МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой

Сирота Александр Анатольевич

Кафедра технологий обработки и защиты информации

03.05.2023

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.ОД1 Информационная безопасность

1. Шифр и наименование специальности:
33.08.02 Управление и экономика фармации

2. Профиль подготовки/специализация: отсутствует

3. Квалификация выпускника: провизор - менеджер

4. Форма обучения: очная

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

6. Составители программы: Филиппова Неля Викторовна, к.ю.н., доцент, Нестеровский Олег Игоревич, к.т.н.

7. Рекомендована: научно-методическим советом ФКН, протокол № 7 от 03.05.2023 г.

8. Учебный год: 2024-2025 Семестр(ы): 3

9. Цели и задачи учебной дисциплины: изучение основ и принципов организации и информационной безопасности в рамках комплексного обеспечения безопасности.

Основные задачи дисциплины:

- обучение студентов базовым правовым и техническим основам обеспечения информационной безопасности государства;
- обучение студентов базовым методологиям создания систем защиты информации;
- обучение студентов базовым основам процесса сбора, передачи, накопления и обработки информации;
- обучение студентов основам методов и средств ведения информационных противоборств;
- обучение студентов базовым способам оценки защищенности и обеспечения информационной безопасности;
- обучение студентов базовым принципам обеспечения безопасности объектов информатизации.

10. Место учебной дисциплины в структуре ООП: дисциплина «Информационная безопасность» относится к дисциплинам блока Фармацевтический менеджмент и изучается на втором курсе, в третьем семестре.

Входные знания в области нормативной и законодательной базы в области соблюдения основных принципов управления в фармации.

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	
ПК-4	Готовность к применению основных принципов управления в профессиональной сфере	**знать:** сущность и понятие информационной безопасности, характеристику ее составляющих; место информационной безопасности в системе национальной безопасности страны; источники угроз информационной безопасности и меры по их предотвращению; жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи; современные средства и способы обеспечения информационной безопасности; **уметь:** применять на практике теоретические знания для реализации основных принципов управления информационной безопасностью в фармации; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; классифицировать основные угрозы безопасности информации; применять основные правила и положения документов системы сертификации Российской Федерации в области информационной безопасности; **владеть:** навыками определения основных угроз безопасности информации; практическими навыками применения методов и средств обеспечения безопасности информации; практическими навыками управления информационной безопасностью в фармации.

12. Объем дисциплины в зачетных единицах/час — 3/72 часа.
Форма промежуточной аттестации: зачет.

13. Виды учебной работы:

Вид учебной работы	Трудоемкость			
	Всего	По семестрам		
		№ семестра 3	№ семестра	Итого
Аудиторные занятия	32	32		32

в том числе: лекции	-	-		-
практические	32	32		32
лабораторные	-	-		-
Контроль самостоятельной работы	2	2		2
Индивидуальные консультации	2	2		2
Самостоятельная работа	36	36		36
Форма промежуточной аттестации *(зачет – 0 час.)*	-	-		-
Итого:	72	72		72

12.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1. Лекции		
1.1	нет	
2. Практические занятия		
2.1	Общие проблемы безопасности. Роль и место информационной безопасности	1. Предметная область информационной безопасности. Исторические сведения и этапы развития проблем и технологий обеспечения информационной безопасности. 2. Математические основы обеспечения информационной безопасности.
2.2	Методы и средства защиты информации	3. Функции непосредственной защиты информации. Механизмы защиты, управление механизмами защиты. 4. Методы защиты информации от преднамеренного доступа, методы защиты информации в вычислительных системах. 5. Методы идентификации и установления подлинности субъектов и различных объектов. 6. Технические, программные и организационно-правовые средства защиты информации. 7. Современные средства и способы обеспечения информационной безопасности.
2.3	Перспективы развития информационной безопасности	8. Методы и средства развития информационной безопасности и методов и средств ведения информационных противоборств
3. Лабораторные работы		
3.1	нет	

12.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)			
		Лекции	Практические	Самостоятельная работа	Всего
1	Общие проблемы безопасности. Роль и место информационной безопасности	-	12	15	27
2	Методы и средства защиты информации	-	10	15	25
3	Перспективы развития информационной безопасности	-	10	10	20
	Итого:	-	32	40	72

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 изучении дисциплины рекомендуется использовать следующие средства**:**

- рекомендуемую основную и дополнительную литературу;
- методические указания и пособия;
- контрольные задания для закрепления теоретического материала;
- электронные версии учебников и методических указаний для выполнения практических работ (при необходимости материалы рассылаются по электронной почте).

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

3) При проведении практических занятий осуществляется экспериментальная проверка знаний основ информационной безопасности.

