

**ГАОУ ВО «Дагестанский государственный университет на-
родного хозяйства»**

*Утверждена решением
Ученого совета ДГУНХ,
протокол № 11
от 06 июня 2023 г*

**Кафедра «Информационные технологии и информационная
безопасность»**

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«СИЕМ-СИСТЕМЫ»**

Направление подготовки

**10.04.01 Информационная безопасность,
профиль «Управление информационной безопасностью и техно-
логии защиты информации»**

Уровень высшего образования - магистратура

Форма обучения – очная

Махачкала – 2023

УДК 681.518(075.8)

ББК 32.81.73

Составитель – Гасанова Зарема Ахмедовна, кандидат педагогических наук, заместитель заведующего кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

Внутренний рецензент – Галяев Владимир Сергеевич, кандидат физико-математических наук, доцент, заведующий кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

Внешний рецензент – Абдурагимов Гусейн Эльдарханович, кандидат физико-математических наук, доцент кафедры "Математические методы в экономике" Дагестанского государственного университета.

Представитель работодателя - Зайналов Джабраил Тажутдинович, директор регионального экспертно-аттестационного центра «Экспертиза», эксперт-представитель работодателя.

Рабочая программа дисциплины «SIEM-системы» разработана в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от 26 ноября 2020 г., № 1455, в соответствии с приказом Министерства науки и высшего образования от 6.04.2021 г., № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам магистратуры, программам специалитета, программам магистратуры»

Рабочая программа по дисциплине «SIEM-системы» размещена на официальном сайте www.dgunh.ru

Гасанова З.А. Рабочая программа по дисциплине «SIEM-системы» для направления подготовки 10.04.01 Информационная безопасность, профиль «Управление информационной безопасностью и технологии защиты информации». – Махачкала: ДГУНХ, 2023 г., 16 с.

Рекомендована к утверждению Учебно-методическим советом ДГУНХ 05 июня 2023 г.

Рекомендована к утверждению руководителем основной профессиональной образовательной программы высшего образования – программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем», к.пед.н., Гасановой З.А.

Одобрена на заседании кафедры «Информационные технологии и информационная безопасность» 31 мая 2023 г., протокол № 10.

Содержание

Раздел 1. Перечень планируемых результатов обучения по дисциплине...	4
Раздел 2. Место дисциплины в структуре образовательной программы...	5
Раздел 3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), на самостоятельную работу обучающихся и форму(ы) промежуточной аттестации.....	6
Раздел 4. Содержание дисциплины, структурированное по темам с указанием отведенного на них количества академических часов и видов учебных занятий.....	7
Раздел 5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.....	1 1
Раздел 6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.....	1 3
Раздел 7. Перечень лицензионного программного обеспечения, информационных справочных систем и профессиональных баз данных.....	13
Раздел 8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.....	1 4
Раздел 9. Образовательные технологии.....	15
Лист актуализации рабочей программы дисциплины.....	16

Раздел 1. Перечень планируемых результатов обучения по дисциплине

Целью дисциплины «SIEM-системы» является формирование компетенции обучающегося в области управления защитой информации на основе SIEM-систем.

Задачами дисциплины являются:

- является приобретение студентами знаний о процессах, процедурах, методах управления информационной безопасностью на основе SIEM-систем;
- приобретение навыков идентификации инцидентов информационной безопасности, формирования правил и процедур реагирования на инциденты информационной безопасности.

1.1. Компетенции выпускников, формируемые в результате освоения дисциплины «SIEM-системы» как часть планируемых результатов освоения образовательной программы

код компетенции	формулировка компетенции
ПК-2	Способен осуществлять сбор, анализ и систематизацию научно-технической информации по вопросам обеспечения информационной безопасности объектов информатизации

1.2. Планируемые результаты обучения по дисциплине

<i>Код и наименование компетенции</i>	<i>Код и наименование индикатора достижения компетенции</i>	<i>Планируемые результаты обучения по дисциплине</i>
ПК-2. Способен осуществлять сбор, анализ и систематизацию научно-технической информации по вопросам обеспечения информационной безопасности объектов информатизации	ИПК-2.1. Проводит анализ безопасности объектов информатизации	<u>Знать:</u> - понятие, назначение классификацию SIEM систем; - принципы работы siem-систем <u>Уметь:</u> - использовать siem-системы для анализа и управления информационной безопасности объектов информатизации <u>Владеть:</u> - навыками применения siem-систем для управления информационной безопасностью

1.3. Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины

Код компетенции	Этапы формирования компетенций					
	Тема 1. Системы управления событиями информационной безопасности (SIEM).	Тема 2. Обзор SIEM-систем на мировом и российском рынке.	Тема 3. Угрозы безопасности в автоматизированных системах	Тема 4. Классификация SIEM-систем	Тема 5. Требования к системе защиты информации автоматизированной системы	Тема 6. Техническая защита автоматизированных систем
ПК-2	+	+	+	+	+	+

