Министерство науки и высшего образования Российской Федерации
Филиал федерального государственного бюджетного образовательного учреждения высшего образования
«Кубанский государственный университет»
в г. Славянске-на-Кубани

УТВЕРЖДАЮ

Проректор по работе с филиалами
ФГБОУ ВО «Кубанский государственный университет»

_____А.А. Евдокимов

«14» июня 2019 г.

Рабочая программа учебной дисциплины

МДК.03.02 БЕЗОПАСНОСТЬ ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

специальность 09.02.02 Компьютерные сети

Краснодар 2019

Рабочая программа учебной дисциплины МДК.03.02 БЕЗОПАСНОСТЬ ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ разработана на основе Федерального государственного образовательного стандарта (далее - ФГОС) по специальности среднего профессионального образования (далее СПО) 09.02.0.2 Компьютерные сети, утвержденного приказом Минобрнауки РФ от 28.07.2014 №803 (зарегистрирован в Минюсте России 20.08.2014 № 33713).

4 курс	7 семестр
Лекции	60 ч.
Практические занятия	60 ч.
Лабораторные занятия	10 ч.
Самостоятельные занятия	65 ч.
Форма итогового контроля	Зачет

Составитель: канд. тех. наук, доцент _____С.А. Осипов,

преподаватель _____О.А. Семенцова

Утверждена на заседании предметно-цикловой комиссии физико-математических и специальных дисциплин специальности Компьютерные сети протокол № 10 от «11» **июня** 2019 г.

Председатель предметно-цикловой комиссии
физико-математических и специальных дисциплин «11» июня 2019 г.
специальности компьютерные сети_____ А .Б. Шишкин
Рецензент (-ы):

Инженер-проводник 1 категории,
отдел УСУТП управление АСУТП,
КИПиА, МОП Краснодарского РПУ
филиала «Макрорегион ЮГ» ООО ИК
«Сибинтек» _____ М.В. Литус

Директор ООО «Бизнес ассистент» _____ Д.С. Зима

ЛИСТ
согласования рабочей программы по дисциплине
МДК.03.02 БЕЗОПАСНОСТЬ ФУНКЦИОНИРОВАНИЯ
ИНФОРМАЦИОННЫХ СИСТЕМ

Специальность среднего профессионального образования:
09.02.2 Компьютерные сети

СОГЛАСОВАНО:

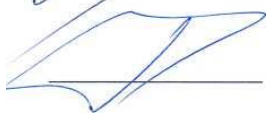
Нач. УМО филиала

А.С. Демченко
«13» июня 2019 г.

Заведующая библиотекой филиала

М.В. Фуфалько
«13» июня 2019 г.

Нач. ИВЦ
(программно-информационное
обеспечение образовательной
программы



В.А. Ткаченко
«13» июня 2019

СОДЕРЖАНИЕ

1 ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1 Область применения программы

Рабочая программа учебной дисциплины «Безопасность функционирования информационных систем» является частью основной профессиональной образовательной программы в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования (далее ФГОС СПО) для специальности 09.02.02 Компьютерные сети.

1.2 Место дисциплины в структуре программы подготовки специалистов среднего звена

Дисциплина «Безопасность функционирования информационных систем» относится к профессиональному модулю «Эксплуатация объектов сетевой инфраструктуры».

1.3 Цели и задачи учебной дисциплины - требования к результатам освоения дисциплины

В результате изучения профессионального модуля обучающийся должен *иметь практический опыт:*

- обслуживания сетевой инфраструктуры;
- удаленного администрирования сетевой инфраструктуры;
- поддержки пользователей сети, настройки аппаратного и программного обеспечения сетевой инфраструктуры.

В результате освоения дисциплины обучающийся должен *уметь:*

- выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств;
- правильно оформлять техническую документацию;
- наблюдать за трафиком, выполнять операции резервного копирования и восстановления данных;
- устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту.

В результате освоения дисциплины обучающийся должен *знать:*

- задачи управления: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией;

- средства мониторинга и анализа локальных сетей;
- основные понятия информационных систем, жизненный цикл, проблемы обеспечения технологической безопасности информационных систем, требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования, оперативные методы повышения безопасности функционирования программных средств и баз данных;
- основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем.

Максимальная учебная нагрузка обучающегося 195 часов, в том числе:
- обязательная аудиторная учебная нагрузка обучающегося 130 часов;
- самостоятельная работа обучающегося 65 часов.

1.4. Перечень планируемых результатов обучения по дисциплине (Перечень формируемых компетенций).

Освоение дисциплины «Безопасность функционирования информационных систем» способствует формированию у студентов следующих профессиональных компетенций:

- ПК 3.1. Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей.
- ПК 3.2. Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях.
- ПК 3.3. Эксплуатация сетевых конфигураций.
- ПК 3.4. Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации.
- ПК 3.5. Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль оборудования после его ремонта.
- ПК 3.6. Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.

Одновременно с профессиональными компетенциями у студентов, обучающихся по дисциплине «Безопасность функционирования информационных систем»

создаются предпосылки для формирования общих компетенций:

- ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
- ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
- ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
- ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
- ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.
- ОК 6. Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.
- ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.
- ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
- ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	иметь практический опыт (владеть)
1	ОК-1	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес	сущность и социальную значимость профессии «Техник по компьютерным сетям»	использовать современные методы в профессиональной деятельности «Техник по компьютерным сетям»	проявлять устойчивый интерес к профессии «Техник по компьютерным сетям»

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	иметь практический опыт (владеть)
2	ОК-2	Организовывать собственную деятельность, определять методы и способы выполнения профессиональных задач, оценивать их эффективность и качество	основные тенденции развития, положений, законов компьютерных наук, знать, как использовать их базовые положения при решении профессиональных задач	критически оценивать компьютерные теории и концепции, границы их применимости; выявлять естественнонаучную и междисциплинарную сущность проблем, возникающих в ходе профессиональной деятельности	критического переосмысливания накопленного опыта, внесения изменений в рабочие процессы с учетом инноваций, оптимизации рабочего процесса с учетом развития науки и технологий
3	ОК 3	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность	меры ответственности за принятые решения	оценить возникшую стандартную или нестандартную ситуацию, предотвратить ее негативные последствия	принятия решений в стандартных и нестандартных ситуациях
4	ОК 4	Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития	основные тенденции развития, положений, законов метрологии, знать, как использовать их базовые положения при решении профессиональных задач	осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по профессии	критического переосмысливания накопленного опыта, внесения изменений в рабочие процессы с учетом инноваций, оптимизации рабочего процесса с учетом развития науки и технологий
5	ОК 5	Использовать информационно-коммуникационные технологии в профессиональной деятельности.	основные теоретические и практические положения информационно-коммуникационные технологий в сфере наладки технологического оборудования	использовать основные теоретические и практические положения информационно-коммуникационные технологий в профессиональной деятельности «Техник по компьютерным сетям»	использования информационно-коммуникационные технологий в профессиональной деятельности «Техник по компьютерным сетям»
6	ОК 6	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.	цели, функции, виды и уровни общения; роли и ролевые ожидания в общении; вилы социальных взаимодействий, механизмы взаимопонимания в общении; техники и приемы общения, правила слушании, веления беседы, убеждения; этические принципы общения;	применять техники и приемы эффективного общения и профессиональной деятельности; использовать приемы саморегуляции поведения в процессе межличностного общения;	— работы в коллективе и команде, — эффективного общения с коллегами, руководством, потребителями

