МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный университет»

«Утверждаю»
Заведующий кафедрой ТО и ЗИ

«31» августа 2020 г.  А.А. Сирота

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.Б.47 Организационное и правовое обеспечение информационной безопасности

1. Шифр и наименование направления подготовки / специальности:
10.05.01 Компьютерная безопасность

2. Профиль подготовки / специализация/магистерская программа:
анализ безопасности компьютерных систем

3. Квалификация выпускника: специалист

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины:
Кафедра технологий обработки и защиты информации

6. Составители программы:
Степанцов Вячеслав Алексеевич, к.т.н., доцент

7. Рекомендована:
Научно-методическим советом ФКН, протокол № 7 от 31.08.2020 г.

(отметки о продлении вносятся вручную)

8. Учебный год: 2020/2021 **Семестр(ы):** 4

9. **Цели и задачи учебной дисциплины:** формирование профессиональных навыков, связанных со структурой правового обеспечения информационной безопасности и соответствующего законодательства в области информации, информационных технологий и защиты информации.

Основные задачи дисциплины:

формирование у студентов профессиональных навыков, связанных

− со структурой правового обеспечения информационной безопасности и соответствующего законодательства в области информации;

− информационных технологий и защиты информации;

− обучение применению основных средств и способов обеспечения информационной безопасности, принципов построения систем защиты информации.

10. Место учебной дисциплины в структуре ООП: Блок Б1.Б обязательные дисциплины общепрофессиональной части.

Входные знания в области основ информационной безопасности.

Дисциплина является предшествующей для дисциплины «Техническая защита информации».

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников):

Компетенция		Планируемые результаты обучения
Код	Название	
ОПК-5	способностью использовать нормативные правовые акты в своей профессиональной деятельности	**знать:** нормативные правовые акты для профессиональной деятельности; **уметь**: использовать нормативные правовые акты в профессиональной деятельности; **владеть**: навыками применения нормативных правовых актов в профессиональной деятельности.
ПК-1	способностью осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности	**знать:** как осуществлять подбор, изучение и обобщение научно- технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности; **уметь:** осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности; **владеть:** навыками подбора, изучения и обобщения научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности.
ПК-14	способностью организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа	**знать:** как организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа; **уметь:** организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа; **владеть:** навыками организации работы по выполнению режима защиты информации, в том числе ограниченного доступа.
ПК-15	способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы	**знать:** как разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы; **уметь:** разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы; **владеть:** навыками разработки предложений по совершенствованию системы управления информационной безопасностью компьютерной системы
ПК-16	способностью разрабатывать проекты нормативных правовых	**знать:** как разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие ра-

	актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем	боту по обеспечению информационной безопасности компьютерных систем; **уметь:** разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем; **владеть:** навыками разработки проектов нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем.

12. Объем дисциплины в зачетных единицах/час — 3/108.

Форма промежуточной аттестации: *зачет с оценкой*.

13. Виды учебной работы:

Вид учебной работы	Трудоемкость			
	Всего	По семестрам		
		№ семестра 4	№ семестра	Итого
Аудиторные занятия	48	48		48
в том числе: лекции	16	16		16
практические	32	32		32
лабораторные	-	-		-
Самостоятельная работа	60	60		60
Форма промежуточной аттестации *(зачет – _ час. / экзамен – 0 час.)*	-	-		-
Итого:	108	108		108

