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.
«17» 04 2023 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по учебной дисциплине
Безопасность информационных технологий
(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.

Луганск – 2023 г.

Паспорт
фонда оценочных средств по учебной дисциплине
«Безопасность информационных технологий»

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	ПК-3	способен проектировать информационные процессы и системы с использованием инновационных инструментальных средств	Тема 1. Информационная безопасность и уровни ее обеспечения Тема 2 Стандарты информационной безопасности: "Общие критерии" Тема 3. Стандарты информационной безопасности распределенных систем Тема 4. Классификация угроз "информационной безопасности" Тема 5. Компьютерные вирусы и защита от них Тема 6.Классификация компьютерных вирусов Тема 7. Характеристика "вирусоподобных" программ Тема 8 Антивирусные программы Тема 9. Механизмы обеспечения "информационной безопасности" Тема 10. Криптография и шифрование	2

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.	ПК-3	ПК-3.1. Знать: инновационные	Тема 1. Информационная	Вопросы для обсуждения (в

		инструментальные средства ИТ-сферы ПК-3.2. Уметь: проектировать информационные процессы и системы с использованием инновационных инструментальных средств ПК-3.3. Владеть: навыками проектирования информационных процессов и систем с использованием инновационных инструментальных средств	безопасность и уровни ее обеспечения Тема 2 Стандарты информационной безопасности: "Общие критерии" Тема 3. Стандарты информационной безопасности распределенных систем Тема 4. Классификация угроз "информационной безопасности" Тема 5. Компьютерные вирусы и защита от них Тема 6.Классификация компьютерных вирусов Тема 7. Характеристика "вирусоподобных" программ Тема 8 Антивирусные программы Тема 9. Механизмы обеспечения "информационной безопасности" Тема 10. Криптография и шифрование	виде докладов и сообщений), лабораторные работы, контрольные работы, индивидуальные задания

Фонды оценочных средств по дисциплине «Безопасность информационных технологий»

Вопросы для обсуждения (в виде докладов и сообщений):

1. Подходы к обеспечению информационной безопасности.
2. Принципы обеспечения информационной безопасности.
3. Формальные модели доступа к данным.
4. Монитор безопасности и его функции.

5. Административный уровень защиты информации.
6. Разработка и реализация политики безопасности.
7. Таксономия нарушений информационной безопасности вычислительной системы
8. Анализ способов нарушений безопасности.
9. Основные нормативные руководящие документы
10. Подходы к обеспечению информационной безопасности.
11. Принципы обеспечения информационной безопасности.
12. Формальные модели доступа к данным.
13. Монитор безопасности и его функции.
14. Административный уровень защиты информации.
15. Концепция информационной безопасности.

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

Для формирования у студентов профессиональных компетенций по данной дисциплине все лабораторные работы разбиты на три группы по типу используемых систем защиты информации (СЗИ): DallasLock 7.5, АККОРД-NT/2000 V3.0, SecretNet 5.0, и объединяются в лабораторный практикум. При этом каждая группа лабораторных работ представляет собой законченную систему, в которой даются теоретические сведения о составе данной СЗИ, функциональных возможностях, описываются принципы работы и особенности настройки основных подсистем СЗИ.

Лабораторный практикум включает 9 лабораторных работ:

1. Система защиты информации «SecretNet 5.0».
2. Обеспечение разграничения доступа к защищаемой информации средствами «SecretNet 5.0».
3. Построение системы защиты на базе СЗИ «SecretNet 5.0».
4. Знакомство с программно-аппаратным комплексом средств защиты

информации от несанкционированного доступа «АККОРД-NT/2000».

5. Построение системы защиты на основе комплекса «АККОРД-NT/2000».

6. Аудит безопасности в СЗИ «АККОРД-NT/2000».

7. Система защиты DallasLock 7.5. Состав и функциональные возможности.

8. Механизмы управления доступом и защиты объектов в системе DallasLock 7.5.

9. Аудит безопасности средствами СЗИ DallasLock 7.5.

Таким образом, изучив теоретическую часть каждой лабораторной работы из практикума и выполнив практические задания, студенты смогут обоснованно подойти к выбору того или иного средства защиты и грамотно использовать выбранное средство для решения профессиональных задач в соответствии с видами профессиональной деятельности и профилем подготовки.

