Учебно-тематический план дополнительной профессиональной программы

АНО ДПО “ФЛЕИН”

Учебно-тематический план программы

«Kaspersky Endpoint Security and Management (KL 002.12.7)»

Цель обучения:	По окончании курса слушатели смогут: ● описать возможности Kaspersky Endpoint Security и Kaspersky Security Center ● спроектировать и внедрить оптимальное решение для защиты небольших сетей, основанное на Kaspersky Endpoint Security и управляемое через Kaspersky Security Center ● осуществлять обслуживание внедренной системы на всех стадиях эксплуатации
Предварительные требования	● Понимание основ сетевых технологий: TCP/IP, DNS, электронной почты, web ● Базовые навыки администрирования ОС Windows и Linux ● Базовые знания об информационной безопасности
Профессиональный стандарт:	06.024 Специалист по технической поддержке информационно-коммуникационных систем (29.09.2020г.) 06.026 Системный администратор
Срок обучения:	32 часа
Режим занятий:	8 часов в день
Форма обучения:	Очная, очно-заочная с применением дистанционных образовательных технологий с отрывом от работы

№	Наименование разделов и тем	Всего, часов	Лекции	Практические занятия
1	Внедрение системы защиты	5	2.5	2.5
2	Управление защитой Windows	5	2.5	2.5
3	Контроль безопасности Windows	5	2.5	2.5
4	EDR Optimum (Windows)	5	2.5	2.5
5	Защита Linux	6	3	3
6	Администрирование и обслуживание системы	6	3	3
	Итого	**32**	**16**	**16**



_____

Богомолов О.А., директор

Учебно-тематический план дополнительной профессиональной программы

АНО ДПО “ФЛЕИН”

Учебно-тематический план программы

«Kaspersky Security Center. Управление системами (KL 009.12)»

Цель обучения:	По окончании курса слушатели смогут: ● управлять уязвимостями и обновлениями программ на компьютерах сети ● захватывать, изменять настройки и устанавливать образы операционных систем ● работать с реестрами программного и аппаратного обеспечения, управлять лицензиями сторонних приложений и настраивать интеграцию с SIEM-системами
Предварительные требования:	● Понимание основ сетевых технологий: TCP/IP, DNS, электронной почты, web ● Базовые навыки администрирования ОС Windows и Linux ● Базовые знания об информационной безопасности
Профессиональный стандарт:	06.024 Специалист по технической поддержке информационно-коммуникационных систем (29.09.2020г.) 06.026 Системный администратор
Срок обучения:	8 часов
Режим занятий:	8 часов в день
Форма обучения:	Очная, очно-заочная с применением дистанционных образовательных технологий с отрывом от работы

№	Наименование разделов и тем	Всего, часов	Лекции	Практические занятия
1	**Введение** Systems Management в Kaspersky Security Center; лицензирование; доступ к функциям Systems Management	2	1	1
2	**Управление уязвимостями и обновлениями программ** Постановка задачи; поиск уязвимостей; синхронизация Windows Update; установка обновлений; устранение уязвимостей; установка стороннего ПО; мониторинг	3	1.5	1.5
3	**Захват и развертывание образов компьютеров** Подготовка; создание образа ОС; кастомизация; развертывание; PXE	2	1	1
4	**Интеграция с SIEM и дополнительные возможности** Учет лицензий; реестр оборудования; удаленное подключение; интеграция с SIEM	1	0.5	0.5
	Итого	**8**	**4**	**4**



Богомолов О.А., директор

Учебно-тематический план дополнительной профессиональной программы

АНО ДПО “ФЛЕИН”

Учебно-тематический план программы

«Kaspersky Hybrid Cloud Security. Virtualization Protection (KL 031.6.2)»

Цель обучения:	По окончании курса слушатели смогут: ● рассказать о различных подходах к защите виртуальных сред и объяснить преимущества и недостатки ● описать возможности Kaspersky Security для виртуальных сред. Легкий агент ● на основе Kaspersky Security для виртуальных сред. Легкий агент спроектировать и развернуть решение ● в полной мере использовать функциональность решения и продемонстрировать эту функциональность другим ● объяснить принципы развертывания решения в больших виртуальных средах
Предварительные требования:	● Понимание основ сетевых технологий: TCP/IP, DNS, электронной почты, web ● Базовые навыки администрирования ОС Windows и Linux ● Базовые знания об информационной безопасности
Профессиональный стандарт:	06.024 Специалист по технической поддержке информационно-коммуникационных систем (29.09.2020г.) 06.026 Системный администратор
Срок обучения:	8 часов
Режим занятий:	8 часов в день

Форма обучения: Очная, очно-заочная с применением дистанционных образовательных технологий

с отрывом от работы

№	Наименование разделов и тем	Всего, часов	Лекции	Практические занятия
1	**Введение** Основы виртуализации; задачи защиты виртуальной инфраструктуры; архитектура Kaspersky Security для виртуальных сред	2	1	1
2	**Развертывание решения** Планирование внедрения; подготовка инфраструктуры; установка сервера защиты; установка легких агентов	2	1	1
3	**Управление защитой** Настройка политик безопасности; управление защитой виртуальных машин; мониторинг состояния; контроль целостности	2	1	1
4	**Масштабирование и сопровождение** Балансировка нагрузки; совместимость компонентов; оптимизация и администрирование системы	2	1	1
	Итого	**8**	**4**	**4**

_____

Богомолов О.А., директор

Учебно-тематический план дополнительной профессиональной программы

АНО ДПО “ФЛЕИН”

Учебно-тематический план программы

«Kaspersky Anti Targeted Attack. Administration. (KL 025.8)»

Цель обучения:	По окончании курса слушатели смогут: ● выполнять задачи по развертыванию и администрированию Kaspersky Anti Targeted Attack Platform
Предварительные требования:	● Базовые навыки управления приложениями для защиты конечных узлов с помощью Сервера администрирования Kaspersky Security Center ● Понимание основ сетевых технологий: DNS, маршрутизации, электронной почты, Web ● Базовые навыки администрирования Windows и Linux ● Представление о современных угрозах и тенденциях развития информационных технологий
Профессиональный стандарт:	06.024 Специалист по технической поддержке информационно-коммуникационных систем (29.09.2020г.) 06.026 Системный администратор
Срок обучения:	16 часов
Режим занятий:	8 часов в день
Форма обучения:	Очная, очно-заочная с применением дистанционных образовательных технологий с отрывом от работы

№	Наименование разделов и тем	Всего, часов	Лекции	Практические занятия
1	**Подготовка к внедрению** Состав и возможности решения; схемы развертывания; масштабирование; совместимость	2	1	1
2	**Развертывание KATA Platform** Установка Central Node и Sensor; настройка Sandbox; подготовка Central Node; подключение серверов и источников трафика; ретроспективный анализ	5	2.5	2.5
3	**Установка и настройка Endpoint Agent** Централизованная и локальная установка; настройка NDR-агентов; отправка файлов в Sandbox; проверка установки	3	1.5	1.5
4	**Обслуживание KATA Platform** Политики безопасности; API (KATA/NDR); уведомления; интеграции (SIEM, KUMA, NGFW); мониторинг; резервное копирование; обновление системы	6	3	3
	Итого	**16**	**8**	**8**



Богомолов О.А., директор

Учебно-тематический план дополнительной профессиональной программы

АНО ДПО “ФЛЕИН”

Учебно-тематический план программы

«Kaspersky Anti Targeted Attack. Investigation (KL 057.7)»

Цель обучения:	По окончании курса слушатели смогут: ● выполнять задачи по детектированию и обнаружению угроз, используя Kaspersky Anti Targeted Attack
Предварительные требования:	● Знания и навыки работы с Kaspersky Anti Targeted Attack, которые вы можете получить, пройдя учебный курс Kaspersky Anti Targeted Attack. Kaspersky EDR. Administration (025.7) ● Также необходимые общие знания о типах современных атак, способах их выявления
Профессиональный стандарт:	06.024 Специалист по технической поддержке информационно-коммуникационных систем (29.09.2020г.) 06.026 Системный администратор
Срок обучения:	16 часов
Режим занятий:	8 часов в день
Форма обучения:	Очная, очно-заочная с применением дистанционных образовательных технологий с отрывом от работы

№	Наименование разделов и тем	Всего, часов	Лекции	Практические занятия

1	**Введение** Назначение Kaspersky Anti Targeted Attack; компоненты KATA и NDR; задачи детектирования и обнаружения угроз	2	1	1
2	**Эксплуатация KATA NDR** Использование KATA и NDR; анализ сетевого трафика; выявление угроз	6	3	3
3	**Результаты анализа Sandbox** Анализ подозрительных объектов; интерпретация результатов; использование в расследовании	6	3	3
4	**Отчетность и оповещения** Формирование отчетов; анализ событий; настройка оповещений	2	1	1
	Итого	**16**	**8**	**8**



Богомолов О.А., директор

Учебно-тематический план дополнительной профессиональной программы

АНО ДПО “ФЛЕИН”

