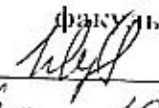


Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Дагестанский государственный технический университет»


РЕКОМЕНДОВАНО
К УТВЕРЖДЕНИЮ

Декан, председатель совета
факультета КТБТнЭ


Ш. А. Юсуфов
«16» 10 2018г.

УТВЕРЖДАЮ

Проректор по учебной работе,
председатель методического совета
ДГТУ


Н. С. Суракатов
«18» 10 2018г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина С1.В.ОД.8 Защита программ и данных
наименование дисциплины по ОЭП и коду по ФГОС

Специальность 10.05.03 «Информационная безопасность автоматизированных систем»

Специализация «Безопасность открытых информационных систем»

Факультет Компьютерных технологий, вычислительной техники и энергетики
наименование факультета, в котором ведется дисциплина

Кафедра Информационная безопасность
наименование кафедры, в которой ведется дисциплина

Квалификация выпускника специалист по защите информации
код катр. специалиста

Форма обучения очная, курс 5, семестр 9

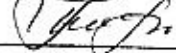
Всего трудоемкость в зачетных единицах (часах) 3 ЗЕД (108 ч.)

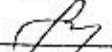
лекции 34 (час); экзамен 9 (ЗЕТ=36ч) (семестр)

практические (семинарские) занятия 34 (час); зачет 9 (семестр)

лабораторные занятия - (час); самостоятельная работа 40 (час);


курсовой проект (работа, РГР) - (семестр).

Зав. кафедрой 
подпись Г.Н. Качаева

Начальник УО 
подпись Э.В. Магомаева

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций ООП ВО по специальности 10.05.03- «Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем».

Программа одобрена на заседании выпускающей кафедры ИБ протокол № 2 от 15.10.2018г.

Зав. выпускающей кафедрой по данной специальности  Г.И.Качаева

ОДОБРЕНО

Методической комиссией по укрупненным группам специальностей и направлению подготовки 10.00.00- «Информационная безопасность»

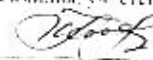
Председатель МК

 Александр В.Б.
И.О. Фамилия

« 15 » 10 20 18.

АВТОР ПРОГРАММЫ

Качаева Г.И. к.э.н., ст.препод. кафедры ИБ
И.О. Фамилия, уч. степень, уч. звание


подпись

1. Цели освоения дисциплины «Защита программ и данных»

Целью дисциплины «Защита программ и данных» является дать основы правового обеспечения информационной безопасности, а также формирование знаний по организационному обеспечению информационной безопасности и навыков по их определению для конкретных условий.

Задачи дисциплины

Дать основы:

- законодательства РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации;
- понятий и видов защищаемой информации по законодательству РФ;
- правовых режимов конфиденциальной информации;
- правового режим защиты государственной тайны, системы защиты государственной тайны;
- лицензирования и сертификации в области защиты информации, в том числе государственной тайны;
- правовых основ защиты информации с использованием технических средств (защита от технических разведок, применение и разработка шифровальных средств, электронная цифровая подпись и т.д.);
- защиты интеллектуальной собственности;
- правовой регламентации охранной деятельности;
- правового регулирования взаимоотношений администрации и персонала в области защиты информации;
- международного законодательства в области защиты информации;
- знаний о преступлениях в сфере компьютерной информации, экспертизах преступлений в области компьютерной информации, криминалистических аспектах проведения расследований;
- угроз информационной безопасности объекта;
- организации службы безопасности объекта;
- подбора и работы с кадрами в сфере информационной безопасности;
- организации и обеспечения режима конфиденциальности;
- охраны объектов.

2. Место дисциплины в структуре ООП специалиста

Дисциплина «Защита программ и данных» относится к обязательным дисциплинам вариативной части учебного плана.

Предшествующими дисциплинами, формирующими начальные знания, являются: Алгебра и геометрия, Дискретная математика, Информатика, Основы информационной безопасности.

Последующими дисциплинами являются: Управление информационной безопасностью, Защита программ и данных, Обеспечение ИБ в интеллектуальных системах.

3 Компетенции обучающегося, формируемые в результате освоения дисциплины «Защита программ и данных»

Процесс изучения дисциплины направлен на формирование следующих компетенций:

способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25);

способностью участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью открытой информационной системы (ПК-4,3).

