Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 30.10.2026 13:36:03
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»)»

Высшая школа интеллектуальных систем и кибертехнологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.01.2 «МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки:
10.03.01 «Информационная безопасность»

Направленность (профиль):
«Организация и технологии защиты информации
(по отрасли или в сфере профессиональной деятельности)»

Квалификация выпускника: **бакалавр**

Тольятти 2023

Рабочая программа дисциплины «Мониторинг информационной безопасности» разработана в соответствии с федеральным государственным образовательным стандартом высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность, утвержденным приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. № 1427.

Составители:

старший преподаватель	Коновалова А.Д.
(ученая степень, ученое звание)	(ФИО)

РПД обсуждена на заседании Высшей школы интеллектуальных систем и кибертехнологий

10.11.2023 г., протокол № 3

	к.э.н., доцент	Филиппова О.А.
Директор ВШИСиКТ	(уч.степень, уч.звание)	(ФИО)

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Цель освоения дисциплины

Целью освоения дисциплины является:

- формирование способности организовывать и поддерживать мониторинг информационной безопасности автоматизированных систем, анализировать его результаты и совершенствовать процесс защиты информации на основе нормативных требований и проверяемых данных.

1.2. Перечень планируемых результатов обучения по дисциплине

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения по дисциплине**	**Основание (ПС)** *для профессиональных компетенций
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	**Знает:** 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 **Умеет:** 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 **Владеет:** 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	06.033 «Специалист по защите информации в автоматизированных системах».

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине	Основание (ПС) *для профессиональных компетенций
	защиты информации, работы с угрозами, инцидентами, автоматизированными системами и системами защиты информации		

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина относится к части, формируемой участниками образовательных отношений, Блока 1. Дисциплины (модули) образовательной программы и является элективной дисциплиной, углубляющей освоение профиля (Дисциплины по выбору).

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1. Объем и структура дисциплины

Общая трудоёмкость дисциплины составляет **3 з.е. (108 час.)**, их распределение по видам работ и семестрам представлено в таблице.

Виды учебных занятий и работы обучающихся	Трудоемкость, час
Общая трудоемкость дисциплины, час	**108**
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего), в т.ч.:	**86/52**
занятия лекционного типа (лекции)	40/20
занятия семинарского типа (семинары, практические занятия, практикумы, коллоквиумы и иные аналогичные занятия)	46/32
Лабораторные работы	0/0
Самостоятельная работа всего, в т.ч.:	**22/52**
Самоподготовка по темам (разделам) дисциплины	22/52
Контроль (часы на зачет)	**0/4**
Промежуточная аттестация	**Зачёт**

Примечание: -/- объем часов соответственно для очной, очно-заочной форм обучения.

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

В процессе освоения дисциплины может применяться электронное обучение и дистанционные образовательные технологии.

В процессе освоения дисциплины обучающиеся обеспечены доступом к электронной информационно-образовательной среде и электронно-библиотечным системам.

