ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Высшая школа электроники и компьютерных наук

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Голлай А. В.
Пользователь: gollaiav
Дата подписания: 13.09.2021

А. В. Голлай

РАБОЧАЯ ПРОГРАММА

дисциплины В.1.06 Катастрофоустойчивость информационных систем
для специальности 10.05.03 Информационная безопасность автоматизированных систем
уровень специалист **тип программы** Специалитет
специализация Информационная безопасность автоматизированных систем критически важных объектов
форма обучения очная
кафедра-разработчик Защита информации

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 01.12.2016 № 1509

Зав.кафедрой разработчика,
к.техн.н., доц.

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Соколов А. Н.
Пользователь: sokolovan
Дата подписания: 13.09.2021

А. Н. Соколов

Разработчик программы,
к.юрид.н., доцент

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Жернова В. М.
Пользователь: zhernovavm
Дата подписания: 13.09.2021

В. М. Жернова

Челябинск

1. Цели и задачи дисциплины

Целью дисциплины является подготовка квалифицированных специалистов способных осуществить защиту информационных ресурсов и систем при катастрофах, авариях, стихийных бедствиях и их последствиях. Задачами дисциплины являются: - изучение основ и методов поиска рациональных решений построения катастрофоустойчивых информационных систем; - изучение основных подходов к обеспечению информационной безопасности катастофоустойчивых информационных систем; - изучение принципов функционирования современных средств построения и аппаратно-программных платформ построения информационных систем. Задачами дисциплины являются: приобретение студентами навыков по проектированию и реализации комплекса мер, обеспечивающих информационную безопасность в условиях чрезвычайных ситуаций, минимизации последствий чрезвычайных ситуаций и выведения информационной системы на заданный уровень.

Краткое содержание дисциплины

В течение дисциплины студентами будут изучены такие темы как: - Виды чрезвычайных ситуаций и их возможные последствия; - Проектирование катастрофоустойчивых информационных систем; - Разработка комплекса мер по реализации проектов катастрофоустойчивых информационных систем; - Ликвидация последствий чрезвычайных ситуаций в работе информационных систем.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине (ЗУНы)
ПК-20 способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	Знать:методы и средства используемые при защите информации и персонала при ЧС и ликвидации последствий ЧС; принципы работы средств обеспечения катастрофоустойчивости ИС
	Уметь:проектировать и реализовывать комплексную систему управления катастрофоустойчивыми ИС
	Владеть:навыками по разработке и реализации комплекса мер по защите персонала, информационных систем при возникновении ЧС и при ликвидации последствий ЧС
ПК-2 способностью создавать и исследовать модели автоматизированных систем	Знать:условия необходимости построения катастрофоустойчивых ИС
	Уметь:выявлять условия необходимости построения катастрофоустойчивых ИС
	Владеть:терминологией и системным подходом построения катастрофоустойчивых ИС
ПК-9 способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	Знать:основные методы и средства реализации катастрофоустойчивых ИС
	Уметь:
	Владеть:

ПК-13 способностью участвовать в проектировании средств защиты информации автоматизированной системы	Знать:основные принципы построения катастрофоустойчивых ИС
	Уметь:проектировать катастрофоустойчивые ИС
	Владеть:навыками по проектированию катастрофоустойчивых ИС
ПК-5 способностью проводить анализ рисков информационной безопасности автоматизированной системы	Знать:виды ЧС и их возможные последствия; требования предъявляемые к проектируемым катастрофоустойчивым ИС
	Уметь:осуществлять мониторинг и аудит безопасности катастрофоустойчивых ИС
	Владеть:навыками анализа угроз ИБ и уязвимостей в катастрофоустойчивых ИС

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Б.1.16 Безопасность жизнедеятельности, Б.1.28 Безопасность операционных систем	Б.1.35 Угрозы информационной безопасности автоматизированных систем, В.1.09 Обеспечение информационной безопасности на критически важных объектах

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
Б.1.16 Безопасность жизнедеятельности	опасные и вредные факторы системы «человек - среда обитания»; научные и организационные основы защиты окружающей среды и ликвидации последствий аварий, катастроф, стихийных бедствий
Б.1.28 Безопасность операционных систем	знать критерии оценки эффективности и надежности средств защиты операционных систем; принципы построения и функционирования современных операционных систем

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 2 з.е., 72 ч.

