ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Утверждено:
на заседании кафедры
протокол №7 от 18 февраля 2022 г.
Зав. кафедрой /Исмагилова А.С.

Согласовано:
Председатель УМК института
/Гильмутдинова Р.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина
Расследование компьютерных инцидентов
Б1.В.ДВ.04.02

программа магистратуры

Направление
10.04.01 Информационная безопасность

Профиль подготовки
Информационная безопасность цифровых технологий

Квалификация
магистр

Разработчик (составитель)
к.ф.-м.н., доцент
/И.А. Шагапов

Для приема: 2022 г.

Уфа – 2022

Составитель: доцент Шагапов Илдар Ахняфович

Рабочая программа дисциплины утверждена на заседании кафедры протокол от «_18_» _февраля_____ 2022 г. № _7_

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры_____
_____
_____, протокол № ____ от «____» _____ 20 _ г.

Заведующий кафедрой / Исмагилова А.С. /

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры_____
_____
_____,
протокол № ____ от «____» _____ 20 _ г.

Заведующий кафедрой _____/ Исмагилова А.С. /

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры _____
_____,
протокол № ____ от «____» _____ 20 _ г.

Заведующий кафедрой _____/ _____Ф.И.О./

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры _____
_____,
протокол № ____ от «____» _____ 20 _ г.

Заведующий кафедрой _____/ _____Ф.И.О./

Список документов и материалов

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

В результате освоения образовательной программы обучающийся должен овладеть следующими результатами обучения по дисциплине:

Категория (группа) компетенций (при наличии ОПК)	Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине
Системное и критическое мышление	УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.	ИУК 1.1. Знает: методы критического анализа и оценки современных научных достижений; основные принципы критического анализа и синтеза информации; основы системного подхода при решении поставленных задач	Знает: методы критического анализа и оценки современных научных достижений; основные принципы критического анализа и синтеза информации; основы системного подхода при решении поставленных задач
		ИУК 1.2. Умеет: получать новые знания на основе анализа и синтеза информации; собирать и обобщать данные по научным проблемам, относящимся к профессиональной области; осуществлять поиск информации и применять системный подход для решения поставленных задач; определять и оценивать практические последствия возможных решений задачи.	Умеет: получать новые знания на основе анализа и синтеза информации; собирать и обобщать данные по научным проблемам, относящимся к профессиональной области; осуществлять поиск информации и применять системный подход для решения поставленных задач; определять и оценивать практические последствия возможных решений задачи.
		ИУК 1.3. Владеет: навыками исследования проблем профессиональной деятельности с применением анализа, синтеза и других методов интеллектуальной деятельности; выявления научных проблем и использования адекватных методов для их решения; формулирования оценочных суждений при решении профессиональных задач	Владеет: навыками исследования проблем профессиональной деятельности с применением анализа, синтеза и других методов интеллектуальной деятельности; выявления научных проблем и использования адекватных методов для их решения; формулирования оценочных суждений при решении профессиональных задач
	ПК-1. Способен проводить предпроектное обследование служебной деятельности и информационных потребностей автоматизируемых подразделений.	ПК-1.1 Знает методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.	Знает методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.
		ПК-1.3 Умеет применять основные методы проведения предпроектного обследования служебной дея-	Умеет применять основные методы проведения предпроектного обследования служебной деятельности и

		тельности и информационных потребностей автоматизируемых подразделений.	информационных потребностей автоматизируемых подразделений.
		ПК-1.5. Владеет навыками проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений	Владеет навыками проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Расследование компьютерных инцидентов» относится к группе дисциплин вариативной части образовательной программы.

Дисциплина изучается на 1 курсе в 1 семестре.

Целью изучения дисциплины является выработка навыков предотвращения и своевременного реагирования на инциденты информационной безопасности.

3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)

Содержание рабочей программы представлено в Приложении 1.

4. Фонд оценочных средств по дисциплине

4.1. Перечень компетенций и индикаторов достижения компетенций с указанием соотнесенных с ними запланированных результатов обучения по дисциплине. Описание критериев и шкал оценивания результатов обучения по дисциплине