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, не обходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1	Варлатая, Светлана Климентьевна. Защита и обработка конфиденциальных доку- ментов : учебно-методический комплекс / С.К. Варлатая, М.В. Шаханова ; Дальне-вост. федер. ун-т .— Москва : Проспект, 2015 .— 178, [1] с.
2	Яковец, Евгений Николаевич. Правовые основы обеспечения информационной безопасности Российской Федерации : учебное пособие / Е.Н. Яковец .— 2-е изд., доп. и перераб. — Москва : Юрлитинформ, 2014 .— 406, [1] с.

б) дополнительная литература:

№ п/п	Источник
2	*Астанин, Иван Константинович*. Защита информации : учебное пособие для вузов / И.К. Астанин, Н.И. Астанин ; Воронеж. гос. ун-т, Лискинский филиал .— Воронеж : Воронеж. гос. ун-т, 2006 .— Библиогр. : с.169 .— ISBN 5-9273-1080-х.
3	Гончаров, Игорь Васильевич. Информационная безопасность. Словарь по терминологии / И.В. Гончаров, Ю.Г. Кирсанов, О.В. Райков .— Воронеж : Воронежская областная типогра- фия, 2015 .— 180 с. — Тираж 300. 11,3 п.л. — ISBN 9785442003246.
4	Мельников, Владимир Павлович. Информационная безопасность и защита информации : учебное пособие для студ. вузов, обуч. по специальности 230201 "Информационные си-стемы и технологии" / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова .— М. : ACADEMIA, 2006 .— 330 с. : ил .— (Высшее профессиональное обра-зование. Информатика и вычислительная техника) .— Библиогр.: с.327-328 .— ISBN 5-7695-2592-4.
5	Андрианов В.И."Шпионские штучки" и устройства для защиты объектов и информации: Справ. пособие / В.А.Бородин, А.В.Соколов. – С-Пб.: Лань, 1996.
6	Кузнецов, Петр Уварович. Основы информационного права : учебник для бакалав- ров : [учебник для студ. вузов, обучающихся по направлению "Юриспруденция" и специальности "Юриспруденция"] / П.У. Кузнецов .— Москва : Проспект, 2015 .— 308, [1] с.
7	Брусницин Н.А. Открытость и шпионаж / Н.А.Брусницин. – М.: Воениздат, 1991.
8	Информационная безопасность : словарь по терминологии / И.В. Гончаров, Ю.Г. Кирсанов, О.В. Райков ; ЗАО "НПО "Информбезопасность" .— Воронеж : НПО "Информбезопасность", 2015 .— 180 с.
9	Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства : / Шаньгин В. Ф. — Москва : ДМК Пресс, 2010 .— 544 с. : ил., табл. ; 24 см .— (Администри-рование и защита) .— ОГЛАВЛЕНИЕ кликните на URL-> .— Допущено Учебно-методическим объединением вузов по университетскому политехническому образованию в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению 230100 «Информатика и вычислительная техника» .— Предм. указ.: с. 530-542 .— Библиогр.: с. 524-529 (105 назв.) .— ISBN 978-5-94074-518-1 .— <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1122>.
10	Просвирнин, Юрий Георгиевич. Информационное право и основы правовой ин-форматики : учебно-методическое пособие : [студентам всех форм обучения юри-

	дического факультета; для направления 030900 - Юриспруденция (бакалавры)] / Ю.Г. Просвирнин, В.Г. Просвирнин ; Воронеж. гос. ун-т .— Воронеж : Издательский дом ВГУ, 2016 .— 98 с.
12	Кайнов, Владимир Иванович. Информационное право России / В.И. Кайнов, Р.А. Сафаров .— Ростов-на-Дону : Феникс, 2014 .— 156 с.

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

№ п/п	Ресурс
13	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/).
14	Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/)
15	ЭБС «Издательства «Лань», Договор №3010-06/71-14 от 25.11.2014, ЭБС «Университетская библиотека online», Договор №3010-06/70-14 от 25.11.14, Национальный цифровой ресурс «РУКОНТ», Договор №ДС-208 от 01.02.2012

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

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Гончаров Игорь Васильевич. Информационная безопасность. Словарь по терминологии / И.В. Гончаров, Ю.Г. Кирсанов, О.В. Райков .— Воронеж : Воронежская областная типография, 2015 .— 180 с. — Тираж 300. 11,3 п.л. — ISBN 9785442003246.