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
		1. Лекции
1.1	Назначение и структура правового обеспечения информационной безопасности	1. Основы правового регулирования отношений в информационной сфере.
1.2	Федеральные нормативные акты по обеспечению защиты информации и персональных данных	2. Информационная сфера как сфера обращения информации и правового регулирования. Информационное законодательство как основной источник информационного права. 3. Юридические особенности и свойства информации.
1.3	Правовые основы защиты тайны и персональных данных	4. Структура и направленность правовых мер обеспечения информационной безопасности. 5. Особенности ведомственного и корпоративного нормативного регулирования обеспечения информационной безопасности. 6. Правовые основы защиты государственной, коммерческой, служебной, профессиональной и личной тайны, персональных данных.
1.4	Организационное обеспечение информационной безопасности	7. Политика безопасности. Требования действующих международных стандартов по вопросам менеджмента информационной безопасности. Принципы организационного обеспечения информационной безопасности.
1.5	Планирование и проведение мероприятий по защите информации в организации	8. Порядок деятельности по осуществлению требований организационно-распорядительной документации, периоды проверок, составы комиссий, привлечение аттестованных организаций.
		2. Практические занятия
2.1	Назначение и структура правового обеспечения информационной безопасности	1. Информационные отношения как объект правового регулирования. Виды нормативно-правовых актов, их иерархия.
2.2	Федеральные нормативные акты по обеспечению защиты информации и персональных данных	2. Государственное регулирование деятельности в области защиты информации. 3. Законодательство РФ в области информационной безопасности и защиты государственной тайны.

		4. Законодательство РФ в области информационной безопасности и защиты тайны в различных сферах деятельности. 5. Правовые основы защиты информации с использованием технических средств. 6. Ответственность за правонарушения в области информационной безопасности и ее виды.
2.3	Правовые основы защиты тайны и персональных данных	7. Правовой режим защиты государственной тайны. 8. Порядок обращение с документами, содержащими сведения, составляющие государственную тайну. 9. Правовой режим защиты информации конфиденциального характера. 10. Институт правовой защиты персональных данных.
2.4	Организационное обеспечение информационной безопасности	11. Понятие и сущность организационной защиты информации. 12. Организация режима секретности. 13. Организация работ по обеспечению безопасности персональных данных в информационных системах персональных данных.
2.5	Планирование и проведение мероприятий по защите информации в организации	14. Разработка политики безопасности предприятия 15. Организация режимных мероприятий. 16. Организация работы службы безопасности предприятия.
3. Лабораторные работы		
3.1	нет	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)			
		Лекции	Практические	Сам. работа	Всего
1	Назначение и структура правого обеспечения информационной безопасности	2	2	8	12
2	Федеральные нормативные акты по обеспечению защиты информации и персональных данных	4	10	16	30
3	Правовые основы защиты тайны и персональных данных	6	8	16	30
4	Организационное обеспечение информационной безопасности	2	6	10	18
5	Планирование и проведение мероприятий по защите информации в организации	2	6	10	18
	Итого:	16	32	60	108

14. Методические указания для обучающихся по освоению дисциплины

(рекомендации обучающимся по освоению дисциплины: работа с конспектами лекций, презентационным материалом, выполнение практических заданий, тестов, заданий текущей аттестации и т.д.)

1) При освоении дисциплины рекомендуется использовать следующие средства:

- изучение рекомендуемой основной и дополнительной литературы методических указаний и пособий;
- работа с текстом конспекта лекций;
- систематическая подготовка к практическим занятиям;
- выполнение контрольных заданий для закрепления теоретического материала;
- работа с электронными версиями учебников и методических указаний для выполнения лабораторно-практических работ (при необходимости материалы рассылаются по электронной почте).

2) Для максимального усвоения дисциплины рекомендуется проведение письменного опроса (тестирование, решение задач) студентов по материалам лекций и лабораторных работ. Подборка вопросов для тестирования осуществляется на основе изученного теоретического материала. Такой подход позволяет повысить мотивацию студентов при конспектировании лекционного материала.

3) При проведении практических занятий обеспечивается максимальная степень соответствия с материалом лекционных занятий и осуществляется экспериментальная проверка методов, алгоритмов и технологий обработки информации, излагаемых в рамках лекций.

4) При переходе на дистанционный режим обучения для создания электронных курсов, чтения лекций онлайн и проведения лабораторно- практических занятий используется информационные ресурсы Образовательного портала "Электронный университет ВГУ (https:\\edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете.

