Документ подписан простой электронной подписью
Информация о владельце:
ФИО: ПАНОВ Юрий Петрович
Должность: Ректор
Дата подписания: 09.06.2025 11:34:26
Уникальный программный ключ:
e30ba4f0895d1683ed43800960e77389e6cbff62

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования "Российский государственный геологоразведочный университет имени Серго Орджоникидзе"

(МГРИ)

Мониторинг информационной безопасности автоматизированных систем управления

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Промышленной кибербезопасности и защиты геоданных**

Учебный план s100503_25_BZO25.plx
Специальность 10.05.03 Информационная безопасность автоматизированных систем

Квалификация **Специалист по защите информации**

Форма обучения **очная**

Общая трудоемкость **4 ЗЕТ**

Часов по учебному плану 144
в том числе:
аудиторные занятия 98,25
самостоятельная работа 45,75

Виды контроля в семестрах:
зачеты с оценкой 10

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**10 (5.2)**		Итого	
Недель	14 2/6			
Вид занятий	УП	РП	УП	РП
Лекции	28	28	28	28
Практические	70	70	70	70
Иные виды контактной работы	0,25	0,25	0,25	0,25
В том числе инт.	4	4	4	4
Итого ауд.	98,25	98,25	98,25	98,25
Контактная работа	98,25	98,25	98,25	98,25
Сам. работа	45,75	45,75	45,75	45,75
Итого	144	144	144	144

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью изучения дисциплины «Мониторинг информационной безопасности автоматизированных систем управления» является теоретическая и практическая подготовка специалистов в области реагирования на инциденты информационной безопасности. В рамках освоения дисциплины студенты знакомятся с возможностями современных систем мониторинга информационной безопасности автоматизированных систем управления. Получают навыки по составлению технического задания на разработку, внедрение и модернизацию системы мониторинга, знакомятся с основными этапами внедрения систем мониторинга, получают представления о жизненном цикле данных систем. Изучение материала ведется в соответствии с действующим законодательством в сфере регулирования
1.2	АСУ.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Современные киберугрозы в промышленных и корпоративных системах автоматизации
2.1.2	Автоматизированные системы управления
2.1.3	Инженерно-техническая защита информации и технические средства охраны
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ПК-3: Способен выполнять работы по мониторингу и аудиту защищенности информации в автоматизированных системах	
Знать:	
Уровень 1	архитектуру промышленных сетей АСУ ТП; физические принципы, на которых строятся системы инженерно-технической защиты объектов; типы современных киберугроз в промышленных и корпоративных системах автоматизации, актуальные векторы атак на промышленные сети АСУ ТП
Уровень 2	средства и меры информационной безопасности, применяемые в промышленных и корпоративных системах автоматизации; основные понятия мониторинга событий, методы сбора информации о событиях, принципы работы систем управления информацией и событиями в безопасности SIEM
Уровень 3	принципы работы систем мониторинга информационной безопасности автоматизированных систем; методы и средства обеспечения информационной безопасности в системах электронного документооборота
Уметь:	
Уровень 1	применять методы и средства регистрации, записи и хранения значимых параметров потоков данных АСУ ТП; проводить оптимизацию структуры комплексов инженерно-технической защиты объектов
Уровень 2	проводить аналитику современных киберугроз в промышленных и корпоративных системах автоматизации, актуальные векторы атак на промышленные сети АСУ ТП; использовать средства сбора и анализа информации о событиях информационной безопасности для целей мониторинга информационной безопасности
Уровень 3	формировать правила анализа событий мониторинга информационной безопасности автоматизированных систем; определять необходимые методы и средства обеспечения информационной безопасности в системах электронного документооборота
Владеть:	
Уровень 1	навыком определения ключевых точек мониторинга значимых параметров потоков данных, распределенных в информационной системе промышленных сетей АСУ ТП; навыком анализа критериев оценки параметров технических средств охраны объектов
Уровень 2	навыком составления программы испытаний систем инженерно- технической защиты объектов; навыком оценки уязвимостей по отношению к современным киберугрозам промышленных сетей АСУ ТП
Уровень 3	навыком использования методов мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; навыком проведения контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**