УК-1 – Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	**Критерии оценивания результатов обучения**			
		«Неудовлетворительно»	«Удовлетворительно»	«Хорошо»	«Отлично»
ИУК-1.1 - методы критического анализа и оценки современных научных достижений; основные принципы критического анализа и синтеза информации; основы системного подхода при решении поставленных задач	Знает: методы критического анализа и оценки современных научных достижений; основные принципы критического анализа и синтеза информации; основы системного подхода при решении поставленных задач	Не знает: методы критического анализа и оценки современных научных достижений; основные принципы критического анализа и синтеза информации; основы системного подхода при решении поставленных задач	Знает: некоторые методы критического анализа и оценки современных научных достижений; основные принципы критического анализа и синтеза информации; основы системного подхода при решении поставленных задач, допускает ошибки	Частично знает: методы критического анализа и оценки современных научных достижений; основные принципы критического анализа и синтеза информации; основы системного подхода при решении поставленных задач	Знает: методы критического анализа и оценки современных научных достижений; основные принципы критического анализа и синтеза информации; основы системного подхода при решении поставленных задач

ИУК-1.2 - получать новые знания на основе анализа и синтеза информации; собирать и обобщать данные по научным проблемам, относящимся к профессиональной области; осуществлять поиск информации и применять системный подход для решения поставленных задач; определять и оценивать практические последствия возможных решений задачи	Умеет: получать новые знания на основе анализа и синтеза информации; собирать и обобщать данные по научным проблемам, относящимся к профессиональной области; осуществлять поиск информации и применять системный подход для решения поставленных задач; определять и оценивать практические последствия возможных решений задачи.	Не умеет: получать новые знания на основе анализа и синтеза информации; собирать и обобщать данные по научным проблемам, относящимся к профессиональной области; осуществлять поиск информации и применять системный подход для решения поставленных задач; определять и оценивать практические последствия возможных решений задачи.	Умеет: получать некоторые новые знания на основе анализа и синтеза информации; собирать и обобщать данные по научным проблемам, относящимся к профессиональной области; осуществлять поиск информации и применять системный подход для решения поставленных задач; определять и оценивать практические последствия возможных решений задачи, допускает ошибки.	Частично умеет: получать новые знания на основе анализа и синтеза информации; собирать и обобщать данные по научным проблемам, относящимся к профессиональной области; осуществлять поиск информации и применять системный подход для решения поставленных задач; определять и оценивать практические последствия возможных решений задачи.	Умеет: получать новые знания на основе анализа и синтеза информации; собирать и обобщать данные по научным проблемам, относящимся к профессиональной области; осуществлять поиск информации и применять системный подход для решения поставленных задач; определять и оценивать практические последствия возможных решений задачи.
ИУК-1.3 - навыками исследования проблем профессиональной деятельности с применением анализа, синтеза и других методов интеллектуальной деятельности; выявления научных проблем и использования адекватных методов для их решения; формулирования оценочных суждений при решении профессиональных задач	Владеет: навыками исследования проблем профессиональной деятельности с применением анализа, синтеза и других методов интеллектуальной деятельности; выявления научных проблем и использования адекватных методов для их решения; формулирования оценочных суждений при решении профессиональных задач	Не владеет: навыками исследования проблем профессиональной деятельности с применением анализа, синтеза и других методов интеллектуальной деятельности; выявления научных проблем и использования адекватных методов для их решения; формулирования оценочных суждений при решении профессиональных	Владеет: некоторыми навыками исследования проблем профессиональной деятельности с применением анализа, синтеза и других методов интеллектуальной деятельности; выявления научных проблем и использования адекватных методов для их решения; формулирования оценочных суждений при решении профессиональных задач, допуска-	Частично владеет: навыками исследования проблем профессиональной деятельности с применением анализа, синтеза и других методов интеллектуальной деятельности; выявления научных проблем и использования адекватных методов для их решения; формулирования оценочных суждений при решении профессиональных задач	Владеет: навыками исследования проблем профессиональной деятельности с применением анализа, синтеза и других методов интеллектуальной деятельности; выявления научных проблем и использования адекватных методов для их решения; формулирования оценочных суждений при решении профессиональных задач

		задач	ет ошибки		

ПК-1 – Способен проводить предпроектное обследование служебной деятельности и информационных потребностей автоматизируемых подразделений.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	**Критерии оценивания результатов обучения**			
		«Неудовлетворительно»	«Удовлетворительно»	«Хорошо»	«Отлично»
ПК-1.1 Знает методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.	Знает методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.	Не знает методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.	Знает некоторые методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений, допускает ошибки	Частично знает методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.	Знает методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.
ПК-1.3 Умеет применять основные методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.	Умеет применять основные методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.	Не умеет применять основные методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.	Умеет применять некоторые методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений, допускает ошибки.	Частично умеет применять основные методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.	Умеет применять основные методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.
ПК-1.5. Владеет навыками проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений	Владеет навыками проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений	Не владеет навыками проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений	Владеет некоторыми навыками проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений, делает ошибки	Частично владеет навыками проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений	Владеет навыками проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений

