Негосударственное частное образовательное учреждение высшего образования «Технический университет УГМК»

24.02.2021

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Хранение и защита компьютерной информации

Закреплена за кафедрой **механики и автоматизации технологических процессов и производств**

Учебный план 15.04.04-заочная АТПП гр. А-2116з ГОА.plx
15.04.04 Автоматизация технологических процессов и производств
Название магистерской программы: "Цифровизация и автоматизация технологических процессов металлургических и горнодобывающих предприятий"

Квалификация **магистр**

Форма обучения **заочная**

Общая трудоемкость **4 ЗЕТ**

Часов по учебному плану 144
в том числе:
аудиторные занятия 10
самостоятельная работа 130
часов на контроль 4

Виды контроля на курсах:
зачеты 2

Распределение часов дисциплины по курсам

Курс	1		2		Итого	
Вид занятий	УП	РП	УП	РП		
Лекции	2	2			2	2
Практические	2	2	6	6	8	8
Итого ауд.	4	4	6	6	10	10
Контактная	4	4	6	6	10	10
Сам. работа	32	32	98	98	130	130
Часы на			4	4	4	4
Итого	36	36	108	108	144	144

Разработчик программы:
канд. техн. наук, доц. кафедры, Ваулин С.С. _____

Рабочая программа дисциплины
Хранение и защита компьютерной информации

разработана в соответствии с ФГОС ВО:

Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 15.04.04 АВТОМАТИЗАЦИЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ И ПРОИЗВОДСТВ (уровень магистратуры) (приказ Минобрнауки России от 25.11.2020г. №1452)

составлена на основании учебного плана:

15.04.04 Автоматизация технологических процессов и производств
Название магистерской программы: "Цифровизация и автоматизация технологических процессов металлургических и горнодобывающих предприятий"
утвержденного учёным советом вуза от 24.02.2021 протокол № 2.

Рабочая программа одобрена на заседании кафедры
механики и автоматизации технологических процессов и производств

Протокол методического совета университета от 20.02.2021 г. № 1/1
Срок действия программы: 2021-2024 уч.г.
Зав. кафедрой канд. физ.-мат. наук, Худяков П.Ю.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
Целью изучения данной дисциплины является формирование у студентов знаний и навыков в области применения передовых информационных технологий, направленных на защиту информации, хранящейся и обрабатываемой на объекте информатизации.
1.1 Задачи
Задачами изучения дисциплины являются освоение современных средств защиты информации, понимание их принципа работы, и применение данных СЗИ на практике.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Государственная итоговая аттестация
2.2.2	Преддипломная практика
2.2.3	Защита выпускной квалификационной работы
2.2.4	Выполнение, подготовка к процедуре защиты выпускной квалификационной работы

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ПК-1.2: Способен обеспечивать надежность и безопасность на всех этапах жизненного цикла продукции, выбирать системы экологической безопасности производства
ИПК-1.2.3: Владеет навыками создания баз данных, использования проблемно-ориентированных методов анализа, синтеза и оптимизации процессов автоматизации, навыками синтеза цифровых систем управления
ИПК-1.2.2: Умеет осуществлять анализ работы систем контроля за экологической безопасностью производства, выбирать системы экологической безопасности производства
ИПК-1.2.1: Знает правила эксплуатации систем управления, показатели безопасности технических систем, методы и средства обеспечения надежности и безопасности систем экологической безопасности производства

