УТВЕРЖДЕНО

решением Ученого совета факультета математики, информационных и авиационных технологий
от «21» 05 2024г., протокол № 5/24
Председатель _____ Волков М.А.
«21» 05 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	**Программно-аппаратные средства защиты информации**
Факультет	Факультет математики, информационных и авиационных технологий
Кафедра	Кафедра информационной безопасности и теории управления
Курс	4

Направление (специальность): 10.05.03 Информационная безопасность автоматизированных систем
Направленность (профиль/специализация): Безопасность открытых информационных систем
Форма обучения: очная
Дата введения в учебный процесс УлГУ: 01.09.2024 г.
Программа актуализирована на заседании кафедры: протокол № 10 от 15.04 2024 г.
Программа актуализирована на заседании кафедры: протокол №_____ от _____ 20___г.
Программа актуализирована на заседании кафедры: протокол №_____ от _____ 20___г.

Сведения о разработчиках:

ФИО	КАФЕДРА	Должность, ученая степень, звание
Иванцов Андрей Михайлович	Кафедра информационной безопасности и теории управления	Доцент, Кандидат технических наук, Доцент

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

Основной целью освоения дисциплины «Программно-аппаратные средства защиты информации» является формирование у студентов знаний о спектре программно-аппаратных средств обеспечения информационной безопасности, а также навыков и умений в применении знаний для конкретных условий. Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач по настройке, выбору и эксплуатации программно-аппаратных средств защиты информации.

Задачи освоения дисциплины:

Основные задачи дисциплины – дать знания:

- о методах и средствах защиты информации в компьютерных системах;

- о защитных механизмах, реализованных в средствах защиты информационных си-стем;

- о современных программно-аппаратных средствах защиты информации;

- о применении средств криптографической защиты информации и средств защиты информации от НСД для решения задач обеспечения информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Программно-аппаратные средства защиты информации» относится к числу дисциплин блока Б1.О.1, предназначенного для студентов, обучающихся по направлению: 10.05.03 Информационная безопасность автоматизированных систем.

В процессе изучения дисциплины формируются компетенции: ОПК-9, ОПК-10, ОПК-13.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: Программно-аппаратные средства защиты информации, Методы и средства криптографической защиты информации, Сети и системы передачи информации, Разработка и эксплуатация автоматизированных систем в защищенном исполнении, Научно-исследовательская работа, Защита информации от утечки по техническим каналам, Проектная деятельность, Подготовка к сдаче и сдача государственного экзамена, Безопасность операционных систем, Безопасность вычислительных сетей, Криптографические протоколы, Основы информационной безопасности, Теоретико-числовые методы в криптографии, Организация электронно вычислительных машин и вычислительных систем.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации;	**знать**: основные задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации **уметь**: решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи **владеть**: навыками решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий
ОПК-13 Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем;	**знать**: порядок диагностики и тестирования систем защиты информации автоматизированных систем **уметь**: организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем **владеть**: навыками организации и проведения диагностики и тестирования систем защиты информации автоматизированных систем, проведения анализа уязвимостей систем защиты информации автоматизированных систем
ОПК-10 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности;	**знать**: основные средства криптографической защиты информации, используемые при решении задач профессиональной деятельности **уметь**: правильно использовать основные средства криптографической защиты информации при решении задач профессиональной деятельности **владеть**: навыками правильного использования основных средств криптографической защиты информации при решении задач профессиональной деятельности

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего): 4 ЗЕТ

4.2. Объем дисциплины по видам учебной работы (в часах): 144 часа

Форма обучения: очная

Вид учебной работы	Количество часов (форма обучения очная)	
	Всего по плану	В т.ч. по семестрам
		8
1	2	3
Контактная работа обучающихся с преподавателем в соответствии с УП	90	90
Аудиторные занятия:	90	90
Лекции	36	36
Семинары и практические занятия	36	36
Лабораторные работы, практикумы	18	18
Самостоятельная работа	18	18
Форма текущего контроля знаний и контроля самостоятельной работы: тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)	Тестирование, Оценивание реферата	Тестирование, Оценивание реферата
Курсовая работа	-	-
Виды промежуточной аттестации (экзамен, зачет)	Экзамен (18)	Экзамен
Всего часов по дисциплине	144	144

4.3. Содержание дисциплины. Распределение часов по темам и видам учебной работы

Форма обучения: очная

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
Раздел 1. Основные принципы и методы создания программно-аппаратных средств обеспечения информационной безопасности							
Тема 1.1. Предмет и задачи дисциплины «Программно-аппаратные	3	2	0	0	0	1	Вопросы к Экзамену, Тестирование, Оценивание реферата