4.2. Типовые контрольные задания или иные материалы, необходимые для оценивания результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине

УК-1 – Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	**Оценочные средства**

ИУК 1.1. Знает: методы критического анализа и оценки современных научных достижений; основные принципы критического анализа и синтеза информации; основы системного подхода при решении поставленных задач	Знает: методы критического анализа и оценки современных научных достижений; основные принципы критического анализа и синтеза информации; основы системного подхода при решении поставленных задач	Практическое задание Лабораторная работа
ИУК 1.2. Умеет: получать новые знания на основе анализа и синтеза информации; собирать и обобщать данные по научным проблемам, относящимся к профессиональной области; осуществлять поиск информации и применять системный подход для решения поставленных задач; определять и оценивать практические последствия возможных решений задачи.	Умеет: получать новые знания на основе анализа и синтеза информации; собирать и обобщать данные по научным проблемам, относящимся к профессиональной области; осуществлять поиск информации и применять системный подход для решения поставленных задач; определять и оценивать практические последствия возможных решений задачи.	Практическое задание Лабораторная работа
ИУК 1.3. Владеет: навыками исследования проблем профессиональной деятельности с применением анализа, синтеза и других методов интеллектуальной деятельности; выявления научных проблем и использования адекватных методов для их решения; формулирования оценочных суждений при решении профессиональных задач	Владеет: навыками исследования проблем профессиональной деятельности с применением анализа, синтеза и других методов интеллектуальной деятельности; выявления научных проблем и использования адекватных методов для их решения; формулирования оценочных суждений при решении профессиональных задач	Практическое задание Лабораторная работа

ПК-1 – Способен проводить предпроектное обследование служебной деятельности и информационных потребностей автоматизируемых подразделений.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	**Оценочные средства**
ПК-1.1 Знает методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.	Знает методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.	Практическое задание Лабораторная работа
ПК-1.3 Умеет применять основные методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.	Умеет применять основные методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.	Практическое задание Лабораторная работа
ПК-1.5. Владеет навыками проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений	Владеет навыками проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений	Практическое задание Лабораторная работа

Критериями оценивания при *модульно-рейтинговой системе* являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины (*для экзамена:* текущий контроль – максимум 40 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания для экзамена:

от 45 до 59 баллов – «удовлетворительно»;

от 60 до 79 баллов – «хорошо»;

от 80 баллов – «отлично».

Рейтинг – план дисциплины

Расследование компьютерных инцидентов

Направление подготовки 10.04.01 ИБ

Курс 1, семестр 1

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1.				
Текущий контроль				
1. Аудиторная работа	2	4	1	8
2. Практическая работа №1	10	1	0	10
Рубежный контроль				
1. Лабораторная работа №1	9	1	0	9
2. Лабораторная работа №2	8	1	0	8
Всего				35
Модуль 2.				
Текущий контроль				
1. Аудиторная работа	2	5	1	10
2. Практическая работа №2	10	1	0	10
Рубежный контроль				
1. Лабораторная работа №3	7	1	0	7
2. Лабораторная работа №4	8	1	0	8
Всего				35
Поощрительные баллы				
1. Студенческая олимпиада			0	3
2. Публикация статей			0	3
3. Участие в конференции			0	4
Всего				10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий				-6
2. Посещение практических занятий				-10
Итоговый контроль				
Экзамен				30

Экзаменационные билеты

Структура экзаменационного билета: экзаменационный билет содержит 2 теоретических вопроса.

Перечень вопросов для экзамена:

1. Нормативная база управления инцидентами ИБ
2. Управление инцидентами ИБ
3. Событие и инцидент ИБ
4. Цели и задачи управления инцидентами
5. Система управления инцидентами ИБ
6. Этапы процесса управления инцидентами ИБ
7. Планирование и подготовка процесса управления инцидентами ИБ
8. Использование системы управления инцидентами ИБ