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

1. Использование информационных (справочных) систем: СПС Гарант v.7 – Справочно-Правовая Система – для ординаторов открыт постоянный доступ в компьютерном классе (7-й корпус, ауд. 309).
2. Организация взаимодействия с ординаторами посредством электронной почты.
3. ЭБС «Консультант студента» МедФарм.
4. Консультант плюс – информационно-справочная система.
5. ЭБС Университетская библиотека ONLAIN.
6. Информационно-обучающая среда Moodle.
7. www.lib.vsu.ru -ЗНБ ВГУ.
8. 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)

Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно-наглядных пособий и используемого программного обеспечения	**Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом (в случае реализации образовательной программы в сетевой форме дополнительно указывается наименование организации, с которой заключен договор)**
Учебная аудитория для проведения учебных занятий: специализированная мебель, мультимедиа-проектор, экран настенный, компьютеры, подключенные к сети Интернет (13 шт.), МФУ, планшет Lenovo (15 шт.). ПО: СПС «ГАРАНТ-Образование», СПС "Консультант	394036, г. Воронеж, ул. Студенческая, д. 3

Плюс" для образования, OfficeSTD 2013 RUS OLP NL Acdmc, WinPro 8, OfficeSTD, Android 8, интернет-браузер Mozilla Firefox.	
Помещение для самостоятельной работы с возможностью подключения к сети «Интернет»: Специализированная мебель, компьютеры (12 шт.), доска магнитно-маркерная. ПО: СПС «ГАРАНТ-Образование», СПС "Консультант Плюс" для образования, OfficeSTD 2013 RUS OLP NL Acdmc, интернет-браузер Mozilla Firefox.	394036, г. Воронеж, ул. Студенческая, д. 3

19. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

19.1 Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

Код и содержание компетенции (или ее части)	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)
ПК-4, Готовность к применению основных принципов управления в профессиональной сфере	**знать:** сущность и понятие информационной безопасности, характеристику ее составляющих; место информационной безопасности в системе национальной безопасности страны; источники угроз информационной безопасности и меры по их предотвращению; жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи; современные средства и способы обеспечения информационной безопасности	Разделы 1-3 Общие проблемы безопасности. Роль и место информационной безопасности. Методы и средства защиты информации. Перспективы развития информационной безопасности.	Контрольная работа по соответствующим разделам.

	уметь: применять на практике теоретические знания для реализации основных принципов управления информационной безопасностью в фармации; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; классифицировать основные угрозы безопасности информации; применять основные правила и положения документов системы сертификации Российской Федерации в области информационной безопасности	Разделы 2-3 Методы и средства защиты информации. Перспективы развития информационной безопасности.	Контрольная работа по соответствующим разделам.
	владеть: навыками определения основных угроз безопасности информации; практическими навыками применения методов и средств обеспечения безопасности информации; практическими навыками управления информационной безопасностью в фармации	Разделы 2-3 Методы и средства защиты информации. Перспективы развитии информационной безопасности.	Контрольная работа по соответствующим разделам.
Промежуточная аттестация			Комплект КИМ

* В графе «ФОС» в обязательном порядке перечисляются оценочные средства текущей и промежуточной аттестаций.

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

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

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

2) умение проводить обоснование и представление основных теоретических и практических результатов (теорем, алгоритмов, методик) с использованием математических выкладок, блок-схем, структурных схем и стандартных описаний к ним;

3) умение связывать теорию с практикой, иллюстрировать ответ примерами, в том числе, собственными, умение выявлять и анализировать основные закономерности, полученные, в том числе, в ходе выполнения лабораторно-практических заданий;

4) умение обосновывать свои суждения и профессиональную позицию по излагаемому вопросу;

5) владение навыками программирования и экспериментирования с компьютерными моделями алгоритмов обработки информации в среде Matlab в

рамках выполняемых лабораторных заданий;

6) владение навыками проведения компьютерного эксперимента, тестирования компьютерных моделей алгоритмов обработки информации.

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 используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Для оценивания результатов обучения на зачете без оценки используется – зачтено, не зачтено по результатам тестирования.

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

Критерии оценивания компетенций и шкала оценок на дифференцированном зачете

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся демонстрирует полное соответствие знаний, умений, навыков по приведенным критериям свобод- но 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	Контрольная работа по разделам дисциплины	Теоретические вопросы по темам/разделам дисциплины	Шкала оценивания соответствует приведенной в разделе 19.2

3	КИМ промежуточной аттестации	Каждый контрольно-измерительный материал для проведения промежуточной аттестации включает 2 заданий вопросов для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции.	Шкалы оценивания приведены в разделе 19.2