5) При использовании дистанционных образовательных технологий и электронного обучения обучающиеся должны выполнять все указания преподавателей, вовремя подключаться к онлайн - занятиям, ответственно подходить к заданиям для самостоятельной работы.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)

а) основная литература:

№ п/п	Источник
1	Организационное и правовое обеспечение информационной безопасности: учебник и практикум для бакалавриата и магистратуры: [для студентов высших учебных заведений, обучающихся по юридическим направлениям и специальностям] / под ред. Т.А. Поляковой, А.А. Стрельцова .— Москва : Юрайт, 2018 .— 324, [1] с. : ил. — (Бакалавр и магистр. Академический курс) .— Библиогр.: с. 324-[325].
2	Романов Олег Алексеевич. Организационное обеспечение информационной безопасности: учебник для студ. вузов, обуч. по специальностям "Организация и технология защиты информации" и "Комплекс. защита объектов информации" направления подгот. "Информ. безопасность" / О.А. Романов, С.А. Бабин, С.Г. Жданов. — Москва: Академия, 2008 .— 188, [1] с. : ил. ; 22 см. — (Высшее профессиональное образование. Информационная безопасность). — Библиогр.: с. 185 .— ISBN 978-5-7695-4272-5.

б) дополнительная литература:

№ п/п	Источник
3	Организационно-правовое обеспечение информационной безопасности : учебное пособие для студ. вузов, обуч. по спец. 090102 "Компьютерная безопасность", 090105 "Комплексное обеспечение информационной безопасности автоматизированных систем", 090105 "Информационная безопасность телекоммуникационных систем" / ; под ред. А.А. Стрельцова .— М. : Академия, 2008 .— 248, [1] с. : ил .— (Высшее профессиональное образование) .— Библиогр.: с. 242-245 .— ISBN 978-5-7695-4240-4.

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет)*:

№ п/п	Ресурсы Интернет
5	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/).
6	Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/)
7	«Университетская библиотека online» - Контракт № 3010-07/33-19 от 11.11.2019 «Консультант студента» - Контракт № 3010-07/34-19 от 11.11.2019 ЭБС «Лань» - Договор 3010-04/05-20 от 26.02.2020. «РУКОНТ» (ИТС Контекстум) - Договор ДС-208 от 01.02.2018 ЭБС «Юрайт» - Договор № 43/8 от 10.02.2020.
8	Организационные основы защиты информации на предприятии (http://content/osnovi-zasiti-informacii/osnovi_zasiti_informacii_part_1.html).
9	Правовое обеспечение системы защиты информации на предприятии (http://old.ci.ru/inform11_97/aiti1.htm)
10	Участие в планировании и организации работ по обеспечению защиты объекта (https://studref.com/651196/prochie/uchastie_v_planirovanii_i_organizatsii_rabot_po_obespecheniyu_zaschity_obekta)

* В начале указываются ЭБС, с которыми имеются договора у ВГУ, затем открытые электронно-образовательные ресурсы

16. Перечень учебно-методического обеспечения для самостоятельной работы

(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению практических (контрольных) работ и др.)

№ п/п	Источник
1	Справочно-информационная система «КонсультантПлюс» [Электронный ресурс]. – URL: http://www.consultant.ru.
2	Методические указания для подготовки и выполнения практических занятий.

17. Информационные технологии, используемые для реализации учебной дисциплины, включая программное обеспечение и информационно-справочные системы (при необходимости)

Для реализации учебного процесса используются:

1. ПО Microsoft в рамках подписки "Imagine/Azure Dev Tools for Teaching", договор №3010-16/96-18 от 29 декабря 2018г.
2. ПО MATLAB Classroom ver. 7.0, 10 конкурентных бессрочных лицензий на каждый, компоненты: Matlab, Simulink, Stateflow, 1 тулбокс, N 21127/VRN3 от 30.09.2011 (за счет проекта ЕК TEMPUS/ERAMIS).
3. ПО Матлаб в рамках подписки "Университетская лицензия на программный комплекс для ЭВМ - MathWorks, Headcount – 25 ": лицензия до 31.01.2022, сублицензионный контракт 3010-07/01-19 от 09.01.19.
4. При проведении занятий в дистанционном режиме обучения используются технические и информационные ресурсы Образовательного портала "Электронный университет ВГУ (https:\\edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете, а также другие доступные ресурсы сети Интернет.

