Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 23.10.2023 17:45:51
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Декан факультета информационных технологий
/Д. Г. Демидов/
"30" августа 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Управление инцидентами информационной безопасности»
Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

Образовательная программа (профиль)
«Безопасность открытых информационных систем»

Квалификация (степень) выпускника
Специалист по защите информации

Форма обучения
Очная
Год приема - 2021

Москва 2021 г.

1. Цели освоения дисциплины.

К **основным целям** освоения дисциплины «Управление инцидентами информационной безопасности» следует отнести:

- приобретение студентами знаний о процессах, процедурах, методах управления инцидентами информационной безопасности систем и умений по идентификации инцидентов информационной безопасности, формированию правил и процедур реагирования на инциденты информационной безопасности информационных систем.

К **основным задачам** освоения дисциплины «Управление инцидентами информационной безопасности» следует отнести:

- знание регламента устранения и учёта выявленных инцидентов и регламента информирования персонала о выявленных инцидентах
- умение оценивать последствия выявленных инцидентов; определять источники и причины возникновения инцидентов;
- владение навыками обнаружения, идентификации, устранения инцидентов в процессе эксплуатации системы; навыками определения правил и процедур выявления инцидентов, реагирования на инциденты в процессе эксплуатации системы; навыками резервирования программного обеспечения, технических средств, каналов передачи данных системы

2. Место дисциплины в структуре ООП.

Дисциплина «Управление инцидентами информационной безопасности» относится к числу профессиональных учебных дисциплин по выбору студента части цикла (Б.1.ДВ) основной образовательной программы (Б.1.ДВ.9).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: Основы управления информационной безопасностью.

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы.

В результате освоения дисциплины (модуля) у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код компетенции	**В результате освоения образовательной программы обучающийся должен обладать**	**Перечень планируемых результатов обучения по дисциплине**
ПК-19	Способен выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности	знать: • регламент устранения и учёта выявленных инцидентов; • регламент информирования персонала о выявленных инцидентах. уметь: • оценивать последствия выявленных инцидентов; • определять источники и причины возникновения инцидентов;

	автоматизированной системы	• организовывать и проводить расследования инцидентов информационной безопасности и выявленных нарушений мер защиты информации; • прогнозировать возможные пути развития действий нарушителя информационной безопасности; • разрабатывать и обосновывать предложения по совершенствованию процедур управления инцидентами информационной безопасности и защитных мер; • применять программные средства резервирования и восстановления информации; • создавать альтернативные места хранения и обработки информации на случай возникновения нештатных ситуаций; владеть: • навыками обнаружения, идентификации, устранения инцидентов в процессе эксплуатации системы; • навыками определения правил и процедур выявления инцидентов, реагирования на инциденты в процессе эксплуатации системы; • навыками резервирования программного обеспечения, технических средств, каналов передачи данных системы.

4. Структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет 2 зачетных единицы, т.е. **72** академических часов (лабораторные занятия – 36 час, самостоятельная работа - 36 часов, форма контроля – экзамен) в 7 семестре.

Структура и содержание дисциплины «Управление инцидентами информационной безопасности» по срокам и видам работы отражены в приложении.

Содержание разделов дисциплины

Тема 1. Общие положения

Термины и определения: событие информационной безопасности (ИБ); инцидент ИБ; менеджмент инцидентов ИБ; группа реагирования на инциденты ИБ. Виды инцидентов ИБ защищенных информационных систем: неавторизованный доступ; отказ в обслуживании; вредоносный код; несоответствующее использование; сбор информации.

Причины возникновения инцидентов ИБ защищенных информационных систем: остаточные риски, изменения внутренней и внешней среды (появление новых угроз), появление новых уязвимостей. Последствия инцидентов ИБ.

Цели менеджмента инцидентов ИБ. Система менеджмента инцидентов ИБ защищенных информационных систем. Процессы менеджмента инцидентов ИБ защищенных информационных систем.

Тема 2. Планирование системы менеджмента инцидентов ИБ защищенных информационных систем

Политика менеджмента инцидентов ИБ. Содержание политики менеджмента инцидентов ИБ. Документационное обеспечение системы менеджмента инцидентов ИБ. Процедуры менеджмента инцидентов ИБ защищенных информационных систем.