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
средства информационной безопасности» (ПАСОИБ).							
Тема 1.2. Анализ угроз информационной безопасности	3	2	0	0	0	1	Вопросы к Экзамену, Тестирование, Оценивание реферата
Тема 1.3. Механизмы защиты. Политика безопасности в информационных системах	5	2	2	0	0	1	Вопросы к Экзамену, Тестирование, Оценивание реферата
Тема 1.4. Основные принципы в создании в создании программно-аппаратных средств обеспечения информационной безопасности	5	2	2	0	0	1	Вопросы к Экзамену, Тестирование, Оценивание реферата
Тема 1.5. Типовая структура и основные программно–аппаратных средств обеспечения информа	5	2	2	0	0	1	Вопросы к Экзамену, Тестирование, Оценивание реферата

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
ционной безопасности							
Тема 1.6. Методы разграничения доступа и управления доступом	3	2	0	0	0	1	Вопросы к Экзамену, Тестирование, Оценивание реферата
Тема 1.7. Методы обеспечения идентификации и аутенти-фикации	5	2	2	0	0	1	Вопросы к Экзамену, Тестирование, Оценивание реферата
Тема 1.8. Методы и средства хранения ключевой информации	9	2	2	4	0	1	Вопросы к Экзамену, Тестирование, Оценивание реферата
Раздел 2. Программно-аппаратные средства защиты информации от несанкционированного доступа							
Тема 2.1. Защита незаконного копирования и использования программ	5	2	2	0	0	1	Вопросы к Экзамену, Тестирование, Оценивание реферата
Тема 2.2. Защита от разрушающих программных воздействий и изучения кода программ	5	2	2	0	0	1	Вопросы к Экзамену, Тестирование, Оценивание реферата

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
Тема 2.3. Основные подходы к защите данных от НСД	5	2	2	0	0	1	Вопросы к Экзамену, Тестирование, Оценивание реферата
Тема 2.4. Определение факта доступа к файлам. Доступ к данным со стороны процесса	11	2	4	4	0	1	Вопросы к Экзамену, Тестирование, Оценивание реферата
Тема 2.5. Особенности защиты данных от изменения	11	2	4	4	0	1	Вопросы к Экзамену, Тестирование, Оценивание реферата
Тема 2.6. Методы криптографической защиты	7	2	2	2	0	1	Вопросы к Экзамену, Тестирование, Оценивание реферата
Тема 2.7. ПАСЗИ в сетях передачи данных. Межсетевые экраны. Средства экранирования. Обнаружение сетевых атак	11	2	4	4	0	1	Вопросы к Экзамену, Тестирование, Оценивание реферата
Тема 2.8. Управление безопасно	5	2	2	0	0	1	Вопросы к Экзамену, Тестирован

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
стью сети							ие, Оценивание реферата
Тема 2.9. Сертификация СЗИ	10	4	4	0	0	2	Вопросы к Экзамену, Тестирование, Оценивание реферата
Итого подлежит изучению	108	36	36	18	0	18	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Основные принципы и методы создания программно-аппаратных средств обеспечения информационной безопасности

Тема 1.1. Предмет и задачи дисциплины «Программно-аппаратные средства информационной безопасности» (ПАСОИБ).

Основные понятия и определения в создании ПАСЗИ. Предмет и задачи дисциплины. Нормативно-правовая база создания и использования ПАСЗИ.

Тема 1.2. Анализ угроз информационной безопасности

Понятие доступа, субъект и объект доступа. Классификация угроз информационной безопасности. Каналы утечки информации. Угрозы, обусловленные человеческим фактором, техническими средствами, форс-мажорными обстоятельствами. Модель нарушителя.

Тема 1.3. Механизмы защиты. Политика безопасности в информационных системах

Требования к защищенности. Оценка защищенности Модели управления доступом. Функции ядра безопасности. Способы защиты конфиденциальности, целостности и доступности в КС. Классификация функциональных требований по защите информации. Требования к защищенности ИС на уровне защиты объектов, защиты линий, защиты БД, защиты подсистем управления. Политика безопасности.

Тема 1.4. Основные принципы в создании в создании программно-аппаратных средств обеспечения информационной безопасности

Классификация ПАСЗИ. Функциональные возможности ПАСЗИ. Принципы разработки ПАСЗИ. Концепция диспетчера доступа. Функционирование диспетчера доступа при управлении доступом к защищаемым ресурсам. Порядок проектирования ПАСЗИ. Модель системы защиты информации (СЗИ).

Тема 1.5. Типовая структура и основные программно–аппаратных средств обеспечения информационной безопасности

Структура ПАСЗИ. Компоненты и подсистемы. Типовые функции ПАСЗИ. Обязательные требования по обеспечению ИБ, предъявляемые к ПАСЗИ. Перспективы развития ПАСЗИ. Принципы действия и технологические особенности ПАСЗИ, реализующих отдельные функциональные требования по защите информации и данных, их взаимодействие с общесистемными компонентами вычислительных систем

Тема 1.6. Методы разграничения доступа и управления доступом

Методы ограничения доступа и управления доступом. Понятие несанкционированного доступа (НСД). Классы и виды НСД. Идентификация и аутентификация. Парольные системы. Дискреционное управление доступом. Мандатное управление доступом. Ролевое управление доступом.