Код компетенции	Этапы формирования компетенций				
	Тема 7. Аудит безопасности автоматизированных (информационных) систем	Тема 8. Планирование системы менеджмента инцидентов ИБ защищенных автоматизированных систем управления	Тема 9. Использование системы менеджмента инцидентов ИБ защищенных автоматизированных систем управления	Тема 10. Анализ и улучшение системы менеджмента инцидентов ИБ защищенных автоматизированных систем управления	Тема 11. Менеджмент конкретных видов инцидентов ИБ защищенных автоматизированных систем управления
ПК-2	+	+	+	+	+

Раздел 2. Место дисциплины в структуре образовательной программы

Дисциплина Б1.В.04 «SIEM-системы» относится к части, формируемой участниками образовательных отношений Блока 1 «Дисциплины» учебного плана направления подготовки 10.04.01 Информационная безопасность, профиля «Управление информационной безопасностью и технологии защиты информации».

Для изучения данной дисциплины необходимы знания, умения и навыки по дисциплинам «Основы информационной безопасности», «Основы управления информационной безопасностью», «Документоведение».

Освоение данной дисциплины необходимо обучающемуся для изучения дисциплин «Комплексное обеспечение защиты информации объекта информатизации», «Мониторинг и аудит защищенности информации в автоматизированных системах».

Раздел 3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), на самостоятельную работу обучающихся, на самостоятельную работу обучающихся и форму промежуточной аттестации

Объем дисциплины в зачетных единицах составляет 5 зачетных единицы.

Очная форма обучения

Количество академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), составляет 72 часа, в том числе:

на занятия лекционного типа – 36 ч.

на занятия семинарского типа – 36 ч.

Количество академических часов, выделенных на самостоятельную работу обучающихся – 72 ч.

Форма промежуточной аттестации: экзамен.

Отдельные учебные занятия по дисциплине реализуются в форме практической подготовки.

Раздел 4. Содержание дисциплины, структурированное по темам с указанием отведенного на них количества академических часов и видов учебных занятий.

Очная форма обучения

№ п/п	Тема дисциплины	Всего академических часов	В т.ч. занятия лекционного типа	В т.ч. занятия семинарского типа:					Самостоятельная работа	Форма текущего контроля успеваемости.
				семинары	Практические занятия	Лабораторные занятия (лабораторные работы, лабораторный практикум)	Коллоквиумы	Иные аналогичные занятия		
1.	Тема 1. Системы управления событиями информационной безопасности (SIEM).	8	2	-	1	1	-	-	4	Устный опрос Тестирование Подготовка реферата Подготовка презентации Выполнение практического задания, Выполнение лабораторной работы, Деловая игра
2.	Тема 2. Обзор SIEM-систем на мировом и российском рынке.	12	4	-	2	2	-	-	4	Устный опрос Тестирование Подготовка реферата Подготовка презентации Выполнение практического задания, Выполнение лабораторной работы, Деловая игра
3.	Тема 3. Угрозы безопасности в автоматизированных системах*	12	4*	-	2*	2*	-	-	4	Устный опрос Тестирование Подготовка реферата Подготовка презентации Выполнение практического задания, Выполнение лабораторной работы, Деловая игра

4.	Тема 4. Классификация SIEM-систем	8	2	-	1	1	-	-	4	Устный опрос Тестирование Подготовка реферата Подготовка презентации Выполнение практического задания, Выполнение лабораторной работы, Деловая игра
5.	Тема 5. Требования к системе защиты информации автоматизированной системы	12	4	-	2	2	-	-	4	Устный опрос Тестирование Подготовка реферата Подготовка презентации Выполнение практического задания, Выполнение лабораторной работы, Деловая игра
6.	Тема 6. Техническая защита автоматизированных систем	8	2	-	1	1	-	-	4	Устный опрос Тестирование Подготовка реферата Подготовка презентации Выполнение практического задания, Выполнение лабораторной работы, Деловая игра
7.	Тема 7. Аудит безопасности автоматизированных (информационных) систем*	16	4	-	2	2	-	-	8	Устный опрос Тестирование Подготовка реферата Подготовка презентации Выполнение практического задания, Выполнение лабораторной работы, Деловая игра
8.	Тема 8. Планирование системы	14	2*	-	1*	1*	-	-	10	Устный опрос Тестирование

