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.09 Мониторинг функционирования распределенных компьютерных систем

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 по защите информации

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины:

кибербезопасности информационных систем

6. Составители программы:

Сафронов Виталий Владимирович, к.т.н., доцент кафедры кибербезопасности информационных систем

7. Рекомендована:

НМС факультета ПММ, протокол № 5 от 22.03.2024

8. Учебный год: 2025/2026 **Семестр(ы):** 4

9. Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются: формирование у обучающихся знания по применению средств мониторинга событий компьютерных систем для обеспечения информационной безопасности конечных систем.

Изучение способов проведения мониторинга структуры информационных процессов и выявления уязвимых компонентов в сетевой инфраструктуре; использование специализированных источников и справочных систем для поиска научно-технической литературы, нормативных и методических материалов; проведение анализа способов, методов, средств и алгоритмов решения задач расследования инцидентов в области информационной безопасности распределенных компьютерных систем.

10. Место учебной дисциплины в структуре ОПОП: дисциплина относится к части, формируемой участниками образовательных отношений, 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-2.	Способен принимать участие в экспертизе и анализе уязвимостей, угроз и инцидентов информационной безопасности в компьютерных системах и сетях	ПК-2.2	способен проводить анализ компьютерных систем с целью определения уровня защищённости и доверия с последующим обобщением и обработкой информации, полученной в ходе исследований	Умеет: проводить анализ компьютерных систем с целью определения уровня защищённости и доверия с последующим обобщением и обработкой информации, полученной в ходе исследований. Владеет: Методами анализа компьютерных систем с целью определения уровня защищённости и доверия.
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: 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. Владеет: методами 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.	

12. Объем дисциплины в зачетных единицах/час – 3/108.
Форма промежуточной аттестации - экзамен.

13. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоёмкость (часы)					
	Всего	В том числе в интерактивной форме	По семестрам			
				4		
Аудиторные занятия	48			48		
в том числе: лекции	16			16		
Практические	0			0		
Лабораторные	32			32		
Самостоятельная работа	24			24		
Контроль	36			36		
Итого:	108			108		
Форма промежуточной аттестации	Экзамен			Экзамен		

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Методы, системы, способы и средства управления ИБ в КС	Виды, типы, классы и методы управления ИБ. Системы и средства управления ИБ. Виды СУ ИБ, их особенности их построения и функционирования. Системы Active Directory, ADFS, FreeIPA. Виды методов управления доступом (УД): ABAC, RBAC, MACL. Системы IAM: Kerberos и KeyCloak. Протоколы OAuth, OIDC, WebAuth. Системы и протоколы защищенного удаленного администрирования. Методы, системы, протоколы и средства удаленного управления ИБ: в VPN; в КС. Управление web безопасностью. Протокол TLS/https.	Б1.В.09 Мониторинг функционирования распределенных компьютерных систем (10.05.01 БКСиС) https://edu.vsu.ru/course/view.php?id=27730
1.2	Методы, системы, способы и средства мониторинга ИБ в КС	Виды и методы мониторинга ИБ. Архитектура мониторинга ИБ: сенсоры, датчики, коллекторы. Типы систем мониторинга ИБ, их особенности. Регистрация, протоколирование, контроль и мониторинг ИБ. Средства мониторинга: снифферы, NTA, UEDA и DLP. Обнаружение компьютерных атак: IDS и IPS, управление ими. Классы средств EDR и XDR. Анализ программно-аппаратных средств мониторинга.	
1.3	Системы управления событиями безопасности	События безопасности. Инциденты ИБ. Анализ событий ИБ. Выявление инцидентов ИБ. SIEM. Требования к SIEM. Системы IRP автоматизации мониторинга и управления ИБ. Методы и способы построения и функционирования SIEM и SOAR. Анализ средств управления событиями ИБ и управления инцидентами ИБ.	
1.4	Центры: SOC, мониторинга ИБ.	Центры мониторинга ИБ. Требования к SOC. Формирование SOC на основе TIP, IDS/IPS, SIEM и SOAR. Требования к лицензиатам ФСТЭК по мониторингу ИБ. Требования к Центрам мониторинга ИБ. Программно-аппаратное оснащение ЦМ ИБ. Значение оценки защищенности, значение упреждающего, оперативного и адаптивного управления ИБ.	
2. Лабораторные работы			
2.1	Программные средства защищенного удаленного администрирования и конфигурирования компьютерных систем и	Исследование характеристик и возможностей программных средств защищенного удаленного администрирования и конфигурирования компьютерных систем и средств защиты информации в КС. Настройка и применение программных средств защищенного	Б1.В.09 Мониторинг функционирования распределенных компьютерных систем