Тема 1.7. Методы обеспечения идентификации и аутенти-фикации

Задача идентификации пользователя. Понятие протокола идентификации. Локальная и удаленная идентификация. Идентифицирующая информация. Понятие идентифицирующей информации. Способы хранения идентифицирующей информации. Связь с ключевыми системами. Симметричные методы аутентификации. Несимметричные методы аутентификации субъекта. Аутентификация объекта. Авторизация. Контроль и управление доступом средствами операционной системы и программно-аппаратными техническими средствами.

Тема 1.8. Методы и средства хранения ключевой информации

Информация, используемая для контроля доступа: ключи и пароли. Злоумышленник и ключи. Классификация средств хранения ключей и идентифицирующей информации. Организация хранения ключей. Магнитные диски прямого доступа. Средство TouchMemory. Типовые решения в организации ключевых систем. Открытое распределение ключей. Метод управляемых векторов. Персональные средства аутентификации и защищенного хранения данных

Раздел 2. Программно-аппаратные средства защиты информации от несанкционированного доступа

Тема 2.1. Защита незаконного копирования и использования программ

Классификация аппаратных и программных компонентов защиты программ. Структура ПО. Способы встраивания средств защиты в ПО. Способы определения факта незаконного копирования и использования программ. Способы защиты от незаконного копирования и использования

программ. Привязка ПО к аппаратному окружению и физическим носителям как единственное средство защиты от копирования ПО.

Тема 2.2. Защита от разрушающих программных воздействий и изучения кода программ

Способы изучения кода программ. Обратное проектирование ПО. Способы защиты программ от изучения кода. Основные принципы обеспечения безопасности программ. Защита от разрушающих программных воздействий. Вирусы как особый класс разрушающих программных воздействий. Необходимые и достаточные условия недопущения разрушающего воздействия. Понятие изолированной программной среды

Тема 2.3. Основные подходы к защите данных от НСД

Файл как объект доступа. Оценка надежности систем ограничения доступа – сведение к задаче оценки стойкости. Иерархический доступ к файлам. Понятие атрибутов доступа. Организация доступа к файлам в различных ОС. Защита сетевого файлового ресурса. Классификация программно-аппаратных средств защиты от несанкционированного доступа к информации, хранимой в ПЭВМ. Характеристики программно-аппаратных средств защиты от несанкционированного доступа к информации, хранимой в ПЭВМ

Тема 2.4. Определение факта доступа к файлам. Доступ к данным со стороны процесса

Способы определения факта доступа. Журналы доступа. Критерии информативности журналов доступа. Выявление следов несанкционированного доступа к файлам, метод инициированного НСД. Понятие доступа к данным со стороны процесса: отличия от доступа со стороны пользователя. Понятие и примеры скрытого доступа. Надежность систем ограничения доступа. Понятие электронного замка. Принципы построения и функционирования электронных замков. Механизмы контроля аппаратной конфигурации ПЭВМ.

Тема 2.5. Особенности защиты данных от изменения

Защита массивов информации от изменения. Имитозащита. Криптографическая постановка защиты от изменения данных. Подходы к решению задачи защиты данных от изменения. Подход на основе формирования имитоприставки. Подход на основе формирования хэш-функции, требования к построению и способы реализации. Формирование электронной подписи (ЭП). Особенности защиты документов и исполняемых файлов. Проблема самоконтроля исполняемых модулей. Использование СЗИ «Dallas Lock» для защиты от несанкционированного изменения, установки или удаление программ и файлов.

Тема 2.6. Методы криптографической защиты

Классификация методов криптографического преобразования. Нормативно-правовая база. Требования к программно-аппаратным комплексам шифрования. Необходимые и достаточные функции аппаратного средства криптозащиты. Построение аппаратных компонент криптозащиты данных, специализированные СБИС как носители алгоритма шифрования. Защита алгоритма шифрования; принцип чувствительной области и принцип главного ключа.

Тема 2.7. ПАСЗИ в сетях передачи данных. Межсетевые экраны. Средства экранирования. Обнаружение сетевых атак

Классификация программно-аппаратных средств защиты информации в сетях передачи данных. Принципы построения и функционирования межсетевых экранов в сетях передачи данных. Программно-аппаратные средства межсетевого экранирования. Основные принципы защиты информации при передаче по каналам связи. Программно-аппаратные средства защиты информации при передаче по каналам связи. Основные принципы обнаружения сетевых атак. Основные принципы защиты от сетевых атак. Межсетевые экраны. Средства экранирования. Обнаружение сетевых атак.