9. Анализ процесса управления инцидентами ИБ
10. Улучшение процесса управления инцидентами ИБ
11. Обнаружение событий ИБ и инцидентов ИБ и оповещение о них
12. Обработка событий ИБ и инцидентов ИБ
13. Первая оценка и предварительное решение по событию
14. Вторая оценка и подтверждение инцидента ИБ
15. Реагирование на инциденты
16. Немедленное реагирование на инцидент ИБ
17. Контролируемость инцидента ИБ
18. Последующее реагирование на инцидент ИБ
19. Антикризисные действия
20. Правовая экспертиза инцидентов
21. Передача информации
22. Расширение области принятия решений
23. Регистрация деятельности и контроль за внесением изменений
24. Техническая поддержка реагирования на инциденты ИБ
25. Документация системы управления инцидентами ИБ
26. Политика управления инцидентами ИБ
27. Программа управления инцидентами ИБ
28. Группа реагирования на инциденты ИБ
29. Обеспечение осведомленности и обучение в области инцидентов ИБ
30. Сохранение доказательств инцидента ИБ
31. Средства управления событиями ИБ

Образец экзаменационного билета:

…

ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Направление 10.04.01 «Информационная безопасность»
Дисциплина «Расследование компьютерных инцидентов»

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 2

1. Система управления инцидентами ИБ
1. Техническая поддержка реагирования на инциденты ИБ

Зав. кафедрой УИБ А.С. Исмагилова

Кафедра управления информационной безопасностью

Критерии оценки экзамена (в баллах):

- **25-30 баллов** выставляется студенту, если студент дал полные, развернутые ответы на все теоретические вопросы билета, продемонстрировал знание функциональных возможностей, терминологии, основных элементов, умение применять теоретические знания при выполнении практических заданий. Студент без затруднений ответил на все дополнительные вопросы. Практическая часть работы выполнена полностью без неточностей и ошибок;

- **17-24 баллов** выставляется студенту, если студент раскрыл в основном теоретические вопросы, однако допущены неточности в определении основных понятий. При ответе на дополнительные вопросы допущены небольшие неточности. При выполнении практической части работы допущены несущественные ошибки;

- 10-16 баллов выставляется студенту, если при ответе на теоретические вопросы студентом допущено несколько существенных ошибок в толковании основных понятий. Логика

и полнота ответа страдают заметными изъянами. Заметны пробелы в знании основных методов. Теоретические вопросы в целом изложены достаточно, но с пропусками материала. Имеются принципиальные ошибки в логике построения ответа на вопрос. Студент не решил задачу или при решении допущены грубые ошибки;

- <u>0-10</u> баллов выставляется студенту, если он отказался от ответа или не смог ответить на вопросы билета, ответ на теоретические вопросы свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Обнаруживается отсутствие навыков применения теоретических знаний при выполнении практических заданий. Студент не смог ответить ни на один дополнительный вопрос.

Комплект практических заданий

Для самостоятельного освоения и/или расширения знаний, умений, владений предусмотрены несколько практических заданий.

Типовое практическое задание №1. Модель угроз информационной безопасности

1. Выбрать объект защиты (документ, АРМ, ПК, помещение, АС и т.д.).
2. Собрать необходимую информацию.
3. Построить модель угроз информационной безопасности.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	5
Выполнены пункты 1-3	10
Максимальный балл	10

Типовое практическое задание №2. Модель нарушителя информационной безопасности

1. Выбрать объект защиты (документ, АРМ, ПК, помещение, АС и т.д.).
2. Собрать необходимую информацию.
3. Построить модель нарушителя безопасности.

Методические указания

а. Использовать известные уровни возможностей нарушителя, различные классификации нарушителя.

б. Помнить, для чего строится модель нарушителя.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	5
Выполнены пункты 1-3	10
Максимальный балл	10

См. подробнее в ФОС дисциплины.

Темы семинарских занятий (18 часов)

Семинар №1

1. Что такое событие ИБ? Примеры.

2. Что такое инцидент ИБ? Примеры. Чем событие отличается от инцидента?
3. Что такое управление инцидентами? Примеры.
4. Что такое менеджмент инцидентов ИБ? Зачем и кому он нужен?
5. Какие основные нормативные документы в РФ регулируют менеджмент инцидентов?
6. Из каких основных этапов состоит менеджмент инцидентов ИБ?

Задание. Подготовить ответ на любые 4 вопроса

Семинар №2

1. Цели и задачи управления инцидентами ИБ
2. Деятельность в рамках управления инцидентами ИБ. В чем она заключается?
3. Диаграмма процесса «Управление инцидентами ИБ». Как пользоваться на практике?
4. Система управления инцидентами ИБ. Что из себя представляет?
5. Ключевые вопросы при создании результативно функционирующей СУИИБ

Задание. Подготовить ответ на любые 3 вопроса

Семинар №3

1. Какие ключевые составляющие этапа использования СУИИБ можно выделить?
2. Какие действия по анализу состояния ИБ и управлению инцидентами ИБ следует предпринять после разрешения/закрытия инцидентов ИБ?
3. Что понимается под улучшением процесса управления инцидентами ИБ? Для чего оно нужно?
4. В чем заключается первая оценка и предварительное решение по событию ИБ? Какова ее роль?

