ФГБОУ ВО «Санкт-Петербургский университет ГПС МЧС России»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И УПРАВЛЕНИЕ КОМПЬЮТЕРНЫМИ ИНЦИДЕНТАМИ

Специалитет по специальности
10.05.03 – Информационная безопасность автоматизированных систем

Специализация «Анализ безопасности информационных систем»

Санкт-Петербург

1. Цели и задачи дисциплины

Цель освоения дисциплины:
является изучение программно-аппаратных средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях, разработка методики мониторинга информационных систем и применять средства мониторинга для оценки защищенности автоматизированных систем

Перечень компетенций, формируемых в процессе изучения дисциплины

Компетенции	Содержание
ПК - 2	Способен проводить инструментальный мониторинг защищенности информации в компьютерных системах и сетях

Задачи дисциплины:

– использовать средства сбора и анализа информации о событиях информационной безопасности для целей мониторинга информационной безопасности;

– изучение методов и мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем;

– изучение основных понятий мониторинга событий, методы сбора информации о событиях, принципы работы систем управления информацией и событиями безопасности SIEM.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
ПК-2.1 Использует основные понятия мониторинга событий, методы сбора информации о событиях, принципы работы систем управления информацией и событиями безопасности	**Знает** основные понятия мониторинга событий, методы сбора информации о событиях, принципы работы систем управления информацией и событиями безопасности **Умеет** применять основные понятия мониторинга событий, методы сбора информации о событиях, принципы работы систем управления информацией и событиями безопасности
ПК-2.2 Демонстрирует навыки сбора и анализа информации о событиях информационной безопасности для целей мониторинга информационной	**Знает** способы проведения проверки работоспособности и эффективности применяемых программно-аппаратных средств защиты информации

безопасности	**Умеет** проводить анализ уязвимости программных и программно-аппаратных средств системы защиты информации и экспертизу состояния защищенности информации автоматизированных систем
ПК-2.3 Применяет методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем	**Знает** основные мероприятия по оценке защищенности компьютерных систем и сетей в рамках расследования инцидентов информационной безопасности **Умеет** проводить основные мероприятия по оценке защищенности компьютерных систем и сетей в рамках расследования инцидентов информационной безопасности

3. Место дисциплины в структуре ОПОП

Дисциплина «Мониторинг информационной безопасности и управление компьютерными инцидентами» относится к части, формируемой участниками образовательных отношений, образовательной программы специалитета по специальности **10.05.03 – Информационная безопасность автоматизированных систем**, специализация **– Анализ безопасности информационных систем**.

4. Структура и содержание

Дисциплина «Мониторинг информационной безопасности и управление компьютерными инцидентами» реализуется:

Для очной формы обучения в рамках вариативной части образовательной программы в объеме 180 академических часов (5 зачетных единицы).

4.1 Распределение трудоемкости дисциплины по видам работ по семестрам для очной формы обучения

Вид учебной работы	Трудоемкость			
	з.е.	час.	по семестрам	
			9	10
Общая трудоемкость дисциплины по учебному плану	**5**	**180**	**72**	**108**
Контактная работа, в том числе:		**74**	**36**	**38**
Аудиторные занятия		**72**	**36**	**36**
Лекции (Л)		28	14	14
Практические занятия (ПЗ)		44	22	22
Консультация		**2**		**2**
Самостоятельная работа (СРС)		**70**	**36**	**34**
Зачет с оценкой			+	
Экзамен		**36**		**36**

4.2. Тематический план, структурированный по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий для очной формы обучения

Наименование разделов и тем	Всего часов	Количество часов по видам занятий				Самостоятельная работа
		Лекции	Практические занятия	Консультации	Контроль	
9 семестр						
Теоретические основы мониторинга защищенности	72	14	22			36
Зачет с оценкой	+					
итого за 9 семестр	**72**	**14**	**22**			**36**
10 семестр						
Проектирование системы мониторинга	70	14	22			34
Консультации	2			2		
Экзамен	36				36	
итого за 10 семестр	**108**	**14**	**22**	**2**	**36**	**34**
Всего	**180**	**28**	**44**	**2**	**36**	**70**