Тема 2.8. Управление безопасностью сети

Основные принципы управления безопасностью сети. Программно-аппаратные средства управления безопасностью сети. Штатные средства сетевого оборудования, предназначенные для защиты информации при передаче по каналам связи

Тема 2.9. Сертификация СЗИ

Система сертификации СЗИ. Задачи сертификации ПАСЗИ на соответствие требованиям информационной безопасности. Нормативно-правовая база сертификации ПАСЗИ на соответствие требованиям информационной безопасности. Технология сертификации ПАСЗИ на соответствие требованиям информационной безопасности

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Раздел 1. Основные принципы и методы создания программно-аппаратных средств обеспечения информационной безопасности

Тема 1.3. Механизмы защиты. Политика безопасности в информационных системах

Вопросы к теме:

Очная форма

1. Модели управления доступом.
2. Способы защиты конфиденциальности, целостности и доступности в КС.
3. Требования к защищенности ИС на уровне защиты объектов, защиты линий, защиты БД, защиты подсистем управления.
4. Политика безопасности.

Тема 1.4. Основные принципы в создании в создании программно-аппаратных средств обеспечения информационной безопасности

Вопросы к теме:

Очная форма

1. Принципы разработки ПАСЗИ.
2. Функционирование диспетчера доступа при управлении доступом к защищаемым ресурсам.
3. Проектирование ПАСЗИ.
4. Модель системы защиты информации (СЗИ).

Тема 1.5. Типовая структура и основные программно–аппаратных средств обеспечения информационной безопасности

Вопросы к теме:

Очная форма

1. Структура ПАСЗИ. Компоненты и подсистемы.
2. Обязательные требования по обеспечению ИБ, предъявляемые к ПАСОИБ.
3. Принципы действия и технологические особенности ПАСЗИ, реализующих отдельные функциональные требования по защите информации и данных, их взаимодействие с общесистемными компонентами вычислительных систем.

Тема 1.7. Методы обеспечения идентификации и аутенти-фикации

Вопросы к теме:

Очная форма

1. Локальная и удаленная идентификация.
2. Способы хранения идентифицирующей информации.
3. Связь с ключевыми системами.
4. Контроль и управление доступом средствами операционной системы и программно-аппаратными техническими средствами.

Тема 1.8. Методы и средства хранения ключевой информации

Вопросы к теме:

Очная форма

1. Информация, используемая для контроля доступа: ключи и пароли.
2. Злоумышленник и ключи.
3. Организация хранения ключей.
4. Персональные средства аутентификации и защищенного хранения данных

Раздел 2. Программно-аппаратные средства защиты информации от несанкционированного доступа

Тема 2.1. Защита незаконного копирования и использования программ

Вопросы к теме:

Очная форма

1. Способы встраивания средств защиты в ПО.
2. Способы определения факта незаконного копирования и использования программ.
3. Способы защиты от незаконного копирования и использования программ.

Тема 2.2. Защита от разрушающих программных воздействий и изучения кода программ

Вопросы к теме:

Очная форма

1. Способы изучения кода программ. Обратное проектирование ПО.
2. Способы защиты программ от изучения кода.
3. Защита от разрушающих программных воздействий.

Тема 2.3. Основные подходы к защите данных от НСД

Вопросы к теме:

Очная форма

1. Оценка надежности систем ограничения доступа – сведение к задаче оценки стойкости.
2. Организация доступа к файлам в различных ОС.
3. Защита сетевого файлового ресурса.

Тема 2.4. Определение факта доступа к файлам. Доступ к данным со стороны процесса

Вопросы к теме:

Очная форма

1. Способы определения факта доступа. Журналы доступа.
2. Выявление следов несанкционированного доступа к файлам, метод инициированного НСД.
3. Понятие доступа к данным со стороны процесса: отличия от доступа со стороны пользователя.
4. Принципы построения и функционирования электронных замков.

5. Механизмы контроля аппаратной конфигурации ПЭВМ.

Тема 2.5. Особенности защиты данных от изменения

Вопросы к теме:

Очная форма

1. Подходы к решению задачи защиты данных от изменения.
2. Подход на основе формирования имитоприставки (MAC), способы построения MAC.
3. Подход на основе формирования хэш-функции, требования к построению и способы реализации. Формирование электронной подписи (ЭЦП).
4. Особенности защиты документов и исполняемых файлов.
5. Использование СЗИ «Dallas Lock» для защиты от несанкционированного изменения, установки или удаление программ и файлов.

Тема 2.6. Методы криптографической защиты

Вопросы к теме:

Очная форма

1. Построение аппаратных компонент криптозащиты данных, специализированные СБИС как носители алгоритма шифрования.
2. Защита алгоритма шифрования; принцип чувствительной области и принцип главного ключа.

Тема 2.7. ПАСЗИ в сетях передачи данных. Межсетевые экраны. Средства экранирования. Обнаружение сетевых атак

Вопросы к теме:

Очная форма

1. Принципы построения и функционирования межсетевых экранов в сетях передачи данных.
2. Основные принципы защиты информации при передаче по каналам связи.
3. Программно-аппаратные средства защиты информации при передаче по каналам связи.
4. Основные принципы обнаружения сетевых атак.
5. Основные принципы защиты от сетевых атак.