	менеджмента инцидентов ИБ защищенных автоматизированных систем управления*									Подготовка реферата Подготовка презентации Выполнение практического задания, Выполнение лабораторной работы, Деловая игра
9.	Тема 9. Использование системы менеджмента инцидентов ИБ защищенных автоматизированных систем управления*	18	4*	-	2*	2*	-	-	10	Устный опрос Тестирование Подготовка реферата Подготовка презентации Выполнение практического задания, Выполнение лабораторной работы, Деловая игра
10.	Тема 10. Анализ и улучшение системы менеджмента инцидентов ИБ защищенных автоматизированных систем управления*	18	4*	-	2*	2*	-	-	10	Устный опрос Тестирование Подготовка реферата Подготовка презентации Выполнение практического задания, Выполнение лабораторной работы, Деловая игра
11.	Тема 11. Менеджмент конкретных видов инцидентов ИБ защищенных автоматизированных систем управления*	18	4*	-	2*	2*	-	-	10	Устный опрос Тестирование Подготовка реферата Подготовка презентации Выполнение практического задания, Выполнение лабораторной работы, Деловая игра
9.	ИТОГО:	0	36	-	18	18	-	-	0	
	Экзамен (групповая)	36								Контроль

	консультация в течение семестра, групповая консультация перед промежуточной аттестацией, экзамен)		
	ИТОГО	180	

*Реализуется в форме практической подготовки

Раздел 5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

№ п/п	Автор	Название основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Выходные данные	Количество экземпляров в библиотеке ДГУНХ/адрес доступа
I. Основная учебная литература				
1.	Аверченков, В.И.	Аудит информационной безопасности : учебное пособие для вузов	Москва : Издательство «Флинта», 2021. - 269 с. - Библиогр. в кн. - ISBN 978-5-9765-1256-6	https://biblioclub.ru/index.php?page=book_red&id=93245&sr=1
2.	Аверченков, В.И.	Служба защиты информации: организация и управление	Москва : Издательство «Флинта», 2021. - 186 с. ISBN 978-5-9765-1271-9	https://biblioclub.ru/index.php?page=book_red&id=93356&sr=1
3.	Веселов, Г.Е.	Менеджмент риска информационной безопасности	Таганрог : Издательство Южного федерального университета, 2016. - 109 с.	https://biblioclub.ru/index.php?page=book_red&id=493331&sr=1
4.	Пелешенко, В.С.	Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления	Ставрополь : СКФУ, 2017. - 86 с.	https://biblioclub.ru/index.php?page=book_red&id=467139&sr=1
II. Дополнительная учебная литература				
A) Дополнительная учебная литература				
1.	-	Аудит информационной безопасности органов исполнительной власти: учебное пособие / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, М.В. Рудановский.	Москва : Издательство «Флинта», 2016. - 100 с. ISBN 978-5-9765-1277-1	https://biblioclub.ru/index.php?page=book_red&id=93259&sr=1
2.	Ковалев Д.В.	Информационная безопасность	Ростов-на-Дону : Издательство Южного федерального университета, 2016. - 74 с.	https://biblioclub.ru/index.php?page=book_red&id=493175&sr=1

			ISBN 978-5-9275-2364-1	
3.	Нестеров С.А.	Основы информационной безопасности	Санкт-Петербург : Издательство Политехнического университета, 2014. - 322 с. ISBN 978-5-7422-4331-1	https://biblioclub.ru/index.php?page=book_red&id=363040&sr=1
4.	Пакин А.И.	Информационная безопасность информационных систем управления предприятием	Москва : Альтаир : МГАВТ, 2009. - 41 с.	https://biblioclub.ru/index.php?page=book_red&id=429778&sr=1

Б) Официальные издания: сборники законодательных актов, нормативно-правовых документов и кодексов РФ

1.	Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями).			
2.	ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. 2008 г. www.standartgost.ru			
3.	ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. www.standartgost.ru			
4.	ГОСТ Р ИСО/МЭК 15026-2002. Информационная технология. Уровни целостности систем и программных средств. 2002 г. www.standartgost.ru			
5.	ГОСТ Р ИСО/МЭК 27001-2006 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» www.standartgost.ru			
6.	ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. www.standartgost.ru			
7.	ГОСТ Р ИСО/МЭК 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности» www.standartgost.ru			

В) Периодические издания

1.	Журнал для пользователей персональных компьютеров «Мир ПК»			
2.	Научный журнал «Информатика и ее применение»			
3.	Информатика и безопасность			
4.	Журнал о компьютерах и цифровой технике «Computer Bild»			

5.	Рецензируемый научный журнал «Информатика и система управления»
6.	Рецензируемый научный журнал «Проблемы информационной безопасности»
Г) Справочно-библиографическая литература	
1.	1. Краткий энциклопедический словарь по информационной безопасности https://biblioclub.ru/index.php?page=book_red&id=58393&sr=1

Раздел 6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к одной или нескольким электронно-библиотечным системам и к электронной информационно-образовательной среде университета (<http://e-dgunh.ru>). Электронно-библиотечная система и электронная информационно-образовательная среда обеспечивает возможность доступа, обучающегося из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети "Интернет", как на территории университета, так и вне ее.

