

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ЛУГАНСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЛГПУ»)**

Структурное подразделение Институт физико-математического
образования, информационных и обслуживающих технологий
Кафедра информационных образовательных технологий и систем

УТВЕРЖДАЮ

Директор ИФМОИОТ

Е.Е. Горбенко

«13» *декабря* 2023 г.



РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Защита информации

По направлению подготовки 09.03.04 Программная инженерия

Профиль подготовки Программное обеспечение систем и комплексов

Квалификация выпускника бакалавр

Форма обучения очная, заочная

Курс ОФО – 3 курс, ЗФО – 4 курс

Луганск, 2023

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

1.1. Область применения

Фонд оценочных средств (ФОС) – неотъемлемая часть рабочей программы дисциплины (модуля) Защита информации и предназначен для контроля и оценки образовательных достижений студентов, освоивших программу дисциплины (модуля).

1.2. Цели и задачи фонда оценочных средств

Цель ФОС – установить соответствие уровня подготовки обучающегося требованиям ФГОС ВО бакалавриат / специалитет / магистратура по направлению подготовки 09.03.04 Программная инженерия, утвержденного приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. № 920 (с изменениями и дополнениями).

1.3. Перечень компетенций, формируемых в процессе освоения основной образовательной программы

Процесс освоения дисциплины направлен на формирование следующих компетенций и индикаторов их достижения:

Код по ФГОС ВО	Индикатор достижения
Универсальные	
Общепрофессиональные	
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1. Знать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности ОПК-3.2. Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности ОПК-3.3. Владеть навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности
Профессиональные	

--	--

1.4. Этапы формирования компетенций и средства оценивания уровня их сформированности

Этапы формирования компетенций	Компетенции	Контрольно-оценочные средства / способ оценивания
Тема 1. Основы информационной безопасности	ОПК-3	Выполнение лабораторных работ
Тема 2. Методы резервного копирования данных	ОПК-3	Выполнение лабораторных работ
Тема 3. Методы аутентификации и авторизации	ОПК-3	Выполнение лабораторных работ
Тема 4. Анализ и настройка безопасности в операционных системах семейства MS Windows	ОПК-3	Выполнение лабораторных работ
Тема 5. Основы криптографической защиты информации	ОПК-3	Выполнение лабораторных работ
Тема 6. Компьютерные вирусы	ОПК-3	Выполнение лабораторных работ
Тема 7. Основы сетевой безопасности	ОПК-3	Выполнение лабораторных работ
Тема 8. Основы захвата и анализа трафика	ОПК-3	Выполнение лабораторных работ
Тема 9. Перехват трафика	ОПК-3	Выполнение лабораторных работ
Тема 10. Анализ сетевых атак	ОПК-3	Выполнение лабораторных работ
	ОПК-3	Выполнение лабораторных работ
	ОПК-3	Выполнение лабораторных работ
	ОПК-3	Выполнение лабораторных работ
	ОПК-3	Выполнение лабораторных работ
	ОПК-3	Выполнение лабораторных работ
	ОПК-3	Выполнение лабораторных работ
Текущая аттестация	ОПК-3	Контрольная работа
Промежуточная аттестация	ОПК-3	Зачет

1.5. Описание показателей формирования компетенций

Код компетенции	Результаты сформированности
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности	<p>ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности</p> <p>ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности</p> <p>ОПК-3.3. Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности</p>

1.6. Критерии оценивания компетенций на разных этапах их формирования

Вид учебной работы	Количество баллов		
6 семестр / 10-11 триместр			
	ОФО	О-ЗФО	ЗФО
Оформление отчетов по лабораторным работам	30 баллов		
Работа на лабораторных занятиях	30 баллов		
Выполнение тестовых заданий	-		
Выполнение заданий самостоятельной работы	10 баллов		
зачета	30 баллов		
Итого за семестр:	100 баллов		
Всего	100 баллов		