3.2. Содержание дисциплины, структурированное по темам

Планируемые результаты освоения: код формируемой компетенции и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы				Формы текущего контроля (наименование оценочного средства)
		Контактная работа			Самостоятельная работа, час	
		Лекции, час	Лабораторные работы, час	Практические занятия, час		
ПК-7 ИПК-7.1 ИПК-7.3	**ТЕМА 1. НАЗНАЧЕНИЕ, НОРМАТИВНЫЕ ОСНОВЫ И ОРГАНИЗАЦИЯ МОНИТОРИНГА** Содержание лекции: Мониторинг как систематическое наблюдение и анализ состояния безопасности информации. Различие события, признака нарушения, оповещения и подтвержденного инцидента. Цели мониторинга: выявление отклонений, контроль выполнения правил защиты, оценка функционирования средств и актуализация защитных мер. Связь мониторинга с управлением рисками, аудитом и реагированием. Объекты наблюдения: активы, процессы, пользователи, каналы взаимодействия и средства защиты. Нормативные и организационно-методические основания. Назначение и область применения ГОСТ Р 59547-2021; разграничение требований к мониторингу и процедур управления инцидентами. Установление границ наблюдения, владельцев активов и критериев критичности. Программа мониторинга: цели, источники, периодичность контроля, ответственные, отчетность. Принципы достаточности данных и проверяемости выводов. Порядок согласования программы с владельцем системы и пересмотра при изменениях инфраструктуры.	4/2	-	-	-	Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по теме лекционного занятия
	Практическая работа 1. Разработка программы мониторинга учебной информационной системы.	-	-	4/4	-	Отчёт по практической работе
	Самостоятельная работа.	-	-	-	2/6	Самостоятельное изучение учебных материалов
ПК-7 ИПК-7.1 ИПК-7.2 ИПК-7.4	**ТЕМА 2. ИСТОЧНИКИ СОБЫТИЙ И ОРГАНИЗАЦИЯ СБОРА ДАННЫХ** Содержание лекции: Источники данных: операционные системы, службы каталогов, приложения, сетевое оборудование и средства защиты. События аутентификации, изменения прав и конфигураций, обращения к ресурсам, состояния защитных компонентов. Агентский и безагентский сбор. Централизованная доставка, буферизация и очереди; контроль потерь, повторов и задержек. Время события, время приема и часовой пояс; синхронизация часов и обработка расхождений. Идентификаторы узла, пользователя, сеанса и источника. Паспорт источника: владелец, состав полей, формат, объем, режим передачи и критерии работоспособности. Учет отказа самого источника и канала доставки. Приоритизация подключения по значимости актива и ценности сведений. Минимальные права сборщика, защищенная	6/3	-	-	-	Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по теме лекционного занятия

Планируемые результаты освоения: код формируемой компетенции и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы				Формы текущего контроля (наименование оценочного средства)
		Контактная работа			Самостоятельная работа, час	
		Лекции, час	Лабораторные работы, час	Практические занятия, час		
	передача и учет технических учетных записей. Организация сопровождения источников и уведомление об изменениях формата. Проверка цепочки от возникновения события до его доступности аналитику.					
	Практическая работа 2. Паспортизация источников и проверка полноты доставки событий.	-	-	6/4	-	Отчёт по практической работе
	Самостоятельная работа.	-	-	-	3/6	Самостоятельное изучение учебных материалов
ПК-7 ИПК-7.1 ИПК-7.3 ИПК-7.4	**ТЕМА 3. НОРМАЛИЗАЦИЯ, ХРАНЕНИЕ И ЗАЩИТА ДАННЫХ МОНИТОРИНГА** Содержание лекции: Сырой журнал и нормализованное представление. Единая схема события: время, источник, субъект, объект, действие, результат и контекст. Сопоставление имен полей и справочников, обработка пустых и неоднозначных значений. Правила сохранения исходного сообщения. Фильтрация, дедупликация и агрегирование; риск потери значимых признаков. Контроль ошибок разбора и учет версии преобразования. Оперативное и архивное хранение, поиск и выгрузка. Оценка емкости по частоте и размеру событий, пиковая нагрузка и резерв. Выбор срока хранения по применимым требованиям и задачам, а не по универсальному числу. Разграничение доступа, защита от изменения и удаления, регистрация действий аналитиков. Журналы как источник конфиденциальных сведений и персональных данных. Минимизация содержимого, безопасная передача учебных выгрузок. Резервирование и проверка восстановления. Порядок воспроизведения результата анализа по сохраненным данным.	6/3	-	-	-	Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по теме лекционного занятия
	Практическая работа 3. Разработка схемы нормализации и политики хранения журналов.	-	-	6/4	-	Отчёт по практической работе
	Самостоятельная работа.	-	-	-	3/7	Самостоятельное изучение учебных материалов
ПК-7 ИПК-7.1 ИПК-7.4	**ТЕМА 4. АНАЛИЗ И КОРРЕЛЯЦИЯ СОБЫТИЙ БЕЗОПАСНОСТИ** Содержание лекции: Аналитическая гипотеза и проверяемый сценарий обнаружения. Поиск по полям, временным диапазонам и связанным сущностям. Базовый профиль активности и отклонение от него. Корреляция событий: последовательность, порог, временное окно и ключ группировки. Различие группировки по учетной записи, узлу и адресу; ограничения адреса как идентификатора. Контекст критичности актива, разрешенных работ и полномочий пользователя. Подтверждение гипотезы независимыми источниками и учет	6/3	-	-	-	Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по теме лекционного занятия