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	иметь практический опыт (владеть)
			источники, причины, виды и способы разрешения конфликтов;		
7.	ОК 7	Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.	меры ответственности за принятые решения	взять на себя ответственность за работу членов команды	принятия решений в стандартных и нестандартных ситуациях
8.	ОК 8	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации	основные тенденции развития, положений, законов метрологии, знать, как использовать их базовые положения при решении профессиональных задач	выбирать методику и средства решения задач, используя научную литературу и электронные информационно-образовательные ресурсы, информационно-коммуникационные технологи	критического переосмысливания накопленного опыта, внесения изменений в рабочие процессы с учетом инноваций, оптимизации рабочего процесса с учетом развития науки и технологий
9.	ОК 9	Ориентироваться в условиях частой смены технологий в профессиональной деятельности	роль и значение информационно-коммуникационных технологий с целью совершенствования своей профессиональной деятельности	осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по профессии,	владеть способностью учитывать современные тенденции развития науки и вычислительной техники, компьютерных технологий в профессиональной деятельности
10	ПК 3.1	Обеспечивать резервное копирование данных	классификацию программно-аппаратного обеспечения по резервному копированию данных;	обеспечить целостность резервирования информации, использование VPN;	обеспечения целостности резервирования информации, использования VPN;
11	ПК 3.2	Осуществлять меры по защите компьютерных сетей от несанкционированного доступа	классификацию программного обеспечения по защите компьютерных сетей от несанкционированного доступа;	обеспечивать защиту при подключении к информационно-телекоммуникационной сети «Интернет» средствами операционной системы;	организации доступа к локальным и глобальным сетям;
12	ПК 3.3	Применять специализированные средства для борьбы с вирусами, несанкционированными рассылками электронной почты, вредоносными программами	классификацию программного обеспечения борьбы с вирусами, несанкционированными рассылками электронной почты, вредоносными программами;	устанавливать н конфигурировать антивирусное программное обеспечение, программное обеспечение баз данных, программное обеспечение мониторинга;	сопровождения и контроля использования почтового сервера, SQL- сервера;
13	ПК 3.4	Осуществлять мероприятия по	классификацию программного обеспечения	устанавливать н конфигурировать	сбора данных для анализа использо-

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	иметь практический опыт (владеть)
		защите персональных данных	по защите персональных данных;	антивирусное программное обеспечение, программное обеспечение баз данных, программное обеспечение мониторинга;	вания и функционирования программно- технических средств компьютерных сетей;
14	ПК 3.5	Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль поступившего из ремонта оборудования.	- общие сведения об элементной базе схемотехники ; - логические элементы и логическое проектирование в базисах микросхем; - функциональные узлы (дешифраторы, шифраторы, мультиплексоры, демультиплексоры, цифровые компараторы, сумматоры, триггеры, регистры, счетчики); - запоминающие устройства; - цифро-аналоговые и аналого-цифровые преобразователи; - систему имен, адресации и маршрутизации трафика в сети Интернет;	идентифицировать полупроводниковые приборы и элементы системотехники и определять их параметры;	- в области по профессии наладчик технологического оборудования; - применения полученных знаний на практике.
15	ПК 3.6	Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.	современные программные средства защиты сетевой инфраструктуры	использовать современные программные средства защиты сетевой инфраструктуры	современными программными средствами защиты сетевой инфраструктуры

2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Семестры
		7
Обязательная учебная нагрузка (всего)	130	130
В том числе:		
занятия лекционного типа	60	60
практические занятия (практикумы)	60	60
лабораторные занятия	10	10
курсовое проектирование	-	-

Самостоятельная работа (всего)	65	65
в том числе:		
Рефераты	15	15
Самостоятельная внеаудиторная работа в виде домашних практических заданий, индивидуальных заданий, самостоятельного подбора и изучения дополнительного теоретического материала и др.	36	36
Консультации	14	14
Вид промежуточной аттестации		Зачет
Вид итоговой аттестации (экзамен)		
Общая трудоемкость 195 часов	195	195

2.2 Структура дисциплины

Освоение учебной дисциплины МДК.03.02 «Безопасность функционирования информационных систем» включает изучение следующих разделов и тем:

Раздел 1. Основы информационной безопасности

1. Понятие национальной безопасности.
2. Информационная безопасность в системе национальной безопасности Российской Федерации
3. Государственная информационная политика
4. Информация - наиболее ценный ресурс современного общества
5. Проблемы информационной войны
6. Проблемы информационной безопасности в сфере государственного и муниципального управления
7. Информационные системы
8. Методы и модели оценки уязвимости информации

Раздел 2. Проблемы информационной безопасности

1. Основные понятия и анализ угроз информационной безопасности.
2. Проблемы информационной безопасности сетей.
3. Политика безопасности.
4. Стандарты информационной безопасности.

Раздел 3. Технологии защиты данных

1. Принципы криптографической защиты информации.
2. Криптографические алгоритмы.
3. Технологии аутентификации.

Раздел 4. Технологии защиты межсетевого обмена данными

1. Обеспечение безопасности операционных систем.
2. Технологии межсетевых экранов.
3. Основы технологии виртуальных защищенных сетей VPN.
4. Защита на канальном и сеансовом уровнях.
5. Защита на сетевом уровне - протокол IPSEC.
6. Инфраструктура защиты на прикладном уровне.
7. Анализ защищенности и обнаружение атак.
8. Защита от вирусов. Методы управления средствами сетевой безопасности.
9. Построение системы антивирусной защиты корпоративной сети.

2.3 Тематический план и содержание учебной дисциплины МДК.03.02 Безопасность функционирования информационных систем

Наименование разделов и тем	Содержание учебного материала, практические и лабораторные работы, самостоятельная работа обучающихся	Объем часов
1	2	3
Раздел 1. Основы информационной безопасности	***Содержание учебного материала***	**44**
	Лекции 1. Понятие национальной безопасности. 2. Информационная безопасность в системе национальной безопасности Российской Федерации 3. Государственная информационная политика 4. Информация - наиболее ценный ресурс современного общества 5. Проблемы информационной войны 6. Проблемы информационной безопасности в сфере государственного и муниципального управления 7. Информационные системы 8. Методы и модели оценки уязвимости информации	20
	Практические занятия Построение структуры нормативно-правовых документов деятельности компании на базе российского законодательства в сфере информационного права Подготовка описания охраняемой информации, модели угроз, построение модели информационной безопасности	8
	Самостоятельная работа Работа с конспектом. Выполнение заданий практической работы.	16
Раздел 2. Проблемы информационной безопасности	***Содержание учебного материала***	**42**
	Лекции 1. Основные понятия и анализ угроз информационной безопасности. 2. Проблемы информационной безопасности сетей. 3. Политика безопасности. 4. Стандарты информационной безопасности.	10
	Практические занятия Проведение анализа сравнительных характеристик у каналов утечки информации Исследование проблем создания и развития национальной системы управления цифровыми сертификатами Исследование защиты в среде Windows , Linux	12
	Лабораторные занятия Использование встроенных средств ОС для обеспечения безопасности Установка программных средств защиты (программные прокси-серверы, диагностические программы и т.п.)	4

Наименование разделов и тем	Содержание учебного материала, практические и лабораторные работы, самостоятельная работа обучающихся	Объем часов
	Самостоятельная работа Работа с конспектом. Выполнение заданий практической работы. Подготовка рефератов.	16
Раздел 3. Технологии защиты данных	***Содержание учебного материала***	**46**
	Лекции **6** Принципы криптографической защиты информации. **7** Криптографические алгоритмы. **8** Технологии аутентификации.	8
	Практические занятия Составление описания основных классов вирусов Системы обнаружения вторжений Количественная оценка стойкости парольной защиты. Описание механизмов и принципов работы систем шифрования с открытым ключом. Изучение стандарта криптографической защиты AES (Advanced Encryption Standart). Изучение отечественных стандартов хэш-функции и цифровой подписи.	18
	Лабораторные занятия Управление пользователями и их правами доступа в ОС Использование программы Ethereal для анализа сетевого трафика	4
	Самостоятельная работа Работа с конспектом. Выполнение заданий практической работы. Подготовка рефератов.	16
Раздел 4. Технологии защиты межсетевого обмена данными	***Содержание учебного материала***	**63**
	Лекции 1. Обеспечение безопасности операционных систем. 2. Технологии межсетевых экранов. 3. Основы технологии виртуальных защищенных сетей VPN. 4. Защита на канальном и сеансовом уровнях. 5. Защита на сетевом уровне - протокол IPSEC. 6. Инфраструктура защиты на прикладном уровне. 7. Анализ защищенности и обнаружение атак. 8. Защита от вирусов. Методы управления средствами сетевой безопасности. 9. Построение системы антивирусной защиты корпоративной сети.	22
	Практические занятия Сканеры безопасности операционных систем. Сканеры безопасности сетевых сервисов и протоколов Межсетевые экраны и фильтры: Outpost Firewall Pro Компоненты межсетевого экрана. Политика межсетевого экранирования. Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне. Организация VPN средствами протокола PPTP. Защита данных на сетевом уровне. Организация VPN средствами СЗИ VipNet. Использование протокола IPSec для защиты сетей. Защита на транспортном уровне. Организация VPN средствами протокола SSL в Windows Server. Распределенные системы обнаружения атак. Система обнаружения атак Snort.	22
	Лабораторные работы Анализ протоколов Ethernet ARP, TCP, IP	2
	Самостоятельная работа Работа с конспектом. Выполнение заданий практической работы. Подготовка рефератов.	17
Всего:		**195**

2.4 Содержание разделов дисциплины

2.4.1 Занятия лекционного типа

Раздел 1. Основы информационной безопасности

1. Информационная безопасность в системе национальной безопасности Российской Федерации.

