Негосударственное частное образовательное учреждение высшего образования
«Технический университет УГМК»
(НЧОУ ВО «ТУ УГМК»)

УТВЕРЖДАЮ

Директор НЧОУ ВО «ТУ УГМК»

_____ В.А. Лапин
(подпись)

«25» 11 2020 г.

УТВЕРЖДАЮ

Генеральный директор
ООО «Траст»

_____ А.Е. Ефимова
(подпись)

«25» 11 2020 г.

ПРОГРАММА

повышения квалификации

«Digital Forensics Analyst / Специалист по компьютерной криминалистике»

(наименование программы)

Верхняя Пышма
2020

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Цель реализации программы:

Освоить компетенции по оперативному реагированию на кибератаки.

1.2. Планируемые результаты обучения

По окончании обучения слушатель способен:

- проводить криминалистическое исследование зараженных хостов, включая дампы памяти и сетевого трафика;
- формировать индикаторы компрометации;
- составлять отчеты для глубокого понимания всего процесса кибератаки с целью предотвращения последующих инцидентов.

Слушатель должен знать:

- технологии, инструменты, цели злоумышленников;
- артефакты ОС Windows;
- инструменты для сбора цифровых данных в рамках криминалистического исследования;
- теорию и практику захвата и анализа сетевого трафика;
- теорию и практику работы с IDS/IPS системами;
- особенности исследования для разных ОС;
- порядок исследования файлов гибернации и подкачки на предмет поиска криминалистических артефактов;
- алгоритм выявления аномалий и вредоносной активности в оперативной памяти.

Слушатель должен уметь:

- выявлять методы первичного заражения, распространения по сети, закрепления, сетевой активности вредоносного ПО;
- выявлять зараженные системы и восстанавливать хронологию заражения посредством plaso;
- проводить анализ журналов веб-сервера;
- находить и извлекать криминалистические артефакты;
- восстанавливать хронологию инцидента на основании извлеченных артефактов из сетевого трафика;
- создавать дампы оперативной памяти и специфику их анализа посредством инструментов volatility, rekall.

1.3. Требования к уровню подготовки слушателя

Технические специалисты, имеющие среднее специальное и (или) высшее профессиональное образование.

1.4. Программа разработана с учетом профессионального стандарта «Менеджер по информационным технологиям», утвержденного приказом Минтруда № 716н от 13.10.2014.

2. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. Учебный план

Наименование раздела		Трудоемкость, час	Всего, ауд. час.	в том числе, час.			СРС, час	Текущий контроль (шт.)			Промежуточная аттестация	
				лекции	лабораторные работы	прак. занятия, семинары		РК, РГР, Реф	КР	КП	Зачет	Экзамен
1		2	3	4	5	6	7	8	9	10	11	12
1.	Тенденции совершения кибератак; введение в реагирование на инциденты	7	7	0	0	7	0	0	0	0	0	0
2.	Windows Forensics	8	8	0	0	8	0	0	0	0	0	0
3.	Network Forensics	8	8	0	0	8	0	0	0	0	0	0
4.	Memory Forensics	8	8	0	0	8	0	0	0	0	0	0
5.	Практические задания с анализом образов и дампов памяти	8	8	0	0	8	0	0	0	0	0	0
Итого		**39**	**39**	**0**	**0**	**39**	**0**	**0**	**0**	**0**	**0**	**0**
Итоговая аттестация		**1**	**1**									
Всего		**40**	**40**									