	средств защиты информации в КС.	удаленного администрирования и конфигурирования компьютерных систем и средств защиты информации в КС.	(10.05.01 БКСиС) https://edu.vsu.ru/course/view.php?id=27730
2.2	Программные средства удаленного управления средствами обнаружения вторжений	Исследование характеристик и возможностей программных средств удаленного управления средствами обнаружения вторжений (компьютерных атак) в КС. Настройка и применение программных средств удаленного управления средствами обнаружения вторжений (компьютерных атак) в КС.	
2.3	Программные средства мониторинга ИБ	Исследование характеристик и возможностей программных средств мониторинга ИБ. Настройка и применение программных средств мониторинга ИБ.	
2.4	SIEM (программные системы управления событиями информационной безопасности).	Исследование характеристик и возможностей SIEM (программных систем управления событиями информационной безопасности). Настройка и применение SIEM (программных систем управления событиями информационной безопасности). Программно-аппаратные потребности Центра мониторинга ИБ.	

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	Методы, системы, способы и средства управления ИБ в КС	4	0	8	6	8	26
1.2	Методы, системы, способы и средства мониторинга ИБ в КС	4	0	8	6	8	26
1.3	Системы управления событиями безопасности	4	0	8	6	10	28
1.4	Центры: SOC, мониторинга ИБ.	4	0	8	6	10	28
	Итого:	16	0	32	24	36	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	Пугин, В. В. Защита информации в компьютерных информационных системах : учебное пособие / В. В. Пугин, Е. Ю. Голубничая, С. А. Лабада. — Самара : ПГУТИ, 2018. — 119 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182299. — Режим доступа: для авториз. пользователей.
2	Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401. — Режим доступа: для авториз. пользователей.

б) дополнительная литература:

№ п/п	Источник
3	Алѐшкин, А. С. Аппаратные и программные средства поиска уязвимостей при моделировании и эксплуатации информационных систем (обеспечение информационной безопасности) : учебное пособие / А. С. Алѐшкин, С. А. Лесько, Д. О. Жуков. — Москва : РТУ МИРЭА, 2020. — 152 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167600. — Режим доступа: для авториз. пользователей.

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

№ п/п	Источник
4	Электронно-библиотечная система «Университетская библиотека online (доступ осуществляется по адресу: https://biblioclub.ru/);
5	Информационно-телекоммуникационная система «Контекстум» (Национальный цифровой ресурс «РУКОНТ»);
6	Электронно-библиотечной системе «Лань» (доступ осуществляется по адресу: https://e.lanbook.com/),
7	ЭБС «BOOK» (доступ осуществляется по адресу: https://book.ru).
8	Электронный каталог Научной библиотеки Воронежского государственного университета. – Режим доступа: http//:www.lib.vsu.ru.
9	Б1.В.09 Мониторинг функционирования распределенных компьютерных систем (10.05.01 БКСиС)/Сафронов В.В. - Образовательный портал «Электронный университет ВГУ». — Режим доступа: https://edu.vsu.ru/course/view.php?id=27730.

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.09 Мониторинг функционирования распределенных компьютерных систем (10.05.01 БКСиС)», размещенный на платформе Электронного университета ВГУ (LMS moodle), а также Интернет-ресурсы, приведенные в п.15 в.9.

18. Материально-техническое обеспечение дисциплины

Учебная аудитория для проведения занятий *лекционного типа*, семинарского типа, организации самостоятельной работы, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации: специализированная мебель, компьютер (ноутбук), мультимедийное оборудование (проектор, экран, средства звуковоспроизведения), допускается использование переносного оборудования.

ОС Windows 8 (10), интернет-браузер (Google Chrome, Mozilla Firefox), ПО Adobe Reader, пакет стандартных офисных приложений для работы с документами, таблицами (MS Office, Мой Офис, Libre Office, Notepad ++ (свободное и/или бесплатное ПО), 7-zip (свободное и/или бесплатное ПО).

Учебная аудитория для проведения практических занятий, *лабораторных работ*, организации самостоятельной работы, проведения текущей и промежуточной аттестаций: специализированная мебель, персональные компьютеры для индивидуальной работы с возможностью подключения к сети «Интернет», мультимедийное оборудование (проектор, экран, средства звуковоспроизведения).