Накопительная система оценивания по 100-балльной шкале

Четырехбалльная система оценивания экзамена	100-балльная шкала	Буквенная шкала, соответствующая 100-балльной шкале	Система оценивания зачета
Отлично	90–100	А – отлично – теоретическое содержание курса освоено полностью, без пробелов; необходимые практические навыки работы с освоенным материалом сформированы; все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному	

Хорошо	83–89	В – очень хорошо – теоретическое содержание курса освоено полностью, без пробелов; необходимые практические навыки работы с освоенным материалом в основном сформированы; все предусмотренные программой обучения учебные задания выполнены, качество выполнения большинства из них оценено числом баллов, близким к максимальному	Зачтено
Хорошо	75–82	С – хорошо – теоретическое содержание курса освоено полностью; некоторые практические навыки работы с освоенным материалом сформированы недостаточно; все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками	
Удовлетворительно	63–74	Д – удовлетворительно – теоретическое содержание дисциплины освоено частично, но пробелы не носят существенного характера; необходимые практические навыки работы с освоенным материалом в основном сформированы; большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий, содержат ошибки	
Удовлетворительно	50–62	Е – посредственно – теоретическое содержание курса освоено частично; некоторые практические навыки работы не сформированы, многие предусмотренные программой обучения учебные задания не выполнены либо качество выполнения некоторых из них оценено числом баллов, близким к минимальному	
Неудовлетворительно	21–49	FX – неудовлетворительно – теоретическое содержание курса освоено частично; необходимые практические навыки работы не сформированы; большинство предусмотренных программой обучения учебных заданий не выполнено либо качество их выполнения оценено числом баллов, близким к минимальному; при дополнительной самостоятельной работе над материалом курса возможно повышение качества выполнения учебных заданий	Не зачтено
Неудовлетворительно	0–20	F – неудовлетворительно – теоретическое содержание курса не освоено; необходимые практические навыки работы не сформированы; все выполненные учебные задания содержат грубые ошибки, дополнительная самостоятельная работа над материалом курса не приведет к какому-либо значимому повышению качества выполнения учебных заданий	

2. КОНТРОЛЬНО-ОЦЕНОЧНЫЕ СРЕДСТВА

2.1. Оценочные средства текущего контроля (типовые)

Вопросы для текущего контроля:

1. Назовите базовые понятия информационной безопасности.
2. Определите основные виды угроз информационным ресурсам.
3. Поясните суть методологии STRIDE?
4. Какие из угроз по методологии STRIDE представляют наибольшую опасность?
5. Поясните методику оценки рисков DREAD?
6. Поясните термин эксплоит?
7. В чем отличия между методиками DREAD и OCTAVE?
8. Поясните суть термина конфиденциальность, приведите примеры конфиденциальной информации.
9. Были получены две оценки безопасности информационной системы: первая -- на основании опроса очень большого числа обычных пользователей, вторая -- на основании мнения узкого круга экспертов. Какая из оценок на ваш взгляд более точная.
10. Приведите примеры санкционированного и несанкционированного доступа.
11. Можно ли считать установку антивируса на ПК комплексной защитой ИС?
12. Какая из методологий анализа информационных угроз на ваш взгляд более эффективна?
13. Назовите методы сжатия данных которые вы знаете.
14. Опишите основную идею алгоритма Хаффмана.
15. Объясните разницу между сжатием и архивацией.
16. Каким образом использование архивов связано с безопасностью информации?
17. В каких случаях целесообразно, а в которых нецелесообразно использование архивов?
18. Могут архивы формата ZIP содержать информацию для восстановления?
19. Покажите, каким образом можно заблокировать архив, что означает данная функция?
20. Опишите общую последовательность действий для защиты информации при создании архива.
21. Назовите основные технологии RAID.
22. Назовите основные методы дублирования информации.
23. Опишите преимущества и недостатки различных уровней RAID.
24. Как называется в соответствии с процедурой дублирования различают метод, который предполагает создание дублей определенных файлов?
25. Уровень RAID в котором предполагается поочередное использование целостности и доступности информации при стихийных бедствиях и крупных авариях называется...