3.1.1	цели и задачи автоматизации управления, общие понятия автоматизированных систем управления (АСУ), жизненный цикл, функции и виды АСУ;
3.1.2	состав автоматизированных систем управления технологическим процессом (АСУ ТП), виды обеспечения, классификацию и уровни управления АСУ ТП, место АСУ ТП в интегрированных системах управления, архитектуру промышленных сетей АСУ ТП;
3.1.3	актуальные угрозы информационной безопасности промышленных компаний, текущее состояние и эволюцию киберугроз как ответную реакцию на внедрение средств и мер информационной безопасности, типы современных киберугроз в промышленных и корпоративных системах автоматизации, актуальные векторы атак на промышленные сети АСУ ТП;
3.1.4	средства и меры информационной безопасности, применяемые в промышленных и корпоративных системах автоматизации;
3.1.5	цели и задачи проектирования систем инженерно-технической защиты объектов;
3.1.6	основные понятия и терминологию, принятые в проектировании систем инженерно-технической защиты объектов;
3.1.7	основные принципы проектирования систем инженерно-технической защиты объектов, физические принципы, на которых строятся системы инженерно-технической защиты объектов
3.2	**Уметь:**
3.2.1	анализировать и моделировать информационные процессы, протекающие в системах промышленной автоматизации, применять методы и средства регистрации, записи и хранения значимых параметров потоков данных АСУ ТП;
3.2.2	анализировать и оценивать риски информационной безопасности в промышленных и корпоративных системах автоматизации, проводить аналитику современных киберугроз в промышленных и корпоративных системах автоматизации, актуальные векторы атак на промышленные сети АСУ ТП;
3.2.3	проводить анализ вероятных угроз охраняемому объекту;выбирать наиболее рациональные методы противодействия угрозам охраняемому объекту;выбирать технические средства для решения задачи охраны объекта, проводить оптимизацию структуры комплексов инженерно- технической защиты объектов
3.3	**Владеть:**
3.3.1	определения ключевых точек мониторинга значимых параметров потоков данных, распределенных в информационной системе промышленных сетей АСУ ТП;
3.3.2	идентификации и моделирования каналов возможного деструктивного информационно-технического воздействия в промышленных и корпоративных системах автоматизации, оценки уязвимостей по отношению к современным киберугрозам промышленных сетей АСУ ТП;
3.3.3	анализа критериев оценки параметров технических средств охраны объектов;
3.3.4	составления программы испытаний систем инженерно-технической защиты объектов

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание
	Раздел 1. Основные понятия мониторинга информационной безопасности автоматизированных систем управления						
1.1	Мониторинг информационной безопасности АСУ. Требования законодательства. Действующие стандарты /Лек/	10	2	ПК-3	Л1.1 Л1.2	0	
1.2	Современные АСУ как объект защиты /Лек/	10	2	ПК-3	Л1.1 Л1.2	0	
1.3	Составные части системы мониторинга информационной безопасности автоматизированных систем управления. Основные принципы работы /Лек/	10	2	ПК-3	Л1.1 Л1.2	0	
1.4	Анализ действующего законодательства в сфере мониторинга информационной безопасности АСУ. /Пр/	10	8,7	ПК-3	Л1.1 Л1.2	0	
1.5	Анализ действующих стандартов в сфере мониторинга информационной безопасности АСУ. /Пр/	10	8,7	ПК-3	Л1.1 Л1.2	2	

