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

УТВЕРЖДАЮ
заведующий кафедрой
кибербезопасности
информационных систем
С.Л. Кенин

17.03.2025

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ Б1.В.07 Кибербезопасность критических систем и инфраструктур

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 № 6 от 17.03.2025

8. Учебный год: 2029/2030 **Семестр(ы):** А

9. Цели и задачи учебной дисциплины

Целями дисциплины является формирование у студентов навыков планирования, организации и проведения работ по определению критических процессов и категорированию значимых объектов критической информационной инфраструктуры с помощью систем безопасности.

Основой является теоретическая и практическая подготовка студентов к деятельности, связанной с организацией работ по выбору специальных систем безопасности значимых объектов КИИ с помощью.

Задачами дисциплины являются:

– ознакомление с правовыми, организационно-распорядительными, нормативными и информационными документами в области безопасности значимых объектов критической информационной инфраструктуры;

– ознакомление с физическими основами реализации угроз безопасности информации на объекте информатизации и порядка их выявления;

– ознакомление с системным подходом, используемым при обеспечении безопасности значимых объектов критической информационной инфраструктуры и правилами выбора систем безопасности;

– ознакомление с методиками проведения категорирования значимых объектов в соответствии с методологией исследований защищенности средств и систем на соответствие требованиям по безопасности информации;

– ознакомление с практикой отработки методик проведения категорирования значимого объекта в соответствии с методологией исследований защищенности средств и систем на соответствие требованиям по безопасности информации.

10. Место учебной дисциплины в структуре ОПОП: дисциплина относится к части, формируемой участниками образовательных отношений блока Б1.

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-2.5	проводит теоретические и прикладное исследование уровней защищенности компьютерных систем и сетей	Умеет: проводить теоретические и прикладное исследование уровней защищенности компьютерных систем и сетей.
ПК-3.	Способен участвовать в работах по проектированию систем защиты информации в компьютерных системах и сетях при решении профессиональных, исследовательских и прикладных задач	ПК-3.3.	способен проводить анализ безопасности компьютерных систем с использованием актуальных стандартов в области компьютерной безопасности	Знает: актуальные стандарты в области компьютерной безопасности. Умеет: – проводить анализ безопасности компьютерных систем с использованием актуальных стандартов в области компьютерной безопасности; – 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			
				А		
Аудиторные занятия	70			70		
в том числе: лекции	28			28		
Практические	0			0		
Лабораторные	42			42		
Самостоятельная работа	38			38		
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	Проблематика защиты критической информационной инфраструктуры и правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры	1. Введение в тематику защиты значимых объектов критической информационной инфраструктуры. 2. Информационная инфраструктура России. Понятие критической информационной инфраструктуры (КИИ). 3. Обеспечение безопасности критической информационной инфраструктуры в иностранных государствах. 4. Основные термины. Уполномоченные органы (регуляторы) в сфере обеспечения безопасности КИИ. Права и обязанности субъектов КИИ. 5. Алгоритм мероприятий по реализации требований ФЗ № 187-ФЗ. Анализ нормативно-правовых актов в сфере КИИ. 6. Уголовная и административная ответственность субъектов КИИ.	Б1.В.07 Кибербезопасность критических систем и инфраструктур (10.05.01 БКСиС)
1.2	Правила категорирования объектов КИИ.	1. Получение информации о видах деятельности организаций. 2. Определение относимости организации к субъектам КИИ. 3. Разбор положений Постановления Правительства РФ № 127 «Об утверждении Правил категорирования объектов КИИ, а также показателей критериев значимости объектов КИИ РФ и их значений» 4. Выделение и учет объектов КИИ. Определение критериев значимости объектов КИИ РФ и их	

