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

УТВЕРЖДАЮ
заведующий кафедрой
кибербезопасности
информационных систем
С.Л. Кенин

22.03.2024

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ Б1.В.11 Теория и методы социальной инженерии в информационной безопасности

1. Код и наименование направления подготовки/специальности:

10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализация:

"Безопасность компьютерных систем и сетей" (по отрасли или в сфере профессиональной деятельности)

3. Квалификация (степень) выпускника: Специалист

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины:

кибербезопасности информационных систем

6. Составители программы:

Иванкин Михаил Петрович, к.т.н., доцент кафедры кибербезопасности информационных систем

7. Рекомендована:
НМС факультета ПММ, протокол № 7 от 26.05.2023г.
Внесены изменения: протокол УС факультета ПММ, протокол № 8 от 27.02.2024г.
Рекомендована с изменениями: протокол НМС факультета ПМ, протокол № 5 от 22.03.2024г.

8. Учебный год: 2027/2028 **Семестр(ы):** 9

9. Цели и задачи учебной дисциплины

Основные понятия социальной инженерии в контексте информационной безопасности. Методы управления действиями человека без использования технических средств. Психологическая манипуляция людей в выполнении действий или разглашении конфиденциальной информации.

Изучение аспектов межличностного общения, связанных с обеспечением информационной безопасности организации. Рассматриваются особенности взаимодействия и сотрудничества администратора безопасности по поводу обеспечения информационной безопасности организации администратора информационной безопасности с руководством организации. Разбираются типичные конфликтные ситуации, которые могут возникнуть при обеспечении информационной безопасности организации.

10. Место учебной дисциплины в структуре ОПОП: дисциплина относится к вариативной части блока Б1 дисциплин учебного плана.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения

Код	Название компетенции	Код(ы)	Индикаторы(ы)	Планируемые результаты обучения
ПК-1.	Способен проводить анализ требований и выполнять работы по проектированию программных и аппаратных компонент системы безопасности компьютерных систем и сетей, в том числе с использованием современных методов и средств защиты информации.	ПК-1.4.	проводит оценку соответствия механизмов безопасности компьютерной системы требованиям нормативных документов, а также их корректности существующим рискам.	Знание: механизмы безопасности компьютерной системы и требования нормативных документов. Умеет: проводить оценку соответствия механизмов безопасности компьютерной системы требованиям нормативных документов, а также их корректности существующим рискам.
ПК-3.	Способен участвовать в работах по проектированию систем защиты информации в компьютерных системах и сетях при решении профессиональных, исследовательских и прикладных задач.	ПК-3.2.	знает методы администрирования систем управления событиями информационной безопасности, систем обнаружения и предотвращения вторжений, мониторинга событий и инцидентов	Знает методы администрирования систем управления событиями информационной безопасности, систем обнаружения и предотвращения вторжений, мониторинга событий и инцидентов. Умеет выполнять проверку устойчивости приложений к внешнему несанкционированному доступу, в том числе проверка устойчивости веб-приложений к атакам, применение средств контроля безопасности, управление криптографическими средствами, а также организация мероприятий по обеспечению кибербезопасности.
		ПК-3.5.	выполняет проверку устойчивости приложений к внешнему несанкционированному доступу, в том числе проверка устойчивости веб-приложений к атакам, применение средств контроля безопасности, управление криптографическими средствами, а также организация	

			мероприятий по обеспечению кибербезопасности.	

12. Объем дисциплины в зачетных единицах/час - 3/108.
Форма промежуточной аттестации - зачет с оценкой.

13. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоёмкость (часы)					
	Всего	В том числе в интерактивной форме	По семестрам			
			9			
Аудиторные занятия	72		72			
в том числе: лекции	36		36			
Практические	0		0			
Лабораторные	36		36			
Самостоятельная работа	36		36			
Контроль	0		0			
Итого:	108		108			
Форма промежуточной аттестации	зачет с оценкой		зачет с оценкой			