Задание. Подготовить ответ на любые 2 вопроса

Семинар №4

1. Реагирование на инциденты ИБ. Из каких этапов состоит? Чем поддерживается? Кем и как осуществляется? Чем заканчивается?
2. Антикризисные действия. В чем заключаются? Когда и зачем они нужны?
3. Основные документы по управлению инцидентами ИБ. Чем они по существу отличаются?
4. Программа управления инцидентами ИБ. Каково ее основное содержание? Кто и как выполняет эту программу? Какие сложности могут возникать при выполнении?

Задание. Подготовить ответ на любые 2 вопроса

Семинар №5

1. Группа реагирования на инциденты ИБ. Цель создания. Состав. Функции и полномочия.
2. В чем различия немедленного и последующего реагирования на инцидент ИБ?
3. Какие стратегии реагирования на инциденты ИБ можно выделить?
4. Что такое режим антикризисных действий?

Задание. Подготовить ответ на любые 2 вопроса

Семинар №6

1. Сохранение доказательств инцидента ИБ. Какие правила и способы применяются?
2. Каких важных принципов необходимо придерживаться при сборе доказательств инцидента ИБ? Какова последовательность действий?
3. Какими средствами осуществляется обеспечение осведомленности и обучения в области инцидентов ИБ?

Задание. Подготовить ответ на любые 2 вопроса

Семинар №7

1. Средства управления событиями ИБ.
2. Моделирование инцидентов ИБ.
3. Что может принести больше пользы: выстраивание процесса управления инцидента ИБ и его последующее непрерывное улучшение или автоматизация операций реагирования на инциденты ИБ без выстраивания процесса? Почему?

Задание. Подготовить ответ на любые 2 вопроса

Семинар №8

1. Что такое организация непрерывности бизнеса (ОНБ)? Как она связана с инцидентами?
2. Что такое УНБ? Какие ключевые аспекты у него есть?
3. Какие результаты может получить организация от реализации УНБ?

Задание. Подготовить ответ на любые 2 вопроса

Семинар №9

1. Что такое СУНБ? Ключевые компоненты и решения СУНБ
2. Жизненный цикл УНБ. Из каких основных элементов состоит жизненный цикл УНБ?
3. Программа УНБ.
4. Из каких этапов состоит программа УНБ?

Задание. Подготовить ответ на любые 3 вопроса

Критерии оценки (в баллах) аудиторной практической работы *(должны строго соответствовать рейтинг плану по макс. и мин. колич. баллов и только для тех, кто учится с использованием модульно-рейтинговой системы обучения и оценки успеваемости студентов*):

- 2 балла выставляется студенту, если выполнил задание на 100%
- 1 балл выставляется студенту, если выполнил задание на 75%
- 0,5 баллов выставляется студенту, если выполнил задание на 50%
- 0 баллов выставляется студенту, если не выполнил задание

Комплект лабораторных работ

Типовая лабораторная работа №1 (5 часов)

Отчеты по событиям и инцидентам ИБ

Задание Для гипотетической организации разработать пакет документов по менеджменту инцидентов ИБ (отчеты о событиях и инцидентах ИБ)

Указание. Желательно, чтобы разработанные документы имели удобный способ заполне-

ния, чтения и обработки (схемы, таблицы, формы и т.д.)

Рекомендации по заполнению

Назначением данной формы (формы отчета о событиях и инцидентах ИБ) является обеспечение информацией о событии ИБ, а затем, если оно определено как инцидент ИБ, то и об инциденте ИБ, для определенных лиц.

Если подозревается, что событие ИБ развивается или уже свершилось, особенно событие, которое может привести к существенным потерям или ущербу собственности или репутации организации, то необходимо немедленно заполнить и передать форму отчета о событии ИБ в соответствии с процедурами, описанными в системе менеджмента инцидентов ИБ организации.

Представленная информация будет использована для инициирования соответствующего процесса оценки, которая определит, должно ли это событие категорироваться как инцидент ИБ и (в случае положительного ответа), какие корректирующие меры, необходимые для предотвращения или ограничения потерь или ущерба, следует предпринять. Поскольку процесс оценки по своему характеру является краткосрочным, то в данный момент необязательно заполнять все поля формы отчета.

Если сотрудник является членом группы обеспечения эксплуатации, анализирующим полностью/частично заполненные формы отчета, то он должен принять решение, надо ли отнести данное событие к категории инцидента ИБ.

