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

Утверждено
на заседании кафедры
протокол № 6 от 31 января 2022 г.
Зав. кафедрой _____ / Исмагилова А.С.

Согласовано
Председатель УМК института

_____ / Гильмутдинова Р.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Расследование инцидентов информационной безопасности

Часть, формируемая участниками образовательных отношений

программа бакалавриата

Направление подготовки
10.03.01 Информационная безопасность

Направленность (профиль) подготовки
Организация и технология защиты информации
(в системе государственного и муниципального управления)

Квалификация
Бакалавр

Форма обучения
Очная

Разработчик (составитель)
Ассистент

_____ / Белова Е. П.

Для приема 2022 г.

Уфа - 2022 г.

Составитель: Белова Елена Петровна

Рабочая программа дисциплины утверждена на заседании кафедры управления информационной безопасностью, протокол № 6 от 31 января 2022 г.

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/

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
2. Цель и место дисциплины в структуре образовательной программы
3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)
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.

   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.
5. Учебно-методическое и информационное обеспечение дисциплины

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

   5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы
6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

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

По итогам освоения дисциплины обучающийся должен достичь следующих результатов обучения:

Категория (группа) компетенций (при наличии ОПК)	Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине
	ПК-2 Способен управлять защитой информации в автоматизированных системах.	*ПК 2.1. Знать методы защиты информации в автоматизированных системах.*	*Знает методы защиты информации в автоматизированных системах.*
		ПК 2.2 Уметь управлять специализированным программным обеспечением для защиты информации в автоматизированных системах.	*Умеет управлять специализированным программным обеспечением для защиты информации в автоматизированных системах.*
		ПК 2.3 Владеть навыками выявления и анализа уязвимостей, выбора оптимальной стратегии для обеспечения информационной безопасности в автоматизированных системах.	*Владеет навыками выявления и анализа уязвимостей, выбора оптимальной стратегии для обеспечения информационной безопасности в автоматизированных системах.*

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Расследование инцидентов информационной безопасности» относится к части, формируемой участниками образовательных отношений.
Дисциплина изучается на 3 курсе в 1 семестре.
Целью учебной дисциплины «Расследование инцидентов информационной безопасности» является получение комплексных навыков своевременного обнаружения, анализа и предотвращения различных инцидентов 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.

ПК-2 - Способен управлять защитой информации в автоматизированных системах.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
ПК 2.1 - Знать методы защиты информации в автоматизированных системах.	Знать методы защиты информации в автоматизированных системах.	Не знает методы защиты информации в автоматизированных системах.	Имеет отдалённые представления о методах защиты информации в автоматизированных системах.	Частично знает методы защиты информации в автоматизированных системах.	Знает методы защиты информации в автоматизированных системах.
ПК 2.2 - Уметь управлять специализированным программным обеспечением для защиты информации в автоматизированных системах.	Уметь управлять специализированным программным обеспечением для защиты информации в автоматизированных системах.	Не умеет управлять специализированным программным обеспечением для защиты информации в автоматизированных системах.	Имеет отдалённые представления об управлении специализированным программным обеспечением для защиты информации в автоматизированных системах.	Частично умеет управлять специализированным программным обеспечением для защиты информации в автоматизированных системах.	Умеет управлять специализированным программным обеспечением для защиты информации в автоматизированных системах.
ПК 2.3 - Владеть навыками выявления и	Владеть навыками выявления и анализа уязвимостей, выбора оптимальной	Не владеет навыками выявления и анализа уязвимостей, выбора оптимальной	Имеет смутные представления о выявлении и анализе уязвимостей,	Частично владеет навыками выявления и анализа уязвимостей, выбора	Владеет навыками выявления и анализа уязвимостей, выбора оптимальной

анализа уязвимостей, выбора оптимальной стратегии для обеспечения информационной безопасности в автоматизированных системах.	стратегии для обеспечения информационной безопасности в автоматизированных системах.	стратегии для обеспечения информационной безопасности в автоматизированных системах.	выборе оптимальной стратегии для обеспечения информационной безопасности в автоматизированных системах.	оптимальной стратегии для обеспечения информационной безопасности в автоматизированных системах.	стратегии для обеспечения информационной безопасности в автоматизированных системах.

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей, 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».

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.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Оценочные средства
ПК-2 Способен управлять защитой информации в автоматизированных системах.	Знать методы защиты информации в автоматизированных системах.	Аудиторная работа, тесты, устный опрос.
	Уметь управлять специализированным программным обеспечением для защиты информации в автоматизированных системах.	Аудиторная работа, тесты, устный опрос.

