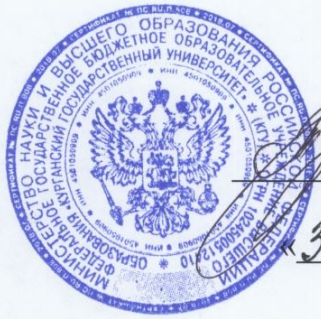
Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Курганский государственный университет»
(КГУ)

Кафедра «Безопасность информационных и автоматизированных систем»



УТВЕРЖДАЮ:
Первый проректор

_____ / Т.Р. Змызгова/

«31» августа 2023 г.

Рабочая программа учебной дисциплины
РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

образовательной программы высшего образования –
программы специалитета

10.05.03 – Информационная безопасность автоматизированных систем

Специализация №5 «Безопасность открытых информационных систем»

Форма обучения: **очная**

Курган 2023

Рабочая программа дисциплины «Реагирование на инциденты информационной безопасности» составлена в соответствии с учебным планом по программе специалитета «Информационная безопасность автоматизированных систем» (Безопасность открытых информационных систем), утвержденным:
- для очной формы обучения «30» июня 2023 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» «31» августа 2023 года, протокол № 1.

Заведующий кафедрой «Безопасность информационных и автоматизированных систем» _____ Д.И. Дик

Согласовано:

Заведующий кафедрой «Безопасность информационных и автоматизированных систем» _____ Д.И. Дик

Специалист по учебно-методической работе учебно-методического отдела _____ Г.В. Казанкова

Начальник управления образовательной деятельности _____ И.В. Григоренко

1. ОБЪЕМ ДИСЦИПЛИНЫ

Всего: 3 зачетных единицы трудоемкости (108 академических часа)

Вид учебной работы	На всю дисциплину	Семестр
		10
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**70**	**70**
Лекции	30	30
Лабораторные работы	40	40
Самостоятельная работа, всего часов в том числе:	**38**	**38**
Подготовка к экзамену	27	27
Другие виды самостоятельной работы (самостоятельное изучение тем (разделов) дисциплины)	11	11
Вид промежуточной аттестации	**Экзамен**	**Экзамен**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**108**	**108**

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Реагирование на инциденты информационной безопасности» относится к части, формируемой участниками образовательных отношений Блока 1.

Изучение дисциплины базируется на результатах обучения, сформированных при изучении следующих дисциплин:

– Безопасность сетей ЭВМ;

– Безопасность операционных систем;

– Безопасность систем баз данных.

Результаты обучения служат основой для дисциплины «Обнаружение и предупреждение компьютерных атак в открытых информационных системах» и необходимы для прохождения производственной практики и успешного написания выпускной квалификационной работы.

3 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Целью изучения дисциплины является формирование знаний и умений в области противодействия возникновению инцидентов информационной безопасности, а также их расследования.

Задачами дисциплины являются:

– ознакомление с теоретическими принципами управления инцидентами информационной безопасности;

– формирование умений по организации процесса реагирования на инциденты;

– приобретение обучающимися навыков по расследованию инцидентов информационной безопасности.

Компетенции, формируемые в результате освоения дисциплины:

– способен проводить расследование инцидентов информационной безопасности (ПК-7);

– способен обеспечивать работоспособность систем защиты информации открытых информационных систем при возникновении нештатных ситуаций (ПК-15);

В результате изучения дисциплины обучающийся должен:

знать:

– положения стандартов в области реагирования на компьютерные инциденты (ПК-15);

– механизмы компьютерного следообразования (ПК-7);

уметь:

– использовать специальное программное обеспечение для расследования инцидентов информационной безопасности (для ПК-7);

– организовывать процесс реагирования на компьютерные инциденты (для ПК-15);

владеть:

– навыками расследования инцидентов информационной безопасности (для ПК-7).