Планируемые результаты освоения: код формируемой компетенции и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы				Формы текущего контроля (наименование оценочного средства)
		Контактная работа			Самостоятельная работа, час	
		Лекции, час	Лабораторные работы, час	Практические занятия, час		
	неполноты наблюдения. Ложноположительные и ложноотрицательные результаты, дубли оповещений, приоритизация. Карточка правила: цель, предпосылки, источники, логика, исключения, приоритет, тесты и ответственный. Тестовая и проверочная выборки; контроль версий, согласование исключений и повторная проверка. Документирование границ применимости правила. Разграничение сигнала, аналитического вывода и установленного факта нарушения.					
	Практическая работа 4. Разработка и проверка правила корреляции.	-	-	6/4	-	Отчёт по практической работе
	Самостоятельная работа.	-	-	-	3/7	Самостоятельное изучение учебных материалов
ПК-7 ИПК-7.1 ИПК-7.3 ИПК-7.4	**ТЕМА 5. КОНТРОЛЬ ЗАЩИЩЕННОСТИ И ФУНКЦИОНИРОВАНИЯ СРЕДСТВ ЗАЩИТЫ** Содержание лекции: Мониторинг состояния защиты: работоспособность компонентов, обновление баз, конфигурация, покрытие активов и соблюдение политики. Различие установленного, работающего и результативного средства защиты. Источники подтверждения: состояние агента, журнал задания, контрольное событие и результаты проверки. Учет уязвимостей и изменений инфраструктуры как контекста мониторинга. Связь угрозы с активом, доступностью уязвимого компонента и защитными мерами. Ограничения автоматических оценок и необходимость проверки применимости. Приоритизация отклонений по критичности и возможным последствиям. Организация проверки на согласованном учебном стенде, критерии остановки и сохранения работоспособности. Регистрация несоответствия: факт, требование, свидетельство и риск. Контроль исполнения корректирующих действий, повторная проверка и закрытие. Обновление программы мониторинга по результатам анализа. Представление руководителю проверяемых выводов вместо перечня технических сообщений.	6/3	-	-	-	Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по теме лекционного занятия
	Практическая работа 5. Оценка покрытия активов и разработка плана устранения отклонений.	-	-	6/4	-	Отчёт по практической работе
	Самостоятельная работа.	-	-	-	3/7	Самостоятельное изучение учебных материалов
ПК-7 ИПК-7.2 ИПК-7.3 ИПК-7.4	**ТЕМА 6. ОБРАБОТКА ОПОВЕЩЕНИЙ И ВЗАИМОДЕЙСТВИЕ ПРИ ИНЦИДЕНТАХ** Содержание лекции: Первичная проверка оповещения: источник, время, полнота, достоверность и связанный актив. Регистрация случая, объединение дублей и	4/2	-	-	-	Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по теме лекционного