Лабораторная работа №1
Система защиты информации «SecretNet 5.0»

Цель: Ознакомиться с системой «SecretNet 5.0». Изучить основные функциональные возможности системы.

Практическое задание

1. Установить СЗИ «SecretNet 5.0» на образ виртуальной машины.
2. Загрузить образ СЗИ «SecretNet 5.0» и зарегистрироваться в системе пользователем Администратор.
3. Пароль Администратора получить от преподавателя в индивидуальном порядке.

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
Обеспечение разграничения доступа к защищаемой информации средствами «SecretNet 5.0»

Цель: Изучить и получить навыки работы с подсистемой разграничения доступа к ресурсам СЗИ «SecretNet 5.0».

Практическая часть

1. Создать учетные записи пользователей: User1, User2, User3, User4, Пароли выбрать произвольно.
2. В соответствии с рисунком создать иерархическую структуру каталогов.

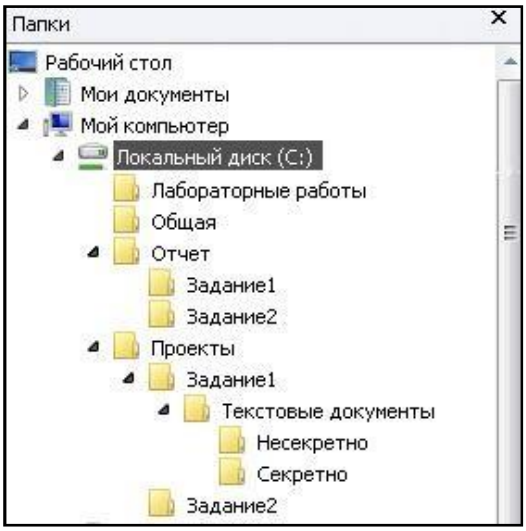

Рис. Дерево каталогов

3. Разграничить права доступа пользователей к созданным каталогам. 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
Построение системы защиты на базе СЗИ «SecretNet 5.0»

Цель: Изучить принципы работы основных защитных функций СЗИ «SecretNet 5.0».

Практическая часть

1. Зарегистрироваться администратором с несекретным уровнем допуска. Запустить программу «Контроль программ и данных». Для включения режима «Замкнутая программная среда» установить галочку «Режим ЗПС включен» на закладке «Субъекты управления» – «Имя компьютера» – «Свойства» – «Режимы».

2. Активировать режимы «Проверить целостность модулей перед запуском» и «Проверять заголовки модулей перед запуском».

3. Отключить «Мягкий режим».

4. Настроить для указанных пользователей замкнутую программную среду таким образом, чтобы он не мог запускать указанные «запрещенные приложения», но мог запускать разрешенные.

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
Знакомство с программно-аппаратным комплексом средств защиты информации от несанкционированного доступа

«АККОРД-NT/2000»

Цель: Ознакомиться с системой СЗИ от НСД «АККОРД- NT/2000». Изучить процесс установки и удаления.

Практическая часть

1. Установите СЗИ НСД Аккорд-NT/2000 на компьютер.
2. Настройте параметры загрузки программы «Аккорд».
3. Проведите временное отключение системы защиты «Аккорд».

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
Построение системы защиты на основе комплекса «АККОРД-NT/2000»

Цель: Изучить основные защитные функции программно- аппаратного комплекса защиты от НСД «Аккорд-NT/2000».

Практическая часть

1. Создайте пользователей в системе User1, User2, User3, User4, присвойте им персональные идентификаторы и задайте пароли (выбрать произвольно с учетом требований сложности).
2. Ограничьте время доступа пользователей в систему.

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
Аудит безопасности в СЗИ «АККОРД-NT/2000»

Цель: Изучить подсистему регистрации событий в системе СЗИ от НСД «Аккорд-NT/2000».

Практическая часть

Перезагрузить компьютер, зарегистрироваться пользователем, указанным в таблице.

Таблица

Задание

	Вариант 1	Вариант 2	Вариант 3	Вариант 4	Вариант 5	Вариант 6
Пользователь	User2	User1	User3	User4	User2	User1

Затем выйти из системы. Зарегистрироваться пользователем Администратор, открыть файл журнала событий с информацией о сеансе предыдущего пользователя. Какие категории событий отражены в журнале?

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 Система защиты DallasLock 7.5. Состав и функциональные возможности

Цель: Ознакомиться с системой защиты DallasLock 7.5.

