Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Анатольевна
Должность: Ректор
Дата подписания: 30.10.2026 13:32:53
Уникальный программный ключ:
c3b3b9c625f6c113afa2a2c42baff9e05a38b76e

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования «Поволжский государственный университет сервиса» (ФГБОУ ВО «ПВГУС»)

УТВЕРЖДЕНО

на заседании Ученого совета Высшей школы интеллектуальных систем и кибертехнологий

Протокол от 23. 05. 2025 № 10

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
(фонд оценочных средств) для проведения промежуточной аттестации по дисциплине

«Кибербезопасность»
наименование дисциплины

по образовательной программе высшего образования – программе **бакалавриата**
бакалавриата, специалитета, магистратуры

«Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)»
наименование образовательной программы

10.03.01 «Информационная безопасность»
шифр, наименование направления подготовки / специальности

Составитель Мунирова Ю.С.,
старший преподаватель Высшей школы интеллектуальных систем и кибертехнологий
ФИО, должность, структурное подразделение, ученая степень, ученое звание

Тольятти
2026

1. Паспорт фонда оценочных средств (далее – ФОС)

1.1. Планируемые результаты обучения по дисциплине

Код компетенции	Наименование компетенции	Код и наименование индикаторов достижения компетенции
УК-1.	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	ИУК-1.1. Осуществляет поиск, анализирует и обрабатывает научно-техническую информацию в ИТ-сфере, в том числе в области кибербезопасности
ПК-2.	Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	ИПК-2.1. Противодействует угрозам безопасности информации с использованием встроенных средств защиты информации
ПК-3.	Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно- аппаратных и технических средств защиты информации	ИПК-3.1. Оценивает работоспособность применяемых средств защиты информации с использованием штатных средств и методик

В результате изучения дисциплины обучающийся должен:

Знает:

основные источники научно-технической информации в области кибербезопасности;
методы поиска, критического анализа и систематизации информации по вопросам защиты информации
состав, назначение и принципы функционирования программных средств защиты информации (антивирусное ПО, средства криптографической защиты, межсетевые экраны, системы обнаружения вторжений)
состав, назначение и принципы функционирования аппаратных средств защиты информации (аппаратные модули доверенной загрузки, токены, аппаратные межсетевые экраны, СКЗИ)

Умеет:

находить, анализировать и обрабатывать научно-техническую информацию в ИТ-сфере при решении задач обеспечения кибербезопасности
инсталлировать и тестировать программные средства защиты информации, оценивать корректность их настройки и работы

инсталлировать и тестировать аппаратные средства защиты информации, оценивать корректность их настройки и работы

Владеет:

навыками системного поиска и критической оценки научно-технической информации в области кибербезопасности

навыками использования программных средств защиты информации для решения задач профессиональной деятельности

навыками использования аппаратных средств защиты информации для решения задач профессиональной деятельности

1.2. Содержание дисциплины

№	Тема (раздел дисциплины)	Код компетенции
1	Тема 1. Основы кибербезопасности: понятия, цели и задачи	УК-1
2	Тема 2. Угрозы информационной безопасности и модель нарушителя	УК-1
3	Тема 3. Вредоносное программное обеспечение и антивирусная защита	ПК-2
4	Тема 4. Криптографические методы защиты информации	ПК-2
5	Тема 5. Сетевая безопасность: межсетевые экраны, VPN, IDS/IPS	ПК-3
6	Тема 6. Идентификация, аутентификация и управление доступом	ПК-2 ПК-3
7	Тема 7. Тестирование и эксплуатация программных и аппаратных средств защиты информации	ПК-2 ПК-3
8	Тема 8. Нормативно-правовое обеспечение кибербезопасности и управление инцидентами	УК-1 ПК-2 ПК-3

1.3. Система оценивания по дисциплине

Дисциплина изучается в течение одного семестра

Форма промежуточной аттестации – экзамен.

