Министерство образования Иркутской области
Государственное бюджетное профессиональное образовательное учреждение Иркутской области
«Иркутский авиационный техникум»

УТВЕРЖДАЮ
Директор
ГБПОУИО «ИАТ»

_____ Якубовский А.Н.
«08» февраля 2023 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

ОП.15 Безопасность компьютерных систем

специальности

09.02.01 Компьютерные системы и комплексы

Иркутск, 2023

Рассмотрена
цикловой комиссией
КС №5 от 07.02.2023 г.

Председатель ЦК

_____/Н.Р. Карпова /

№	Разработчик ФИО
1	Кондратенко Архип Эдуардович

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Область применения фонда оценочных средств (ФОС)

ФОС по дисциплине является частью программы подготовки специалистов среднего звена по специальности 09.02.01 Компьютерные системы и комплексы

1.2. Место дисциплины в структуре ППССЗ:

ОП.00 Общепрофессиональный цикл.

1.3. Цели и задачи дисциплины – требования к результатам освоения дисциплины

Результаты освоения дисциплины	№ результата	Формируемый результат
Знать	1.1	сущность и понятие информационной безопасности, характеристику ее составляющих
	1.2	место информационной безопасности в системе национальной безопасности страны
	1.3	источники угроз информационной безопасности и меры по их предотвращению
	1.4	современные средства и способы обеспечения информационной безопасности
	1.5	жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи
Уметь	2.1	классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности
	2.2	классифицировать основные угрозы безопасности информации
	2.3	применять основные правила и документы сертификации Российской Федерации
Личностные результаты реализации программы воспитания	4.1	Осознающий себя гражданином России и защитником Отечества, выражающий свою российскую идентичность в поликультурном и многоконфессиональном российском обществе, и современном мировом сообществе. Сознающий свое единство с народом России, с Российским государством, демонстрирующий ответственность за развитие страны. Проявляющий готовность к защите Родины, способный аргументированно отстаивать

		суверенитет и достоинство народа России, сохранять и защищать историческую правду о Российском государстве
	4.2	Проявляющий и демонстрирующий уважение законных интересов и прав представителей различных этнокультурных, социальных, конфессиональных групп в российском обществе; национального достоинства, религиозных убеждений с учётом соблюдения необходимости обеспечения конституционных прав и свобод граждан. Понимающий и деятельно выражающий ценность межрелигиозного и межнационального согласия людей, граждан, народов в России. Выражающий сопричастность к преумножению и трансляции культурных традиций и ценностей многонационального российского государства, включенный в общественные инициативы, направленные на их сохранение
	4.3	Сознающий ценность жизни, здоровья и безопасности. Соблюдающий и пропагандирующий здоровый образ жизни (здоровое питание, соблюдение гигиены, режим занятий и отдыха, физическая активность), демонстрирующий стремление к физическому совершенствованию. Проявляющий сознательное и обоснованное неприятие вредных привычек и опасных наклонностей (курение, употребление алкоголя, наркотиков, психоактивных веществ, азартных игр, любых форм зависимостей), деструктивного поведения в обществе, в том числе в цифровой среде
	4.4	Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации

1.4. Формируемые компетенции:

ОК.1 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК.2 Использовать современные средства поиска, анализа и интерпретации

информации, и информационные технологии для выполнения задач профессиональной деятельности
ОК.3 Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях
ОК.6 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения
ОК.9 Пользоваться профессиональной документацией на государственном и иностранном языках

2. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ, ИСПОЛЬЗУЕМЫЙ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ

2.1 Текущий контроль (ТК) № 1

Тема занятия: 1.3.4.Итоговое занятие по теме "Введение в информационную безопасность".

Метод и форма контроля: Письменный опрос (Опрос)

Вид контроля: Проверочная работа

Дидактическая единица: 1.1 сущность и понятие информационной безопасности, характеристику ее составляющих

Занятие(-я):

1.1.1.Основные понятия информационной безопасности.

1.1.2.Анализ угроз информационной безопасности.

1.2.2.Сущность и понятие информационной безопасности. Принципы обеспечения информационной безопасности.

1.2.4.Доктрина информационной безопасности Российской Федерации.

Задание №1

Дать определение "информационной безопасности","защита информации", "Доступность", "целостность информации", "конфиденциальность информации".

Оценка	*Показатели оценки*
3	Дано определение 3-м понятиям.
4	Дано определение 4-м понятиям.
5	Дано определение 5-и понятиям.