		значений. Определение категории значимости объектов КИИ и подготовка сведений о категорировании для направления во ФСТЭК России. 5. Положения приказа ФСТЭК России № 236 "Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий" **Выделение критических для деятельности процессов.** 1. Процессный подход 2. Сбор информации о процессах 3. Анализ бизнес-процессов 4. Выделение критических процессов	
1.3	Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры	1. Характеристика приказов ФСБ России в сфере КИИ. 2. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) в соответствии с приказом ФСБ России № 367 "Об утверждении Перечня информации, представляемой в ГосСОПКА и Порядка представления информации в ГосСОПКА" 3. Приказ ФСБ России № 366 "О Национальном координационном центре по компьютерным инцидентам". Порядок обмена информацией о компьютерных инцидентах между субъектами КИИ в соответствии с приказом ФСБ России № 368. 4. Разработка регламента управления инцидентами и плана реагирования на компьютерные инциденты. 5. Анализ требований к обеспечению безопасности значимых объектов КИИ в соответствии с ФЗ № 187, приказом ФСТЭК № 239 "Об утверждении Требований по обеспечению безопасности ЗО КИИ РФ", приказом ФСТЭК № 235 "Об утверждении Требований к созданию систем безопасности ЗО КИИ РФ и обеспечению их функционирования" 6. Разработка организационных и технических мер по обеспечению безопасности значимого объекта КИИ. Разработка рабочей (эксплуатационной) документации на значимый объект (в части обеспечения его безопасности). Порядок аттестации значимых объектов КИИ.	
1.4	Обеспечение внутреннего контроля и эксплуатации значимых объектов КИИ	1. Регламент аудита информационной безопасности. 2. Аудит информационной безопасности. План мероприятий по реагированию на компьютерные инциденты и мерами по ликвидации последствий компьютерных атак. 3. Обеспечение безопасности значимых объектов КИИ в ходе их эксплуатации. 4. Обеспечение безопасности значимых объектов КИИ при выводе их из эксплуатации. 5. Подключение значимых объектов КИИ к госСОПКА.	
2. Лабораторные работы			
2.1	Проблематика защиты критической информационной инфраструктуры и правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры	Лабораторная работа 1. Подготовка сведений об организации. Лабораторная работа 2. Создание комиссии по категорированию.	Б1.В.07 Кибербезопасность критических систем и инфраструктур (10.05.01 БКСиС)
2.2	Правила категорирования объектов КИИ.	Лабораторная работа 3. Формирование перечня объектов КИИ.	

		Лабораторная работа 4. Категорирование объектов КИИ.	
2.3	Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры	Лабораторная работа 5. Анализ возможных действий нарушителей в отношении объектов критической информационной инфраструктуры	
2.4	Обеспечение внутреннего контроля и эксплуатации значимых объектов КИИ	Лабораторная работа 6. Выбор средств защиты информации для нейтрализации угроз безопасности информации. Лабораторная работа 7. Разработка ОРД ЗОКИИ	

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	Проблематика защиты критической информационной инфраструктуры и правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры	6	0	16	10	0	32
1.2	Правила категорирования объектов КИИ.	6	0	4	10	0	20
1.3	Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры	8	0	8	10	0	26
1.4	Обеспечение внутреннего контроля и эксплуатации значимых объектов КИИ	8	0	14	8	0	30
	Итого:	28	0	42	38	0	108

14. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины включает в себя лекционные занятия, лабораторныезанятия 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	ГОСТ Р ИСО/МЭК 27007-2014 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности»
2	Демидов О. Глобальное управление Интернетом и безопасность в сфере использования ИКТ: Ключевые вызовы для мирового сообщества - Москва: Альпина Паблишер, 2016.

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.
4	«Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», утверждена Президентом РФ 12.12.2014 № К 1274.
5	Информационное сообщение ФСТЭК России №240/25/3752 от 24.08.2018 «По вопросам представления перечней объектов КИИ, подлежащих категорированию, и направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий».

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

№ п/п	Источник
6	Электронно-библиотечная система «Университетская библиотека online (доступ осуществляется по адресу: https://biblioclub.ru/);
4	Информационно-телекоммуникационная система «Контекстум» (Национальный цифровой ресурс «РУКОНТ»);
8	Электронно-библиотечной системе «Лань» (доступ осуществляется по адресу: https://e.lanbook.com/),
9	ЭБС «BOOK» (доступ осуществляется по адресу: https://book.ru).
10	Электронный каталог Научной библиотеки Воронежского государственного университета. – Режим доступа: http//:www.lib.vsu.ru.
11	Б1.В.07 Кибербезопасность критических систем и инфраструктур (10.05.01 БКСиС)/Сафронов В.В. - Образовательный портал «Электронный университет ВГУ».

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.07 Кибербезопасность критических систем и инфраструктур (10.05.01 БКСиС)», размещенный на платформе Электронного университета ВГУ (LMS moodle), а также Интернет-ресурсы, приведенные в п.15 в.11.

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).

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	Проблематика защиты критической информационной инфраструктуры и правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры Правила категорирования объектов КИИ.	ПК-2 ПК-3	ПК-2.5 ПК-3.3	устный опрос, тест, лабораторная работа
2	Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Проблематика защиты критической информационной инфраструктуры и правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры	ПК-2 ПК-3	ПК-2.5 ПК-3.3 ПК-3.5	устный опрос, тест, лабораторная работа
3	Правила категорирования объектов КИИ. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры	ПК-2 ПК-3	ПК-2.5 ПК-3.3	устный опрос, тест, лабораторная работа
4	Проблематика защиты критической информационной инфраструктуры и правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры	ПК-2 ПК-3	ПК-2.5 ПК-3.5	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	Проблематика защиты критической информационной инфраструктуры и правовое регулирование отношений в области обеспечения безопасности критической	Лабораторная работа 1. Подготовка сведений об организации. Лабораторная работа 2. Создание комиссии по категорированию.