Шкала оценки уровня сформированности компетенций		Шкала оценки уровня освоения дисциплины	
Уровневая шкала оценки компетенций	100 балльная шкала, %	100 балльная шкала, %	недифференцированная оценка
Допороговый	ниже 61	ниже 61	не зачтено
Пороговый	61-85,9	61-69,9	зачтено
		70-85,9	зачтено
Повышенный	86-100	86-100	зачтено

2. Перечень оценочных материалов для проведения промежуточной аттестации

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в ходе текущего контроля успеваемости (в процессе проведения практических занятий, лабораторных работ, тестирования, опросов).

В ходе проведения экзамена осуществляется итоговый контроль и оценка результатов освоения компетенций.

Вопросы для подготовки к экзамену

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач

1. Понятие кибербезопасности, информационной безопасности и защиты информации, их соотношение.
2. Цели, задачи и объекты обеспечения кибербезопасности.
3. Классификация угроз информационной безопасности.
4. Источники и каналы утечки информации.
5. Модель нарушителя и модель угроз информационной безопасности.
6. Нормативно-правовые акты Российской Федерации в области защиты информации (ФЗ-149, ФЗ-152, приказы ФСТЭК и ФСБ России).
7. Международные и национальные стандарты информационной безопасности (ISO/IEC 27001, ГОСТ Р ИСО/МЭК 27001).
8. Организация реагирования на инциденты информационной безопасности.
9. Методика поиска и критического анализа научно-технической информации в области кибербезопасности.

ПК-2. Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач

1. Классификация вредоносного программного обеспечения.
2. Механизмы распространения и заражения вредоносным программным обеспечением.
3. Принципы работы и виды антивирусных программных средств защиты информации.
4. Порядок инсталляции и тестирования антивирусных программных средств защиты информации.
5. Симметричные криптографические алгоритмы: назначение и область применения.
6. Асимметричные криптографические алгоритмы: назначение и область применения.
7. Электронная подпись и хеширование: назначение, принципы функционирования.
8. Отечественные средства криптографической защиты информации (СКЗИ).
9. Программные межсетевые экраны: назначение, порядок инсталляции и тестирования.
10. Программные средства идентификации и аутентификации пользователей.
11. Методика тестирования программных средств защиты информации и оценки эффективности их функционирования.

ПК-3. Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно- аппаратных и технических средств защиты информации

1. Архитектура защищенных сетей: основные принципы построения.

2. Аппаратные межсетевые экраны: назначение, классификация, порядок инсталляции и тестирования.

3. Технологии VPN: назначение и принципы функционирования.

4. Системы обнаружения и предотвращения вторжений (IDS/IPS).

5. Аппаратные средства аутентификации (токены, смарт-карты): инсталляция и тестирование.

6. Модели разграничения доступа: дискреционная, мандатная, ролевая.

7. Методика тестирования аппаратных средств защиты информации и оценки эффективности их функционирования.

8. Порядок эксплуатации и сопровождения программных и аппаратных средств защиты информации.

Примерный тест для итогового тестирования

Правильный вариант ответа выделен полужирным шрифтом с подчеркиванием.

1. Кибербезопасность направлена прежде всего на обеспечение

А) конфиденциальности, целостности и доступности информации в компьютерных системах и сетях

Б) только конфиденциальности информации

В) только физической сохранности носителей информации

Г) только бесперебойной работы оборудования

2. Модель нарушителя описывает

А) предполагаемые возможности, мотивацию и уровень доступа лица, способного реализовать угрозу

Б) перечень технических средств защиты информации

В) структуру службы информационной безопасности организации

Г) порядок резервного копирования данных

3. Вирус, троян, червь и шифровальщик являются разновидностями

А) вредоносного программного обеспечения

Б) средств криптографической защиты информации

В) систем обнаружения вторжений

Г) аппаратных модулей доверенной загрузки

4. Основное назначение антивирусного программного средства защиты информации

А) обнаружение, блокирование и удаление вредоносного программного обеспечения

Б) шифрование сетевого трафика

В) разграничение прав доступа к файловой системе

Г) резервное копирование данных

5. К симметричным криптографическим алгоритмам относится

А) ГОСТ 28147-89 (Магма)