4.3 Содержание дисциплины для очной формы обучения

Раздел 1. Теоретические основы мониторинга защищенности

Лекции. Основные понятия. Структура системы. Основные понятия мониторинга событий. Методы сбора информации о событиях. Методы обработки информации о событиях. Структура системы мониторинга. Программно-техническая часть системы. Структура SIEM. Агенты мониторинга. Сервер событий. Хранилище данных. Консоль управления. Документационная и кадровая части системы. Задачи персонала системы мониторинга. Роли персонала: системный администратор, администратор информационной безопасности, оператор, аналитик. Нормативные документы. Политика мониторинга информационных систем. Виды информации и основные методы ее защиты. Виды угроз информационной безопасности Российской Федерации. Причины, виды, каналы утечки и искажения информации. Технические средства и методы защиты информации.

Практические занятия. Анализ рисков ИБ. Подготовка к менеджменту инцидентов ИБ. Политика обработки сообщений о событиях и инцидентах ИБ. Создание группы реагирования на инциденты информационной безопасности. Использование системы менеджмента инцидентов ИБ. Обнаружение и оповещение о событиях ИБ. Отчеты о событиях и инцидентах информационной безопасности.

Самостоятельная работа. Событие информационной безопасности. Инцидент информационной безопасности. Структурный подход к менеджменту инцидентов ИБ. Этапы менеджмента инцидентов ИБ. Менеджмент и анализ рисков ИБ. Инциденты информационной безопасности и их причины. Планирование и подготовка к менеджменту инцидентов ИБ. Политика обработки сообщений о событиях и инцидентах ИБ. Структура менеджмента инцидентов ИБ. Политика менеджмента инцидентов информационной безопасности. Программа менеджмента инцидентов информационной безопасности. Политики менеджмента рисков и информационной безопасности. Создание группы реагирования на инциденты информационной безопасности. Использование системы менеджмента инцидентов ИБ. Обнаружение и оповещение о событиях ИБ. Оценка и принятие решений по событиям/инцидентам. Реагирование на инциденты. Анализ инцидентов ИБ и процесса менеджмента инцидентов ИБ. Улучшение анализа рисков и менеджмента ИБ.

Рекомендуемая литература:

основная: [1];

дополнительная: [1,2]

Раздел 2. Проектирование системы мониторинга

Лекции. Обследование информационной системы. Идентификация основных источников событий безопасности, определение технологии сбора, хранения и обработки данных. Формирование требований к архитектуре и функциональным возможностям системы мониторинга информационно безопасности. Структура SIEM. Агенты мониторинга. Сервер событий. Хранилище данных. Консоль управления. Выбор оборудования и программного обеспечения. Конфигурация оборудования и программного обеспечения. Порядок внедрения, схема информационных потоков, требования к внешнему окружению системы мониторинга. Пилотное внедрение. Тестовый район. Апробация решений. Корректировка системы. Промышленное внедрение. Организация обучения персонала. Техническое сопровождение проекта. Реагирование на инциденты. Разработка новых правил анализа событий мониторинга. Программно-аппаратные средства обеспечения информационной безопасности. Тестовые испытания программных средств защиты. Защита от утечек по каналу ПЭМИН, по акустическому и виброакустическому каналам. Анализ сетевой топологии и установленных сервисов.

Практические занятия. Установка и настройка MaxPatrol SIEM. Управление компьютерами в MaxPatrol SIEM. Сбор событий в MaxPatrol SIEM. Работа с инцидентами в MaxPatrol SIEM. Работа с отчетами и мониторинг в MaxPatrol SIEM.

