | Тестирование | - 2 часа |

|  |  |
| --- | --- |
|  | РАЗРАБОТАНО  Руководитель программы    \_\_\_\_\_\_\_\_\_\_\_ Березницкий А.С.  «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_ 2020 г. |

Ставрополь, 2020 г

**«Противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий»**

|  |  |
| --- | --- |
| **Версия программы** | **1** |
| **Дата Версии** | **14.10.2020** |

1. **Сведения о Провайдере**

|  |  |  |
| --- | --- | --- |
| 1.1 | Провайдер | **ФГАОУ ВО «Северо-Кавказский федеральный университет»** |
| 1.2 | Логотип образовательной организации |  |
| 1.3 | Провайдер ИНН | 2635014955 |
| 1.4 | Ответственный за программу ФИО | **Огур Максим Геннадьевич** |
| 1.5 | Ответственный должность | **Старший преподаватель кафедры прикладной математики и компьютерной безопасности института математики и информационных технологий имени профессора Н.И. Червякова Северо-Кавказского федерального университета** |
| 1.6 | Ответственный Телефон | **+79887091810** |
| 1.7 | Ответственный Е-mail | [**mogur@ncfu.ru**](mailto:mogur@ncfu.ru)  **ogur26@gmail.com** |

1. **Основные Данные**

|  |  |  |
| --- | --- | --- |
| **№** | **Название** | **Описание** |
| 2.1 | Название программы | **Противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий** |
| 2.2 | Ссылка на страницу программы | [**https://el.ncfu.ru/course/view.php?id=1413**](https://el.ncfu.ru/course/view.php?id=1413)  [**https://www.ncfu.ru/education/dop-prof/proekt-cifrovoi-sertifikat/**](https://www.ncfu.ru/education/dop-prof/proekt-cifrovoi-sertifikat/)  **https://www.ncfu.ru/education/dop-prof/proekt-cifrovoi-sertifikat/Protivodeistvie-prestupleniyam-soveraemym-s-ispol\_zovaniem-informacionno-telekommunikacionnyh-tehnologii/#** |
| 2.3 | Формат обучения | **Онлайн** |
| 2.4 | Подтверждение от ОО наличия возможности реализации образовательной программы с применением электронного обучения и (или) дистанционных образовательных технологий с возможностью передачи данных в форме элементов цифрового следа | **Есть** |
| 2.5 | Уровень сложности | **Базовый/Продвинутый** |
| 2.6 | Количество академических часов | **72** |
| 2.7 | Практикоориентированный характер образовательной программы: не менее 50 % трудоёмкости учебной деятельности отведено практическим занятиям и (или) выполнению практических заданий в режиме самостоятельной работы (кол-во академических часов) | **26 часов выделено на выполнение практических и семинарских занятий,**  **20 часов выделено на выполнение практических заданий в режиме самостоятельной работы.** |
| 2.8 | Стоимость обучения одного обучающегося по образовательной программе, а также предоставление ссылок на 3 (три) аналогичные образовательные программы иных организаций, осуществляющих обучение, для оценки объективности стоимости или обоснование уникальности представленной образовательной программы в случае отсутствия аналогичных образовательных программ на рынке образовательных услуг | **30 000 (тридцать тысяч ) рублей 00 коп.**  **Аналогичные программы:**  [**https://www.infosystems.ru/courses/avtorskie\_kursy/**](https://www.infosystems.ru/courses/avtorskie_kursy/)  **kompyuternaya\_kriminalistika/**  (32 ак. часа, стоимость 49000 руб.)  [**https://itsecurity.ru/catalog/bt16/**](https://itsecurity.ru/catalog/bt16/)  (40 ак. часов, стоимость 59500 руб.)  [**https://tu-ugmk.com/study/corporate/prochee/informatsionnye-tekhnologii/digital-forensics-analyst/**](https://tu-ugmk.com/study/corporate/prochee/informatsionnye-tekhnologii/digital-forensics-analyst/)  (40 ак. часов, стоимость 72000 руб.) |
| 2.9 | Минимальное количество человек на курсе | **1** |
| 2.10 | Максимальное количество человек на курсе | **300** |
| 2.11 | Данные о количестве слушателей, ранее успешно прошедших обучение по образовательной программе | **Программа на платформе 20.35 реализуется впервые**  **Очное обучение по аналогичной программе у провайдера ФГАОУ ВО «Северо-Кавказский федеральный университет» прошли более 40 человек (Слушатели из числа студентов ФГАОУ ВО СКФУ и ГУ МВД России по Ставропольскому краю)** |
| 2.12 | Формы аттестации | **Компьютерное тестирование** |
| 2.13 | Указание на область реализации компетенций цифровой экономики, к которой в большей степени относится образовательная программа, в соответствии с Перечнем областей | **Кибербезопасность и защита данных** |

1. **Аннотация программы**

«Противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий» – практико-ориентированная дополнительная профессиональная программа повышения квалификации, нацелена на формирование практических умений, навыков и (или) приобретение опыта, необходимого для выполнения вида профессиональной деятельности №06.032 «Защита информации в компьютерных системах и сетях», конкретного самостоятельного вида деятельности при соответствии требованиям работодателя, либо осуществление работы по укрупненной группе специальностей «Информационная безопасность» наряду с основным видом деятельности в области цифровой экономики и соответствует области «Кибербезопасность и защита данных».

Программа соответствует действующему законодательству РФ (Федеральному закону «Об образовании в Российской Федерации» от 29.12.2012 N 273-ФЗ (актуальная редакция), Приказу Министерства образования и науки Российской Федерации (Минобрнауки России) от 1 июля 2013 г. № 499 г. Москва «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам», Приказом Министерства образования и науки РФ от 23 августа 2017 г. № 816 «Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»).

Программа соответствует профессиональному стандарту №842 «Специалист по безопасности компьютерных систем и сетей».

**Цель реализации программы**

Целью реализации программы является обучение основным навыкам современных технологий поиска, фиксации, анализа и документирования следов компьютерных преступлений, правонарушений и инцидентов, совершаемых с использованием информационно-телекоммуникационных технологий, прочное усвоение слушателями фундаментальных основ современных технологий цифровой криминалистики, поиска цифровых доказательств и обеспечения кибербезопасности, практики применения данных технологий, а также совершенствование умений и навыков слушателей с учетом специализации их профессиональной деятельности, повышения профессионального уровня в рамках имеющейся квалификации.

**Требования к уровню образования и (или) квалификации обучающегося:**

Необходимо наличие среднего профессионального или высшего образования по группам направлений и специальностей из списка:

* 02.00.00 – Компьютерные и информационные науки;
* 09.00.00 – Информатика и вычислительная техника;
* 10.00.00 – Информационная безопасность.

**МИНИCTEPCTBO НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ**

**РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Федеральное государственное автономное образовательное учреждение высшего образования**

**«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»**

«УТВЕРЖДАЮ»

и.о. проректора по учебной работе

Мезенцева О.С.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

«\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_2020 г.

**Дополнительная профессиональная программа**

**повышения квалификации**

**«Противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий»**

|  |  |  |
| --- | --- | --- |
| Объём занятий: | Всего: | - 72 часа |
|  | в т.ч.: лекций | - 26 часов |
|  | практические занятия | - 24 часа |
|  | самостоятельная работа | - 20 часов |
|  | Тестирование | - 2 часа |

|  |  |
| --- | --- |
| СОГЛАСОВАНО  Зав. кафедрой прикладной математики и компьютерной безопасности  \_\_\_\_\_\_\_\_\_\_\_\_\_ Тебуева Ф.Б.  «\_\_\_»\_\_\_\_\_\_\_\_\_\_ 2020 г. | РАЗРАБОТАНО  Руководитель программы    \_\_\_\_\_\_\_\_\_\_\_ Березницкий А.С.  «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_ 2020 г. |

СОГЛАСОВАНО

И.о. директора института математики

и информационных технологий

имени профессора Н.И. Червякова

\_\_\_\_\_\_\_\_\_\_\_\_\_ Петренко В.И.

«\_\_\_»\_\_\_\_\_\_\_\_\_\_ 2020 г.

СОГЛАСОВАНО

Начальник УДОПК СКФУ

\_\_\_\_\_\_\_\_\_\_\_\_\_ Федотова Н.Н.

«\_\_\_»\_\_\_\_\_\_\_\_\_\_ 2020 г.

Ставрополь, 2020 г

**Общее описание программы**

1. **Цель реализации программы**

Целью реализации программы является обучение основным навыкам современных технологий поиска, фиксации, анализа и документирования следов компьютерных преступлений, правонарушений и инцидентов, совершаемых с использованием информационно-телекоммуникационных технологий, прочное усвоение слушателями фундаментальных основ современных технологий цифровой криминалистики, поиска цифровых доказательств и обеспечения кибербезопасности, практики применения данных технологий, а также совершенствование умений и навыков слушателей с учетом специализации их профессиональной деятельности, повышения профессионального уровня в рамках имеющейся квалификации.

«Противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий» – практико-ориентированная дополнительная профессиональная программа повышения квалификации, нацелена на формирование практических умений, навыков и (или) приобретение опыта, необходимого для выполнения вида профессиональной деятельности №06.032 «Защита информации в компьютерных системах и сетях», конкретного самостоятельного вида деятельности при соответствии требованиям работодателя, либо осуществление работы по укрупненной группе специальностей «Информационная безопасность» наряду с основным видом деятельности в области цифровой экономики и соответствует области «Кибербезопасность и защита данных».