Группа реагирования на инциденты ИБ (ГРИИБ). Назначение. Члены группы реагирования и её структура. Взаимодействие с другими подразделениями организации. Отношения со сторонними лицами и организациями.

Техническая поддержка обработки инцидентов ИБ и восстановления после них.

Обеспечение осведомленности сотрудников об обнаружении и оповещении об инцидентах ИБ защищенных информационных систем. Обучение персонала ГРИИБ менеджменту инцидентов ИБ защищенных информационных систем.

Контрольный перечень действий по обработке инцидентов ИБ защищенных информационных систем.

Приоритетный порядок обработки инцидентов ИБ на основе классификации инцидентов защищенных информационных систем

.

Тема 3. Использование системы менеджмента инцидентов ИБ защищенных информационных систем

Обнаружение и оповещение об инциденте ИБ защищенных информационных систем. Средства обнаружения инцидентов ИБ. Предвестники и указатели инцидентов ИБ защищенных информационных систем.

Анализ инцидентов ИБ защищенных информационных систем. Порядок анализа событий ИБ и инцидентов ИБ. Первичная оценка. Отчётность о событии ИБ. Вторичная оценка. Отчётность об инциденте ИБ.

Сдерживание инцидента ИБ защищенных информационных систем. Принятие решения о сдерживании. Стратегии сдерживания инцидента ИБ.

Устранение инцидента ИБ защищенных информационных систем и восстановление после него. Действия по устранению инцидента и восстановлению после него. Резервное копирование данных. Резервный фонд оборудования.

Сбор и обработка данных об инцидентах ИБ защищенных информационных систем. Цель сбора данных. Статистические данные об инцидентах ИБ. Итоговая отчётность об инцидентах ИБ. Срок хранения данных об инцидентах ИБ.

Тема 4. Анализ и улучшение системы менеджмента инцидентов ИБ защищенных информационных систем

Изучение полученного опыта. Определение и осуществление улучшений оценки риска и управления информационной безопасностью. Определение и осуществление улучшений системы менеджмента инцидентов ИБ защищенных информационных систем.

Тема 5. Менеджмент конкретных видов инцидентов ИБ защищенных информационных систем

Определение инцидента неавторизованного доступом. Примеры инцидентов неавторизованного доступа. Менеджмент инцидентов неавторизованного доступа.

Определение инцидента отказа в обслуживании. Примеры инцидентов отказа в обслуживании: рефлекторные атаки, усилительные атаки, атаки распределенного отказа в обслуживании. Менеджмент инцидентов отказа в обслуживании.

Определение инцидента, связанного с применением вредоносного кода. Примеры инцидентов, связанных с применением вредоносного кода. Менеджмент инцидентов, связанных с применением вредоносного кода.

Определение инцидента, связанного с несоответствующим использованием. Примеры инцидентов, связанных с несоответствующим использованием. Менеджмент инцидентов, связанных с несоответствующим использованием.

Определение инцидента сбора информации. Примеры инцидентов сбора информации. Менеджмент инцидентов сбора информации.

5. Образовательные технологии.

Методика преподавания дисциплины «Управление инцидентами информационной безопасности» и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся:

- подготовка к выполнению лабораторных работ;

Удельный вес занятий, проводимых в интерактивных формах по дисциплине, составляет 20 % аудиторных занятий

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов.

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- экзамен.

Образцы экзаменационных билетов, приведены в приложении.

6.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю).

6.1.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

В результате освоения дисциплины (модуля) формируются следующие компетенции:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать
ПК-19	Способен выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин (модулей), практик в соответствии с учебным планом и календарным графиком учебного процесса.

6.1.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины (модуля), описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине (модулю):