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Введение в социальную инженерию	Определение социальной инженерии и ее влияние на информационную безопасность. История и развитие социальной инженерии. Классификация типов социальной инженерии и их особенности. Основные концептуальные положения СИ	Б1.В.11 Теория и методы социальной инженерии в информационной безопасности (10.05.01)
1.2	Психологические аспекты социальной инженерии	Основные принципы психологии, используемые социальными инженерами. Методы манипуляции и влияния на жертву. Психологические барьеры и уязвимости, которые могут быть использованы социальными инженерами. Основные направления социоинженерной деятельности.	
1.3	Тактики и методы социальной инженерии	Фишинг-атаки и методы подбора паролей. Использование поддельных источников и подделка личности. Социальные сети и особенности социальной инженерии в онлайн-среде. Манипуляции через телефонные звонки и электронную почту. Пределы последствий при социоинженерных атаках. Сопровождение социальных процессов в обществе.	
1.4	Методы противодействия социальной инженерии	Разработка политик безопасности и обучение сотрудников. Технические меры защиты информации от социальной инженерии. Предотвращение фишинг-атак и обнаружение мошенничества. Управление доступом и контроль аутентификации. Технологии защиты от социальных «хакеров». Принципы оценки эффективности средств защиты.	

1.5	Законодательство и этика	Законодательство в контексте социальной инженерии. Этические вопросы в противодействии социальной инженерии.	
2. Лабораторные работы			
2.1	Лабораторная работа № 1.	Разработка классификации типов социальной инженерии и их особенностей	Б1.В.11 Теория и методы социальной инженерии в информационной безопасности (10.05.01)
2.2	Лабораторная работа № 2.	Анализ уязвимостей и психологических барьеров.	
2.3	Лабораторная работа № 3.	Разработка стратегии противодействия психологическим методам манипуляций.	
2.4	Лабораторная работа № 4.	Симуляция фишинг-атаки и ее анализ.	
2.5	Лабораторная работа № 5.	Создание поддельного профиля и подделка личности, анализ атаки.	
2.6	Лабораторная работа № 6.	Использование технических мер защиты от социальной инженерии.	
2.7	Лабораторная работа № 7.	Этические аспекты противодействия социальной инженерии и разработка этических кодексов.	
2.8	Лабораторная работа № 8.	Судебные дела связанных с социальной инженерией.	
2.9	Лабораторная работа № 9.	Анализ эффективности мер по защите информации в социальной инженерии.	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)					
		Лекции	Практ.	Лаб. раб.	Самостоятельная работа	Контроль	Всего
1.1	Введение в социальную инженерию	6		6	6	0	18
1.2	Психологические аспекты социальной инженерии	8		8	8	0	24
1.3	Тактики и методы социальной инженерии	8		8	8	0	24
1.4	Методы противодействия социальной инженерии	8		8	8	0	24
1.5	Законодательство и этика	6		6	6	0	18
	Итого:	36		36	36	0	108

14. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины включает в себя лекционные занятия, лабораторные занятия и самостоятельную работу обучающихся. На первом занятии студент получает информацию для доступа к комплексу учебно-методических материалов.

Лекционные занятия посвящены рассмотрению теоретических основ дисциплины. Лабораторные занятия предназначены для формирования умений и навыков, закрепленных компетенциями по ОПОП. Самостоятельная работа студентов включает в себя проработку учебного материала лекций, разбор лабораторных заданий, подготовку к экзамену.

Для успешного освоения дисциплины рекомендуется подробно конспектировать лекционный материал, просматривать презентации (при наличии) по соответствующей теме, изучать основную и дополнительную литературу рекомендуемой библиографии,

При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей по работе на LMS-платформе, своевременно подключаться к online-занятиям, соблюдать рекомендации по организации самостоятельной работы.

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

а) основная литература:

№ п/п	Источник
1	Импортозамещающие технологии обеспечения информационной безопасности и защиты данных : учебное пособие / Д. А. Короченцев, Л. В. Черкесова, Е. А. Ревякина [и др.]. – Ростов-на-Дону : Донской ГТУ, 2021. – 335 с. – ISBN 978-5-7890-1893-4. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/237782. – Режим доступа: для авториз. пользователей.
2	Хэднеги, К. Искусство обмана. Социальная инженерия в мошеннических схемах / К. Хэднеги ; перевод А. Соломина. – Москва : Альпина Паблишер, 2020. – 430 с. – ISBN 978-5-9614-1072-3. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/140447. – Режим доступа: для авториз. пользователей.