Дидактическая единица: 1.2 место информационной безопасности в системе национальной безопасности страны

Занятие(-я):

1.1.2.Анализ угроз информационной безопасности.

1.2.1.Информационная безопасность в системе национальной безопасности Российской Федерации.

1.2.3.Основные положения государственной информационной политики России.

1.2.4.Доктрина информационной безопасности Российской Федерации.

Задание №1

1. Дать определение "угроза", "окно опасности". Дать классификацию угроз.
2. Дать определение - "вредоностное ПО",привести пример.
3. "Основные угрозы целостности" - дать определение, привести пример. "Угроза конфиденциальности" - дать определение.

Оценка	*Показатели оценки*
3	Выполнен один пункт задания.
4	Выполнено два пункта задания.
5	Выполнено три пункта задания.

Дидактическая единица: 2.1 классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности
Занятие(-я):
1.2.1.Информационная безопасность в системе национальной безопасности Российской Федерации.
1.2.2.Сущность и понятие информационной безопасности. Принципы обеспечения информационной безопасности.
1.2.3.Основные положения государственной информационной политики России.
1.2.4.Доктрина информационной безопасности Российской Федерации.
1.2.5.Анализ Доктрины информационной безопасности Российской Федерации.
Задание №1

1. Описать методы оценки уязвимости информации. Виды утечки информации.
2. Используя "Доктрину информационной безопасности РФ" описать уровни информационной безопасности РФ.
3. Дать определение : лицензия, лицензирующие органы (привести примеры), электронная цифровая подпись (открытая и закрытая).

Оценка	*Показатели оценки*
3	Выполнен один пункт задания.
4	Выполнено два пункта задания.
5	Выполнено три пункта задания.

2.2 Текущий контроль (ТК) № 2

Тема занятия: 3.1.8.Средства и способы обеспечения информационной безопасности.
Метод и форма контроля: Письменный опрос (Опрос)
Вид контроля: Проверочная работа
Дидактическая единица: 1.4 современные средства и способы обеспечения информационной безопасности
Занятие(-я):
1.2.1.Информационная безопасность в системе национальной безопасности Российской Федерации.

1.2.3.Основные положения государственной информационной политики России.
1.2.4.Доктрина информационной безопасности Российской Федерации.
1.2.5.Анализ Доктрины информационной безопасности Российской Федерации.
1.3.2.Методы оценки уязвимости информации. Виды утечки информации.
1.3.3.Информация как объект защиты.
1.3.4.Итоговое занятие по теме "Введение в информационную безопасность".
2.1.1.Понятие конфиденциальной информации.
2.1.2.Классификация конфиденциальной информации по видам тайны и степени конфиденциальности.
2.1.4.Защита информации составляющей государственную тайну.
2.1.5.Защита информации, охраняемая авторским и патентным правом.
2.1.6.Анализ защищенности объекта защиты информации.
3.1.1.Интегральная безопасность. Угрозы безопасности автоматизированных систем обработки данных (АСОД).
3.1.2.Стандарты в области информационной безопасности АСОД.
3.1.3.Показатели защищенности СВТ. Защита информации в АСОД.
3.1.4.Методы и системы защиты информации. Виды доступа. Уровни доступа. Контроль доступа.
3.1.5.Автоматизированная система, как объект информационной защиты.
3.1.6.Основные методы и приемы защиты от несанкционированного доступа.
3.1.7.Методы и средства защиты информации.

Задание №1

1. Дать определение авторское и потентное право.
2. Описать угрозы безопасности автоматизированных систем обработки данных (естественные угрозы,искусственные угрозы,непреднамеренные угрозы, преднамеренные угрозы).
3. Написать стандарты в области информационной безопасности автоматизированных систем обработки данных . Описать показатели защищенности СВТ.

Оценка	***Показатели оценки***
3	Выполнен один пункт задания.
4	Выполнено два пункта задания.
5	Выполнено три пункта задания.

Дидактическая единица: 1.3 источники угроз информационной безопасности и меры по их предотвращению

Занятие(-я):

1.2.3.Основные положения государственной информационной политики России.
1.2.4.Доктрина информационной безопасности Российской Федерации.
1.2.5.Анализ Доктрины информационной безопасности Российской Федерации.
1.3.1.Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации.
1.3.2.Методы оценки уязвимости информации. Виды утечки информации.
1.3.4.Итоговое занятие по теме "Введение в информационную безопасность".
2.1.1.Понятие конфиденциальной информации.
2.1.2.Классификация конфиденциальной информации по видам тайны и степени конфиденциальности.
3.1.5.Автоматизированная система, как объект информационной защиты.

