ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Высшая школа электроники и компьютерных наук

ЮУрГУ
Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Голлай А. В.
Пользователь: gollaiav
Дата подписания: 12.02.2022

А. В. Голлай

РАБОЧАЯ ПРОГРАММА

дисциплины 1.О.33 Комплексное обеспечение защиты информации объектов информатизации
для направления 10.03.01 Информационная безопасность
уровень Бакалавриат
форма обучения очная
кафедра-разработчик Защита информации

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность, утверждённым приказом Минобрнауки от 17.11.2020 № 1427

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

ЮУрГУ
Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Соколов А. Н.
Пользователь: sokolovan
Дата подписания: 12.02.2022

А. Н. Соколов

Разработчик программы,
к.техн.н., доц., заведующий кафедрой

ЮУрГУ
Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Соколов А. Н.
Пользователь: sokolovan
Дата подписания: 12.02.2022

А. Н. Соколов

СОГЛАСОВАНО

Руководитель направления
к.техн.н., доц.

ЮУрГУ
Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Соколов А. Н.
Пользователь: sokolovan
Дата подписания: 12.02.2022

А. Н. Соколов

Челябинск

1. Цели и задачи дисциплины

Целью изучения дисциплины является теоретическая и практическая подготовка специалистов к деятельности, связанной с комплексным анализом возможных угроз и созданием адекватной модели нарушителя, постановкой конкретных задач заданной степени сложности в рамках модели для обеспечения информационной безопасности автоматизированных систем, а также содействие фундаментализации образования и развитию системного мышления. Задачи дисциплины: - изучение основных аспектов обеспечения информационной безопасности государства; - изучение методологии создания систем защиты информации; - изучение процессов сбора, передачи и накопления информации; - изучение основных элементов теории компьютерной безопасности; - изучение математических основ моделей безопасности; - изучение вопросов оценки защищенности и обеспечения безопасности компьютерных систем.

Краткое содержание дисциплины

Понятие национальной безопасности Российской Федерации. Роль и место информационной безопасности в системе национальной безопасности. Основы государственной политики Российской Федерации в области информационной безопасности. Информационное противоборство и способы его осуществления. Методы и средства обеспечения безопасности объектов информационной инфраструктуры Российской Федерации.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Знает: принципы формирования комплекса мер по защите информации ограниченного доступа объектов информатизации в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю Умеет: определять комплекс мер для обеспечения защиты информации объектов информатизации Имеет практический опыт: анализа информационной инфраструктуры информационной системы и ее безопасности объектов информатизации
ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	Знает: принципы организации информационных систем в соответствии с требованиями по защите информации; особенности комплексного подхода к обеспечению информационной безопасности организации Умеет: определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; разрабатывать

	проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
1.О.29.02 Организационное обеспечение информационной безопасности, 1.О.32 Программно-аппаратные средства защиты информации, ФД.02 Мониторинг информационной безопасности и активный поиск киберугроз	Не предусмотрены

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

Дисциплина	Требования
1.О.29.02 Организационное обеспечение информационной безопасности	Знает: основы организации и деятельности органов государственной власти в Российской Федерации, систему стандартов и нормативных правовых актов уполномоченных федеральных органов исполнительной власти по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации; систему нормативных правовых актов уполномоченных федеральных органов исполнительной власти по аттестации объектов информатизации и сертификации средств защиты информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях Умеет: обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав;анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации;формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации;формулировать основные требования информационной безопасности при эксплуатации автоматизированной системы;формулировать основные требования по

	защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации, использовать систему организационных мер, направленных на защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами ФСБ России, ФСТЭК России Имеет практический опыт:
1.О.32 Программно-аппаратные средства защиты информации	Знает: программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях Умеет: конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности Имеет практический опыт:
ФД.02 Мониторинг информационной безопасности и активный поиск киберугроз	Знает: методы мониторинга информационной безопасности и средства реализации удаленных сетевых атак на автоматизированные системы, организационную структуру и функциональную часть автоматизированных систем; методы и средства реализации удаленных сетевых атак на автоматизированные системы Умеет: осуществлять диагностику и мониторинг систем защиты автоматизированных систем, осуществлять управление и администрирование защищенных автоматизированных систем; разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем Имеет практический опыт: разработки политик информационной безопасности автоматизированных систем

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 4 з.е., 144 ч., 82,5 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		8
Общая трудоёмкость дисциплины	144	144
Аудиторные занятия:	72	72
Лекции (Л)	36	36
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	36	36
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	61,5	61,5
с применением дистанционных образовательных	0	

технологий		
Подготовка к практическим занятиям	22	22
Подготовка к экзамену	16	16
Подготовка к контрольным работам	23,5	23.5
Консультации и промежуточная аттестация	10,5	10,5
Вид контроля (зачет, диф.зачет, экзамен)	-	экзамен