Планируемые результаты освоения: код формируемой компетенции и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы				Формы текущего контроля (наименование оценочного средства)
		Контактная работа			Самостоятельная работа, час	
		Лекции, час	Лабораторные работы, час	Практические занятия, час		
	построение хронологии. Оценка приоритета с учетом значимости актива и возможного воздействия. Разделение фактов, предположений и недостающих данных. Передача информации ответственным за реагирование; критерии эскалации, согласование действий и обратная связь. Сохранение исходных записей, контрольных сумм, сведений о выгрузке и условиях доступа. Ограничение полномочий аналитика: отсутствие автоматического права изменять рабочую систему. Подтверждение или отклонение гипотезы, документирование основания решения. Связь мониторинга с процедурами управления инцидентами, восстановления и последующего анализа. Требования к краткому сообщению руководителю и техническому приложению. Контроль сроков, передача незавершенных случаев между сменами, учет повторных обращений. Уточнение правил обнаружения по результатам разбора.					занятия
	Практическая работа 6. Первичный анализ оповещения и подготовка пакета эскалации.	-	-	6/4	-	Отчёт по практической работе
	Самостоятельная работа.	-	-	-	3/7	Самостоятельное изучение учебных материалов
ПК-7 ИПК-7.1 ИПК-7.2 ИПК-7.3 ИПК-7.4	**ТЕМА 7. РЕГЛАМЕНТЫ, РОЛИ ПЕРСОНАЛА И ЭКСПЛУАТАЦИЯ МОНИТОРИНГА** Содержание лекции: Организационная модель процесса мониторинга: владелец, аналитик, администратор платформы, владелец актива и ответственный за реагирование. Содержание полномочий и разделение обязанностей. Регламент работы: прием и проверка данных, анализ, регистрация, эскалация, отчетность и пересмотр. Планирование нагрузки и обеспечение непрерывности наблюдения. Передача смены, очереди незавершенных случаев, замещение и обучение персонала. Организация доступа к журналам и контроль привилегированных действий. Управление изменениями источников, правил и инфраструктуры; согласование, тестирование и возврат к предыдущей версии. План сопровождения: контроль времени, емкости, очередей, сертификатов и состояния сборщиков. Порядок обслуживания без скрытой потери наблюдения. Взаимодействие с внешним исполнителем и требования к передаваемым данным. Проверка исполнения регламента и контроль документации. Ответственность за актуальность перечней активов, источников и контактных лиц.	4/2	-	-	-	Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по теме лекционного занятия
	Практическая работа 7. Разработка регламента мониторинга и матрицы ответственности.	-	-	6/4	-	Отчёт по практической работе

Планируемые результаты освоения: код формируемой компетенции и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы				Формы текущего контроля (наименование оценочного средства)
		Контактная работа			Самостоятельная работа, час	
		Лекции, час	Лабораторные работы, час	Практические занятия, час		
	Самостоятельная работа.	-	-	-	3/6	Самостоятельное изучение учебных материалов
ПК-7 ИПК-7.1 ИПК-7.2 ИПК-7.3 ИПК-7.4	**ТЕМА 8. ОЦЕНКА КАЧЕСТВА МОНИТОРИНГА И СОВЕРШЕНСТВОВАНИЕ ПРОЦЕССА ЗАЩИТЫ** Содержание лекции: Показатели качества: покрытие активов и источников, полнота и задержка доставки, ошибки нормализации, доступность конвейера обработки. Метрики аналитики: подтвержденные и ложные срабатывания, пропущенные контрольные сценарии, время выявления и обработки. Определение начальной и конечной точки измерения; медиана, среднее и выбросы. Ограничения метрик при отсутствии полной информации об атаках. Сопоставление показателей с целями и критичностью активов; недопустимость улучшения показателя путем скрытого исключения сложных случаев. Проверочные наборы, воспроизводимость, критерии приемки и независимая проверка. Отчет о мониторинге: существенные отклонения, последствия, причины, корректирующие меры и остаточные ограничения. План улучшения: приоритет, ресурсы, владелец и измеримый результат. Проверка согласованности программы, источников, правил, регламента и отчетов. Итоговая защита проекта и демонстрация выполнения контрольного сценария.	4/2	-	-	-	Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по теме лекционного занятия
	Практическая работа 8. Оценка эффективности мониторинга и защита итогового проекта.	-	-	6/4	-	Отчёт по практической работе
	Самостоятельная работа.	-	-	-	2/6	Самостоятельное изучение учебных материалов
	ИТОГО	**40/20**	**0/0**	**46/32**	**22/52**	

Примечание: -/- объем часов соответственно для очной, очно-заочной форм обучения.

4. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

4.1. Общие методические рекомендации по освоению дисциплины, образовательные технологии

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

При проведении учебных занятий по дисциплине обеспечивается развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплины в форме курса, составленного на основе результатов научных исследований, проводимых университетом, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

- балльно-рейтинговая технология оценивания;
- электронное обучение;

Для оценки знаний, умений, навыков и уровня сформированности компетенции по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. В основу балльно-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего контроля успеваемости. Максимальное количество баллов в семестре – 100.

