

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
ЛУГАНСКОЙ НАРОДНОЙ РЕСПУБЛИКИ

**ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ ЛУГАНСКОЙ НАРОДНОЙ РЕСПУБЛИКИ
«ЛУГАНСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ГОУ ВО ЛНР «ЛГПУ»)**

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

Кафедра информационных образовательных технологий и систем

УТВЕРЖДАЮ

Директор ИФМОИОТ

Горбенко Е.Е.

«03» _____ 2022 г.



Приложение к рабочей программе учебной дисциплины

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения текущего контроля и промежуточной аттестации
обучающихся по дисциплине
«Безопасность программ и данных»**

По направлению подготовки 44.03.04 Профессиональное обучение (по
отраслям)

Профиль подготовки – Разработка программного обеспечения
образовательных систем

Квалификация выпускника – бакалавр

Форма обучения – очная, заочная

Курс – ОФО – 3 курс (6 семестр), ЗФО – 4 курс (10-11 триместр)

Разработчик

Швыров В.В.

канд. физ.-мат. наук, доцент, доцент
кафедры информационных образовательных технологий и систем

И.о. заведующего кафедрой

Д.А. Капустин

«26» апреля 2022 г.

Луганск, 2022

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

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

Процесс освоения дисциплины направлен на овладение следующими компетенциями:

ПК-8 - Владение навыками использования операционных систем, сетевых технологий, средств разработки программного интерфейса, применения языков и методов формальных спецификаций, систем управления базами данных.

ПК-10 - Владение концепциями и атрибутами качества программного обеспечения (надежности, безопасности, удобства использования), в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества.

1.2. Этапы формирования компетенций и средства оценивания уровня их сформированности

Этапы формирования компетенций	Компетенции	Контрольно-оценочные средства / способ оценивания
Тема 1. Основы информационной безопасности	ПК-8; ПК-10	Выполнение лабораторных работ
Тема 2. Методы резервного копирования данных	ПК-8; ПК-10	Выполнение лабораторных работ
Тема 3. Методы аутентификации и авторизации	ПК-8; ПК-10	Выполнение лабораторных работ
Тема 4. Анализ и настройка безопасности в операционных системах семейства MS Windows	ПК-8; ПК-10	Выполнение лабораторных работ
Тема 5. Основы криптографической защиты информации	ПК-8; ПК-10	Выполнение лабораторных работ
Тема 6. Компьютерные вирусы	ПК-8; ПК-10	Выполнение лабораторных работ
Тема 7. Основы сетевой безопасности	ПК-8; ПК-10	Выполнение лабораторных работ
Тема 8. Основы захвата и анализа трафика	ПК-8; ПК-10	Выполнение лабораторных работ
Промежуточная аттестация	ПК-8; ПК-10	Выполнение лабораторных работ
Форма аттестации	ПК-8; ПК-10	Экзамен (письменный)

1.3. Описание показателей формирования компетенций

Код и наименование	Код и наименование индикатора достижения
--------------------	------------------------------------------

универсальной компетенции	универсальной компетенции
ПК-8 - Владение навыками использования операционных систем, сетевых технологий, средств разработки программного интерфейса, применения языков и методов формальных спецификаций, систем управления базами данных.	Знать методы и технологии использования операционных систем, сетевых технологий, средств разработки программного интерфейса, применения языков и методов формальных спецификаций, систем управления базами данных Уметь применять современные средства разработки программного интерфейса, методы формальных спецификаций, разрабатывать системы управления базами данных Владеть навыками использования операционных систем, сетевых технологий, средств разработки программного интерфейса, применения языков и методов формальных спецификаций, систем управления базами данных
ПК-10 - Владение концепциями и атрибутами качества программного обеспечения (надежности, безопасности, удобства использования), в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества.	Знать концепции и атрибуты качества программного обеспечения (надежности, безопасности, удобства использования). Уметь анализировать концепции и атрибуты качества программного обеспечения. Владеть навыками в использовании методов, инструментов и технологий обеспечения качества контроля качества программного обеспечения