Тема 2.8. Управление безопасностью сети

Вопросы к теме:

Очная форма

1. Основные принципы управления безопасностью сети.
2. Программно-аппаратные средства управления безопасностью сети.
3. Штатные средства сетевого оборудования, предназначенные для защиты информации при передаче по каналам связи

Тема 2.9. Сертификация СЗИ

Вопросы к теме:

Очная форма

1. Система сертификации СЗИ.
2. Технология сертификации ПАСЗИ на соответствие требованиям информационной безопасности.

7. ЛАБОРАТОРНЫЕ РАБОТЫ, ПРАКТИКУМЫ

Настройка усиленной аутентификации с использованием СЗИ от НСД Dallas Lock на базе eToken
Цели: Настройка и использование «eToken» для аутентификации и получение практических навыков работы с персональным средством аутентификации и защищенного хранения данных
Содержание: Если на компьютере уже установлена система защиты, ее необходимо удалить. 2. Необходимо убедиться, что на диске С имеется необходимое свободное пространство для установки системы защиты. 3. Проверить состояние жестких дисков компьютера, например, при помощи приложения chkdsk.exe или служебной программы проверки диска из состава ОС Windows, и устранить выявленные дефекты. 4. Рекомендуется произвести дефрагментацию диска. 5. Проверить компьютер на отсутствие компьютерных вирусов. 6. Перед установкой системы защиты необходимо выгрузить из памяти все резидентные антивирусы. 7. Закрыть все запущенные приложения, так как установка системы потребует принудительной перезагрузки. 8. Настроить и показать использование «eToken» для аутентификации и получения практических навыков работы с персональным средством аутентификации и защищенного хранения данных
Результаты: Настроить и показать использование «eToken» для аутентификации и получения практических навыков работы с персональным средством аутентификации и защищенного хранения данных
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/10728
Использование электронного замка ПАК Соболь
Цели: Использование «ПАК Соболь» для контроля аппаратной конфигурации ПЭВМ, получение практических навыков работы с электронным замком
Содержание: 1. Ознакомление с теоретической частью электронного замка "Соболь". 2. Установка программного обеспечения комплекса "Соболь". 3. Подготовка комплекса к инициализации. 4. Инициализация электронного замка "Соболь". 5. Подготовка электронного замка к эксплуатации. 6.

Настройка и эксплуатация комплекса "Соболь". 7. Удаление программного обеспечения электронного замка "Соболь".
Результаты: - изучить электронный замок «Соболь» и научиться устанавливать, настраивать и эксплуатировать его; - составить отчет о проделанной работе и отчитаться по нему у преподавателя.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/10728
Использование СЗИ Dallas Lock
Цели: Использование СЗИ «Dallas Lock» для защиты от несанкционированного изменения, установки или удаления программ и файлов, получение практических навыков работы с СЗИ от НСД
Содержание: Если на компьютере уже установлена система защиты, ее необходимо удалить. 2. Необходимо убедиться, что на диске С имеется необходимое свободное пространство для установки системы защиты. 3. Проверить состояние жестких дисков компьютера, например, при помощи приложения chkdsk.exe или служебной программы проверки диска из состава ОС Windows, и устранить выявленные дефекты. 4. Рекомендуется произвести дефрагментацию диска. 5. Проверить компьютер на отсутствие компьютерных вирусов. 6. Перед установкой системы защиты необходимо выгрузить из памяти все резидентные антивирусы. 7. Закрыть все запущенные приложения, так как установка системы потребует принудительной перезагрузки.
Результаты: изучить и продемонстрировать основные возможности Dallas Lock как системы защиты информации от НСД. - составить отчет о проделанной работе и защитить его у преподавателя.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/10728
Назначение и возможности Программно-аппаратного комплекса средств защиты информации от НСД “Аккорд–АМДЗ
Цели: Изучить возможности и научиться работать с комплексом средств защиты от НСД.
Содержание: 1. Ознакомление с теоретической частью СЗИ НСД «Аккорд- АМДЗ». 2. Установка платы контроллера и программного обеспечения комплекса, включающая три основных этапа: - установка платы контроллера в свободный слот ПЭВМ и регистрацию администратора безопасности информации (БИ) (супервизора), в том числе, настройка комплекса в соответствии с конфигурацией технических средств ПЭВМ; - регистрация пользователей, назначение пользователям личных ТМ-идентификаторов, паролей и времени доступа; - назначение списка дисков, файлов, разделов реестра, контролируемых на целостность. 3. Инициализация СЗИ НСД «Аккорд- АМДЗ»: - регистрация супервизора (администратора безопасности информации); - регистрация нового пользователя. 4. Эксплуатация комплекса «Аккорд- АМДЗ». 5. Снятие средств защиты комплекса «Аккорд- АМДЗ».
Результаты: - изучить СЗИ НСД «Аккорд- АМДЗ» и научиться устанавливать, настраивать и эксплуатировать его; - составить отчет о проделанной работе и отчитаться по нему у преподавателя.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/10728
Назначение, возможности и порядок работы с системой SecretNet Studio
Цели: Изучить возможности и научиться работать с системой SecretNet Studio
Содержание: 1. Ознакомление с теоретической частью «Secret Net Studio». 2. Установка программного обеспечения средства защиты информации «Secret Net Studio» на локальный ПК. 3. Подготовка средства защиты информации к инициализации. 4. Инициализация «Secret Net Studio». 5. Подготовка к эксплуатации. 6. Настройка и эксплуатация «Secret Net Studio». 7. Удаление программного обеспечения «Secret Net Studio».
Результаты: - изучить «Secret Net Studio» и научиться устанавливать, настраивать, эксплуатировать и корректно удалять СЗИ с компьютера; - подготовить письменный отчет о проделанной работе и защитить его у преподавателя.

Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/10728
Использование программно-аппаратных комплексов VipNet
Цели: Организация межсетевого взаимодействия защищенных сетей ViPNet. Получение практических навыков работы со средством криптографической защиты информации».
Содержание: Для установки ViPNet Client требуются: • Установочный EXE-файл программы. • Дистрибутив ключей для сетевого узла — файл с расширением *.dst или *.enc. • Пароль пользователя сетевого узла или внешнее устройство аутентификации Дистрибутив ключей и пароль пользователя можно получить у администратора сети ViPNet.
Результаты: - изучить процесс установки, настройки, удаления ПК VipNet Client. - продемонстрировать основные возможности ПК VipNet Client. - составить отчет о проделанной работе и защитить его у преподавателя.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/10728

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Темы рефератов

Тема 1. Классификация программно-аппаратных средств обеспечения информационной безопасности
Тема 2. Классификация угроз информационной безопасности
Тема 3. Политики безопасности в информационных системах
Тема 4. Основные принципы и механизмы защиты информации
Тема 5. Типовая структура и основные функции программно–аппаратных средств обеспечения информационной безопасности
Тема 6. Основные методы разграничения доступа и управления доступом
Тема 7. Основные методы обеспечения идентификации и аутентификации
Тема 8. Методы и средства хранения ключевой информации
Тема 9. Защита от незаконного копирования программ
Тема 10. Защита от незаконного использования программ
Тема 11. Основные подходы к защите данных от НСД
Тема 12. Защита от незаконного использования программ
Тема 13. Защита данных от изменения
Тема 14. Программно-аппаратные средства защиты от несанкционированного доступа к информации, хранимой в ПЭВМ
Тема 15. Методы и средства криптографической защиты
Тема 16. Сертификация средств защиты информации
Тема 17. Программно-аппаратные средства управления безопасностью сети
Тема 18. Программно-аппаратные средства защиты информации в сетях передачи данных
Тема 19. Способы и средства обнаружения сетевых атак
Тема 20. Защита от разрушающих программных воздействий

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

1. Основные понятия и определения в создании программно-аппаратных средств защиты информации (ПАСЗИ). Нормативно-правовая база создания ПАСЗИ.

2. Понятие доступа, субъект и объект доступа. Классификация угроз безопасности.Каналы утечки информации. Угрозы, обусловленные человеческим фактором, техническими средствами, форс-мажорными обстоятельствами.
3. Понятие несанкционированного доступа (НСД). Классы и виды НСД. Понятие злоумышленника; злоумышленник в криптографии и при решении проблем компьютерной безопасности.
4. Модели управления доступом. Функции ядра безопасности. Способы защиты конфиденциальности, целостности и доступности в КС.
5. Классификация функциональных требований по защите информации. Требования к защищенности ИС на уровне защиты объектов, защиты линий, защиты БД, защиты подсистем управления. Политика безопасности.
6. Классификация ПАСЗИ. Функциональные возможности ПАСЗИ. Принципы разработки ПАСЗИ. Порядок проектирования ПАСЗИ.
7. Концепция диспетчера доступа. Функционирование диспетчера доступа при управлении доступом к защищаемым ресурсам.
8. Структура ПАСЗИ. Компоненты и подсистемы. Типовые функции ПАСЗИ. Обязательные требования по обеспечению ИБ, предъявляемые к ПАСЗИ.
9. Принципы действия и технологические особенности ПАСЗИ, реализующих отдельные функциональные требования по защите информации и данных, их взаимодействие с общесистемными компонентами вычислительных систем.
10. Методы ограничения доступа и управления доступом. Идентификация и аутентификация. Парольные системы. Управление доступом.
11. Задача идентификации пользователя. Понятие протокола идентификации. Локальная и удаленная идентификация. Идентифицирующая информация. Понятие идентифицирующей информации. Способы хранения идентифицирующей информации. Связь с ключевыми системами.
12. Классификация средств хранения ключей и идентифи-цирующей информации. Организация хранения ключей. Типовые решения в организации ключевых систем.
13. Способы изучения кода программ. Обратное проектирование ПО. Способы защиты программ от изучения кода. Основные принципы обеспечения безопасности программ.
14. Защита от разрушающих программных воздействий. Вирусы как особый класс разрушающих программных воздействий. Необходимые и достаточные условия недопущения разрушающего воздействия. Понятие изолированной программной среды.
15. Классификация программно-аппаратных средств защиты от несанкционированного доступа к информации, хранимой в ПЭВМ. Характеристики программно-аппаратных средств защиты от несанкционированного доступа к информации, хранимой в ПЭВМ
16. Способы определения факта доступа. Журналы доступа. Критерии информативности журналов доступа. Выявление следов несанкционированного доступа к файлам, метод инициированного НСД.
17. Понятие доступа к данным со стороны процесса: отличия от доступа со стороны пользователя. Понятие и примеры скрытого доступа. Надежность систем ограничения доступа.
18. Понятие доступа к данным со стороны процесса: отличия от доступа со стороны пользователя. Понятие и примеры скрытого доступа. Надежность систем ограничения доступа.
19. Подходы к решению задачи защиты данных от изменения. Особенности защиты документов и исполняемых файлов.
20. Классификация методов криптографического преобразования. Нормативно-правовая база. Требования к программно-аппаратным комплексам шифрования. Необходимые и достаточные функции аппаратного средства криптозащиты.
21. Построение аппаратных компонент криптозащиты данных, специализированные СБИС как