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	1. Знать способы и средства ограничения физического доступа к информации.
3.1.2	2. Знать возможности разграничения доступа различных СЗИ, а также возможности разграничения доступа различных операционных систем.
3.1.3	3. Знать механизмы хранения компьютерной информации.
3.1.4	4. Знать основные способы и средства обеспечения ограничения физического доступа.
3.1.5	5. Знать механизмы идентификации и аутентификации пользователей.
3.1.6	6. Знать различные способы на ограничения доступа на вход в систему.
3.1.7	7. Знать возможности разграничения доступа различных СЗИ, а также возможности разграничения доступа различных операционных систем.
3.1.8	8. Понимать информацию предоставляемую списками регистрации событий.
3.1.9	
3.2	**Уметь:**
3.2.1	1. Ограничить физический доступ к информации.
3.2.2	2. Ограничить доступ на вход в систему.
3.2.3	3. Разграничить доступ.
3.2.4	4. Умение использования средств резервирования данных.
3.2.5	5. Ограничить физический доступ.
3.2.6	6. Обеспечить идентификацию и аутентификацию пользователей.
3.2.7	7. Ограничить доступ на вход в систему.
3.2.8	8.Разграничить доступ.
3.2.9	9. Обеспечить аудит.
3.2.10	10. Обеспечить криптографическую защиту информации.
3.2.11	11. Обеспечить контроль целостности.
3.2.12	12. Обеспечить управление политикой безопасности.
3.2.13	13. Обеспечить антивирусную защиту.

3.2.14	14. Обеспечить резервирование данных.
3.2.15	11. Обеспечить сетевую защиту.
3.2.16	12. Обеспечить защиту от утечки и перехвата информации по техническим каналам.
3.3	**Владеть:**
3.3.1	Навыками:
3.3.2	- ограничивать доступ к информации.
3.3.3	- выявлять попытки несанкционированного доступа к информации.
3.3.4	- полного уничтожения компьютерной информации.
3.3.5	- резервирования данных.
3.3.6	- принимать полный комплекс мер по защите компьютерной информации.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература	Ресурсы	Интеракт.	Примечание
	Раздел 1. Законодательные и правовые основы защиты компьютерной информации.							
1.1	Законодательные и правовые основы защиты компьютерной информации. /Лек/	1	0,5	ИПК-1.2.1 ИПК-1.2.2 ИПК-1.2.3	Л1.1 Л1.2Л2.1 Л2.2	Э1 Э2	0	
1.2	Законодательные и правовые основы защиты компьютерной информации. /Ср/	1	8	ИПК-1.2.1 ИПК-1.2.2 ИПК-1.2.3	Л1.1 Л1.2Л2.1 Л2.2	Э1 Э2	0	
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов**	**Компетенции**	**Литература**	**Ресурсы**	**Интеракт.**	**Примечание**
	Раздел 2. Теоретические основы компьютерной безопасности.							
2.1	Теоретические основы компьютерной безопасности. /Лек/	1	0,5	ИПК-1.2.1 ИПК-1.2.2 ИПК-1.2.3	Л1.1 Л1.2Л2.1 Л2.2	Э1 Э2	0	
2.2	Теоретические основы компьютерной безопасности. /Ср/	1	8	ИПК-1.2.1 ИПК-1.2.2 ИПК-1.2.3	Л1.1 Л1.2Л2.1 Л2.2	Э1 Э2	0	
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов**	**Компетенции**	**Литература**	**Ресурсы**	**Интеракт.**	**Примечание**
	Раздел 3. Современные криптосистемы для защиты компьютерной информации.							
3.1	Современные криптосистемы для защиты компьютерной информации. /Лек/	1	0,5	ИПК-1.2.1 ИПК-1.2.2 ИПК-1.2.3	Л1.1 Л1.2Л2.1 Л2.2	Э1 Э2	0	
3.2	Применение СКЗИ Strong Disk /Пр/	1	1	ИПК-1.2.1 ИПК-1.2.2 ИПК-1.2.3	Л1.1 Л1.2Л2.1 Л2.2	Э1 Э2	0	
3.3	Применение СКЗИ Secret Disk /Пр/	1	1	ИПК-1.2.1 ИПК-1.2.2 ИПК-1.2.3	Л1.1 Л1.2Л2.1 Л2.2	Э1 Э2	0	
3.4	Современные криптосистемы для защиты компьютерной информации. /Ср/	1	8	ИПК-1.2.1 ИПК-1.2.2 ИПК-1.2.3	Л1.1 Л1.2Л2.1 Л2.2	Э1 Э2	0	
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов**	**Компетенции**	**Литература**	**Ресурсы**	**Интеракт.**	**Примечание**
	Раздел 4. Математические основы криптографических методов.							