	Владеть навыками выявления и анализа уязвимостей, выбора оптимальной стратегии для обеспечения информационной безопасности в автоматизированных системах.	Аудиторная работа, тесты, устный опрос.

Рейтинг-план

дисциплины «Расследование инцидентов информационной безопасности»

Виды учебной деятельности	**Балл за конкретное задание**	**Число заданий за семестр**	**Баллы**	
			Минимальный	**Максимальный**
Модуль 1. Система менеджмента инцидентов ИБ защищенных телекоммуникационных систем и её планирование				
Текущий контроль			**0**	35
1. Аудиторная работа	5	6	0	30
2. Устный опрос	1	5	0	5
Рубежный контроль			**0**	10
1.Тесты	1	10	0	10
Модуль 2. Использование, анализ и улучшение системы менеджмента инцидентов ИБ защищенных телекоммуникационных систем. Менеджмент конкретных видов инцидентов телекоммуникационных систем				
Текущий контроль			**0**	35
1. Аудиторная работа	5	6	0	30
2. Устный опрос	1	5	0	5
Рубежный контроль			**0**	10
1.Тесты	1	10	0	10
Поощрительные баллы				
1. Студенческая олимпиада, участие в конференциях	5			5
2. Публикация статей	5			5
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
Посещение лекционных занятий			0	–6
2. Посещение практических (семинарских, лабораторных занятий)			0	–10
Итоговый контроль				
Экзамен			0	30

Устный индивидуальный опрос

Устный индивидуальный опрос проводится после изучения новой темы с целью выяснения наиболее сложных вопросов, степени усвоения информации.

Обучающийся излагает содержание вопроса изученной темы.

Критерии и методика оценивания:

- 5 баллов выставляется обучающемуся, если точно используется специализированная терминология, показано уверенное владение нормативной базой;

- 4 балла выставляется обучающемуся, допущены один-два недочета при освещении основного содержания ответа, нет определенной логической последовательности, неточно используется специализированная терминология;

- 3 балла выставляется обучающемуся, нет общего понимания вопроса, имеются затруднения или допущены ошибки в определении понятий, использовании терминологии.

Устный групповой опрос

Устный групповой опрос проводится после изучения новой темы с целью выяснения наиболее сложных вопросов, степени усвоения информации, поддержания внимания слушающей аудитории.

Критерии и методика оценивания:

- 5 баллов выставляется обучающемуся, если точно используется специализированная терминология, показано уверенное владение нормативной базой;

- 4 балла выставляется обучающемуся, допущены один-два недочета при освещении основного содержания ответа, нет определенной логической последовательности, неточно используется специализированная терминология;

- 3 балла выставляется обучающемуся, нет общего понимания вопроса, имеются затруднения или допущены ошибки в определении понятий, использовании терминологии

Экзамен

Проводится в 5 семестре. Экзаменационный билет содержит 2 теоретических вопроса.

Типовые экзаменационные вопросы:

1. Термины и определения: событие информационной безопасности (ИБ); инцидент ИБ; менеджмент инцидентов ИБ; группа реагирования на инциденты ИБ.
2. Виды инцидентов ИБ защищенных телекоммуникационных систем: неавторизованный доступ; отказ в обслуживании; вредоносный код; несоответствующее использование; сбор информации.
3. Причины возникновения инцидентов ИБ защищенных телекоммуникационных систем: остаточные риски, изменения внутренней и внешней среды (появление новых угроз), появление новых уязвимостей.
4. Последствия инцидентов ИБ.
5. Цели менеджмента инцидентов ИБ. Система менеджмента инцидентов ИБ защищенных телекоммуникационных систем.
6. Процессы менеджмента инцидентов ИБ защищенных телекоммуникационных систем.
7. Политика менеджмента инцидентов ИБ.
8. Содержание политики менеджмента инцидентов ИБ.
9. Документационное обеспечение системы менеджмента инцидентов ИБ.
10. Процедуры менеджмента инцидентов ИБ защищенных телекоммуникационных систем.
11. Группа реагирования на инциденты ИБ (ГРИИБ). Назначение. Члены группы реагирования и её структура.
12. Группа реагирования на инциденты ИБ (ГРИИБ). Взаимодействие с другими подразделениями организации.
13. Группа реагирования на инциденты ИБ (ГРИИБ). Отношения со сторонними лицами и организациями.
14. Техническая поддержка обработки инцидентов ИБ и восстановления после них.