Для самостоятельного изучения материала и ознакомления с регламентирующими документами и текущей практикой в области менеджмента информационной безопасности, рекомендуется использовать следующие Интернет-ресурсы:

1. <http://www.fsb.ru/> – официальный сайт ФСБ
2. <http://fstec.ru/> – официальный сайт ФСТЭК
3. <http://www.consultant.ru/> – онлайн-версия информационно-правовой системы "КонсультантПлюс"
4. <http://Standartgost.ru> - Открытая база ГОСТов

Раздел 7. Перечень лицензионного программного обеспечения, информационных справочных систем и профессиональных баз данных

7.1. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

- Windows 10
- Microsoft Office Professional
- Adobe Acrobat Reader DC
- VLC Media player
- 7-zip
- Справочно-правовая система «КонсультантПлюс»

7.2. Перечень информационных справочных систем:

- информационно справочная система «КонсультантПлюс».

7.3. Перечень профессиональных баз данных:

- Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 (<https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n>

ross-ru-0001-01bi00).

- Реестр операторов, осуществляющих обработку персональных данных (<https://rkn.gov.ru/personal-data/register/>);
- <http://Standartgost.ru> - Открытая база ГОСТов

Раздел 8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для преподавания дисциплины «СИЕМ-системы» используются следующие специальные помещения и учебные аудитории:

Учебная аудитория для проведения учебных занятий № 4.9 (Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 2 литер «В»)

Перечень основного оборудования:

Комплект специализированной мебели.

Доска меловая.

Набор демонстрационного оборудования: проектор, персональный компьютер с доступом к сети Интернет и корпоративной сети университета, ЭБС «Университетская библиотека ONLINE» (www.biblioclub.ru), ЭБС «ЭБС Юрайт» (www.ura.it.ru), интерактивная доска, акустическая система.

Перечень учебно-наглядных пособий:

Комплект наглядных материалов (баннеры, плакаты);

Комплект электронных иллюстративных материалов (презентации, видеоролики).

Перечень используемого программного обеспечения:

1. Windows 10
2. Microsoft Office Professional
3. Adobe Acrobat Reader DC
4. VLC Media player
5. 7-zip

Лаборатория управления информационной безопасностью, учебная аудитория для проведения учебных занятий № 4.8 (Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 2 литер «В»)

Перечень основного оборудования:

Комплект специализированной мебели.

Доска меловая.

Набор демонстрационного оборудования: проектор, акустическая система.

Персональные компьютеры с доступом к сети Интернет и корпоративной сети университета, ЭБС «Университетская библиотека ONLINE» (www.biblioclub.ru), ЭБС «ЭБС Юрайт» (www.ura.it.ru) – 20 ед.

Перечень учебно-наглядных пособий:

Комплект наглядных материалов (баннеры, плакаты);

Комплект электронных иллюстративных материалов (презентации, видеоролики).

Помещение для самостоятельной работы № 4.5 (Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 2 литер «В»)

Перечень основного оборудования:

Персональные компьютеры с доступом к сети «Интернет» и в электронную информационно-образовательную среду – 19 ед.

Помещение для самостоятельной работы № 1-1 (Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 1)

Перечень основного оборудования:

Персональные компьютеры с доступом к сети «Интернет» и в электронную информационно-образовательную среду – 60 ед.

Раздел 9. Образовательные технологии

При освоении дисциплины «Основы управления информационной безопасностью» используются следующие образовательные технологии:

- деловые и ролевые игры для выработки навыков принятия решения в случаи инцидентов информационной безопасности;
- разбор конкретных ситуаций как для иллюстрации той или иной ситуации, так и в целях выработки навыков применения управленческих решений;
- проектная деятельность для выработки умений анализа информационных активов предприятия и разработки документов, регламентирующих деятельность по управлению информационной безопасностью в организации.
- внеаудиторная работа в форме обязательных консультаций и индивидуальных занятий со студентами (помощь в понимании тех или иных моделей и концепций, подготовка рефератов и эссе, а также тезисов для студенческих конференций и т.д.).

Лист актуализации рабочей программы дисциплины

«СИЕМ-системы»

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «_____» _____ 20__ г. № _____

Зав. кафедрой _____

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «_____» _____ 20__ г. № _____

Зав. кафедрой _____

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «_____» _____ 20__ г. № _____

Зав. кафедрой _____

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «_____» _____ 20__ г. № _____

Зав. кафедрой _____