Программа соответствует действующему законодательству РФ (Федеральному закону «Об образовании в Российской Федерации» от 29.12.2012 N 273-ФЗ (актуальная редакция), Приказу Министерства образования и науки Российской Федерации (Минобрнауки России) от 1 июля 2013 г. № 499 г. Москва «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам», Приказом Министерства образования и науки РФ от 23 августа 2017 г. № 816 «Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»).

Программа соответствует профессиональному стандарту №842 «Специалист по безопасности компьютерных систем и сетей».

1. **Планируемые результаты обучения**

|  |  |
| --- | --- |
| Наименование компетенции | ПСК-7.1 – способность использовать современные технологии поиска, фиксации, анализа и документирования следов компьютерных преступлений, правонарушений и инцидентов.  ПСК-7.2 – способность проводить экспертизу вычислительной техники и носителей компьютерной информации.  ПСК-7.3 –способность руководствоваться в своей работе законодательной базой и требованиями, предъявляемыми к работе привлекаемого эксперта при проведении следственных и судебных действий.  ПСК-7.4 – Способность подготавливать научно-технические экспертные заключения по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных преступлений и инцидентов. |
| Указание типа компетенции | Профессионально-специализированная |
| Определение, содержание и основные сущностные характеристики компетенции | Получение навыков современных технологий поиска, фиксации, анализа и документирования следов компьютерных преступлений, правонарушений и инцидентов, совершаемых с использованием информационно-телекоммуникационных технологий, прочное усвоение фундаментальных основ современных технологий цифровой криминалистики, поиска цифровых доказательств и обеспечения кибербезопасности, практики применения данных технологий, а также совершенствование умений и навыков слушателей с учетом специализации их профессиональной деятельности, повышения профессионального уровня в рамках имеющейся квалификации. |
| Дескриптор знаний, умений и навыков по уровням | ПСК-7.1:  Знать:  современные технологии поиска, фиксации, анализа и документирования следов компьютерных преступлений, правонарушений и инцидентов.  Уметь:  использовать современные технологии поиска, фиксации, анализа и документирования следов компьютерных преступлений, правонарушений и инцидентов.  Владеть:  способностью использовать современные технологии поиска, фиксации, анализа и документирования следов компьютерных преступлений, правонарушений и инцидентов.  ПСК-7.2:  Знать:  правила проведения экспертизы вычислительной техники и носителей компьютерной информации.  Уметь:  проводить экспертизу вычислительной техники и носителей компьютерной информации.  Владеть:  способностью проводить экспертизу вычислительной техники и носителей компьютерной информации.  ПСК-7.3:  Знать:  законодательную базу и требования, предъявляемые к работе при проведении следственных и судебных действий.  Уметь:  руководствоваться в своей работе законодательной базой и требованиями, предъявляемыми к работе при проведении следственных и судебных действий.  Владеть:  способностью руководствоваться в своей работе законодательной базой и требованиями, предъявляемыми к работе привлекаемого эксперта при проведении следственных и судебных действий  ПСК-7.4:  Знать:  правила подготовки научно-технических экспертных заключений по результатам выполненных работ по информационно-аналитической и технической экспертизе преступлений и инцидентов, совершаемых с использованием информационно-телекоммуникационных технологий.  Уметь:  подготавливать научно-технические экспертные заключения по результатам выполненных работ по информационно-аналитической и технической экспертизе преступлений и инцидентов, совершаемых с использованием информационно-телекоммуникационных технологий.  Владеть:  способностью подготавливать научно-технические экспертные заключения по результатам выполненных работ по информационно-аналитической и технической экспертизе преступлений и инцидентов, совершаемых с использованием информационно-телекоммуникационных технологий. |
| Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | ОПК-8 - способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач.  ОПК-9 - способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации. |
| Средства и технологии оценки | Тесты, кейс-тесты. |

1. **Категория слушателей:**

Лица со средним профессиональным и/или высшим образованием, не получающие пенсионные выплаты.

Требований к квалификации нет.

Требований к наличию опыта профессиональной деятельности нет.

Базовые знания в области информатики и информационных технологий

1. **Учебный план программы Противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№**  **п/п** | **Наименование модулей, тем** | **Всего**  **часов** | **В том числе** | | | **Форма проведения занятий** |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| 1 | Входное анкетирование, тестирование, диагностика | 2 | 0 | 2 | 0 | Компьютерное тестирование |
| 2 | Представление программы | 6 | 2 | 2 | 2 | Вебинар |
| 3 | Цифровая криминалистика и её значение для расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. | 10 | 4 | 4 | 2 | Вебинар |
| 4 | Цифровая криминалистика как фактор защиты цифровой экономики | 12 | 4 | 4 | 4 | Вебинар |
| 5 | Технические аспекты квалификации преступлений, совершаемых с использованием информационно-телекоммуникационных технологий и цифровые доказательства | 12 | 4 | 4 | 4 | Вебинар |
| 6 | Нормативные и правовые акты, регламентирующие деятельность эксперта по компьютерной криминалистике | 12 | 4 | 4 | 4 | Вебинар |
| 7 | Правила осмотра места происшествия | 10 | 4 | 4 | 2 | Вебинар |
| 8 | Проблемы при расследовании преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. | 6 | 2 | 2 | 2 | Вебинар |
| 9 | Предупреждение преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. | 4 | 2 | 2 | 0 | Вебинар |
| 10 | Итоговая диагностика | 2 | 0 | 2 | 0 | Тестирование |
|  | **Всего** | **72** | **26** | **26** | **20** |  |

1. **Календарный план-график программы Менеджмент инцидентов кибербезопасности**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование учебных модулей** | **Трудоёмкость (час)** | **Сроки обучения** |
| 1 | Входное анкетирование, тестирование, диагностика | 2 | 02.11.2020 |
| 2 | Представление программы | 6 | 02.11.2020 |
| 3 | Цифровая криминалистика и её значение для расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. | 10 | 02.11.2020 - 03.11.2020 |
| 4 | Цифровая криминалистика как фактор защиты цифровой экономики | 12 | 03.11.2020 -  04.11.2020 |
| 5 | Технические аспекты квалификации преступлений, совершаемых с использованием информационно-телекоммуникационных технологий и цифровые доказательства | 12 | 05.11.2020 -  06.11.2020 |
| 6 | Нормативные и правовые акты, регламентирующие деятельность эксперта по компьютерной криминалистике | 12 | 09.11.2020 -  10.11.2020 |
| 7 | Правила осмотра места происшествия | 10 | 11.11.2020-12.11.2020 |
| 8 | Проблемы при расследовании преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. | 6 | 12.11.2020-13.11.2020 |
| 9 | Предупреждение преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. | 4 | 13.11.2020 |
| 10 | Итоговая диагностика | 2 | 13.11.2020 |
| **Всего:** | | 72 | 02.11.2020 - 13.11.2020 |

Максимальное количество человек, которые могут одновременно обучаться по образовательной программе в организации: 300

Минимальное количество человек, которые могут быть зачислены для обучения по образовательной программе: 1

1. **Учебно-тематический план программы Противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№**  **п/п** | **Наименование модулей, тем** | **Всего**  **часов** | **В том числе** | | | **Форма проведения занятий** |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| 1 | Входное анкетирование, тестирование, диагностика | 2 | 0 | 2 | 0 | Компьютерное тестирование |
| 2 | Представление программы | 6 | 2 | 2 | 2 | Вебинар |
| 3 | Цифровая криминалистика и её значение для расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. | 10 | 4 | 4 | 2 | Вебинар |
| 4 | Цифровая криминалистика как фактор защиты цифровой экономики | 12 | 4 | 4 | 4 | Вебинар |
| 5 | Технические аспекты квалификации преступлений, совершаемых с использованием информационно-телекоммуникационных технологий и цифровые доказательства | 12 | 4 | 4 | 4 | Вебинар |
| 6 | Нормативные и правовые акты, регламентирующие деятельность эксперта по компьютерной криминалистике | 12 | 4 | 4 | 4 | Вебинар |
| 7 | Правила осмотра места происшествия | 10 | 4 | 4 | 2 | Вебинар |
| 8 | Проблемы при расследовании преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. | 6 | 2 | 2 | 2 | Вебинар |
| 9 | Предупреждение преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. | 4 | 2 | 2 | 0 | Вебинар |
| 10 | Итоговая диагностика | 2 | 0 | 2 | 0 | Тестирование |
|  | **Всего** | **72** | **26** | **26** | **20** |  |

1. **Учебная (рабочая) программа повышения квалификации Противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий**

Модуль 1 – Цифровая криминалистика и её значение для расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

Модуль 2 – Цифровая криминалистика как фактор защиты цифровой экономики.

Модуль 3 – Технические аспекты квалификации преступлений, совершаемых с использованием информационно-телекоммуникационных технологий и цифровые доказательства.

Модуль 4 – Нормативные и правовые акты, регламентирующие деятельность эксперта по компьютерной криминалистике.

Модуль 5 – Правила осмотра места происшествия.