	информационной инфраструктуры	
2	Правила категорирования объектов КИИ.	Лабораторная работа 3. Формирование перечня объектов КИИ. Лабораторная работа 4. Категорирование объектов КИИ.
3	Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры	Лабораторная работа 5. Анализ возможных действий нарушителей в отношении объектов критической информационной инфраструктуры
4	Обеспечение внутреннего контроля и эксплуатации значимых объектов КИИ	Лабораторная работа 6. Выбор средств защиты информации для нейтрализации угроз безопасности информации. Лабораторная работа 7. Разработка ОРД ЗОКИИ

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. Информация, характеристики безопасности информации.
2. Информация как объект правовых отношений.
3. Обладатель информации и оператор информационной системы: их права и обязанности.
4. Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации, положения кодекса об административных правонарушениях и уголовного кодекса.
5. Информационная инфраструктура России.
6. Понятие критической информационной инфраструктуры (КИИ).
7. В какие сферы деятельности входят значимые объекты КИИ?
8. Задачи ФСТЭК России в сфере безопасности информации и объектов КИИ.
9. Задачи ФСБ России в сфере безопасности информации и объектов КИИ.
10. Какие основные НПА в сфере безопасности значимых объектов КИИ
11. Определение относимости организации к субъекту КИИ.
12. Выделение критических процессов.
13. Подготовка реестра КИИ для направления во ФСТЭК.
14. Расскажите алгоритм категорирования объектов КИИ.
15. Как определяются критерии значимости объектов КИИ РФ и их значения?
16. Какие сведения об объектах КИИ необходимо направлять во ФСТЭК России.
17. Какие сведения об объектах КИИ необходимо направлять в ФСБ России.
18. Что из себя представляет и зачем нужна госСОПКА?
19. Зачем необходимо направлять информацию в госСОПКУ?
20. Цели и задачи НКЦКИ.
21. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры.
22. Организационные и технические меры по обеспечению безопасности значимого объекта КИИ.

23. Порядок аттестации значимых объектов КИИ.
24. Аудит информационной безопасности.
25. Мероприятия по реагированию на компьютерные инциденты и меры по ликвидации последствий компьютерных атак.
26. Обеспечение безопасности значимых объектов КИИ в ходе их эксплуатации.
27. Обеспечение безопасности значимых объектов КИИ при выводе их из эксплуатации.
28. Подключение объектов КИИ к госСОПКА.
29. Каковы составляющие российской системы обеспечения безопасности критических информационных систем от компьютерных атак?
30. Каковы функции участников реализации системы обеспечения безопасности критических информационных систем от компьютерных атак?
31. Как определить критические процессы на предприятии (в организации).
32. Критерии отнесения информационных систем к объектам КИИ.
33. Требования приказов ФСТЭК в отношении КИИ.
34. Требования приказов ФСБ в отношении КИИ.
35. Взаимодействие с госСОПКА.
36. Подготовка организационно-распорядительной документации по категорированию значимых объектов КИИ.

Критерии оценки ответов на вопросы экзамена

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». Приэтом, 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 На основании каких факторов кибербезопасность в настоящее время рассматривается как часть ESG?

- Социальная инженерия

- Нехватка специалистов в области кибербезопасности
- **Атаки на КИИ**
- Модель “кибератаки как услуга”

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

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

3 Продолжите утверждение: главный постулат DATA-DRIVEN состоит в том, что решения нужно принимать, опираясь на…

- **Анализ данных, а не интуицию и личный опыт**
- Результаты анализа AI
- Усредненную экспертную оценку
- Результаты статистических исследований

4 Какие предпосылки возникновения Центра операций по безопасности (Security Operation Center – SOC) являются ключевыми? Выберите все правильные ответы.

- **Непрерывность**
- **Оперативность**
- **Технологичность**
- Реактивность
- Доступность
- Универсальность

5 На какой класс SOC по локализации функций следует ориентироваться компании для развертывания SOC в течение нескольких месяцев?

- Внутренний
- **Внешний**
- Гибридный
- Любой из вышеперечисленных

6 Какую модель рекомендуется использовать при реагировании на инциденты кибербезопасности?

- ITIL
- COBIT
- **Cyber Kill-Chain**
- TIP

7 Из каких компонентов состоит UseCase?

- **Правила детектирования.**
- **PlayBook**
- **Описание дизайна кибератаки**
- Отчет по расследованию киберинцидента
- Текущая статистика по киберинцидентам
- Политика учетных записей

8 Какие технологии обязательно должны присутствовать в SOC базового уровня? Выберите все правильные ответы.