Основные понятия, общеметодологические принципы обеспечения информационной безопасности. Национальные интересы в информационной сфере. Источники и содержание угроз в информационной сфере.

2. Государственная информационная политика.

Основные положения государственной информационной политики Российской Федерации. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности.

3. Информация - наиболее ценный ресурс современного общества.

Понятие "информационный ресурс”. Классы информационных ресурсов.

4. Проблемы информационной войны.

Информационное оружие и его классификация. Информационная война.

5. Проблемы информационной безопасности в сфере государственного и муниципального управления.

6. Проблемы информационной безопасности в сфере государственного и муниципального управления.

Информационные процессы в сфере государственного и муниципального управления. Виды информации и информационных ресурсов в сфере ГМУ. Состояние и перспективы информатизации сферы ГМУ.

7. Информационные системы.

Общие положения. Информация как продукт. Информационные услуги. Источники конфиденциальной информации в информационных системах.

8. Методы и модели оценки уязвимости информации Эмпирический подход к оценке уязвимости информации. Система с полным перекрытием. Практическая реализация модели «угроза-защита.

Раздел 2. Проблемы информационной безопасности

1. Основные понятия и анализ угроз информационной безопасности.

Основные понятия защиты информации и информационной безопасности. Анализ угроз информационной безопасности.

2. Проблемы информационной безопасности сетей.

Введение в сетевой информационный обмен. Анализ угроз сетевой безопасности. Обеспечение информационной безопасности сетей.

3. Политика безопасности.

Основные понятия политики безопасности. Структура политики безопасности организации.

4. Стандарты информационной безопасности.

Роль стандартов информационной безопасности. Международные стандарты информационной безопасности. Отечественные стандарты безопасности информационных технологий.

Раздел 3. Технологии защиты данных

1. Принципы криптографической защиты информации.

Основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Асимметричные криптосистемы шифрования. Комбинированная криптосистема шифрования. Электронная цифровая подпись и функция хэширования.

2. Криптографические алгоритмы.

Классификация криптографических алгоритмов. Симметричные алгоритмы шифрования. Асимметричные криптоалгоритмы.

3. Технологии аутентификации.

Аутентификация, авторизация и администрирование действий пользователей. Методы аутентификации, использующие пароли и PIN-коды. Строгая аутентификация. Биометрическая аутентификация пользователя.

Раздел 4. Технологии защиты межсетевого обмена данными

1. Обеспечение безопасности операционных систем.

Проблемы обеспечения безопасности ОС. Архитектура подсистемы защиты ОС.

2. Технологии межсетевых экранов.

Функции межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Схемы сетевой защиты на базе МЭ.

3. Основы технологии виртуальных защищенных сетей VPN.

Концепция построения виртуальных защищенных сетей VPN. VPN-решения для построения защищенных сетей. Достоинства применения технологий VPN.

4. Защита на канальном и сеансовом уровнях.

Протоколы формирования защищенных каналов на канальном уровне. Протоколы формирования защищенных каналов на сеансовом уровне. Защита беспроводных сетей.

5. Защита на сетевом уровне - протокол IPSEC.

Архитектура средств безопасности IPSec. Защита передаваемых данных с помощью протоколов AH и ESP. Протокол управления криптоключами IK E . Особенности реализации средств IPSec

6. Инфраструктура защиты на прикладном уровне.

Управление идентификацией и доступом. Организация защищенного удаленного доступа. Управление доступом по схеме однократного входа с авторизацией Single Sign-On. Протокол Kerberos. Инфраструктура управления открытыми ключами РЮ.

7. Анализ защищенности и обнаружение атак.

Концепция адаптивного управления безопасностью. Технология анализа защищенности. Технологии обнаружения атак.

8. Защита от вирусов. Методы управления средствами сетевой безопасности.

Компьютерные вирусы и проблемы антивирусной защиты. Антивирусные программы и комплексы

9. Построение системы антивирусной защиты корпоративной сети. Задачи управления системой сетевой безопасности. Архитектура управления средствами сетевой безопасности.

2.4.2 Занятия семинарского типа

- не предусмотрены

2.4.3 Практические занятия (Лабораторные занятия)

Практические занятия

Практическое занятие №1. Построение структуры нормативно-правовых документов деятельности компании на базе российского законодательства в сфере информационного права.

Практическое занятие №2. Подготовка описания охраняемой информации, модели угроз, построение модели информационной безопасности.

Практическое занятие №3. Проведение анализа сравнительных характеристик у каналов утечки информации.

Практическое занятие №4. Исследование проблем создания и развития национальной системы управления цифровыми сертификатами.

Практическое занятие №5. Исследование защиты в среде Windows, Linux.

Практическое занятие №6. Составление описания основных классов вирусов.

Практическое занятие №7. Системы обнаружения вторжений.

Практическое занятие №8. Количественная оценка стойкости парольной защиты.

Практическое занятие №9. Описание механизмов и принципов работы систем. шифрования с открытым ключом.

Практическое занятие №10. Изучение стандарта криптографической защиты AES (Advanced Encryption Standart).

Практическое занятие №11. Изучение отечественных стандартов хэш-функции и цифровой подписи.

Практическое занятие №12. Сканеры безопасности операционных систем.

Практическое занятие №13. Сканеры безопасности сетевых сервисов и протоколов

Практическое занятие №14. Межсетевые экраны и фильтры: Outpost Firewall Pro

Практическое занятие №15. Компоненты межсетевого экрана. Политика межсетевого экранирования.

Практическое занятие №16. Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне.

Практическое занятие №17. Организация VPN средствами протокола PPTP. Защита данных на сетевом уровне.

Практическое занятие №18. Организация VPN средствами СЗИ VipNet.

Использование протокола IPSec для защиты сетей. Защита на транспортном уровне.

Практическое занятие №19. Организация VPN средствами протокола SSL в Windows Server.

Практическое занятие №20. Распределенные системы обнаружения атак. Система обнаружения атак Snort.

Лабораторные занятия

Лабораторная работа №1. Использование встроенных средств ОС для обеспечения безопасности.

Лабораторная работа №2. Установка программных средств защиты (программные прокси-серверы, диагностические программы и т.п.).

Лабораторная работа №3. Управление пользователями и их правами доступа в ОС Windows.

Лабораторная работа №4. Использование программы Ethereal для анализа сетевого трафика.

Лабораторная работа №5. Анализ протоколов Ethernet ARP, TCP, IP.

2.4.4 Содержание самостоятельной работы (Примерная тематика рефератов)

1. Виртуальные частные сети.

2. Свойства вирусов, фазы исполнения вируса, основные подходы к классификации компьютерных вирусов.

3. Полиморфные и стелс-вирусы.

4. Модель защиты Кларка-Вилсона.

5. Модель защиты Балла-Ла Падулы.

6. Понятие изолированной программной среды, условия создания изолированной программной среды. Потенциально возможные злоумышленные действия.

7. Понятие функции хэширования, дайджест сообщения, свойства необратимости, рассеивания и чувствительности к изменениям.

8. Принцип функционирования асимметричных криптосистем, Функциональная схема взаимодействия участников асимметричного криптографического обмена.

9. Понятие однонаправленной функции, примеры однонаправленных функций, имеющих большое значение для криптографии (целочисленное умножение,

модульная экспонента).

10. Функциональная схема взаимодействия участников симмет-ричного крипто-графического обмена. Недостатки симметричных криптосистем.

11. Шифрование методами перестановки**.** Суть метода. Шифрую-щие таблицы, метод простой перестановки, перестановки по маршрутам Гамильтона.

12. Алгоритмы работы генераторов псевдослучайных чисел (метод фон Неймана, линейный конгруэнтный метод).

2.4.5 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Самостоятельная работа учащихся является важнейшей формой учебно-воспитательного процесса.