4 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Учебно-тематический план

Рубеж	Номер темы	Наименование темы	Количество часов контактной работы с преподавателем	
			Лекции	Лабораторные работы
Рубеж 1	1	Нормативные документы по управлению компьютерными инцидентами.	4	–
	2	Организация реагирования на инциденты информационной безопасности	4	4
	3	Обнаружение и регистрация компьютерных инцидентов	2	–
	4	Механизмы компьютерного следообразования	6	14
		1-ый рубежный контроль (Тестирование)		2
Рубеж 2	5	Реагирование на инциденты	4	–
	6	Расследование инцидентов	4	16
	7	Реагирование на компьютерные инциденты в рамках функционирования центров мониторинга ГосСОПКА	2	2
	8	Анализ результатов инцидента	4	–
		2-ый рубежный контроль (Тестирование)		2
		Всего:	**30**	**40**

4.2 Содержание лекционных занятий

Тема №1. Нормативные документы по управлению компьютерными инцидентами

Основные положения Федерального законодательства. Требования приказов ФСТЭК России и положения приказов ФСБ России.

Стандарт ITU-T E.409. Общие требования к построению системы управления ИБ, относящиеся к процессам управления инцидентами в стандарте ISO/IEC 27001-2005.

Процесс управления инцидентами информационной безопасности согласно стандартам ISO/IEC 27035.

Инфраструктура управления инцидентами ИБ в стандарте ISO/IEC TR 18044. Описание методологии планирования, внедрения, оценки и улучшения процессов управления инцидентами в документе CMU/SEI-2004-TR-015. Практики по построению процессов управления инцидентами и реагирования на них в рекомендациях NIST SP 800-61.

Менеджмент инцидентов информационной безопасности согласно РС БР ИББС-2.5-2014, Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств согласно СТО БР ИББС-1.3-2016. Реагирование на инциденты согласно PCI DSS.

Тема №2. Организация реагирования на инциденты информационной безопасности

Цели процесса реагирования на инциденты. Основные этапы процесса реагирования на инциденты. Организация реагирования на инциденты. Создание политики управления инцидентами информационной безопасности. Разработка плана управления инцидентами информационной безопасности. Создание группы реагирования на инциденты информационной безопасности. Взаимодействие с другими подразделениями организации и другими организациями. Организация технической и другой поддержки. Повышение осведомленности, обучение и тренинги по инцидентам информационной безопасности. Тестирование плана управления инцидентами информационной безопасности.

Тема №3. Обнаружение и регистрация компьютерных инцидентов

Обнаружение атак и распознавание вторжений. Регистрация признаков возможного возникновения компьютерных инцидентов. Подтверждение компьютерных инцидентов.

Тема №4. Механизмы компьютерного следообразования

Общая информация о цифровых следах. Классификация компьютерных следов. Формы существования компьютерной информации. Причины следообразования. Поиск следов подключения устройств к компьютеру под управлением операционной системы Windows. Поиск следов запуска и установки программ в операционной системе Windows. Поиск следов открытия файлов и папок в операционной системе Windows. Использование истории введенных пользователем команд и журналов операционных систем на базе ядра Linux.

Тема №5. Реагирование на инциденты

Локализация компьютерного инцидента. Определение конкретных параметров нарушения (нападения), его характера.

Выявление последствий компьютерного инцидента. Ликвидация последствий компьютерного инцидента. Организация информационной работы о произошедших инцидентах.

Тема №6. Расследование инцидентов

Анализ технических аспектов нападения. Качественный анализ процесса нападения в контексте функционирования атакуемой системы защиты информации. Организация взаимодействия со сторонними организациями, которые могут содействовать в идентификации нападающего. Анализ целей и мотивов нападавших.

Тема №7. Реагирование на компьютерные инциденты в рамках функционирования центров мониторинга ГосСОПКА

Национальный координационный центр по компьютерным инцидентам (далее — НКЦКИ); ГосСОПКА. Нормативное регулирование деятельности центров ГосСОПКА. Подключение к ГосСОПКА. Реагирование на инцидент в рамках ГосСОПКА.