Модуль 6 – Проблемы при расследовании преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

Модуль 7 – Предупреждение преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

**Описание практико-ориентированных заданий и кейсов**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Номер темы/модуля** | **Наименование практического занятия** | **Описание** |
| **1** | **1** | Цифровая криминалистика и её значение для расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. | Изучение основных понятий цифровой криминалистики (форензики) |
| **2** | **2** | Цифровая криминалистика как фактор защиты цифровой экономики | Изучение основных форм, процедур и инструментов защиты цифровой экономики |
| **3** | **3** | Технические аспекты квалификации преступлений, совершаемых с использованием информационно-телекоммуникационных технологий и цифровые доказательства | Изучение основных аспектов квалификации преступлений, совершаемых с использованием информационно-телекоммуникационных технологий и цифровые доказательства |
| **4** | **4** | Нормативные и правовые акты, регламентирующие деятельность эксперта по компьютерной криминалистике | Изучение нормативных и правовых актов, регламентирующих деятельность эксперта по компьютерной криминалистике |
| **5** | **5** | Правила осмотра места происшествия | Изучение основных правил и технологий осмотра места происшествия |
| **6** | **6** | Проблемы при расследовании преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. | Изучение проблем, возникающих при расследовании преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. |
| **7** | **7** | Предупреждение преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. | Изучение основных технологий, процедур и инструментов предупреждения преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. |

**8.Оценочные материалы по образовательной программе**

**8.1. Вопросы тестирования по модулям**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ модуля** | **Вопросы входного тестирования** | **Вопросы промежуточного тестирования** | **Вопросы итогового тестирования** |
| **1** | S: Базовые принципы информационной безопасности:  -: Целостность данных  +: Конфиденциальность информации и, одновременно, ее доступность для всех авторизованных пользователей  -: Доступность для всех пользователей в сети Интернет | S: Базовые принципы информационной безопасности:  -: Целостность данных  +: Конфиденциальность информации и, одновременно, ее доступность для всех авторизованных пользователей  -: Доступность для всех пользователей в сети Интернет | S: Базовые принципы информационной безопасности:  -: Целостность данных  +: Конфиденциальность информации и, одновременно, ее доступность для всех авторизованных пользователей  -: Доступность для всех пользователей в сети Интернет |
| **2** | S: Компьютерные преступления – это  +: Предусмотренные уголовным кодексом общественно опасные действия, в которых информация является объектом преступного посягательства  -: Представляет собой любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку данных или передачу данных  -: Процесс внедрения вредоносной программы с целью нарушения работы ПК. | S: Компьютерные преступления – это  +: Предусмотренные уголовным кодексом общественно опасные действия, в которых информация является объектом преступного посягательства  -: Представляет собой любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку данных или передачу данных  -: Процесс внедрения вредоносной программы с целью нарушения работы ПК. | S: Компьютерные преступления – это  +: Предусмотренные уголовным кодексом общественно опасные действия, в которых информация является объектом преступного посягательства  -: Представляет собой любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку данных или передачу данных  -: Процесс внедрения вредоносной программы с целью нарушения работы ПК. |
| **2** | S: Хакер –  +: Лицо, совершающее систематические несанкционированные доступы в компьютерные системы и сети с целью развлечения, мошенничества или нанесения ущерба  -: Человек, который прекрасно знает компьютер и пишет хорошие программы  -: Человек, который двигает технический прогресс и используют свои знания и умения на благо человечества | S: Хакер –  +: Лицо, совершающее систематические несанкционированные доступы в компьютерные системы и сети с целью развлечения, мошенничества или нанесения ущерба  -: Человек, который прекрасно знает компьютер и пишет хорошие программы  -: Человек, который двигает технический прогресс и используют свои знания и умения на благо человечества | S: Хакер –  +: Лицо, совершающее систематические несанкционированные доступы в компьютерные системы и сети с целью развлечения, мошенничества или нанесения ущерба  -: Человек, который прекрасно знает компьютер и пишет хорошие программы  -: Человек, который двигает технический прогресс и используют свои знания и умения на благо человечества |
| **2** | S: Временная бомба –  +: Разновидность “логической бомбы”, которая срабатывает по достижении определенного момента времени  -: Состоит в тайном введении в чужую программу таких команд, которые позволяют осуществлять новые, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность | S: Временная бомба –  +: Разновидность “логической бомбы”, которая срабатывает по достижении определенного момента времени  -: Состоит в тайном введении в чужую программу таких команд, которые позволяют осуществлять новые, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность | S: Временная бомба –  +: Разновидность “логической бомбы”, которая срабатывает по достижении определенного момента времени  -: Состоит в тайном введении в чужую программу таких команд, которые позволяют осуществлять новые, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность |
| **3** | S: Методические документы определяют  +: Основные процессы и этапы работ по разработке политик менеджмента инцидентов кибербезопасности  -: Набор правил  -: Систему разработки ИС  -: Технологию проектирования ИС | S: Методические документы определяют  +: Основные процессы и этапы работ по разработке политик менеджмента инцидентов кибербезопасности  -: Набор правил  -: Систему разработки ИС  -: Технологию проектирования ИС | S: Методические документы определяют  +: Основные процессы и этапы работ по разработке политик менеджмента инцидентов кибербезопасности  -: Набор правил  -: Систему разработки ИС  -: Технологию проектирования ИС |
| **3** | S: Подделка компьютерной информации – это  -: Подделка выходной информации компьютеров с целью имитации работоспособности больших систем, составной частью которых является компьютер  -: Подделка выходной информации компьютеров загруженной из Китая  +: Подделка выходной информации с целью замести следы присутствия в сети, составной частью которых является компьютер | S: Подделка компьютерной информации – это  -: Подделка выходной информации компьютеров с целью имитации работоспособности больших систем, составной частью которых является компьютер  -: Подделка выходной информации компьютеров загруженной из Китая  +: Подделка выходной информации с целью замести следы присутствия в сети, составной частью которых является компьютер | S: Подделка компьютерной информации – это  -: Подделка выходной информации компьютеров с целью имитации работоспособности больших систем, составной частью которых является компьютер  -: Подделка выходной информации компьютеров загруженной из Китая  +: Подделка выходной информации с целью замести следы присутствия в сети, составной частью которых является компьютер |
| **3** | S: asynchronous attack – это  -: Состоит в смешивании и одновременном выполнении компьютерной системой команд двух или нескольких пользователей  +: Разновидность логической бомбы, которая срабатывает при достижении определенного момента времени  -: Используется как для анализа процессов, в которые преступники хотят вмешаться, так и для планирования методов совершения преступления. Таким образом, осуществляется "оптимизация" способа совершения преступления | S: asynchronous attack – это  -: Состоит в смешивании и одновременном выполнении компьютерной системой команд двух или нескольких пользователей  +: Разновидность логической бомбы, которая срабатывает при достижении определенного момента времени  -: Используется как для анализа процессов, в которые преступники хотят вмешаться, так и для планирования методов совершения преступления. Таким образом, осуществляется "оптимизация" способа совершения преступления | S: asynchronous attack – это  -: Состоит в смешивании и одновременном выполнении компьютерной системой команд двух или нескольких пользователей  +: Разновидность логической бомбы, которая срабатывает при достижении определенного момента времени  -: Используется как для анализа процессов, в которые преступники хотят вмешаться, так и для планирования методов совершения преступления. Таким образом, осуществляется "оптимизация" способа совершения преступления |
| **4** | S: Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц это:  -: Уничтожение информации  +: Распространение информации  -: Предоставление информации  -: Конфиденциальность информации  -: Доступ к информации | S: Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц это:  -: Уничтожение информации  +: Распространение информации  -: Предоставление информации  -: Конфиденциальность информации  -: Доступ к информации | S: Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц это:  -: Уничтожение информации  +: Распространение информации  -: Предоставление информации  -: Конфиденциальность информации  -: Доступ к информации |
| **4** | S: Отношения, связанные с обработкой персональных данных, регулируются законом…  -: «Об информации, информационных технологиях»  -: «О защите информации»  +: Федеральным законом «О персональных данных»  -: Федеральным законом «О конфиденциальной информации»  -: «Об утверждении перечня сведений конфиденциального характера» | S: Отношения, связанные с обработкой персональных данных, регулируются законом…  -: «Об информации, информационных технологиях»  -: «О защите информации»  +: Федеральным законом «О персональных данных»  -: Федеральным законом «О конфиденциальной информации»  -: «Об утверждении перечня сведений конфиденциального характера» | S: Отношения, связанные с обработкой персональных данных, регулируются законом…  -: «Об информации, информационных технологиях»  -: «О защите информации»  +: Федеральным законом «О персональных данных»  -: Федеральным законом «О конфиденциальной информации»  -: «Об утверждении перечня сведений конфиденциального характера» |
| **4** | S: Тактическое планирование – это:  +: Среднесрочное планирование  -: Долгосрочное планирование  -: Ежедневное планирование  -: Планирование на 6 месяцев | S: Тактическое планирование – это:  +: Среднесрочное планирование  -: Долгосрочное планирование  -: Ежедневное планирование  -: Планирование на 6 месяцев | S: Тактическое планирование – это:  +: Среднесрочное планирование  -: Долгосрочное планирование  -: Ежедневное планирование  -: Планирование на 6 месяцев |
| **5** | S: Эффективная программа безопасности требует сбалансированного применения:  +: Технических и нетехнических методов  -: Контрмер и защитных механизмов  -: Физической безопасности и технических средств защиты  -: Процедур безопасности и шифрования | S: Эффективная программа безопасности требует сбалансированного применения:  +: Технических и нетехнических методов  -: Контрмер и защитных механизмов  -: Физической безопасности и технических средств защиты  -: Процедур безопасности и шифрования | S: Эффективная программа безопасности требует сбалансированного применения:  +: Технических и нетехнических методов  -: Контрмер и защитных механизмов  -: Физической безопасности и технических средств защиты  -: Процедур безопасности и шифрования |
| **5** | S: Процесс, а также результат процесса проверки некоторых обязательных параметров пользователя и, при успешности, предоставление ему определённых полномочий на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом  +: Авторизация  -: Идентификация  -: Аутентификация  -: Обезличивание  -: Деперсонализация | S: Процесс, а также результат процесса проверки некоторых обязательных параметров пользователя и, при успешности, предоставление ему определённых полномочий на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом  +: Авторизация  -: Идентификация  -: Аутентификация  -: Обезличивание  -: Деперсонализация | S: Процесс, а также результат процесса проверки некоторых обязательных параметров пользователя и, при успешности, предоставление ему определённых полномочий на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом  +: Авторизация  -: Идентификация  -: Аутентификация  -: Обезличивание  -: Деперсонализация |
| **5** | S: За правонарушения в сфере информации, информационных технологий и защиты информации данный вид наказания на сегодняшний день не предусмотрен:  -: Дисциплинарные взыскания  -: Административный штраф  -: Уголовная ответственность  -: Лишение свободы  +: Смертная казнь | S: За правонарушения в сфере информации, информационных технологий и защиты информации данный вид наказания на сегодняшний день не предусмотрен:  -: Дисциплинарные взыскания  -: Административный штраф  -: Уголовная ответственность  -: Лишение свободы  +: Смертная казнь | S: За правонарушения в сфере информации, информационных технологий и защиты информации данный вид наказания на сегодняшний день не предусмотрен:  -: Дисциплинарные взыскания  -: Административный штраф  -: Уголовная ответственность  -: Лишение свободы  +: Смертная казнь |
| **6** | S: Может ли сотрудник быть привлечен к уголовной ответственности за нарушения правил информационной безопасности предприятия:  -: Нет, только к административной ответственности  -: Нет, если это государственное предприятие  +: Да  -: Да, но только в случае, если действия сотрудника нанесли непоправимый вред  -: Да, но только в случае осознанных неправомочных действий сотрудника | S: Может ли сотрудник быть привлечен к уголовной ответственности за нарушения правил информационной безопасности предприятия:  -: Нет, только к административной ответственности  -: Нет, если это государственное предприятие  +: Да  -: Да, но только в случае, если действия сотрудника нанесли непоправимый вред  -: Да, но только в случае осознанных неправомочных действий сотрудника | S: Может ли сотрудник быть привлечен к уголовной ответственности за нарушения правил информационной безопасности предприятия:  -: Нет, только к административной ответственности  -: Нет, если это государственное предприятие  +: Да  -: Да, но только в случае, если действия сотрудника нанесли непоправимый вред  -: Да, но только в случае осознанных неправомочных действий сотрудника |
| **6** | S: Информация об уголовной ответственности за преступление в сфере компьютерной информации описана в:  -: 1 главе Уголовного кодекса  -: 5 главе Уголовного кодекса  +: 28 главе Уголовного кодекса  -: 100 главе Уголовного кодекса  -: 1000 главе Уголовного кодекса | S: Информация об уголовной ответственности за преступление в сфере компьютерной информации описана в:  -: 1 главе Уголовного кодекса  -: 5 главе Уголовного кодекса  +: 28 главе Уголовного кодекса  -: 100 главе Уголовного кодекса  -: 1000 главе Уголовного кодекса | S: Информация об уголовной ответственности за преступление в сфере компьютерной информации описана в:  -: 1 главе Уголовного кодекса  -: 5 главе Уголовного кодекса  +: 28 главе Уголовного кодекса  -: 100 главе Уголовного кодекса  -: 1000 главе Уголовного кодекса |
| **7** | S: В статье 272 уголовного кодекса говорится…  +: О неправомерном доступе к компьютерной информации  -: О создании, исполнении и распространении вредоносных программ для ЭВМ  -: О нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети  -: О преступлениях в сфере компьютерной информации  -: Об ответственности за преступления в сфере компьютерной информации | S: В статье 272 уголовного кодекса говорится…  +: О неправомерном доступе к компьютерной информации  -: О создании, исполнении и распространении вредоносных программ для ЭВМ  -: О нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети  -: О преступлениях в сфере компьютерной информации  -: Об ответственности за преступления в сфере компьютерной информации | S: В статье 272 уголовного кодекса говорится…  +: О неправомерном доступе к компьютерной информации  -: О создании, исполнении и распространении вредоносных программ для ЭВМ  -: О нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети  -: О преступлениях в сфере компьютерной информации  -: Об ответственности за преступления в сфере компьютерной информации |
| **7** | S: Информацией, составляющей государственную тайну, владеют:  +: Государство  -: Только образовательные учреждения  -: Только президиум Верховного Совета РФ  -: Граждане Российской Федерации  -: Только министерство здравоохранения | S: Информацией, составляющей государственную тайну, владеют:  +: Государство  -: Только образовательные учреждения  -: Только президиум Верховного Совета РФ  -: Граждане Российской Федерации  -: Только министерство здравоохранения | S: Информацией, составляющей государственную тайну, владеют:  +: Государство  -: Только образовательные учреждения  -: Только президиум Верховного Совета РФ  -: Граждане Российской Федерации  -: Только министерство здравоохранения |
| **7** | S: Документированная информация, доступ к которой ограничивается в соответствии с законодательством российской федерации это:  +: Конфиденциальная информация  -: Документы офера и договоров  -: Факс  -: Личный дневник  -: Законы РФ | S: Документированная информация, доступ к которой ограничивается в соответствии с законодательством российской федерации это:  +: Конфиденциальная информация  -: Документы офера и договоров  -: Факс  -: Личный дневник  -: Законы РФ | S: Документированная информация, доступ к которой ограничивается в соответствии с законодательством российской федерации это:  +: Конфиденциальная информация  -: Документы офера и договоров  -: Факс  -: Личный дневник  -: Законы РФ |