18. Материально-техническое обеспечение дисциплины:

(при использовании лабораторного оборудования указывать полный перечень, при большом количестве оборудования можно вынести данный раздел в приложение к рабочей программе)

1) Мультимедийная лекционная аудитория (корп.1а, ауд. № 381), ПК-Intel-i3, рабочее место преподавателя: проектор, видеокоммутатор, специализированная мебель: доска маркерная 1 шт., столы 16 шт., стулья 33 шт.; доступ к фондам учебно-методической документации и электронным библиотечным системам, выход в Интернет.

2) Компьютерный класс (один из №1-4 корп. 1а, ауд. № 382-385), ПК-Intel-i3 16 шт., специализированная мебель: доска маркерная 1 шт., столы 16 шт., стулья 33 шт.; доступ к фондам учебно-методической документации и электронным изданиям, доступ к электронным библиотечным системам, выход в Интернет.

19. Фонд оценочных средств:

19.1. Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

Код и содержание компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы (темы) дисциплины или модуля и их наименование)	ФОС* (средства оценивания)
ОПК-5 способность использовать нормативные правовые акты в своей профессиональной деятельности	**знать:** нормативные правовые акты для профессиональной деятельности	Разделы 1-2 Назначение и структура правового обеспечения информационной безопасности. Федеральные нормативные акты по обеспечению защиты информации и персональных данных.	Устный опрос

	уметь: использовать нормативные правовые акты в профессиональной деятельности	Разделы 3-4 Правовые основы защиты тайны и персональных данных. Организационное обеспечение информационной безопасности.	Тест № 1
	владеть: навыками применения нормативных правовых актов в профессиональной деятельности.	Раздел 5 Планирование и проведение мероприятий по защите информации в организации.	Практическое задание
ПК-1 способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности	**знать:** как осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности	Разделы 1-2 Назначение и структура правового обеспечения информационной безопасности. Федеральные нормативные акты по обеспечению защиты информации и персональных данных.	Устный опрос
	уметь: осуществлять подбор, изучение и обобщение научно- технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности	Разделы 3-4 Правовые основы защиты тайны и персональных данных. Организационное обеспечение информационной безопасности.	Тест № 2
	владеть: навыками подбора, изучения и обобщения научно- технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности	Раздел 5 Планирование и проведение мероприятий по защите информации в организации.	Практическое задание
ПК-14 способность организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа	**знать:** как организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа	Разделы 1-2 Назначение и структура правового обеспечения информационной безопасности. Федеральные нормативные акты по обеспечению защиты информации и персональных данных.	Устный опрос
	уметь: организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа	Разделы 3-4 Правовые основы защиты тайны и персональных данных. Организационное обеспечение информационной безопасности.	Тест № 3
	владеть: навыками организации работы по выполнению режима защиты информации, в том числе ограниченного доступа	Раздел 5 Планирование и проведение мероприятий по защите информации в организации.	Практическое задание

ПК-15 способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы	**знать:** как разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы	Разделы 1-2 Назначение и структура правового обеспечения информационной безопасности. Федеральные нормативные акты по обеспечению защиты информации и персональных данных.	Устный опрос
	уметь: разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы	Разделы 3-4 Правовые основы защиты тайны и персональных данных. Организационное обеспечение информационной безопасности.	Тест № 4
	владеть: навыками разработки предложений по совершенствованию системы управления информационной безопасностью компьютерной системы	Раздел 5 Планирование и проведение мероприятий по защите информации в организации.	Практическое задание
ПК-16 способность разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем	**знать:** как разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем	Разделы 1-2 Назначение и структура правового обеспечения информационной безопасности. Федеральные нормативные акты по обеспечению защиты информации и персональных данных.	Устный опрос
	уметь: разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем	Разделы 3-4 Правовые основы защиты тайны и персональных данных. Организационное обеспечение информационной безопасности.	Тест № 5
	владеть: навыками разработки проектов нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем	Раздел 5 Планирование и проведение мероприятий по защите информации в организации.	Практическое задание
Промежуточная аттестация			Комплект КИМ