Тема №8. Анализ результатов инцидента

Оценка ущерба от произошедшего нарушения информационной безопасности. Анализ фундаментальных (организационных и технических) причин, которые сделали нападение возможным и успешным. Анализ последствий нападения для деятельности предприятия. Анализ и оценка работы персонала и взаимоотношений с предприятиями-партнерами.

4.3 Лабораторные работы

Номер темы	Наименование темы	Наименование лабораторной работы	Норматив времени, час.
2	Организация реагирования на инциденты информационной безопасности	Создание политики управления инцидентами информационной безопасности	2
		Разработка плана управления инцидентами информационной безопасности	2
4	Механизмы компьютерного следообразования	Копирование информации с машинных носителей	2
		Анализ и восстановление данных из файловой системы	4
		Анализ событий аудита операционной системы	4
		Исследование образов оперативной памяти	4
	2-ой рубежный контроль	***Тестирование***	***2***
6	Расследование инцидентов	Исследование вредоносных документов Microsoft Office	4
		Расследование заражения компьютера вредоносным программным	6

		обеспечением	
		Расследование взлома веб-сервера	6
7	Реагирование на компьютерные инциденты в рамках функционирования центров мониторинга ГосСОПКА	Подготовка отчета об инциденте в рамках взаимодействия с системой ГосСОПКА	2
	2-ой рубежный контроль	***Тестирование***	***2***
		Итого:	**40**

5 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Лекционный курс базируется на пассивном методе обучения, реализующем традиционную объяснительно-иллюстративную образовательную технологию, в рамках которой обучающиеся выступают в роли слушателей, воспринимающих учебный материал и участвующих в дискуссиях и экспресс-опросах.

При прослушивании лекций рекомендуется в конспекте отмечать все важные моменты, на которых заостряет внимание преподаватель, в частности те, которые направлены на качественное выполнение соответствующей лабораторной работе.

Залогом качественного выполнения лабораторных работ является самостоятельная подготовка к ним накануне путем повторения материалов лекций. Преподавателем запланировано применение на лабораторных работах разбор конкретных ситуаций.

Для текущего контроля успеваемости по очной форме обучения преподавателем используется балльно-рейтинговая система контроля и оценки академической активности. Поэтому настоятельно рекомендуется тщательно прорабатывать материал дисциплины при самостоятельной работе, участвовать во всех формах обсуждения и взаимодействия, как на лекциях, так лабораторных работах в целях лучшего освоения материала и получения высокой оценки по результатам освоения дисциплины.

Выполнение самостоятельной работы подразумевает самостоятельное изучение разделов дисциплины, подготовку к лабораторным работам, к рубежным контролям (для очной формы обучения) и подготовку к экзамену.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Подготовка к лабораторным работам (по 1 часу на каждую работу)	10
Подготовка к рубежным контролям (по 0,5 часа на каждый рубежный контроль)	1

Подготовка к экзамену	27
Всего:	**38**

6 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1 Перечень оценочных средств

1. Балльно-рейтинговая система контроля и оценки академической активности обучающихся в КГУ
2. Отчеты обучающихся по лабораторным работам.
3. Банк тестовых заданий к рубежным контролям № 1, № 2.
4. Вопросы к экзамену.

6.2 Система балльно-рейтинговой оценки работы обучающихся по дисциплине (для очной формы обучения)

№	Наименование	Содержание					
1	Распределение баллов за семестры по видам учебной работы, сроки сдачи учебной работы *(доводятся до сведения обучающихся на первом учебном занятии)*	Распределение баллов					
		Вид учебной работы:	Посещение лекций	Выполнение лабораторных работ	Рубежный контроль №1	Рубежный контроль №2	Экзамен
		Балльная оценка:	$2_б$ x 15 =$30_б$	$2_б$ x 10 = $20_б$	10	10	30
2	Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и экзамена	60 и менее баллов – неудовлетворительно; 61…73 – удовлетворительно; 74… 90 – хорошо; 91…100 – отлично					