При положительном решении сотрудник должен внести в форму отчета об инциденте ИБ как можно больше информации и передать формы отчетов о событии и инциденте ИБ в ГРИИБ. Независимо от того, будет ли событие ИБ отнесено к категории инцидента ИБ, база данных событий/инцидентов ИБ должна быть обновлена.

Если сотрудник является сотрудником ГРИИБ, анализирующим формы отчетов о событиях и инцидентах ИБ, переданные членом группы обеспечения эксплуатации, то форма отчета об инциденте ИБ должна обновляться по ходу расследования и, соответственно, должна обновляться база данных событий/инцидентов ИБ.

При заполнении форм следует соблюдать следующие рекомендации:

- по возможности формы отчета должны заполняться и передаваться в электронном виде. В случае, если существуют проблемы или считается, что существуют проблемы с принятыми по умолчанию механизмами электронного оповещения (например, электронная почта), включая случаи, когда система может подвергаться атаке и формы отчета могут быть прочитаны несанкционированными лицами, должны использоваться альтернативные средства связи. Альтернативными средствами связи могут быть телефон или текстовые сообщения, а также использование курьеров следует представить информацию, основанную на фактах, в которой сотрудник уверен, не следует что-либо придумывать для того, чтобы заполнить все формы. Если сотрудник считает уместным включить иную информацию, которую не может подтвердить, следует указать, что это неподтвержденная информация, и причину убежденности в ее недостоверности;
- следует подробно указать, как можно связаться с сотрудником. Немедленно или спустя некоторое время может возникнуть необходимость контакта с ним для получения дальнейшей информации, касающейся Вашего отчета. Если позднее сотрудник обнаружит, что какая-либо представленная им информация неточна, неполна или ошибочна, то следует внести поправки в отчет и представить его повторно.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	4
Выполнены пункты 1-4	9

Максимальный балл	9

Типовая лабораторная работа №2 (4 часа)
События в инциденты ИБ

Задание На примере гипотетической организации разработать (придумать) событие (события) ИБ, развить его (их) до инцидента ИБ. Подробно расписать путь развития, включая хронологию, участников, организационные и технические средства, задействованные ресурсы, задетые активы организации и причиненный ущерб.

Указание. При описании инцидента можно использовать материалы из лабораторной работы №1 (схемы, таблицы, формы и т.д.).

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-3	4
Выполнены пункты 1-5	8
Максимальный балл	8

Типовая лабораторная работа №3 (4 часа)
Компьютерные инциденты

Задание

1. На примере гипотетической организации разработать (придумать)два компьютерных инцидента. Подробно расписать путь развития, включая хронологию, участников, организационные и программные средства, задействованные ресурсы, задетые активы организации и причиненный ущерб
2. Провести анализ и оценку инцидента
3. Провести процедуру немедленного реагирования
4. Подготовить антикризисные действия
5. Провести процедуру последующего реагирования

Указание. При описании инцидента можно использовать материалы из лабораторной работы №1,2 (схемы, таблицы, формы и т.д.).

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-3	4
Выполнены пункты 1-5	7
Максимальный балл	7

Типовая лабораторная работа №4 (5 часов)
Сохранение доказательств инцидента

Задание Для инцидентов из лабораторной работы №4 описать процедуру сохранения доказательств (подробно расписать применяемые принципы, правила и способы, последовательность действий)

Указание. При описании инцидента можно использовать материалы из лабораторной работы №1,2,3,4 (схемы, таблицы, формы и т.д.).

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-3	4

Выполнены пункты 1-5	8
Максимальный балл	8

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Лукаш, Ю.А. Контроль персонала как составляющая безопасности и развития бизнеса : учебное пособие / Ю.А. Лукаш. - 2-е изд., стер. - Москва : Издательство «Флинта», 2017. - 24 с. - ISBN 978-5-9765-1377-8 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=115078.
2. Милославская, Н.Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса : учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - Москва : Горячая линия - Телеком, 2013. - 170 с. : ил. - (Вопросы управления информационной безопасностью. Вып. 3). - Библиогр. в кн. - ISBN 978-5-9912-0273-2 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=253577.