б) дополнительная литература:

№ п/п	Источник
3	Райтман, М. Старший брат следит за тобой: Как защитить себя в цифровом мире / М. Райтман. – Москва : Альпина Паблишер, 2022. – 694 с. – ISBN 978-5-96147-881-5. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/259514. – Режим доступа: для авториз. пользователей.
4	Жемерикина, Ю. И. Социальная инженерия. Практикум : учебное пособие / Ю. И. Жемерикина, Т. А. Талалуева. – Москва : РТУ МИРЭА, 2022. – 82 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/310898. – Режим доступа: для авториз. пользователей.

в) информационные электронно-образовательные ресурсы**:**

№ п/п	Источник
5	Электронно-библиотечная система «Лань» - Режим доступа: https://e.lanbook.com
6	Электронный каталог Научной библиотеки Воронежского государственного университета. - Режим доступа: http//:www.lib.vsu.ru.
7	Криптографические протоколы (10.05.01)/Степанец Ю.А. - Образовательный портал «Электронный университет ВГУ». — Режим доступа: https://edu.vsu.ru

16. Перечень учебно-методического обеспечения для самостоятельной работы

В качестве формы организации самостоятельной работы применяются методические указания для самостоятельного освоения и приобретения навыков работы со специализированным программным обеспечением. Самостоятельная работа

студентов: изучение теоретического материала; подготовка к лекциям, работа с учебно-методической литературой, подготовка отчётов по лабораторным работам, подготовка к экзамену.

Для обеспечения самостоятельной работы студентов в электронном курсе дисциплины на образовательном портале «Электронный университет ВГУ» сформирован учебно-методический комплекс, который включает в себя: программу курса, учебные пособия и справочные материалы, методические указания по выполнению заданий лабораторных работ. Студенты получают доступ к данным материалам на первом занятии по дисциплине.

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение)

Дисциплина реализуется с применением электронного обучения и дистанционных образовательных технологий. Для организации занятий рекомендован онлайн-курс «Б1.В.11 Теория и методы социальной инженерии в информационной безопасности (10.05.01)», размещенный на платформе Электронного университета ВГУ (LMS moodle), а также Интернет-ресурсы, приведенные в п.15в.5.

18. Материально-техническое обеспечение дисциплины

Учебная аудитория для лекций: специализированная мебель, компьютер преподавателя, мультимедийный проектор, экран.
Учебная аудитория для лабораторных занятий: специализированная мебель, персональные компьютеры, мультимедийный проектор, экран, лабораторное оборудование программно-аппаратных средств обеспечения информационной безопасности.
Аудитория для самостоятельной работы: учебная мебель, компьютер с возможностью подключения к сети «Интернет» и электронной платформе Электронного университета ВГУ.

Программное обеспечение (см.файл МТО): ОС Windows v.7, 8, 10, набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

ПК-1. Способен проводить анализ требований и выполнять работы по проектированию программных и аппаратных компонент системы безопасности компьютерных систем и сетей, в том числе с использованием современных методов и средств защиты информации.

–ПК-1.4. проводит оценку соответствия механизмов безопасности компьютерной системы требованиям нормативных документов, а также их корректности существующим рискам.

ПК-3. Способен участвовать в работах по проектированию систем защиты информации в компьютерных системах и сетях при решении профессиональных, исследовательских и прикладных задач.

–ПК-3.2. знает методы администрирования систем управления событиями информационной безопасности, систем обнаружения и предотвращения вторжений, мониторинга событий и инцидентов.

–ПК-3.5. выполняет проверку устойчивости приложений к внешнему несанкционированному доступу, в том числе проверка устойчивости веб-приложений к атакам, применение средств контроля безопасности, управление криптографическими средствами, а также организация мероприятий по обеспечению кибербезопасности.

№ п/п	Наименования раздела дисциплины	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1	Введение в социальную инженерию	ПК-1	ПК-1.4	устный опрос, тест, лабораторная работа
2	Психологические аспекты социальной инженерии	ПК-1	ПК-1.4	устный опрос, тест, лабораторная работа
		ПК-3	ПК-3.2.	устный опрос, тест, лабораторная работа
			ПК-3.5.	устный опрос, тест, лабораторная работа
3	Тактики и методы социальной инженерии	ПК-1	ПК-1.4	устный опрос, тест, лабораторная работа
		ПК-3	ПК-3.2.	устный опрос, тест, лабораторная работа
			ПК-3.5.	устный опрос, тест, лабораторная работа
4	Методы противодействия социальной инженерии	ПК-1	ПК-1.4	устный опрос, тест, лабораторная работа
		ПК-3	ПК-3.2.	устный опрос, тест, лабораторная работа
			ПК-3.5.	устный опрос, тест, лабораторная работа
5	Законодательство и этика	ПК-1	ПК-1.4	устный опрос, тест, лабораторная работа
		ПК-3	ПК-3.2.	устный опрос, тест, лабораторная работа
Промежуточная аттестация, форма контроля - зачет с оценкой				Перечень вопросов (КИМ№1)

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

- лабораторные работы.