В результате изучения дисциплины обучающийся должен:

знать – понятия процессор, машинные команды, оперативная память, регистры, смещение, сегмент, разрядность, прерывание; основные машинные команды сложения; основные машинные команды вычитания; основные машинные команды умножения; основные машинные команды деления; основные машинные команды битовой арифметики; основные машинные команды низкоуровневой адресации; способы создания побочных эффектов программы, позволяющие скрыть, затруднить отладку; современные средства защиты ПО; основные виды закладок ПО; основные способы анализа ПО;

уметь – разрабатывать простые программы на языке ассемблер; понимать логику работы программы на языке ассемблер; определять основные побочные эффекты программы, позволяющие скрыть, затруднить отладку; использовать современные средства защиты ПО;

владеть – методами создания побочных эффектов программы, позволяющие скрыть, затруднить отладку; современными методами защиты ПО.

4. Структура и содержание дисциплины «Защита программ и данных»
 Общая трудоемкость дисциплины составляет 3 зачетные единицы - 108 часов, в том числе: лекционных - 34 часа, практических - 34 часа, СРС - 40 часов, форма отчетности зачет в 9 семестре.

4.1. Содержание дисциплины

№ п/п	Раздел дисциплины Тема лекции и вопросы	Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего* контроля успеваемости (по срокам текущих аттестаций в семестре) Форма промежуточной аттестации (по семестрам)
			Неделя семестра				
			ЛК	ПЗ	ЛР	СР	
1.	Лекция №1. Тема: «Организационные основы и принципы деятельности службы защиты информации».	9	1	2	2	2	Входная контрольная
2.	Лекция №2. Тема: «Законодательство РФ в области информационной безопасности».		2	2	2	2	
3.	Лекция №3. Тема: «Правовые основы защиты конфиденциальной информации».		3	2	2	4	
4.	Лекция №4. Тема: «Правовые основы защиты государственной тайны».		4	2	2	2	
5.	Лекция №5. Тема: «Лицензирование и сертификация».		5	2	2	2	АКР №1
6.	Лекция №6. Тема: «Нормы ответственности за правонарушения в сфере компьютерных технологий».		6	2	2	2	
7.	Лекция №7. Тема: «Анализ объекта защиты с позиции организационного обеспечения информационной безопасности».		7	2	2	2	
8.	Лекция № 8. Деятельность по обеспечению информационной безопасности, средства и субъекты обеспечения информационной безопасности».		8	2	2	2	
9.	Лекция №9. Тема: «Структура службы защиты информации».		9	2	2	2	
10.	Лекция №10. Тема: «Организационные основы и принципы деятельности службы защиты информации».		10	2	2	4	АКР №2
11.	Лекция №11. Тема: «Сущность, организация и принципы управления службой защиты информации на предприятии».		11	2	2	4	
12.	Лекция №12. Тема: «Методы и технологии управления службой защиты информации на предприятии».		12	2	2	2	
13.	Лекция №13. Тема: «Средства и методы физической защиты объектов».		13	2	2	2	
14.	Лекция №14. Тема: «Организация службы безопасности и работа с кадрами».		14	2	2	2	
15.	Лекция №15. Тема: «Организация и обеспечения режима секретности».		15	2	2	2	АКР №3
16.	Лекция №16. «Организация труда сотрудников».		16	2	2	2	

	подразделения мониторинга информационной безопасности».						
17.	Лекция №17. Тема: «Организация пропускного и внутри объектового режима».	17	2	2		2	
Итого за 9 семестр			34	34		40	Экзамен 1 ЗЕТ =36 часов