Практическая часть

Установка системы защиты DallasLock 7.5 на компьютер.

Для размещения файлов и работы DallasLock 7.5 требуется не менее 30 Мбайт пространства на системном разделе жесткого диска. При варианте установки DallasLock 7.5 в раздел требуется не менее 7 Мбайт не распределенного (unpartitioned) пространства на загрузочном жестком диске.

Также при установке СЗИ DallasLock 7.5 необходимо учитывать следующие ограничения, накладываемые системой:

1. При наличии на компьютере нескольких разделов операционная система и СЗИ должны быть установлены на диск C:.
2. Установка СЗИ всегда производится в каталог C:\DlLock75.
3. Для установки СЗИ необходимо обладать правами администратора.
4. На время активации и деактивации СЗИ необходимо отключать антивирусную защиту в BIOS компьютера и программные антивирусные средства.
5. После установки DallasLock нельзя на сервере создавать котроллер домена, то есть DallasLock необходимо устанавливать только после создания контроллера домена.
6. Инсталлировать систему защиты может только пользователь, обладающий правами администратора. Это должен быть локальный пользователь. Пользователь, установивший СЗИ, автоматически становится привилегированным пользователем – суперадминистратором. Рекомендуется запомнить имя и пароль этого пользователя, так как некоторые операции можно выполнить только из-под его учетной записи. Изменять (переименовывать) имя суперадминистратора запрещено.

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

Механизмы управления доступом и защиты объектов в системе DallasLock 7.5

Цель: Получить навыки работы со средствами защиты данных системы DallasLock 7.5.

Практическая часть

1. Создайте 5 пользователей (User1 – User5) и зарегистрируйте их в СЗИ DallasLock 7.5. Настройте для каждого свою парольную политику и срок действия учетной записи, включите пользователей в различные группы.
2. Присвойте каждому пользователю свой уровень доступа.
3. Создайте для каждого пользователя свои именные каталоги и настройте для них мандатную политику доступа.
4. Настройте механизм, позволяющий предотвратить понижение уровня секретности данных.
5. Настройте политику очистки остаточной информации следующим образом:
   Количество циклов затирания:
   - очищать выделяемую память;
   - очищать освобождаемое дисковое пространство;
   - очистка файла подкачки виртуальной памяти;

- принудительная зачистка файлов и папок.

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
Аудит безопасности средствами СЗИ DallasLock7.5

Цель: Изучить средства протоколирования событий, происходящих в системе.

Практическая часть

1. Создать папку Test в каталоге C:\Documents\.
2. Установить «регистрировать для всех пользователей попытки доступа к файлам в этой папке».
3. Для личной папки пользователя включите аудит только успешной записи.
4. Для каждого из журналов регистрации событий установить свой размер.
5. Для журнала доступа к ресурсам установить фильтрацию по имени пользователя

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 контрольным работам:

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.

11. Критерии оценки безопасности компьютерных систем («Оранжевая книга»). Структура требований безопасности. Классы защищенности.

12. Основные положения руководящих документов Гостехкомиссии России. Классификация автоматизированных систем по классам защищенности. Показатели защищенности средств вычислительной техники от несанкционированного доступа.

13. Единые критерии безопасности информационных технологий. Понятие профиля защиты. Структура профиля защиты.

14. Единые критерии безопасности информационных технологий. Проект защиты. Требования безопасности (функциональные требования и требования адекватности).

15. Административный уровень защиты информации. Задачи различных уровней управления в решении задачи обеспечения информационной безопасности.

16. Процедурный уровень обеспечения безопасности. Авторизация пользователей в информационной системе.

17. Идентификация и аутентификация при входе в информационную систему. Использование парольных схем. Недостатки парольных схем.

18. Идентификация и аутентификация пользователей. Применение программно-аппаратных средств аутентификации (смарт-карты, токены).

19. Биометрические средства идентификации и аутентификации пользователей.

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

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%)

Индивидуальные задания

Для выполнения индивидуального задания необходимо:

Подготовить реферат согласно требованиям по выбранным вопросам. Каждый студент получает вопросы из предложенных разделов, согласно таблице составленной преподавателем.

Требования к выполнению реферата

Реферат готовится в текстовом процессоре и должен содержать ответы на вопросы из предложенных разделов. Объем реферата - не менее десяти страниц машинописного текста. Титульный лист оформляется по стандарту, далее следует содержание (оглавление) работы, сформированное автоматически.