4.2. Методические указания для обучающихся по освоению дисциплины на занятиях лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов тематического плана. В ходе лекционных занятий раскрываются базовые вопросы в рамках каждой темы дисциплины. Обозначаются ключевые аспекты тем, а также делаются акценты на наиболее сложные и важные положения изучаемого материала.

Лекционные занятия проводятся в поточной аудитории с применением мультимедийного проектора в виде учебной презентации или в ЭИОС университета.

В ходе лекционных занятий рекомендуется конспектирование учебного материала. Возможно ведение конспекта лекций в виде интеллект-карт.

Отдельные темы предлагаются для самостоятельного изучения (конспектируются).

Материалы лекций являются опорной основой для подготовки обучающихся к практическим занятиям / лабораторным работам и выполнения заданий самостоятельной работы, а также к мероприятиям текущего контроля успеваемости и промежуточной аттестации по дисциплине.

4.4. Методические указания для обучающихся по освоению дисциплины на занятиях семинарского типа / на практических занятиях

Практические (семинарские) занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы. Основной формой проведения семинаров и практических занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение задач и разбор примеров и ситуаций в аудиторных условиях.

Практические (семинарские) занятия обучающихся обеспечивают:

- проверку и уточнение знаний, полученных на лекциях;

- получение умений и навыков составления докладов и сообщений, обсуждения вопросов по учебному материалу дисциплины;

- подведение итогов занятий по рейтинговой системе, согласно технологической карте дисциплины.

Практические занятия организуются, в том числе в форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

4.5. Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обеспечивает подготовку обучающегося к аудиторным занятиям и мероприятиям текущего контроля и промежуточной аттестации по изучаемой дисциплине. Результаты этой подготовки проявляются в активности обучающегося на занятиях и в качестве выполненных практических заданий и других форм текущего контроля.

Самостоятельная работа студентов включает:

1. Изучение учебной литературы по курсу.
2. Работу с ресурсами Интернет
3. Самостоятельное изучение учебных материалов

При выполнении заданий для самостоятельной работы рекомендуется проработка материалов лекций по каждой пройденной теме, а также изучение рекомендуемой литературы.

Для обучающихся по заочной форме обучения самостоятельная работа является основным видом учебной деятельности.

Для обеспечения самостоятельной работы обучающихся используется электронный учебный курс, созданный в ЭИОС университета http://sdo.tolgas.ru/.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Вся литература, включенная в данный перечень, представлена в виде электронных ресурсов в электронной библиотеке университета (ЭБС). Литература, используемая в печатном виде, представлена в научной библиотеке университета в объеме не менее 0,25 экземпляров на одного обучающегося.

Основная литература

1. Лагоша, О. Н. Сертификация информационных систем: учеб. пособие для СПО / О. Н. Лагоша. - Изд. 3-е, стер. - Документ reader. - Санкт-Петербург [и др.]: Лань, 2023. - 109 с. - URL: https://reader.lanbook.com/book/297659 (дата обращения: 12.04.2023). - Режим доступа: для авториз. пользователей. - ISBN 978-5-507-46102-8: 0-00. - Текст: электронный. URL: https://reader.lanbook.com/book/297659

Дополнительная литература

2. Технические средства и методы защиты информации: учеб. пособие для вузов по специальностям "Компьютер. безопасность", "Комплекс. обеспеч. информ. безопасности автоматизир. систем", "Информ. безопасность телекоммуникац. систем" / А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков [и др.]; под ред. А. П. Зайцева, А. А. Шелупанова. - 4-е изд., испр. и доп. - Москва: Горячая линия - Телеком, 2009. - 615 с.: ил. - (Учебное пособие для высших учебных заведений). - Прил. - ISBN 978-5-9912-0084-4: 293-81. - Текст: непосредственный.

5.2. Профессиональные базы данных, информационно-справочные системы, интернет-ресурсы

1. КонсультантПлюс [Электронный ресурс]: справочная правовая система. – Режим доступа: http://www.consultant.ru/.

