МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ЛУГАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ ВЛАДИМИРА ДАЛЯ»

Факультет компьютерных систем и информационных технологий

Кафедра информатики и программной инженерии

УТВЕРЖДАЮ
Декан факультета Компьютерных
систем и информационных технологий
_____ Кочевский А.А.
«19» 04 2023 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по учебной дисциплине
Теория информации и обеспечение информационной безопасности
(наименование учебной дисциплины, практики)
09.04.03 Прикладная информатика
(код и наименование направления подготовки (специальности))
09.04.03.01 Прикладная информатика в экономике
(наименование профиля подготовки (специальности, магистерской программы); при отсутствии ставится прочерк)

Разработчик (разработчики):
старший преподаватель _____ Сычева Л.Ф.

ФОС рассмотрен и одобрен на заседании кафедры информатики и программной инженерии
от 18 апреля 2023 г., протокол № 17

Заведующий кафедрой _____ Кочевский А.А.
(подпись)

Луганск – 2023 г.

Паспорт
фонда оценочных средств по учебной дисциплине
«Теория информации и обеспечение информационной безопасности»

Перечень компетенций (элементов компетенций), формируемых в результате освоения учебной дисциплины (модуля) или практики

№ п/п	Код контролируемой компетенции	Формулировка контролируемой компетенции	Контролируемые темы учебной дисциплины, практики	Этапы формирования (семестр изучения)
1	ОПК-3	способность анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями	Тема 1. Основы теории информации. Тема 2. Понятие энтропии. Тема 3. Количество информации и его оценка. Тема 4. Информация в системах управления. Тема 5. Понятие "информационная безопасность" Тема 6. Составляющие информационной безопасности	3
2	ПК-5	способность использовать современные методы оценки качества, надежности и информационной безопасности информационных систем в процессе их проектирования и эксплуатации	Тема 7. Система формирования режима информационной безопасности Тема 8. Механизмы обеспечения "информационной безопасности" Тема 9. Методы разграничение доступа Тема 10. Регистрация и аудит Тема 11. Межсетевое экранирование Тема 12. Технология виртуальных частных сетей (vpn)	3

Показатели и критерии оценивания компетенций, описание шкал оценивания

№ п/п	Код контролируемой компетенции	Показатель оценивания (знания, умения, навыки)	Контролируемые темы учебной дисциплины	Наименование оценочного средства
1	ОПК-3	ОПК-3.1. Знать: принципы, методы и средства анализа и структурирования профессиональной информации ОПК-3.2. Уметь: анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров ОПК-3.3. Владеть: навыками анализа профессиональной информации, подготовки аналитических обзоров с обоснованными выводами и рекомендациями	Тема 1. Основы теории информации. Тема 2. Понятие энтропии. Тема 3. Количество информации и его оценка. Тема 4. Информация в системах управления. Тема 5. Понятие "информационная безопасность" Тема 6. Составляющие информационной безопасности	Вопросы для обсуждения (в виде докладов и сообщений), лабораторная работа
2	ПК-5	ПК-5.1. Знать: современные методы оценки качества, надежности и информационной безопасности ИС в процессе проектирования и эксплуатации ПК-5.2. Уметь: применять современные методы оценки качества, надежности и информационной безопасности ИС в процессе проектирования и эксплуатации ПК-5.3. Владеть: навыками применения современных методов оценки качества, надежности и информационной безопасности ИС в процессе проектирования и эксплуатации прикладных ИС	Тема 7. Система формирования режима информационной безопасности Тема 8. Механизмы обеспечения "информационной безопасности" Тема 9. Методы разграничение доступа Тема 10. Регистрация и аудит Тема 11. Межсетевое экранирование Тема 12. Технология виртуальных частных сетей (vpn)	Вопросы для обсуждения (в виде докладов и сообщений), лабораторная работа

Фонды оценочных средств по дисциплине «Теория информации и обеспечение информационной безопасности»

Вопросы для обсуждения (в виде докладов и сообщений):

1. Классификация угроз информационной безопасности автоматизированных систем по базовым признакам.
2. Угроза нарушения конфиденциальности. Особенности и примеры реализации угрозы.
3. Угроза нарушения целостности данных. Особенности и примеры реализации угрозы.
4. Угроза отказа служб (угроза отказа в доступе). Особенности и примеры реализации угрозы.
5. Угроза раскрытия параметров системы. Особенности и примеры реализации угрозы.
6. Понятие политики безопасности информационных систем. Назначение политики безопасности.
7. Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики.
8. Требования к системам криптографической защиты: криптографические требования, требования надежности, требования по защите от НСД, требования к средствам разработки.
9. Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.
10. Функции и назначение стандартов информационной безопасности. Примеры стандартов, их роль при проектировании и разработке информационных систем.