3	Критерии допуска к промежуточной аттестации, возможности получения автоматического экзамена по дисциплине, возможность получения бонусных баллов	Для допуска к промежуточной аттестации по дисциплине за семестр обучающийся должен набрать по итогам текущего и рубежного контроля не менее 51 баллов. В случае если обучающийся набрал менее 51 балла, то к аттестационным испытаниям он не допускается. Для получения экзамена без проведения процедуры промежуточной аттестации обучающемуся необходимо набрать в ходе текущего и рубежных контролей не менее 61 балла. В этом случае итог балльной оценки, получаемой обучающимся, определяется по количеству баллов, набранных им в ходе текущего и рубежного контролей. При этом, на усмотрение преподавателя, бальная оценка обучающегося может быть повышена за счет получения дополнительных баллов за академическую активность. Обучающийся, имеющий право на получение оценки без проведения процедуры промежуточной аттестации, может повысить ее путем сдачи аттестационного испытания. В случае получения обучающимся на аттестационном испытании 0 баллов итог бальной оценки по дисциплине не снижается. За академическую активность в ходе освоения дисциплины, участие в учебной, научно-исследовательской, спортивной, культурно-творческой и общественной деятельности обучающемуся могут быть начислены дополнительные баллы. Максимальное количество дополнительных баллов за академическую активность составляет 30. Основанием для получения дополнительных баллов являются: - выполнение дополнительных заданий по дисциплине; дополнительные баллы начисляются преподавателем; - участие в течение семестра в учебной, научно-исследовательской, спортивной, культурно-творческой и общественной деятельности КГУ.
4	Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) обучающихся для получения недостающих баллов в конце семестра	В случае если к промежуточной аттестации (экзамену) набрана сумма менее 51 баллов, обучающемуся необходимо набрать недостающее количество баллов за счет выполнения дополнительных заданий, до конца последней (зачетной) недели семестра. Ликвидация академических задолженностей, возникших из-за разности в учебных планах при переводе или восстановлении, проводится путем выполнения дополнительных заданий, форма и объем которых определяется преподавателем.

6.3 Процедура оценивания результатов освоения дисциплины

Мероприятия текущего контроля проводятся на аудиторных занятиях в соответствии с расписанием.

Основной вид текущего контроля результатов освоения дисциплины - защита отчетов по выполненным лабораторным работам.

В процессе защиты отчетов оценивается уровень понимания обучающимися методики проведения работы, полнота и качество выполнения заданий, а также обоснованность выводов, сделанных обучающимся по результатам выполнения заданий.

Рубежные контроли проводятся в форме письменного тестирования.

Перед проведением каждого рубежного контроля преподаватель прорабатывает с обучающимися основной материал соответствующих разделов дисциплины. Варианты тестовых заданий состоят для 1 и 2 рубежного контроля из 10 вопросов. На каждое тестирование при рубежном контроле обучающемуся отводится 2 академических часа.

Баллы обучающемуся выставляются в зависимости от числа правильно выбранных ответов. Итоговая оценка по тесту формируется путем суммирования набранных баллов и отнесения их к общему количеству вопросов в задании.

Экзамен проводится в форме устного ответа на 2 вопроса. Билет состоит из 2 вопросов. Перечень вопросов преподаватель выдает заранее. Время, отводимое обучающемуся на подготовку вопросов, составляет 1 академический час. Каждый вопрос оценивается в 15 баллов.

Результаты текущего контроля успеваемости и экзамена заносятся преподавателем в экзаменационную ведомость, которая сдается в организационный отдел института в день экзамена, а также выставляются в зачетную книжку обучающегося.

6.4 Примеры оценочных средств для рубежных контролей и экзамена

Примерные тестовые задания для рубежного контроля №1

1) Событие информационной безопасности

а) происшествие, указывающее на возможное нарушение политики ИБ или отказ защитных мер

б) акт нарушения явной или подразумеваемой политики безопасности

в) только атака на информационную систему

г) нет верного ответа

2) Инцидент информационной безопасности

а) происшествие, указывающее на возможное нарушение политики ИБ или отказ защитных мер

б) акт нарушения явной или подразумеваемой политики безопасности

в) только атака на информационную систему

г) нет верного ответа

3) Утилита dd это:

