ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«Облачные сети»

УТВЕРЖДАЮ
Директор по развитию бизнеса

_____ К.И. Клокова
(подпись)

«03» сентября 2025 г.

Дополнительная профессиональная программа повышения квалификации

«Управление решением и инцидентами WAF»

Нормативный срок освоения программы: 16 академических часов.

Форма обучения: заочная с применением дистанционных образовательных технологий и электронного обучения

2025

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ 3
2. ЦЕЛЬ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ 3
3. УЧЕБНЫЙ ПЛАН 5
4. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК 6
5. РАБОЧИЕ ПРОГРАММЫ УЧЕБНЫХ МОДУЛЕЙ 7
6. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ 9
7. ФОРМЫ АТТЕСТАЦИИ 11
8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ 12

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Нормативно-правовые основы разработки программы

1. Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;
2. Постановление Правительства Российской Федерации от 11.10.2023 г. №1678 «Об утверждении Правил применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»;
3. Приказ Министерства науки и высшего образования Российской Федерации от 24.03.2025 № 266 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;
4. Приказ Министерства труда и социальной защиты Российской Федерации от 12 апреля 2013 г. № 148н «Об утверждении уровней квалификаций в целях разработки проектов профессиональных стандартов»;
5. Письмо Министерства образования и науки Российской Федерации от 30 марта 2015 г. № АК-821/06 «О направлении методических рекомендаций по итоговой аттестации слушателей»;
6. Письмо Министерства образования и науки Российской Федерации от 21 апреля 2015 г. № ВК-1013/06 «О направлении методических рекомендаций по реализации дополнительных профессиональных программ с использованием дистанционных образовательных технологий, электронного обучения и в сетевой форме.
7.. Профессиональный стандарт 06.033 «Специалист по защите информации в автоматизированных системах» (утвержден приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н).

1.2. Требования к слушателям

К освоению программы допускаются:
- лица, имеющие среднее профессиональное и (или) высшее образование;
- лица, получающие среднее профессиональное и (или) высшее образование.

2. ЦЕЛЬ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ.

2.1. Цель освоения программы

Цель программы «Управление решением и инцидентами WAF» – совершенствование имеющихся компетенций или получение новой компетенции, необходимой для профессиональной деятельности в области защиты веб-приложений, администрирования и эксплуатации WAF-решения, включая развертывание, настройку политик безопасности, анализ инцидентов.

2.2. Характеристика нового вида профессиональной деятельности, новой квалификации

Содержание дополнительной профессиональной программы учитывает профессиональные стандарты, указанные в разделе 1.1 настоящей программы.

Таблица №1

Код компетенции/ трудовой функции	Формируемые и (или) совершенствуемые компетенции/трудовые функции
ПК-1	Администрирование систем защиты информации автоматизированных систем.
ПК-2	Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем.

ПК-3	Установка и настройка средств защиты информации в автоматизированных системах.

В результате освоения программы слушатель будет:

Знать:

- десять наиболее критических уязвимостей веб-приложений, согласно OWASP, и методов их предотвращения;
- схемы лицензирования и развертывания решения WAF;
- как создавать и управлять изолированными пространствами для повышения безопасности;
- функции агрегации для анализа и обработки данных о трафике и событиях;

Уметь:

- эффективно использовать WSC для установки и настройки решения WAF;
- анализировать события в веб-интерфейсе решения WAF и фильтровать их по различным параметрам для более глубокого понимания происходящего;
- выполнять развертывание и первоначальную конфигурацию решения WAF;
- создавать и настраивать политики безопасности, адаптированные под конкретные требования веб-приложений;
- проводить повторное тестирование уязвимостей в защищенных приложениях;
- управлять глобальными списками и пользовательскими правилами;
- использовать REST API для автоматизации задач администрирования и интеграции с другими системами;
- настраивать мониторинг и отчетность по событиям безопасности;

Владеть навыками:

- объяснения архитектуры и компонентов решения WAF, а также их роли в обеспечении безопасности веб-приложений;
- настройки защиты веб-приложений, используя возможности решения WAF, включая балансировку нагрузки;
- разработки правил обработки трафика для защиты от различных угроз.

3. УЧЕБНЫЙ ПЛАН

Таблица №2

№	Наименования этапов/блоков/модулей	Всего часов	Лекции	Практические занятия	СРС*	Формы аттестации
Блок I						
1.	Модуль 1. Безопасность веб-приложений и архитектура решения WAF.	5,4	2,6	-	2,8	-
2.	Модуль 2. Развертывание решения WAF	3,8	2,6	-	1,2	-
Промежуточная аттестация		0,5	-	-	-	**Зачет**
Блок II						
3.	Модуль 3. Работа в решении WAF	3	1,6	1,4	-	-
4.	Модуль 4. Администрирование решения WAF	1,3	1,3	-	-	-
Итоговая аттестация		**2**	-	-	-	**Зачет**
Итого:		**16**				

* СРС – самостоятельная работа слушателя.

4. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Таблица №3

№	Наименования этапов/блоков/модулей	Неделя обучения
Блок I		
1.	Модуль 1. Безопасность веб-приложений и архитектура решения WAF.	1-я неделя
2.	Модуль 2. Развертывание решения WAF	1-я неделя
	Промежуточная аттестация	1-я неделя
Блок II		
3.	Модуль 3. Работа в решении WAF	1-я неделя
4.	Модуль 4. Администрирование решения WAF	1-я неделя
	Итоговая аттестация	1-я неделя

5. РАБОЧИЕ ПРОГРАММЫ УЧЕБНЫХ МОДУЛЕЙ

Таблица №4

№	Наименования этапов/блоков/модулей	Содержание
Блок I		
1.	Модуль 1. Безопасность веб-приложений и архитектура решения WAF.	- угрозы безопасности веб-приложений; - OWASP TOP 10; - архитектура решения WAF; - схема лицензирования; - схема развертывания решения WAF; - тестирование уязвимостей (SQL-инъекции, XSS, Path Traversal, CSRF, XXE, XML Bomb, RCE, SSTI) в уязвимых приложениях (VulnBank, VulnLab, Juice Shop);
	Самостоятельная работа.	Реализация базовых уязвимостей - SQL Injection, XSS, CSRF, Path Traversal, File Inclusion, Data Bomb, XXE, SSTi Слушатель изучает теорию и дополнительные материалы;
2.	Модуль 2. Развертывание решения WAF.	- работа с WSC; - обзор веб-интерфейса, анализ событий, фильтрация событий по параметрам; - изолированные пространства; - настройка защиты веб-приложений; - балансировка нагрузки; - развертывание и первоначальная конфигурация решения WAF;
	Самостоятельная работа.	Развертывание решения WAF (минимальная конфигурация) Слушатель изучает теорию и дополнительные материалы;
Блок II		
3.	Модуль 3. Работа в решении WAF.	- работа с шаблонами политик безопасности; - работа с политиками безопасности; - правила обработки трафика; - действия; - глобальные списки; - агрегация;

		- обеспечение защиты уязвимых веб-приложений с помощью решения WAF; - создание и настройка политик безопасности. Создание пользовательских правил; - работа со списками; - повторное тестирование уязвимостей в уязвимых приложениях, защищенных решений WAF. *Практическое занятие:* - Настройка политики безопасности, создание пользовательских правил, добавление исключений в правила, фильтрация событий по критериям, создание глобальных списков.
4.	Модуль 4. Администрирование решения WAF.	- работа с Grafana; - работа с REST API;A - работа с логами; - настройка интеграции с Grafana.

6. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ

6.1. Материально-техническое обеспечение

Слушатели программы имеют доступ в режиме 24 часа в сутки 7 дней в неделю без учета объемов потребляемого трафика к электронной информационно-образовательной среде (далее – ЭИОС), в которой размещены учебные материалы:

- учебный план,
- календарный учебный график,
- расписание занятий,
- рабочие программы модулей,
- различные текстовые материалы,
- задания для самостоятельной работы,
- методические рекомендации для слушателя по изучению учебного материала и организации самостоятельной работы, прохождению форм текущего контроля успеваемости и итоговой аттестации.

6.2. Организация образовательного процесса

Образовательная программа предусматривает контактную и самостоятельную работу слушателей.

Контактная работа слушателей проходит в рамках таких видов учебных занятий, проводимых с применением дистанционных образовательных технологий в следующих формах:

1. Лекция - представляет собой видеозапись, вебинар с использованием дистанционных образовательных технологий, в ходе которого лектор раскрывает систему представлений о том или ином предмете, явлении, помогая слушателям осмыслить проблему и прийти к определенному выводу.

2. Практическое занятие - представляет собой форму организации учебного процесса, направленную на выработку у слушателей практических умений и навыков для решения профессиональных задач. В образовательном процессе используются различные виды практических занятий, в т. ч. такие как решение кейсов, решение учебных задач.

3. Самостоятельная работа слушателей проходит в таких формах как:

- изучение теоретического материала, в т.ч. текстовых материалов и дополнительных материалов по темам лекций.
- работа с основной и дополнительной литературой.

