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: 05.10.2021

А. В. Голлай

РАБОЧАЯ ПРОГРАММА

дисциплины Ф.02 Мониторинг информационной безопасности и активный поиск киберугроз
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.

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: 05.10.2021

А. Н. Соколов

Разработчик программы,
преподаватель

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Уфимцев М. С.
Пользователь: ufimtcevms
Дата подписания: 04.10.2021

М. С. Уфимцев

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 (ЗУНы)
ПК-28 способностью управлять информационной безопасностью автоматизированной системы	Знать:основные методы управления информационной безопасностью
	Уметь:разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем
	Владеть:методами управления информационной безопасностью автоматизированных систем
ПК-20 способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	Знать:программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях
	Уметь:проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы
	Владеть:навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных

	сетей, программных систем с учетом требований по обеспечению информационной безопасности; навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ
ПСК-3.5 способностью проектировать, внедрять и использовать системы мониторинга средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов	Знать:организационную структуру и функциональную часть автоматизированных систем; методы и средства реализации удаленных сетевых атак на автоматизированные системы
	Уметь:осуществлять управление и администрирование защищенных автоматизированных систем; разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем
	Владеть:навыками разработки политик информационной безопасности автоматизированных систем

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Б.1.27 Безопасность сетей электронных вычислительных машин, Б.1.28 Безопасность операционных систем, Б.1.36 Информационная безопасность открытых систем	Б.1.30.01 Разработка защищенных автоматизированных систем

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: принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows; методы администрирования операционных систем семейств UNIX и Windows. Уметь: формулировать и настраивать политику безопасности операционных систем семейств UNIX и Windows.
Б.1.36 Информационная безопасность открытых систем	Знать: принципы формирования политики информационной безопасности в информационных (автоматизированных) системах. Уметь: разрабатывать частные политики информационной безопасности информационных (автоматизированных) систем
Б.1.27 Безопасность сетей электронных вычислительных машин	Знать: основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в сетях ЭВМ. Уметь: эффективно использовать различные методы и средства защиты информации для компьютерных

	сетей; проводить мониторинг угроз безопасности компьютерных сетей. Владеть: навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ

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
		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)	40	40
Самостоятельная работа с предоставленными источниками информации	20	20
Самостоятельная проработка лекционного и практического материала	20	20
Вид итогового 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		
Вид работы и содержание задания	Список литературы (с указанием разделов, глав, страниц)	Кол-во часов
Подготовка отчетов к проделанным практическим работам.	Электронная учебно-методическая документация Основная литература: [2] - Главы 1-26, [3] - Главы 1-15. Дополнительная литература: [4] - Страницы 38-84.	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-28 способностью управлять информационной безопасностью автоматизированной системы	Текущий контроль (проверка отчетов)	1-29
Все разделы	ПСК-3.5 способностью проектировать, внедрять и использовать системы мониторинга средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов	Зачет	1-29
Все разделы	ПК-20 способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	Зачет	1-29

7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
Зачет	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.	Зачтено: знает основной материал дисциплины; верно излагает и интерпретирует знания; изложение материала логически выстроено Не зачтено: не знает значительной части материала дисциплины; ответ не дан или допускает грубые ошибки при изложении ответа на вопрос; неверно излагает и интерпретирует знания
Текущий контроль (проверка отчетов)	По каждой практической работе студент составляет отчет, содержащий скриншоты или тексты конфигураций систем защиты информации, рассматриваемых в практической работе, а также пояснения, касающиеся хода выполнения практической работы. Проверяется правильность работы системы защиты, полнота тестирования и уровень самостоятельности выполнения задания.	Зачтено: Отчет соответствует требованиям. Работа выполнена самостоятельно. Конфигурация системы защиты соответствует требованиям. Отчет сдан своевременно. Не зачтено: Отчет не соответствует требованиям. Работа выполнена с невысоким уровнем самостоятельности. Конфигурация содержит ошибки.

7.3. Типовые контрольные задания

Вид контроля	Типовые контрольные задания

Зачет	1. Задачи и подходы операционной безопасности. Архитектура, процессы и инструменты SOC. Типичная инфраструктура SOC 2. Сетевые экраны. Системы обнаружения и предотвращения вторжений (IPS/IDS) 3. Решения для обнаружения нарушений безопасности 4. Аналитика угроз (Threat intelligence, TI). Что такое TI. Уровни TI: тактический, стратегический, операционный, Источники и методы TI: HUMINT, OSINT 5. От реактивного к проактивному: атаки без вредоносного ПО, целевые атаки, бесфайловые атаки 6. Фреймворк MITRE ATT&CK и цепочка поражения атаки. Обнаружение на основе TTP1 7. Процесс активного поиска угроз. Что такое стек ELK. Возможности Logstash. KIBANA: синтаксис запросов и панели мониторинга, Beats. 8. Архитектура безопасности сети: сегментация, безопасность зон. 9. Устройства для обеспечения безопасности сети. 10. Типовые сетевые атаки, инструменты атак и мониторинг сети 11. Что такое NSM. Источники данных для NSM. Основные возможности NSM 12. Анализ журналов транзакций: прокси, почта, DNS, веб 13. Обнаружение вторжений на уровне сети (Network intrusion detection system, NIDS): Snort, Suricata 14. Фреймворк мониторинга безопасности сети Bro 15. Архитектура и средства безопасности Windows 16. Журналы Windows и мониторинг 17. Расширенная и устаревшая политики аудита 18. Важные события Windows и причины их значимости 19. Анализ журналов вручную: средство просмотра событий Windows, PowerShell, LogParser 20. Переадресация событий Windows 21. Дополнительные источники журналов Windows: Sysmon, Autoruns 22. Тактики, инструменты и платформы для постэксплуатации в Windows 23. Атаки на Active Directory и их обнаружение 24. Архитектура и средства безопасности Linux 25. Журналы Linux и мониторинг 26. Важные журналы Linux и какую информацию из них можно извлечь 27. Централизованная обработка журналов Linux 28. Аудит систем в Linux с помощью Auditd 29. Тактики, инструменты и платформы для постэксплуатации в Linux
Текущий контроль (проверка отчетов)	Пример вопросов и тем, которые должен освятить студент в отчете. 1. Скриншот KIBANA с логами Suricata 2. Скриншот KIBANA, где видно срабатывание созданного кастомного правила 3. Скриншот с KIBANA, где видна реакция на срабатывание кастомного правила

8. 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 электронной форме	Библиографическое описание
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.

9. Информационные технологии, используемые при осуществлении образовательного процесса

Перечень используемого программного обеспечения:

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

Перечень используемых информационных справочных систем:

Нет

10. 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.