* В графе «ФОС» в обязательном порядке перечисляются оценочные средства текущей и промежуточной аттестаций. Примерный перечень оценочных средств представлен в приложении

19.2. Описание критериев и шкалы оценивания компетенций (результатов обучения) при промежуточной аттестации

Для оценивания результатов обучения на экзамене (зачете) используются следующие содержательные показатели (формулируется с учетом конкретных требований дисциплины):

1) знание теоретических основ учебного материала, основных определений, понятий и используемой терминологии;

2) умение связывать теорию с практикой, иллюстрировать ответ примерами, в том числе, собственными;

3) умение обосновывать свои суждения и профессиональную позицию по излагаемому вопросу.

Различные комбинации перечисленных показателей определяют критерии оценивания результатов обучения (сформированности компетенций) на государственном экзамене:

- высокий (углубленный) уровень сформированности компетенций;
- повышенный (продвинутый) уровень сформированности компетенций;
- пороговый (базовый) уровень сформированности компетенций.

Для оценивания результатов обучения на государственном экзамене используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Для оценивания результатов обучения на зачете используется – «зачтено» («отлично», «хорошо», «удовлетворительно»), «не зачтено» («неудовлетворительно»).

Соотношение показателей, критериев и шкалы оценивания результатов обучения на государственном экзамене представлено в следующей таблице.

Критерии оценивания компетенций и шкала оценок на экзамене

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся демонстрирует полное соответствие знаний, умений, навыков по приведенным критериям свободно оперирует понятийным аппаратом и приобретенными знаниями, умениями, применяет их при решении практических задач.	Повышенный уровень	Отлично
Ответ на контрольно-измерительный материал не полностью соответствует одному из перечисленных выше показателей, но обучающийся дает правильные ответы на дополнительные вопросы. При этом обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач.	Базовый уровень	Хорошо
Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач. При этом ответ на контрольно-измерительный материал не соответствует любым двум из перечисленных показателей, обучающийся дает неполные ответы на дополнительные вопросы.	Пороговый уровень	Удовлетворительно
Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки	–	Неудовлетворительно

19.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы

19.3.1 Примерный перечень применяемых оценочных средств

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	2	3	4
1	Устный опрос	Вопросы по темам/разделам дисциплины	Правильный ответ – зачтено, неправильный или принципиально неточный ответ - не зачтено
2	Тест	Теоретические вопросы по темам/разделам дисциплины	Содержит 4 тестовых вопроса, за правильный ответ на каждый из которых дается 1 балл
3	Контрольная работа по разделам дисциплины	Теоретические вопросы по темам/разделам дисциплины	Шкала оценивания соответствует приведенной в разделе 19.2
4	Практическое задание		Оценка «отлично» выставляется студенту, если он исчерпывающе и свободно справляется с практическими заданиями, дает правильное обоснование принятого решения;

			Оценка «хорошо» выставляется студенту, если он правильно, но недостаточно полно выполняет задания, не допускает существенных неточностей; Оценка «удовлетворительно» выставляется студенту, если он допускает неточности в ответе, испытывает затруднения в выполнении практических заданий, при указании на существенные ошибки может их исправить; Оценка «неудовлетворительно» выставляется студенту, если он допускает существенные ошибки и неправильно выполняет практические задания.
5	КИМ промежуточной аттестации	Каждый контрольно-измерительный материал для проведения промежуточной аттестации включает 2 задания для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции.	Шкалы оценивания приведены в разделе 19.2