6.3. Кадровое обеспечение образовательного процесса

Реализация программы обеспечивается:

- педагогическими работниками;
- административным персоналом, который обеспечивает условия для эффективной работы педагогического коллектива, осуществляет контроль и текущую организационную работу;
- техническим персоналом, который обеспечивает функционирование информационной структуры (включая ремонт техники, оборудования, иного технического обеспечения образовательного процесса, поддержание сайта и т.п.).

Уровень квалификации работников в ООО «Облачные сети» соответствует квалификационным характеристикам должностей работников образования, утвержденным приказом Минздравсоцразвития России от 26 августа 2010 г. № 761н.

6.4. Перечень основной и дополнительной литературы, необходимой для освоения программы

1. Hoffman, A. (2021). «Web Application Security: Exploitation and Countermeasures for Modern Web Applications». O’Reilly Media.

2. Stuttard, D., Pinto, M. (2011). «The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws». Wiley.
3. Anderson, R. (2020, 3rd ed.). «Security Engineering: A Guide to Building Dependable Distributed Systems». Wiley.
4. Shevchenko, N. (2022). «Threat Modeling: Designing for Security». Addison-Wesley Professional.

6.5. Перечень ресурсов информационно-коммуникационной сети «Интернет», необходимых для освоения дисциплины

1. O PT AF // https://help.ptsecurity.com/ URL: https://help.ptsecurity.com/ru RU/projects/af/4.1.7/help/2067936651 (дата обращения: 27.03.2025).
2. Technical documentation // https://grafana.com URL: https://grafana.com/docs/ (дата обращения: 27.03.2025).
3. OWASP Top Ten // https://owasp.org URL: https://owasp.org/www-project-top-ten/ (дата обращения: 27.03.2025).

7. ФОРМЫ АТТЕСТАЦИИ

7.1. Промежуточная аттестация

Оценка качества освоения дополнительной профессиональной программы проводится с помощью промежуточной аттестации.

Промежуточная аттестация проводится в форме зачета. Зачет представляет собой тестирование.

7.2. Итоговая аттестация

Цель итоговой аттестации – оценка соответствия компетенций слушателя планируемым результатам освоения дополнительной профессиональной программы.

Итоговая аттестация проводится в форме зачета. Зачет представляет собой тестирование.

Итоговое аттестационное испытание проводится с использованием дистанционных образовательных технологий и электронного обучения.

8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Оценочные материалы регулярно актуализируются и формируются на основе реальных профессиональных проблем (кейсов). Работая над решением кейсовых задач, слушатель приобретает профессиональные знания, умения, навыки в результате активной творческой работы. Он самостоятельно формулирует цели, находит и собирает различную информацию, анализирует ее, выдвигает гипотезы, ищет варианты решения проблемы, формулирует выводы, обосновывает оптимальное решение ситуации.

Типовое задание для выполнения промежуточной аттестации по блоку I.

Описание задания: выполнить тест по тематике модулей.

Пример вопросов:

Что такое инъекции и как они могут использоваться злоумышленниками?

a) Ошибка в коде, из-за которой сайт медленно загружается;

b) Уязвимость, позволяющая выполнять непредусмотренные команды через непроверенные данные;

c) Метод ускорения работы базы данных;

d) Тип авторизации в веб-приложениях.

Критерии оценивания промежуточной аттестации:

Критерий	Оценка
75% и более правильных ответов на вопросы теста	Зачтено
74% и менее правильных ответов на вопросы теста	Не зачтено

Типовое задание для выполнения итоговой аттестации

Описание задания: выполнить итоговый тест, охватывающих материалы всех модулей программы. Вопросы теста могут содержать один или несколько правильных ответов.

1. Порядок развертывания решении WAF:

a) Развертывание из образа → настройка виртуальных IP-адресов → изменение имени сервера → Настройка NTP → Настройка сетевых интерфейсов → Настройка кластера Kubernetes → Настройка DNS → Запуск скриптов установки;

b) Развертывание из образа → изменение имени сервера → настройка виртуальных IP-адресов → Настройка NTP → Настройка DNS → Настройка сетевых интерфейсов → Настройка кластера Kubernetes → Запуск скриптов установки;

c) Развертывание из образа → изменение имени сервера → настройка виртуальных IP-адресов → Настройка сетевых интерфейсов → Настройка NTP → Настройка кластера Kubernetes → Настройка DNS → Запуск скриптов установки;

d) Развертывание из образа → изменение имени сервера → настройка виртуальных IP-адресов → Настройка NTP → Настройка сетевых интерфейсов → Настройка кластера Kubernetes → Настройка DNS → Запуск скриптов установки.

Критерии оценивания итоговой аттестации:

Критерий	Оценка
75% и более правильных ответов на вопросы теста	Зачтено
74% и менее правильных ответов на вопросы теста	Не зачтено