Задание №1

1. Понятие конфиденциальной информации, классификация, степени конфиденциальности.
2. Описать жизненные циклы конфиденциальной информации.
3. Понятие "государственная тайна". Описать способы защиты государственной информации.

Оценка	***Показатели оценки***
3	Выполнен один пункт задания.
4	Выполнено два пункта задания.
5	Выполнено три пункта задания.

Дидактическая единица: 2.2 классифицировать основные угрозы безопасности информации

Занятие(-я):

1.1.1.Основные понятия информационной безопасности.
1.1.2.Анализ угроз информационной безопасности.
1.2.1.Информационная безопасность в системе национальной безопасности Российской Федерации.
1.2.3.Основные положения государственной информационной политики России.
1.2.4.Доктрина информационной безопасности Российской Федерации.
1.2.5.Анализ Доктрины информационной безопасности Российской Федерации.
1.3.1.Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации.
1.3.2.Методы оценки уязвимости информации. Виды утечки информации.
1.3.4.Итоговое занятие по теме "Введение в информационную безопасность".
2.1.1.Понятие конфиденциальной информации.

2.1.2.Классификация конфиденциальной информации по видам тайны и степени конфиденциальности.

Задание №1

1. Описать методы и системы защиты информации.
2. Написать виды доступа,уровни доступа. Дать определение - контроль доступа.
3. Описать основные методы и приемы защиты от несанкционированного доступа.

Оценка	*Показатели оценки*
3	Выполнен один пункт задания.
4	Выполнено два пункта задания.
5	Выполнено три пункта задания.

2.3 Текущий контроль (ТК) № 3

Тема занятия: 3.3.10.Анализ защищенности объекта защиты информации.

Метод и форма контроля: Письменный опрос (Опрос)

Вид контроля: Проверочная работа

Дидактическая единица: 1.4 современные средства и способы обеспечения информационной безопасности

Занятие(-я):

3.1.8.Средства и способы обеспечения информационной безопасности.

3.2.1.Проблема вирусного заражения программ. Классификация вирусов. Способы заражения программ.

3.2.2.Структура современных вирусных программ. Перспективные методы антивирусной защиты. Основные классы антивирусных программ.

3.3.3.Методы анализа сетевой информации.

3.3.4.Проблемы безопасности IP-сетей. Угрозы и уязвимости проводных корпоративных сетей. Угрозы и уязвимости беспроводных сетей.

3.3.5.Основы сетевого и межсетевого взаимодействия.

3.3.6.Технологии межсетевых экранов. Требования и показатели защищенности межсетевых экранов. Схемы сетевой защиты на базе межсетевых экранов.

3.3.7.Политика безопасности. Сетевая политика безопасности.

3.3.8.Классификация систем обнаружения атак. Компоненты и архитектура системы обнаружения атак. Особенности обнаружения атак на сетевом и операционном уровне. Реагирование на атаку.

3.3.9.Обзор современных средств обнаружения атак.

Задание №1

1. Дать определение - вирус. Описать классификация вирусов и способы заражения.
2. Дать определение - анитивирус. Описать основные классы антивирусных программ.
3. Написать средства анализа защищенности сетевых протоколов и ОС. Перечислить требования к антивирусам.

Оценка	*Показатели оценки*
3	Выполнен один пункт задания.
4	Выполнено два пункта задания.
5	Выполнено три пункта задания.

Дидактическая единица: 1.5 жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи

Занятие(-я):

1.2.4.Доктрина информационной безопасности Российской Федерации.
1.3.3.Информация как объект защиты.
1.3.4.Итоговое занятие по теме "Введение в информационную безопасность".
2.1.3.Жизненные циклы конфиденциальной информации.
2.1.5.Защита информации, охраняемая авторским и патентным правом.
2.1.6.Анализ защищенности объекта защиты информации.
3.1.1.Интегральная безопасность. Угрозы безопасности автоматизированных систем обработки данных (АСОД).
3.1.2.Стандарты в области информационной безопасности АСОД.
3.1.3.Показатели защищенности СВТ. Защита информации в АСОД.
3.1.4.Методы и системы защиты информации. Виды доступа. Уровни доступа. Контроль доступа.
3.1.6.Основные методы и приемы защиты от несанкционированного доступа.
3.1.7.Методы и средства защиты информации.
3.2.2.Структура современных вирусных программ. Перспективные методы антивирусной защиты. Основные классы антивирусных программ.
3.3.1.Адаптивное управление безопасностью.
3.3.2.Средства анализа защищенности сетевых протоколов. Средства анализа защищенности операционной системы. Общие требования к выбираемым средствам анализа защищенности.
3.3.7.Политика безопасности. Сетевая политика безопасности.