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Информационная безопасность в системе национальной безопасности Российской Федерации	8	4	4	0
2	Основы государственной политики Российской Федерации в области информационной безопасности	20	10	10	0
3	Информационное противоборство, методы и средства его осуществления	8	4	4	0
4	Методы и средства обеспечения информационной безопасности объектов информационной инфраструктуры	36	18	18	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Понятие национальной безопасности Российской Федерации. Национальные интересы и угрозы национальной безопасности	2
2	1	Роль и место информационной безопасности в системе национальной безопасности Российской Федерации	2
3	2	Национальные интересы Российской Федерации в информационной сфере	2
4	2	Виды и источники угроз информационной безопасности Российской Федерации	2
5	2	Конституция Российской Федерации о правах и свободах человека и гражданина в информационной сфере. Виды защищаемой информации	2
6	2	Организационная система обеспечения информационной безопасности Российской Федерации	2
7	2	Структура законодательства Российской Федерации в информационной сфере. Уголовно-процессуальная характеристика компьютерных преступлений	2
8	3	Понятие информационного противоборства. Информационные войны, методы и средства их ведения	2
9	3	Информационное оружие, его классификация и возможности	2
10	4	Стратегические цели и основные направления, принципы и общие методы обеспечения информационной безопасности	2
11	4	Автоматизированная информационная система как объект защиты	2
12	4	Понятие комплексного обеспечения информационной безопасности	2
13	4	Модели и стратегии обеспечения информационной безопасности автоматизированных информационных систем	2
14	4	Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем	4

15	4	Общая характеристика методов и средств защиты информации в автоматизированных информационных системах	4
16	4	Задачи и организационная структура подразделения обеспечения информационной безопасности	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Понятие национальной безопасности Российской Федерации. Национальные интересы и угрозы национальной безопасности	2
2	1	Роль и место информационной безопасности в системе национальной безопасности Российской Федерации	2
3	2	Национальные интересы Российской Федерации в информационной сфере	2
4	2	Виды и источники угроз информационной безопасности Российской Федерации	2
5	2	Конституция Российской Федерации о правах и свободах человека и гражданина в информационной сфере. Виды защищаемой информации	2
6	2	Система обеспечения информационной безопасности Российской Федерации	2
7	2	Структура законодательства Российской Федерации в информационной сфере. Уголовно-процессуальная характеристика компьютерных преступлений	2
8	3	Понятие информационного противоборства. Информационные войны, методы и средства их ведения	2
9	3	Информационное оружие, его классификация и возможности	2
10	4	Стратегические цели и основные направления, принципы и общие методы обеспечения информационной безопасности	2
11	4	Автоматизированная информационная система как объект защиты	2
12	4	Понятие комплексного обеспечения информационной безопасности	2
13	4	Модели и стратегии обеспечения информационной безопасности автоматизированных информационных систем	4
14	4	Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем	4
15	4	Общая характеристика методов и средств защиты информации в автоматизированных информационных системах	2
16	4	Задачи и организационная структура подразделения обеспечения информационной безопасности	2

5.3. Лабораторные работы

Не предусмотрены

5.4. Самостоятельная работа студента

Выполнение СРС			
Подвид СРС	Список литературы (с указанием разделов, глав, страниц) / ссылка на ресурс	Семестр	Кол-во часов
Подготовка к практическим занятиям	Основная и дополнительная литература	8	22
Подготовка к экзамену	Основная и дополнительная литература	8	16
Подготовка к контрольным работам	Основная и дополнительная литература	8	23,5

6. Текущий контроль успеваемости, промежуточная аттестация

Контроль качества освоения образовательной программы осуществляется в соответствии с Положением о балльно-рейтинговой системе оценивания результатов учебной деятельности обучающихся.

6.1. Контрольные мероприятия (КМ)

№ КМ	Се-местр	Вид контроля	Название контрольного мероприятия	Вес	Макс. балл	Порядок начисления баллов	Учи-тыва-ется в ПА
1	8	Текущий контроль	Контрольная работа 1	2	15	Работа включает 5 вопросов. Каждый максимально оценивается в 3 балла. 3 балла – дан верный и развернутый ответ. 2 балла – дан верный, недостаточно полный ответ. 1 балл – дан верный, односложный ответ. 0 баллов – нет ответа.	экзамен
2	8	Текущий контроль	Контрольная работа 2	3	15	Работа включает 5 вопросов. Каждый максимально оценивается в 3 балла. 3 балла – дан верный и развернутый ответ. 2 балла – дан верный, недостаточно полный ответ. 1 балл – дан верный, односложный ответ. 0 баллов – нет ответа.	экзамен
3	8	Текущий контроль	Выступления на семинарах	4	10	За каждое подготовленное выступление на семинаре начисляется 2 балла. Максимальное количество выступлений за семестр - 5	экзамен
4	8	Бонус	Выступление на студенческой конференции и сдача статьи в печать	-	15	1. За подготовленный доклад и выступление на студенческой конференции под руководством преподавателя, ведущего дисциплину начисляется 5%. 2. За сдачу статьи, подготовленной по итогам выступления, в печать: - в сборник трудов конференции (РИНЦ): 5%; - в журнал, включенный в перечень ВАК: 10%.	экзамен
5	8	Проме-жуточная аттестация	Экзамен	-	10	Билет содержит 10 вопросов. Форма билета - тест. Максимально ответ на каждый вопрос оценивается в 1 балл. 1 балл - дан верный ответ; 0 балл - дан неверный ответ, либо ответ отсутствует.	экзамен