Критерии и шкала оценивания по оценочному средству доклад, сообщение

Шкала оценивания (интервал баллов)	Критерий оценивания
5	Доклад (сообщение) представлен(о) на высоком уровне (студент в полном объеме осветил рассматриваемую проблематику, привел аргументы в пользу своих суждений, владеет профильным понятийным (категориальным) аппаратом и т.п.)
4	Доклад (сообщение) представлен(о) на среднем уровне (студент в целом осветил рассматриваемую проблематику, привел аргументы в пользу своих суждений, допустив некоторые неточности и т.п.)
3	Доклад (сообщение) представлен(о) на низком уровне (студент допустил существенные неточности, изложил материал с ошибками, не владеет в достаточной степени профильным категориальным аппаратом и т.п.)
2	Доклад (сообщение) представлен(о) на неудовлетворительном

	уровне или не представлен (студент не готов, не выполнил задание и т.п.)

Лабораторные работы

ЛАБОРАТОРНАЯ РАБОТА № 1

Тема: Виды информации и основные методы ее защиты.

Цель работы

Применение основ информационной безопасности для имитации действий нарушителя по раскрытию (нарушению конфиденциальности) при использовании одного и того же одноразового блокнота (гаммы) на основе побитового сложения по модулю 2 (взлом двухразового блокнота).

Отчет должен включать в себя следующие разделы:

- формулировку задания;
- описание основных методов, используемых в лабораторной работе;
- результаты работы (в виде файла или в виде скриншота);
- анализ результатов.

ЛАБОРАТОРНАЯ РАБОТА № 2

Тема: Виды угроз информационной безопасности Российской Федерации.

Цель работы

Применение основ информационной безопасности для нахождения путей противодействия угрозе раскрытия (нарушения конфиденциальности) при наличии дискреционной модели доступа путем реализации модели типовой атаки «Троянский конь» в ОС Novell Netware 4.12.

Отчет должен включать в себя следующие разделы:

- формулировку задания;
- описание основных методов, используемых в лабораторной работе;
- результаты работы (в виде файла или в виде скриншота);
- анализ результатов.

ЛАБОРАТОРНАЯ РАБОТА № 3

Тема: Источники угроз информационной безопасности Российской Федерации.

Цель работы

Применение основ информационной безопасности для нахождения путей противодействия угрозе раскрытия (нарушения конфиденциальности) в мандатной модели доступа при наличии пары: нарушитель – высокоуровневый сообщник.

Отчет должен включать в себя следующие разделы:

- формулировку задания;
- описание основных методов, используемых в лабораторной работе;
- результаты работы (в виде файла или в виде скриншота);
- анализ результатов.

ЛАБОРАТОРНАЯ РАБОТА № 4

Тема: Анализ информационной инфраструктуры государства.

Цель работы

Изучение процессов идентификации и аутентификации в вычислительной системе посредством создания собственной программы обработки пользовательского запроса на вход в систему. Реализация атаки на процесс идентификации/аутентификации

пользователя в ОС Novell Netware 4.12 с целью определения пароля на вход в систему, а также изучение основных методов противодействия подбору пароля.

Отчет должен включать в себя следующие разделы:

- формулировку задания;
- описание основных методов, используемых в лабораторной работе;
- результаты работы (в виде файла или в виде скриншота);
- анализ результатов.

ЛАБОРАТОРНАЯ РАБОТА № 5

Тема: Исследование атаки переполнения буфера как примера нарушения конфиденциальности, целостности и доступности информации.

Цель работы

Изучение алгоритмов вызова программ в ОС MS DOS, а также принципов действия атак переполнения буфера ("buffer-overflow"). Применение основ информационной безопасности для нахождения путей противодействия угрозе. Реализация на практике модели атаки переполнения буфера в ОС MS DOS.

Отчет должен включать в себя следующие разделы:

- формулировку задания;
- описание основных методов, используемых в лабораторной работе;
- результаты работы (в виде файла или в виде скриншота);
- анализ результатов.