Дополнительная литература:

1. Сердюк, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий : учебное пособие / В.А. Сердюк ; Высшая Школа Экономики Национальный Исследовательский Университет. - Москва : Издательский дом Высшей школы экономики, 2015. - 574 с. : ил. - Библиогр. в кн. - ISBN 978-5-7598-0698-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=440285
2. Милославская, Н.Г. Технические, организационные и кадровые аспекты управления информационной безопасностью : учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - Москва : Горячая линия - Телеком, 2013. - 216 с. : ил. - (Вопросы управления информационной безопасностью. Вып. 4). - Библиогр. в кн. - ISBN 978-5-9912-0274-9; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=253578
3. Инструментальный контроль и защита информации : учебное пособие / Н.А. Свинарев, О.В. Ланкин, А.П. Данилкин и др. ; Министерство образования и науки РФ, ФГБОУ ВПО «Воронежский государственный университет инженерных технологий». - Воронеж : Воронежский государственный университет инженерных технологий, 2013. - 192 с. : табл., ил. - Библиогр. в кн. - ISBN 978-5-00032-018-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=255905

5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы

1. Справочная правовая система «КонсультантПлюс» – http://www.consultant-plus.ru.
2. Электронная библиотечная система «Университетская библиотека онлайн» – https://biblioclub.ru.
3. Электронная библиотечная система издательства «Лань» – https://e.lanbook.com/
4. Электронный каталог Библиотеки БашГУ – http://www.bashlib.ru/catalogi/
5. www.fstec.ru –сайт ФСТЭК России

6. www.fsb.ru – сайт ФСБ России
7. http://window.edu.ru/ – Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам»;
8. http://univertv.ru/video/matematika/ – Открытый образовательный видеопортал UniverTV.ru. Образовательные фильмы на различные темы. Лекции в ведущих российских и зарубежных вузах. Научная конференция или научно-популярная лекция по интересующему вопросу);
9. www.newlibrary.ru – Новая электронная библиотека;
10. www. edu.ru – Федеральный портал российского образования;
11. www.elibrary.ru – Научная электронная библиотека;
12. www.nehudlit.ru – Электронная библиотека учебных материалов.

Перечень лицензионного программного обеспечения:

1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные.
2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
3. Система централизованного тестирования БашГУ (Moodle).GNU General Public License.

6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения	
1. Учебная аудитория для проведения занятий лекционного типа: Аудитория № 515 **2. Учебная аудитория для проведения занятий семинарского типа:** Аудитория № 508. Специализированная аудитория с лабораторным оборудованием. Аудитория № 509. Лаборатория моделирования процессов защиты информации. **3. Учебная аудитория для проведения групповых и индивидуальных консультаций:** Аудитория № 608 **4. Учебная аудитория для текущего контроля и промежуточной аттестации:** Аудитория № 609 Адрес всех аудиторий 450076, Республика Башкортостан, Городской Округ Город Уфа, город Уфа, улица Карла Маркса, дом 3/4, помещение 2	Лекции, практические занятия, лабораторные занятия, групповые и индивидуальные консультации, текущий контроль, промежуточная аттестация	**Аудитория № 515** Оборудование: учебная мебель, доска, терминал видео конференц-связи LifeSizeIcon 600-камера, интерактивная система со встроенным короткофокусным проектором PrometheanActivBoard 387 RPOMOUNTEST, профессиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMARTPodiumSP518 с ПО SMARTNotebook, матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H, интерактивная напольная кафедра докладчика, ком-ер встраиваемый в кафедру INTEL-Corei3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/ThermaltakeVL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром. **Аудитория № 508. Специализированная аудитория с лабораторным оборудованием.** Оборудование: учебная мебель, доска, мобильное мультимедийное оборудование, учебно-демонстрационная панель «Монтаж средств технической защиты информации. **Аудитория № 509. Лаборатория моделирования процессов защиты информации.** Оборудование: учебная мебель, доска, мобильное мультимедийное оборудование, учебно-лабораторный стенд «Сетевая безопасность». **Аудитория № 608** Оборудование: учебная мебель, доска, мобильное мультимедийное оборудование, телевизор TCL-L55P6US. **Аудитория № 609** Оборудование: учебная мебель, доска, мобильное мультимедийное оборудование.	**Перечень лицензионного программного обеспечения:** 1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные. 2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные. 3. Система централизованного тестирования БашГУ (Moodle).GNU General Public License.

