Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 30.10.2026 13:32:54
Уникальный программный ключ:
c3b3b9c625f6c113afa2a2c42ba...

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

УТВЕРЖДЕНО

на заседании Высшей школы интеллектуальных систем и кибертехнологий

Протокол от 10.11.2023 № 3

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

Б1.В.ДВ.01.2 «Мониторинг информационной безопасности»
наименование дисциплины

по образовательной программе высшего образования – программе **бакалавриат**

«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

Составители Коновалова Анжелика Денисовна, старший преподаватель, Высшая школа интеллектуальных систем и кибертехнологий
ФИО, должность, структурное подразделение, ученая степень, ученое звание

Тольятти
2023

1. Паспорт фонда оценочных средств (далее – ФОС)

1.1. Планируемые результаты обучения по дисциплине

Код компетенции	Наименование компетенции	Код и наименование индикаторов достижения компетенции
ПК-7	Способен организовать, поддерживать и управлять процессом защиты информации автоматизированных систем в соответствии с требованиями нормативной правовой и организационно-методической документации	ИПК-7.1. Принимает участие в организации, поддержании в актуальном состоянии процесса защиты информации автоматизированных систем и совершенствовании системы управления защиты информации автоматизированных систем ИПК-7.2. Организует работу (содержание и порядок) деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации. ИПК-7.3. Осуществляет управление процессом защиты информации автоматизированных систем в соответствии с требованиями нормативной правовой и организационно-методической документации по защите информации ИПК-7.4. Осуществляет разработку, внедрение и контроль реализации правил и процедур управления системой защиты информации, работы с угрозами, инцидентами, автоматизированными системами и системами защиты информации

В результате изучения дисциплины обучающийся должен:

владеть: навыками составления программы мониторинга, паспорта источника и матрицы ответственности; анализа учебных журналов и подтверждения выводов исходными событиями; ведения карточки события и хронологии; проверки правил на контрольной выборке; подготовки отчета, показателей качества и плана улучшения процесса защиты информации

уметь: определять границы мониторинга и необходимые источники данных; организовывать сбор, нормализацию и анализ событий; проверять работоспособность средств мониторинга; распределять обязанности и порядок эскалации; обосновывать приоритеты обработки, разрабатывать регламент и правила обнаружения, оценивать их результаты и корректировать процедуры

знать: назначение и этапы мониторинга информационной безопасности, виды источников событий, требования к качеству и защите данных мониторинга; порядок распределения функций персонала, контроля функционирования системы защиты и документирования результатов; принципы разработки и проверки правил обнаружения, обработки событий и совершенствования мониторинга

1.2. Содержание дисциплины

№	Тема (раздел дисциплины) (в соответствии с РПД)	Код компетенции
1	Назначение, нормативные основы и организация мониторинга	ПК-7
2	Источники событий и организация сбора данных	ПК-7
3	Нормализация, хранение и защита данных мониторинга	ПК-7
4	Анализ и корреляция событий безопасности	ПК-7
5	Контроль защищенности и функционирования средств защиты	ПК-7
6	Обработка оповещений и взаимодействие при инцидентах	ПК-7
7	Регламенты, роли персонала и эксплуатация мониторинга	ПК-7
8	Оценка качества мониторинга и совершенствование процесса защиты	ПК-7

1.3. Система оценивания по дисциплине

Дисциплина изучается в течении одного семестра.

Форма промежуточной аттестации по дисциплине: зачет

Уровень сформированности	100-балльная шкала, %	Шкала освоения, %	5-балльная дифференцированная оценка/балл
допороговый	ниже 61	ниже 61	не зачтено
пороговый	61–85,9	61–69,9	зачтено
пороговый	61–85,9	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: практических занятий, тестирования, опросов, проверки самостоятельной работы.

В ходе проведения промежуточной аттестации осуществляется контроль и оценка результатов освоения компетенций.

Перечень вопросов и заданий для подготовки к зачету

ПК-7. Способен организовать, поддерживать и управлять процессом защиты информации автоматизированных систем в соответствии с требованиями нормативной правовой и организационно-методической документации

1. Назначение мониторинга информационной безопасности и его связь с процессом защиты информации.
2. Событие, оповещение, признак нарушения и инцидент: различия и примеры.
3. Границы мониторинга, критичные активы и критерии приоритизации источников.
4. Нормативные и локальные основания мониторинга. Область применения ГОСТ Р 59547-2021.
5. Состав программы мониторинга и порядок ее согласования.
6. Основания пересмотра программы при изменении системы и угроз.
7. Источники событий безопасности и их аналитическая ценность.
8. Агентский и безагентский сбор: условия выбора и ограничения.
9. Паспорт источника и порядок его подключения.
10. Время события и приема, часовые пояса и синхронизация часов.
11. Контроль потерь, дублей и задержек доставки.
12. Действия персонала при прекращении поступления событий.
13. Единая схема события и сопоставление полей разных источников.
14. Обработка неизвестных значений и ошибок нормализации.
15. Фильтрация, дедупликация и агрегирование: назначение и риски потери данных.
16. Расчет емкости хранилища и факторы, изменяющие итоговый объем.
17. Выбор сроков хранения, разграничение доступа и контроль целостности журналов.
18. Сохранение исходного сообщения и воспроизводимость анализа.

19. Аналитическая гипотеза и сценарий обнаружения.

20. Пороговые и последовательностные правила корреляции.

21. Временное окно и ключ группировки событий.

22. Контекст актива, пользователя и согласованных работ при анализе.

23. Ложноположительные и ложноотрицательные результаты и способы их исследования.

24. Состав карточки правила, тестирование и контроль версий.

25. Контроль работоспособности и результативности средств защиты.

26. Оценка покрытия активов и источников мониторингом.

27. Использование сведений об уязвимостях и угрозах при анализе защищенности.

28. Приоритизация отклонений состояния защиты.

29. Состав записи о несоответствии и плана корректирующих действий.

30. Повторная проверка и критерии закрытия замечаний.

31. Первичная проверка оповещения и регистрация случая.

32. Построение хронологии и разграничение фактов и гипотез.

33. Оценка приоритета и критерии эскалации.

34. Сохранение свидетельств и контроль доступа к материалам случая.

35. Полномочия аналитика и взаимодействие с ответственным за реагирование.

36. Подтверждение, отклонение и закрытие случая с обратной связью в мониторинг.

37. Роли участников мониторинга и разделение обязанностей.

38. Структура регламента мониторинга и контроль его исполнения.

39. Передача смены, замещение и учет незавершенных случаев.

40. Управление изменениями источников и правил обнаружения.

41. Плановое обслуживание платформы и компенсация потери наблюдения.

42. Взаимодействие с внешним исполнителем и защита передаваемых данных.

43. Показатели качества сбора и нормализации событий.

44. Точность и полнота обнаружения: расчет и ограничения.

45. Средняя и медианная задержка, точки начала и окончания измерения.

46. Контрольные сценарии и критерии приемки мониторинга.

47. Структура отчета о мониторинге и представление выводов руководству.

48. План совершенствования процесса защиты и проверка результата улучшений.