ПК-19 Способен выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать: •регламент устранения и учёта выявленных инцидентов; •регламент информирования персонала о выявленных инцидентах.	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: •регламент устранения и учёта выявленных инцидентов; •регламент информирования персонала о выявленных инцидентах. .	Обучающийся демонстрирует неполное соответствие следующих знаний: •регламент устранения и учёта выявленных инцидентов; •регламент информирования персонала о выявленных инцидентах. Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих знаний: •регламент устранения и учёта выявленных инцидентов; •регламент информирования персонала о выявленных инцидентах, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний: •регламент устранения и учёта выявленных инцидентов; •регламент информирования персонала о выявленных инцидентах, свободно оперирует приобретенными знаниями.
уметь: •оценивать последствия выявленных инцидентов; •определять источники и причины возникновения инцидентов; •организовывать и проводить расследования инцидентов информационной безопасности и выявленных нарушений мер защиты информации;	Обучающийся не умеет или в недостаточной степени умеет •оценивать последствия выявленных инцидентов; •определять источники и причины возникновения инцидентов; •организовывать и проводить расследования инцидентов информационной безопасности и выявленных	Обучающийся демонстрирует неполное соответствие следующих умений: •оценивать последствия выявленных инцидентов; •определять источники и причины возникновения инцидентов; •организовывать и проводить расследования инцидентов информационной безопасности и выявленных нарушений мер защиты информации;	Обучающийся демонстрирует частичное соответствие следующих умений: •оценивать последствия выявленных инцидентов; •определять источники и причины возникновения инцидентов; •организовывать и проводить расследования инцидентов информационной	Обучающийся демонстрирует полное соответствие следующих умений: •оценивать последствия выявленных инцидентов; •определять источники и причины возникновения инцидентов; •организовывать и проводить расследования инцидентов информационной безопасности и

•прогнозировать возможные пути развития действий нарушителя информационной безопасности; •разрабатывать и обосновывать предложения по совершенствованию процедур управления инцидентами информационной безопасности и защитных мер; •применять программные средства резервирования и восстановления информации; •создавать альтернативные места хранения и обработки информации на случай возникновения нештатных ситуаций.	нарушений мер защиты информации; •прогнозировать возможные пути развития действий нарушителя информационной безопасности; •разрабатывать и обосновывать предложения по совершенствованию процедур управления инцидентами информационной безопасности и защитных мер; •применять программные средства резервирования и восстановления информации; •создавать альтернативные места хранения и обработки информации на случай возникновения нештатных ситуаций.	•прогнозировать возможные пути развития действий нарушителя информационной безопасности; •разрабатывать и обосновывать предложения по совершенствованию процедур управления инцидентами информационной безопасности и защитных мер; •применять программные средства резервирования и восстановления информации; •создавать альтернативные места хранения и обработки информации на случай возникновения нештатных ситуаций. Допускаются значительные ошибки, проявляется недостаточность умений.	безопасности и выявленных нарушений мер защиты информации; •прогнозировать возможные пути развития действий нарушителя информационной безопасности; •разрабатывать и обосновывать предложения по совершенствованию процедур управления инцидентами информационной безопасности и защитных мер; •применять программные средства резервирования и восстановления информации; •создавать альтернативные места хранения и обработки информации на случай возникновения нештатных ситуаций. Умения освоены, но допускаются незначительные ошибки, неточности.	выявленных нарушений мер защиты информации; •прогнозировать возможные пути развития действий нарушителя информационной безопасности; •разрабатывать и обосновывать предложения по совершенствованию процедур управления инцидентами информационной безопасности и защитных мер; •применять программные средства резервирования и восстановления информации; •создавать альтернативные места хранения и обработки информации на случай возникновения нештатных ситуаций. Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.
владеть: •навыками обнаружения, идентификации, устранения инцидентов в процессе эксплуатации системы; •навыками определения правил и процедур выявления инцидентов, реагирования на инциденты в процессе эксплуатации	Обучающийся не владеет или в недостаточной степени владеет •навыками обнаружения, идентификации, устранения инцидентов в процессе эксплуатации системы; •навыками определения правил и процедур выявления инцидентов,	Обучающийся владеет •навыками обнаружения, идентификации, устранения инцидентов в процессе эксплуатации системы; •навыками определения правил и процедур выявления инцидентов, реагирования на инциденты в процессе эксплуатации системы; •навыками резервирования программного обеспечения, технических средств,	Обучающийся частично владеет •навыками обнаружения, идентификации, устранения инцидентов в процессе эксплуатации системы; •навыками определения правил и процедур выявления инцидентов, реагирования на инциденты в процессе	Обучающийся в полном объеме владеет •навыками обнаружения, идентификации, устранения инцидентов в процессе эксплуатации системы; •навыками определения правил и процедур выявления инцидентов, реагирования на

системы; •навыками резервирования программного обеспечения, технических средств, каналов передачи данных системы.	реагирования на инциденты в процессе эксплуатации системы; •навыками резервирования программного обеспечения, технических средств, каналов передачи данных системы.	каналов передачи данных системы, но допускаются значительные ошибки, проявляется недостаточность владения	эксплуатации системы; •навыками резервирования программного обеспечения, технических средств, каналов передачи данных системы, навыки освоены, но допускаются незначительные ошибки, неточности, затруднения.	инциденты в процессе эксплуатации системы; •навыками резервирования программного обеспечения, технических средств, каналов передачи данных системы, свободно применяет полученные навыки в ситуациях повышенной сложности.