26. В чем особенности дискреционной политики безопасности? В каких случаях ее использование нецелесообразно?
27. Опишите преимущества и недостатки мандатной политики безопасности.
28. В каких случаях применяется пассивная аутентификация?
29. Назовите два основных подхода при создании набора прав и привилегий пользователей.
30. Кто управляет разрешениями на доступ к разделам реестра и почему?
31. Какие из объектов могут наследовать разрешения на доступ к ним и от кого?
32. Для чего предназначены параметры создаваемой учетной записи пользователя?
33. В чем разница между отключением и блокировкой учетной записи?
34. В чем целесообразность разбиения множества пользователей на группы?
35. Как назначаются права пользователям и группам в защищенных версиях операционной системы Windows?
36. Какие требования по сложности могут предъявляться к паролям в операционной системе Windows?
37. Что такое криптография и каковы ее основные цели в контексте защиты информации?
38. Какие основные методы криптографии существуют и как они классифицируются?
39. Что представляет собой шифрование и какие виды шифрования существуют?
40. Каким образом работает симметричное шифрование, и какие примеры алгоритмов используются в этом типе шифрования?
41. Что такое асимметричное шифрование и в чем заключается принцип использования открытого и закрытого ключей?
42. Какие основные принципы работы криптографических хеш-функций и в чем их применение?
43. Что представляют собой цифровые подписи и как они обеспечивают аутентификацию и целостность данных?
44. Как работает протокол обмена ключами Diffie-Hellman, и как он обеспечивает безопасный обмен ключами для шифрования?
45. Что такое атака посередине (man-in-the-middle) и какие методы применяются для ее предотвращения в криптографии?
46. Какие принципы лежат в основе атаки на шифр с использованием подбора ключа и как этому можно противостоять?
47. Что такое стойкость криптосистемы и почему это важный аспект в обеспечении криптографической безопасности?
48. Каким образом реализуется защита от атаки по времени (timing attack) в криптографии?
49. Какие существуют методы криптографической аутентификации и как они применяются в системах безопасности?

50. Что такое криптографическая соль и как она повышает стойкость хеширования паролей?
51. Каким образом криптография используется для обеспечения конфиденциальности данных в сети?
52. Что такое биометрические методы аутентификации и как они сочетаются с криптографией?
53. Как шифрование конечных точек (end-to-end encryption) обеспечивает конфиденциальность данных в коммуникационных приложениях?
54. Каким образом работает квантовая криптография и в чем заключается ее стойкость к атакам квантовых компьютеров?
55. Что такое криптографические протоколы и как они применяются в обеспечении безопасной коммуникации?
56. Какие вызовы возникают при использовании криптографии в области интернета вещей (IoT)?
57. Каким образом криптография используется в системах электронной подписи для обеспечения доверия к электронным документам?
58. Как происходит обеспечение безопасности в блокчейн-технологиях с использованием криптографии?
59. Какие методы криптографии применяются для защиты информации на уровне файлов и дисков?
60. Что такое криптографические атаки с использованием каналов обратной стороны (side-channel attacks) и как им противостоять?
61. Каким образом обеспечивается безопасность криптографических ключей и их хранение?
62. Какие стандарты и алгоритмы шифрования широко применяются в современной криптографии?
63. Что представляют собой криптографические протоколы TLS и SSL, и как они обеспечивают безопасность в интернете?
64. Каким образом технология квантового ключа (quantum key distribution) обеспечивает безопасный обмен ключами?
65. Что такое криптографический принцип нулевого доверия (zero-trust) и как он применяется в современных системах безопасности?
66. Что представляют собой компьютерные вирусы и как они различаются от других форм вредоносных программ?
67. Каким образом компьютерные вирусы распространяются и какие методы защиты могут предотвратить их передачу?
68. Что такое троянские программы и какие основные цели они могут преследовать в контексте компьютерных вирусов?
69. Какие виды повреждений могут вызывать компьютерные вирусы и как они могут воздействовать на работу компьютерной системы?
70. Что представляют собой черви (worms) и в чем заключается их основное отличие от обычных вирусов?