4.1	Математические основы криптографических методов. /Лек/	1	0,5	ИПК-1.2.1 ИПК-1.2.2 ИПК-1.2.3	Л1.1 Л1.2Л 2.1 Л2.2	Э1 Э2	0	
4.2	Математические основы криптографических методов. /Ср/	1	8	ИПК-1.2.1 ИПК-1.2.2 ИПК-1.2.3	Л1.1 Л1.2Л 2.1 Л2.2	Э1 Э2	0	
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литер атура**	**Ресу рсы**	**Инте ракт.**	**Примечание**
	Раздел 5. Методы идентификации и проверки подлинности пользователей компьютерных систем							
5.1	Методы идентификации и проверки подлинности пользователей компьютерных систем /Ср/	2	24	ИПК-1.2.1 ИПК-1.2.2 ИПК-1.2.3	Л1.1 Л1.2Л 2.1 Л2.2	Э1 Э2	0	
5.2	Применение системы защиты от несанкционированного доступа Dallas Lock /Пр/	2	3	ИПК-1.2.1 ИПК-1.2.2 ИПК-1.2.3	Л1.1 Л1.2Л 2.1 Л2.2	Э1 Э2	0	
5.3	Применение программно-аппаратного комплекса защиты информации от несанкционированного доступа Аккорд -NT/2000 /Пр/	2	3	ИПК-1.2.1 ИПК-1.2.2 ИПК-1.2.3	Л1.1 Л1.2Л 2.1 Л2.2	Э1 Э2	0	
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литер атура**	**Ресу рсы**	**Инте ракт.**	**Примечание**
	Раздел 6. Методы защиты программ от излучения и разрушающих программных воздействий							
6.1	Методы защиты программ от излучения и разрушающих программных воздействий /Ср/	2	25	ИПК-1.2.1 ИПК-1.2.2 ИПК-1.2.3	Л1.1 Л1.2Л 2.1 Л2.2	Э1 Э2	0	
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литер атура**	**Ресу рсы**	**Инте ракт.**	**Примечание**
	Раздел 7. Защита компьютерных сетей от удаленных атак							
7.1	Защита компьютерных сетей от удаленных атак /Ср/	2	24	ИПК-1.2.1 ИПК-1.2.2 ИПК-1.2.3	Л1.1 Л1.2Л 2.1 Л2.2	Э1 Э2	0	
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литер атура**	**Ресу рсы**	**Инте ракт.**	**Примечание**
	Раздел 8. Комплексная защита процесса обработки информации в компьютерных системах							
8.1	Комплексная защита процесса обработки информации в компьютерных системах /Ср/	2	25	ИПК-1.2.1 ИПК-1.2.2 ИПК-1.2.3	Л1.1 Л1.2Л 2.1 Л2.2	Э1 Э2	0	

4.1 Образовательные технологии

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания

Перечень примерных вопросов для зачета:

1. Компьютерная система и защита информации.
2. Методы защиты информации.
3. Идентификация и аутентификация пользователей.
4. Ограничение доступа на вход в систему.
5. Разграничение доступа.
6. Регистрация событий (аудит).

7.	Криптографическая защита.
8.	Контроль целостности.
9.	Управление политикой безопасности.
10.	Уничтожение остаточной информации.
11.	Комплексный подход к защите информации.
12.	Использование криптографических средств для обеспечения безопасности персональных данных.
13.	Требования по организации и обеспечению функционирования шифровальных (криптографических) средств.
14.	Рекомендации по применению криптосредств.
15.	Классификация и общая характеристика программно-аппаратных средств защиты информации.

5.2. Темы письменных работ

Примерный перечень тем контрольных работ

1. Описать различия разграничения доступа в ОС WindowsиLinux.
2. Описать все недостатки программы Страж NT, выявить уязвимости данной программы. Написать свои предложения для оптимизации работы данной программы.
3. Смоделировать предприятие и реализовать модель разграничения доступа с помощью программы Dallas Lock. На предприятии минимум 3 отдела, в каждом отделе есть сотрудники с различным уровнем доступа.
4. Смоделировать предприятие и реализовать модель разграничения доступа с помощью программы Аккорд-NT/2000. На предприятии минимум 3 отдела, в каждом отделе есть сотрудники с различным уровнем доступа.
5. Описать принципы шифрования для всех изученных СКЗИ.