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации: экзамен.

Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	**Описание**
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.

Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

Фонды оценочных средствпредставлены в приложении к рабочей программе.

7. Учебно-методическое и информационное обеспечение дисциплины.

а) основная литература:

1. ГОСТ Р ИСО/МЭК 18044-2007 Информационная технология - Методы и средства обеспечения безопасности - Менеджмент инцидентов информационной безопасности.

б) дополнительная литература:

.

1.Зефиров С.Л. Менеджмент инцидентов информационной безопасности: учебное пособие. – Пенза: Издательство Пензенского государственного университета, 2008. – 124с.
2. ISO/IEC 27035:2011 Information technology - Security techniques - Information security incident management

в) программное обеспечение и интернет-ресурсы:

«Антивирус Касперского 6.0»,
«GFI LANguard System Integrity Monitor»,
Secret Net.

8. Материально-техническое обеспечение дисциплины.

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, экран) – 1 комплект.

Для проведения лабораторных занятий необходимо наличие компьютерных классов оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

9. Методические рекомендации для самостоятельной работы студентов

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются лекции.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

10. Методические рекомендации для преподавателя

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки **10.05.03 «Информационная безопасность автоматизированных систем»**.

Программу составил: к.т.н., доцент Н.В. Федоров

Программа утверждена на заседании кафедры “Информационная безопасность” «30» августа 2021 г., протокол № 1

Заведующий кафедрой
«Информационная безопасность»



к.т.н., доцент Н.В. Федоров

Приложение.

**Структура и содержание дисциплины «Управление инцидентами информационной безопасности»
по направлению подготовки
10.05.03 «Информационная безопасность автоматизированных систем»
(специалист)**

n/n	Раздел	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов, и трудоемкость в часах					Виды самостоятельной работы студентов					Формы аттестации	
				Л	П/С	Лаб	СРС	КСР	К.Р.	К.П.	ДЗ	Реферат	К/р	Э	З
	7 семестр														
1	Виды инцидентов ИБ защищенных информационных систем: неавторизованный доступ; отказ в обслуживании; вредоносный код; несоответствующее использование; сбор информации.	7	1-2			4	4								
2	Планирование системы менеджмента инцидентов ИБ защищенных информационных систем		3-5			6	6								
3	Использование системы менеджмента инцидентов ИБ защищенных информационных систем		6-9			8	8								
4	Анализ и улучшение системы менеджмента инцидентов ИБ защищенных		10-14			10	10								

	информационных систем														
5	Менеджмент конкретных видов инцидентов ИБ защищенных информационных систем		15-18			8	8								
	Форма аттестации		19-21							.				Э	
	Всего часов по дисциплине во седьмом семестре					36	36								
	Всего часов по дисциплине					36	36								

Приложение к
рабочей программе

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Направление подготовки: 10.05.03 «Информационная безопасность автоматизированных систем»

ОП (профиль): «Безопасность открытых информационных систем»

Форма обучения: очная

Вид профессиональной деятельности: эксплуатационная; проектно-технологическая; экспериментально-исследовательская; организационно-управленческая

.

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ

«Управление инцидентами информационной безопасности»

Состав: 1. Паспорт фонда оценочных средств

2. Описание оценочных средств:

Экзамен

Составители: к.т.н., доцент Н.В. Федоров

Москва, 2021 год

Таблица 1

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Управление инцидентами информационной безопасности					
ФГОС ВО **10.05.03 «Информационная безопасность автоматизированных систем»**					
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **общепрофессиональные и профессиональные компетенции**:					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования компетен**	**Форма оценоч-ного**	**Степени уровней освоения компетенций**
ИН-ДЕКС	**ФОРМУЛИРОВКА**				