Основная цель самостоятельной работы при изучении дисциплины - закрепить теоретические знания, полученные в ход лекционных занятий, а также сформировать практические навыки подготовки в области технических средств информатизации.

Самостоятельная работа учащихся в процессе освоения дисциплины включает:

- изучение основной и дополнительной литературы по предмету;
- изучение (конспектирование) вопросов, вызывающих затруднения при их изучении;
- работу с электронными учебными ресурсами;
- изучение материалов периодической печати, интернет ресурсов;
- подготовку к тестированию;
- подготовку к практическим (лабораторным) занятиям,
- выполнение домашних заданий,
- подготовку реферата (доклада, эссе) по одной из тем курса.

На самостоятельную работу студентов отводится 65 часов учебного времени.

Наименование раздела, темы	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
Понятие национальной безопасности.	Кияев, В. Безопасность информационных систем : курс / В. Кияев, О. Граничин. - М. : Национальный Открытый Уни-

	верситет «ИНТУИТ», 2016. - 192 с. : ил. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429032
Информационная безопасность в системе национальной безопасности Российской Федерации	Кияев, В. Безопасность информационных систем : курс / В. Кияев, О. Граничин. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. : ил. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429032
Государственная информационная политика	Кияев, В. Безопасность информационных систем : курс / В. Кияев, О. Граничин. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. : ил. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429032
Информация - наиболее ценный ресурс современного общества	Кияев, В. Безопасность информационных систем : курс / В. Кияев, О. Граничин. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. : ил. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429032
Проблемы информационной войны	Кияев, В. Безопасность информационных систем : курс / В. Кияев, О. Граничин. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. : ил. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429032
Проблемы информационной безопасности в сфере государственного и муниципального управления	Кияев, В. Безопасность информационных систем : курс / В. Кияев, О. Граничин. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. : ил. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429032
Информационные системы	Кияев, В. Безопасность информационных систем : курс / В. Кияев, О. Граничин. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. : ил. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429032
Методы и модели оценки уязвимости информации	Кияев, В. Безопасность информационных систем : курс / В. Кияев, О. Граничин. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. : ил. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429032
Основные понятия и анализ угроз информационной безопасности.	Кияев, В. Безопасность информационных систем : курс / В. Кияев, О. Граничин. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. : ил. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429032
Проблемы информационной безопасности сетей.	Кияев, В. Безопасность информационных систем : курс / В. Кияев, О. Граничин. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. : ил. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429032
Политика безопасности.	Кияев, В. Безопасность информационных систем : курс / В. Кияев, О. Граничин. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. : ил. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429032
Стандарты информационной безопасности.	Кияев, В. Безопасность информационных систем : курс / В. Кияев, О. Граничин. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. : ил. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429032
Принципы криптографической защиты информации.	Кияев, В. Безопасность информационных систем : курс / В. Кияев, О. Граничин. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. : ил. ; То же [Электронный

	ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429032
Криптографические алгоритмы.	Кияев, В. Безопасность информационных систем : курс / В. Кияев, О. Граничин. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. : ил. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429032
Технологии аутентификации.	Кияев, В. Безопасность информационных систем : курс / В. Кияев, О. Граничин. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. : ил. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429032
Обеспечение безопасности операционных систем.	Кияев, В. Безопасность информационных систем : курс / В. Кияев, О. Граничин. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. : ил. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429032
Технологии межсетевых экранов.	Лапонина, О.Р. Протоколы безопасного сетевого взаимодействия / О.Р. Лапонина. - 2-е изд., исправ. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 462 с. - (Основы информационных технологий). - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429094
Основы технологии виртуальных защищенных сетей VPN.	Лапонина, О.Р. Протоколы безопасного сетевого взаимодействия / О.Р. Лапонина. - 2-е изд., исправ. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 462 с. - (Основы информационных технологий). - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429094
Защита на канальном и сеансовом уровнях.	Лапонина, О.Р. Протоколы безопасного сетевого взаимодействия / О.Р. Лапонина. - 2-е изд., исправ. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 462 с. - (Основы информационных технологий). - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429094
Защита на сетевом уровне - протокол IPSEC.	Лапонина, О.Р. Протоколы безопасного сетевого взаимодействия / О.Р. Лапонина. - 2-е изд., исправ. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 462 с. - (Основы информационных технологий). - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429094
Инфраструктура защиты на прикладном уровне.	Лапонина, О.Р. Протоколы безопасного сетевого взаимодействия / О.Р. Лапонина. - 2-е изд., исправ. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 462 с. - (Основы информационных технологий). - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429094
Анализ защищенности и обнаружение атак.	Кияев, В. Безопасность информационных систем : курс / В. Кияев, О. Граничин. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. : ил. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429032
Защита от вирусов. Методы управления средствами сетевой безопасности.	Кияев, В. Безопасность информационных систем : курс / В. Кияев, О. Граничин. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. : ил. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429032
Построение системы антивирусной защиты корпоративной сети.	Кияев, В. Безопасность информационных систем : курс / В. Кияев, О. Граничин. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. : ил. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429032

Кроме перечисленных источников учащийся может воспользоваться поисковыми системами сети Интернет по теме самостоятельной работы.

Началом организации любой самостоятельной работы должно быть привитие навыков и умений грамотной работы с учебной и научной литературой. Этот процесс, в первую очередь, связан с нахождением необходимой для успешного овладения учебным материалом литературой. Учащийся должен уметь пользоваться фондами библиотек и справочно-библиографическими изданиями.

3 ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Для обучения организации администрирования компьютерных систем предусматривается использование в учебном процессе активных и интерактивных форм проведения аудиторных и внеаудиторных занятий с целью формирования и развития профессиональных навыков обучающихся.

В процессе обучения применяются образовательные технологии личностно-деятельностного, развивающего и проблемного обучения. Обязателен лабораторный практикум по разделам дисциплины.

В учебном процессе наряду с традиционными образовательными технологиями используются компьютерное тестирование, тематические презентации, интерактивные технологии.

3.1 Образовательные технологии при проведении лекций

Тема	Виды применяемых образовательных технологий
Понятие национальной безопасности.	Технология развивающего обучения
Информационная безопасность в системе национальной безопасности Российской Федерации	Личностно-деятельностное обучение
Государственная информационная политика	Технология развивающего обучения
Информация - наиболее ценный ресурс современного общества	Личностно-деятельностное обучение
Проблемы информационной войны	Технология развивающего обучения
Проблемы информационной безопасности в сфере государственного и муниципального управления	Дифференцированное обучение
Информационные системы	Технология развивающего обучения
Методы и модели оценки уязвимости информации	Технология развивающего обучения
Основные понятия и анализ угроз информационной безопасности.	Личностно-деятельностное обучение
Проблемы информационной безопасности сетей.	Технология развивающего обучения
Политика безопасности.	Личностно-деятельностное обучение
Стандарты информационной безопасности.	Дифференцированное обучение
Принципы криптографической защиты информации.	Личностно-деятельностное обучение
Криптографические алгоритмы.	Дифференцированное обучение

Технологии аутентификации.	Технология развивающего обучения
Обеспечение безопасности операционных систем.	Личностно-деятельностное обучение
Технологии межсетевых экранов.	Технология развивающего обучения
Основы технологии виртуальных защищенных сетей VPN.	Технология развивающего обучения
Защита на канальном и сеансовом уровнях.	Технология развивающего обучения
Защита на сетевом уровне - протокол IPSEC.	Личностно-деятельностное обучение
Инфраструктура защиты на прикладном уровне.	Технология развивающего обучения
Анализ защищенности и обнаружение атак.	Технология развивающего обучения
Защита от вирусов. Методы управления средствами сетевой безопасности.	Личностно-деятельностное обучение
Построение системы антивирусной защиты корпоративной сети.	Технология развивающего обучения

3.2 Образовательные технологии при проведении практических и лабораторных занятий