Самостоятельная работа. Техническая и другая поддержка реагирования на инциденты информационной безопасности. Электронные базы данных событий/инцидентов ИБ и технические средства для быстрого пополнения и обновления базы данных. SIEM-системы: IBM QRadar, MaxPatrol SIEM, ArcSight, Splunk и другие. Технологические трендыразвития SIEM-систем.

Рекомендуемая литература:

основная: [1];

дополнительная: [1,2]

5. Методические рекомендации по организации изучения дисциплины «Мониторинг информационной безопасности и управление компьютерными инцидентами»

При реализации программы дисциплины используются лекционные и практические занятия.

Общими целями занятий являются:

– обобщение, систематизация, углубление, закрепление теоретических знаний по конкретным темам дисциплины;

– формирование умений применять полученные знания на практике, реализация единства интеллектуальной и практической деятельности;

– выработка при решении поставленных задач профессионально значимых качеств: самостоятельности, ответственности, точности, творческой инициативы.

Целями лекции являются:

– систематизированные основы научных знаний по дисциплине, раскрывать состояние и перспективы развития соответствующей области науки и техники;

– концентрировать внимание обучающихся на наиболее сложных и узловых вопросах;

– стимулировать их активную познавательную деятельность и способствовать формированию творческого мышления.

В ходе практического занятия обеспечивается процесс активного взаимодействия обучающихся с преподавателем; приобретаются практические навыки и умения. Цели практического занятия: выработка практических умений и приобретение навыков, закрепление пройденного материала по соответствующей теме дисциплины.

Самостоятельная работа обучающихся направлена на углубление и закрепление знаний, полученных на лекциях и других занятиях, выработку навыков самостоятельного активного приобретения новых, дополнительных знаний, подготовку к предстоящим занятиям.

6. Оценочные материалы по дисциплине «Мониторинг информационной безопасности и управление компьютерными инцидентами»

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины, проводится в соответствии с содержанием дисциплины по видам занятий в форме опроса и тестирования.

Промежуточная аттестация обеспечивает оценивание промежуточных и окончательных результатов обучения по дисциплине, проводится в форме зачета с оценкой в 9 семестре и экзамена в 10 семестре.

6.1. Примерные оценочные материалы:

6.1.1. Текущего контроля

Типовые вопросы для опроса:

1. Общая модель процесса аудита информационной безопасности объекта
2. Методы оценки информационной безопасности защищённых автоматизированных систем.
3. Этапы, процедуры аудита информационной безопасности защищённых автоматизированных систем и организаций.

Типовые вопросы для теста:

1. Какие ресурсы используют при построении модели информационных потоков в ГРИФ?

Группы пользователей и права доступа
Сервер и рабочая станция
Риски и контрмеры

2. По каким угрозам в системе ГРИФ не оценивается ущерб?

Конфиденциальности
Целостности
Достоверность
Доступность

3. Как повлияет на веса средств защиты ответ «Положения политики внедрены частично»на первый вопрос раздела о политике безопасности?

Не повлияет
Приравняет к нулю
Вызовет уменьшение
Вызовет рост

4. Какие данные нельзя указать при задании контрмер в системе ГРИФ?

Стоимость внедрения
Возможное снижение затрат на ИБ
Срок внедрения контрмеры
Название для отчета

5. Что понимается под эффективностью средства защиты информации?
Показатель быстродействия системы в условиях использования средств защиты информации
Коэффициент снижения уровня риска по отношению к первоначальному уровню
Степень влияния на защищенность информации и рабочего места группы пользователей
Субъективная оценка экспертами корректности функционирования средства защиты информации

Примерный перечень вопросов выносимых на зачет с оценкой

1. Основные понятия. Структура системы.
2. Основные понятия мониторинга событий.
3. Методы сбора информации о событиях.
4. Методы обработки информации о событиях.
5. Структура системы мониторинга.
6. Программно-техническая часть системы.
7. Структура SIEM. Агенты мониторинга. Сервер событий. Хранилище данных. Консоль управления.
8. Документационная и кадровая части системы.
9. Задачи персонала системы мониторинга.
10. Роли персонала: системный администратор, администратор информационной безопасности, оператор, аналитик.
11. Нормативные документы мониторинга защищенности.
12. Политика мониторинга информационных систем.
13. Виды информации и основные методы ее защиты.
14. Виды угроз информационной безопасности Российской Федерации.
15. Причины, виды, каналы утечки и искажения информации.
16. Технические средства и методы защиты информации.

