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: 25.12.2022

А. Н. Соколов

РАБОЧАЯ ПРОГРАММА

дисциплины ФД.02 Мониторинг информационной безопасности и активный поиск киберугроз
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: 25.12.2022

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: 25.12.2022

И. С. Антясов

Челябинск

1. Цели и задачи дисциплины

Целью изучения дисциплины «Мониторинг информационной безопасности и активный поиск киберугроз» является теоретическая и практическая подготовка специалистов в области реагирования на инциденты информационной безопасности. В рамках освоения дисциплины студенты знакомятся с тактикой, техниками и процедурами атак, а также способами противостояния им. На практических занятиях студенты сформируют навыки обнаружения и расследования атак. Задачи дисциплины: - планирование и организация мониторинга безопасности в компании; - использование различных источников аналитических данных об угрозах для обнаружения новых продвинутых угроз; - обнаружение и расследование вредоносной активности в инфраструктурах на базе Windows и Linux с учетом использованных злоумышленниками методов; - создание инфраструктуры для активного поиска угроз на основе решения с открытым исходным кодом.

Краткое содержание дисциплины

Архитектура, процессы и инструменты SOC. Аналитика угроз, активный поиск киберугроз. Архитектура безопасности сети, программные и аппаратные средства обеспечения безопасности сети. Типовые сетевые атаки. Методы мониторинга сети. Архитектура и средства безопасности Windows. Тактики, инструменты и платформы для постэксплуатации в Windows, методы детектированя и противодействия. Архитектура и средства безопасности Linux.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ОПК-13 Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем	Знает: организационную структуру и функциональную часть автоматизированных систем; методы и средства реализации удаленных сетевых атак на автоматизированные системы Умеет: 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
ОПК-15 Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	Знает: методы мониторинга информационной безопасности и средства реализации удаленных сетевых атак на автоматизированные системы Умеет: осуществлять диагностику и мониторинг систем защиты автоматизированных систем

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
1.О.36 Информационная безопасность открытых систем, 1.О.35 Безопасность операционных систем, 1.О.34 Безопасность сетей электронных вычислительных машин	1.О.38.02 Эксплуатация автоматизированных систем в защищенном исполнении, 1.О.41 Управление информационной безопасностью, 1.О.47 Измерительная аппаратура контроля защищенности объектов информатизации, 1.О.39 Контроль безопасности автоматизированных систем

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

Дисциплина	Требования
1.О.34 Безопасность сетей электронных вычислительных машин	Знает: методы администрирования вычислительных сетей, методы проектирования вычислительных сетей Умеет: администрировать вычислительные сети и реализовывать политику безопасности вычислительной сети, проектировать вычислительные сети Имеет практический опыт: администрирования локальных вычислительных сетей с учетом требований по обеспечению информационной безопасности, эксплуатации локальных вычислительных сетей
1.О.36 Информационная безопасность открытых систем	Знает: принципы формирования политики информационной безопасности в автоматизированных системах , риски подсистем защиты информации автоматизированных систем и экспериментальные методы их оценки Умеет: разрабатывать частные политики информационной безопасности автоматизированных систем , анализировать и оценивать угрозы информационной безопасности автоматизированных систем Имеет практический опыт: управления процессами обеспечения безопасности автоматизированных систем, анализа информационной инфраструктуры автоматизированных систем
1.О.35 Безопасность операционных систем	Знает: методы администрирования операционных систем семейств UNIX и Windows, принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows Умеет: настраивать политику безопасности операционных систем семейств UNIX и Windows, формулировать политику безопасности операционных систем семейств UNIX и Windows Имеет практический опыт: настройки операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности, установки операционных систем семейств

	Windows и Unix

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 2 з.е., 72 ч., 36,25 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		7
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)	35,75	35,75
Самостоятельная проработка лекционного и практического материала	20	20
Самостоятельная работа с предоставленными источниками информации	15,75	15.75
Консультации и промежуточная аттестация	4,25	4,25
Вид 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	Основные концепции построения и функционирования SOC	6	4	2	0
2	Безопасность сети и периметра, мониторинг безопасности сети	10	4	6	0
3	Архитектура и средства безопасности Windows	12	4	8	0
4	Архитектура и средства безопасности Linux	4	4	0	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Современное положение в области киберугроз. Задачи и подходы операционной безопасности. Архитектура, процессы и инструменты SOC	2
2	1	Аналитика угроз, активный поиск киберугроз	2
3	2	Архитектура безопасности сети, программные и аппаратные средства обеспечения безопасности сети	1
4	2	Типовые сетевые атаки	2
5	2	Методы мониторинга сети	1
6	3	Архитектура и средства безопасности Windows	2