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		8
Общая трудоёмкость дисциплины	72	72
Аудиторные занятия:	32	32
Лекции (Л)	16	16
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	16	16

Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	40	40
Самостоятельное изучение отдельных тем курса	40	40
Вид итогового контроля (зачет, диф.зачет, экзамен)	-	зачет

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Катастрофоустойчивость в российской и зарубежной системе безопасности	4	2	2	0
2	Методы обеспечения катастрофоустойчивости автоматизированных систем	8	4	4	0
3	Средства и практические решения по обеспечению катастрофоустойчивости ав-томатизированных систем	12	6	6	0
4	Организация функционирования катстрофоустойчивых автоматизированных систем	8	4	4	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Национальные интересы и угрозы катастрофоустойчивости Российской Федерации в информационной сфере и их обеспечение. Международная база законодательных актов и методических указаний.	2
2	2	Жизненный цикл информационной системы. Обеспечение катастрофоустойчивости системы на каждом из этапов жизненного цикла информационной системы . Жизненный цикл информационной и функциональной безопасности.	2
3	2	Теория надежности технических и информационных систем . Выбор рациональных решений по организации средств восстановления информационных систем после отказов и катастроф	2
5	3	Средства и практические решения по обеспечению катастрофоустойчивости автоматизированных систем. Практические решения построения средств восстановления после катастроф	2
6	3	Организация функционирования катстрофоустойчивых автоматизированных систем. Основы обеспечения информационной безопасности в катастрофоустойчивых центрах обработки информации	2
7	3	Принципы построения организационно-режимных мер обеспечения безопасности информации. Предотвращение систематических отказов	2
8	4	Организационно-технические решения по обеспечению защиты от несанкционированного доступа со стороны обслуживающего персонала к ресурсам ИС в особых режимах ее функционирования. Методы разработки связанного с безопасностью объектно-ориентированного программного обеспечения	2
9	4	Типовой сценарий переноса обработки в случае частичного или полного выхода из строя центра обработки информации. Управление случайными отказами технических средств	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Понятие национальной безопасности; Стандарты безопасности ; Виды защищаемой информации	2
2	2	Расчет показателей доступности информационно-телекоммуникационных систем. Расчет надежности информационных систем .	2
3	2	Анализ текущих показателей катастрофоустойчивости системы. Оценка эффективности катастрофоустойчивых решений .	2
4	3	Средства обеспечения катастрофоустойчивости.	4
5	3	Разработка технического задания на катастрофоустойчивые системы	2
6	4	Организация работ по развертыванию катастрофоустойчивых решений.	2
7	4	Планы восстановления после катастроф.	2

5.3. Лабораторные работы

Не предусмотрены

5.4. Самостоятельная работа студента

Выполнение СРС		
Вид работы и содержание задания	Список литературы (с указанием разделов, глав, страниц)	Кол-во часов
Изучение дополнительной информации, не вошедшей в план лекций и практических занятий	Информационная безопасность открытых систем Т. 1 Угрозы, уязвимости, атаки и подходы к защите Учеб. для вузов по специальности 075500 (090105) "Комплекс. обеспечение информ. безопасности автоматизир. систем": В 2 т. С. В. Запечников, Н. Г. Милославская, А. И. Толстой, Д. В. Ушаков	40

6. Инновационные образовательные технологии, используемые в учебном процессе

Инновационные формы учебных занятий	Вид работы (Л, ПЗ, ЛР)	Краткое описание	Кол-во ауд. часов
Интерактивные лекции	Лекции		16

Собственные инновационные способы и методы, используемые в образовательном процессе

Не предусмотрены

Использование результатов научных исследований, проводимых университетом, в рамках данной дисциплины: нет

7. Фонд оценочных средств (ФОС) для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

7.1. Паспорт фонда оценочных средств

Наименование разделов дисциплины	Контролируемая компетенция ЗУНы	Вид контроля (включая текущий)	№№ заданий
Все разделы	ПК-2 способностью создавать и исследовать модели автоматизированных систем	Тест	1-3
Все разделы	ПК-5 способностью проводить анализ рисков информационной безопасности автоматизированной системы	Тест	4-6
Все разделы	ПК-9 способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	Тест	7-9
Все разделы	ПК-13 способностью участвовать в проектировании средств защиты информации автоматизированной системы	Тест	10-12
Все разделы	ПК-20 способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	Тест	13-15