4.2. Содержание лабораторных занятий

№ п/п	№ лекции из рабочей программы	Наименование практического занятия	Количество часов	Рекомендуемая литература и методические разработки (№ источника из списка литературы)
1	2	3	4	5
1	№1	Организационные основы и принципы деятельности службы защиты информации.	2	№№ 1-11
2	№2	Законодательство РФ в области информационной безопасности.	2	№№ 1-11
3	№3	Правовые основы защиты конфиденциальной информации.	2	№№ 1-11
4	№4	Правовые основы защиты государственной тайны.	2	№№ 1-11
5	№5	Лицензирование и сертификация.	2	№№ 1-11
6	№ 6	Нормы ответственности за правонарушения в сфере компьютерных технологий.	2	№№ 1-11
7	№7	Анализ объекта защиты с позиции организационного обеспечения информационной безопасности.	2	№№ 1-11
8	№8	Деятельность по обеспечению информационной безопасности, средства и субъекты обеспечения информационной безопасности.	2	№№ 1-11
9	№9	Структура службы защиты информации.	2	№№ 1-11
10	№10	Организационные основы и принципы деятельности службы защиты информации».	2	№№ 1-11
11	№11	Сущность, организация и принципы управления службой защиты информации на предприятии.	2	№№ 1-11
12	№12	Методы и технологии управления службой защиты информации на предприятии.	2	№№ 1-11
13	№13	Средства и методы физической защиты объектов.	2	№№ 1-11
14	№14	Организация службы безопасности и работа с кадрами.	2	№№ 1-11
15	№15	Организация и обеспечения режима секретности.	2	№№ 1-11
16	№16	Организация труда сотрудников подразделения мониторинга информационной безопасности.	2	№№ 1-11
17	№17	Организация пропускного и внутри объектового режима.	2	№№ 1-11
Итого			34	

4.3. Тематика для самостоятельной работы студента

№ п/п	Тематика по содержанию дисциплины, выделенная для самостоятельного изучения	Количество часов из содержания дисциплины	Рекомендуемая литература и источники информации	Формы контроля СРС
1	Организационные основы и принципы деятельности службы защиты информации.	2	№№ 1-11	Опрос, реферат, статья
2	Законодательство РФ в области информационной безопасности.	2	№№ 1-11	Опрос, реферат, статья
3	Правовые основы защиты конфиденциальной информации.	4	№№ 1-11	Опрос, реферат, статья
4	Правовые основы защиты государственной тайны.	2	№№ 1-11	Опрос, реферат, статья
5	Лицензирование и сертификация.	2	№№ 1-11	Опрос, реферат, статья
6	Нормы ответственности за правонарушения в сфере компьютерных технологий.	2	№№ 1-11	Опрос, реферат, статья
7	Анализ объекта защиты с позиции организационного обеспечения информационной безопасности.	2	№№ 1-11	Опрос, реферат, статья
8	Деятельность по обеспечению информационной безопасности, средства и субъекты обеспечения информационной безопасности.	2	№№ 1-11	Опрос, реферат, статья
9	Структура службы защиты информации.	2	№№ 1-11	Опрос, реферат, статья
10	Организационные основы и принципы деятельности службы защиты информации».	4	№№ 1-11	Опрос, реферат, статья
11	Сущность, организация и принципы управления службой защиты информации на предприятии.	4	№№ 1-11	Опрос, реферат, статья
12	Методы и технологии управления службой защиты информации на предприятии.	2	№№ 1-11	Опрос, реферат, статья
13	Средства и методы физической защиты объектов.	2	№№ 1-11	Опрос, реферат, статья
14	Организация службы безопасности и работа с кадрами.	2	№№ 1-11	Опрос, реферат, статья
15	Организация и обеспечения режима секретности.	2	№№ 1-11	Опрос, реферат, статья
16	Организация труда сотрудников подразделения мониторинга информационной безопасности.	2	№№ 1-11	Опрос, реферат, статья
17	Организация пропускного и	2	№№ 1-11	Опрос, реферат,

внутри объектового режима.			
Итого:	40		статья

5. Образовательные технологии

В соответствии с требованиями ФГОС ВО по специальности подготовки реализация компетентностного подхода предусматривается широкое использование в учебном процессе активных и интерактивных форм проведения занятий.

Аудиторная работа включает: лекции, практические занятия, мастер-классы, консультации.

В курсе лекций использованы наглядные, иллюстрированные материалы, обширная информация в табличной и графической формах, а также электронные ресурсы сети Интернет. Разработаны продвинутые лекции (с визуализацией) в формате презентаций, с использованием пакета прикладных программ MS Power Point.