Перечень лабораторных работ

1	Лабораторная работа № 1.	Разработка классификации типов социальной инженерии и их особенностей
2	Лабораторная работа № 2.	Анализ уязвимостей и психологических барьеров.
3	Лабораторная работа № 3.	Разработка стратегии противодействия психологическим методам манипуляций.
4	Лабораторная работа № 4.	Симуляция фишинг-атаки и ее анализ.
5	Лабораторная работа № 5.	Создание поддельного профиля и подделка личности, анализ атаки.
6	Лабораторная работа № 6.	Использование технических мер защиты от социальной инженерии.
7	Лабораторная работа № 7.	Этические аспекты противодействия социальной инженерии и разработка этических кодексов.
8	Лабораторная работа № 8.	Судебные дела связанных с социальной инженерией.
9	Лабораторная работа № 9.	Анализ эффективности мер по защите информации в социальной инженерии.

Технология проведения
Все лабораторные работы обязательны для выполнение. Задание является общим для всех, выполняется индивидуально под наблюдением преподавателя.

Критерии оценивания

- оценивается «зачтено», если работа выполнена в полном объеме (приведены все задания, и они правильные, даны пояснения);

оценивается «не зачтено», работа выполнена не полностью или в представленной части много ошибок

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств: вопросы к экзамену.

Перечень вопросов к экзамену (КИМ №1)

1. История и современные направления защиты информации.
2. Правовая основа защиты информации за рубежом.
3. Правовая основа защиты информации в России.
4. Источники угроз защищаемой информации.
5. Утечка, разглашение, раскрытие и распространение защищаемой информации. Объективные и субъективные условия утечки информации.
6. Легальные, агентурные и технические каналы утечки информации.
7. Засекречивание информации. Политический и социальный аспекты засекречивания информации.
8. Принципы засекречивания информации: законность, обоснованность, своевременность.
9. Организационно-правовые формы засекречивания информации: перечневая форма и система первоначального засекречивания.
10. Рассекречивание информации. Виды сведений, подлежащих и не подлежащих рассекречиванию.
11. Классификация защищаемой информации по принадлежности, содержанию и степени секретности.
12. Носители секретной информации: документы, изделия (предметы), электромагнитные излучения.
13. Понятие государственной тайны. Сведения, которые подлежат засекречиванию и которые не могут быть засекречены.
14. Определение грифа секретности сведений, составляющих государственную тайну.
15. Порядок допуска к государственной тайне. Основания для отказа в допуске. Прекращение допуска.
16. Понятие коммерческой тайны и ее виды: технологическая, организационная, коммерческая. Методы промышленного шпионажа.
17. Правовые основы защиты коммерческой тайны за рубежом и в России.
18. Ответственность за нарушение законодательства о коммерческой тайне.
19. Цели незаконного получения сведений, составляющих коммерческую тайну.
20. Субъекты незаконного собирания сведений, составляющих коммерческую тайну.
21. Способы незаконного получения сведений, составляющих коммерческую тайну.
22. Закрытие свободного доступа к сведениям, составляющим коммерческую тайну.
23. Политический, экономический и моральный ущерб от утечки сведений, составляющих

государственную тайну.

24. Выявление, предупреждение и пресечение попыток неправомерного завладения сведениями и документами, составляющими коммерческую тайну.

25. Организация защиты от несанкционированного доступа конфиденциальной информации, обрабатываемой средствами вычислительной техники.

26. Организация защиты конфиденциальной информации от утечки по техническим каналам.

27. Ограничения в предоставлении государственным органам сведений, составляющих коммерческую тайну. Охрана коммерческой тайны.

28. Защита информации, составляющей профессиональную тайну.

29. Защита информации, составляющей банковскую тайну.

30. Защита сведений, составляющих личную тайну.

31. Понятие защиты информации и режима секретности (конфиденциальности). Меры по обеспечению режима конфиденциальности.