2.2. Оценочные средства для промежуточной аттестации

Вопросы для проведения аттестации

1. Какие основные функции брандмауэра? Способы включения и выключения брандмауэра.
2. Как запустить брандмауэр в режиме повышенной безопасности с помощью командной строки?
3. Как создать новое правило для исходящих или входящих подключений?
4. Как открыть или закрыть порт с помощью брандмауэра?
5. Как разрешить произвольной программе доступ к сети с помощью брандмауэра?
6. Какой из стандартных профилей должен быть наиболее защищен?
7. Как быстро открыть панель управления?
8. Как быстро запустить брандмауэр в режиме повышенной безопасности?
9. Что делает команда `services.msc`?
10. Как запустить утилиту `cmd` в режиме администратора?
11. Как открыть окно локальных политик безопасности?
12. Зачем проверять системные файлы?
13. Каким образом можно проверить цифровую подпись файлов?
14. Как открыть реестр Windows?
15. Приведите основные команды оболочки `cmd`.
16. Какие из утилит системы Windows непосредственно связаны с безопасностью информации?
17. Назовите оснастки, используемые для настройки параметров безопасности.
18. Назовите основные способы запуска локальных политик безопасности.
19. Назовите и объясните уровни групповых политик.
20. Назовите порядок применения групповых политик.
21. Как запустить консоль управления?
22. Как добавить новую оснастку в консоль управления?
23. Объясните основные политики паролей.
24. Объясните термин групповая политика.
25. Какие виды групповых и локальных политик вы знаете?
26. Назовите три способа запуска редактора групповых политик.
27. Объясните параметры узла Параметры безопасности.
28. Для чего предназначены политики аудита, как настроить эти политики?
29. Какие события возможно фиксировать с помощью политик аудита?
30. Каким образом аудит может быть использован для повышения безопасности системы?
31. Объясните назначение основных политик аудита.
32. Дайте определение понятия шаблона безопасности.
33. Какие преимущества дает использование шаблонов безопасности?
34. Какие из служб по вашему мнению следует выключить для повышения безопасности?
35. Какие инструменты операционной системы следует блокировать для обычного пользователя?

37. Какие политики можно настраивать с помощью шаблонов безопасности?
38. Как вы считаете, какие параметры следует устанавливать и групповые политики настраивать при создании шаблона безопасности.
39. Какое основное назначение оснастки Анализ безопасности компьютера?
40. Возможно ли открыть оснастку Анализ безопасности
41. компьютера с помощью панели управления?
42. Каким образом добавляются шаблоны безопасности к оснастке Анализ безопасности компьютера?
43. Изменяются настройки компьютера при проведении анализа?
44. Объясните, что означают отметки у названий политик после
45. проведения анализа.
46. Объясните команды контекстного меню узла Анализ и
47. настройка безопасности.
48. Можно ли менять шаблон безопасности непосредственно в оснастке
49. Анализ безопасности компьютера?
50. Какая отметка будет показана у названия политики после анализа по шаблону безопасности, если данная политика не существует на компьютере?
51. Какое основное назначение средства AppLocker?
52. Какие задачи можно решать с помощью AppLocker?
53. Какие службы должны работать для того, чтобы использовать правила AppLocker?
54. Объясните, какие шаги нужно сделать для создания нового правила в AppLocker.
55. Какие средства операционной системы используются для блокировки сменных носителей?
56. Как узнать ID устройства?
57. Объясните, что такое VID и PID?
58. Какие политики применяются для блокирования устройств, в чем между ними разница?
59. Объясните термины белый список и черный список устройств.
60. Что представляет собой сетевая безопасность и почему она важна для информационных систем?
61. Какие основные принципы конфиденциальности, целостности и доступности данных касаются сетевой безопасности?
62. Что такое аутентификация в сетевой безопасности и какие методы могут быть использованы для подтверждения легитимности пользователя?
63. Каким образом шифрование данных влияет на обеспечение конфиденциальности в сетевой безопасности?
64. Какие виды угроз могут быть представлены в сетевой среде, и как классифицируются эти угрозы?