6.2. Процедура проведения, критерии оценивания

Не предусмотрены

6.3. Оценочные материалы

Компетенции	Результаты обучения	№ КМ				
		1	2	3	4	5
ОПК-6	Знает: принципы формирования комплекса мер по защите информации ограниченного доступа объектов информатизации в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	+	+	+	+	+
ОПК-6	Умеет: определять комплекс мер для обеспечения защиты информации объектов информатизации	+	+	+	+	+
ОПК-6	Имеет практический опыт: анализа информационной инфраструктуры информационной системы и ее безопасности объектов информатизации	+	+	+	+	+
ОПК-10	Знает: принципы организации информационных систем в соответствии с требованиями по защите информации; особенности комплексного подхода к обеспечению информационной безопасности организации	+	+	+	+	+
ОПК-10	Умеет: определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации	+	+	+	+	+

Фонды оценочных средств по каждому контрольному мероприятию находятся в приложениях.

7. 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. Безопасность информационных технологий 12+ М-во образования и науки Рос. Федерации, Моск. инж.-физ. ин-т (гос. ун-т), ВНИИПВТИ журнал. - М., 1997-
2. Вестник УрФО : Безопасность в информационной сфере Юж.-Урал. гос. ун-т; ЮУрГУ журнал. - Челябинск: Издательство ЮУрГУ, 2011-

г) методические указания для студентов по освоению дисциплины:

1. Перечень ГОСТов по защите информации

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Перечень ГОСТов по защите информации

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в	Библиографическое описание

		электронной форме	
1	Основная литература	Электронно-библиотечная система издательства Лань	Аверченков, В. И. Автоматизация проектирования комплексных систем защиты информации : монография / В. И. Аверченков, М. Ю. Рытов, О. М. Голембиовская. — 2-е изд. — Москва : ФЛИНТА, 2017. — 145 с. — ISBN 978-5-9765-2945-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/92913 (дата обращения: 09.01.2022). — Режим доступа: для авториз. пользователей.
2	Основная литература	Электронно-библиотечная система издательства Лань	Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2019. — 344 с. — ISBN 978-5-8114-3940-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/125739 (дата обращения: 09.01.2022). — Режим доступа: для авториз. пользователей.
3	Дополнительная литература	Электронно-библиотечная система издательства Лань	Бондаренко, И. С. Методы и средства защиты информации : учебное пособие / И. С. Бондаренко, Ю. В. Демчишин. — Москва : МИСИС, 2018. — 32 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/115269 (дата обращения: 09.01.2022). — Режим доступа: для авториз. пользователей.
4	Дополнительная литература	Электронно-библиотечная система издательства Лань	Пржегорлинский, В. Н. Объекты защиты информации : учебное пособие / В. Н. Пржегорлинский. — Рязань : РГРТУ, 2012 — Часть 1 : Элементарные объекты защиты информации — 2012. — 132 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/168181 (дата обращения: 09.01.2022). — Режим доступа: для авториз. пользователей.
5	Дополнительная литература	Электронно-библиотечная система издательства Лань	Пржегорлинский, В. Н. Объекты защиты информации : учебное пособие / В. Н. Пржегорлинский. — Рязань : РГРТУ, 2014 — Часть 2 : Комплексные объекты защиты информации — 2014. — 64 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/168180 (дата обращения: 09.01.2022). — Режим доступа: для авториз. пользователей.
6	Дополнительная литература	Электронно-библиотечная система издательства Лань	Аверченков, В. И. Автоматизация проектирования комплексных систем защиты информации : монография / В. И. Аверченков, М. Ю. Рытов, О. М. Голембиовская. — 2-е изд. — Москва : ФЛИНТА, 2017. — 145 с. — ISBN 978-5-9765-2945-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/92913 (дата обращения: 09.01.2022). — Режим доступа: для авториз. пользователей.

Перечень используемого программного обеспечения:

1. -Dia Diagram Editor(бессрочно)

Перечень используемых профессиональных баз данных и информационных справочных систем:

1. ООО "ГарантУралСервис"-Гарант(бессрочно)

8. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Практические занятия и семинары	913 (3б)	Комплект компьютерного оборудования, минитор, маршрутизатор, программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+; Операционные системы семейства Linux, Windows, СУБД промышленного масштаба (например, Microsoft SQL Server 2010, Oracle 9i и т.п), свободно распространяемые пакеты прикладных программ: утилиты резервного копирования и восстановления файловых систем и разделов НЖМД; средства диагностики и тестирования ПК; межсетевые экраны; системы обнаружения вторжений; антивирусы
Лекции	912 (3б)	Комплект компьютерного оборудования, LCD Проектор, Экран проекционный, настенные стенды по защите информации (5 шт.), программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox