ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Руководитель специальности

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: 11.06.2023

А. Н. Соколов

РАБОЧАЯ ПРОГРАММА

дисциплины 1.Ф.06 Мониторинг информационной безопасности автоматизированных систем управления
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.

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: 11.06.2023

А. Н. Соколов

Разработчик программы,
старший преподаватель

ЮУрГУ
Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Антясов И. С.
Пользователь: antiasovis
Дата подписания: 07.06.2023

И. С. Антясов

Челябинск

1. Цели и задачи дисциплины

Целью изучения дисциплины «Мониторинг информационной безопасности автоматизированных систем управления» является теоретическая и практическая подготовка специалистов в области реагирования на инциденты информационной безопасности. В рамках освоения дисциплины студенты знакомятся с возможностями современных систем мониторинга информационной безопасности автоматизированных систем управления. Получают навыки по составлению технического задания на разработку, внедрение и модернизацию системы мониторинга, знакомятся с основными этапами внедрения систем мониторинга, получают представления о жизненном цикле данных систем. Изучение материала ведется в соответствии с действующим законодательством в сфере регулирования АСУ.

Краткое содержание дисциплины

Основные понятия мониторинга информационной безопасности автоматизированных систем управления. Этапы построения системы мониторинга. Процессы в системах мониторинга информационной безопасности в автоматизированных системах управления.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ПК-3 Способен выполнять работы по мониторингу и аудиту защищенности информации в автоматизированных системах	Знает: основные понятия мониторинга событий, методы сбора информации о событиях, принципы работы систем управления информацией и событиями в безопасности SIEM; принципы работы систем мониторинга информационной безопасности автоматизированных систем Умеет: использовать средства сбора и анализа информации о событиях информационной безопасности для целей мониторинга информационной безопасности; формировать правила анализа событий мониторинга информационной безопасности автоматизированных систем Имеет практический опыт: использования методов мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
1.Ф.02 Современные киберугрозы в промышленных и корпоративных системах автоматизации,	1.Ф.07 Защита электронного документооборота

1.Ф.01 Автоматизированные системы управления, 1.Ф.03 Инженерно-техническая защита информации и технические средства охраны	

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

Дисциплина	Требования
1.Ф.01 Автоматизированные системы управления	Знает: цели и задачи автоматизации управления, общие понятия автоматизированных систем управления (АСУ), жизненный цикл, функции и виды АСУ;состав автоматизированных систем управления технологическим процессом (АСУ ТП), виды обеспечения, классификацию и уровни управления АСУ ТП, место АСУ ТП в интегрированных системах управления, архитектуру промышленных сетей АСУ ТП Умеет: анализировать и моделировать информационные процессы, протекающие в системах промышленной автоматизации, применять методы и средства регистрации, записи и хранения значимых параметров потоков данных АСУ ТП Имеет практический опыт: определения ключевых точек мониторинга значимых параметров потоков данных, распределенных в информационной системе промышленных сетей АСУ ТП
1.Ф.02 Современные киберугрозы в промышленных и корпоративных системах автоматизации	Знает: актуальные угрозы информационной безопасности промышленных компаний, текущее состояние и эволюцию киберугроз как ответную реакцию на внедрение средств и мер информационной безопасности, типы современных киберугроз в промышленных и корпоративных системах автоматизации, актуальные векторы атак на промышленные сети АСУ ТП;средства и меры информационной безопасности, применяемые в промышленных и корпоративных системах автоматизации Умеет: анализировать и оценивать риски информационной безопасности в промышленных и корпоративных системах автоматизации, проводить аналитику современных киберугроз в промышленных и корпоративных системах автоматизации, актуальные векторы атак на промышленные сети АСУ ТП Имеет практический опыт: идентификации и моделирования каналов возможного деструктивного информационно-технического воздействия в промышленных и корпоративных системах автоматизации, оценки уязвимостей по отношению к современным киберугрозам промышленных сетей АСУ ТП
1.Ф.03 Инженерно-техническая защита	Знает: цели и задачи проектирования систем

информации и технические средства охраны	инженерно-технической защиты объектов;основные понятия и терминологию, принятые в проектировании систем инженерно-технической защиты объектов;основные принципы проектирования систем инженерно-технической защиты объектов, физические принципы, на которых строятся системы инженерно-технической защиты объектов Умеет: проводить анализ вероятных угроз охраняемому объекту;выбирать наиболее рациональные методы противодействия угрозам охраняемому объекту;выбирать технические средства для решения задачи охраны объекта, проводить оптимизацию структуры комплексов инженерно-технической защиты объектов Имеет практический опыт: анализа критериев оценки параметров технических средств охраны объектов;составления программы испытаний систем инженерно-технической защиты объектов

