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: 14.02.2022

А. В. Голлай

РАБОЧАЯ ПРОГРАММА

дисциплины 1.О.44 Обеспечение безопасности значимых объектов критической информационной инфраструктуры
для специальности 10.05.03 Информационная безопасность автоматизированных систем
уровень Специалитет
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 26.11.2020 № 1457

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: 13.02.2022

А. Н. Соколов

Разработчик программы,
старший преподаватель

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Антясов И. С.
Пользователь: antiasovis
Дата подписания: 13.02.2022

И. С. Антясов

СОГЛАСОВАНО

Руководитель специальности
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: 13.02.2022

А. Н. Соколов

Челябинск

1. Цели и задачи дисциплины

Целью преподавания дисциплины является знакомство студентов с принципами, особенностями и способами обеспечения информационной безопасности всего жизненного цикла на критически важных объектах. Задачами дисциплины являются: - изучение системы государственного контроля в области обеспечения информационной безопасности на критически важных объектах и системы признаков критически важных объектов; - обучение принципам анализа с целью выявления потенциальных уязвимостей информационной безопасности на критически важных объектах; - выработка умений классифицировать и оценивать угрозы информационной безопасности для критически важных объектов, эффективно использовать различные методы и средства защиты информации; - изучение основных средств и способов обеспечения информационной безопасности на критически важных объектах, принципов построения систем защиты информации.

Краткое содержание дисциплины

Дисциплина «Обеспечение информационной безопасности на критически важных объектах» является неотъемлемой составной частью профессиональной подготовки специалистов по специальности 090303 «Информационная безопасность автоматизированных систем», специализации «Информационная безопасность автоматизированных систем критически важных объектов». Вместе с другими дисциплинами специального цикла изучение данной дисциплины призвано формировать специалиста и, в частности, вырабатывать у него такие качества, как способностью к логическому мышлению, обобщению, анализу, критическому осмыслению и систематизации информации, а также способность самостоятельно применять методы и средства познания, обучения и самоконтроля для приобретения новых знаний и умений.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ОПК-17 (11.1) Способен планировать и разрабатывать меры по обеспечению безопасности значимых объектов критической информационной инфраструктуры	Знает: требования нормативных правовых актов в области защиты информации значимых объектов критической информационной инфраструктуры; методику формирования моделей нарушителей и методику оценки угроз безопасности информации значимых объектов критической информационной инфраструктуры; методы и средства обеспечения безопасности значимых объектов критической информационной инфраструктуры Умеет: проводить анализ исходных данных и проектных решений при разработке подсистем и средств обеспечения безопасности значимых объектов критической информационной инфраструктуры; определять источники угроз безопасности информации и проводить оценку

	возможностей нарушителей по реализации угроз безопасности информации; планировать и разрабатывать организационно-правовые и программно-технические меры по обеспечению безопасности значимых объектов критической информационной инфраструктуры Имеет практический опыт: проектирования подсистем безопасности значимых объектов критической информационной инфраструктуры

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Нет	Не предусмотрены

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

Нет

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 4 з.е., 144 ч., 75,5 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		9
Общая трудоёмкость дисциплины	144	144
Аудиторные занятия:	64	64
Лекции (Л)	32	32
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	32	32
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	68,5	68,5
с применением дистанционных образовательных технологий	0	
Проработка лекционного материала	34	34
Выполнение заданий поисково – исследовательского характера	34,5	34.5
Консультации и промежуточная аттестация	11,5	11,5
Вид контроля (зачет, диф.зачет, экзамен)	-	экзамен,КР