2. Электронная библиотечная система Поволжского государственного университета сервиса [Электронный ресурс]. – Режим доступа: http://elib.tolgas.ru/.

3. Электронно-библиотечная система Znanium.com [Электронный ресурс]. – Режим доступа: http://znanium.com/.

4. Электронно-библиотечная система «Издательство Лань» [Электронный ресурс]. – Режим доступа: https://e.lanbook.com/.

5. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс]. – Режим доступа: http://elibrary.ru/defaultx.asp.

6. Открытое образование [Электронный ресурс]. – Режим доступа: https://openedu.ru/.

7. Базы данных Всероссийского института научной и технической информации (ВИНИТИ РАН) по естественным, точным и техническим наукам [Электронный ресурс]. – Режим доступа: http://www.viniti.ru.

5.3. Программное обеспечение

Информационное обеспечение учебного процесса по дисциплине осуществляется с использованием следующего программного обеспечения (лицензионного и свободно распространяемого), в том числе отечественного производства:

№ п/п	Наименование	Условия доступа
1	Microsoft Windows	из внутренней сети университета (лицензионный договор)
2	Microsoft Office	из внутренней сети университета (лицензионный договор)
3	КонсультантПлюс	из внутренней сети университета (лицензионный договор)
4	СДО MOODLE	из любой точки с доступом к сети Интернет (доступ через ЭИОС университета)

6. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных учебным планом и рабочей программой дисциплины, оснащенные оборудованием и техническими средствами обучения.

Занятия лекционного типа. Учебные аудитории для занятий лекционного типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук), учебно-наглядные пособия (презентации по темам лекций), обеспечивающие тематические иллюстрации, соответствующие данной программе дисциплины.

Занятия семинарского типа. Учебные аудитории для занятий семинарского типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук). Для проведения лабораторных работ используется учебная аудитория «Лаборатория информационных технологий, информатики и методов программирования // Учебная аудитория для проведения занятий лекционного типа, семинарского типа, курсового проектирования, консультаций, текущего контроля и промежуточной аттестации // Помещение для хранения и профилактического обслуживания учебного оборудования (Г-413)», оснащенная следующим оборудованием: рабочие места обучающихся; Рабочее место преподавателя; Учебно-наглядные пособия, обеспечивающие тематические иллюстрации. Компьютер Acyc Intel G530\iH61\GeForceGT430\4096 Mb DDR3\500Gb\LCD 22" - 14 шт., Компьютер в сборе iP2.0 LCD - 1 шт., принтер HP 1200 - 1 шт., мобильный экран проекционный DraperLuma - 1 шт., мобильный проектор Sanyo PLC, Сетевое оборудование D-Link DES-1024D, 24-портовый; локальная сеть 100 мб с доступом в Интернет 50 мб. Лаборатория оснащена кондиционером.

Промежуточная аттестация. Для проведения промежуточной аттестации по дисциплине используются компьютерные классы, оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду университета и/или учебные аудитории, укомплектованные мебелью и техническими средствами обучения.

Самостоятельная работа. Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде университета. Для организации самостоятельной работы обучающихся используются:

- компьютерные классы университета;
- библиотека (медиазал), имеющая места для обучающихся, оснащенные компьютерами с доступом к базам данных и сети Интернет.

Электронная информационно-образовательная среда университета (ЭИОС). Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде университета (ЭИОС) http://sdo.tolgas.ru/ из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети "Интернет", как на территории университета, так и вне ее.

ЭИОС университета обеспечивает:

- доступ к учебным планам, рабочим программам дисциплин (модулей), программам практик, электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочих программах дисциплин (модулей), программах практик;
- формирование электронного портфолио обучающегося, в том числе сохранение его работ и оценок за эти работы.

В случае реализации образовательной программы с применением электронного обучения, дистанционных образовательных технологий ЭИОС дополнительно обеспечивает:

фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения образовательной программы;

проведение учебных занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий;

взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействия посредством сети "Интернет".

7. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБУЧЕНИЯ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

При необходимости рабочая программа дисциплины может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья, в том числе для дистанционного обучения. Для этого требуется заявление студента (его законного представителя) и заключение психолого-медико-педагогической комиссии (ПМПК).