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 4 з.е., 144 ч., 72,5 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		10
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)	71,5	71,5
Подготовка к практическим занятиям	50	50
Подготовка к зачету	21,5	21.5
Консультации и промежуточная аттестация	8,5	8,5
Вид контроля (зачет, диф.зачет, экзамен)	-	диф.зачет

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Основные понятия мониторинга информационной безопасности автоматизированных систем управления	16	8	8	0
2	Этапы построения системы мониторинга	17	9	8	0
3	Процессы в системах мониторинга информационной безопасности в автоматизированных системах управления	31	15	16	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Мониторинг информационной безопасности АСУ. Требования законодательства. Действующие стандарты	3
2	1	Современные АСУ как объект защиты	2
3	1	Составные части системы мониторинга информационной безопасности автоматизированных систем управления. Основные принципы работы	3
4	2	Этапы построения системы мониторинга. Инвентаризация. Внедрение инструментальных средств мониторинга	3
5	2	Этапы построения системы мониторинга. Особенности работы современных АСУ, поиск входных точек мониторинга	3
6	2	Этапы построения системы мониторинга. Агрегация, сбор, обогащение и представление информации	3
7	3	Мониторинг инцидентов информационной безопасности	3
8	3	Особенности сбора и анализа данных событий информационной безопасности	3
9	3	Реагирование на инцидент информационной безопасности	3
10	3	Экспертиза и расследование инцидента информационной безопасности на основании данных мониторинга	3
11	3	Анализ инцидента, ликвидация последствий, разработка корректирующих мероприятий	3

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Анализ действующего законодательства в сфере мониторинга информационной безопасности АСУ.	4
2	1	Анализ действующих стандартов в сфере мониторинга информационной безопасности АСУ.	4
3	2	Этапы построения системы мониторинга. Инвентаризация. Внедрение инструментальных средств мониторинга	4
4	2	Этапы построения системы мониторинга. Агрегация, сбор, обогащение и представление информации	4
5	3	Способы и технические средства мониторинга информационной безопасности	4
6	3	Расследование и реагирование на инцидент информационной безопасности	4
7	3	Анализ причин возникновения инцидента, разработка компенсирующих мер	4
8	3	Разработка технического задания на модернизацию системы мониторинга информационной безопасности	4

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	10	50
Подготовка к зачету	Основная и дополнительная литература	10	21,5

6. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации

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	10	Текущий контроль	Защита отчета к Практической работе №1	1	10	Защита отчета по практической работе осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается своевременность предоставления отчета, качество оформления и ответы на вопросы (задаются 2 вопроса). Своевременно и правильно оформленная работа получает оценку 10 баллов. Оценка снижается: - при несвоевременной сдаче отчета на 1 балл за каждую неделю просрочки; на 1 балл за каждый неправильный (отсутствующий) ответ при защите отчета; на 2 балла, если оформление работы не соответствует требованиям либо выполнены не все задания.	дифференцированный зачет
2	10	Текущий контроль	Защита отчета к Практической работе №2	1	10	Защита отчета по практической работе осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается своевременность предоставления отчета,	дифференцированный зачет

						качество оформления и ответы на вопросы (задаются 2 вопроса). Своевременно и правильно оформленная работа получает оценку 10 баллов. Оценка снижается: - при несвоевременной сдаче отчета на 1 балл за каждую неделю просрочки; на 1 балл за каждый неправильный (отсутствующий) ответ при защите отчета; на 2 балла, если оформление работы не соответствует требованиям либо выполнены не все задания.	
3	10	Текущий контроль	Защита отчета к Практической работе №3	1	10	Защита отчета по практической работе осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается своевременность предоставления отчета, качество оформления и ответы на вопросы (задаются 2 вопроса). Своевременно и правильно оформленная работа получает оценку 10 баллов. Оценка снижается: - при несвоевременной сдаче отчета на 1 балл за каждую неделю просрочки; на 1 балл за каждый неправильный (отсутствующий) ответ при защите отчета; на 2 балла, если оформление работы не соответствует требованиям либо выполнены не все задания.	дифференцированный зачет
4	10	Текущий контроль	Защита отчета к Практической работе №4	1	10	Защита отчета по практической работе осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается своевременность предоставления отчета, качество оформления и ответы на вопросы (задаются 2 вопроса). Своевременно и правильно	дифференцированный зачет