Тема	Виды применяемых образовательных технологий
Построение структуры нормативно-правовых документов деятельности компании на базе российского законодательства в сфере информационного права.	Технология развивающего обучения
Подготовка описания охраняемой информации, модели угроз, построение модели информационной безопасности.	Технология личностно-деятельностного обучения
Проведение анализа сравнительных характеристик у каналов утечки информации.	Технология проблемного обучения
Исследование проблем создания и развития национальной системы управления цифровыми сертификатами.	Проективное обучение
Исследование защиты в среде Windows, Linux.	Технология проблемного обучения
Составление описания основных классов вирусов.	дифференцированное обучение
Системы обнаружения вторжений	Технология личностно-деятельностного обучения
Количественная оценка стойкости парольной защиты.	Проективное обучение
Описание механизмов и принципов работы систем шифрования с открытым ключом.	Технология личностно-деятельностного обучения
Изучение стандарта криптографической защиты AES (Advanced Encryption Standard).	Технология личностно-деятельностного обучения
Изучение отечественных стандартов хэш-функции и цифровой подписи.	Технология проблемного обучения
Сканеры безопасности операционных систем.	Технология проблемного обучения
Сканеры безопасности сетевых сервисов и протоколов	Технология проблемного обучения
Межсетевые экраны и фильтры: Outpost Firewall Pro	Технология проблемного обучения
Компоненты межсетевого экрана. Политика межсетевого экранирования.	Технология личностно-деятельностного обучения
Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне.	Технология личностно-деятельностного обучения
Организация VPN средствами протокола PPTP. Защита данных на сетевом уровне.	Технология личностно-деятельностного обучения
Организация VPN средствами СЗИ VipNet. Использование протокола IPSec для защиты сетей. Защита на транспортном уровне.	Технология личностно-деятельностного обучения
Организация VPN средствами протокола SSL в Windows Server.	Технология проблемного обучения
Распределенные системы обнаружения атак. Система обнаружения атак Snort.	дифференцированное обучение

Использование встроенных средств ОС для обеспечения безопасности.	Личностно-деятельностное обучение
Установка программных средств защиты (программные прокси-серверы, диагностические программы и т.п.).	Технология развивающего обучения
Управление пользователями и их правами доступа в ОС Windows	Технология личностно-деятельностного обучения
Использование программы Ethereal для анализа сетевого трафика.	Технология проблемного обучения
Анализ протоколов Ethernet ARP, TCP, IP	Технология развивающего обучения

4 УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

4.1 Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Реализация учебной дисциплины «Программное обеспечение компьютерных сетей» осуществляется в специально оборудованных кабинетах.

1. Лаборатория программно-аппаратной защиты объектов сетевой инфраструктуры (М23) включает: доска интерактивная, компьютер, мониторы — 30, мультимедиа-проектор, компьютерный стол, наглядные пособия, учебно-методические материалы, доска учебная, выход в Интернет.

4.2 Перечень необходимого программного обеспечения

1. 7-zip (лицензия на англ. http://www.7-zip.org/license.txt)
2. Adobe Acrobat Reade (лицензия - https://get.adobe.com/reader/?loc=ru&promoid=KLXME)
3. Adobe Flash Player (лицензия - https://get.adobe.com/reader/?loc=ru&promoid=KLXME)
4. Apache Open Office (лицензия - http://www.openoffice.org/license.html)
5. Free Commander (лицензия -https://freecommander.com/ru/%d0%bb%d0%b8%d1%86%d0%b5%d0%bd%d0%b7%d0%b8%d1%8f/)
6. Google Chrome (лицензия - https://www.google.ru/chrome/browser/privacy/eula_text.html)
7. Libre Office (в свободном доступе)
8. Mozilla Firefox (лицензия - https://www.mozilla.org/en-US/MPL/2.0/)
9. VirtualBox (в свободном доступе)

5 ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

5.1 Основная литература

1. Васильков А. В. Информационные системы и их безопасность : учебное пособие / А. В. Васильков, А. А. Васильков, И. А. Васильков. - М. : ФОРУМ, 2015. - 528 с.: ил. - (Профессиональное образование). - ISBN 978-5-91134-289-0.

2. Кияев, В. Безопасность информационных систем : курс / В. Кияев, О. Граничин. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. : ил. ; То же [Электронный ресурс]. - URL: http://biblioclub .ru/index.php ?page=book&id=429032

3. Лапонина, О.Р. Протоколы безопасного сетевого взаимодействия / О.Р. Лапонина. - 2-е изд., исправ. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 462 с. - (Основы информационных технологий). - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub .ru/index.php ?page=book&id=429094

5.2 Дополнительная литература

1. Мэйволд, Э. Безопасность сетей / Э. Мэйволд. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 572 с. : схем., ил. ; То же [Электронный ресурс]. - URL: http://biblioclub .ru/index.php ?page=book&id=429035

2. Царев, Р.Ю. Теоретические основы информатики : учебник / Р.Ю. Царев, А.Н. Пупков, В.В. Самарин и др. . - Красноярск : Сибирский федеральный университет, 2015. - 176 с. : табл., схем., ил. - Библиогр.: с. 140. - ISBN 978-57638-3192-4 ; То же [Электронный ресурс]. - URL:http://biblioclub.ru/index .php ?page=book&id=435 850

3. Прохорова, О.В. Информационная безопасность и защита информации : учебник / О.В. Прохорова. - Самара : Самарский государственный архитектурно-строительный университет, 2014. - 113 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-9585-0603-3 ; То же [Электронный ресурс]. - URL: http://biblioclub .ru/index.php ?page=book&id=43 8331

4. Надёжность информационных систем : лабораторный практикум / Ю.Ю.

Громов, И.В. Дидрих, О.Г. Иванова и др. ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет». - Тамбов : Издательство ФГБОУ ВПО «ТГТУ», 2015. - 113 с. : ил.,табл. - Библ. в кн. - ISBN 978-5-8265-1436-8 ; То же [Электронный ресурс]. -URL:**http://biblioclub.ru/index.php?page=book&id=444906**

5. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для СПО / Т. А. Полякова, А. А. Стрельцов, С. Г. Чу- букова, В. А. Ниесов ; отв. ред. Т. А. Полякова, А. А. Стрельцов. — М. : Юрайт, 2017. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. URL: **https://www.biblio-online.ru/book/054509D0-1E35-4080-9E86-19742B336897**

5.3 Периодические издания

1. Вестник Московского Университета. Серия 15. Вычислительная математика и кибернетика. - URL: **http://biblioclub.ru/index.php?page=journal_red&jid=237323**

2. Инновации на основе информационных и коммуникационных технологий. - URL: **http://elibrary.ru/contents.asp?issueid=1438371**.

3. Информатика в школе. URL: **http://dlib.eastview.com/browse/publication/18988/udb/1270**.

4. Информатика и образование. - URL: http://dlib.eastview.com/browse/publication/18946/udb/1270.

5. Информатика, вычислительная техника и инженерное образование. - URL: http://elibrary .ru/contents.asp?issueid= 1567393.

6. Методические вопросы преподавания инфокоммуникаций в высшей школе. - URL: http://elibrary.ru/contents.asp?titleid=55718

7. Мир ПК. - URL: http://dlib.eastview.com/browse/publication/64067/udb/2071.

8. Открытые системы. СУБД. - URL: http: //dlib .eastview.com/browse/publication/64072/udb/2071

9. Программные продукты и системы. - URL: http://dlib.eastview.com/browse/publication/64086/udb/2071.

10. Computerworld Россия. - URL:

http://dlib.eastview.com/browse/publication/64081/udb/2071.

11. Windows IT Pro / Re. - URL: http://dlib.eastview.com/browse/publication/64079/udb/2071.

5.4. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. ЭБС «Университетская библиотека ONLINE» [учебные, научные здания, первоисточники, художественные произведения различных издательств; журналы; мультимедийная коллекция: аудиокниги, аудиофайлы, видеокурсы, интерактивные курсы, экспресс-подготовка к экзаменам, презентации, тесты, карты, онлайн-энциклопедии, словари] сайт. - URL: http ://biblioclub.ru/index .php?page=main_ub_red.

2. ЭБС издательства «Лань» [учебные, научные издания, первоисточники, художественные произведения различных издательств; журналы] : сайт. - URL: http://edanbook.com.

3. ЭБС «Юрайт» [раздел «ВАША ПОДПИСКА: Филиал КубГУ (г. Славянск-на-Кубани): учебники и учебные пособия издательства «Юрайт»] : сайт. - URL: https://www.biblio-online.ru/catalog/E121B99F-E5ED-430E-A737-37D3A9E6DBFB.

4. ЭБС «Znanium.com» [учебные, научные, научно-популярные материалы различных издательств, журналы] : сайт. - URL: http://znanium.com/.

5. ЭБС «BOOK.ru» [учебные издания - коллекция для СПО] : сайт. - URL: https://www.book.ru/cat/576.