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) а для инвалидов также в соответствии с индивидуальной программой реабилитации инвалида, могут предлагаться следующие варианты восприятия учебной информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации.

- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (ФОНД ОЦЕНОЧНЫХ СРЕДСТВ) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Для оценки знаний, умений, навыков и уровня сформированности компетенции по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. В основу балльно-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего контроля успеваемости. Максимальное количество баллов в семестре – 100

Шкала оценки результатов освоения дисциплины, сформированности результатов обучения

Форма промежуточной аттестации	Уровень сформированности	100-балльная шкала, %	Шкала освоения, %	5-балльная дифференцированная оценка/балл
зачет	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

По итогам текущей успеваемости студенту может быть выставлена оценка по промежуточной аттестации в соответствии за набранными за семестр баллами (по накопительному рейтингу). Студентам, набравшим в ходе текущего контроля успеваемости по дисциплине от 61 до 100 баллов и выполнившим все обязательные виды запланированных учебных занятий, по решению преподавателя без прохождения промежуточной аттестации выставляется оценка в соответствии со шкалой оценки результатов освоения дисциплины.

Результат обучения считается сформированным (повышенный уровень), если теоретическое содержание курса освоено полностью; при устных собеседованиях студент исчерпывающе, последовательно, четко и логически стройно излагает учебный материал; свободно справляется с задачами, вопросами и другими видами заданий, требующих применения знаний, использует в ответе дополнительный материал; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 86 до 100, что соответствует повышенному уровню сформированности результатов обучения.

Результат обучения считается сформированным (пороговый уровень), если теоретическое содержание курса освоено полностью; при устных собеседованиях студент последовательно, четко и логически стройно излагает учебный материал; справляется с задачами, вопросами и другими видами заданий, требующих применения знаний; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 61 до 85,9, что соответствует пороговому уровню сформированности результатов обучения.

Результат обучения считается несформированным, если студент при выполнении заданий не демонстрирует знаний учебного материала, допускает ошибки, неуверенно, с большими затруднениями выполняет задания, не демонстрирует необходимых умений, качество выполненных заданий не соответствует установленным требованиям, качество их выполнения оценено числом баллов ниже 61, что соответствует допороговому уровню.

Формы текущего контроля успеваемости

Формы текущего контроля	Количество контрольных точек	Количество баллов за 1 контр. точку	Макс. возм. кол-во баллов
Посещение лекционного занятия (конспект лекций)	8	2	16
Выполнение лабораторных работ	8	8	64
Самостоятельная работа (портфолио по темам)	8	2	16
Творческий рейтинг (итоговая защита проекта)	1	4	4
Итого по дисциплине			**100 баллов**

Системаоценивания представлена в электронном учебном курсе по дисциплине http://sdo.tolgas.ru/.

8.2. Типовые контрольные задания или иные материалы для ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

8.2.1. Типовые задания к практическим (семинарским) занятиям

Практическая работа 1. Разработка программы мониторинга учебной информационной системы

Задание 1. Составьте перечень активов, их владельцев и возможных последствий нарушения безопасности; укажите допущения о границах системы.

Задание 2. Определите пять целей мониторинга и для каждой укажите событие или показатель, позволяющий проверить достижение цели.

Задание 3. Подберите нормативные и локальные основания и разграничьте обязательное требование, методическую рекомендацию и учебное проектное решение.

Задание 4. Подготовьте программу мониторинга с этапами внедрения, ответственными, периодичностью контроля и критериями приемки.

Практическая работа 2. Паспортизация источников и проверка полноты доставки событий

Задание 1. Определите для каждого источника необходимые поля, формат времени, владельца и ответственного за подключение.

Задание 2. Рассчитайте полноту доставки уникальных записей источника A, объясните, почему повторы не компенсируют потери.

Задание 3. Приведите временные метки к одной шкале, сохранив исходное значение и часовой пояс; составьте порядок проверки рассинхронизации.