Внеаудиторная работа призвана для формирования и развития профессиональных навыков обучающихся. Самостоятельная работа включает: выполнение домашних заданий, подготовка рефератов, участие в дискуссиях, работа в информационно-образовательной среде. В конце обучения проводится экзамен.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью программы, особенностью контингента обучающихся и содержанием дисциплины, и в целом в учебном процессе они составляют не менее 20% аудиторных занятий.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины «Защита программ и данных»

ФОНД ВОПРОСОВ (ЗАДАЧ) ДЛЯ КОНТРОЛЬНЫХ РАБОТ

Вопросы для входной контрольной работы

1. Формальное описание структуры информационной системы.
2. Составление модели угроз информационной системе.
3. Формирование требований к системе защиты информации.
4. Формирование требований к политике информационной безопасности.
5. Формирование регламента действий при возникновении нештатных ситуаций.

Контрольные работы по проверке текущих знаний студентов

Аттестационная контрольная работа №1

1. Организационные основы и принципы деятельности службы защиты информации.
2. Законодательство РФ в области информационной безопасности.
3. Правовые основы защиты конфиденциальной информации.
4. Правовые основы защиты государственной тайны.
5. Лицензирование и сертификация.

Аттестационная контрольная работа №2

1. Нормы ответственности за правонарушения в сфере компьютерных технологий.
2. Анализ объекта защиты с позиции организационного обеспечения информационной безопасности.
3. Деятельность по обеспечению информационной безопасности, средства и субъекты обеспечения информационной безопасности.
4. Структура службы защиты информации.
5. Организационные основы и принципы деятельности службы защиты информации.

Аттестационная контрольная работа №3

6. Сущность, организация и принципы управления службой защиты информации на предприятии.
7. Методы и технологии управления службой защиты информации на предприятии.
8. Средства и методы физической защиты объектов.
9. Организация службы безопасности и работа с кадрами.
10. Организация и обеспечения режима секретности.

Перечень вопросов на зачет по дисциплине «Основы управления информационной безопасностью»

1. Охарактеризуйте информацию и ее основные показатели.
2. Основные положения закона об информации, информационных технологиях и защите информации.
3. Основные положения закона о государственной тайне.
4. Основные положения закона о защите персональных данных.
5. Основные положения закона об электронной цифровой подписи.
6. Что такое «политика безопасности»?
7. Чем отличается понятие «модели безопасности» от понятия «политики безопасности»?
8. В каких случаях применяются модели безопасности?
9. Основные модели политик безопасности?
10. Организационные основы и принципы деятельности службы защиты информации.
11. Законодательство РФ в области информационной безопасности.
12. Правовые основы защиты конфиденциальной информации.
13. Правовые основы защиты государственной тайны.
14. Лицензирование и сертификация.
15. Нормы ответственности за правонарушения в сфере компьютерных технологий.
16. Анализ объекта защиты с позиции организационного обеспечения информационной безопасности.
17. Деятельность по обеспечению информационной безопасности, средства и субъекты обеспечения информационной безопасности.
18. Структура службы защиты информации.
19. Организационные основы и принципы деятельности службы защиты информации.
20. Сущность, организация и принципы управления службой защиты информации на предприятии.
21. Методы и технологии управления службой защиты информации на предприятии.
22. Средства и методы физической защиты объектов.
23. Организация службы безопасности и работа с кадрами.
24. Организация и обеспечения режима секретности.
25. Организация труда сотрудников подразделения мониторинга информационной безопасности.
26. Организация пропускного и внутри объектового режима.

Вопросы для проверки остаточных знаний студентов

1. Охарактеризуйте информацию и ее основные показатели.
2. Основные положения закона об информации, информационных технологиях и защите информации.
3. Основные положения закона о государственной тайне.
4. Основные положения закона о защите персональных данных.
5. Основные положения закона об электронной цифровой подписи.
6. Что такое «политика безопасности»?
7. Чем отличается понятие «модели безопасности» от понятия «политики безопасности»?
8. В каких случаях применяются модели безопасности?
9. Основные модели политик безопасности?

7. Учебно-методическое и информационное обеспечение дисциплины
«Защита программ и данных»

Зав. библиотекой _____

М.А.А.