носители алгоритма шифрования. Защита алгоритма шифрования; принцип чувствительной области и принцип главного ключа.
22. Основные принципы защиты информации при передаче по каналам связи. Программно-аппаратные средства защиты информации при передаче по каналам связи. Основные принципы обнаружения сетевых атак. Основные принципы защиты от сетевых атак.
23. Назначение и возможности Программно-аппаратного комплекса средств защиты информации от НСД “Аккорд–АМДЗ”
24. Классификация программно-аппаратных средств защиты информации в сетях передачи данных. Принципы построения и функционирования межсетевых экранов в сетях передачи данных. Программно-аппаратные средства межсетевого экранирования.
25. Основные принципы управления безопасностью сети. Программно-аппаратные средства управления безопасностью сети. Штатные средства сетевого оборудования, предназначенные для защиты информации при передаче по каналам связи
26. Назначение, возможности и порядок работы с Электронным замком "Соболь".
27. Назначение, возможности и порядок работы с СЗИ «Dallas Lock».
28. Назначение, возможностиипорядокработысперсональнымисредствамиаутентификации и защищѐнногохраненияданных(USB-ключи и смарт-карты eToken).
29. Назначение,возможностиипорядокработыссистемой SecretNet Studio
30. Назначение, возможности и порядок работы с программно-аппаратным комплексом VipNet».
31. Состав и основные функции программно-аппаратного комплекса VipNet».
32. Основные принципы сертификации СЗИ

10. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩИХСЯ

Содержание, требования, условия и порядок организации самостоятельной работы обучающихся с учетом формы обучения определяются в соответствии с «Положением об организации самостоятельной работы обучающихся», утвержденным Ученым советом УлГУ (протокол №8/268 от 26.03.2019г.).

По каждой форме обучения: очная/заочная/очно-заочная заполняется отдельная таблица

Форма обучения: очная

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
Раздел 1. Основные принципы и методы создания программно-аппаратных средств обеспечения информационной безопасности			
Тема 1.1. Предмет и задачи дисциплины «Программно-аппаратные средства информационной безопасности» (ПАСОИБ).	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	1	Тестирование, Оценивание реферата

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
Тема 1.2. Анализ угроз информационной безопасности	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	1	Тестирование, Оценивание реферата
Тема 1.3. Механизмы защиты. Политика безопасности в информационных системах	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	1	Тестирование, Оценивание реферата
Тема 1.4. Основные принципы в создании в создании программно-аппаратных средств обеспечения информационной безопасности	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	1	Тестирование, Оценивание реферата
Тема 1.5. Типовая структура и основные программно–аппаратных средств обеспечения информационной безопасности	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	1	Тестирование, Оценивание реферата
Тема 1.6. Методы разграничения доступа и управления доступом	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	1	Тестирование, Оценивание реферата
Тема 1.7. Методы обеспечения идентификации и аутенти-фикации	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	1	Тестирование, Оценивание реферата
Тема 1.8. Методы и средства хранения ключевой информации	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	1	Тестирование, Оценивание реферата
Раздел 2. Программно-аппаратные средства защиты информации от несанкционированного доступа			
Тема 2.1. Защита незаконного копирования и использования программ	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	1	Тестирование, Оценивание реферата
Тема 2.2. Защита от разрушающих программных воздействий и изучения кода	Проработка учебного материала с использованием ресурсов учебно-методического и	1	Тестирование, Оценивание реферата