ПК-19	Способен выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	знать: • регламент устранения и учёта выявленных инцидентов; • регламент информирования персонала о выявленных инцидентах. уметь: • оценивать последствия выявленных инцидентов; • определять источники и причины возникновения инцидентов; • организовывать и проводить расследования инцидентов информационной безопасности и выявленных нарушений мер защиты информации; • прогнозировать возможные пути развития действий нарушителя информационной безопасности; • разрабатывать и обосновывать предложения по совершенствованию процедур управления инцидентами информационной безопасности и защитных мер; • применять программные средства резервирования и восстановления информации; • создавать альтернативные места хранения и обработки информации на случай возникновения нештатных ситуаций; владеть: • навыками обнаружения, идентификации, устранения инцидентов в процессе эксплуатации системы; • навыками определения правил и процедур выявления инцидентов, реагирования на инциденты в процессе эксплуатации системы; • навыками резервирования программного обеспечения, технических средств, каналов передачи данных системы.	самостоятельная работа, лабораторные занятия	экзамен	Базовый уровень: знать: • регламент устранения и учёта выявленных инцидентов; • регламент информирования персонала о выявленных инцидентах. уметь: • оценивать последствия выявленных инцидентов; • определять источники и причины возникновения инцидентов; • организовывать и проводить расследования инцидентов информационной безопасности и выявленных нарушений мер защиты информации; • прогнозировать возможные пути развития действий нарушителя информационной безопасности; владеть: • навыками обнаружения, идентификации, устранения инцидентов в процессе эксплуатации системы; • • навыками резервирования программного обеспечения, технических средств, каналов передачи данных системы. Повышенный уровень: уметь: разрабатывать и обосновывать предложения по совершенствованию процедур управления инцидентами информационной безопасности и защитных мер; • применять программные средства резервирования и восстановления информации; • создавать альтернативные места хранения и обработки информации на случай возникновения нештатных ситуаций; владеть: навыками определения правил и процедур выявления инцидентов, реагирования на инциденты в процессе эксплуатации системы;

Приложение 2
к рабочей программе

Оценочные средства для промежуточной аттестации

Экзамен.

Список вопросов для экзамена по дисциплине

1 вопрос

1.Формирование политики управления инцидентами ИБ. Основное содержание политики управления 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. Стратегии управления непрерывностью функционирования АС для поставщиков
17. Стратегии управления непрерывностью функционирования АС для компьютеров
18. Стратегии управления непрерывностью функционирования АС для серверов
19. Стратегии управления непрерывностью функционирования АС для локальной сети

2 вопрос

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

2. Привести пример формы сообщения «Отчет об инциденте ИБ» сотрудника ГРИИБ, проводившего первичную оценку событий ИБ
3. Привести пример матрицы для определения значимости инцидентов неавторизованного доступа
4. Определить предвестники и указатели инцидентов неавторизованного доступа
5. Определить меры по сдерживанию, устранению инцидентов неавторизованного доступа и восстановлению после них
6. Привести пример матрицы для определения значимости инцидентов отказа в обслуживании
7. Определить предвестники и указатели инцидентов отказа в обслуживании
8. Определить меры по сдерживанию, устранению инцидентов отказа в обслуживании и восстановлению после них
9. Привести пример матрицы для определения значимости инцидентов сбора информации
10. Определить предвестники и указатели инцидентов сбора информации
11. Определить меры по сдерживанию, устранению инцидентов сбора информации и восстановлению после них
12. Привести пример матрицы для определения значимости инцидентов внедрения вредоносного кода
13. Определить предвестники и указатели инцидентов внедрения вредоносного кода
14. Определить меры по сдерживанию, устранению инцидентов внедрения вредоносного кода и восстановлению после них
15. Привести пример матрицы для определения значимости инцидентов несоответствующего использования
16. Определить предвестники и указатели инцидентов несоответствующего использования. Определить меры по сдерживанию, устранению инцидентов несоответствующего использования и восстановлению после них

3 вопрос

1. Построить возможные сценарии инцидента неавторизованного доступа
2. Построить возможные сценарии инцидента отказа в обслуживании
3. Построить возможные сценарии инцидента внедрения вредоносного кода
4. Построить возможные сценарии инцидента сбора информации
5. Построить возможные сценарии инцидента несоответствующего использования

Пример билета.

1. Тестирование системы управления инцидентами ИБ

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

3. Построить возможные сценарии инцидента внедрения вредоносного кода