НОЧУ ДПО УЦ «Сетевая Академия»

УТВЕРЖДАЮ
Директор НОЧУ ДПО УЦ «Сетевая Академия»

_____/Шикова Ю.В./

Образовательная программа
дополнительного профессионального образования
(повышения квалификации)
«SUSE Linux Enterprise Server 12 – Безопасность»
(SLE341v12 Securing SUSE Linux Enterprise Server 12)

Содержание

Описание образовательной программы 2
Цели программы 3
Планируемые результаты обучения 4
Учебный план 6
Календарный учебный график 7
Рабочая программа 8
Организационно-педагогические условия реализации Программы 8
Формы аттестации и оценочные материалы 10

Описание образовательной программы

Настоящая образовательная программа повышения квалификации (далее – Программа) разработана в соответствии с:

1. Федеральным законом от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации»
2. Приказом Минобрнауки России от 1 июля 2013 г. N 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»
3. Уставом НОЧУ ДПО УЦ «Сетевая Академия»

Структура Программы включает цели, планируемые результаты обучения, учебный план, календарный учебный график, рабочую программу, организационно-педагогические условия, формы аттестации и оценочные материалы.

Цели Программы содержат описание целевой аудитории, целей обучения и необходимых начальных знаний и навыков слушателей.

Планируемые результаты обучения представлены в виде перечня профессиональных компетенций в рамках имеющейся квалификации (с отсылкой к профессиональному стандарту), качественное изменение которых осуществляется в результате обучения.

Учебный план определяет перечень, трудоемкость, последовательность и распределение модулей, иных видов учебной деятельности обучающихся и формы аттестации.

Календарный учебный график определяет основные параметры учебного процесса при организации занятий по освоению настоящей Программы, включая формы обучения, расписание занятий очных групп и т.п.

Рабочая программа раскрывает рекомендуемую последовательность изучения разделов (модулей).

Описание организационно-педагогических условий реализации Программы определяет организационные и методические требования НОЧУ ДПО УЦ «Сетевая Академия» к организации и проведению обучения по Программе.

Формы аттестации и оценочные материалы определяют формы проведения промежуточной и итоговой аттестации по Программе и форму учебно-методических материалов, необходимых для проведения указанных видов аттестации.

Цели программы

Данная Программа предназначена для:

- для системных администраторов SUSE, которые хотят научиться настраивать безопасность в системе.

Целью обучения является предоставить слушателям знания и навыки, необходимые для обеспечения безопасного использования SUSE Linux Enterprise Server в корпоративной сети.

Для изучения данной Программы рекомендуется обладать следующими знаниями и навыками:

- знания и опыт работы с SUSE Linux Enterprise Server (версии 12 или 15) в объеме курсов SLE201 "SUSE Linux Enterprise Server 12 - Администрирование" и SLE301 "SUSE Linux Enterprise Server 12 – Продвинутое администрирование").

Планируемые результаты обучения

Реализация Программы направлена на повышение профессионального уровня в рамках имеющейся квалификации, определяемой профессиональным стандартом «06.026 Системный администратор информационно-коммуникационных систем», утвержденным Приказом Минтруда России от 05.10.2015 N 684н "Об утверждении профессионального стандарта "Системный администратор информационно-коммуникационных систем"

Результатами обучения по Программе станут знания и умения, соответствующие следующим обобщенным трудовым функциям указанного профессионального стандарта:

- Администрирование системного программного обеспечения инфокоммуникационной системы организации.

