ORIGIN SECURITY

ДОКУМЕНТ ПОДПИСАН УСИЛЕННОЙ КВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 02cb8e660022b205bd4c8a3f1aceb57fab
Владелец: Антонов Роман Андреевич
Действителен: 08.11.2024 16:03 - 08.02.2026 16:13

УТВЕРЖДАЮ
Генеральный директор ООО
«Ориджин Секьюрити»
Р.А. Антонов
Подпись
31 января 2025 г.

Дополнительная профессиональная программа – программа повышения квалификации «Основы практической ИБ с использованием решений с открытым исходным кодом»

г. Хабаровск
2025

Оглавление

1. Цель реализации программы

Целью освоения дополнительной профессиональной программы – программы повышения квалификации «Основы практической ИБ с использованием решений с открытым исходным кодом» является подготовка специалистов по мониторингу ИБ и реагирования на компьютерные инциденты.

2. Планируемые результаты обучения

В результате освоения дисциплины обучающийся должен:

1) знать: основы инфраструктурной ИБ, методы мониторинга ИБ, методологию реагирования на компьютерные инциденты;
2) уметь: определять основные угрозы ИБ, выявлять признаки компьютерного инцидента и реагировать на него;
3) владеть: программными средствами с открытым исходным кодом для мониторинга ИБ (Security Onion и другие) и реагирования на КИ (tcpdump, wireshark и другие).

В результате освоения программы у обучающегося должны быть сформированы общекультурные, общепрофессиональные и профессиональные компетенции:

- способностью к абстрактному мышлению, анализу, синтезу (ОК-1);
- готовностью к коммуникации в устной и письменной формах для решения задач профессиональной деятельности (ОПК-1);
- способностью использовать и применять углубленные теоретические и практические знания в области информационных технологий (ОПК-2);
- способностью самостоятельно приобретать и использовать в практической деятельности новые знания и умения (ОПК-3);
- способностью управлять проектами, планировать профессиональную деятельность, анализировать риски, управлять командой проекта (ПК-1);
- способностью к углубленному анализу проблем, постановке и обоснованию задач научной и проектно-технологической деятельности (ПК-2).

3. Требования к обучающимся

Данная дополнительная профессиональная программа предназначена для лиц, имеющих высшее образование по направлению подготовки (специальности) в области технологий и технических наук.

4. Форма обучения

Программа реализуется дистанционно, с применением исключительно электронного обучения, дистанционных образовательных технологий.

5. Структура и содержание программы повышения квалификации «Основы практической ИБ с использованием решений с открытым исходным кодом»

Общая трудоемкость дисциплины составляет 45 академических часов.

Итоговая аттестация – тестирование.

№ п/п	Раздел Программы	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в ак. часах)		Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
				Л	П	
1.	Лекция 1: Инфраструктурная ИБ. Что защищаем? От кого защищаем? Как защищаем? а) Выделение критических активов и определение недопустимых событий б) Определение модели злоумышленника в) Определение политики ИБ	1	1	1		
2.	Лекция 2: Инфраструктурная ИБ. Кибергигиена а) Определение кибергигиены б) Корпоративная кибергигиена в) Личная кибергигиена	1	1	1		
3.	Лекция 3: Инфраструктурная ИБ. Угрозы информационной безопасности а) Виды угроз б) Источники угроз	1	1	2		
4.	Лекция 4: Мониторинг ИБ. Компьютерные атаки. SOC а) Типы компьютерных атак б) SOC	1	1	4		
5.	Лекция 5: Мониторинг ИБ. Источники информации а) Источники информации б) Агрегация и мониторинг	1	1	4		

	ИБ. в) Threat Intelligence. Threat Hunting					
6.	Лекция 6: Мониторинг ИБ. Инструменты для мониторинга ИБ. Security Onion. а) Инструменты для мониторинга ИБ б) Security Onion	1	1	6		
7.	Лекция 7: Реагирование на инциденты. Разновидности инцидентов. Понятие KillChain, развитие компьютерной атаки. а) Определение компьютерного инцидента б) Понятие цепочки атак, виды в) Развитие компьютерной атаки	1	1	4		
8.	Лекция 8: Реагирование на инциденты. Реагирование на КИ. Цели. Основные этапы. а) Методология реагирования на компьютерные инциденты б) Инструменты	1	2	2		
9.	Лекция 9. Реагирование на инциденты. Выявление. Индикаторы компрометации. а) Типы индикаторов компрометации б) Выявление признаков компьютерного инцидента. Инструменты	1	2	2		
10.	Лекция 10: Реагирование на инциденты. Сдерживание. Удаление. Восстановление. Выводы и перестройка системы. а) Жизненный цикл реагирования на компьютерные инциденты	1	2	1		
11.	Лекция 11: Реагирование на инциденты. Форензика. а) Определение цифровой форензики б) Типы форензики в) Инструментарий	1	2	15		
12.	Лекция 12: Реагирование на инциденты. Атрибуция. MITRE ATT&CK. а) Определение атрибуции. Методы б) MITRE ATT&CK. Альтернативы	1	2	2		
13.	Итоговая аттестация в форме тестирования	1	2	–	1	Итоговый
Итого 45 часов				**44**	**1**	

6. Календарный учебный график

Всего в периоде обучения – две учебные недели. Учебная неделя не привязана к началу или окончанию учебного и календарного года.

7. Условия реализации программы

7.1. Требования к педагогам

К реализации программы допускаются педагогические работники с высшим профессиональным (техническим) образованием и стажем работы в области защиты информации не менее 5 лет.

7.2. Материально-техническое и информационное обеспечение программы

Образовательная платформа «Fogsdemy».

Программное обеспечение и Интернет-ресурсы:

- https://rezbez.ru/;
- https://github.com/;
- https://habr.com/.

8. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Встроенная система мониторинга и оценки успеваемости на платформе «Fogsdemy».

Форма документа, выдаваемого по результатам освоения программы – удостоверение о повышении квалификации.

9. Авторы программы

Антонов Р.А. – генеральный директор.

Теплов М.Ю. – технический директор.