32. Меры по защите секретных и конфиденциальных сведений: правовые, организационные, инженерно-технические и программно-математические.

33. Система защиты информации, ее структурная и функциональная части.

34. Методы защиты информации: скрытие, ранжирование, дезинформация, дробление, морально нравственные методы, учет, кодирование, шифрование.

35. Средства защиты информации, требования к ним и решаемые с их помощью задачи.

36. Уголовная ответственность за государственную измену, шпионаж, разглашение государственной тайны и утрату секретных документов, объективная и субъективная сторона этих преступлений.

Критерии оценки ответов на вопросы зачета с оценкой

Для оценивания результатов обучения на зачете с оценкой используется - 4-балльная шала:
«отлично», «хорошо», «удовлетворительно», «неудовлетворительно», критерии оценивания приведены ниже.

Оценка «отлично» - студент демонстрирует глубокое понимание темы, умеет распространять вытекающие из теории выводы.
Оценка «хорошо» - студент демонстрирует понимание теоретических положений темы и базовых понятий, но допускает неточности в ответах, испытывает затруднения в применении знаний к анализу состояния проекта.
Оценка «удовлетворительно» - студент отвечает не на все предложенные вопросы, но не менее, чем на половину из них; не демонстрирует способности применения теоретических знаний для анализа ситуаций.
Оценка «неудовлетворительно» - студент демонстрирует непонимание теоретических основ и базовых понятий курса.

Оценка промежуточной аттестации формируется как интегральная оценка по следующей формуле (При округлении оценки используется правило правильного округления. При получении оценки не менее 3 баллов, выставляется «зачтено», менее 3 баллов - «не зачтено». При этом, все лабораторные работы должны быть выполнены и защищены

$$Q_{пром\_ат} = 0{,}2Q_{КР1} + 0{,}2Q_{КР2} + 0{,}6Q_{экз}$$

При округлении оценки используется правило правильного округления. При получении оценки не менее 3 баллов, выставляется «зачтено», менее 3 баллов - «не зачтено». При этом, все лабораторные работы должны быть выполнены и защищены.

20.3 Фонд оценочных средств сформированности компетенций студентов, рекомендуемый для проведения диагностических работ

ПК-1. Способен проводить анализ требований и выполнять работы по проекти-рованию программных и аппаратных компонент системы безопасности компьютер-ных систем и сетей, в том числе с использованием современных методов и средств защиты информации.

1. Угрозы безопасности ПДн:

а) совокупность условий факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий при их обработке в ИСПДн;

б) совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности персональных данных;

в) только стихийное или бедствие техногенного характера.

2. Несанкционированный доступ (НСД) к информации:

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

б) доступ к информации, нарушающий установленные правила разграничения доступа, с использованием специально разработанных технических средств;

в) копирование, искажение или модификация информации с нарушением установленных правил разграничения доступа.

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

а) несанкционированный доступ к информации, вредительские программы;

б) электромагнитные излучения и наводки, несанкционированная модификация структур;

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

4. Для защиты от случайных угроз компьютерной информации используют:

а) обучение пользователей правилам работы с КС, разрешительную систему доступа в помещение;

б) межсетевые экраны, идентификацию и аутентификацию пользователей;

в) дублирование информации, создание отказоустойчивых КС, блокировка ошибочных операций.

5. Блокирование персональных данных:

а) временное прекращение обработки персональных данных;

б) действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

в) действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

6. Обезличивание персональных данных:

а) действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

б) действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных;

в) все перечисленные действия.

7. Срок хранения персональных данных в форме, позволяющей определить субъекта персональных данных:

а) 1 год;

б) 5 лет;

в) не дольше, чем этого требуют цели обработки персональных данных, если иное не установлено законом или договором.

8. Свойство открытости означает, что система реализует открытые спецификации, достаточные для того, чтобы обеспечить:

1. возможность переноса разработанного прикладного программного обеспечения на широких диапазон систем с минимальными изменениями (мобильность приложений, переносимость)
2. совместную работу (взаимодействие) с другими прикладными приложениями на локальных и удаленных платформах (интероперабельность, способность к взаимодействию)
3. взаимодействие с пользователями в стиле, облегчающим последним переход от системы к системе (мобильность пользователей)
4. **все вышеперечисленное**

ПК-3. Способен участвовать в работах по проектированию систем защиты информации в компьютерных системах и сетях при решении профессиональных, исследовательских и прикладных задач.