2.2. Учебно-тематический план

№ п/п	Наименование раздела и тем	Трудоемкость, час	Всего, ауд. час.	в том числе, час.			СРС, час
				лекции	лабораторные работы	прак. занятия, семинары	
1	2	3	4	5	6	7	8
1.	**Тенденции совершения кибератак; Введение в реагирование на инциденты**	**7**	**7**	**0**	**0**	**7**	**0**
1.1.	Тенденции совершения киберпреступлений	1	1	0	0	1	0
1.2.	Образ современного киберпреступника – возможности, мотивации	1	1	0	0	1	0
1.3.	Цели и техники совершения кибератак	1	1	0	0	1	0
1.4.	Основы первичного реагирования на инциденты ИБ: использование моделей угроз для понимания тактик, техник и процедур атакующих. CyberKillChain	2	2	0	0	2	0
1.5.	Процесс реагирования: идентификация, локализация, формирование индикаторов, поиск новых зараженных узлов	1	1	0	0	1	0
1.6.	Сбор цифровых доказательств	1	1	0	0	1	0
2.	**Windows Forensics**	**8**	**8**	**0**	**0**	**8**	**0**
2.1.	Артефакты ОС Windows	1	1	0	0	1	0
2.2.	Инструменты для сбора цифровых данных в рамках криминалистического исследования	1	1	0	0	1	0
2.3.	Инструменты для анализа Windows-based систем	1	1	0	0	1	0
2.4.	Выявление методов первичного заражения, распространения по сети, закрепления, сетевой активности вредоносного ПО	2	2	0	0	2	0
2.5.	Выявление зараженных систем и восстановление хронологии заражения	2	2	0	0	2	0
2.6.	Практические задания для самостоятельного выполнения	1	1	0	0	1	0
3.	**Network Forensics**	**8**	**8**	**0**	**0**	**8**	**0**
3.1.	Теория и практика по захвату и анализу сетевого трафика	2	2	0	0	2	0
3.2.	Анализ журналов веб-сервера;	1	1	0	0	1	0
3.3.	Теория и практика работы с IDS/IPS системами	1	1	0	0	1	0
3.4.	Поиск и извлечение криминалистических артефактов;	2	2	0	0	2	0
3.5.	Восстановление хронологии инцидента на основании извлеченных артефактов из сетевого трафика	1	1	0	0	1	0
3.6.	Практические задания для самостоятельного выполнения	1	1	0	0	1	0
4.	**Memory Forensics**	**8**	**8**	**0**	**0**	**8**	**0**
4.1.	Строение оперативной памяти	1	1	0	0	1	0
4.2.	Создание дампов оперативной памяти и специфика их анализа	1	1	0	0	1	0

№ п/п	Наименование раздела и тем	Трудоемкость, час	Всего, ауд. час.	в том числе, час.			СРС, час
				лекции	лабораторные работы	прак. занятия, семинары	
1	2	3	4	5	6	7	8
4.3.	Особенности исследования для разных ОС	1	1	0	0	1	0
4.4.	Исследование файлов гибернации и подкачки на предмет поиска Криминалистических артефактов	2	2	0	0	2	0
4.5.	Алгоритм выявления аномалий и вредоносной активности в оперативной памяти	2	2	0	0	2	0
4.6.	Особенности исследования дампов памяти в рамках расследования различных инцидентов	1	1	0	0	1	0
4.7.	Практические задания для самостоятельного выполнения	2	2	0	0	2	0
5.	**Практические задания с анализом образов и дампов памяти**	**8**	**8**	**0**	**0**	**8**	**0**
Итого		**39**	**39**	**0**	**0**	**39**	**0**
Итоговая аттестация		**1**	**1**				
Всего		**40**	**40**				

2.3. Примерный календарный учебный график

Период обучения (дни, недели)[1)]	Наименование раздела
Первый день	Тенденции совершения кибератак; Введение в реагирование на инциденты
Второй день	Windows Forensics
Третий день	Network Forensics
Четвертый день	Memory Forensics
Пятый день	Практические задания с анализом образов и дампов памяти

[1)] Даты обучения будут определены в расписании занятий при наборе группы на обучение

2.4. Рабочие программы разделов

№, наименование темы	Содержание лекций (количество часов)	Наименование лабораторных работ (количество часов)	Наименование практических занятий или семинаров (количество часов)	Виды СРС (количество часов)
1	2	3	4	5
Раздел 1. Тенденции совершения кибератак; Введение в реагирование на инциденты (7)				
1.1.	-	-	Тенденции совершения киберпреступлений (1)	-
1.2.	-	-	Образ современного киберпреступника – возможности, мотивации (1)	-
1.3.	-	-	Цели и техники совершения кибератак (1)	-
1.4.	-	-	Основы первичного реагирования на инциденты ИБ: использование моделей угроз для понимания тактик, техник и процедур атакующих. CyberKillChain (2)	-
1.5.	-	-	Процесс реагирования: идентификация, локализация, формирование индикаторов, поиск новых зараженных узлов (1)	-
1.6.	-	-	Сбор цифровых доказательств (1)	-
Раздел 2. Windows Forensics (8)				
2.1.	-	-	Артефакты ОС Windows (1)	-
2.2.	-	-	Инструменты для сбора цифровых данных в рамках криминалистического исследования (1)	-
2.3.	-	-	Инструменты для анализа Windows-based систем (1)	-
2.4.	-	-	Выявление методов первичного заражения, распространения по сети, закрепления, сетевой активности вредоносного ПО (2)	-
2.5.	-	-	Выявление зараженных систем и восстановление хронологии заражения (2)	-
2.6.	-	-	Практические задания по криминалистике Windows (1)	-
Раздел 3. Network Forensics (8)				
3.1.	-	-	Теория и практика по захвату и анализу сетевого трафика (2)	-
3.2.	-	-	Анализ журналов веб-сервера (1)	-
3.3.	-	-	Теория и практика работы с IDS/IPS системами (1)	-
3.4.	-	-	Поиск и извлечение криминалистических артефактов (2)	-
3.5.	-	-	Восстановление хронологии инцидента на основании извлеченных артефактов из сетевого трафика (1)	-
3.6.	-	-	Практические задания по криминалистике сети (1)	-
Раздел 4. Memory Forensics (8)				
4.1.	-	-	Строение оперативной памяти (1)	-
4.2.	-	-	Создание дампов оперативной памяти и специфика их анализа (1)	-
4.3.	-	-	Особенности исследования для разных ОС (1)	-
4.4.	-	-	Исследование файлов гибернации и подкачки на предмет поиска Криминалистических артефактов (1)	-