1.6	Подготовка к практическим занятиям /Ср/	10	33,75	ПК-3	Л1.1 Л1.2	0	
	Раздел 2. Этапы построения системы мониторинга						
2.1	Этапы построения системы мониторинга. Инвентаризация. Внедрение инструментальных средств мониторинга /Лек/	10	2	ПК-3	Л1.1 Л1.2	0	
2.2	Этапы построения системы мониторинга. Особенности работы современных АСУ, поиск входных точек мониторинга /Лек/	10	2	ПК-3	Л1.1 Л1.2	0	
2.3	Этапы построения системы мониторинга. Агрегация, сбор, обогащение и представление информации /Лек/	10	3	ПК-3	Л1.1 Л1.2	0	
2.4	Этапы построения системы мониторинга. Инвентаризация. Внедрение инструментальных средств мониторинга /Пр/	10	8,7	ПК-3	Л1.1 Л1.2	0	
2.5	Этапы построения системы мониторинга. Агрегация, сбор, обогащение и представление информации /Пр/	10	8,7	ПК-3	Л1.1 Л1.2	0	
	Раздел 3. Процессы в системах мониторинга информационной безопасности в автоматизированных системах управления						
3.1	Мониторинг инцидентов информационной безопасности /Лек/	10	3	ПК-3	Л1.1 Л1.2	0	
3.2	Особенности сбора и анализа данных событий информационной безопасности /Лек/	10	3	ПК-3	Л1.1 Л1.2	0	
3.3	Реагирование на инцидент информационной безопасности /Лек/	10	3	ПК-3	Л1.1 Л1.2	0	
3.4	Экспертиза и расследование инцидента информационной безопасности на основании данных мониторинга /Лек/	10	3	ПК-3	Л1.1 Л1.2	0	
3.5	Анализ инцидента, ликвидация последствий, разработка корректирующих мероприятий /Лек/	10	3	ПК-3	Л1.1 Л1.2	0	
3.6	Способы и технические средства мониторинга информационной безопасности /Пр/	10	8,7	ПК-3	Л1.1 Л1.2	0	
3.7	Расследование и реагирование на инцидент информационной безопасности /Пр/	10	8,7	ПК-3	Л1.1 Л1.2	2	
3.8	Анализ причин возникновения инцидента, разработка компенсирующих мер /Пр/	10	8,8	ПК-3	Л1.1 Л1.2	0	
3.9	Разработка технического задания на модернизацию системы мониторинга информационной безопасности /Пр/	10	9	ПК-3	Л1.1 Л1.2	0	
3.10	Подготовка к зачету /Ср/	10	12	ПК-3	Л1.1 Л1.2	0	
3.11	Зачет /ИВКР/	10	0,25	ПК-3	Л1.1 Л1.2	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

Тема 1: Введение в мониторинг ИБ АСУ. Требования законодательства
1. Что такое мониторинг информационной безопасности АСУ и зачем он нужен?
2. Какие нормативно-правовые акты регулируют вопросы обеспечения ИБ в АСУ в РФ?
3. Какие стандарты и рекомендации используются при организации мониторинга ИБ (ГОСТ Р, ISO/IEC)?
4. Как связаны Федеральный закон №187-ФЗ и Приказ ФСТЭК №31 с мониторингом ИБ?
5. Каково значение международных стандартов (например, IEC 62443) в области промышленной кибербезопасности?
Тема 2: Современные АСУ как объект защиты
6. Что понимается под современной АСУ ТП в контексте информационной безопасности?
7. Чем отличаются традиционные и цифровые АСУ?
8. Какие компоненты АСУ требуют особого внимания с точки зрения защиты?
9. Как влияет интеграция IT и OT на безопасность систем?
10. Какие угрозы наиболее актуальны для современных АСУ?
Тема 3: Составные части системы мониторинга ИБ АСУ
11. Какие основные компоненты входят в систему мониторинга ИБ?
12. Какие функции выполняет система сбора логов и событий?
13. Что такое SIEM и какова его роль в мониторинге?
14. Какие средства анализа и корреляции событий применяются?
15. Как организуется хранение и представление информации о состоянии ИБ?
Тема 4: Принципы работы системы мониторинга ИБ АСУ
16. Какие цели преследует система мониторинга ИБ?
17. Какие задачи решаются при построении системы мониторинга?
18. Как происходит обработка и фильтрация потоков событий?
19. Какие принципы положены в основу эффективного мониторинга?
20. Как строится модель поведения системы и пользователей?
Тема 5: Этапы построения системы мониторинга ИБ. Инвентаризация
21. Какие этапы включает создание системы мониторинга ИБ?
22. Как проводится инвентаризация активов в рамках АСУ?
23. Какие объекты необходимо учитывать при инвентаризации?
24. Как определяется уровень значимости объектов?
25. Как инвентаризация влияет на выбор средств мониторинга?
Тема 6: Внедрение инструментальных средств мониторинга
26. Какие инструменты используются для реализации мониторинга ИБ?
27. Как осуществляется внедрение агентов и датчиков на объектах АСУ?
28. Какие требования предъявляются к инструментальным средствам мониторинга?
29. Как обеспечить совместимость с legacy-системами АСУ?
30. Как выбрать подходящее ПО для мониторинга ИБ?
Тема 7: Особенности построения мониторинга в современных АСУ
31. Какие специфические особенности имеют современные АСУ?
32. Какие входные точки мониторинга существуют в промышленных сетях?
33. Как организовать мониторинг в условиях ограниченного доступа к системам?
34. Какие протоколы и технологии используются для мониторинга АСУ?
35. Как обеспечить минимальное влияние на работу технологических процессов?
Тема 8: Сбор, агрегация и обогащение информации
36. Какие источники данных используются при мониторинге ИБ?
37. Как происходит сбор и объединение данных из различных систем?
38. Что такое обогащение данных и зачем оно нужно?
39. Как формируется единая информационная картина состояния ИБ?
40. Как данные мониторинга используются для построения отчетов и метрик?
Тема 9: Представление информации. Визуализация
41. Как представляются данные мониторинга оператору?
42. Какие виды визуализации используются (графики, карты, панели)?
43. Как строятся KPI и SLI для системы ИБ?
44. Как использовать графы и диаграммы для анализа угроз?
45. Как организовать централизованное управление и отображение событий?
Тема 10: Мониторинг инцидентов информационной безопасности
46. Что такое инцидент ИБ и как он классифицируется?
47. Какие события считаются предвестниками инцидентов?
48. Как организовать раннее выявление инцидентов?
49. Какие метрики используются для оценки инцидентов?
50. Как автоматизировать обнаружение и классификацию инцидентов?
Тема 11: Сбор и анализ данных событий ИБ
51. Как собираются данные о событиях безопасности в АСУ?
52. Какие типы событий регистрируются (логи, алерты, метаданные)?
53. Как проводится корреляция событий из разных источников?
54. Как используется машинное обучение в анализе событий ИБ?
55. Какие проблемы возникают при обработке больших объемов данных?
Тема 12: Реагирование на инцидент ИБ
56. Что входит в понятие "реагирование на инцидент"?