- **SIEM**
- Платформа Threat Intelligence
- Business intelligence
- **Система электронных заявок**
- Управление уязвимостями
- SOAR

9 Что понимается под управлением уязвимостями?

- Управление обновлениями программного обеспечения
- **Выявление, оценка, устранение уязвимостей безопасности в информационных системах и составление отчетов**

- Выявление, оценка, устранение уязвимостей безопасности в программном коде на всех этапах разработки
- Исследование и оценка методов эксплуатации уязвимостей хакерскими группами

10 Какая из перечисленных моделей применяется для описания хакерских группировок?
- Kill Chain
- MITRE ATT&CK
- **Diamond Model**
- OWASP Top 10

11 К какой категории информации CTI следует отнести сведения о техниках атаки?
- Технической
- **Тактической**
- Операционной
- Стратегической

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

1. Какие атаки предпринимают хакеры на программном уровне?

1) атаки на уровне ОС

2) атаки на уровне сетевого ПО

3) атаки на уровне пакетов прикладных программ

4) атаки на уровне СУБД

2. Из каких компонентов состоит программное обеспечение любой универсальной компьютерной системы?

1) операционной системы, сетевого программного обеспечения

2) операционной системы, сетевого программного обеспечения и системы управления базами данных;

3) операционной системы, системы управления базами данных;

4) сетевого программного обеспечения и системы управления базами данных.

3. Комплекс мер и средств, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов угроз безопасности объектам защиты называется

1) системой угроз;

2) системой защиты;

3) системой безопасности;

4) системой уничтожения.

4. Информационно-техническое воздействие – это…

А) применение способов и средств информационного воздействия на базы данных противника.

Б) применение способов и средств информационного воздействия на программно-аппаратные средства противника.

В) применение способов и средств информационного воздействия на информационно-технические объекты страны, на технику и вооружение противника в интересах достижения поставленных целей.

5. Информационно-психологическое воздействие – это…

А) использование информации, подготовленной соответствующим образом и воздействующей на индивидуальное и общественное сознание объекта (групп объектов) с помощью различных форм психологического внедрения.

Б) использование информации для подавления психологического сознание объекта (групп объектов).

В) применение способов и средств информационного воздействия на вооруженные силы противника в интересах достижения поставленных целей.

6. Манипуляция – это…

А) психологическое воздействие с использование информации, исполнение которого ведет к скрытому возбуждению у человека или групп людей намерений, не совпадающих с их актуальными существующими поведениями.

Б) использование информации для подавления психологического сознание объекта (групп объектов).

В) применение способов и средств информационного воздействия на общественное сознание в интересах достижения поставленных целей.

7. Как подразделяются вирусы в зависимости от деструктивных возможностей?

1) Сетевые, файловые, загрузочные, комбинированные

2) Безвредные, неопасные, опасные, очень опасные

3) Резидентные, нерезидентные

4) Полиморфные, макровирусы, вирусы-невидимки, "паразитические", "студенческие", "черви", компаньон-вирусы

8. Нежелательная цепочка носителей информации, один или несколько из которых являются правонарушителем или его специальной аппаратурой называется

Запишите ответ: _____

Верный ответ: "каналом утечки информации".

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

A. Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования

B. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

C. Улучшить контроль за безопасностью этой информации +

D. Снизить уровень классификации этой информации

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

A. Владельцы данных

B. Пользователи

C. Администраторы

D. Руководство +

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

A. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски +

B. Когда риски не могут быть приняты во внимание по политическим соображениям

C. Когда необходимые защитные меры слишком сложны

D. Когда стоимость контрмер превышает ценность актива и потенциальные потери

4. Что такое политики безопасности?

A. Пошаговые инструкции по выполнению задач безопасности

B. Общие руководящие требования по достижению определенного уровня безопасности +

C. Широкие, высокоуровневые заявления руководства

D. Детализированные документы по обработке инцидентов безопасности

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

A. Анализ рисков

B. Анализ затрат / выгоды +

C. Результаты ALE

D. Выявление уязвимостей и угроз, являющихся причиной риска

6. Эффективная программа безопасности требует сбалансированного применения:

A. Технических и нетехнических методов

B. Контрмер и защитных механизмов

C. Физической безопасности и технических средств защиты +

D. Процедур безопасности и шифрования

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

A. Внедрение управления механизмами безопасности+

B. Классификацию данных после внедрения механизмов безопасности

C. Уровень доверия, обеспечиваемый механизмом безопасности

D. Соотношение затрат / выгод +

8. Что из перечисленного не является целью проведения анализа рисков?

A. Делегирование полномочий +

B. Количественная оценка воздействия потенциальных угроз

C. Выявление рисков

D. Определение баланса между воздействием риска и стоимостью необходимых контрмер

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