Совершенствуемые компетенции в соответствии с трудовыми функциями профессионального стандарта:

Компетенция	**Содержание компетенции** Трудовые функции	**Код**
Администрирование системного программного обеспечения инфокоммуникационной системы организации	Установка системного программного обеспечения	F/01.7
	Оптимизация работы дисковой подсистемы (подсистемы ввода-вывода)	F/02.7
	Администрирование файловых систем	F/03.7
	Оценка критичности возникновения инцидентов для системного программного обеспечения	F/04.7
	Реализация регламентов обеспечения информационной безопасности системного программного обеспечения инфокоммуникационной системы организации	F/05.7

После обучения слушатель сможет:

- Понимать концепции безопасности и основы криптографии.
- Настроить безопасный процесс загрузки системы.
- Использовать модуль безопасности YaST.
- Понимать настраиваемые параметры безопасности ядра.
- Понимать важность исправлений и обновлений.
- Учитывать безопасность в файловой системе.
- Обезопасить локальные учетные записи пользователей и ограничивать доступ к учетной записи «root».
- Понимать управление сессиями Systemd и управление ресурсами.
- Управлять модулями аутентификации PAM.
- Делегировать администраторские привилегии (sudo, polkit).
- Понимать фильтрацию сетевых пакетов, а также использовать TCP Wrappers и Xinetd.
- Ограничить сетевой доступ при помощи инструментов в Systemd.
- Понимать и настраивать VPN.
- Использовать инструменты аудита безопасности: SUSE Seccheck, AIDE, Linux Audit Framework, централизованное ведение журналов.
- Понимать структуру модулей безопасности Linux (LSM).

- Сравнить AppArmor и SELinux.
- Представлять отличия технологий безопасности используемых в SLES12 с последней версией SLE15 (дополнительно).

Учебный план

Учебный план Программы определяет перечень, трудоемкость, последовательность и распределение модулей, иных видов учебной деятельности обучающихся и формы аттестации.

№ п/п	Наименование разделов (модулей)	Всего, час	В том числе		Форма аттестации
			Лекции	Практические занятия	
1.	Введение в безопасность	3	2	1	Опрос, практические занятия
2.	Базовые ограничения системы	3	1,5	1,5	Опрос, практические занятия
3.	Безопасность для локальных учетных записей	3	1	2	Опрос, практические занятия
4.	Повышение привилегий	3	1,5	1,5	Опрос, практические занятия
5.	Ограничения сетевых служб	3	1,5	1,5	Опрос, практические занятия
6.	Инструменты аудита безопасности	3	1	2	Опрос, практические занятия
7.	Модули безопасности Linux	4	2	2	Опрос, практические занятия
8.	**Итоговая аттестация**	**2**	**-**	**2**	**Тестирование**
	Итого:	**24**	**10,5**	**13,5**	

Допускается формирование индивидуального учебного плана для каждого слушателя в пределах осваиваемой Программы в порядке, установленном Положением об организации образовательного процесса в НОЧУ ДПО УЦ «Сетевая Академия».

Календарный учебный график

Учебный год: круглогодичное обучение.

Продолжительность Программы: 24 академических часа.

Форма организации образовательного процесса: очная, очно-заочная (вечерняя) и заочная формы обучения, в том числе, с применением дистанционных образовательных технологий и электронного обучения.

Сменность занятий (при очной форме обучения): I смена.

Количество учебных дней в неделю при очном обучении: 3 дня.

Начало учебных занятий: 9.30

Окончание учебных занятий: 17.00

Продолжительность урока: 45 минут (1 академический час).

Продолжительность перемен: 15 минут, перерыв на обед – 60 минут.

Расписание занятий для очных групп:

	№ урока	**Время**
Конкретный день недели согласовывается во время учебного процесса	1-2	09:30 - 11:00
	3-4	11:15 - 12:45
	5-6	13:45 - 15:15
	7-8	15:30 - 17:00

Модуль 1: Введение в безопасность

- Основные концепции безопасности.
- Основы криптографии.
- Ресурсы SUSE, посвященные безопасности.
- SLES 12 Сертификация безопасности.

Модуль 2: Базовые ограничения системы

- Безопасный процесс загрузки.
- Модуль безопасности YaST.
- Настройки безопасности ядра.
- Важность использования обновлений и исправлений.
- Безопасность файловой системы.

Модуль 3: Безопасность для локальных учетных записей

- Защита учетных записей локальных пользователей.
- Управления сеансами Systemd.
- Управлением ресурсами Systemd.
- Модули PAM.

