

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

Технические средства информатизации

название учебной дисциплины

1. Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина входит в состав дисциплин общепрофессионального цикла.

2. Цели и задачи дисциплины – требования к результатам освоения дисциплины:

Код ПК, ОК, ЛР	Умения	Знания
ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10; ПК 1.1, ПК 1.2, ЛР 3, 17, 18	<ul style="list-style-type: none">- выявлять и оценивать угрозы безопасности информации в ИТКС;- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;-проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации;-проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;-выявлять и оценивать угрозы безопасности информации в ИТКС;- проводить контроль показателей и процесса функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации;- проводить восстановление процесса и параметров функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации;- проводить техническое обслуживание и ремонт программно-аппаратных (в том числе криптографических) средств защиты информации;	<ul style="list-style-type: none">- способов защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на нее;- типовых программных и программно-аппаратных средств защиты информации в ИТКС;- криптографических средств защиты информации конфиденциального характера, которые применяются в ИТКС;- возможных угроз безопасности информации в ИТКС;- способов защиты информации от НСД и специальных воздействий на нее;- порядка тестирования функций программных и программно-аппаратных (в том числе криптографических) средств защиты информации;- организации и содержания технического обслуживания и ремонта программно-аппаратных (в том числе криптографических) средств защиты информации;- порядка и правил ведения эксплуатационной документации на программные и программно-аппаратные (в том числе криптографические) средства защиты информации;- возможных угроз безопасности информации в ИТКС;- способов защиты информации НСД и специальных воздействий на нее;- типовых программных и программно-аппаратных средств защиты информации в ИТКС;

	<p>-выявлять и оценивать угрозы безопасности информации в ИТКС; -настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; -проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации; -проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации российского производства; -проводить настройку систем защиты от внутренних угроз информационной безопасности</p>	<p>-криптографических средств защиты информации конфиденциального характера, которые применяются в ИТКС; -порядка и правил ведения эксплуатационной документации на программные и программно-аппаратные (в том числе криптографические) средства защиты информации -программные и программно-аппаратные средства защиты информации в ИТКС российского производства;</p>
--	---	---

3. Рекомендуемое количество часов на освоение программы дисциплины:

Объем работы обучающихся во взаимодействии с преподавателем 116 часов, в том числе:

- 116 часов вариативной части, направленных на усиление обязательной части программы.

4. Объем учебной дисциплины и виды учебной работы

Вид учебной деятельности	Объем часов
Объем образовательной программы	116
Объем работы обучающихся во взаимодействии с преподавателем	100
в том числе:	
- теоретическое обучение	40
- лабораторные работы (если предусмотрено)	-
- практические занятия (если предусмотрено)	60
- курсовая работа (проект) (если предусмотрено)	-
- самостоятельная работа	12
- промежуточная аттестация (дифференцированный зачет)	4

5. Содержание дисциплины

Раздел 1. Linux. Виртуализация в ESXI.

Тема 1.1 Изучение серверных и десктопных версий. ОС Linux. Знакомство с ESXI

Раздел 2. Настройка оборудования. Создание защищённой сети.

Тема 2.1 Обеспечение безопасности компьютерных систем и сетей. Технологии Data Leakage Prevention (DLP).