7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
Тест	Подсчет верных ответов	Зачтено: >50% Не зачтено: <=50%

7.3. Типовые контрольные задания

Вид контроля	Типовые контрольные задания
Тест	1) Источники угроз безопасности информации могут быть: А) антропогенными Б) техногенными В) стихийными Г) все выше перечисленное 2) Выберите верное описание угрозы безопасности информации А) УБИj = [нарушитель (источник угрозы); способы реализации угрозы; объекты воздействия; последствия от реализации угрозы]. Б) УБИj = [нарушитель (источник угрозы); уязвимости; объекты воздействия; последствия от реализации угрозы]. В) УБИj = [нарушитель (источник угрозы); уязвимости; способы реализации угрозы; объекты воздействия]. Г) УБИj = [нарушитель (источник угрозы); уязвимости; способы реализации угрозы; объекты воздействия; последствия от реализации угрозы]. 3) Какой из перечисленных видов нарушителей имеет наибольший потенциал? А) Конкурирующие организации Б) Специальные службы иностранных государств В) Лица, обеспечивающие функционирование информационных систем Г) Экстремистские группировки 4) Что не характерно для верхнего уровня политики информационной безопасности? А) политика информационной безопасности служит для формулирования и демонстрации отношения руководства предприятия к вопросам информационной безопасности и отражения общих целей всего предприятия в этой области; Б) политика информационной безопасности служит основой для разработки индивидуальных политик безопасности (на более низких уровнях), правил и

	инструкций, регулирующих отдельные вопросы; В) политика информационной безопасности определяет отношение и требования к определенным информационным и телекоммуникационным технологиям, методам и подходам к обработке информации и построения информационных систем Г) политика информационной безопасности является средством информирования персонала предприятия об основных задачах и приоритетах предприятия в сфере информационной безопасности. 5) Что не характерно для среднего уровня политики информационной безопасности? А) политика информационной безопасности служит для формулирования и демонстрации отношения руководства предприятия к вопросам информационной безопасности; Б) политика информационной безопасности определяет отношение и требования предприятия к отдельным информационным потокам и информационным системам, обслуживающим различные сферы деятельности; В) политика информационной безопасности отношение и требования к определенным информационным и телекоммуникационным технологиям, методам и подходам к обработке информации и построения информационных систем; Г) политика информационной безопасности отношение и требования к сотрудникам предприятия как к участникам процессов обработки информации. 6) Что характерно для низкого уровня политики информационной безопасности? А) политика информационной безопасности служит для формулирования и демонстрации отношения руководства предприятия к вопросам информационной безопасности; Б) политика информационной безопасности определяет отношение и требования к сотрудникам предприятия как к участникам процессов обработки информации. В) Политика безопасности относится к отдельным элементам информационных систем и участкам обработки и хранения информации и описывают конкретные процедуры и документы, связанные с обеспечением информационной безопасности. Г) политика информационной безопасности является средством информирования персонала предприятия об основных задачах и приоритетах предприятия в сфере информационной безопасности. 7) Что позволяет выявить аудит информационной безопасности? А) оценить текущую безопасность функционирования корпоративной информационной системы; Б) оценить и спрогнозировать риски, а также управлять их влиянием на бизнес-процессы компании; В) корректно и обоснованно подойти к вопросу обеспечения безопасности информационных активов компании Г) все выше перечисленное 8) Что входит в число задач, решаемых в ходе проведения анализа информационной безопасности объектов на соответствие требованиям стандартов в области информационной безопасности? А) сбор и анализ данных об организационной и функциональной структуре информационной системы компании Б) анализ существующей политики обеспечения информационной безопасности В) построение модели нарушителей информационной безопасности Г) все выше перечисленное 9) Что не входит в заключительный этап аудита помещений? А) обработка результатов исследования, проведение необходимых инженерных расчетов Б) визуальный осмотр конструкций В) составление описания проведенных работ и исследований с приложением необходимых схем и планов помещений Г) составление акта проведения комплексной специальной проверки помещений 10) Для обеспечения защиты информации, содержащейся в информационной системе, проводятся следующие мероприятия: А) формирование требований к защите информации, содержащейся в информационной