19.3.2. Примерный перечень вопросов к экзамену

№	Содержание
1	Виды национальной безопасности и их краткая характеристика
2	Средства обеспечения информационной безопасности
3	Системные связи информационной безопасности с другими видами национальной безопасности
4	Аппаратные средства обеспечения информационной безопасности
5	Информационные уязвимости объектов
6	Программные средства обеспечения информационной безопасности
7	Антропогенные информационные уязвимости
8	Криптографические средства обеспечения информационной безопасности
9	Техногенные информационные уязвимости
10	Стеганографические средства обеспечения информационной безопасности
11	Организационно-правовые информационные уязвимости
12	Организационно-правовые средства обеспечения информационной безопасности
13	Комбинированные информационные уязвимости
14	Государственная политика в области информационной безопасности
15	Угрозы информационной безопасности и их источники
16	Государственные органы обеспечения информационной безопасности
17	Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация
18	Приоритетные направления обеспечения информационной безопасности в условиях информационного общества
19	Эндогенные и экзогенные, угрозы информационной безопасности, их классификация
20	Приоритетные проблемы обеспечения информационной безопасности в условиях информационного общества
21	Антропогенные и техногенные угрозы информационной безопасности, их классификация
22	Технические каналы утечки конфиденциальной информации. Основные методы защиты
23	Системная классификация угроз информационной безопасности
24	Пассивные средства противодействия техническим разведкам
25	Угрозы конфиденциальности, целостности и доступности информации
26	Активные средства противодействия техническим разведкам
27	Информационная война как высшая форма угрозы информационной безопасности
28	Базовые стратегии организации защиты информации
29	Категорирование информации
30	Полное множество функций защиты информации

Примеры тестовых заданий

1. Что такое защита информации?

а) Состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

б) Реализация конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также защита информации, обеспечивающая личную безопасность.

в) Деятельность, направленная на предотвращение НСД к информации.

г) Деятельность, направленная на предотвращение утечки защищаемой информации, непреднамеренных и несанкционированных воздействий на защищаемую информацию.

2. Какие из перечисленных угроз относятся к случайным угрозам компьютерной информации:

а) несанкционированный доступ к информации, вредительские программы, ошибки при разработке компьютерной системы;

б) электромагнитные излучения и наводки, несанкционированная модификация структур компьютерной системы;

в) стихийные бедствия и аварии, сбои и отказы технических средств, ошибки пользователей и обслуживающего персонала;

г) технические каналы утечки информации.

3. Безопасность информации – это:

а) доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или автоматизированными системами (АС);

б) состояние защищенности информации (данных) при котором обеспечивается ее (их) конфиденциальность, доступность и целостность;

в) реализация конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также защита информации, обеспечивающая личную безопасность;

г) деятельность, направленная на предотвращение НСД к информации.

4. Структурная комплексность включает:

а) обеспечение маскировки (скрытия) назначения, архитектуры, технологии функционирования системы;

б) обеспечение текущей защиты, обеспечение защиты на заданном интервале времени, обеспечение защиты на всех этапах жизненного цикла;

в) защиту информации в элементах и отдельных средствах, защиту информации в отдельно взятой системе обработки информации, защиту информации в системах обработки информации страны, региона, ведомства;

г) комплексный учет концепций развития и использования современных средств обработки информации, учет аспектов системности подхода.

5. Временная комплексность включает:

а) обеспечение маскировки (скрытия) назначения, архитектуры, технологии функционирования системы;

б) обеспечение текущей защиты, обеспечение защиты на заданном интервале времени, обеспечение защиты на всех этапах жизненного цикла;

в) защиту информации в элементах и отдельных средствах, защиту информации в отдельно взятой системе обработки информации, защиту информации в системах обработки информации страны, региона, ведомства;

г) комплексный учет концепций развития и использования современных средств обработки информации, учет аспектов системности подхода.

6. Целевая комплексность включает:

а) обеспечение маскировки (скрытия) назначения, архитектуры, технологии функционирования системы;

б) обеспечение текущей защиты, обеспечение защиты на заданном интервале времени, обеспечение защиты на всех этапах жизненного цикла;

в) защиту информации в элементах и отдельных средствах, защиту информации в отдельно взятой системе обработки информации, защиту информации в системах обработки информации страны, региона, ведомства;

г) комплексный учет концепций развития и использования современных средств обработки информации, учет аспектов системности подхода.

7. Концептуальная комплексность включает:

а) обеспечение маскировки (скрытия) назначения, архитектуры, технологии функционирования системы;

б) обеспечение текущей защиты, обеспечение защиты на заданном интервале времени, обеспечение защиты на всех этапах жизненного цикла;

в) защиту информации в элементах и отдельных средствах, защиту информации в отдельно взятой системе обработки информации, защиту информации в системах обработки информации страны, региона, ведомства;

г) комплексный учет концепций развития и использования современных средств обработки информации, учет аспектов системности подхода.