ОС Windows 8 (10), интернет-браузер (Google Chrome, Mozilla Firefox), ПО Adobe Reader, пакет стандартных офисных приложений для работы с документами, таблицами (MS Office, Мой Офис, Libre Office), специализированное ПО по тематике дисциплины (допускается демоверсия или виртуальный аналог ПО), Intellij IDEA Community Edition (свободное и/или бесплатное ПО); Jet Brains PyCharm Community Edition (свободное и/или бесплатное ПО); Anaconda (свободное и/или бесплатное ПО); Maxima (свободное и/или бесплатное ПО); Scilab (свободное и/или бесплатное ПО); NetBeans IDE (свободное и/или бесплатное ПО); Microsoft Visual Studio Community Edition (свободное и/или бесплатное ПО); Notepad ++ (свободное и/или бесплатное ПО); Справочно-правовая система Гарант (лицензионное ПО); 7-zip (свободное и/или бесплатное ПО); Matlab (лицензионное ПО); Visual Studio Code (свободное и/или бесплатное ПО); Apache Spark (свободное и/или бесплатное ПО); PostgreSql (свободное и/или бесплатное ПО), Anylogic (свободное и/или бесплатное ПО), 1С:Предприятие 8.3 (лицензионное ПО).

Учебная аудитория для проведения *лекционных* и практических занятий, *лабораторных работ, организации самостоятельной работы*, проведения текущей и промежуточной аттестаций: специализированная мебель, персональные компьютеры для индивидуальной работы с возможностью подключения к сети «Интернет», мультимедийное оборудование (проектор, экран, средства звуковоспроизведения). Типовой комплект учебного

оборудования "Сетевая безопасность", SECURITY (страна изготовитель – Россия).

ОС Windows 8 (10), интернет-браузер (Google Chrome, Mozilla Firefox), ПО Adobe Reader, пакет стандартных офисных приложений для работы с документами, таблицами (MS Office, Мой Офис, Libre Office), специализированное ПО по тематике дисциплины (допускается демоверсия или виртуальный аналог ПО), Intellij IDEA Community Edition (свободное и/или бесплатное ПО); Jet Brains PyCharm Community Edition (свободное и/или бесплатное ПО); Anaconda (свободное и/или бесплатное ПО); Maxima (свободное и/или бесплатное ПО); Scilab (свободное и/или бесплатное ПО); NetBeans IDE (свободное и/или бесплатное ПО); Microsoft Visual Studio Community Edition (свободное и/или бесплатное ПО); Notepad ++ (свободное и/или бесплатное ПО); Справочно-правовая система Гарант (лицензионное ПО); 7-zip (свободное и/или бесплатное ПО); Matlab (лицензионное ПО); Visual Studio Code (свободное и/или бесплатное ПО); Apache Spark (свободное и/или бесплатное ПО); PostgreSql (свободное и/или бесплатное ПО), Anylogic (свободное и/или бесплатное ПО).

19. Оценочные средства для проведения текущей и промежуточной аттестаций

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

№ п/п	Наименования раздела дисциплины	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1	Методы, системы, способы и средства управления ИБ в КС	ПК-2	ПК-2.2	устный опрос, тест, лабораторная работа
		ПК-3	ПК-3.2	
2	Методы, системы, способы и средства мониторинга ИБ в КС	ПК-2	ПК-2.2	устный опрос, тест, лабораторная работа
		ПК-3	ПК-3.2	
			ПК-3.5	
3	Системы управления событиями безопасности	ПК-2	ПК-2.2	устный опрос, тест, лабораторная работа
		ПК-3	ПК-3.2	
			ПК-3.5	
4	Центры: SOC, мониторинга ИБ.	ПК-2	ПК-2.2	устный опрос, тест, лабораторная работа
		ПК-3	ПК-3.2	
			ПК-3.5	
Промежуточная аттестация, форма контроля - экзамен				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	Программные средства защищенного удаленного администрирования и конфигурирования компьютерных систем и средств защиты информации в КС.	В соответствии с заданным вариантом: провести исследование характеристик и возможностей программного средств защищенного удаленного администрирования и конфигурирования компьютерных систем и средств защиты информации в КС; выполнить настройку и применение программных средств защищенного удаленного администрирования и конфигурирования компьютерных систем и средств защиты информации в КС.
2	Программные средства удаленного управления средствами обнаружения вторжений	В соответствии с заданным вариантом: провести исследование характеристик и возможностей программных средств удаленного управления средствами обнаружения вторжений (компьютерных атак) в КС; выполнить настройку и применение программных средств удаленного

		управления средствами обнаружения вторжений (компьютерных атак) в КС.
3	Программные средства мониторинга ИБ	В соответствии с заданным вариантом: провести исследование характеристик и возможностей программных средств мониторинга ИБ; выполнить настройку и применение программных средств мониторинга ИБ.
4	SIEM (программные системы управления событиями информационной безопасности).	В соответствии с заданным вариантом: провести исследование характеристик и возможностей SIEM (программных систем управления событиями информационной безопасности); выполнить настройку и применение SIEM (программных систем управления событиями информационной безопасности).