57. Как организовать процедуру первичного реагирования?
58. Какие действия должны быть выполнены при обнаружении угрозы?
59. Как работает система автоматического реагирования (SOAR)?
60. Как взаимодействуют службы безопасности при реагировании?
Тема 13: Экспертиза и расследование инцидента
61. Что такое экспертиза инцидента и какие цели она преследует?
62. Как проводится анализ следов атаки в логах и трассировках?
63. Какие инструменты используются при расследовании инцидентов?
64. Как восстанавливается последовательность событий (forensics)?
65. Как формируются выводы и рекомендации после расследования?
Тема 14: Анализ инцидента. Ликвидация последствий. Корректирующие мероприятия
66. Как проводится комплексный анализ причин инцидента?
67. Какие действия необходимы для ликвидации последствий инцидента?
68. Как оценивается масштаб и ущерб от инцидента?
69. Как разрабатываются корректирующие и профилактические меры?
70. Как осуществляется документирование и передача данных для расследования?

5.2. Темы письменных работ

не предусмотрены

5.3. Оценочные средства

Рабочая программа "Мониторинг информационной безопасности автоматизированных систем управления" обеспечена оценочными средствами для проведения текущего контроля и промежуточной аттестации, включающими контрольные вопросы для проведения промежуточной аттестации, критерии оценивания учебной деятельности обучающихся по балльно-рейтинговой системе, примеры заданий для практических и лабораторных занятий, билеты для проведения промежуточной аттестации.
Все оценочные средства представлены в Приложении 1.

5.4. Перечень видов оценочных средств

Оценочные средства разработаны для всех видов учебной деятельности студента - лекций, практических занятий, самостоятельной работы и промежуточной аттестации. Оценочные средства представлены в виде:
- средства текущего контроля: проверочных работ по решению задач, дискуссии по теме;
- средств итогового контроля - промежуточной аттестации: экзамена в 10 семестре.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Никифоров С. Н.	Методы защиты информации. Защищенные сети	Санкт-Петербург: Лань, 2021
Л1.2	Трофимов В. В., Барабанова М. И., Кияев В. И.	Глобальные и локальные сети: учебник для вузов	Москва: Юрайт, 2024

6.3.1 Перечень программного обеспечения

6.3.1.1	Office Professional Plus 2019	
6.3.1.2	Windows 10	
6.3.1.3	МТС-Линк	Комплексная платформа для коммуникаций, обучения и совместной работы, разработанная с использованием современных технологий. Доступны десктопные и мобильные приложения для удобной работы с системой.