**8.2. Критерии и шкала оценки**

Промежуточная аттестация

Учебным планом предусмотрен зачет по результатам тестирования.

Рейтинговый балл, выставляемый за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

|  |  |
| --- | --- |
| Уровень выполнения контрольного задания | Рейтинговый балл (в % от максимального балла за контрольное задание) |
| Отличный | 100 |
| Хороший | 80 |
| Удовлетворительный | 60 |
| Неудовлетворительный | 0 |

**8.3. Примеры контрольных заданий по модулям или всей образовательной программе**

**Практическое занятие № 1. Представление программы**

**Цель**: изучить основной инструментарий и тренировочные площадки по форензике.

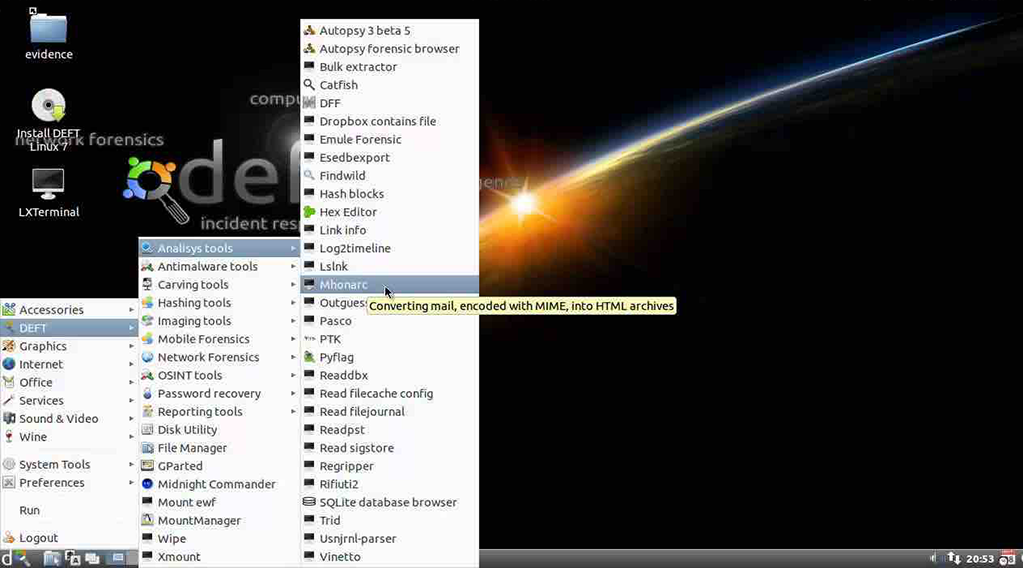
**Ход работы:**

Форензика (компьютерная криминалистика, расследование киберпреступлений) — прикладная наука о раскрытии преступлений, связанных с компьютерной информацией, об исследовании цифровых доказательств, методах поиска, получения и закрепления таких доказательств. В этой статье мы рассмотрим популярные инструменты для проведения криминалистического анализа и сбора цифровых доказательств.

Дистрибутивы

Начнем обзор утилит со специализированного дистрибутива, содержащего большинство утилит, фреймворков и средств для криминалистического анализа.

Digital Evidence & Forensics Toolkit: DEFT Linuix

Этот дистрибутив разработан на платформе Lubuntu и оснащен удобным графическим интерфейсом. Кроме того, в продукт добавлен набор профильных утилит, начиная от антивирусов, систем поиска информации в кэше браузера, сетевыми сканерами и утилитами для выявления руткитов и заканчивая инструментами, необходимыми при проведении поиска скрытых на диске данных.  
  