Технология проведения
Все лабораторные работы обязательны для выполнения. 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. Виды, типы, классы и методы управления ИБ.
2. Системы и средства управления ИБ.
3. Виды СУ ИБ, их особенности
4. Структуры, способы построения и функционирования СУ ИБ.
5. Методы, системы, протоколы и средства защищенного удаленного администрирования.
6. Методы, системы, протоколы и средства удаленного конфигурирования и управления средствами защиты информации (сенсорами обнаружения вторжений, межсетевыми экранами, СКЗИ (VPN) и МПО в КС).
7. Методы, системы, протоколы и средства локального конфигурирования и управления средствами защиты информации (управление средствами защиты НСД, DLP, антивирусной защиты).
8. Концепция мониторинга безопасности в КС.
9. Виды мониторинга ИБ, методы его осуществления.
10. Архитектура сетевого мониторинга ИБ. Сенсоры, датчики, коллекторы.
11. Типы систем мониторинга ИБ, их особенности.
12. Регистрация, протоколирование, контроль и мониторинг.
13. Регистрация и мониторинг безопасности в операционных системах.
14. Средства мониторинга безопасности в операционных системах
15. Средства мониторинга безопасности трафика.
16. Системы управления событиями информационной безопасности (SIEM).
17. Анализ отечественных программно-аппаратных средств мониторинга и анализа протоколов и программных средств из открытого ПО.

18. Центры: SOC, мониторинга ИБ.
19. Средства управления и мониторинга ИБ
20. Применение средства мониторинга ИБ в сети.
21. Применение средства мониторинга ИБ в операционных системах.
22. Применение средства удаленного защищенного управления ИБ.
23. Применение средства удаленного управления межсетевым экраном.
24. Установка и администрирование SIEM.
25. Обнаружение инцидентов ИБ посредством SIEM.
26. Применение SIEM в различных вариантах
27. Использование парольной защиты.
28. Виртуальные частные сети.
29. Подсистемы системы информационной безопасности.
30. Протоколирование.
31. Активный аудит.
32. Несанкционированный доступ (НСД) к информации.
33. Системы анализа уязвимостей.
34. Что является инженерно-технической формой защиты информации.
35. Что является правовой формой защиты информации.
36. Определяющие признаки, по которым производится классификация информационных систем.
37. Основным механизмы защиты компьютерной системы от несанкционированного доступа.
38. Основные способы разграничения доступа в компьютерных системах.
39. Протоколы маршрутизации. Назначение и типовые уязвимости.
40. Правила, применяемые в брандмауэрах.
41. Модели типа «черный ящик».
42. Топология сети.
43. Средства контроля динамической целостности.
44. Криптографические средства.
45. Угроза типа навязывание ложного маршрута.
46. Угроза типа внедрение ложного объекта сети.
47. Угроза типа отказ в обслуживании.
48. Угроза типа «Анализ сетевого траффика».
49. Алгоритмы идентификации и аутентификации хостов, пользователей.
50. Каналы утечки, использование которых для несанкционированного доступа не требует непосредственного доступа к техническим устройствам компьютерных систем.
51. Какие киберугрозы являются ключевыми в современных реалиях.
52. Модель Kill Chain.
53. В чем особенность кибератак с применением вирусов-шифровальщиков в современных реалиях.
54. Какую опасность представляют open-source библиотеки и инструменты.

Критерии оценки ответов на вопросы экзамена

Для оценивания результатов обучения на экзамене 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-2. Способен принимать участие в экспертизе и анализе уязвимостей, угроз и инцидентов информационной безопасности в компьютерных системах и сетях

1. Для средств обработки информации оформляется
   - допуск
   - **сертификат**
   - аттестат
2. Что относится к показателям надёжности?
   - экономичность;
   - **долговечность;**
   - технологичность.
3. Угрозы информации направлены на:
   - **конфиденциальность;**
   - **целостность;**
   - **доступность.**
4. Источники внешних угроз это:
   - **хакеры;**
   - **криминальные структуры;**
   - **представители силовых структур**
5. Источники внутренних угроз это:
   - **персонал;**
   - **транспорт;**
   - **средства связи.**
6. К каналам утечки информации относят:
   - **разглашение;**
   - **отказ средств обработки;**
   - несанкционированный доступ.
7. При оценке рисков используют понятия:
   - **риск;**
   - несанкционированный доступ.
   - **уязвимость.**
8. Как называется доступ к информации, нарушающий правила разграничения доступа

с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами?