В тексте устанавливаются поля: слева - 20 мм, справа – 15 мм, сверху – 15 мм, снизу – 20 мм, выравнивание по ширине. Шрифт текста - Times New Roman, размер шрифта – 12, начертание – обычный, интервал - полуторный. Для заголовков установить размер шрифта - 14, начертание – полужирный, курсив, выравнивание по центру. Абзац начинается с красной строки с отступом 15 мм, нумерация страниц начинается с 3 номера, внизу, по центру, арабскими цифрами. По всему тексту вставить 4 тематических рисунка, таблицы, диаграммы или графики. В конце указать список используемых источников.

1. Представить реферат в распечатанном и электронном вариантах.
2. По вопросам реферата подготовить презентацию, использовать не менее 10 слайдов.
3. Реферат и презентацию представить преподавателю в указанный срок.

Индивидуальное задание состоит из двух теоретических вопросов. Принцип выбора вопросов. Первый - по номеру в студенческом журнале, второй – номер студента в журнале +10.

Перечень вопросов

1. Кратко сформулируйте виды безопасности для соответствующих сфер жизнедеятельности личности, общества и государства.
2. В чем состоят источники угроз интересам личности?
3. В чем состоят источники угроз интересам общества?
4. Что положено в основу дискреционной модели доступа?
5. Раскройте понятие троянской программы в контексте защиты информации в вычислительной системе.
6. Какова роль субъектов и объектов в операционной системе?
7. Перечислите источники угроз безопасности информационного общества.

8. В чем заключается угроза раскрытия информации? Какие еще угрозы Вы знаете?

9. Что положено в основу мандатной модели доступа?

10. Раскройте структуру понятия «безопасность национальных интересов в информационной сфере».

11. В чем заключается угроза нарушения целостности информации? Какие еще угрозы Вы знаете?

12. Для чего предназначены идентификация и аутентификация в вычислительной системе?

13. Каковы основные направления обеспечения информационной безопасности объектов информационной сферы государства?

14. Дайте классификацию методов нарушения конфиденциальности, целостности и доступности информации.

15. В чем заключается атака переполнения буфера?

16. Перечислите источники угроз безопасности информационного общества.

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

18. Объясните понятие аудита в контексте безопасности вычислительных систем.

19. Для чего предназначена подсистема обеспечения целостности?

20. Что такое проверка на целостность?

21. Какие средства называются аппаратными?

22. Что такое несанкционированный доступ?

Критерии и шкала оценивания по оценочному средству индивидуальное задание

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

Оценочные средства для промежуточной аттестации (экзамен)

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

2. Понятие электронной цифровой подписи. Процедуры формирования цифровой подписи.

3. Законодательный уровень применения цифровой подписи.

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

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

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

7. Средства обеспечения информационной безопасности в ОС Windows'2000. Разграничение доступа к данным. Групповая политика.

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

9. Применение средств ОС для предотвращения угроз раскрытия конфиденциальности данных. Шифрование данных. Функции и назначение EFS.

10. Разграничение доступа к данным в ОС семейства UNIX.

11. Пользователи и группы в ОС UNIX.

12. Пользователи и группы в ОС Windows.

13. Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.

14. Причины нарушения безопасности информации при ее обработке криптографическими средствами.

15. Понятие атаки на систему информационной безопасности. Особенности локальных атак.

16. Распределенные информационные системы. Удаленные атаки на информационную систему.

17. Каналы передачи данных. Утечка информации. Атаки на каналы передачи данных.

18. Физические средства обеспечения информационной безопасности.

19. Электронная почта. Проблемы обеспечения безопасности почтовых сервисов и их решения.

20. Вирусы и методы борьбы с ними. Антивирусные программы и пакеты.

21. Программно-аппаратные защиты информационных ресурсов в Интернет. Межсетевые экраны, их функции и назначения.

22. Виртуальные частные сети, их функции и назначение.

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

Шкала оценивания (интервал баллов)	Критерий оценивания
отлично (5)	Студент глубоко и в полном объёме 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.
хорошо (4)	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.
удовлетворительно (3)	Студент знает только основной программный материал, допускает неточности, недостаточно чёткие 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.
неудовлетворительно (2)	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

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 «Безопасность информационных технологий»* 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.