19.3.2. Комплект вопросов для контрольных работ

Контрольная работа № 1	
1	Понятие информационной безопасности.
2	Принципы построения систем защиты информации.
3	Актуальность проблемы обеспечения безопасности в информационном обществе.
4	Содержание объектов и субъектов безопасности.
5	Источники и классификация угроз информационной безопасности.
6	Нормативные правовые акты в области обеспечения информационной безопасности
7	Основные составляющие информационной инфраструктуры
8	Федеральный закон «Об информации, информатизации и защите информации» от 20.02.95 №24-ФЗ
9	ГОСТ Р 50922-96 «Защита информации. Основные термины и определения»
10	Средства и способы обеспечения информационной безопасности
11	Система национальной безопасности Российской Федерации
Контрольная работа № 2	
1	Содержание интересов личности в информационной сфере.
2	Стратегия развития информационного общества в России.
3	Какую информацию относят к защищаемой?
4	Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.
5	Содержание интересов общества в информационной сфере.
6	Классификация мер защиты информации.
7	Основные задачи в области обеспечения информационной безопасности.
8	Доктрина информационной безопасности РФ.
9	Содержание способов и средств обеспечения безопасности информации.
10	Организационные меры защиты информации и информационных систем
11	Содержание интересов государства в информационной сфере.
12	Правовые средства защиты информации и информационных систем.
13	Понятие угрозы. Анализ угроз информационной безопасности.
14	Содержание способов и средств обеспечения информационной безопасности.
15	Организационно-административные средства защиты информации.
16	Виды «нарушителей» информационной безопасности.
17	Основные причины утечки информации.
Контрольная работа № 3	
1	Политика безопасности. Основные типы политики безопасности.
2	Основные методы реализации угроз информационной безопасности.

3	Основные задачи обеспечения информационной безопасности.
4	Основные каналы утечки информации.
5	Защита информации ограниченного доступа: государственная тайна, коммерческая тайна.
6	Нормативные методические документы ФСБ России в области защиты информации.
7	Противодействие иностранным техническим разведкам на территории РФ
8	Нормативные методические документы ФСТЭК России в области защиты информации.
9	Стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны.
10	Структура нормативной базы по вопросам информационной безопасности
11	Государственная система обеспечения информационной безопасности.
12	Стандарты информационной безопасности.

19.3.3. Примерный перечень вопросов к зачету

№	Содержание
1	Что такое «информационное» общество?
2	Каковы основные составляющие информационной инфраструктуры
3	Что такое информация?
4	Основные формы и свойства информации
5	Чем обусловлена актуальность проблемы обеспечения безопасности в информационном обществе?
6	Каким образом современные информационные технологии оказывают влияние на экономическую и духовную сферы жизни общества, на сферу государственного управления?
7	Что такое информационная инфраструктура?
8	Основные составляющие информационной инфраструктуры.
9	Раскройте содержание объектов и субъектов безопасности.
10	Раскройте содержание объектов и субъектов обеспечения информационной безопасности.
11	Приведите определение организации.
12	Приведите определение юридического лица.
13	Перечислите виды организаций, участвующих в гражданских отношениях
14	Приведите определение государства.
15	Перечислите основные функции государства.
16	В чем заключается сущность информационной безопасности организаций и государства?
17	Правила защиты информации.
18	Меры ответственности за нарушение правил защиты информации.
19	Какую информацию относят к защищаемой?
20	Государственная система правового обеспечения защиты информации в Российской Федерации.
21	Доктрина информационной безопасности Российской Федерации.
22	Противодействию иностранным техническим разведкам на территории РФ.
23	Критерии оценки безопасности информационных технологий.
24	Организация секретного делопроизводства.

19.3.4. Пример контрольно-измерительного материала

УТВЕРЖДАЮ
Заведующий кафедрой технологий обработки и защиты информации

_____ А.А. Сирота
«____»_____ 2019

Направление подготовки / специальность 10.05.01 Компьютерная безопасность
Дисциплина Б1.Б.47 Организационное и правовое обеспечение информационной безопасности
Форма обучения Очное
Вид контроля Зачет
Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

1. Понятие информационной безопасности.
2. Принципы построения систем защиты информации.

Преподаватель _____ В.А. Степанцов

19.3.5. Пример практических занятий

Практическая работа №1

Тема: Разработка политики безопасности предприятия

Цель работы: Разработать политику безопасности для конкретного предприятия

Теоретические сведения

Политика безопасности трактуется как набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации. На практике политика безопасности трактуется несколько шире – как совокупность документированных административных решений, направленных на обеспечение безопасности информационного ресурса. Результатом политики является высокоуровневый документ, представляющий систематизированное изложение целей, задач, принципов и способов достижения информационной безопасности.