ЛАБОРАТОРНАЯ РАБОТА № 6

Тема: Причины, виды, каналы утечки и искажения информации.

Цель работы

Изучение основных задач, моделирование и реализация на практике процесса регистрации и учета событий в ОС MS-DOS с целью практического применения основ защиты информации, а также для ознакомления с системой прерываний данной операционной системы. Ознакомление с основными методами обработки результатов аудита Осуществление на практике одного из методов обработки аудита клавиатуры с целью более полного представления об алгоритмах работы программ типа «Intrusion Detection».

Отчет должен включать в себя следующие разделы:

- формулировку задания;
- описание основных методов, используемых в лабораторной работе;
- результаты работы (в виде файла или в виде скриншота);
- анализ результатов.

ЛАБОРАТОРНАЯ РАБОТА № 7

Тема: Технические средства и методы защиты информации.

Цель работы

Разработать комплекс мероприятий по защите информации от возможной утечки информации за счет постоянных электромагнитных излучений (ПЭМИ) и наводок, основанных на использовании система активной защиты (САЗ) ВОЛНА-3М указанной зоны.

Отчет должен включать в себя следующие разделы:

- формулировку задания;
- описание основных методов, используемых в лабораторной работе;
- результаты работы (в виде файла или в виде скриншота);
- анализ результатов.

ЛАБОРАТОРНАЯ РАБОТА № 8

Тема: Программно-аппаратные средства обеспечения информационной безопасности.

Цель работы

Получение навыков по практическому применению Программно-аппаратного комплекса средств защиты информации (ПАК СЗИ) от несанкционированного доступа (НСД) «Аккорд-АМДЗ (аппаратный модуль доверенной загрузки)».

Отчет должен включать в себя следующие разделы:

- формулировку задания;
- описание основных методов, используемых в лабораторной работе;
- результаты работы (в виде файла или в виде скриншота);
- анализ результатов.

ЛАБОРАТОРНАЯ РАБОТА № 9

Тема: Тестовые испытания программных средств защиты.

Цель работы

Применение методов и технологий испытания программного и аппа-ратного уровней комплексной защиты информации для проверки наличия и работоспособности встроенных программных и иных средств защиты КИС.

Отчет должен включать в себя следующие разделы:

- формулировку задания;
- описание основных методов, используемых в лабораторной работе;
- результаты работы (в виде файла или в виде скриншота);
- анализ результатов.

ЛАБОРАТОРНАЯ РАБОТА № 10

Тема: Защита от утечек по каналу ПЭМИН, по акустическому и виброакустическому каналам.

Цель работы

Применение методов и технологий испытания аппаратного уровня комплексной защиты информации.

Отчет должен включать в себя следующие разделы:

- формулировку задания;
- описание основных методов, используемых в лабораторной работе;
- результаты работы (в виде файла или в виде скриншота);
- анализ результатов.

ЛАБОРАТОРНАЯ РАБОТА № 11

Тема: Анализ сетевой топологии и установленных сервисов

Цель работы

Применение методов и технологий испытания программного и аппаратного уровней комплексной защиты информации для проведения атаки на КИС с целью установления уязвимостей.

Отчет должен включать в себя следующие разделы:

- формулировку задания;
- описание основных методов, используемых в лабораторной работе;
- результаты работы (в виде файла или в виде скриншота);
- анализ результатов.

ЛАБОРАТОРНАЯ РАБОТА № 12

Тема: Сетевое сканирование

Цель работы

Применение методов и технологий испытания программного и аппаратного уровней комплексной защиты информации для проведения атаки на КИС с целью установления уязвимостей.

Отчет должен включать в себя следующие разделы:

- формулировку задания;
- описание основных методов, используемых в лабораторной работе;
- результаты работы (в виде файла или в виде скриншота);
- анализ результатов.

ЛАБОРАТОРНАЯ РАБОТА № 13

Тема: Анализ трафика и сбор критичной информации программами пассивного анализа

Цель работы

Применение методов и технологий испытания программного и аппаратного уровней комплексной защиты информации для проведения атаки на КИС с целью установления уязвимостей

Отчет должен включать в себя следующие разделы:

- формулировку задания;
- описание основных методов, используемых в лабораторной работе;
- результаты работы (в виде файла или в виде скриншота);
- анализ результатов.