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах

		Всего	Л	ПЗ	ЛР
1	Объекты критической информационной инфраструктуры РФ	4	4	0	0
2	Порядок категорирования объектов критической информационной инфраструктуры	18	6	12	0
3	Особенности обеспечения информационной безопасности для всего жизненного цикла объектов критической информационной инфраструктуры.	18	8	10	0
4	Организационно-технические и режимные меры информационной безопасности на объектах критической информационной инфраструктуры.	16	8	8	0
5	Средства защиты информации, использующиеся на значимых объектах и оценка их эффективности.	6	4	2	0
6	Государственный контроль и надзор в области обеспечения информационной безопасности на значимых объектах.	2	2	0	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Основные направления государственной политики в области обеспечения безопасности критически важных объектов инфраструктуры Российской Федерации	2
2	1	Организационные основы обеспечения информационной безопасности критической информационной инфраструктуры.	2
3	2	Общий порядок категорирования. Виды категорий значимости	2
4	2	Перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значения	2
5	2	Права и обязанности субъектов критической информационной инфраструктуры	1
6	2	Порядок взаимодействия с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры	1
7	3	Стадии жизненного цикла безопасности объектов критической информационной инфраструктуры в целом	2
8	3	Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры и обеспечению их функционирования .	2
9	3	Анализ угроз безопасности информации и разработка модели угроз безопасности информации	4
10	4	Планирование и разработка мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры	2
11	4	Силы обеспечения безопасности значимых объектов	1
12	4	Установление требований к обеспечению безопасности значимого объекта	3
13	4	Политики информационной безопасности критически важных объектов	2
14	5	Средства защиты информации, использующиеся на значимых объектах и оценка их эффективности.	2
15	5	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации	2
16	6	Контроль мер обеспечения информационной безопасности на значимых объектах.	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	2	Определение принадлежности организации к субъектам критической информационной инфраструктуры	2
2	2	Определение критических процессов, нарушение и/или прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка	2
3	2	Формирование сводного перечня объектов критической информационной инфраструктуры в организации	2
4	2	Формирование исходных данных на каждый объект критической информационной инфраструктуры	4
5	2	Категорирование объектов критической информационной инфраструктуры в соответствии с перечнем показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений	2
6	3	Рассмотрение возможных действий нарушителей, иных источников угроз безопасности. Анализ угроз и уязвимостей. Подготовка модели угроз.	6
7	3	Подготовка формы направления сведений о результатах присвоения объекту одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий	2
8	3	Разработка требований к оформлению концепции для всего жизненного цикла обеспечения информационной безопасности объекта.	2
9	4	Составление плана мероприятий по обеспечению безопасности на значимом объекте	2
10	4	Разработка организационно-распорядительных документов по безопасности значимых объектов критической информационной инфраструктуры	4
11	4	Обеспечение безопасности значимого объекта в ходе его эксплуатации	2
12	5	Выбор средств защиты информации	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
Проработка лекционного материала	http://e.lanbook.com/book/94555	9	34
Выполнение заданий поисково – исследовательского характера	http://e.lanbook.com/book/111049	9	34,5

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	9	Курсовая работа/проект	курсовая работа	-	5	Отлично: Соблюдены все сроки, выполнены все этапы Хорошо: Имеются небольшие нарушения промежуточных сроков сдачи или этапы курсовой работы не выполнены в полном объеме Удовлетворительно: Нарушен срок итоговой сдачи работы или имеются существенные недостатки в проделанной работе Неудовлетворительно: Не соблюдены сроки сдачи и не выполнены основные этапы работы	кур-совые работы
2	9	Текущий контроль	проверка категорирования объектов КИИ	1	6	По окончании изучения раздела 2 проверяется этап курсовой работы в части категорирования объектов критической информационной инфраструктуры в соответствии с перечнем показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений в формате выступления. Время, отведенное на каждое выступление, 10-15 минут. Тезисы доклада и презентация представляются в виде отчета в электронный ЮУрГУ. Показатели оценивания: 1. Соответствие заданию, знание нормативно-правовой базы: 2 балла – полное соответствие заданию, все ссылки на нормативно-правовые документы корректны; 2 балл – в целом соответствие заданию, однако имеются ссылки на утратившие актуальность нормативно-правовые документы; 0 баллов – не соответствие заданию; 2. Качество оформления практической работы и презентации: 2 балла – работа имеет логичное, последовательное изложение материала. презентация дополняет и иллюстрирует доклад; 1 балл – работа в целом имеет, последовательное изложение материала, однако презентация содержит только тезисы доклада; 0 баллов - просматривается непоследовательность изложения материала, презентация не	экзамен

						соответствует содержанию доклада. 3. Качество выступления: 2 балла – студент демонстрирует глубокое знание вопросов темы, грамотно формулирует выводы и предложения, уверенно отвечает на уточняющие вопросы; 1 балл – в процессе выступления студент в целом показывает знание вопросов темы, однако затрудняется при формулировании выводов и предложений, неуверенно отвечает на уточняющие вопросы; 0 баллов – студент проявляет неуверенность, демонстрирует слабое знание вопросов темы, не в состоянии сформулировать выводы и предложения.	
3	9	Бонус	участие в конференциях	-	15	Начисляется за личное призовое место на олимпиаде конкурсе по направлению "информационная безопасность". +15% к рейтингу за международный уровень (13,5 баллов) +10% к рейтингу за российский уровень (9 баллов) +5% к рейтингу за университетский уровень (4,5 балла)	экзамен
4	9	Проме-жуточная аттестация	экзамен	-	4	Студент вытягивает два билета, 1 балл начисляется за промежуточную часть курсовой работы, 1 бонусный балл за посещаемость. Отлично: Дан развернутый правильный ответ на каждый билет (+4) Хорошо: Дан развернутый правильный ответ на каждый билет, но есть замечания в одном из ответов (+3) Удовлетворительно: Ответы на каждый билет даны с замечаниями (+2) Неудовлетворительно: Дан ответ с замечаниями только на один билет (+1)	экзамен

