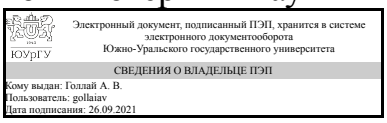
ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Высшая школа электроники и компьютерных наук



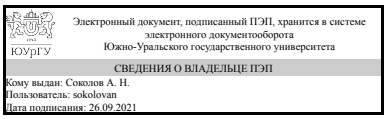
А. В. Голлай

РАБОЧАЯ ПРОГРАММА

дисциплины В.1.06 Контроль безопасности автоматизированных 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

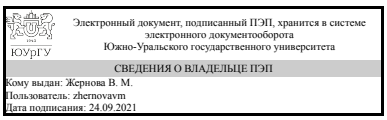
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 01.12.2016 № 1509

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



А. Н. Соколов

Разработчик программы,
к.юрид.н., доцент



В. М. Жернова

Челябинск

1. Цели и задачи дисциплины

Целью дисциплины является подготовка квалифицированных специалистов способных осуществить контроль безопасности 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; 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; вопросы 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-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-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-21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	Знать:руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; организационные меры по защите информации;
	Уметь:Уметь:разрабатывать политики безопасности информации

	автоматизированынных систем; осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации; разрабатывать документы в области обеспечения безопасности информации в автоматизированной системе при её эксплуатации (включая управление инцидентами информационной безопасности)
	Владеть:

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Б.1.28 Безопасность операционных систем	Не предусмотрены

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

Дисциплина	Требования
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
Составление технического задание на разработку катастрофоустойчивой информационной системы	40	40
Вид итогового контроля (зачет, диф.зачет, экзамен)	-	зачет

5. Содержание дисциплины

№	Наименование разделов дисциплины	Объем аудиторных занятий

раздела		по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Катастрофоустойчивость в системе национальной безопасности Российской Федерации	4	2	2	0
2	Методы обеспечения катастрофоустойчивости автоматизированных систем	10	4	6	0
3	Средства и практические решения по обеспечению катастрофоустойчивости ав-томатизированных систем	10	6	4	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	2
2	2	Обеспечение катастрофоустойчивости системы	2
3	2	Выбор рациональных решений по организации средств восстановления информационных систем после отказов и катастроф и Оптимизация средств восстановления после отказов	2
4	3	Практические решения построения средств восстановления после катастроф	2
5	3	Основы обеспечения информационной безопасности в катастрофоустойчивых центрах обработки информации	2
6	3	Принципы построения организационно-режимных мер обеспечения безопасности информации	2
7	4	Организационно-технические решения по обеспечению защиты от несанкционированного доступа со стороны обслуживающего персонала к ресурсам ИС в особых режимах ее функционирования	2
8	4	Типовой сценарий переноса обработки в случае частичного или полного выхода из строя центра обработки информации	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Понятие национальной безопасности; Виды защищаемой информации	2
2	2	Расчет показателей доступности информационно-телекоммуникационных систем	2
3	2	Методы обеспечения катастрофоустойчивости	4
4	3	Средства обеспечения катастрофоустойчивости	2
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
Составление технического задание на разработку катастрофоустойчивой информационной системы	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

Не предусмотрены

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-21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	тест	1-5
Все разделы	ПК-20 способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	тест	11-15
Все разделы	ПК-13 способностью участвовать в проектировании средств защиты информации автоматизированной системы	тест	6-10

7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
	Подсчет ответов	Зачтено: 8 и более правильных ответов Не зачтено: 7 и менее правильных ответов

7.3. Типовые контрольные задания

Вид контроля	Типовые контрольные задания
	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 кбас.pdf

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. Катастрофоустойчивость информационных систем [Текст : непосредственный] : учеб. пособие по направлению 10.03.01 и др. / В. М. Жернова, Н. В. Плотникова ; Юж.-Урал. гос. ун-т, Каф. Кафедра Защита информации ; ЮУрГУ Челябинск : Издательский Центр ЮУрГУ , 2020

из них: учебно-методическое обеспечение самостоятельной работы студента:

2. Катастрофоустойчивость информационных систем [Текст : непосредственный] : учеб. пособие по направлению 10.03.01 и др. / В. М. Жернова, Н. В. Плотникова ; Юж.-Урал. гос. ун-т, Каф. Кафедра Защита информации ; ЮУрГУ Челябинск : Издательский Центр ЮУрГУ , 2020

Электронная учебно-методическая документация

№	Вид литературы	Наименование разработки	Наименование ресурса в электронной форме	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
1	Основная литература	Катастрофоустойчивость информационных систем [Текст : непосредственный] : учеб. пособие по направлению 10.03.01 и др. / В.	Электронный каталог ЮУрГУ	ЛокальнаяСеть / Авторизованный

		М. Жернова, Н. В. Плотникова ; Юж.-Урал. гос. ун-т, Каф. Кафедра Защита информации ; ЮУрГУ Челябинск : Издательский Центр ЮУрГУ , 2020		
2	Дополнительная литература	Организация и технологии защиты информации. Обнаружение и предотвращение информационных атак в автоматизированных системах предприятий Текст учеб. пособие В. А. Сердюк ; Гос. ун-т, Высш. школа экономики. М. Издательский дом Высшей школы экономики 2011	Электронный каталог ЮУрГУ	ЛокальнаяСеть / Авторизованный
3	Основная литература	Фот, Ю. Д. Стандарты информационной безопасности : учебное пособие / Ю. Д. Фот. — Оренбург : ОГУ, 2018. — 226 с. — ISBN 978-5-7410-2297-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/159804 (дата обращения: 22.09.2021). — Режим доступа: для авториз. пользователей.	Электронно-библиотечная система издательства Лань	ЛокальнаяСеть / Авторизованный
4	Дополнительная литература	Безопасность информационных систем Текст учеб. пособие по направлению 230400 "Информ. системы и технологии" (степень "бакалавр") В. В. Ерохин, Д. А. Погонышева, И. Г. Степченко ; Брян. гос. ун-т им. И. Г. Петровского 3-е изд., стер. М. Флинта : Наука 2016	Электронный каталог ЮУрГУ	ЛокальнаяСеть / Авторизованный

9. Информационные технологии, используемые при осуществлении образовательного процесса

Перечень используемого программного обеспечения:

1. Microsoft-Office(бессрочно)

Перечень используемых информационных справочных систем:

1. ООО "ГарантУралСервис"-Гарант(бессрочно)

10. Материально-техническое обеспечение дисциплины

Не предусмотрено