1. Системы анализа уязвимостей позволяют:

а) выявить злоумышленника, работающего в компьютерной сети;

б) выявить уязвимости проектируемой системы защиты информации; *в) выявить уязвимости действующей системы защиты информации.*

2. Использование электронной подписи позволяет не допустить (лишнее исключить):

а) отказ от авторства;

б) приписывание авторства;

в) несанкционированное ознакомление с подписанным документов.

3. Обязано ли лицо, осуществляющее обработку персональных данных по поручению оператора, получать согласие субъекта персональных данных на обработку его персональных данных:

а) не обязано;

б) обязано;

в) не обязано только в случаях, предусмотренных законом.

4. В общедоступные источники персональных данных (в том числе справочники, адресные книги) персональные данные включаются:

а) с письменного согласия субъекта персональных данных;

б) согласия субъекта персональных данных не требуется;

в) согласия субъекта персональных данных не требуется, но по требованию субъекта данные в любое время должны быть исключены из общедоступных источников персональных данных.

5. Что такое несанкционированный доступ (нсд)?

1) Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа

2) Создание резервных копий в организации

3) Правила и положения, выработанные в организации для обхода парольной защиты

4) Вход в систему без согласования с руководителем организации

5) Удаление не нужной информации

6. В чем заключается основная причина потерь информации, связанной с ПК?

1) с глобальным хищением информации

2) с появлением интернета

3) с недостаточной образованностью в области безопасности

7. Открытость для изменения и дополнения мер обеспечения безопасности информации - это общее требование к защите информации (1) или требование, предъявляемое к системе безопасности информации (2), или условие, которому должна удовлетворять система защиты информации (3)?

- (1).
- (2).
- **(3).**
- Ни одно из этих понятий.

8. Нестандартность, разнообразность - это общие требования к защите информации (1) или требование, предъявляемое к системе безопасности информации (2), или условие, которому должна удовлетворять система защиты информации (3)?

- (1).
- (2).
- **(3).**
- Ни одно из этих понятий.

9. Комплексность - это общие требования к защите информации (1) или требование, предъявляемое к

системе безопасности информации (2), или условие, которому должна удовлетворять система защиты информации (3)?

- **(1).**
- (2).
- (3).
- Ни одно из этих понятий.

10) Программные закладки могут выполнять действия
a) вносить произвольные искажения в коды программ
b) переносить фрагменты информации
c) искажать выводимую информацию
d) Все из перечисленного
e) Ничего из перечисленного

11) Конфигурация системы Windows не включает в себя
a) Настройку файловой системы
b) Настройку параметров сети
c) Настройку учетных записей
d) Проверку на вирусы

12) Угрозами конфиденциальной информации не являются
a) ознакомление без нарушения ее целостности
b) модификация информации
c) разрушение информации
d) создание и распространение вирусов

13) Вредоносный код проникает в организации способами
a) Файлы с общим доступом с домашних и рабочих компьютеров
b) Файлы, загружаемые с сайтов интернета
c) Файлы, поступающие в организацию в виде вложений электронной почты
d) Файлы, внедряемые в системы посредством использования уязвимостей
e) Все из перечисленного
f) Ничего из перечисленного

14. Какую опасность представляют open-source библиотеки и инструменты в корпоративной среде? Выберите все правильные ответы.

1. **Часто отсутствуют механизмы аутентификации**
2. **Присутствуют избыточные права и повышение привилегий**
3. Используются нестандартные сетевые протоколы
4. **Встречаются незаблокированные стандартные учетные записи**
5. Не допускается сканирование антивирусом
6. **В конфигурационных файлах встречаются пароли в открытом виде**

15. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

1. Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
2. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
3. **Улучшить контроль за безопасностью этой информации**
4. Снизить уровень классификации этой информации

16. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

1. Внедрение управления механизмами безопасности
2. Классификацию данных после внедрения механизмов безопасности
3. **Уровень доверия, обеспечиваемый механизмом безопасности**
4. Соотношение затрат / выгод

17. Где применяются средства контроля динамической целостности?

1. **анализе потока финансовых сообщений**
2. обработке данных
3. **при выявлении кражи, дублирования отдельных сообщений**

Задания раздела 20.3 рекомендуются к использованию при проведении диагностических работ с целью оценки остаточных результатов освоения данной дисциплины (знаний, умений, навыков).