6.2. Процедура проведения, критерии оценивания

Не предусмотрены

6.3. Оценочные материалы

Компетенции	Результаты обучения	№ КМ			
		1	2	3	4
ОПК-17	Знает: требования нормативных правовых актов в области защиты информации значимых объектов критической информационной инфраструктуры; методику формирования моделей нарушителей и методику оценки угроз безопасности информации значимых объектов критической	+	+	+	+

	информационной инфраструктуры; методы и средства обеспечения безопасности значимых объектов критической информационной инфраструктуры				
ОПК-17	Умеет: проводить анализ исходных данных и проектных решений при разработке подсистем и средств обеспечения безопасности значимых объектов критической информационной инфраструктуры; определять источники угроз безопасности информации и проводить оценку возможностей нарушителей по реализации угроз безопасности информации; планировать и разрабатывать организационно-правовые и программно-технические меры по обеспечению безопасности значимых объектов критической информационной инфраструктуры	+	+		+
ОПК-17	Имеет практический опыт: проектирования подсистем безопасности значимых объектов критической информационной инфраструктуры	+			+

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. Открытые системы. СУБД: информ.-аналит. журн. / учредитель ЗАО "Изд-во "Открытые системы". – 1996- .-М.: Издательство "Открытые системы", 1996- .-Ежемес.

г) методические указания для студентов по освоению дисциплины:

1. Конспект лекций
2. методические указания к практическим работам
3. Прохоров, А. В.Основы защиты информации [Текст] : метод. указания к практ. занятиям / А. В. Прохоров, С. В. Денисов ; Юж.-Урал. гос. ун-т, Озерск. фил., Каф. Информатика ; ЮУрГУ. – Челябинск : Издательский Центр ЮУрГУ, 2012. – 38 с.:ил.

из них: учебно-методическое обеспечение самостоятельной работы студента:

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Основная литература	Электронно-библиотечная система издательства Лань	Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс] — Электрон. дан. — М. : Горячая линия-Телеком, 2017. — 338 с. — Режим доступа: http://e.lanbook.com/book/111049 — Загл. с экрана.

2	Дополнительная литература	Электронно-библиотечная система издательства Лань	Технические средства и методы защиты информации. [Электронный ресурс] : учеб. пособие / А.П. Зайцев [и др.]. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 616 с. — Режим доступа: http://e.lanbook.com/book/5154 — Загл. с экрана.
3	Дополнительная литература	Электронно-библиотечная система издательства Лань	Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам. [Электронный ресурс] — Электрон. дан. — М. : Горячая линия-Телеком, 2015. — 586 с. — Режим доступа: http://e.lanbook.com/book/94555 — Загл. с экрана.
4	Основная литература	Электронно-библиотечная система издательства Лань	Криулин, А. А. Основы безопасности прикладных информационных технологий и систем : учебное пособие / А. А. Криулин, В. С. Нефедов, С. И. Смирнов. — Москва : РТУ МИРЭА, 2020. — 136 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167606 (дата обращения: 16.09.2021). — Режим доступа: для авториз. пользователей.
5	Основная литература	Электронно-библиотечная система издательства Лань	Алѐшкин, А. С. Аппаратные и программные средства поиска уязвимостей при моделировании и эксплуатации информационных систем (обеспечение информационной безопасности) : учебное пособие / А. С. Алѐшкин, С. А. Лесько, Д. О. Жуков. — Москва : РТУ МИРЭА, 2020. — 152 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167600 (дата обращения: 16.09.2021). — Режим доступа: для авториз. пользователей.

Перечень используемого программного обеспечения:

Нет

Перечень используемых профессиональных баз данных и информационных справочных систем:

Нет

8. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
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, Консультант+.
Практические занятия и семинары	910 (3б)	Комплект компьютерного оборудования, Стенд по методам и средствам защиты телефонных аппаратов и телефонных линий, Стенд по биометрическим способам индикации, Стенд по противопожарной защите, Стенд по системам аналогового видеонаблюдения, Стенд по системам цифрового видеонаблюдения, Стенд по техническим средствам охраны на базе приборов «Сигнал 20» и «Сигнал 20 П», Стенд по техническим средствам охраны на базе контроллера «С200-КФЛ», Переносной комплекс для измерений «Навигатор П3Г», Комплекс контроля эффективности защиты речевой информации «Спрут-мини-А», Лабораторный стенд для исследования линий связи, Селективный микровольтметр, Осциллограф

		С1-65, Генератор импульсов Г5-54, Аппаратный шифратор, Поисковый комплекс «Пиранья», Нелинейный локатор «Родник-2К», Детектор поля, Устройство комбинированной защиты, настенные информационные стенды (3 шт.), программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Орион, VidioNET.