а) средство восстановления удаленных файлов

б) средство клонирования дисков

в) средство необратимого удаления данных

Примерные тестовые задания для рубежного контроля №2

1) Цель локализации компьютерного инцидента:

а) предотвратить нарушения конфиденциальности, целостности или доступности информации в следствие НСД

б) предотвратить несанкционированное вмешательство в работу информационного ресурса

в) предотвратить использование информационного ресурса для атаки на смежные ресурсы

г) сбор доказательств действий злоумышленника

д) исследование поведения злоумышленника

2) Критерии определения правильной стратегии локализации инцидента включают:

а) потенциальный ущерб ресурсам и хищение ресурсов

б) потребность в сохранении свидетельств

в) обязательное завершение сбора свидетельств

г) время простоя функционирования информационных ресурсов

д) время и ресурсы, необходимые для реализации стратегии

е) эффективность стратегии

ж) длительность реализации решения

и) завершение расследования инцидента

3) После устранения непосредственной опасности ИС необходимо:

а) контратаковать систему нарушителей

б) обратиться в полицию за квалифицированной помощью

в) сделать копии всех важных данных для просмотра в автономном режиме в соответствии с догматами надлежащего судебного анализа

Примерный перечень вопросов к экзамену

1. Основные положения Федерального законодательства. Требования приказов ФСТЭК России и положения приказов ФСБ России.
2. Требования стандарт ITU-T E.409.
3. Общие требования к построению системы управления ИБ, относящиеся к процессам управления инцидентами в стандарте ISO/IEC 27001-2005.
4. Процесс управления инцидентами информационной безопасности согласно стандартам ISO/IEC 27035.
5. Инфраструктура управления инцидентами ИБ в стандарте ISO/IEC TR 18044.
6. Описание методологии планирования, внедрения, оценки и улучшения процессов управления инцидентами в документе CMU/SEI-2004-TR-015.
7. Практики по построению процессов управления инцидентами и реагирования на них в рекомендациях NIST SP 800-61.
8. Менеджмент инцидентов информационной безопасности согласно РС БР ИББС-2.5-2014,
9. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств согласно СТО БР ИББС-1.3-2016.
10. Реагирование на инциденты согласно PCI DSS.
11. Цели процесса реагирования на инциденты.
12. Основные этапы процесса реагирования на инциденты.
13. Организация реагирования на инциденты.

14. Политика управления инцидентами информационной безопасности.
15. Плана управления инцидентами информационной безопасности.
16. Группа реагирования на инциденты информационной безопасности.
17. Тестирование плана управления инцидентами информационной безопасности.
18. Обнаружение атак и распознавание вторжений
19. . Регистрация признаков возможного возникновения компьютерных инцидентов.
20. Подтверждение компьютерных инцидентов.
21. Классификация компьютерных следов.
22. Локализация компьютерного инцидента.
23. Определение конкретных параметров нарушения (нападения), его характера.
24. Выявление последствий компьютерного инцидента.
25. Ликвидация последствий компьютерного инцидента.
26. Организация информационной работы о произошедших инцидентах.
27. Анализ технических аспектов нападения. Качественный анализ процесса нападения в контексте функционирования атакуемой системы защиты информации.
28. Анализ целей и мотивов нападавших.
29. Национальный координационный центр по компьютерным инцидентам (далее — НКЦКИ); ГосСОПКА.
30. Нормативное регулирование деятельности центров ГосСОПКА. Подключение к ГосСОПКА.
31. Реагирование на инцидент в рамках ГосСОПКА.
32. Оценка ущерба от произошедшего нарушения информационной безопасности.
33. Анализ фундаментальных (организационных и технических) причин, которые сделали нападение возможным и успешным.
34. Анализ последствий нападения для деятельности предприятия.
35. Анализ и оценка работы персонала и взаимоотношений с предприятиями-партнерами.