8. Техническая защита информации – это:

а) защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств;

б) защита информации с помощью ее криптографического преобразования;

в) защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты;

г) защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

9. Физическая защита информации – это:

а) защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств;

б) защита информации с помощью ее криптографического преобразования;

в) защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты;

г) защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

10. Правовая защита информации – это:

а) защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств;

б) защита информации с помощью ее криптографического преобразования;

в) защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты;

г) защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

11. Криптографическая защита информации – это:

а) защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств;

б) защита информации с помощью ее криптографического преобразования;

в) защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты;

г) защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

12. Способ защиты информации – это:

а) основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации;

б) заранее намеченный результат защиты информации;

в) совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации;

г) порядок и правила применения определенных принципов и средств защиты информации.

13. Цель защиты информации – это:

а) основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации;

б) заранее намеченный результат защиты информации;

в) совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации;

г) порядок и правила применения определенных принципов и средств защиты информации.

14. Система защиты информации – это:

а) основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации;

б) заранее намеченный результат защиты информации;

в) совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и

функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации;

г) порядок и правила применения определенных принципов и средств защиты информации.

15. Лицензирование в области защиты информации – это:

а) деятельность, заключающаяся в проверке (экспертизе) возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями и выдаче разрешения на выполнение этих работ;

б) форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров. К объектам оценки могут относиться: средство защиты информации, средство контроля эффективности защиты информации;

в) исследование, проводимое в целях выявления технических каналов утечки защищаемой информации и оценки соответствия защиты информации (на объекте защиты) требованиям нормативных правовых документов в области безопасности информации;

г) проверка объекта информатизации в целях выявления и изъятия возможно внедренных закладочных устройств.

16. Специальная проверка – это:

а) деятельность, заключающаяся в проверке (экспертизе) возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями и выдаче разрешения на выполнение этих работ;

б) форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров. К объектам оценки могут относиться: средство защиты информации, средство контроля эффективности защиты информации;

в) исследование, проводимое в целях выявления технических каналов утечки защищаемой информации и оценки соответствия защиты информации (на объекте защиты) требованиям нормативных правовых документов в области безопасности информации;

г) проверка объекта информатизации в целях выявления и изъятия возможно внедренных закладочных устройств.

17. Сертификация на соответствие требованиям по безопасности информации – это:

а) деятельность, заключающаяся в проверке (экспертизе) возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями и выдаче разрешения на выполнение этих работ;

б) форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров. К объектам оценки могут относиться: средство защиты информации, средство контроля эффективности защиты информации;

в) исследование, проводимое в целях выявления технических каналов утечки защищаемой информации и оценки соответствия защиты информации (на объекте защиты) требованиям нормативных и правовых документов в области безопасности информации;

г) проверка объекта информатизации в целях выявления и изъятия возможно внедренных закладочных устройств.

Короткий ответ

1. К каким методам защиты информации относится шумоподавление информационного сигнала: **активным**.

2. К каким методам защиты информации относится звукоизоляция: **пассивным**.

3. Что является объектом системы сертификации: **средства защиты информации**.

5. Что является объектом системы лицензирования: **вид деятельности**.

5. Диапазон акустических частот: **20 Гц – 20 КГц**.

Длинный ответ

1. Замысел защиты информации – это: **основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации**.

2. Несанкционированный доступ (НСД) к информации – это: **доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или автоматизированными системами (АС)**.

3. Технический канал утечки информации – это: **совокупность объекта разведки, средства разведки, среды распространения сигнала**.

4. Система защиты информации – это: **совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации**.

5. Специальное исследование (объекта защиты информации) – это: **исследование, проводимое в целях выявления технических каналов утечки защищаемой информации и оценки соответствия защиты информации (на объекте защиты) требованиям нормативных и правовых документов в области безопасности информации**.

Пример контрольно-измерительного материала

УТВЕРЖДАЮ
Заведующий кафедрой технологий обработки и защиты информации

_____ А.А. Сирота
__.__.2022

Направление подготовки / специальность 33.08.02 Управление и экономика фармации

Дисциплина Информационная безопасность Форма обучения Очная

Вид контроля Зачет

Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

1. Виды национальной безопасности и их краткая характеристика
2. Средства обеспечения информационной безопасности

Преподаватель _____ О.И. Нестеровский

19.3 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.

Задания раздела 19 рекомендуются к использованию при проведении диагностических работ с целью оценки остаточных знаний по результатам освоения данной дисциплины.