Учебно-тематический план программы

«Kaspersky Unified Monitoring and Analysis Platform. Administration (KL 034.4)»

Цель обучения:	По окончании курса слушатели смогут: ● развернуть Kaspersky Unified Monitoring and Analysis Platform для демонстрации решения ● настроить получение событий из разных источников и в разных форматах ● настроить взаимодействие с внешними системами с целью обогащения событий и реагирования на инциденты ● отслеживать состояние источников и компонентов системы
Предварительные требования:	● Понимание основ сетевых технологий: TCP/IP, DNS, электронной почты, web ● Базовые навыки администрирования ОС Windows и Linux ● Базовые знания об информационной безопасности
Профессиональный стандарт:	06.024 Специалист по технической поддержке информационно-коммуникационных систем (29.09.2020г.) 06.026 Системный администратор
Срок обучения:	20 часов
Режим занятий:	8 часов в день
Форма обучения:	Очная, очно-заочная с применением дистанционных образовательных технологий с отрывом от работы

№	Наименование разделов и тем	Всего, часов	Лекции	Практические занятия
1	**Общие сведения** Назначение SIEM; задачи; примеры использования KUMA	2	1	1
2	**Архитектура** Принципы работы KUMA; компоненты; лицензирование; требования	2	1	1
3	**Установка** Развертывание (all-in-one и распределенное); роли; доступ; веб-консоль	2	1	1
4	**Сбор и обработка событий** Настройка источников; обработка и нормализация событий	3	1.5	1.5
5	**Интеграции** Интеграция с внешними системами; обогащение событий	2	1	1
6	**Хранение событий** Настройка хранения; управление данными	2	1	1
7	**Корреляция** Правила корреляции; выявление инцидентов	2	1	1
8	**Алерты** Настройка уведомлений; реагирование на события	2	1	1
9	**Реагирование** Механизмы реагирования; автоматизация действий	2	1	1
10	**Мониторинг состояния источников и метрики** Контроль состояния компонентов; метрики; диагностика	1	0.5	0.5
	Итого	**20**	**10**	**10**

Богомолов О.А., директор

Учебно-тематический план дополнительной профессиональной программы

АНО ДПО “ФЛЕИН”

Учебно-тематический план программы

«Kaspersky Unified Monitoring and Analysis Platform. Investigation (KL 051.4)»

Цель обучения:	По окончании курса слушатели смогут: ● выполнять задачи по детектированию и обнаружению угроз, используя Kaspersky Unified Monitoring and Analysis Platform ● настраивать обработку событий (нормализация, агрегация, обогащение и т.д.) ● создавать правила корреляции и анализа данных для выявления угроз ● создавать различные правила реагирования на угрозы ● использовать ресурсы и функции KUMA для анализа и выявления угроз (активные списки, словари, переменные, API и т.п.) ● выявить угрозы, анализируя полученные события
Предварительные требования:	● Знания и навыки работы с KUMA, которые вы можете получить пройдя учебный курс Kaspersky Unified Monitoring and Analysis Platform. Administration (034.4). ● Также необходимы общие знания о типах современных атак, способах их выявления.
Профессиональный стандарт:	06.024 Специалист по технической поддержке информационно-коммуникационных систем (29.09.2020г.) 06.026 Системный администратор
Срок обучения:	20 часов
Режим занятий:	8 часов в день
Форма обучения:	Очная, очно-заочная с применением дистанционных образовательных технологий с отрывом от работы

№	Наименование разделов и тем	Всего, часов	Лекции	Практические занятия
1	**Введение** Назначение SIEM; принципы работы KUMA; архитектура и задачи системы	2	1	1
2	**Сбор событий** Сбор и нормализация событий; обработка данных; интеграции с источниками	3	1.5	1.5
3	**Работа с активами** Источники активов; свойства; категории; обогащение событий	2	1	1
4	**Поиск событий** Интерфейс поиска; построение запросов; анализ событий	2	1	1
5	**Корреляция** Правила корреляции; переменные; активные списки; выявление угроз	3	1.5	1.5
6	**AI и аналитика** Использование аналитики и автоматизации при выявлении угроз	2	1	1
7	**Реагирование** Механизмы реагирования; автоматизация; сценарии обработки инцидентов	3	1.5	1.5
8	**Панели мониторинга и отчеты** Визуализация данных; отчётность; контроль состояния системы	3	1.5	1.5
	Итого	**20**	**10**	**10**

Богомолов О.А., директор

Учебно-тематический план дополнительной профессиональной программы

АНО ДПО “ФЛЕИН”