6. Научная электронная библиотека. Монографии, изданные в издательстве Российской Академии Естествознания [полнотекстовый ресурс свободного доступа] : сайт. - URL: https://www.monographies.ru/.

7. Научная электронная библиотека статей и публикаций «eLibrary.ru» [российский информационно-аналитический портал в области науки, технологии, медицины, образования; большая часть изданий - свободного доступа] : сайт. - URL: http://elibrary.ru.

8. Базы данных компании «Ист Вью» [раздел: Периодические издания (на русском языке) включает коллекции: Издания по общественным и

гуманитарным наукам; Издания по педагогике и образованию; Издания по информационным технологиям; Статистические издания России и стран СНГ] : сайт. - URL: http://dlib.eastview.com.

9. КиберЛенинка : научная электронная библиотека [научные журналы в полнотекстовом формате свободного доступа]: сайт. - URL: http://cyberleninka.ru.

10. Единое окно доступа к образовательным ресурсам : федеральная информационная система свободного доступа к интегральному каталогу образовательных интернет-ресурсов и к электронной библиотеке учебно-методических материалов для всех уровней образования: дошкольное, общее, среднее профессиональное, высшее, дополнительное : сайт. - URL: http://window.edu.ru.

11. Федеральный центр информационно-образовательных ресурсов [для общего, среднего профессионального, дополнительного образования; полнотекстовый ресурс свободного доступа] : сайт. - URL: http://fcior.edu.ru.

12. Единая коллекция цифровых образовательных ресурсов [для преподавания и изучения учебных дисциплин начального общего, основного общего и среднего (полного) общего образования; полнотекстовый ресурс свободного доступа] : сайт. - URL: http://school-collection.edu.ru.

13. Официальный интернет-портал правовой информации. Государственная система правовой информации [полнотекстовый ресурс свободного доступа] : сайт. - URL: http://publication.pravo.gov.ru.

14. Энциклопедиум [Энциклопедии. Словари. Справочники: полнотекстовый ресурс свободного доступа]// ЭБС «Университетская библиотека ONLINE» : сайт. - URL: http://enc.biblioclub.ru/.

15. Электронный каталог Кубанского государственного университета и филиалов. - URL: http://212.192.134.46/MegaPro/Web/Home/About

6. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ОБУЧАЮЩИМСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учащиеся для полноценного освоения курса «Безопасность функционирования информационных систем» должны составлять конспекты как при прослушивании его теоретической (лекционной) части, так и при подготовке к практическим (семинарским) занятиям. Желательно, чтобы конспекты лекций и семинаров записывались в логической последовательности изучения курса и содержались в одной тетради. Это обеспечит более полную подготовку как к текущим учебным занятиям, так и сессионному контролю знаний.

Самостоятельная работа учащихся является важнейшей формой учебно-познавательного процесса. Цель заданий для самостоятельной работы - закрепить и расширить знания, умения, навыки, приобретенные в результате изучения дисциплины; овладеть умением использовать полученные знания в практической работе; получить первичные навыки профессиональной деятельности по установке, настройке и обслуживанию технических и программно-аппаратных средств компьютерных сетей.

Задания для самостоятельной работы выполняются в письменном виде во внеаудиторное время. Работа должна носить творческий характер, при ее оценке преподаватель в первую очередь оценивает обоснованность и оригинальность выводов. В письменной работе по теме задания учащийся должен полно и всесторонне рассмотреть все аспекты темы, четко сформулировать и аргументировать свою позицию по исследуемым вопросам.

Отчеты по лабораторным и практическим занятиям должны содержать полные ответы на поставленные задания, необходимые таблицы должны быть заполнены. Защита лабораторных работ будет включать в себя просмотр письменных отчетов, устный опрос.

Общие правила выполнения письменных работ

На первом занятии студенты должны быть проинформированы о необходимости соблюдения норм академической этики и авторских прав в ходе обучения. В частности, предоставляются сведения:

1. общая информация об авторских правах;

2. правила цитирования;

3. правила оформления ссылок;

Все имеющиеся в тексте сноски тщательно выверяются и снабжаются «адресами».

Недопустимо включать в свою работу выдержки из работ других авторов без указания на это, пересказывать чужую работу близко к тексту без отсылки к ней, использовать чужие идеи без указания первоисточников (это касается и информации, найденной в Интернете). Все случаи плагиата должны быть исключены.

Список использованной литературы должен включать все источники информации, изученные и проработанные студентом в процессе выполнения работы, и должен быть составлен в соответствии с ГОСТ Р 7.0.5-2008 «Библиографическая ссылка. Общие требования и правила».

Требования к написанию реферата

Реферат по данному курсу является одним из методов организации самостоятельной работы. Темы рефератов являются дополнительным материалом для изучение данной дисциплины. Реферат оценивается в один балл в оценке итого экзамена

Реферат должен быть подготовлен согласно теме, предложенной преподавателем. Допускается самостоятельный выбор темы реферата, но по согласованию с преподавателем.

Для написания реферата студент самостоятельно подбирает источники информации по выбранной теме (литература учебная, периодическая и Интернет-ресурсы). Объем реферата - не менее 10 страниц формата А4.

Реферат должен иметь титульный лист, содержание, текст должен быть разбит на разделы, согласно содержанию, заключение, список литературы (не менее 5 источников). Обсуждение тем рефератов проводится на тех практических занятиях, по которым они распределены.

Доклад по теме по реферата не должен превышать 10 минут. Выступающий должен подготовить краткие выводы по теме реферата для конспектирования.

Сдача реферата преподавателю обязательна.

7 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ УСПЕВАЕМОСТИ

7.1 Паспорт фонда оценочных средств

№ п/п	Контролируемые разделы (темы) дисциплины	Компетенции	Наименование оценочного средства
1	Понятие национальной безопасности.	ОК 1-9, ПК 3.1	Проверка конспектов, практ. работа, тест
2	Информационная безопасность в системе национальной безопасности Российской Федерации	ОК 1-9, ПК 3.1	Проверка конспектов, практ. работа, тест, реферат
3	Государственная информационная политика	ОК 1-9, ПК 3.1	Проверка конспектов, практ. работа, тест
4	Информация - наиболее ценный ресурс современного общества	ОК 1-9, ПК 3.1	Проверка конспектов, практ. работа, тест
5	Проблемы информационной войны	ОК 1-9, ПК 3.1	Проверка конспектов, практ. работа, реферат, тест
6	Проблемы информационной безопасности в сфере государственного и муниципального управления	ОК 1-9, ПК 3.1	Проверка конспектов, практ. работа, реферат, тест
7	Информационные системы	ОК 1-9, ПК 3.1-3.3	Проверка конспектов, практ. работа, тест
8	Методы и модели оценки уязвимости информации	ОК 1-9, ПК 3.1-3.6	Проверка конспектов, практ. работа, тест
9	Основные понятия и анализ угроз информационной безопасности.	ОК 1-9, ПК 3.1	Проверка конспектов, практ. работа, реферат, тест
10	Проблемы информационной безопасности сетей.	ОК 1-9, ПК 3.1	Проверка конспектов, практ. работа, тест
11	Политика безопасности.	ОК 1-9, ПК 3.1	Проверка конспектов, практ. работа, реферат, тест
12	Стандарты информационной безопасности.	ОК 1-9, ПК 3.1	Проверка конспектов, практ. работа, реферат, тест
13	Принципы криптографической защиты информации.	ОК 1-9, ПК 3.1,3.3	Проверка конспектов, практ. работа, тест
14	Криптографические алгоритмы.	ОК 1-9, ПК 3.1,3.3	Проверка конспектов, практ. работа, тест
15	Технологии аутентификации.	ОК 1-9, ПК 3.1,3.3	Проверка конспектов, практ. работа, тест
16	Обеспечение безопасности операционных систем.	ОК 1-9, ПК 3.1,3.3-3.6	Проверка конспектов, практ. работа, тест
17	Технологии межсетевых экранов.	ОК 1-9, ПК 3.1,3.3	Проверка конспектов, практ. работа, тест
18	Основы технологии виртуальных защищенных сетей VPN.	ОК 1-9, ПК 3.1,3.3	Проверка конспектов, практ. работа, тест
19	Защита на канальном и сеансовом уровнях.	ОК 1-9, ПК 3.1,3.3	Проверка конспектов, практ. работа, тест
20	Защита на сетевом уровне - протокол IPSEC.	ОК 1-9, ПК 3.1,3.3	Проверка конспектов, практ. работа, тест
21	Инфраструктура защиты на прикладном уровне.	ОК 1-9, ПК 3.1,3.3	Проверка конспектов, практ. работа, тест
22	Анализ защищенности и обнаружение атак.	ОК 1-9, ПК 3.1,3.3	Проверка конспектов, практ. работа, тест
23	Защита от вирусов. Методы управления средствами сетевой безопасности.	ОК 1-9, ПК 3.1,3.3	Проверка конспектов, практ. работа, тест, реферат
24	Построение системы антивирусной защиты корпоративной сети.	ОК 1-9, ПК 3.1,3.3-3.6	Проверка конспектов, практ. работа, тест

7.2 Критерии оценки результатов обучения

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения практических работ, тестирования, собеседования по результатам выполнения лабораторных работ, а также решения задач, составления рабочих таблиц и подготовки сообщений к уроку. Знания студентов на практических занятиях оцениваются отметками «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно».