65. Что такое атаки перехвата (sniffing) и как они могут быть предотвращены в рамках сетевой безопасности?
66. Какие методы используются для обеспечения целостности данных в передаче через сеть?
67. Что представляет собой фильтрация пакетов (packet filtering) в сетевой безопасности и как она работает?
68. Каким образом атаки типа "отказ в обслуживании" (DoS) могут угрожать сетевой безопасности, и как предотвратить такие атаки?
69. Что такое виртуальная частная сеть (VPN) и как она может обеспечить безопасное соединение через открытую сеть, такую как Интернет?
70. Как работает брандмауэр в контексте сетевой безопасности и какие функции он выполняет?
71. Что представляют собой атаки "фишинга" (phishing) и как пользователи могут избегать поддаваться на такие атаки в сетевой безопасности?
72. Какие методы аутентификации могут быть использованы для обеспечения безопасности в беспроводных сетях?
73. Что такое многофакторная аутентификация и почему она является важным элементом сетевой безопасности?
74. Как сетевые устройства, такие как маршрутизаторы и коммутаторы, могут быть сконфигурированы для повышения безопасности сети?
75. Что такое веб-приложения и какие угрозы они могут представлять для сетевой безопасности?
76. Какие меры могут быть предприняты для защиты от атак межсетевых протоколов (MITM) в сетевой безопасности?
77. Что представляет собой аутентификация по сертификатам и как она применяется в сетевой безопасности?
78. Каким образом сетевая безопасность связана с управлением правами доступа и какие роли могут быть назначены пользователям?
79. Что такое сетевые уязвимости и какие методы используются для их обнаружения и устранения в сетевой безопасности?
80. Какие роли могут выполнять мобильные устройства в аспекте сетевой безопасности, и как они могут быть защищены?
81. Что такое управление сетевой безопасностью и какие задачи включают в себя процессы управления?
82. Каким образом применение политик безопасности может улучшить сетевую безопасность организации?
83. Что представляют собой атаки на уровне приложений и как они могут быть предотвращены в сетевой безопасности?
84. Какие технологии сетевой безопасности используются для обнаружения и предотвращения вредоносных программ?
85. Что такое "белые списки" и "черные списки" в сетевой безопасности, и как они применяются к управлению доступом?

Перечень типовых практических заданий:

№ п/п	Перечень типовых практических заданий
1	<p>1. Выполните комплексный анализ информационных угроз и составьте рекомендации по защите для следующих предприятий:</p> <p>а) полиграфическое предприятие с двумя офисами и одной базой данных клиентов в облаке;</p> <p>б) сеть коммерческих центров из 20 отделений, которые имеют один главный офис;</p> <p>в) магазин по продаже мебели, который имеет доступ к базе данных завода производителя мебели;</p> <p>г) сервисный центр по ремонту мобильных телефонов.</p>
2	Используя программу CheckUDisk определить VID, PID флеш накопителя.
3	<p>1. Для произвольной программы (например пасьянс Паук) предоставьте доступ к сети с помощью брандмауэра Windows (см. теоретические сведения).</p> <p>2. программы Total Commander откройте порт 3128 по помощью брандмауэра (см. теоретические сведения).</p> <p>3. Запретите доступ к сети интернет для произвольной программы по помощью брандмауэра и файла hosts.</p> <p>Способ блокировки доступа к сети программам с помощью брандамуеру уже описано в теоретической части работы. Выполните для пасьянса Косынка (или другой программы) такие блокировки.</p>
4	В консоли управления создайте новый шаблон безопасности с именем Конфигурация служб, в описании шаблона укажите операционную систему, в которой будет применен этот шаблон, и собственную фамилию.
5	Выполните анализ безопасности с помощью шаблона, который были создан ранее.
6	Добавьте подключенный накопитель в черный список.
7	Зашифруйте с помощью магического квадрата свое ФИО