Основное предназначение — проведение мероприятий по форензике — анализа последствий взлома компьютерных систем, определения потерянных и скомпрометированных данных, а также для сбора т.н. цифровых доказательств совершения киберпреступлений.  
   
[www.deftlinux.net](http://www.deftlinux.net/)  
   
  
 

Фреймворки

Одним из самых популярных фреймворков является [Volatility Framework](https://github.com/volatilityfoundation/volatility) — фреймворк для исследования образов содержимого оперативной памяти и извлечения цифровых артефактов из энергозависимой памяти (RAM).  
Извлекаемые данные:

* дата и время;
* список запущенных процессов;
* список открытых сетевых сокетов;
* список открытых сетевых соединений;
* список загруженных библиотек для каждого процесса;
* имена открытых файлов для каждого процесса;
* адреса памяти;
* модули ядра ОС;
* маппинг физических смещений на виртуальные адреса.

Список поддерживаемых образов RAM для следующих операционных систем:

* 32-bit Windows XP Service Pack 2 and 3
* 32-bit Windows 2003 Server Service Pack 0, 1, 2
* 32-bit Windows Vista Service Pack 0, 1, 2
* 32-bit Windows 2008 Server Service Pack 1, 2 (there is no SP0)
* 32-bit Windows 7 Service Pack 0, 1
* 32-bit Windows 8, 8.1, and 8.1 Update 1
* 32-bit Windows 10 (initial support)
* 64-bit Windows XP Service Pack 1 and 2 (there is no SP0)
* 64-bit Windows 2003 Server Service Pack 1 and 2 (there is no SP0)
* 64-bit Windows Vista Service Pack 0, 1, 2
* 64-bit Windows 2008 Server Service Pack 1 and 2 (there is no SP0)
* 64-bit Windows 2008 R2 Server Service Pack 0 and 1
* 64-bit Windows 7 Service Pack 0 and 1
* 64-bit Windows 8, 8.1, and 8.1 Update 1
* 64-bit Windows Server 2012 and 2012 R2
* 64-bit Windows 10 (including at least 10.0.14393)
* 64-bit Windows Server 2016 (including at least 10.0.14393.0)
* 32-bit Linux kernels 2.6.11 to 4.2.3
* 64-bit Linux kernels 2.6.11 to 4.2.3
* 32-bit 10.5.x Leopard (the only 64-bit 10.5 is Server, which isn't supported)
* 32-bit 10.6.x Snow Leopard
* 64-bit 10.6.x Snow Leopard
* 32-bit 10.7.x Lion
* 64-bit 10.7.x Lion
* 64-bit 10.8.x Mountain Lion (there is no 32-bit version)
* 64-bit 10.9.x Mavericks (there is no 32-bit version)
* 64-bit 10.10.x Yosemite (there is no 32-bit version)
* 64-bit 10.11.x El Capitan (there is no 32-bit version)
* 64-bit 10.12.x Sierra (there is no 32-bit version)

Для тестирования фреймворка рекомендую воспользоваться готовыми [образами RAM](https://github.com/volatilityfoundation/volatility/wiki/Memory-Samples).  
  
[DFF](https://github.com/arxsys/dff) (Digital Forensics Framework) — фреймворк для криминалистического анализа, интерфейсы представлены как в виде командной строки, так и GUI. DFF можно использовать для исследования жестких дисков и энергозависимой памяти и создания отчетов о пользовательских и системных действиях.  
  
[PowerForensics](https://github.com/Invoke-IR/PowerForensics) предоставляет единую платформу для криминалистического анализа жестких дисков в реальном времени.  
  
[Sleuth Kit (TSK)](https://github.com/sleuthkit/sleuthkit) — это набор средств командной строки для цифровой судебной экспертизы, которые позволяют исследовать данные томов жестких дисков и файловой системы.  
  
[MIG: Mozilla InvestiGator](http://mig.mozilla.org/) — это платформа для проведения оперативных исследований на удаленных конечных точках. Фремйворк позволяет исследователям параллельно получать информацию из большого количества источников, ускоряя тем самым расследование инцидентов и обеспечение безопасности повседневных операций.  
  
[bulk\_extractor](http://downloads.digitalcorpora.org/downloads/bulk_extractor/) — позволяет извлекать информацию с помощью специальных сканеров (почта, номер кредитной карты, GPS координаты, номера телефонов, EXIF данные в изображениях). Быстрота работы достигается за счет использования многопоточности и работы с жестким диском «напрямую».  
  
[PhotoRec](http://www.cgsecurity.org/wiki/PhotoRec) — мультисистемная платформа для поиска и извлечения файлов с исследуемых образов операционных систем, компакт-дисков, карт памяти, цифровых фотокамер и т.д. Основное предназначение — извлечение удаленных (или утраченных) файлов.

Анализ сетевого взаимодействия

[SiLK (System for Internet-Level Knowledge)](https://tools.netsa.cert.org/silk/) — предназначен для эффективного сбора, хранения и анализа данных сетевого потока. SiLK идеально подходит для анализа трафика на магистрали или границе крупного, распределенного предприятия или провайдера среднего размера.  
  
[Wireshark](https://www.wireshark.org/) — этот сетевой анализатор пакетов (или сниффер) может быть эффективно использован для анализа трафика (в том числе и вредоносного). Один из популярнейших инструментов. Функциональность, которую предоставляет Wireshark, очень схожа с возможностями программы tcpdump, однако Wireshark имеет графический пользовательский интерфейс и гораздо больше возможностей по сортировке и фильтрации информации. Программа позволяет пользователю просматривать весь проходящий по сети трафик в режиме реального времени, переводя сетевую карту в неразборчивый режим (promiscuous mode).

Материал для изучения

Для того чтобы проводить те или иные действия по анализу данных необходимо иметь базис теоретического материала по расследования киберпреступлений. Для этого я рекомендую ознакомиться со следующими изданиями:

* Н.Н.Федотов: Форензика – компьютерная криминалистика
* Darren Quick, Ben Martini, Raymond Choo: Cloud Storage Forensics
* Suzanne Widup: Computer Forensics and Digital Investigation with EnCase Forensic v7
* Brian Carrier: File System Forensic Analysis
* Brett Shavers, John Bair: Hiding Behind the Keyboard: Uncovering Covert Communication Methods with Forensic Analysis
* Philip Polstra: Linux Forensics
* Jonathan Levin: Mac OS X and iOS Internals: To the Apple's Core
* Ric Messier: Operating System Forensics
* Satish Bommisetty, Rohit Tamma, Heather Mahalik: Practical Mobile Forensics
* Michael Hale Ligh, Andrew Case, Jamie Levy, AAron Walters: The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory
* Harlan Carvey: Windows Registry Forensics, Second Edition: Advanced Digital Forensic Analysis of the Windows Registry
* Laura Chappell: The Official Wireshark Certified Network Analyst Study Guide

Практические площадки

Для тестирования вышеперечисленного инструментария можно воспользоваться специализированными платформами или образами для анализа, представленными на визуализированой [mindmap](http://www.amanhardikar.com/mindmaps/ForensicChallenges.html). В качестве первых образцов для тренировки рекомендую:

* готовые [образы RAM](https://github.com/volatilityfoundation/volatility/wiki/Memory-Samples) для volatility;
* [Wireshark Sample Captures](https://wiki.wireshark.org/SampleCaptures);
* [p0wnlabs Sample Challenges](http://www.p0wnlabs.com/free/forensics).

**Заключение**

Форензика, как ответвление информационной безопасности, развита гораздо в меньшем объеме нежели тестирование на проникновение или организация защитных средств. Грамотный подход при проведении мероприятий по сбору цифровых доказательств не только даст восстановить картину возможного инцидента, но и позволит выявить пути и предпосылки возникновения инцидента.

**8.4.** **Тесты и обучающие задачи (кейсы), иные практикоориентированные формы заданий**

**Пример тестового задания по практической работе:**

**Практическое занятие № 7. Проблемы при расследовании преступлений, совершаемых с использованием информационно-телекоммуникационных технологий**

**Цель**: изучить основную проблематику при расследовании преступлений, совершаемых с использованием ИКТ.

## **Ход работы:**

**Типичные следственные ситуации первоначального этапа и следственные действия**

Типовые ситуации - наиболее часто встречающиеся ситуации расследования, предопределяющие особенности методики расследования.  
Они включают в себя типовые следственные версии, типовые задачи расследования и методы и средства их решения.

Анализ отечественного и зарубежного опыта показывает, что можно выделить **три типичные следственные ситуации:**

1. Собственник информационной системы собственными силами выявил нарушение целостности / конфиденциальности информации в системе, обнаружил виновное лицо и заявил об этом в правоохранительные органы.
2. Собственник информационной системы собственными силами выявил нарушение целостности / конфиденциальности информации в системе, не смог обнаружить виновное лицо и заявил об этом в правоохранительные органы.
3. Данные о нарушении целостности / конфиденциальности информации в информационной системе и виновном лице стали общеизвестными или непосредственно обнаружены органом дознания (например, в ходе проведения оперативно-розыскных мероприятий по другому делу).

При наличии заподозренного виновного лица первоначальная задача следствия заключается в сборе с помощью собственника информационной системы и процессуальной фиксации доказательств:

* нарушения целостности / конфиденциальности информации в системе;
* размера ущерба, причиненного нарушением целостности / конфиденциальности информации;
* причинной связи между действиями, образующими способ нарушения, и наступившими последствиями путем детализации способа нарушения целостности / конфиденциальности информации в системе и характера совершенных виновным действий;
* отношения виновного лица к совершенным действиям и наступившим последствиям.