						оформленная работа получает оценку 10 баллов. Оценка снижается: - при несвоевременной сдаче отчета на 1 балл за каждую неделю просрочки; на 1 балл за каждый неправильный (отсутствующий) ответ при защите отчета; на 2 балла, если оформление работы не соответствует требованиям либо выполнены не все задания.	
5	10	Проме-жуточная аттестация	Зачет	-	9	Преподаватель формирует билеты, которые содержат по три вопроса из списка вопросов. Во время проведения зачета студент вытягивает случайный билет, затем в аудитории письменно отвечает на 3 вопроса в билете, которые включают теоретические и практические вопросы по пройденным разделам, преподаватель проверяет ответ, беседует со студентом и оценивает ответ. За каждый вопрос студент может получить максимум 3 балла. 3 балла - студент верно изложил ответ на вопрос билета, ответил на 2 дополнительных вопросы 2 балла - студент верно изложил ответ на вопрос билета, ответил на 1 дополнительный вопрос 1 балл - студент дал частичный ответ на вопрос билета либо не ответил на дополнительные вопросы 0 баллов - студент не смог ответить на вопрос в билете	дифференцированный зачет

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
дифференцированный зачет	На зачете происходит оценивание учебной деятельности обучающихся по дисциплине на основе полученных оценок за контрольно-рейтинговые мероприятия текущего контроля и промежуточной аттестации. 90% - оценка "Отлично" 75% - оценка "Хорошо" 60% - оценка	В соответствии с пп. 2.5, 2.6 Положения

	"Удовлетворительно"	

6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ				
		1	2	3	4	5
ПК-3	Знает: основные понятия мониторинга событий, методы сбора информации о событиях, принципы работы систем управления информацией и событиями в безопасности SIEM; принципы работы систем мониторинга информационной безопасности автоматизированных систем	+	+	+	+	+
ПК-3	Умеет: использовать средства сбора и анализа информации о событиях информационной безопасности для целей мониторинга информационной безопасности; формировать правила анализа событий мониторинга информационной безопасности автоматизированных систем	+	+	+	+	+
ПК-3	Имеет практический опыт: использования методов мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем	+	+	+	+	+

Типовые контрольные задания по каждому 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:

Не предусмотрены

г) методические указания для студентов по освоению дисциплины:

1. Безопасность сетей электронных вычислительных машин [Текст : непосредственный] : метод. указания для бакалавров направления "Информ. безопасность" / С. В. Скурлаев ; под ред. А. Н. Соколова ; Юж.-Урал. гос. ун-т, Каф. Защита информации ; ЮУрГУ

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Безопасность сетей электронных вычислительных машин [Текст : непосредственный] : метод. указания для бакалавров направления "Информ. безопасность" / С. В. Скурлаев ; под ред. А. Н. Соколова ; Юж.-Урал. гос. ун-т, Каф. Защита информации ; ЮУрГУ

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Дополнительная литература	Электронно-библиотечная	Олифер, В. Г. Основы сетей передачи данных : учебное пособие / В. Г. Олифер, Н. А. Олифер. — 2-е изд. — Москва

		система издательства Лань	: ИНТУИТ, 2016. — 219 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100346 (дата обращения: 11.02.2022). — Режим доступа: для авториз. пользователей.
2	Основная литература	Электронно-библиотечная система издательства Лань	Бондарев, В. В. Анализ защищенности и мониторинг компьютерных сетей. Методы и средства : учебное пособие / В. В. Бондарев. — Москва : МГТУ им. Н.Э. Баумана, 2017. — 228 с. — ISBN 978-5-7038-4757-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/103518 (дата обращения: 11.02.2022). — Режим доступа: для авториз. пользователей.
3	Основная литература	Электронно-библиотечная система издательства Лань	Коллинз, М. Защита сетей. Подход на основе анализа данных / М. Коллинз ; перевод с английского А. В. Добровольская. — Москва : ДМК Пресс, 2020. — 308 с. — ISBN 978-5-97060-649-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/131682 (дата обращения: 11.02.2022). — Режим доступа: для авториз. пользователей.
4	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: 11.02.2022). — Режим доступа: для авториз. пользователей.
5	Дополнительная литература	Электронно-библиотечная система издательства Лань	Белоус, А. И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения : энциклопедия / А. И. Белоус, В. А. Солодуха. — Москва : Техносфера, 2021. — 482 с. — ISBN 978-5-94836-612-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/181222 (дата обращения: 15.02.2022). — Режим доступа: для авториз. пользователей.

Перечень используемого программного обеспечения:

1. -Oracle VM VirtualBox(бессрочно)

Перечень используемых профессиональных баз данных и информационных справочных систем:

1. ООО "ГарантУралСервис"-Гарант(31.12.2022)

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)	Проектор, компьютеры с операционной системой Windows 10, Средство виртуализации VIrtualBox. Дистрибутивы свободно распространяемых операционных систем и средств безопасности.