Данный документ представляет методологическую основу практических мер (процедур) по реализации обеспечения безопасности информации (ОБИ) и содержит следующие группы сведений:

1. Основные положения информационной безопасности.
2. Область применения.
3. Цели и задачи обеспечения информационной безопасности.
4. Распределение ролей и ответственности.
5. Общие обязанности.

Основные положения определяют важность ОБИ, общие проблемы безопасности, направления их решения, роль сотрудников, нормативно-правовые основы.
Областью применения политики безопасности являются основные активы и подсистемы АС, подлежащие защите. Типовыми активами являются программно-аппаратное и информационное обеспечение АС, персонал, в отдельных случаях – информационная инфраструктура предприятия.

Цели, задачи, критерии ОБИ вытекают из функционального назначения предприятия. Например, для режимных организаций на первое место ставится соблюдение конфиденциальности. Для сервисных информационных служб реального времени важным является обеспечение доступности (оперативной готовности) подсистем. Для информационных хранилищ актуальным может быть обеспечение целостности данных и т. д. Здесь указываются законы и правила организации, которые следует учитывать при проведении работ по ОБИ.

Типовыми целями могут быть следующие:

- обеспечение уровня безопасности, соответствующего нормативным документам предприятия;
- следование экономической целесообразности в выборе защитных мер;
- обеспечение соответствующего уровня безопасности в конкретных функциональных областях АС;
- обеспечение подотчетности всех действий пользователей с информационными ресурсами и анализа регистрационной информации;
- выработка планов восстановления после критических ситуаций и обеспечения непрерывности работы АС и др.

Если предприятие не является изолированным, цели и задачи рассматриваются в более широком контексте: должны быть оговорены вопросы безопасного взаимного влияния локальных и удаленных подсистем.

В рассматриваемом документе могут быть конкретизированы некоторые стратегические принципы безопасности (вытекающие из целей и задач ОБИ). Таковыми являются стратегии действий в случае нарушения политики безопасности предприятия и сторонних организаций, взаимодействия с внешними организациями, правоохранительными органами, прессой и др.

В качестве примера можно привести две стратегии ответных действий на нарушение безопасности:

- «выследить и осудить», когда злоумышленнику позволяют продолжить действия с целью его компрометации и наказания (данную стратегию одобряют правоохранительные органы);

- «защититься и продолжить», когда организация опасается за уязвимость информационных ресурсов и оказывает максимальное противодействие нарушению.

Задание: Составить политику безопасности предприятия, придерживаясь вышеизложенного плана.

Вопросы для проверки знаний и умений:

1. Что такое политика безопасности?
2. Перечислите цели и задачи политики безопасности на предприятии.
3. Дайте определение понятию объект и субъект политики безопасности.
4. Назовите основное назначение политики информационной безопасности.

19.3.6. Пример вариант теста

1. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

A. Владельцы данных
B. Пользователи
C. Администраторы
D. Руководство

2. Что такое политика безопасности?

A. Пошаговые инструкции по выполнению задач безопасности
B. Общие руководящие требования по достижению определенного уровня безопасности.
C. Широкие, высокоуровневые заявления руководства.
D. Детализированные документы по обработке инцидентов безопасности.

3. Эффективная программа безопасности требует сбалансированного применения:

A. Технических и нетехнических методов.
B. Контрмер и защитных механизмов.
C. Физической безопасности и технических средств защиты.
D. Процедур безопасности и шифрования.

19.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах устного опроса (индивидуальный опрос, фронтальная беседа) и письменных работ (контрольные, лабораторные работы). При оценивании могут использоваться количественные или качественные шкалы оценок.

Промежуточная аттестация может включать в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и/или практическое (ие) задание(я), позволяющее (ие) оценить степень сформированности умений и навыков.

При оценивании используется количественная шкала. Критерии оценивания приведены выше в таблице раздела 19.2.