Если преступник задержан на месте совершения преступления или сразу же после его совершения для данной ситуации характерны следующие первоначальные следственные действия:

* личный обыск задержанного;
* допрос задержанного;
* обыск по месту жительства задержанного.

К типичным следственным действиям на данной стадии можно отнести осмотр и фиксацию состояния ЭВМ, сетей ЭВМ и машинных носителей, допросы очевидцев, а также лиц, обеспечивающих работу информационной системы, в том числе должностных лиц. Важнейшим элементом работы является выемка (предпочтительно с участием специалиста) документов, в том числе на машинных носителях, фиксировавших состояние информационной системы в момент вторжения в нее злоумышленника или его программ и отражающих последствия вторжения.  
Одновременно следует принять меры к фиксации состояния рабочего места заподозренного, откуда он осуществил вторжение в информационную систему и где могут сохраняться следы его действий. Полученные в результате доказательства могут дать основания для принятия решения о привлечении лица к делу в качестве подозреваемого или сразу в качестве обвиняемого.

При отсутствии заподозренного виновного лица первоначальная задача следствия заключается в сборе доказательств:

* нарушения целостности / конфиденциальности *т*формации в системе;
* размера ущерба;
* причинной связи между действиями и наступившими последствиями.

Типичные следственные действия аналогичные первой типичной ситуации. Однако одновременно следует принять меры к поиску рабочего места заподозренного, откуда он осуществил вторжение в информационную систему.

Осуществляется поиск:

* места входа в информационную систему и способа входа в систему (с помощью должностных лиц);
* "путей следования" злоумышленника или его программы к "атакованной" системе (с помощью должностных лиц).

Такое место может находиться как у него на службе, так и дома, а также в иных местах, где установлена соответствующая аппаратура.

Круг типичных общих версий сравнительно невелик:

* преступление действительно имело место при тех обстоятельствах, которые вытекают из первичных материалов;
* ложное заявление о преступлении.

Типичными частными версиями являются:

* версии о личности преступника (ов);
* версии о местах совершения внедрения в компьютерную систему;
* версии об обстоятельствах, при которых было совершено преступление;
* версии о размерах ущерба, причиненного преступлением.

**Практические особенности отдельных следственных действий**

Осмотр и обыск (выемка) по делам данной категории являются важнейшими инструментами установления обстоятельств расследуемого события.  
Известно, что главными процессуальными способами изъятия вещественных доказательств являются осмотр, обыск и выемка.  
Следует напомнить, что осмотр -это непосредственное обнаружение, восприятие и исследование следователем материальных объектов, имеющих отношение к исследуемому событию. Обыск - следственное действие, в процессе которого производится поиск и принудительное изъятие объектов, имеющих значение для правильного решения задач уголовного судопроизводства. Выемка - следственное действие, в процессе которого производится изъятие объектов, имеющих значение для правильного решения задач уголовного судопроизводства, в тех случаях, когда их местонахождение точно известно следователю и изъятие прямо или косвенно не нарушает прав личности.  
Носители информации, имеющей отношение к расследуемому событию, могут быть с соблюдением установленного УПК РСФСР порядка изъяты и приобщены к уголовному делу в качестве вещественного доказательства. Для участия в обыске и выемке целесообразно приглашать специалиста в области компьютерной техники. При осмотрах, обысках, выемках, сопряженных с изъятием ЭВМ, машинных носителей и информации возникает ряд общих проблем, связанных со спецификой изымаемых технических средств. Так, необходимо предвидеть меры безопасности, предпринимаемые преступниками с целью уничтожения вещественных доказательств.  
Например, они могут использовать специальное оборудование, в критических случаях создающее сильное магнитное поле, стирающее магнитные записи. Известна легенда о хакере, который создал в дверном проеме магнитное поле такой силы, что оно уничтожало магнитные носители информации при выносе их из его комнаты.  
Преступник имеет возможность включить в состав программного обеспечения своей машины программу, которая заставит компьютер периодически требовать пароль, и, если несколько секунд правильный пароль не введен, данные в компьютере автоматически уничтожаются.  
Желательно иметь с собой и использовать при обыске и осмотре устройство для определения и измерения магнитных полей.  
Вещественные доказательства в виде ЭВМ, машинных носителей требуют особой аккуратности при транспортировке и хранении. Им противопоказаны резкие броски, удары, повышенные температуры, влажность. Все эти внешние факторы могут повлечь потерю данных, информации и свойств аппаратуры. Не следует забывать при осмотрах и обысках о возможностях сбора традиционных доказательств (скрытых отпечатков пальцев на клавиатуре, выключателях и др., шифрованных рукописных записей и пр.). Осмотру подлежат все устройства конкретной ЭВМ.  
Фактически оптимальный вариант изъятия ЭВМ и машинных носителей информации - это фиксация их и их конфигурации на месте обнаружения и упаковка таким образом, чтобы аппаратуру можно было бы успешно, правильно и точно так же, как на месте обнаружения, соединить в лабораторных условиях или в месте производства следствия с участием специалистов.

Указанные следственные действия могут производиться с целями:

* осмотра и изъятия ЭВМ и ее устройств;
* поиска и изъятия информации и следов воздействия на нее в ЭВМ и ее устройствах;
* поиска и изъятия информации и следов воздействия на нее вне ЭВМ.

По прибытии на место осмотра или обыска следует принять меры к обеспечению сохранности информации на находящихся здесь компьютерах и магнитных носителях. Для этого необходимо:

1. не разрешать кому бы то ни было из лиц, работающих на объекте обыска, прикасаться к работающим компьютерам, магнитным носителям, включать и выключать компьютеры;
2. самому не производить никаких манипуляций с компьютерной техникой, если результат этих манипуляций заранее не известен;
3. при наличии в помещении, где находятся СКТ и магнитные носители информации, взрывчатых, легковоспламеняющихся, токсичных и едких веществ или материалов как можно скорее удалить эти вещества в другое помещение.

**8.5. Описание процедуры оценивания результатов обучения**

Оценка «отлично» выставляется, если студент:

знает полностью: направления развития информационных (телекоммуникационных) технологий, способы и механизмы прогнозирования эффективности функционирования, оценки затрат и рисков, формирования политики безопасности объектов защиты; методики разработки систем, комплексов, средств и технологий обеспечения информационной безопасности;

умеет полностью: анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты; разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности;

владеет полностью: способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты; способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности.

Оценка «хорошо» выставляется, если студент:

знает на хорошем уровне: направления развития информационных (телекоммуникационных) технологий, способы и механизмы прогнозирования эффективности функционирования, оценки затрат и рисков, формирования политики безопасности объектов защиты; методики разработки систем, комплексов, средств и технологий обеспечения информационной безопасности;

умеет на хорошем уровне: анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты; разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности;

владеет на хорошем уровне: способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты; способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности.

Оценка «удовлетворительно» выставляется, если студент:

знает частично: направления развития информационных (телекоммуникационных) технологий, способы и механизмы прогнозирования эффективности функционирования, оценки затрат и рисков, формирования политики безопасности объектов защиты; методики разработки систем, комплексов, средств и технологий обеспечения информационной безопасности;

умеет частично: анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты; разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности;

владеет частично: способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты; способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности.

Оценка «неудовлетворительно» выставляется, если студент:

знает на недостаточном уровне: направления развития информационных (телекоммуникационных) технологий, способы и механизмы прогнозирования эффективности функционирования, оценки затрат и рисков, формирования политики безопасности объектов защиты; методики разработки систем, комплексов, средств и технологий обеспечения информационной безопасности;

умеет на недостаточном уровне: анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты; разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности;

владеет на недостаточном уровне: способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты; способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности.

**9.Организационно-педагогические условия реализации программы**

**9.1. Кадровое обеспечение программы**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№**  **п/п** | **Фамилия, имя, отчество (при наличии)** | **Место основной работы и должность, ученая степень и ученое звание (при наличии)** | **Ссылки на веб-страницы с портфолио (при наличии)** | **Фото в формате jpeg** | **Отметка о полученном согласии на обработку персональных данных** |
|  |  |  |  |  |  |
| **1** | **Березницкий Андрей Сергеевич** | Доцент, к.э.н., доцент кафедры прикладной математики и компьютерной безопасности института математики и информационных технологий имени профессора Н.И. Червякова Северо-Кавказского федерального университета,  заместитель начальника Центра -зав. отделом по производству экспертиз и экспертных исследований по делам, связанным с проявлением экстремизма ФБУ Северо-Кавказского РЦСЭ Минюста России |  |  | **Согласен** |
| **2** | **Огур Максим Геннадьевич** | Старший преподаватель кафедры прикладной математики и компьютерной безопасности института математики и информационных технологий имени профессора Н.И. Червякова Северо-Кавказского федерального университета | [**https://www.ncfu.ru/for-employee/list-of-employees/employee/12e34695-53b2-11ea-821d-0050568c7ce8/**](https://www.ncfu.ru/for-employee/list-of-employees/employee/12e34695-53b2-11ea-821d-0050568c7ce8/) |  | **Согласен** |