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
программ	информационного обеспечения дисциплины.		
Тема 2.3. Основные подходы к защите данных от НСД	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	1	Тестирование, Оценивание реферата
Тема 2.4. Определение факта доступа к файлам. Доступ к данным со стороны процесса	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	1	Тестирование, Оценивание реферата
Тема 2.5. Особенности защиты данных от изменения	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	1	Тестирование, Оценивание реферата
Тема 2.6. Методы криптографической защиты	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	1	Тестирование, Оценивание реферата
Тема 2.7. ПАСЗИ в сетях передачи данных. Межсетевые экраны. Средства экранирования. Обнаружение сетевых атак	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	1	Тестирование, Оценивание реферата
Тема 2.8. Управление безопасностью сети	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	1	Тестирование, Оценивание реферата
Тема 2.9. Сертификация СЗИ	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование, Оценивание реферата

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы

основная

1. Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В. Славнов ; Душкин А.В.; Барсуков О.М.; Кравцов Е.В.; Славнов К.В. - Москва : Горячая линия - Телеком, 2016. - 248 с. - URL: https://www.studentlibrary.ru/book/ISBN9785991204705.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-9912-0470-5. / .— ISBN 0_250838

2. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам : учебное пособие / Г.А. Бузов ; Бузов Г.А. - Москва : Горячая линия - Телеком, 2015. - 586 с. - URL: https://www.studentlibrary.ru/book/ISBN9785991204248.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-9912-0424-8. / .— ISBN 0_251025

дополнительная

1. Бузов Г.А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации : практическое пособие / Г.А. Бузов ; Бузов Г.А. - Москва : Горячая линия - Телеком, 2010. - 240 с. - URL: https://www.studentlibrary.ru/book/ISBN9785991201216.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-9912-0121-6. / .— ISBN 0_242453

2. Солонская, О. И. Средства защиты информации : учебное пособие / О. И. Солонская ; О. И. Солонская. - Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2021. - 89 с. - Книга находится в премиум-версии IPR SMART. - Текст. - Гарантированный срок размещения в ЭБС до 09.12.2026 (автопролонгация). - электронный. - Электрон. дан. (1 файл). - URL: https://www.iprbookshop.ru/117115.html. - Режим доступа: Цифровой образовательный ресурс IPR SMART; для авторизир. пользователей. - ISBN 2227-8397. / .— ISBN 0_404597

3. Галатенко В.А. Стандарты информационной безопасности : учебник / В.А. Галатенко ; Галатенко В.А. - Москва : ИНТУИТ, 2016. - . - URL: https://www.studentlibrary.ru/book/ISBN5955600531.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 5-9556-0053-1. / .— ISBN 0_257176

учебно-методическая

1. Иванцов А. М. Методические указания для самостоятельной работы студентов по дисциплине «Программно-аппаратные средства защиты информации» для студентов специалитета по специальности 10.05.03 очной формы обучения / А. М. Иванцов ; УлГУ, ФМИиАТ. - 2021. - 22 с. - Неопубликованный ресурс. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/10728. - Режим доступа: ЭБС УлГУ. - Текст : электронный. / .— ISBN 0_261314.

б) Программное обеспечение

- Операционная система "Альт образование"
- Офисный пакет "Мой офис"
- Академическая лицензия на УМК ViPNet "Защита сетей"
- Альт рабочая станция
- Комплект «Максимальная защита» Средства защиты информации Secret Net Studio 8

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2024]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2024]. - URL: https://urait.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2024]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача. Электронная медицинская библиотека : база данных : сайт / ООО Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг. – Москва, [2024]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО Букап. – Томск, [2024]. – URL: https://www.books-up.ru/ru/library/ . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. ЭБС Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2024]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС **Znanium.com** : электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2024]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2024].

3. eLIBRARY.RU: научная электронная библиотека : сайт / ООО «Научная Электронная Библиотека». – Москва, [2024]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2024]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. Российское образование : федеральный портал / учредитель ФГАУ «ФИЦТО». – URL:

http://www.edu.ru. – Текст : электронный.

6. Электронная библиотечная система УлГУ : модуль «Электронная библиотека» АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: http://lib.ulsu.ru/MegaPro/Web. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Аудитории для проведения лекций, семинарских занятий, для выполнения лабораторных работ и практикумов, для проведения текущего контроля и промежуточной аттестации, курсового проектирования, групповых и индивидуальных консультаций *(выбрать необходимое)*

Аудитории укомплектованы специализированной мебелью, учебной доской. Аудитории для проведения лекций оборудованы мультимедийным оборудованием для представления информации большой аудитории. Помещения для самостоятельной работы оснащены компьютерный техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде, электронно-библиотечной системе. Перечень оборудования, используемого в учебном процессе:

- Мультимедийное оборудование: компьютер/ноутбук, экран, проектор/телевизор
- Компьютерная техника

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации;
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, организация работы ППС с обучающимися с ОВЗ и инвалидами предусматривается в электронной информационно-образовательной среде с учетом их индивидуальных психофизических особенностей.

Разработчик	Доцент, Кандидат технических наук, Доцент	Иванцов Андрей Михайлович

	Должность, ученая степень, звание	ФИО