1.4. Критерии оценивания компетенций на разных этапах их формирования

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

Накопительная система оценивания по 100-балльной шкале

Четырехбал- льная 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	Зачтено
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	
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	
--	--	----------------------------------------------------------------------------------------------------------	--

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ ЛНР
ГОУ ВО ЛНР «ЛГПУ»
ИНСТИТУТ ФИЗИКО-МАТЕМАТИЧЕСКОГО ОБРАЗОВАНИЯ, ИНФОРМАЦИОННЫХ
И ОБСЛУЖИВАЮЩИХ ТЕХНОЛОГИЙ

2021 – 2022 учебный год

Направление подготовки (специальность): 44.03.04 Профессиональное обучение (по отраслям)

курс / форма обучения (ОФО,ЗФО): ОФО, ЗФО

Семестр / триместр 6 семестр / 10-11 триместр

Учебная дисциплина: Безопасность программ и данных

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Цель и задачи изучения дисциплины «Безопасность программ и данных». Требования к уровню освоения содержания дисциплины.
- 2.
3. Практическое задание.

Утверждено на заседании кафедры информационных образовательных технологий и систем

Протокол № ____ от ____ г.

И.о. заведующего кафедрой ИОТС _____

Капустин Д.А.

(подпись)

Экзаменатор

(подпись)

доцент, Швыров В.В.

(должность, ФИО преподавателя)

2. КОНТРОЛЬНО-ОЦЕНОЧНЫЕ СРЕДСТВА

2.1. Оценочные средства текущего контроля (типовые)

Вопросы для текущего контроля (темы 1-8):

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?

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 объяснит уровне 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?
36. Какие политики можно настраивать с помощью шаблонов безопасности?
37. Как вы считаете, какие параметры следует устанавливать и групповые политики настраивать при создании шаблона безопасности.
38. Какое основное назначение оснастки Анализ безопасности компьютера?
39. Возможно ли открыть оснастку Анализ безопасности компьютера с помощью панели управления?
40. Каким образом добавляются шаблоны безопасности к оснастке Анализ безопасности компьютера?
41. Изменяются настройки компьютера при проведении анализа?
42. Объясните, что означают отметки у названий политик после проведения анализа.
43. Объясните команды контекстного меню узла Анализ и настройка безопасности.
44. Можно ли менять шаблон безопасности непосредственно в оснастке Анализ безопасности компьютера?
45. Какая отметка будет показана у названия политики после анализа по шаблону безопасности, если данная политика не существует на компьютере?
46. Какое основное назначение средства AppLocker?
47. Какие задачи можно решать с помощью AppLocker?
48. Какие службы должны работать для того, чтобы использовать

правила AppLocker?

49. Объясните, какие шаги нужно сделать для создания нового правила в AppLocker.

50. Какие средства операционной системы используются для блокировки сменных носителей?

51. Как узнать ID устройства?

52. Объясните, что такое VID и PID?

53. Какие политики применяются для блокирования устройств, в чем между ними разница?

54. Объясните термины белый список и черный список устройств.

Перечень практических заданий к зачету по дисциплине «Защита информации»:

№ п/п	Перечень типовых практических заданий
1	1. Выполните комплексный анализ информационных угроз и составьте рекомендации по защите для следующих предприятий: а) полиграфическое предприятие с двумя офисами и одной базой данных клиентов в облаке; б) сеть коммерческих центров из 20 отделений, которые имеют один главный офис; в) магазин по продаже мебели, который имеет доступ к базе данных завода производителя мебели; г) сервисный центр по ремонту мобильных телефонов.
2	Используя программу CheckUDisk определить VID, PID флеш накопителя.
3	1. Для произвольной программы (например пасьянс Паук) предоставьте доступ к сети с помощью брандмауэра Windows (см. теоретические сведения). 2. программы Total Commander откройте порт 3128 по помощью брандмауэра (см. теоретические сведения). 3. Запретите доступ к сети интернет для произвольной программы по помощью брандмауэра и файла hosts. Способ блокировки доступа к сети программам с помощью брандамуеру уже описано в теоретической части работы. Выполните для пасьянса Косынка (или другой программы) такие блокировки.
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