**9.2. Учебно-методическое обеспечение и информационное сопровождение**

|  |  |
| --- | --- |
| **Учебно-методические материалы** | |
| Методы, формы и технологии | Методические разработки,  материалы курса, учебная литература |
| Лекционные занятия. В виде изучения курса лекций | Курс лекции к программе |
| Практические занятия. Изучение методических рекомендаций по выполнению практических занятий. Выполнение индивидуальных заданий. Изучение дополнительной литературы | Методические указания к выполнению практических занятий.  Варианты индивидуальных заданий |
| Самостоятельная работа. Выполнение индивидуальных заданий для закрепления знаний | Методические указания к выполнению практических занятий.  Варианты индивидуальных заданий |
| Изучение дополнительной литературы | Основная |
| Проведение индивидуальных и групповых консультаций по практическим работам в режиме видеоконференцсвязи |  |
| 1. Просис, К. Расследование компьютерных преступлений / Крис Просис, Кевин Мандиа ; [пер. с англ. О. Труфанов]. – М.: Лори, 2013. - 476 с.: ил.d23. - ISBN 978-5-85582-314-1  2. Современные компьютерные технологии Электронный ресурс: Учебное пособие / Р. Г. Хисматов [и др.]. - Казань: Казанский национальный исследовательский технологический университет, 2014. - 83 с. - Книга находится в премиум-версии ЭБС IPR BOOKS. - ISBN 978-5-7882-1559-4 | |
| 1. Acharyulum, G.V.R.K. (2011), Information Management in a Health Care System: Knowledge Management Perspective. International Journal of Innovation, Management and Technology, Vol. 2(6), 534–537.  2. Biros, David P., Mark Weiser and John Witfield. (2007). Managing digital forensic knowledge an applied approach. Proceedings of the 5th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia. https://ro.ecu.edu.au/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsedir=1&article=1010&context=adf.  3. Brown, John Seely and Paul Duguid. (1998). Organizing Knowledge. California Management Review, Vol. 40(3), 90-111.  4. Chang, Weiping and Peifang Chung. (2014). Knowledge Management in Cybercrime Investigation – A Case Study of Identifying Cybercrime Investigation Knowledge in Taiwan. Pacific-Asia Workshop on Intelligence and Security Informatics (PAISI 2014: Intelligence and Security Informatics), pp. 8-17.  5. Chow, Peter. (2012). Surfing the Web Anonymously - The Good and Evil of the Anonymizer. SANS Institute InfoSec Reading Room. https://www.sans.org/reading-room/whitepapers/detection/surfing-webanonymously-good-evil-anonymizer-33995. Citizen Lab (n.d.). Research. https://citizenlab.ca/category/research/.  6. Cybercrime Centres of Excellence Network for Training, Research and Education. | |

|  |  |
| --- | --- |
| **Информационное сопровождение** | |
| Электронные  образовательные ресурсы | Электронные  информационные ресурсы |
| Образовательный портал Северо-Кавказского федерального университета  https://el.ncfu.ru/ | https://rvision.pro/blog-posts/upravlenie-intsidentami-informatsionnoj-bezopasnosti/ |
|  | http://docs.cntd.ru/document/1200068822 |

**9.3.Материально-технические условия реализации программы**

|  |  |
| --- | --- |
| Вид занятий | Наименование оборудования,  программного обеспечения |
| Лекции | Для слушателей - ноутбук с возможностью подключения к сети Интернет.  Со стороны университета занятия проводятся в лаборатории расследования компьютерных преступлений и инцидентов кафедры прикладной математики и компьютерной безопасности института математики и информационных технологий имени профессора Н.И. Червякова Северо-Кавказского федерального университета. |
| Практические занятия | Для слушателей - ноутбук с возможностью подключения к сети Интернет.  Со стороны университета занятия проводятся в лаборатории расследования компьютерных преступлений и инцидентов кафедры прикладной математики и компьютерной безопасности института математики и информационных технологий имени профессора Н.И. Червякова Северо-Кавказского федерального университета. |
| Самостоятельная работа | Для слушателей - ноутбук с возможностью подключения к сети Интернет.  Со стороны университета занятия проводятся в лаборатории расследования компьютерных преступлений и инцидентов кафедры прикладной математики и компьютерной безопасности института математики и информационных технологий имени профессора Н.И. Червякова Северо-Кавказского федерального университета. |

**Календарный план-график**

Дата начала обучения: 02.11.2020.

Дата завершения обучения: по согласованию: 13.11.2020.

Максимальное количество человек, которые могут одновременно обучаться по образовательной программе в организации: 300

Минимальное количество человек, которые могут быть зачислены для обучения по образовательной программе: 1

**Объем образовательной программы:** 72 ч**.** (акад. час 45 минут)

**Форма обучения:** Электронная реализация с применением дистанционных образовательных технологий, с возможностью передачи данных в форме элементов цифрового следа.

**Уровень сложности содержания образовательной программы:**

Программа может соответствовать двум уровням сложности – базовому и продвинутому уровням.

**Режим занятий:** ежедневно, 6-8 часов в день.

**Стоимость обучения:** 30 тыс. руб.

Возможные сценарии профессиональной траектории слушателей **(**по итогам освоения образовательной программы): Трудоустройство, Развитие компетенций в текущей сфере занятости, Переход в новую сферу занятости.

**Категория слушателей:** Лица со средним профессиональным и/или высшим образованием, не получающие пенсионные выплаты

**Требования к уровню образования и (или) квалификации обучающегося:**

Необходимо наличие среднего профессионального или высшего образования по группам направлений и специальностей из списка:

* 02.00.00 – Компьютерные и информационные науки;
* 09.00.00 – Информатика и вычислительная техника;
* 10.00.00 – Информационная безопасность.

**Ссылка на действующую интернет-страницу образовательной программы:**

[**https://el.ncfu.ru/course/view.php?id=1413**](https://el.ncfu.ru/course/view.php?id=1413)

[**https://www.ncfu.ru/education/dop-prof/proekt-cifrovoi-sertifikat/**](https://www.ncfu.ru/education/dop-prof/proekt-cifrovoi-sertifikat/)

[**https://www.ncfu.ru/education/dop-prof/proekt-cifrovoi-sertifikat/Protivodeistvie-prestupleniyam-soveraemym-s-ispol\_zovaniem-informacionno-telekommunikacionnyh-tehnologii/#**](https://www.ncfu.ru/education/dop-prof/proekt-cifrovoi-sertifikat/Protivodeistvie-prestupleniyam-soveraemym-s-ispol_zovaniem-informacionno-telekommunikacionnyh-tehnologii/#)

**Ссылки на 3 (три) аналогичные образовательные программы иных организаций, осуществляющих обучение:**

[**https://www.infosystems.ru/courses/avtorskie\_kursy/kompyuternaya\_kriminalistika/**](https://www.infosystems.ru/courses/avtorskie_kursy/kompyuternaya_kriminalistika/)

(32 ак. часа, стоимость 49000 руб.)

[**https://itsecurity.ru/catalog/bt16/**](https://itsecurity.ru/catalog/bt16/)

(40 ак. часов, стоимость 59500 руб.)

[**https://tu-ugmk.com/study/corporate/prochee/informatsionnye-tekhnologii/digital-forensics-analyst/**](https://tu-ugmk.com/study/corporate/prochee/informatsionnye-tekhnologii/digital-forensics-analyst/)

(40 ак. часов, стоимость 72000 руб.)

**Учебно-методические материалы**

Примеры практико-ориентированных заданий и кейсов:

1. Цифровая криминалистика и её значение для расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.
2. Цифровая криминалистика как фактор защиты цифровой экономики.
3. Технические аспекты квалификации преступлений, совершаемых с использованием информационно-телекоммуникационных технологий и цифровые доказательства.
4. Нормативные и правовые акты, регламентирующие деятельность эксперта по компьютерной криминалистике.
5. Правила осмотра места происшествия.
6. Проблемы при расследовании преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.
7. Предупреждение преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

*Методическое обеспечение:*

Методические указания к практическим занятиям по курсу «Противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий».

*Формы и технологии, применяемые при реализации программы*:

Программа реализуется с применением дистанционных образовательных технологий (ДОТ) на базе системы управления обучением СКФУ LMS Moodle, образовательного портала «Электронный Кампус СКФУ» https://ecampus.ncfii.ru (далее - еКампус), платформ Cisco WebEx, BigBlueButton, обеспечивающих поддержку контактного взаимодействия преподавателя и обучающихся в дистанционном формате.

Видом проведения итоговой аттестации (контрольное мероприятие) с применением электронного обучения, дистанционных образовательных технологий является компьютерное тестирование.

Компьютерное тестирование проводится с использованием специализированного программного обеспечения посредством сервисов системы управления обучением LMS Moodle.