Задание №1

1. Описать проблемы безопасности IP-сетей.
2. Описать угрозы и уязвимости проводных корпоративных сетей.Описать угрозы и уязвимости беспроводных сетей.
3. Пояснить и описать технологии межсетевых экранов. Перечислить показатели защищенности межсетевых экранов.

Оценка	***Показатели оценки***
3	Выполнен один пункт задания.
4	Выполнено два пункта задания.
5	Выполнено три пункта задания.

Дидактическая единица: 2.3 применять основные правила и документы сертификации Российской Федерации

Занятие(-я):

1.2.3.Основные положения государственной информационной политики России.
1.2.4.Доктрина информационной безопасности Российской Федерации.
1.2.5.Анализ Доктрины информационной безопасности Российской Федерации.
1.3.2.Методы оценки уязвимости информации. Виды утечки информации.
1.3.3.Информация как объект защиты.
1.3.4.Итоговое занятие по теме "Введение в информационную безопасность".
2.1.3.Жизненные циклы конфиденциальной информации.
2.1.5.Защита информации, охраняемая авторским и патентным правом.
2.1.6.Анализ защищенности объекта защиты информации.
3.1.1.Интегральная безопасность. Угрозы безопасности автоматизированных систем обработки данных (АСОД).
3.1.2.Стандарты в области информационной безопасности АСОД.
3.1.3.Показатели защищенности СВТ. Защита информации в АСОД.
3.1.4.Методы и системы защиты информации. Виды доступа. Уровни доступа. Контроль доступа.
3.1.5.Автоматизированная система, как объект информационной защиты.
3.1.6.Основные методы и приемы защиты от несанкционированного доступа.
3.1.7.Методы и средства защиты информации.
3.2.1.Проблема вирусного заражения программ. Классификация вирусов. Способы заражения программ.
3.2.2.Структура современных вирусных программ. Перспективные методы антивирусной защиты. Основные классы антивирусных программ.
3.3.1.Адаптивное управление безопасностью.
3.3.2.Средства анализа защищенности сетевых протоколов. Средства анализа защищенности операционной системы. Общие требования к выбираемым средствам анализа защищенности.

3.3.3.Методы анализа сетевой информации.
3.3.4.Проблемы безопасности IP-сетей. Угрозы и уязвимости проводных корпоративных сетей. Угрозы и уязвимости беспроводных сетей.
3.3.5.Основы сетевого и межсетевого взаимодействия.
3.3.6.Технологии межсетевых экранов. Требования и показатели защищенности межсетевых экранов. Схемы сетевой защиты на базе межсетевых экранов.
3.3.8.Классификация систем обнаружения атак. Компоненты и архитектура системы обнаружения атак. Особенности обнаружения атак на сетевом и операционном уровне. Реагирование на атаку.
3.3.9.Обзор современных средств обнаружения атак.

Задание №1

1. Дать определение - "политика безопасности ","сетевая политика безопасности ".
2. Перечислить классификация систем обнаружения атак.
3. Описать компоненты и архитектура системы обнаружения атак.

Оценка	***Показатели оценки***
3	Выполнен один пункт задания.
4	Выполнено два пункта задания.
5	Выполнено три пункта задания.

3. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ, ИСПОЛЬЗУЕМЫЙ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

№ семестра	Вид промежуточной аттестации
7	Экзамен

Экзамен может быть выставлен автоматически по результатам текущих контролей
Текущий контроль №1
Текущий контроль №2
Текущий контроль №3

Метод и форма контроля: Письменный опрос (Опрос)
Вид контроля: по выбору выполнить одно теоретическое задание и одно практическое задание
Дидактическая единица для контроля:
1.1 сущность и понятие информационной безопасности, характеристику ее составляющих
Задание №1 (из текущего контроля)
Дать определение "информационной безопасности","защита информации", "Доступность", "целостность информации", "конфиденциальность информации".