Задание 4. Разработайте процедуру диагностики источника B: наличие событий, доступность сборщика, очередь, канал и приемник. Укажите критерий восстановления.

Практическая работа 3. Разработка схемы нормализации и политики хранения журналов

Задание 1. Составьте таблицу соответствия полей и значений; выделите обязательные поля и правила обработки неизвестного результата.

Задание 2. Опишите обработку записей без имени узла без выдумывания значения. Сохраните исходный текст и отметку ошибки качества.

Задание 3. Рассчитайте объем необработанных данных за 30 суток в десятичных ГБ; отдельно обозначьте резерв, индексы, репликацию и сжатие как дополнительные параметры.

Задание 4. Подготовьте политику доступа, архивирования, контроля целостности и восстановления. Объясните, почему учебный срок не является универсальным нормативным требованием.

Практическая работа 4. Разработка и проверка правила корреляции

Задание 1. Опишите правило «не менее пяти отказов за пять минут и последующий успешный вход в пределах двух минут» с точными границами окна и ключом группировки.

Задание 2. Составьте положительный, отрицательный и граничный тесты; отдельно проверьте повторы и события, поступившие с задержкой.

Задание 3. Укажите дополнительные данные для проверки accountA и объясните, почему само срабатывание не доказывает компрометацию.

Задание 4. Подготовьте карточку правила, условия исключений, порядок изменения и протокол проверки версии.

Практическая работа 5. Оценка покрытия активов и разработка плана устранения отклонений

Задание 1. Рассчитайте долю узлов с подтвержденной доставкой событий; не приравнивайте наличие агента к работоспособности.

Задание 2. Разделите обнаруженные отклонения по активам, последствиям и достоверности свидетельств; укажите необходимые уточнения.

Задание 3. Составьте план корректирующих действий с ответственными, сроками и проверяемыми критериями восстановления контроля.

Задание 4. Разработайте повторную проверку, включающую контрольное событие и

подтверждение его приема. Обоснуйте условия закрытия замечаний.

Практическая работа 6. Первичный анализ оповещения и подготовка пакета эскалации

Задание 1. Составьте хронологию с указанием источника каждого факта; отдельно запишите гипотезы и сведения для проверки.

Задание 2. Назначьте предварительный приоритет, обоснуйте его критичностью актива и возможными последствиями, отметьте неопределенность.

Задание 3. Подготовьте карточку случая и пакет эскалации: описание, границы, свидетельства, ответственный, срок следующего контроля и необходимые согласования.

Задание 4. Опишите сохранение исходных данных и порядок получения обратной связи. Предложите условия подтверждения, опровержения и закрытия случая.

Практическая работа 7. Разработка регламента мониторинга и матрицы ответственности

Задание 1. Выделите конфликты полномочий и составьте матрицу ролей с исполнителем, согласующим и информируемыми участниками.

Задание 2. Определите порядок приема и передачи смены, критерии эскалации и действия при отсутствии доступного ответственного.

Задание 3. Разработайте процедуру изменения правила: заявка, оценка влияния, тестирование, разрешение, внедрение, проверка и откат.

Задание 4. Составьте план обслуживания платформы с компенсацией временной потери наблюдения и последующей сверкой полноты данных.

Практическая работа 8. Оценка эффективности мониторинга и защита итогового проекта

Задание 1. Рассчитайте точность и полноту обнаружения, среднюю и медианную задержку; запишите формулы и единицы измерения.

Задание 2. Объясните пределы переноса результатов контрольной выборки на рабочую среду и влияние отсутствующего актива.

Задание 3. Сопоставьте программу, реестр источников, правила и регламент из предыдущих работ. Найдите не менее трех проверяемых условий приемки.

Задание 4. Защитите отчет и план улучшения с ответственными и ожидаемым результатом. Продемонстрируйте путь одного контрольного события от источника до решения аналитика.

8.3. Типовые контрольные задания или иные материалы для проведения промежуточной аттестации

Форма проведения промежуточной аттестации по дисциплине: зачет (по результатам накопительного рейтинга или в форме компьютерного тестирования).

Устно-письменная форма по билетам предполагается, как правило, для сдачи академической задолженности.

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.