### ПАСПОРТ КОМПЕТЕНЦИИ

**Дополнительная профессиональная программа**

**повышения квалификации**

**«Противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий»**

**Федеральное государственное автономное образовательное учреждение высшего образования**

**«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | Наименование компетенции | | ПСК-7.1 – способность использовать современные технологии поиска, фиксации, анализа и документирования следов компьютерных преступлений, правонарушений и инцидентов  ПСК-7.2 – способность проводить экспертизу вычислительной техники и носителей компьютерной информации  ПСК-7.3 – способность руководствоваться в своей работе законодательной базой и требованиями, предъявляемыми к работе привлекаемого эксперта при проведении следственных и судебных действий  ПСК-7.4 – способность подготавливать научно-технические экспертные заключения по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных преступлений и инцидентов | |
| 2. | **Указание типа компетенции** | Общекультурная универсальная |  | |
| Общепрофессиональная |  | |
| Профессиональная |  | |
| Профессионально-специализированная | + | |
| 3 | **Определение, содержание и основные сущностные характеристики компетенции** | | Получение навыков современных технологий поиска, фиксации, анализа и документирования следов компьютерных преступлений, правонарушений и инцидентов, совершаемых с использованием информационно-телекоммуникационных технологий, прочное усвоение фундаментальных основ современных технологий цифровой криминалистики, поиска цифровых доказательств и обеспечения кибербезопасности, практики применения данных технологий, а также совершенствование умений и навыков слушателей с учетом специализации их профессиональной деятельности, повышения профессионального уровня в рамках имеющейся квалификации. | |
| 4. | **Дескриптор знаний, умений и навыков по уровням** | | **Уровни сформированности компетенции обучающегося** | **Индикаторы** |
|  |  | | **Начальный уровень** (Компетенция недостаточно развита. Частично проявляет навыки, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается.) | ПСК-7.1:  Знать:  современные технологии поиска следов компьютерных преступлений.  Уметь:  использовать современные технологии поиска следов компьютерных преступлений.  Владеть:  способностью использовать современные технологии поиска следов компьютерных преступлений.  ПСК-7.2:  Знать:  правила проведения экспертизы вычислительной техники и носителей компьютерной информации.  Уметь:  проводить экспертизу вычислительной техники и носителей компьютерной информации.  Владеть:  способностью проводить экспертизу вычислительной техники и носителей компьютерной информации.  ПСК-7.3:  Знать:  законодательную базу и требования, предъявляемые к работе при проведении следственных и судебных действий.  Уметь:  руководствоваться в своей работе законодательной базой и требованиями, предъявляемыми к работе при проведении следственных и судебных действий.  Владеть:  способностью руководствоваться в своей работе законодательной базой и требованиями, предъявляемыми к работе привлекаемого эксперта при проведении следственных и судебных действий.  ПСК-7.4:  Знать:  правила подготовки научно-технических экспертных заключений по результатам выполненных работ по информационно-аналитической и технической экспертизе преступлений и инцидентов, совершаемых с использованием информационно-телекоммуникационных технологий.  Уметь:  подготавливать научно-технические экспертные заключения по результатам выполненных работ по информационно-аналитической и технической экспертизе преступлений и инцидентов, совершаемых с использованием информационно-телекоммуникационных технологий.  Владеть:  способностью подготавливать научно-технические экспертные заключения по результатам выполненных работ по информационно-аналитической и технической экспертизе преступлений и инцидентов, совершаемых с использованием информационно-телекоммуникационных технологий. |
|  |  | | **Базовый уровень**  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределённости, сложности.) | ПСК-7.1:  Знать:  современные технологии поиска, фиксации, анализа и документирования следов компьютерных преступлений, правонарушений и инцидентов.  Уметь:  использовать современные технологии поиска, фиксации, анализа и документирования следов компьютерных преступлений, правонарушений и инцидентов.  Владеть:  способностью использовать современные технологии поиска, фиксации, анализа и документирования следов компьютерных преступлений, правонарушений и инцидентов.  ПСК-7.2:  Знать:  правила проведения экспертизы вычислительной техники и носителей компьютерной информации.  Уметь:  проводить экспертизу вычислительной техники и носителей компьютерной информации.  Владеть:  способностью проводить экспертизу вычислительной техники и носителей компьютерной информации.  ПСК-7.3:  Знать:  законодательную базу и требования, предъявляемые к работе при проведении следственных и судебных действий.  Уметь:  руководствоваться в своей работе законодательной базой и требованиями, предъявляемыми к работе при проведении следственных и судебных действий.  Владеть:  способностью руководствоваться в своей работе законодательной базой и требованиями, предъявляемыми к работе привлекаемого эксперта при проведении следственных и судебных действий  ПСК-7.4:  Знать:  правила подготовки научно-технических экспертных заключений по результатам выполненных работ по информационно-аналитической и технической экспертизе преступлений и инцидентов, совершаемых с использованием информационно-телекоммуникационных технологий.  Уметь:  подготавливать научно-технические экспертные заключения по результатам выполненных работ по информационно-аналитической и технической экспертизе преступлений и инцидентов, совершаемых с использованием информационно-телекоммуникационных технологий.  Владеть:  способностью подготавливать научно-технические экспертные заключения по результатам выполненных работ по информационно-аналитической и технической экспертизе преступлений и инцидентов, совершаемых с использованием информационно-телекоммуникационных технологий. |
| 3. |  | | **Продвинутый**  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | ПСК-7.1:  Знать:  современные технологии поиска, фиксации, анализа и документирования следов компьютерных преступлений, правонарушений и инцидентов.  Уметь:  использовать современные технологии поиска, фиксации, анализа и документирования следов компьютерных преступлений, правонарушений и инцидентов  Владеть:  способностью использовать современные технологии поиска, фиксации, анализа и документирования следов компьютерных преступлений, правонарушений и инцидентов.  ПСК-7.2:  Знать:  правила проведения экспертизы вычислительной техники и носителей компьютерной информации.  Уметь:  проводить экспертизу вычислительной техники и носителей компьютерной информации.  Владеть:  способностью проводить экспертизу вычислительной техники и носителей компьютерной информации.  ПСК-7.3:  Знать:  законодательную базу и требования, предъявляемые к работе при проведении следственных и судебных действий.  Уметь:  Руководствоваться в своей работе законодательной базой и требованиями, предъявляемыми к работе при проведении следственных и судебных действий.  Владеть:  способностью руководствоваться в своей работе законодательной базой и требованиями, предъявляемыми к работе привлекаемого эксперта при проведении следственных и судебных действий  ПСК-7.4:  Знать:  правила подготовки научно-технических экспертных заключений по результатам выполненных работ по информационно-аналитической и технической экспертизе преступлений и инцидентов, совершаемых с использованием информационно-телекоммуникационных технологий.  Уметь:  подготавливать научно-технические экспертные заключения по результатам выполненных работ по информационно-аналитической и технической экспертизе преступлений и инцидентов, совершаемых с использованием информационно-телекоммуникационных технологий.  Владеть:  способностью подготавливать научно-технические экспертные заключения по результатам выполненных работ по информационно-аналитической и технической экспертизе преступлений и инцидентов, совершаемых с использованием информационно-телекоммуникационных технологий. |
|  |  | | **Профессиональный**  (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействую щими факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуация повышенной сложности.) | ПСК-7.1:  Знать:  современные технологии поиска, фиксации, анализа и документирования следов компьютерных преступлений, правонарушений и инцидентов.  Уметь:  использовать современные технологии поиска, фиксации, анализа и документирования следов компьютерных преступлений, правонарушений и инцидентов.  Владеть:  способностью использовать современные технологии поиска, фиксации, анализа и документирования следов компьютерных преступлений, правонарушений и инцидентов.  ПСК-7.2:  Знать:  правила проведения экспертизы вычислительной техники и носителей компьютерной информации.  Уметь:  проводить экспертизу вычислительной техники и носителей компьютерной информации.  Владеть:  способностью проводить экспертизу вычислительной техники и носителей компьютерной информации.  ПСК-7.3:  Знать:  законодательную базу и требования, предъявляемые к работе при проведении следственных и судебных действий.  Уметь:  руководствоваться в своей работе законодательной базой и требованиями, предъявляемыми к работе при проведении следственных и судебных действий.  Владеть:  способностью руководствоваться в своей работе законодательной базой и требованиями, предъявляемыми к работе привлекаемого эксперта при проведении следственных и судебных действий.  ПСК-7.4:  Знать:  правила подготовки научно-технических экспертных заключений по результатам выполненных работ по информационно-аналитической и технической экспертизе преступлений и инцидентов, совершаемых с использованием информационно-телекоммуникационных технологий.  Уметь:  подготавливать научно-технические экспертные заключения по результатам выполненных работ по информационно-аналитической и технической экспертизе преступлений и инцидентов, совершаемых с использованием информационно-телекоммуникационных технологий.  Владеть:  способностью подготавливать научно-технические экспертные заключения по результатам выполненных работ по информационно-аналитической и технической экспертизе преступлений и инцидентов, совершаемых с использованием информационно-телекоммуникационных технологий. |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | | Компетенция связана со следующими компетенциями:  ОПК-8 - способностью использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач.  ОПК-9 - способностью разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации. | |
| 6. | Средства и технологии оценки | | Тесты, кейс-тесты. | |

**VI.Иная информация о качестве и востребованности образовательной программы**

В очном формате программа была востребована для повышения квалификации сотрудников ГУ МВД России по Ставропольскому краю и Следственного Комитета по ставропольскому краю.

**V.Рекомендации к программе от работодателей**:

Программа рекомендована к реализации компаниями ООО «ЕНДС-Ставрополь», ООО «Кронвел» и ООО «Цитрикс».

Указанные организации готовы рассмотреть возможность трудоустройства слушателей, успешно прошедших обучение по данной образовательной программе.

**VI.Указание на возможные сценарии профессиональной траектории граждан**

Трудоустройство, Развитие компетенций в текущей сфере занятости, Переход в новую сферу занятости в разрезе вида профессиональной деятельности №06.032 «Защита информации в компьютерных системах и сетях», конкретного самостоятельного вида деятельности при соответствии требованиям работодателя, либо осуществление работы по укрупненной группе специальностей «Информационная безопасность»

**VII.Дополнительная информация**

**VIII.Приложенные Скан-копии**

Полная скан копия утвержденной программы в формате PDF прикреплена к пакету документов.

И.о. проректора по учебной работе,

заместитель проректора Мезенцева О.С.