7	3	Тактики, инструменты и платформы для постэксплуатации в Windows, методы детектированя и противодействия	2
8	4	Архитектура и средства безопасности Linux	2
9	4	Журналы Linux, средства мониторинга, Auditd	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Стек Elasticsearch, Logstash, Kibana (ELK). Настройка среды ELK	2
2	2	Обнаружение атаки ARP-poisoning	1
3	2	Система обнаружения вторжений Bro	2
4	2	Система обнаружения вторжений Suricata IDS	2
5	2	Детектирование атак на сервер	1
6	3	Безопасность Windows: права пользователей, незашифрованные пароли и хеши в памяти, привилегии, атаки с кражей токенов, UAC	2
7	3	Аудит безопасности Windows. Конфигурация политики аудита. Переадресация событий в TELK. Аудит доступа к объектам. Обогащение данными с помощью Logstash. Поиск угроз и анализ журналов вручную	2
8	3	Автоматический поиск угроз с использованием X-Pack watcher	2
9	3	Развертывание и использование Sysmon	1
10	3	Autorun, анализ данных Logstash и проверка потоков	1

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
Самостоятельная проработка лекционного и практического материала		7	20
Самостоятельная работа с предоставленными источниками информации	Учебно-методические материалы в электронном виде - источники № 1-4	7	15,75

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	Вес	Макс. балл	Порядок начисления баллов	Учи-тыва

			мероприятия				- ется в ПА
1	7	Текущий контроль	Защита отчета к Практической работе №1 "Стек Elasticsearch, Logstash, Kibana (ELK). Настройка среды ELK Обнаружение атаки ARP-poisoning"	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.	зачет
2	7	Текущий контроль	Защита отчета к Практической работе №2 "Система обнаружения вторжений Bro Система обнаружения вторжений Suricata IDS"	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.	зачет
3	7	Текущий контроль	Защита отчета к Практической работе №3 "Аудит безопасности Windows. Конфигурация политики аудита. Переадресация событий в TELK. Аудит доступа к объектам. Обогащение данными с помощью Logstash."	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	зачет

						либо выполнены не все задания.	
4	7	Текущий контроль	Защита отчета к Практической работе №4 "Поиск угроз и анализ журналов вручную"	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.	зачет
5	7	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	зачет

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
зачет	На зачете происходит оценивание учебной деятельности обучающихся по дисциплине на основе полученных оценок за контрольно-рейтинговые мероприятия текущего контроля. Зачтено: рейтинг обучающегося по результатам работы в семестре больше или равен 60 %. Не зачтено: рейтинг обучающегося менее 60 %.	В соответствии с пп. 2.5, 2.6 Положения

6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ				
		1	2	3	4	5
ОПК-13	Знает: организационную структуру и функциональную часть автоматизированных систем; методы и средства реализации удаленных сетевых атак на автоматизированные системы	+	+	+	+	+
ОПК-13	Умеет: осуществлять управление и администрирование защищенных автоматизированных систем; разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	+	+	+	+	+
ОПК-13	Имеет практический опыт: разработки политик информационной безопасности автоматизированных систем	+	+	+	+	+
ОПК-15	Знает: методы мониторинга информационной безопасности и средства реализации удаленных сетевых атак на автоматизированные системы	+	+	+	+	+
ОПК-15	Умеет: осуществлять диагностику и мониторинг систем защиты 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:

1. Таненбаум, Э. Компьютерные сети [Текст] пер. с англ. Э. Таненбаум, Д. Уэзеролл. - 5-е изд. - СПб. и др.: Питер, 2015. - 955 с. ил.
2. Таненбаум, Э. Современные операционные системы [Текст] Э. Таненбаум. - 3-е изд. - СПб. и др.: Питер, 2010. - 1115 с. ил.

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	Библиографическое описание

		электронной форме	
1	Основная литература	Электронно-библиотечная система издательства Лань	Олифер, В. Г. Основы сетей передачи данных : учебное пособие / В. Г. Олифер, Н. А. Олифер. — 2-е изд. — Москва : ИНТУИТ, 2016. — 219 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100346 (дата обращения: 18.09.2021). — 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: 18.09.2021). — 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: 18.09.2021). — Режим доступа: для авториз. пользователей.
4	Дополнительная 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: 18.09.2021). — Режим доступа: для авториз. пользователей.

Перечень используемого программного обеспечения:

1. Microsoft-Windows server(бессрочно)
2. Microsoft-Windows(бессрочно)
3. -Oracle VM VirtualBox(бессрочно)

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
Практические занятия и семинары	913 (3б)	Проектор, компьютеры с операционной системой Windows 10, Средство виртуализации VIrtualBox. Дистрибутивы свободно распространяемых операционных систем и средств безопасности.