6.5. Фонд оценочных средств

Полный банк заданий для текущего, рубежных контролей и промежуточной аттестации по дисциплине, показатели, критерии, шкалы оценивания компетенций, методические материалы, определяющие процедуры оценивания образовательных результатов, приведены в учебно-методическом комплексе дисциплины.

7. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА

7.1. Основная учебная литература

1. Энсон, С. Реагирование на компьютерные инциденты. Прикладной курс / С. Энсон. пер. с англ. Д. А. Беликова. – Москва: ДМК Пресс, 2021. – 436 с. – Доступ ЭБС «Консультант студента».

2. Милославская, Н. Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса [Электронный ресурс]: учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – Вып. 3. – Москва: Горячая линия, – Телеком, 2013. – 170 с. – Доступ ЭБС «Консультант студента».

7.2Дополнительная учебная литература

1. Жукова, М. Н. Управление информационной безопасностью [Электронный ресурс]. Ч. 2: Управление инцидентами информационной безопасности: учебное пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. – Красноярск: Сиб. гос. аэрокосмич. ун-т, 2012. – 100 с. – Доступ ЭБС «Znanium»

2. Методологии реагирования на инциденты [Электронный ресурс] / CERT Societe Generale. – Режим доступа: https://github.com/certsocietegenerale/IRM-deprecated, свободный.

7.3 Методическая литература

1. Методические указания по выполнению лабораторных работ по дисциплине «Обнаружение и предупреждение компьютерных атак в открытых информационных системах».

2. Методические указания по выполнению практических работ по дисциплине «Обнаружение и предупреждение компьютерных атак в открытых информационных системах».

8. РЕСУРСЫ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. Сайт дистанционного обучения в НОУ (Национальный Открытый Университет) «ИНТУИТ» содержит бесплатные курсы, программы повышения квалификации и профессиональной переподготовки, интересные доклады и другую полезную информацию http://www.intuit.ru.

2. Федеральный портал «Российское образование» http://www.edu.ru/

3. Портал «Информационно-коммуникационные технологии в образовании» http://www.ict.edu.ru.

4. Федеральный портал ЭБС «Лань» - https://e.lanbook.com/;

5. ЭБС «Znanium» - https://znanium.com/;

6. ЭБС «Консультант студента» - https://www.studentlibrary.ru;

7. Электронная библиотека КГУ - http://dspace.kgsu.ru/xmlui/

9. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

1. ЭБС «Лань».

2. ЭБС «Консультант студента».

3. ЭБС «Znanium.com».

4. «Гарант» - справочно-правовая система.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Материально-техническое обеспечение по реализации дисциплины осуществляется в соответствии с требования ФГОС ВО по данной образовательной программе.

11. Для обучающихся с использованием дистанционных образовательных технологий

При использовании электронного обучения и дистанционных образовательных технологий (далее ЭО и ДОТ) занятия полностью или частично проводятся в режиме онлайн. Объем дисциплины и распределение нагрузки по видам работ соответствует п. 4.1. Распределение баллов соответствует п. 6.2 либо может быть изменено в соответствии с решением кафедры, в случае перехода на ЭО и ДОТ в процессе обучения. Решение кафедры об используемых технологиях и системе оценивания достижений обучающихся принимается с учетом мнения ведущего преподавателя и доводится до обучающихся.

Аннотация
рабочей программы учебной дисциплины
«Реагирование на инциденты информационной безопасности»
образовательной программы высшего образования –
программы специалитета
10.05.03 – Информационная безопасность автоматизированных систем
Специализация №5 «Безопасность открытых информационных систем»

Формы обучения: **очная**

Трудоемкость дисциплины: 3 ЗЕ (108 академических часа)
Семестры: 10-й
Форма промежуточной аттестации: экзамен

Содержание дисциплины

Нормативные документы по управлению компьютерными инцидентами. Организация реагирования на инциденты информационной безопасности. Обнаружение и регистрация компьютерных инцидентов. Механизмы компьютерного следообразования. Реагирование на инциденты. Расследование инцидентов. Реагирование на компьютерные инциденты в рамках функционирования центров мониторинга ГосСОПКА. Анализ результатов инцидента.