ЛАБОРАТОРНАЯ РАБОТА № 14

Тема: Обнаружение уязвимостей по сигнатурам

Цель работы

Применение методов и технологий испытания программного и аппаратного уровней комплексной защиты информации для проведения атаки на КИС с целью установления уязвимостей

Отчет должен включать в себя следующие разделы:

- формулировку задания;
- описание основных методов, используемых в лабораторной работе;
- результаты работы (в виде файла или в виде скриншота);
- анализ результатов.

ЛАБОРАТОРНАЯ РАБОТА № 15

Тема: Оценка уязвимости коммутируемого доступа

Цель работы:

Применение методов и технологий испытания программного и аппаратного уровней комплексной защиты информации для проведения атаки на КИС с целью установления уязвимостей.

Отчет должен включать в себя следующие разделы:

- формулировку задания;
- описание основных методов, используемых в лабораторной работе;
- результаты работы (в виде файла или в виде скриншота);
- анализ результатов.

ЛАБОРАТОРНАЯ РАБОТА № 16

Тема: Анализ угроз и рисков комплексной защиты информации на объекте с использованием системы «Гриф»

Цель работы

Применение принципов организации, проектирования и анализа систем защиты информации и основ их комплексного построения на различных уровнях защиты.

Отчет должен включать в себя следующие разделы:

- формулировку задания;
- описание основных методов, используемых в лабораторной работе;
- результаты работы (в виде файла или в виде скриншота);
- анализ результатов.

ЛАБОРАТОРНАЯ РАБОТА № 17

Тема: Анализ и управление политикой информационной безопасности на объекте с использованием системы «Кондор»

Цель работы

Применение принципов организации, проектирования и анализа систем защиты информации и основ их комплексного построения на различных уровнях защиты.

Отчет должен включать в себя следующие разделы:

- формулировку задания;
- описание основных методов, используемых в лабораторной работе;
- результаты работы (в виде файла или в виде скриншота);
- анализ результатов.

ЛАБОРАТОРНАЯ РАБОТА № 18

Тема: Аудит комплексной защиты информации предприятия

Цель работы

Применение принципов организации, проектирования и анализа систем защиты информации и основ их комплексного построения на различных уровнях защиты.

Отчет должен включать в себя следующие разделы:

- формулировку задания;
- описание основных методов, используемых в лабораторной работе;
- результаты работы (в виде файла или в виде скриншота);
- анализ результатов.

Критерии и шкала оценивания по оценочному средству лабораторная работа

Шкала оценивания (интервал баллов)	Критерий оценивания
5	Лабораторная работа выполнена на высоком уровне (правильность выполнения 90-100%)
4	Лабораторная работа выполнена на среднем уровне (правильность выполнения 75-89%)
3	Лабораторная работа выполнена на низком уровне (правильность выполнения 50-74%)
2	Лабораторная работа выполнена на неудовлетворительном уровне (правильность выполнения менее чем на 50%)

Вопросы к контрольной работе:

1. В чем состоят источники угроз интересам личности?
2. В чем состоят источники угроз интересам общества?
3. В чем состоят источники угроз интересам государства?
4. Перечислите виды информации и основные методы ее защиты.
5. В чем состоят национальные интересы Российской Федерации в информационной сфере и их что собой представляет их обеспечение.
6. Раскройте понятие информационно-безопасного шифрования.

7. В чем состоит сложность использования симметричных криптографических систем?

8. В чем заключаются слабости решения с помощью псевдослучайных генераторов чисел?

9. Приведите несколько примеров применения одноразовых блокнотов.

10. Расскажите о методах противодействия данной атаке.

11. Аутентификация субъектов в распределенных системах, проблемы и решения. Схема Kerberos.

12. Аудит в информационных системах. Функции и назначение аудита, его роль в обеспечении информационной безопасности.

13. Понятие электронной цифровой подписи. Процедуры формирования цифровой подписи.

14. Законодательный уровень применения цифровой подписи.

15. Методы несимметричного шифрования. Использование несимметричного шифрования для обеспечения целостности данных.

16. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.

17. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.

18. Средства обеспечения информационной безопасности в ОС Windows. Разграничение доступа к данным. Групповая политика.

19. Применение файловой системы NTFS для обеспечения информационной безопасности в Windows. Списки контроля доступа к данным (ACL) их роль в разграничении доступа к данным.

20. Применение средств Windows для предотвращения угроз раскрытия конфиденциальности данных. Шифрование данных. Функции и назначение EFS.