Оценка «отлично» выставляется, когда студень показывает глубокое всестороннее знание раздела дисциплины, обязательной и дополнительной литературы, аргументировано и логически стройно излагает материал, может применять знания для анализа конкретных ситуаций.

Оценка «хорошо» ставится при твердых знаниях раздела дисциплины, обязательной литературы, знакомстве с дополнительной литературой,

аргументированном изложении материала, умении применить знания для анализа конкретных ситуаций.

Оценка «удовлетворительно» ставится, когда студент в основном знает раздел дисциплины, может практически применить свои знания.

Оценка «неудовлетворительно» ставится, когда студент не освоил основного содержания предмета и слабо знает изучаемый раздел дисциплины.

7.3 Оценочные средства для проведения текущей аттестации

Текущий контроль может проводиться в форме:

-фронтальный опрос -индивидуальный устный опрос

-письменный контроль

-тестирование по теоретическому материалу

-практическая (лабораторная) работа -защита реферата,

-защита выполненного задания,

-разработка проблемы курса (сообщение).

Форма аттестации	Знания	Умения	Владения (навыки)	Личные качества студента	Примеры оценочных средств
Устный (письменный) опрос по темам	Контроль знаний по определенным проблемам	Оценка умения различать конкретные понятия	Оценка навыков работы с литературными источниками	Оценка способности оперативно и качественно отвечать на поставленные вопросы	Контрольные вопросы по темам прилагаются
Рефераты	Контроль знаний по определенным проблемам	Оценка умения различать конкретные понятия	Оценка навыков работы с литературными источниками	Оценка способности к самостоятельной работе и анализу литературных источников	Темы рефератов прилагаются
Практические (лабораторные) работы	Контроль знания теоретических основ информатики и информационных технологий, возможностей и принципов использования современной компьютерной техники.	Оценка умения работать с современной компьютерной техникой, использовать возможности вычислительной техники и программного обеспечения при решении практических задач.	Оценка навыков работы с техническими средствами информатизации, специальными программными средствами	Оценка способности оперативно и качественно решать поставленные на практических работах задачи и аргументировать результаты	Темы работ прилагаются
Тестирование	Контроль знаний по определенным проблемам	Оценка умения различать конкретные понятия	Оценка навыков логического анализа и синтеза при сопоставлении конкретных понятий	Оценка способности оперативно и качественно отвечать на поставленные вопросы	Вопросы прилагаются

Реферат.

Реферат является продуктом самостоятельной работы учащегося и представляет собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где раскрывается суть исследуемой проблемы, приводятся различные точки зрения, а также собственные взгляды учащегося на нее.

Контрольная работа.

Контрольная работа является набором практических заданий и задач по темам изучаемой дисциплины, позволяющих формировать знания, а также умения обучающихся в области физики.

Примеры задач и вопросов к контрольной работе:

1. Терминология в области безопасности информационных сетей.
2. Методология построения безопасных информационных сетей.

3. Типовые модели атак, направленные на преодоление защиты информационных систем, условия их осуществимости, возможные последствия, способы предотвращения.

4. Описать роль человеческого фактора в обеспечении безопасности сетей.

5 Сформировать и произвести назначение ролей пользователям информационной системы.

6. Описать классификацию компьютерных вирусов.

7. Перечислить основные законодательные документы в области обеспечения безопасности хранения и обработки информации.

Примеры тестовых заданий:

1. Информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации и представляет собой коммерческую, служебную или личную тайны, охраняющиеся её владельцем, называется

А) конфиденциальной

Б) доступной

В) целостной

Г) все варианты верны

2. Набор правил, которые регламентируют функционирование механизма информационной безопасности называются

А) политикой

Б) идентификацией

В) конфиденциальностью

Г)все варианты верны

3. Формирование профиля прав для конкретного участника процесса информационного обмена, называется

А) авторизацией

Б)идентификацией

В) аутентификацией

Г)все варианты верны

4. Устройства контроля доступа из одной информационной среды в другую предоставляют

А) межсетевые экраны

Б) антивирусное обеспечение

В) сканеры безопасности

Г) все варианты верны

5. Устройства проверки качества функционирования модели безопасности для конкретной информационной системы обеспечивают

А) сканеры безопасности

Б)антивирусные программы

В) межсетевые экраны

Г) все варианты верны

6. Обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети - это

А) модель межсетевого взаимодействия OSI

Б)виртуальная частная сеть VPN

В) протокол IPSEC

Г) межсетевые экраны

7. Сетевой протокол аутентификации, который предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними - это

А) протокол Kerberos

Б) протокол ARP

В) протокол ICMP

Г)протокол POP3

7.4 Оценочные средства для проведения промежуточной аттестации

Форма аттестации	Знания	Умения	Владение (навыки)	Личные качества студента	Примеры оценочных средств
Итоговая аттестация					
Экзамен	Контроль знания базовых положений в области администрирования компьютерных систем	Оценка умения понимать специальную терминологию. Оценка умения решать типовые задачи в области эксплуатации объектов сетевой инфраструктуры	Оценка навыков логического сопоставления и характеристики объектов Оценка навыков логического мышления при решении задач в области эксплуатации объектов сетевой инфраструктуры	Оценка способности грамотно и четко излагать материал Оценка способности грамотно и четко излагать ход решения задач в области эксплуатации объектов сетевой инфраструктуры	Вопросы прилагаются Задачи прилагаются

7.4.1 Примерные вопросы для проведения промежуточной аттестации

Вопросы зачета

1. Понятие национальной безопасности
2. Национальные интересы в информационной сфере.
3. Источники и содержание угроз в информационной сфере
4. Понятие "информационный ресурс". Классы информационных ресурсов
5. Понятие информационной системы. Источники конфиденциальной информации в информационных системах
6. Основные понятия политики безопасности.
7. Структура политики безопасности организации
8. Стандарты информационной безопасности
9. Основные понятия криптографической защиты информации.
10. Симметричные криптосистемы шифрования.
11. Асимметричные криптосистемы шифрования.
12. Электронная цифровая подпись и функция хэширования
13. Аутентификация, авторизация и администрирование действий пользователей
14. Концепция построения виртуальных защищенных сетей VPN
15. Протоколы формирования защищенных каналов на канальном и сеансовом уровнях.

16. Технологии защиты в беспроводных сетях.
17. Протокол Kerberos
18. Технологии обнаружения атак
19. Компьютерные вирусы и проблемы антивирусной защиты
10. Антивирусные программы и комплексы

7.4.2 Примерные задачи для проведения промежуточной аттестации

1. Продемонстрировать использование встроенных средств ОС для обеспечения безопасности.
2. Продемонстрировать процесс установки и настройки программных средств защиты (программные прокси-серверы, диагностические программы и т.п.).
4. Продемонстрировать управление пользователями и их правами доступа в ОС Windows
5. Продемонстрировать использование программы Ethereal для анализа сетевого трафика
6. Провести анализ уровня безопасности защиты данных в ОС Windows

8 ДОПОЛНИТЕЛЬНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Средства защиты каналов при передаче персональных данных

Для обеспечения безопасности ПДн при передаче по открытым каналам или в несегментированной сети служит подсистема криптографической защиты каналов связи. Помимо вышеназванной задачи данная подсистема позволяет обеспечивать безопасное взаимодействие с технологическими сетями и доступ для осуществления удаленного администрирования. Данная подсистема может быть реализована на основе программно-аппаратного комплекса Cisco Adaptive Security Appliance. Этот комплекс сертифицирован ФСТЭК (соответствие руководящим документам по межсетевым экранам (3 и 4 Класс) и требованиям технических условий).