5.3. Фонд оценочных средств

Фонд оценочных средств предназначен для выявления уровня сформированности компетенций по дисциплине. Фонд оценочных средств, состоящий из материалов для текущего контроля и проведения промежуточной аттестации обучающихся, систему оценивания результатов промежуточной аттестации и критерии выставления оценок представлен в УМК дисциплины.

5.4. Перечень видов оценочных средств

Комплексные домашние задания, контрольные работы, тестирование.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Аверченков В. И., Рытов М. Ю.	Служба защиты информации: организация и управление: учебное пособие	Москва: ФЛИНТА, 2016,http://biblioclub.ru/index.php?page=book&id=93356
Л1.2	Свинарев Н. А., Ланкин О. В., Данилкин А. П., Потехецкий С. В., Перетокин О. И.	Инструментальный контроль и защита информации: учебное пособие	Воронеж: Воронежский государственный университет инженерных технологий, 2013,http://biblioclub.ru/index.php?page=book&id=255905

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Сергеева Ю. С.	Защита информации: конспект лекций: учебное пособие	Москва: А-Приор, 2011,http://biblioclub.ru/index.php?page=book&id=72670
Л2.2	Скрипник Д. А.	Общие вопросы технической защиты информации	Москва: Национальный Открытый Университет «ИНТУИТ», 2016,http://biblioclub.ru/index.php?page=book&id=429070

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	http://www2.viniti.ru
Э2	http://cnb.uran.ru/resource/katalog

6.3.1 Перечень программного обеспечения

6.3.1.1	Windows 7
6.3.1.2	Windows 10
6.3.1.3	Google Chrome

6.3.2 Перечень информационных справочных систем

6.3.2.1	Консультант-плюс

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)		
Ауд. №	Назначение	Оснащение
Лекционная аудитория (206 НИЦ, 220, 225, 226, 227, 228, 300, 301, 303, 317, 423,424)	Учебная аудитория для проведения занятий лекционного и семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Учебные места, оборудованные блочной мебелью с расположением амфитеатром. Рабочее место преподавателя в составе стол, стул, тумба, трибунка, компьютер преподавателя, дополнительное устройство отображения: интерактивная доска с проектором или настенная ЖК-панель или маркерная доска с проектором и сенсорным датчиком. Проектор и моторизованный экран. Потолочные поворотные камеры. Документ-камера. Звуковая система. Планшетный компьютер. Флипчарт.
Компьютерная аудитория (209 НИЦ, 210 НИЦ, 308 НИЦ, 324)	Учебная аудитория для проведения занятий лекционного, семинарского, практического типа, курсового проектирования, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации с использованием учебных мест с компьютерами.	Учебные места с компьютерами. Рабочее место преподавателя в составе стол, стул, тумба, компьютер. Интерактивная доска с проектором. Потолочная поворотная камера. Документ-камера. Звуковая система. Компьютеры (моноблоки) с операционной системой Windows
412	Лаборатория Автоматизированных систем управления позволяет решать весь комплекс задач подготовки специалистов по автоматизации непрерывных технологических процессов и производств. Обучающиеся могут выполнить весь набор действий, которые входят в обязанность слесаря по ремонту и обслуживанию полевого уровня АСУ. Обучающиеся могут производить сборку электрических схем подключения датчиков и оборудования к контроллерам, выстраивать различные схемы сетевого обмена между оборудованием, строить модели реальных распределенных АСУТП предприятий. Осуществляется обучение со сложным технологическим процессом с помощью 3D и математических моделей трех технологических процессов непрерывных производств.	Рабочее место преподавателя в составе стол, стул, тумба, компьютер. Потолочная поворотная камера. Документ-камера. Звуковая система. 10 стендов с контроллерами АСУ таких производителей как: Siemens, Schneider Electric, DirectLOGIC, ОВЕН, Mitsubishi и т.д. Каждый стенд оборудован не только контроллерами, но и “мозгом” системы - управляющим компьютером (автоматизированным рабочим местом (АРМ)), панелью оператора и специализированным программным обеспечением. Верхний уровень АСУТП реализован при помощи SCADA-систем производителей контроллеров и сторонних разработчиков, возможно изучение принципов создания проектов для визуализации технологических процессов, архивирования данных и управления технологией на уровне оператора. В лаборатории АСУ ТУ УГМК созданы 3D и математические модели трех технологических процессов непрерывных производств. Лаборатория обладает программным обеспечением, которое является главным направлением развития систем автоматизации, а именно MES-системами. Оборудование объединено в единую систему таким образом, что имеется возможность построения сложной, комплексной системы управления производственными процессами с решением задач оптимизации загрузки оборудования и отдельных систем.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Методические указания для обучающихся по освоению дисциплины
1. Изучение рабочей программы дисциплины.
2. Посещение и конспектирование лекций.
3. Обязательная подготовка к практическим занятиям.
4. Изучение основной и дополнительной литературы, интернет-источников.
5. Выполнение всех видов самостоятельной работы.