- мандатный доступ;
- атака;
- **несанкционированный доступ.**

9. Как называется способ защиты информации от утечки через ПЭМИН, основанный на локализации электромагнитной энергии в определенном пространстве за счет ограничения распространения ее всеми возможными способами?

- **экранирование;**
- подавление;
- зашумление.

10. В криптосистемах с открытым ключом

A) открытый ключ доступен всем желающим, закрытый ключ доступен только получателю сообщения

B) для шифрования и дешифрования используется один ключ

C) закрытый ключ доступен всем желающим, открытый ключ доступен только получателю сообщения

D) закрытый и открытый ключи доступны всем желающим

11. Присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения, называется

A) электронной подписью

B) идентификатором

C) ключом

D) шифром

12. Характеристика шифра, определяющая стойкость шифра к дешифрованию без знания ключа, называется

A) криптостойкостью

B) надежностью

C) эффективностью

D) уровнем безопасности

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

1. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

А) сотрудники

Б) хакеры

В) атакующие

Г) контрагенты, лица, работающие по договору

2. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

А) когда для обеспечения хорошей безопасности учтены все риски

Б) когда риски не могут быть приняты во внимание по политическим соображениям

В) когда необходимые защитные меры слишком сложны

Г) когда стоимость контрмер превышает ценность актива и потенциальные потери

3. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

А) анализ рисков

Б) анализ затрат / выгоды

В) результаты аттестации

Г) выявление уязвимостей и угроз, являющихся причиной риска

4. Тактическое планирование – это:

А) долгосрочное планирование

Б) среднесрочное планирование

В) ежедневное планирование

Г) планирование на 6 месяцев

5. Эффективная программа безопасности требует сбалансированного применения:

А) технических и нетехнических методов

Б) контрмер и защитных механизмов

В) физической безопасности и технических средств защиты

Г) процедур безопасности и шифрования

6. В перечень этапов проведения аудита ИС входит:
1) выработка рекомендаций
2) сбор информации для аудита
3) выявление недостатков при обработке информации
4) выработка рекомендаций
7. Результаты проведения аудита подразделяются на:
1) организационные
2) технические
3) программные
4) методологические
8. Оценка рисков для ИС производится с помощью следующих шкал:
1) количественной
2) логарифмической
3) качественной
4) матричной

9. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?
А) чтобы убедиться, что проводится справедливая оценка
Б) это не требуется. для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
В) поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа
Г) поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку
10. Естественные угрозы безопасности информации вызваны:
А) деятельностью человека
Б) ошибками при проектировании системы безопасности, ее элементов или разработке программного обеспечения
В) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека
Г) ошибками при действиях персонала
11. Искусственные угрозы безопасности информации вызваны:
А) деятельностью человека
Б) ошибками при проектировании системы безопасности, ее элементов или разработке программного обеспечения
В) ошибками при действиях персонала
Г) корыстными устремлениями злоумышленников
12. Создание политики ИБ должно учитывать следующие направления защиты:
1) защита каналов связи
2) мониторинг деятельности сотрудников фирмы
3) подавление побочных электромагнитных излучений и наводок
4) защита процессов, процедур и программ обработки информации
13. Иерархия управления ИБ включают следующее число основных процессов:
1) 4
2) 5
3) 6
4) 7
14. Выделите гипермакеры ИНС?
- Внутренняя реализация нейрона;
- **Количество нейронов в сети;**
- **Количество слоев;**
- Механизм обучения.

15. Какой атаки на DNS протокол не существует?
- DNS DDOS;
- Fake DNS;
- **XSS DNS.**

16. Какой атаки на ARP протокол не существует?

- ARP Spoofing;
- **ARP Stuffing;**
- ARP Sniffing.

17. Расположите в порядке следование модели OSI типы атак
    - **DNS Sniffing;**
    - ARP Spoofing;
    - **XSS.**
18. Используется ли условная вероятность в методах обнаружения злоупотреблений?
    - **да;**
    - нет.
19. Является ли система обнаружения вторжений активным компонентом по защите от угроз?
    - да;
    - **нет.**

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