Cisco ASA 5500 предназначен для решения сразу нескольких задач - разграничения доступа к сетевым ресурсам, защиты от атак, защиты взаимодействия с удаленными территориями, блокирования вирусов, червей, шпионского ПО и других вредоносных программ, спама и атак типа «фишинг». Это достигается за счет

объединения в одном устройстве лучших защитных средств - межсетевого экрана Cisco Pix, системы предотвращения атак Cisco IPS и Cisco VPN 3000 Concentrator.

Помимо описанных выше программно-технических средств защиты компания «Инфосистемы Джет» широко использует продукты других ведущих производителей на рынке информационной безопасности. К ним, в частности, относятся Oracle, Aladdin, Check Point, «С-Терра СиЭсПи», «КриптоПро». Данные компании проводят активную позицию по соответствию требований регуляторов и сертификации своих продуктов с целью их применения в решениях по защите персональных данных.

Требования к средствам защиты ПДн

Для реализации перечисленных подсистем, общая структура СЗПДн может включать в себя как существующие, так и дополнительные программно аппаратные средства защиты информации.

В соответствии с Постановлением Правительства РФ от 17 ноября 2007 г. № 781 «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» технические и программные средства, используемые для обработки данных в информационных системах персональных данных (ИСПДн), должны в установленном порядке проходить процедуру оценки соответствия, включая сертификацию на соответствие требованиям по безопасности информации.

В отношении разработанных шифровальных (криптографических) средств защиты информации, предназначенных для обеспечения безопасности персональных данных при их обработке в информационных системах, проводятся тематические исследования и контрольные тематические исследования в целях проверки выполнения требований по безопасности информации10.

Результаты оценки соответствия (сертификации) и тематических исследований средств защиты информации, предназначенных для обеспечения безопасности персональных данных при их обработке в информационных системах, оцениваются в ходе экспертизы, осуществляемой Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности РФ.

К средствам защиты информации, предназначенным для обеспечения безопасности персональных данных при их обработке в информационных системах,

прилагаются правила пользования этими средствами, согласованные с Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

Изменение условий применения средств защиты информации (происходящие, например, в ходе модернизации ИСПДн), предусмотренных указанными правилами, согласовывается с ФСТЭК и ФСБ.

Средства защиты информации, предназначенные для обеспечения безопасности персональных данных при их обработке в информационных системах, подлежат учету с использованием индексов или условных наименований и регистрационных номеров. Перечень индексов, условных наименований и регистрационных номеров определяется Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации.

Особенности разработки, производства, реализации и эксплуатации шифровальных (криптографических) средств защиты информации и предоставления услуг по шифрованию персональных данных при их обработке в информационных системах устанавливаются Федеральной службой безопасности Российской Федерации.

Все сертифицированные ФСТЭК средства защиты представлены на сайте ФСТЭК (http://www.fstec.ru/) в разделе «Сведения о Системе сертификации средств защиты информации по требованиям безопасности информации» (http://www.fstec.ru/_razd/_serto.htm) в подразделе «Государственный реестр сертифицированных средств защиты информации».

Этапы создания СЗПДн

Рекомендуются следующие этапы создания систем защиты персональных данных:

- предпроектная стадия, включающая предпроектное обследование ИСПДн, разработку технического (частного технического) задания на ее создание;
- стадия проектирования (разработки проектов) и реализации ИСПДн, включающая разработку СЗПДн в составе ИСПДн;
- стадия ввода в действие СЗПДн, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку

соответствия ИСПДн требованиям безопасности информации.

Предпроектное обследование

На этапе предпроектного обследования рекомендуются следующие мероприятия:

- устанавливается необходимость обработки данных в ИСПДн;
- определяется перечень ПДн, подлежащих защите от несанкционированного доступа;
- определяются условия расположения ИСПДн относительно границ контролируемой зоны (КЗ);
- определяются конфигурация и топология ИСПДн в целом и ее отдельных компонент, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;
- определяются технические средства и системы, предполагаемые к использованию в разрабатываемой ИСПДн, условия их расположения, общесистемные и прикладные программные средства, имеющиеся и предлагаемые к разработке;
- определяются режимы обработки ПДн в ИСПДн в целом и в отдельных компонентах;
- определяется класс ИСПДн;
- уточняется степень участия персонала в обработке данных, характер их взаимодействия между собой;
- определяются (уточняются) угрозы безопасности ПДн в конкретных условиях функционирования (разработка частной модели угроз).

Разработка технического задания

По результатам предпроектного обследования с учетом установленного класса ИСПДн задаются конкретные требования по обеспечению безопасности данных, включаемые в техническое (частное техническое) задание на разработку системы защиты.

Техническое (частное техническое) задание на разработку СЗПДн должно содержать:

- обоснование разработки СЗПДн;
- исходные данные создаваемой (модернизируемой) ИСПДн в техническом, программном, информационном и организационном аспектах; класс ИСПДн;

- ссылку на нормативные документы, с учетом которых будет разрабатываться СЗПДн и приниматься в эксплуатацию информационная система; конкретизацию мероприятий и требований к СЗПДн;
- перечень предполагаемых к использованию сертифицированных средств защиты информации;
- обоснование проведения разработок собственных средств защиты информации при невозможности или нецелесообразности использования имеющихся на рынке сертифицированных средств защиты информации;
- состав, содержание и сроки проведения работ по этапам разработки и внедрения СЗПДн.

Проектирование СЗПДн

На стадии проектирования и создания ИСПДн (СЗПДн) проводятся следующие мероприятия:

- разработка задания и проекта на строительные, строительно-монтажные работы (или реконструкцию) ИСПДн в соответствии с требованиями технического (частного технического) задания на разработку СЗПДн;
- разработка раздела технического проекта на ИСПДн в части защиты информации;
- строительно-монтажные работы в соответствии с проектной документацией;
- использование серийно выпускаемых технических средств обработки, передачи и хранения информации;
- разработка мероприятий по защите информации в соответствии с предъявляемыми требованиями;
- использование сертифицированных технических, программных и программно-технических средств защиты информации и их установка;
- сертификация программных средств защиты информации по требованиям безопасности данных в случае, когда на рынке отсутствуют требуемые сертифицированные средства защиты информации;
- разработка и реализация разрешительной системы доступа пользователей к обрабатываемой в ИСПДн информации;
- определение подразделений и назначение лиц, ответственных за эксплуатацию

средств защиты информации, с их обучением по направлению обеспечения безопасности ПДн;

- разработка эксплуатационной документации на ИСПДн и средства защиты информации, а также организационно-распорядительной документации по защите информации (приказов, инструкций и других документов);
- выполнение других мероприятий, характерных для конкретных ИСПДн и направлений обеспечения безопасности персональных данных.

ЛИСТ

изменений рабочей учебной программы по дисциплине

МДК.03.02 БЕЗОПАСНОСТЬ ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

Дополнения и изменения, вносимые в рабочую программу

дисциплины на 2019/2020 уч.г.

Основания внесения дополнений и изменений	Раздел РПД, в который вносятся изменения*	Содержание вносимых дополнений, изменений*
Предложение работодателя	нет	нет
Предложение составителя программы	нет	нет
Приобретение, издание литературы, обновление перечня и содержания ЭБС, баз данных	Разделы №2.4.5 и №5 Перечень основной и дополнительной учебной литературы	Обновлен список рекомендуемой литературы

Составитель: канд. техн. наук, доцент _____ С.А. Осипов

преподаватель _____ О.А. Семенцова

Утвержден на заседании предметно-цикловой комиссии физико-математических дисциплин и специальных дисциплин специальности Компьютерные сети,
протокол № 10 от 11 июня 2019 г

Председатель предметной (цикловой) комиссии физико-математических дисциплин и специальных дисциплин специальности
Компьютерные сети _____ А.Б. Шишкин
«11» июня 2019 г

Начальник УМО филиала _____ А.С. Демченко
«13» июня 2019 г

Заведующая библиотекой филиала _____ М.В. Фуфалько
«13» июня 2019 г

Начальник ИВЦ (программно-информационное обеспечение образовательной программы) _____ В. А. Ткаченко

13 июня 2019 г.