6.3.2 Перечень информационных справочных систем

6.3.2.1	Электронно-библиотечная система «Книжный Дом Университета» ("БиблиоТех")
6.3.2.2	Электронно-библиотечная система "Лань" Доступ к коллекциям электронных изданий ЭБС "Издательство "Лань"
6.3.2.3	База данных научных электронных журналов "eLibrary"

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Аудитория	Назначение	Оснащение	Вид

1	Специализированная многофункциональная учебная аудитория № 1 для проведения учебных занятий лекционного и семинарского типов, групповых и индивидуальных консультаций, текущего контроля и промежуточной/ итоговой аттестации	Столы обучающихся; Стулья обучающихся; Письменный стол педагогического работника; Стул педагогического работника; Кафедра; Магнитно-маркерная доска; Мультимедийный проектор; Экран; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде	
5	Помещение № 5 для самостоятельной работы обучающихся	Письменный стол обучающегося; Стул обучающегося; Письменный стол обучающегося с ограниченными возможностями здоровья; Стул обучающегося с ограниченными возможностями здоровья; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Моноблок (в том числе, клавиатура, мышь, наушники) с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде	

6-25	Специализированная многофункциональная лаборатория № 6-25 для проведения практических и лабораторных занятий, текущего контроля и промежуточной/ итоговой аттестации, в том числе для организации практической подготовки обучающихся	Компьютерные столы; Стулья; Письменный стол педагогического работника; Стул педагогического работника; Магнитно-маркерная доска; Мультимедийный проектор; Экран; ПК с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Телекоммуникационные шкафы; Средства отображения информации. Стенды сетей передачи информации с коммутацией пакетов и коммутацией каналов в составе: Учебный стенд "Основы IP-сетей" (маршрутизаторы, коммутаторы L2/L3); Учебный стенд "Виртуальные сети (VLAN, VPN)"; Учебный стенд "Беспроводные сети (Wi-Fi, IoT)"; Учебный стенд "Телефония (ISDN, VoIP)"; Учебный стенд "Оптические сети (PON, DWDM)"; Стенд "Цифровые системы передачи (E1, SDH)". Стенды для изучения проводных и беспроводных компьютерных сетей в составе: абонентские устройства; коммутаторы; маршрутизаторы; точкидоступа, межсетевые экраны; средства обнаружения компьютерных атак; системы углубленной проверки сетевых пакетов; системы защиты от утечки данных; анализаторы кабельных сетей. Учебно-лабораторные комплексы в составе: Учебный лабораторный комплекс контроля сетевой безопасности (системы обнаружения вторжений и анализа защищенности, сетевые сканеры). Учебный лабораторный комплекс проведения анализа защищенности значимого объекта КИИ на соответствие	

		требованиям по обеспечению безопасности. Учебный лабораторный комплекс для обеспечения исследований специального программного обеспечения и аппаратного СЗИ в составе: средства защиты информации от НСД; программно-аппаратный комплекс доверенной нагрузки; антивирусные программные комплексы; межсетевые экраны; средства создания модели разграничения доступа; программа контроля полномочий доступа к информационным ресурсам; программа фиксации и контроля исходного состояния программного комплекса; программа поиска и гарантированного уничтожения информации на дисках; аппаратные средства аутентификации пользователя; системы обнаружения вторжений и анализа защищенности; средства анализа защищенности компьютерных сетей; сканеры безопасности; устройства чтения смарт-карт и радиометок; программно-аппаратные комплексы защиты информации; средства криптографической защиты информации. Учебный лабораторный комплекс для обеспечения исследований типовых сертифицированных программных и программно-технических средств защиты информации от НСД. Учебный лабораторный комплекс для обеспечения исследований сертифицированных средств в которых реализованы средства защиты информации от НСД. УЛК для проведения аттестационных испытаний автоматизированных систем от НСД по требованиям безопасности информации. Аппаратно-программные комплексы в составе: аппаратно-программные средства управления	

		доступом к данным; средства криптографической защиты информации; средства дублирования и восстановления данных; средства мониторинга состояния автоматизированных систем; средства контроля и управления доступом в помещения.	
Ауд. 8	Аудитория для научно-исследовательской работы обучающихся, курсового и дипломного проектирования № 8	Рабочие места на базе вычислительной техники с набором необходимых для проведения и оформления результатов исследований дополнительных аппаратных и/или программных средств; Письменный стол обучающегося; Стул обучающегося; Письменный стол обучающегося с ограниченными возможностями здоровья; Стул обучающегося с ограниченными возможностями здоровья; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Моноблок (в том числе, клавиатура, мышь, наушники) с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде; Многофункциональное устройство (принтер, сканер, ксерокс).	

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Методические указания по изучению дисциплины "Мониторинг информационной безопасности автоматизированных систем управления" представлены в Приложении 2 и включают в себя:
1. Методические указания для обучающихся по организации учебной деятельности.
2. Методические указания по организации самостоятельной работы обучающихся.
3. Методические указания по организации процедуры оценивания знания, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.