Оценка	*Показатели оценки*
3	Дано определение 3-м понятиям.
4	Дано определение 4-м понятиям.
5	Дано определение 5-и понятиям.

Дидактическая единица для контроля:
1.2 место информационной безопасности в системе национальной безопасности страны
Задание №1 (из текущего контроля)

1. Дать определение "угроза", "окно опасности". Дать классификацию угроз.
2. Дать определение - "вредоностное ПО",привести пример.
3. "Основные угрозы целостности" - дать определение, привести пример. "Угроза конфиденциальности" - дать определение.

Оценка	*Показатели оценки*

3	Выполнен один пункт задания.
4	Выполнено два пункта задания.
5	Выполнено три пункта задания.

Дидактическая единица для контроля:
1.3 источники угроз информационной безопасности и меры по их предотвращению
Задание №1 (из текущего контроля)

1. Понятие конфиденциальной информации, классификация, степени конфиденциальности.
2. Описать жизненные циклы конфиденциальной информации.
3. Понятие "государственная тайна". Описать способы защиты государственной информации.

Оценка	*Показатели оценки*
3	Выполнен один пункт задания.
4	Выполнено два пункта задания.
5	Выполнено три пункта задания.

Дидактическая единица для контроля:
1.4 современные средства и способы обеспечения информационной безопасности
Задание №1 (из текущего контроля)

1. Дать определение авторское и потентное право.
2. Описать угрозы безопасности автоматизированных систем обработки данных (естественные угрозы,искусственные угрозы,непреднамеренные угрозы, преднамеренные угрозы).
3. Написать стандарты в области информационной безопасности автоматизированных систем обработки данных . Описать показатели защищенности СВТ.

Оценка	*Показатели оценки*
3	Выполнен один пункт задания.
4	Выполнено два пункта задания.
5	Выполнено три пункта задания.

Задание №2 (из текущего контроля)

1. Дать определение - вирус. Описать классификация вирусов и способы заражения.
2. Дать определение - анитивирус. Описать основные классы антивирусных программ.
3. Написать средства анализа защищенности сетевых протоколов и ОС. Перечислить требования к антивирусам.

Оценка	*Показатели оценки*
3	Выполнен один пункт задания.
4	Выполнено два пункта задания.
5	Выполнено три пункта задания.

Дидактическая единица для контроля:
1.5 жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи

Задание №1 (из текущего контроля)

1. Описать проблемы безопасности IP-сетей.
2. Описать угрозы и уязвимости проводных корпоративных сетей.Описать угрозы и уязвимости беспроводных сетей.
3. Пояснить и описать технологии межсетевых экранов. Перечислить показатели защищенности межсетевых экранов.

Оценка	*Показатели оценки*
3	Выполнен один пункт задания.
4	Выполнено два пункта задания.
5	Выполнено три пункта задания.

Дидактическая единица для контроля:
2.1 классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности

Задание №1 (из текущего контроля)

1. Описать методы оценки уязвимости информации. Виды утечки информации.

2. Используя "Доктрину информационной безопасности РФ" описать уровни информационной безопасности РФ.
3. Дать определение : лицензия, лицензирующие органы (привести примеры), электронная цифровая подпись (открытая и закрытая).

Оценка	*Показатели оценки*
3	Выполнен один пункт задания.
4	Выполнено два пункта задания.
5	Выполнено три пункта задания.

Дидактическая единица для контроля:
2.2 классифицировать основные угрозы безопасности информации
Задание №1 (из текущего контроля)

1. Описать методы и системы защиты информации.
2. Написать виды доступа,уровни доступа. Дать определение - контроль доступа.
3. Описать основные методы и приемы защиты от несанкционированного доступа.

Оценка	*Показатели оценки*
3	Выполнен один пункт задания.
4	Выполнено два пункта задания.
5	Выполнено три пункта задания.

Дидактическая единица для контроля:
2.3 применять основные правила и документы сертификации Российской Федерации
Задание №1 (из текущего контроля)

1. Дать определение - "политика безопасности ","сетевая политика безопасности ".
2. Перечислить классификация систем обнаружения атак.
3. Описать компоненты и архитектура системы обнаружения атак.

Оценка	*Показатели оценки*
3	Выполнен один пункт задания.

4	Выполнено два пункта задания.
5	Выполнено три пункта задания.