21. Разграничение доступа к данным в ОС семейства UNIX.

Критерии и шкала оценивания по оценочному средству контрольная работа

Шкала оценивания (интервал баллов)	Критерий оценивания
5	Контрольная работа выполнена на высоком уровне (правильные ответы даны на 90-100% вопросов/задач)
4	Контрольная работа выполнена на среднем уровне (правильные ответы даны на 75-89% вопросов/задач)
3	Контрольная работа выполнена на низком уровне (правильные ответы даны на 50-74% вопросов/задач)
2	Контрольная работа выполнена на неудовлетворительном уровне (правильные ответы даны менее чем на 50%)

Оценочные средства для промежуточной аттестации (зачет)

1. Перечислите источники угроз безопасности информационного общества.

2. В чем заключается угроза распространения и утечки информации? Какие еще угрозы Вы знаете?

3. Объясните понятие аудита в контексте безопасности вычислительных систем.

4. С помощью какого механизма ОС MS-DOS поддерживает одновременную работу нескольких программ?

5. Как реализовать перехват прерывания средствами языка Си?

6. В чем заключается задача аудита клавиатуры?

7. Как реализовать аудит клавиатуры в ОС MS-DOS?

8. Что необходимо для эффективного применения комплекса и поддержания соответствующего уровня защищенности ПЭВМ и информационных ресурсов?

9. В виде каких взаимодействующих между собой подсистем можно пред-ставить средства разграничения доступа к ресурсам?

10. Что такое процедура идентификации?

11. Что такое процедура аутентификации?

12. Что означает использование дискреционного принципа управления доступом?

13. Что означает использование мандатного принципа управления доступом?

14. Для чего предназначена подсистема регистрации и учета?

15. Что фиксируется в системном журнале при регистрации событий?

16. Для чего предназначена подсистема обеспечения целостности?

17. Что такое проверка на целостность?

18. Какие средства называются аппаратными?

19. Что такое несанкционированный доступ?

20. Что происходит при непосредственном несанкционированном доступе?

Критерии и шкала оценивания по оценочному средству промежуточный контроль (зачет)

Характеристика знания предмета и ответов	Зачеты
Студент глубоко и в полном объѐме владеет программным материалом. Грамотно, исчерпывающе и логично его излагает в устной или письменной форме. При этом знает рекомендованную литературу, проявляет творческий подход в ответах на вопросы и правильно обосновывает принятые решения, хорошо владеет умениями и навыками при выполнении практических задач.	зачтено

Студент знает программный материал, грамотно и по сути излагает его в устной или письменной форме, допуская незначительные неточности в утверждениях, трактовках, определениях и категориях или незначительное количество ошибок. При этом владеет необходимыми умениями и навыками при выполнении практических задач.	
Студент знает только основной программный материал, допускает неточности, недостаточно чѐткие формулировки, непоследовательность в ответах, излагаемых в устной или письменной форме. При этом недостаточно владеет умениями и навыками при выполнении практических задач. Допускает до 30% ошибок в излагаемых ответах.	
Студент не знает значительной части программного материала. При этом допускает принципиальные ошибки в доказательствах, в трактовке понятий и категорий, проявляет низкую культуру знаний, не владеет основными умениями и навыками при выполнении практических задач. Студент отказывается от ответов на дополнительные вопросы.	не зачтено

Лист изменений и дополнений

№ п/п	Виды дополнений и изменений	Дата и номер протокола заседания кафедры (кафедр), на котором были рассмотрены и одобрены изменения и дополнения	Подпись (с расшифровкой) заведующего кафедрой (заведующих кафедрами)

Экспертное заключение

Представленный фонд оценочных средств (далее - ФОС) *по дисциплине «Теория информации и обеспечение информационной безопасности»* соответствует требованиям ФГОС ВО.

Предлагаемые формы и средства текущего и промежуточного контроля адекватны целям и задачам реализации основной образовательной программы по направлению подготовки 09.04.03 Прикладная информатика.

Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы обучающегося представлены в полном объеме.

Виды оценочных средств, включенные в представленный фонд, отвечают основным принципам формирования ФОС.

Разработанный и представленный для экспертизы фонд оценочных средств рекомендуется к использованию в процессе подготовки магистров, по указанному направлению.

Председатель учебно-методической комиссии факультета компьютерных систем и информационных технологий Ветрова Н. Н.