Б) RSA

В) алгоритм Диффи – Хеллмана

Г) ГОСТ Р 34.10-2018

6. Асимметричное шифрование, в отличие от симметричного, использует

А) пару ключей – открытый и закрытый

Б) один и тот же ключ для шифрования и расшифрования

В) только хеш-функции без ключей

Г) исключительно аппаратные средства

7. Электронная подпись обеспечивает

А) подтверждение авторства и целостности электронного документа

Б) ускорение передачи данных по сети

В) сжатие объема хранимой информации

Г) автоматическое резервное копирование

8. СКЗИ – это средства

А) криптографической защиты информации

Б) контроля физического доступа в помещение

В) видеонаблюдения

Г) кадрового делопроизводства

9. Межсетевой экран (файрвол) предназначен для

А) фильтрации сетевого трафика в соответствии с заданными правилами безопасности

Б) хранения резервных копий данных

В) проверки орфографии в документах

Г) управления кадровым составом организации

10. Технология VPN обеспечивает

А) создание защищенного (шифрованного) канала передачи данных поверх открытой сети

Б) ускорение работы процессора

В) автоматическое обновление операционной системы

Г) визуализацию сетевого трафика

11. Система обнаружения вторжений (IDS) в отличие от системы предотвращения вторжений (IPS)

А) только выявляет и сигнализирует о подозрительной активности, не блокируя ее автоматически

Б) всегда блокирует любую сетевую активность

В) устанавливается исключительно на аппаратном уровне

Г) не требует настройки правил

12. Аппаратный токен применяется для

А) аппаратной аутентификации пользователя

Б) увеличения объема оперативной памяти

В) охлаждения серверного оборудования

Г) печати документов

13. Дискреционная модель разграничения доступа предполагает, что

А) владелец ресурса самостоятельно определяет права доступа других субъектов к этому ресурсу

Б) права доступа определяются исключительно меткой секретности

В) доступ предоставляется на основании должностной роли пользователя

Г) доступ к ресурсу невозможно ограничить

14. Мандатная модель разграничения доступа основана на

А) сопоставлении меток конфиденциальности субъекта и объекта доступа

Б) решении владельца ресурса

В) случайном распределении прав доступа

Г) исключительно биометрических данных пользователя

15. Ролевая модель разграничения доступа (RBAC) назначает права доступа на основании

А) роли (должностной функции) пользователя в организации

Б) времени суток

В) географического местоположения пользователя

Г) объема оперативной памяти компьютера пользователя

16. Федеральный закон № 149-ФЗ регулирует отношения в области

А) информации, информационных технологий и защиты информации

Б) персональных данных исключительно медицинских учреждений

В) государственной тайны

Г) бухгалтерского учета

17. Федеральный закон № 152-ФЗ регулирует отношения в области

А) обработки и защиты персональных данных

Б) защиты государственной тайны

В) лицензирования образовательной деятельности

Г) антимонопольного регулирования

18. Стандарт ГОСТ Р ИСО/МЭК 27001 устанавливает требования к

А) системе менеджмента информационной безопасности организации

Б) бухгалтерской отчетности предприятия

В) качеству печатной продукции

Г) охране труда на производстве

19. Реагирование на инцидент информационной безопасности начинается с этапа

А) обнаружения и регистрации инцидента

Б) уничтожения всех журналов событий

В) увольнения ответственного сотрудника

Г) отключения всей организации от сети Интернет

20. Оценка эффективности функционирования средства защиты информации проводится с целью

А) подтверждения соответствия его работы установленным требованиям безопасности

Б) увеличения стоимости средства защиты

В) сокращения штата специалистов по информационной безопасности

Г) изменения дизайна пользовательского интерфейса