Эффективное освоение дисциплины предполагает регулярное посещение всех видов аудиторных занятий, выполнение плана самостоятельной работы в полном объеме и прохождение аттестации в соответствии с календарным учебным графиком.
Студенту рекомендуется ознакомиться со списком основной и дополнительной литературы. Доступ к информационным ресурсам библиотеки и информационно-справочным системам сети "Интернет" организован в читальном зале библиотеки со стационарных ПЭВМ, либо с личного ПЭВМ (ноутбука, планшетного компьютера или иного мобильного устройства) посредством беспроводного доступа при активации индивидуальной учетной записи.
Пользование информационными ресурсами расширяет возможности освоения теоретического курса, выполнения

самостоятельной работы.

Задания и методические указания к выполнению практических занятий составлены в соответствии с рабочей программой дисциплины и представлены в УМК дисциплины.
Практические занятия включают в себя освоение действий, обсуждение проблем по основным разделам курса и направлены на углубление изученного теоретического материала и на приобретение умений и навыков.
При подготовке к практическим занятиям используются методические указания, в которых описаны содержание и методы их проведения, условия выполнения, сформулированы вопросы к результатам выполнения заданий.

Методические рекомендации к организации и выполнению самостоятельной работы составлены в соответствии с рабочей программой дисциплины и представлены в УМК дисциплины.
Самостоятельная работа студентов включает освоение теоретического материала, подготовку к выполнению заданий практических занятий, и подготовку к зачету.

Задания и методические указания к выполнению контрольных работ составлены в соответствии с рабочей программой дисциплины в УМК дисциплины.

Методические рекомендации по организации образовательного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья
При необходимости программа дисциплины может быть адаптирована для инклюзивного обучения инвалидов и лиц с ограниченными возможностями здоровья с учетом особенностей их психофизического развития, индивидуальных возможностей и необходимых специальных условий их обучения.
При наличии в группе студентов с ограниченными возможностями здоровья возможно использовать адаптивные технологии.
Для студентов с ограниченным слухом:
- использование разнообразных дидактических материалов (карточки, рисунки, письменное описание, схемы и т.п.) как помощь для понимания и решения поставленной задачи;
- использование видеоматериалов, которые дают возможность понять тему занятия и осуществить коммуникативные действия;
- выполнение проектных заданий по изучаемым темам.
Для студентов с ограниченным зрением:
- использование фильмов с возможностью восприятия на слух даваемой в них информации для последующего ее обсуждения;
- использование аудиоматериалов по изучаемым темам, имеющимся на кафедре;
- индивидуальное общение с преподавателем по изучаемому материалу;
- творческие задания по изучаемым темам или по личному желанию с учетом интересов обучаемого.