Примерный перечень вопросов выносимых на экзамен

1. Формирование политики управления инцидентами ИБ. Основное содержание политикиуправления инцидентами ИБ.
2. Создание группы реагирования на инциденты ИБ. Цель создания. Роли группы реагирования на инциденты ИБ .

3. Подготовка к обработке инцидентов ИБ. Классификация инцидентов ИБ по значимости.

4. Обеспечение осведомленности и обучение управлению инцидентами. Цель осведомления об управлении инцидентами ИБ. Цель обучения управлению инцидентами ИБ.

5. Тестирование системы управления инцидентами ИБ.

6. Первичная оценка событий ИБ. Цель проведения первичной оценки. Последовательность действий при проведении первичной оценки.

7. Вторичная оценка инцидента ИБ. Цель проведения вторичной оценки. Последовательность действий при проведении вторичной оценки.

8. Сдерживание, устранение инцидента ИБ и восстановление после него.

9. Формирование и хранение свидетельств инцидентов ИБ.

10. Определение инцидента неавторизованного доступа. Цели инцидента неавторизованного доступа.

11. Определение инцидента отказа в обслуживании. Цели инцидента отказа в обслуживании. Примеры инцидентов отказа в обслуживании.

12. Определение инцидента сбора информации. Цели инцидента сбора информации.

13. Определение инцидента внедрения вредоносного кода. Средства реализации инцидента внедрения вредоносного кода. Цели инцидента.

14. Определение инцидента несоответствующего использования. Примеры инцидентов несоответствующего использования.

15. Стратегии управления непрерывностью функционирования АС для помещений и технологий.

16. Стратегии управления непрерывностью функционирования АС для данных.

17. Стратегии управления непрерывностью функционирования АС для поставщиков.

18. Стратегии управления непрерывностью функционирования АС для компьютеров.

19. Стратегии управления непрерывностью функционирования АС для серверов.

20. Стратегии управления непрерывностью функционирования АС для локальной сети.

21. Привести пример формы сообщения «Отчет о событии ИБ» сотрудника, обнаружившего нештатную ситуацию, имеющую отношение к ИБ.

22. Привести пример формы сообщения «Отчет об инциденте ИБ» сотрудника ГРИИБ, проводившего первичную оценку событий ИБ.

23. Привести пример матрицы для определения значимости инцидентов неавторизованного доступа.

24. Определить предвестники и указатели инцидентов неавторизованного доступа.

25. Определить меры по сдерживанию, устранению инцидентов

неавторизованного доступа и восстановлению после них.

26. Привести пример матрицы для определения значимости инцидентов отказа в обслуживании.

27. Определить предвестники и указатели инцидентов отказа в обслуживании.

28. Определить меры по сдерживанию, устранению инцидентов отказа в обслуживании ивосстановлению после них.

29. Привести пример матрицы для определения значимости инцидентов сбора информации

30. Определить предвестники и указатели инцидентов сбора информации.

31. Определить меры по сдерживанию, устранению инцидентов сбора информации и восстановлению после них.

32. Привести пример матрицы для определения значимости инцидентов внедрения вредоносного кода.

33. Определить предвестники и указатели инцидентов внедрения вредоносного кода.

34. Определить меры по сдерживанию, устранению инцидентов внедрения вредоносного кода и восстановлению после них.

35. Привести пример матрицы для определения значимости инцидентов несоответствующего использования.

36. Определить предвестники и указатели инцидентов несоответствующего использования. Определить меры по сдерживанию, устранению инцидентов несоответствующего использования и восстановлению после них.