Учебно-тематический план программы

«Kaspersky Container Security (KL 044.2.4)»

Цель обучения:	По окончании курса слушатели смогут: ● Защищать контейнерные инфраструктуры с помощью агентов Kaspersky Container Security ● Проверять контейнеры на наличие уязвимостей, вредоносного кода, ошибок конфигурации и конфиденциальных данных ● Интегрировать средства защиты в конвейер CI\CD
Предварительные требования:	● Базовые навыки администрирования ОС Linux ● Базовые знания об информационной безопасности ● Желательно иметь базовые знания о технологиях контейнеризации
Профессиональный стандарт:	06.024 Специалист по технической поддержке информационно-коммуникационных систем (29.09.2020г.) 06.026 Системный администратор
Срок обучения:	8 часов
Режим занятий:	8 часов в день
Форма обучения:	Очная, очно-заочная с применением дистанционных образовательных технологий с отрывом от работы

№	Наименование разделов и тем	Всего, часов	Лекции	Практические занятия
1	**Введение в безопасность контейнеров** CI/CD и микросервисы; контейнеры; Kubernetes; DevSecOps; безопасность Kubernetes	2	1	1
2	**Архитектура и развертывание** Архитектура решения; подготовка к развертыванию; развертывание; масштабирование	2	1	1
3	**Эксплуатация решения** Пользователи и роли; интеграции; развертывание агентов; политики безопасности; журнал событий и отчёты; сканирование; контроль CI/CD	3	1.5	1.5
4	**Поддержка и устранение неполадок** Жизненный цикл данных; поиск неисправностей	1	0.5	0.5
	Итого	**8**	**4**	**4**



Богомолов О.А., директор

Учебно-тематический план дополнительной профессиональной программы

АНО ДПО “ФЛЕИН”

Учебно-тематический план программы

«Kaspersky NGFW (KL 007.1)»

Цель обучения:

По окончании курса слушатели смогут:

- разбираться в архитектуре и схеме обработки трафика NGFW, понимать взаимодействие модулей безопасности
- выполнять базовую настройку NGFW, управлять сетевыми объектами и правилами фильтрации
- настраивать и управлять ключевыми модулями безопасности: контроль приложений (App-Control), система обнаружения и предотвращения вторжений (IDPS), антивирус, веб-контроль (Web Control) и фильтрация DNS
- настраивать и применять политики расшифровки и инспектирования TLS/SSL трафика для противодействия скрытым угрозам
- реализовывать трансляцию сетевых адресов (NAT) и настраивать динамическую маршрутизацию (BGP)
- организовывать интеграцию NGFW с внешними системами (оркестратор KNBE, платформа OSMP, Zabbix) для автоматизации и мониторинга

Предварительные требования:

- Понимание основ сетевых технологий: TCP/IP, DHCP, NAT, знание принципов работы маршрутизации и коммутации на уровне CCNA/HCNA.
- Иметь представление о работе классических межсетевых экранов предыдущего поколения.
- Базовые знания сетевой безопасности: правила МЭ, SSL/TLS, контроль приложений.

- Базовый опыт работы с системами мониторинга.
- Умение читать и интерпретировать сетевую статистику и журналы событий.
- Начальные навыки администрирования операционных систем Windows Server и Linux, включая основы работы с Active Directory (AD).
- Знания установки платформы OSMP.
- Основные представления о настройке протокола динамической маршрутизации BGP.
- Иметь представление о базовом управлении платформы KUMA.

Профессиональный стандарт:	06.024 Специалист по технической поддержке информационно-коммуникационных систем (29.09.2020г.) 06.026 Системный администратор
Срок обучения:	16 часов
Режим занятий:	8 часов в день
Форма обучения:	Очная, очно-заочная с применением дистанционных образовательных технологий с отрывом от работы

№	Наименование разделов и тем	Всего, часов	Лекции	Практические занятия
1	**Введение** Вызовы безопасности; решение Kaspersky; принцип работы KSN	2	1	1
2	**Базовая настройка NGFW** Начальная конфигурация; сетевые интерфейсы; базовые политики	2	1	1
3	**Архитектура обработки трафика** Пакет и поток; App-control; DPI; SSL Inspection; схема обработки трафика	4	2	2

4	**Модули безопасности** Firewall; сегментация; контроль приложений; IDPS; антивирус; Web Control; DNS Security	4	2	2
5	**Функции и интеграции** NAT; маршрутизация (BGP); интеграция с KNBE, OSMP, Zabbix; мониторинг и диагностика	4	2	2
	Итого	**16**	**8**	**8**



Богомолов О.А., директор