4.5.	-	-	Алгоритм выявления аномалий и вредоносной активности в оперативной памяти (2)	-
4.6.	-	-	Особенности исследования дампов памяти в рамках расследования различных инцидентов (1)	-
4.7.	-	-	Практические задания по криминалистике памяти (1)	-
Раздел 5. Практические задания с анализом образов и дампов памяти (8)				
5.1.	-	-	Самостоятельное расследование кейса (8)	-

2.5. Оценка качества освоения программы (формы аттестации, оценочные и методические материалы).

2.5.1. Форма итоговой аттестации.

Итоговая аттестация проводится путем устного опроса результатов обобщающего практического задания.

2.5.2. Оценочные материалы

Критерии оценки уровня освоения программы.

- Минимальный уровень – соответствует оценке «удовлетворительно» и обязательный для всех слушателей по завершении освоения программы обучения.
- Базовый уровень – соответствует оценке «хорошо» и характеризуется превышением минимальных характеристик сформированности компетенции.
- Повышенный уровень – соответствует оценке «отлично» и характеризуется максимально возможной выраженностью компетенции, важен как качественный ориентир для самосовершенствования.

Оценка «зачтено» соответствует одному из уровней сформированности компетенций: минимальный, базовый, повышенный.

Оценка «не зачтено» ставится слушателю, имеющему существенные пробелы в знании основного материала по программе, а также допустившему принципиальные ошибки при изложении материала.

2.5.3. Методические материалы

Положение об итоговой аттестации слушателей по дополнительным профессиональным программам в Негосударственном частном образовательном учреждении высшего образования «Технический университет УГМК».

3. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

3.1. Материально-технические условия

Наименование специализированных учебных помещений	Вид занятий	Наименование оборудования, программного обеспечения
Аудитории ТУ УГМК	Практические занятия, семинары	- мультимедийное оборудование; - компьютеры, подключенные к сети Интернет; - интернет-браузер; - Windows 10; - 50 GB пустого места на диске; - FTK Imager; - Strawberry Perl;

		- Wireshark; - NetworkMiner; - Microsoft Excel; - .net 3.5; - аккаунт на Virus Total.

3.2. Учебно-методическое и информационное обеспечение

3.2.1. Тумбинская М.В. Защита информации на предприятии: учебное пособие / Тумбинская М.В., Петровский М.В. Санкт-Петербург: Лань, 2020 – 184 с. – ISBN 978-5-8114-4291-1: ил. – (Учебники для вузов. Специальная литература). – Текст: непосредственный // Электронно-библиотечная система «Лань»: [сайт]. — URL: https://e.lanbook.com/reader/book/130184/#182 (дата обращения: 28.07.2020). — Режим доступа: свободный.

3.3. Кадровые условия

Кадровое обеспечение программы осуществляют преподаватели-практики, имеющие опыт проведения криминалистических исследований зараженных хостов и анализа кибератак с целью предотвращения последующих инцидентов.

3.4. Условия для функционирования электронной информационно-образовательной среды:

Электронные информационные ресурсы	Вид занятий	Наименование оборудования, программного обеспечения
Система для проведения вебинаров	Практические занятия, семинары	- компьютеры, подключенные к сети Интернет; - интернет-браузер; - Windows 10; - 50 GB пустого места на диске; - FTK Imager; - Strawberry Perl; - Wireshark; - NetworkMiner; - Microsoft Excel; - .net 3.5; - аккаунт на Virus Total.

4. РУКОВОДИТЕЛЬ И СОСТАВИТЕЛИ ПРОГРАММЫ

Руководитель программы: Жуков Денис Васильевич, начальник управления ДПО НЧОУ ВО «Технический университет УГМК».

Составители программы:

1. Баринова Анастасия Владимировна, заместитель руководителя лаборатории компьютерной криминалистики по обучению, ООО «Траст»;
2. Островская Светлана Сергеевна, тренер по компьютерной криминалистике, ООО «Траст»;
3. Тыкушин Анатолий Владимирович, специалист по компьютерной криминалистике, ООО «Траст».