	системе; разработка системы защиты информации информационной системы; Б) внедрение системы защиты информации информационной системы; аттестация информационной системы по требованиям защиты информации и ввод ее в действие; В) обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы; Г) все выше перечисленное 11) в информационных системах 1 класса защищенности применяются средства защиты информации: А) не ниже 4 класса Б) не ниже 3 класса В) не ниже 2 класса Г) 1 класса 12) Защита беспроводных соединений, применяемых в информационной системе необходимы для информационных систем: А) 1 Класса защищенности информационной системы Б) 2 Класса защищенности информационной системы В) 3 Класса защищенности информационной системы Г) всех классов защищенности 13) Что такое отказоустойчивость программного средства? А) Совокупность свойств программного средства, характеризующая его способность поддерживать необходимый уровень пригодности при проявлении дефектов программного средства или нарушении установленных интерфейсов. Б) Совокупность свойств аппаратного средства, характеризующая его способность поддерживать необходимый уровень пригодности при проявлении дефектов программного средства или нарушении установленных интерфейсов. В) Совокупность свойств программного средства, характеризующая его способность поддерживать высокий уровень пригодности при проявлении дефектов программного средства или нарушении установленных интерфейсов. Г) Совокупность свойств программного средства, подверженная проявлению дефектов программного средства или нарушению установленных интерфейсов. 14) Для какого вида отказоустойчивости верно следующее предложение: система продолжает работать в случае отказов отдельных ее элементов без существенной потери функциональных свойств А) полная Б) нулевая В) частичная Г) фрагментарная 15) Исходя из каких критериев происходит категорирование объектов критической информационной инфраструктуры? А) социальная значимость Б) политическая значимость В) экономическая значимость Г) все выше перечисленное

8. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

Не предусмотрена

б) дополнительная литература:

Не предусмотрена

в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

1. Журнал "Вестник УРФО. Безопасность в информационной сфере"

г) методические указания для студентов по освоению дисциплины:

1. Методические указания к дисциплине

из них: учебно-методическое обеспечение самостоятельной работы студента:

2. Методические указания к дисциплине

Электронная учебно-методическая документация

№	Вид литературы	Наименование разработки	Наименование ресурса в электронной форме	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
1	Основная литература	1. Российские и международные нормативные акты и стандарты в области защиты информации (доступ через сеть «Интернет»): ISO/IEC 17799 — стандарт информационной безопасности; Стандарт ЦБ РФ СТО БР ИБ БС-1.0-2010 «Обеспечение ИБ организаций банковской системы РФ. Общие положения»; BS 25777 - 2008 Управление непрерывностью информационных и телекоммуникационных услуг. Свод практик; РС БР ИББС-2.2. 2009 Методика оценки рисков нарушения информационной безопасности; ГОСТ Р МЭК 61508-2-2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью.	Консультант плюс	Интернет / Свободный
2	Основная литература	Безопасность информационных систем // Ерохин, В.В.. Москва: Флинта, 2015 База данных: Ibooks.ru	Электронный каталог ЮУрГУ	Интернет / Авторизованный
3	Основная литература	Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных систем предприятий //directmedia.74298	Электронный каталог ЮУрГУ	Интернет / Авторизованный
4	Дополнительная литература	Мельников, Д.А. Информационная безопасность открытых систем. [Электронный ресурс] : учеб. — Электрон. дан. — М. : ФЛИНТА, 2014. — 448 с. — Режим доступа: http://e.lanbook.com/book/48368 — Загл. с экрана.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
5	Основная литература	Технология построения защищенных автоматизированных систем //Карпов В.В.; Мельник В.А.. Москва: Российский новый университет База данных: IPRbooks	Электронный архив ЮУрГУ	Интернет / Авторизованный
6	Основная	Учебное пособие "Катастрофоустойчивость	Электронный	ЛокальнаяСеть /

	литература	информационных систем", авторы Плотникова Н.В,, Жернова В.М.	каталог ЮУрГУ	Авторизованный

9. Информационные технологии, используемые при осуществлении образовательного процесса

Перечень используемого программного обеспечения:

1. Microsoft-Windows(бессрочно)

Перечень используемых информационных справочных систем:

1. -Консультант Плюс(31.07.2017)
2. -База данных ВИНИТИ РАН(бессрочно)

10. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Лекции	912 (3б)	Мультимедиа
Практические занятия и семинары	913 (3б)	Компьютерный класс