№ п/п	Виды занятий	Необходимая учебная, учебно-методическая (основная и дополнительная) литература, программное обеспечение и Интернет ресурсы	Автор(ы)	Изда-тельство и год издания	Количество изданий	
					В библио-теке	На кафед-ре
1	2	3	4	5	6	7
ОСНОВНАЯ ЛИТЕРАТУРА						
1.	Лк., пз, ере	Защита информации техническими средствами. Учебное пособие	Ю.Ф. Каторин, А.В. Разумовский, А.И. Спивак.	Спб.: НИУ ИТМО (Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики), 2012. — 417 с.	http://e.lanbook.com/books/element.php?pl1_id=40850	
2.	Лк., пз, ере	Инструментальный контроль и защита информации [Электронный ресурс]: учебное пособие	Н.А. Свиричев, О.В. Ланкин, А.П. Данилкин [и др.].	Воронеж: ВГУИТ (Воронежский государственный университет инженерных технологий), 2013. — 192 с.	http://e.lanbook.com/books/element.php?pl1_id=72884	
3.	Лк., пз, ере	Криптографическая защита информации. Учебное пособие	Н.А. Гатченко, А.С. Исаев, А.Д. Яковлев.	Спб.: НИУ ИТМО (Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики), 2012. — 142 с.	http://e.lanbook.com/books/element.php?pl1_id=40849	
ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА						
4.	Лк., пз, ере	Интеллектуальные системы защиты информации [Электронный ресурс]	Васильев В.И.	М.: Машиностроение, 2013. — 172 с.	http://e.lanbook.com/books/element.php?pl1_id=5792	
5.	Лк., пз, ере	Методы и средства инженерно-технической защиты информации [Электронный ресурс]: учебное пособие.	В.И. Аверченков, М.Ю. Рыгов, А.В. Кувыкин [и др.].	М.: ФЛИНТА, 2011. — 187 с.	http://e.lanbook.com/books/element.php?pl1_id=60717	
6.	Лк., пз, ере	Методы и средства защиты компьютерной информации. Часть 1	Борисова С.Н.	Пенза: ПензГТУ (Пензенский государственный	http://e.lanbook.com/books/element.php?pl1_id=62780	

		[Электронный ресурс]	технологический университет). 2013. – 55 с.
ИНТЕРНЕТ-ИСТОЧНИКИ			
7.	Лк., из, ерс	http://kmb.ufoctf.ru/index.html	
8.	Лк., из, ерс	https://habrhabr.ru/hub/crypto/	
9.	Лк., из, ерс	http://training.hackerdom.ru/	
10.	Лк., из, ерс	http://fstec.ru/	
11.	Лк., из, ерс	Виртуальная операционная система Microsoft Windows XP SP3 (VirtualBox, доступ из локальной сети каф. КИБ ЭВС. URL: file://cesir/vm/WinXPBasic).	

8. Материально-техническое обеспечение дисциплины «Защита программ и данных»

Материально-техническое обеспечение дисциплины «Основы управления информационной безопасностью» включает:

- библиотечный фонд (учебная, учебно-методическая, справочная экономическая литература, экономическая научная и деловая периодика);
- компьютеризированные рабочие места для обучаемых с доступом в сеть Интернет (лаборатории по автоматизированным информационным системам, оснащенные современной электронно-вычислительной техникой с соответствующим программным обеспечением);
- аудитории, оборудованные проекционной техникой.

Для проведения практических занятий используются компьютерные классы кафедры ИБ, оборудованные современными персональными компьютерами, характеристики которых не ниже:

Pentium 4, DDR 1 Gb, HDD – 150 GB, Video Card – 126 MB, CD/DVD, USB -2.

Все персональные компьютеры подключены к сети университета и имеют выход в глобальную сеть Интернет.

На компьютере предустанавливается ОС Windows XP/Vista/7 и программное обеспечение MS Office 2010, Borland C++ , Borland C++ Builder 6 и др. Приложение командной строки dumpasn1 Питера Гутмана (Peter Gutmann) для просмотра файлов формата ASN.1 BER/DER: dumpasn1.jar (Windows, x86).

КриптоПро ОСPCOM (версия 1.05.0726).

КриптоПро TSPCOM (версия 1.05.0972).

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

При проведении лекционных и практических (семинарских) занятий предусматривается использование систем мультимедиа, программного обеспечения и информационных справочных систем:

Microsoft Office (Word, Excel, PowerPoint, Access)

ЭБС <http://library.mirea.ru>.

Дистрибутив КриптоПро WinLogon и КриптоПро EAP-TLS;

Дистрибутив КриптоПро JCP и КриптоПро JTLS

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем»

Рецензент от выпускающей кафедры (работодателя) по специальности

И.И.И. *С.П.Р.*