Приложение 1

ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Содержание рабочей программы
дисциплины Расследование компьютерных инцидентов
(1 семестр)

Вид работы	**Объем дисциплины**
Общая трудоемкость дисциплины (ЗЕТ / часов)	4 ЗЕТ / 144 часа
Учебных часов на контактную работу с преподавателем:	55,2
лекций	18
практических/ семинарских	18
лабораторных	18
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	1,2
Учебных часов на самостоятельную работу обучающихся (СР)	52,8
Учебных часов на подготовку к экзамену	36

Форма контроля:
Экзамен 1 семестр

1 семестр

№	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Задания по самостоятельной работе	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР	ЛР	СРС		
1	2	3	4	5	6	7	8
1	НОРМАТИВНАЯ БАЗА УПРАВЛЕНИЯ ИНЦИДЕНТАМИ ИБ И ОБЕСПЕЧЕНИЕ НЕПРЕРЫВНОСТИ БИЗНЕСА ISO/1EC 27035:2011 — управление инцидентами ИБ. ISO/IEC 27037 — руководство по идентификации, сбору и/или получению и обеспечению сохранности свидетельств, представленных в электронной форме. ISO/IEC 27031:2011 — руководство по готовности информационных и телекоммуникационных технологий для обеспечения непрерывности бизнеса. BS 25999 и ГОСТ Р 53647 – управление непрерывностью бизнеса	2	2	2	6	Каков порядок использования нормативной базы управления инцидентами ИБ?	Лабораторная работа Практическое задание
2	УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИБ Событие и инцидент ИБ. Цели и задачи управления инцидентами ИБ. Деятельность в рамках управления инцидентами ИБ	2	2	2	6	Для чего надо разделять событие и инцидент ИБ?	Лабораторная работа Практическое задание
3	СИСТЕМА УПРАВЛЕНИЯ ИНЦИДЕНТАМИ ИБ Ключевые вопросы при создании системы. Обязательства руководства и поддержка. Эффективность и качество функционирования СУИИБ. Конфиденциальность в СУИИБ. Независимость деятельности ГРИИБ. Правовые и нормативные аспекты управления инцидентами ИБ и СУИИБ. Специальные нормативные требования	2	2	2	6	Можно ли обойтись без СУИИБ при работе с инцидентами?	Лабораторная работа Практическое задание
4	ЭТАПЫ ПРОЦЕССА УПРАВЛЕНИЯ ИНЦИДЕНТАМИ ИБ Планирование и подготовка процесса управления инцидентами ИБ. Использование системы управления инцидентами ИБ. Анализ процесса управления инцидентами ИБ. Улучшение процесса управления инцидентами ИБ. Обнаружение событий ИБ и инцидентов иб и оповещение о них. Обработка событий ИБ и инцидентов ИБ. Первая оценка и предварительное решение по событию ИБ. Вторая оценка и подтверждение инцидента ИБ	2	2	2	6	Для чего процесс управления делят на этапы, можно ли обойтись без этого?	Лабораторная работа Практическое задание
5	КОНТРОЛИРУЕМОСТЬ ИНЦИДЕНТА ИБ Последующее реагирование на инцидент ИБ. Антикризисные действия. Правовая экспертиза инцидентов ИБ. Передача информации. Расширение области принятия решений. Регистрация деятельности и контроль над вне-	2	2	2	6	В чем смысл регистрации деятельности и контроль над внесением измене-	Лабораторная работа Практическое задание

	сением изменений. Техническая поддержка реагирования на инциденты ИБ					ний?	
6	ДОКУМЕНТАЦИЯ СИСТЕМЫ УПРАВЛЕНИЯ ИНЦИДЕНТАМИ ИБ Политика управления инцидентами ИБ. Программа управления инцидентами ИБ	2	2	2	6	Чем по существу отличаются политика и программа управления инцидентами ИБ?	Лабораторная работа Практическое задание
7	ГРУППА РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИБ Распределение обязанностей членов ГРИИБ. Уровень полномочий руководителя ГРИИБ и членов его группы. Основные источники научно-методических разработок по тематике ГРИИБ	2	2	2	6	В каком случае организации обязательно иметь ГРИИБ?	Лабораторная работа Практическое задание
8	ОБЕСПЕЧЕНИЕ ОСВЕДОМЛЕННОСТИ И ОБУЧЕНИЕ В ОБЛАСТИ ИНЦИДЕНТОВ ИБ Программа обеспечения осведомленности. Инструктажи по обеспечению осведомленности. Сохранение доказательств инцидента ИБ	2	2	2	6	К чему может привести отсутствие осведомленности?	Лабораторная работа Практическое задание
9	СРЕДСТВА УПРАВЛЕНИЯ СОБЫТИЯМИ ИБ Уровни управления событиями ИБ. Ядро. База данных. Управляющий интерфейс. Визуализация собранных данных. Моделирование инцидентов	2	2	2	4,8	Что по существу дает моделирование инцидентов?	Лабораторная работа Практическое задание
	Всего	18	18	18	52,8		