6.2. Шкала оценивания результатов промежуточной аттестации и критерии выставления оценок

Форма контроля	Показатели оценивания	Критерии выставления оценок	Шкала оценивания
Экзамен, зачет с оценкой	правильность и полнота ответа; выполнение контрольных нормативов	дан правильный, полный ответ на поставленный вопрос, показана совокупность осознанных знаний по дисциплине, доказательно раскрыты основные положения вопросов; могут быть допущены недочеты, исправленные самостоятельно в процессе ответа.	отлично
		дан правильный, недостаточно полный ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи; могут быть допущены недочеты, исправленные с помощью преподавателя.	хорошо
		дан недостаточно правильный и	удовлетворительно

		полный ответ; логика и последовательность изложения имеют нарушения; в ответе отсутствуют выводы.	
		ответ представляет собой разрозненные знания с существенными ошибками по вопросу; присутствуют фрагментарность, нелогичность изложения; дополнительные и уточняющие вопросы не приводят к коррекции ответа на вопрос.	неудовлетворительно

7. Ресурсное обеспечение дисциплины «Мониторинг информационной безопасности и управление компьютерными инцидентами»

7.1. Лицензионное и свободно распространяемое программное обеспечение

Перечень лицензионного и свободно распространяемого программного обеспечения:

- МойОфис Образование [ПО-41В-124] - Полный комплект редакторов текстовых документов и электронных таблиц, а также инструментарий для работы с графическими презентациями [Свободно распространяемое. Номер в Едином реестре российских программ для электронных вычислительных машин и баз данных - 4557]

- Astra Linux Common Edition релиз Орел [ПО-25В-603] - Операционная система общего назначения "Astra Linux Common Edition" [Коммерческая (Full Package Product). Номер в Едином реестре российских программ для электронных вычислительных машин и баз данных - 4433]

7.2. Профессиональные базы данных и информационные справочные системы

1. Информационная система «Единое окно доступа к образовательным ресурсам» [Электронный ресурс]. – Режим доступа: http://window.edu.ru/, доступ только после самостоятельной регистрации
2. Научная электронная библиотека «eLIBRARY.RU» [Электронный ресурс]. – Режим доступа: https://www.elibrary.ru/, доступ только после самостоятельной регистрации
3. Справочная правовая система «КонсультантПлюс: Студент» [Электронный ресурс]. – Режим доступа: http://student.consultant.ru/, свободный доступ
4. Информационно-правовой портал «Гарант» [Электронный ресурс]. – Режим доступа: http://www.garant.ru/, свободный доступ

7.3. Литература

Основная литература:

1. Давидюк, Н.В. Мониторинг безопасности информационных систем :

учебное пособие / Н. В. Давидюк, И. М. Космачева. — Санкт-Петербург : Интермедия, 2020. — 116 с. — ISBN 978-5-4383-0204-9. — Текст : электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/161352 (дата обращения: 30.08.2023). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

1. Методика предотвращения инцидентов информационной безопасности за счет применения SIEM-систем : монография / О.М. Голембиовская [и др.].. — Москва: Ай Пи Ар Медиа, 2023. — 110 с. — ISBN 978-5-4497-2317-8. — Текст : электронный // IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/132568.html (дата обращения: 30.08.2023). — Режим доступа: для авторизир. пользователей

2. Филиппов А.А. Операционные системы: учебное пособие / Филиппов А.А.. — Ульяновск: Ульяновский государственный технический университет, 2021. — 100 с. — ISBN 978-5-9795-2129-9. — Текст: электронный // IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/121273.html

7.4. Материально-техническое обеспечение

Для проведения и обеспечения занятий используются помещения, которые представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой специалитета, оснащенные оборудованием и техническими средствами обучения: автоматизированное рабочее место преподавателя, маркерная доска, мультимедийный проектор, документ-камера, посадочные места обучающихся.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде университета.

Авторы: к.ю.н., Метельков А.Н., к.т.н., доцент Матвеев А.В.