Модуль 4: Повышение привилегий

- Ограничение доступа к учетной записи root.
- Использование sudo для делегирования административных прав.
- Использование Polkit для делегирования административных прав.

Модуль 5: Ограничения сетевых служб

- Фильтрация сетевых пакетов.
- TCP-wrappers и xinetd.
- Ограничение доступа к сети с помощью systemd.
- VPN.

Модуль 6: Инструменты аудита безопасности

- SUSE seccheck.
- Определения вторжения в систему: AIDE.
- Linux Audit Framework.
- Централизованное ведение журналов.

Модуль 7: Модули безопасности Linux

- Обзор функций безопасности ядра Linux.
- Инфраструктура модулей безопасности Linux (LSM).
- AppArmor.
- SELinux.
- Сравнение AppArmor и SELinux.

Организационно-педагогические условия реализации Программы

При реализации Программы применяется форма организации образовательной деятельности, основанная на модульном принципе представления содержания образовательной программы и построения учебных планов, использовании различных образовательных технологий, в том числе дистанционных образовательных технологий и электронного обучения.

Организационные условия реализации программы в разных формах обучения регулируются следующими локальными нормативными актами:

- Положение об организации образовательного процесса в НОЧУ ДПО УЦ «Сетевая Академия».
- Положение о порядке применения электронного обучения, дистанционных образовательных технологий в НОЧУ ДПО УЦ «Сетевая Академия».

Учебные материалы по Программе включают: рабочую программу, раздаточные материалы по курсу, методические материалы по курсу, данные примеров по курсу. Учебное пособие по Программе выдается слушателям в бумажном или электронном виде в зависимости от формы обучения в порядке, установленном Положением о библиотеке в НОЧУ ДПО УЦ «Сетевая Академия».

Занятия по Программе проводятся преподавателями, предварительно подтвердившими свою квалификацию. В числе базовых требований ко всем преподавателям – требование обязательного прохождения программы «Андрагогика. Эффективное обучение взрослых» в форме учебного курса и пробной лекции, а также сдачи технических сертификационных тестов по продукту или технологии, рассматриваемым в курсе.

Формы аттестации и оценочные материалы

Освоение Программы сопровождается промежуточной аттестацией обучающихся в формах, определенных учебным планом, и в порядке, установленном Положением об организации образовательного процесса в НОЧУ ДПО УЦ «Сетевая Академия».

Освоение Программы завершается итоговой аттестацией обучающихся в форме, определенной учебным планом, и в порядке, установленном Положением об организации образовательного процесса в НОЧУ ДПО УЦ «Сетевая Академия».

Слушателям, успешно освоившим соответствующую Программу и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации на бланке, образец которого самостоятельно устанавливается организацией.

Слушателям, не прошедшим итоговой аттестации или получившим на итоговой аттестации неудовлетворительные результаты, а также лицам, освоившим часть Программы и (или) отчисленным из организации, выдается справка об обучении или о периоде обучения по образцу, самостоятельно устанавливаемому организацией.

Оценочные материалы для промежуточной аттестации по Программе разрабатываются в форме лабораторных работ и/или контрольных вопросов после изучения каждого модуля.

Оценочные материалы для итоговой аттестации по Программе разрабатываются в форме теста.

Контрольные задания и вопросы для оценки знаний и навыков слушателей задаются и выполняются в следующих областях:

- Основные концепции безопасности.
- Основы криптографии.
- Безопасный процесс загрузки.
- Модуль безопасности YaST.
- Настройки безопасности ядра.
- Безопасность файловой системы.
- Защита учетных записей локальных пользователей.
- Управления сеансами Systemd. Управлением ресурсами Systemd.
- Ограничение доступа к учетной записи root.
- Использование sudo и Polkit для делегирования административных прав.
- Фильтрация сетевых пакетов.
- Ограничение доступа к сети с помощью systemd.
- Инструменты аудита безопасности
- Модули безопасности Linux