15. Обеспечение осведомленности сотрудников об обнаружении и оповещении об инцидентах ИБ защищенных телекоммуникационных систем.
16. Обучение персонала ГРИИБ менеджменту инцидентов ИБ защищенных телекоммуникационных систем.
17. Контрольный перечень действий по обработке инцидентов ИБ защищенных телекоммуникационных систем.
18. Приоритетный порядок обработки инцидентов ИБ на основе классификации инцидентов защищенных телекоммуникационных систем.
19. Использование системы менеджмента инцидентов ИБ защищенных телекоммуникационных систем.
20. Обнаружение и оповещение об Инциденте ИБ защищенных телекоммуникационных систем.
21. Средства обнаружения инцидентов ИБ.
22. Предвестники и указатели инцидентов ИБ защищенных телекоммуникационных систем.
23. Анализ инцидентов ИБ защищенных телекоммуникационных систем. Порядок анализа событий ИБ и инцидентов ИБ. Первичная оценка. Отчётность о событии ИБ. Вторичная оценка. Отчётность об инциденте ИБ.
24. Сдерживание инцидента ИБ защищенных телекоммуникационных систем. Принятие решения о сдерживании.
25. Стратегии сдерживания инцидента ИБ.
26. Устранение инцидента ИБ защищенных телекоммуникационных систем и восстановление после него. Действия по устранению инцидента и восстановлению после него.
27. Резервное копирование данных. Резервный фонд оборудования.
28. Сбор и обработка данных об инцидентах ИБ защищенных телекоммуникационных систем. Цель сбора данных.
29. Статистические данные об инцидентах ИБ. Итоговая отчётность об инцидентах ИБ. Срок хранения данных об инцидентах ИБ.
30. Определение и осуществление улучшений оценки риска и управления информационной безопасностью.
31. Определение и осуществление улучшений системы менеджмента инцидентов ИБ защищенных телекоммуникационных систем.
32. Определение инцидента неавторизованного доступом. Примеры инцидентов неавторизованного доступа.
33. Менеджмент инцидентов неавторизованного доступа.
34. Определение инцидента отказа в обслуживании. Примеры инцидентов отказа в обслуживании: рефлекторные атаки, усилительные атаки, атаки распределенного отказа в обслуживании.
35. Менеджмент инцидентов отказа в обслуживании.
36. Определение инцидента, связанного с применением вредоносного кода. Примеры инцидентов, связанных с применением вредоносного кода.
37. Менеджмент инцидентов, связанных с применением вредоносного кода.
38. Определение инцидента, связанного с несоответствующим использованием. Примеры инцидентов, связанных с несоответствующим использованием.
39. Менеджмент инцидентов, связанных с несоответствующим использованием.
40. Определение инцидента сбора информации. Примеры инцидентов сбора информации.
41. Менеджмент инцидентов сбора информации.

Критерии оценивания результатов экзамена: При выставлении баллов именно за экзамен (до 30 баллов в дополнение к баллам, полученным за другие виды отчетности) действует

такой критерий оценки:

25-30 баллов

Студент дал полные, развернутые ответы на теоретический вопрос билета и правильно выполнил практическое задание, продемонстрировал знание функциональных возможностей, терминологии, умение применять теоретические знания при выполнении практических заданий. Студент без затруднений ответил на дополнительные вопросы. Практическая часть работы выполнена полностью без неточностей и ошибок.

17-24 баллов

Студент раскрыл в основном теоретический вопрос, однако допущены неточности в определении основных понятий. При ответе на дополнительные вопросы допущены небольшие неточности. При выполнении практической части работы допущены несущественные ошибки, но все задание выполнено до конца.

10-16 баллов

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. Теоретические вопросы в целом изложены достаточно, но с пропусками материала. Имеются принципиальные ошибки в логике построения ответа на вопрос. Студент сделал практическое задание лишь частично.

1-10 баллов

Ответ на теоретический вопрос свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Студент не смог ответить ни на один дополнительный вопрос. При этом студент не решил задачу или лишь частично (на ½ от задания).

Перевод оценки из 100-балльной в 4-балльную производится следующим образом:
- отлично – от 80 до 110 баллов (включая 10 поощрительных баллов);
- хорошо – от 60 до 79 баллов;
- удовлетворительно – от 45 до 59 баллов;
- неудовлетворительно – менее 45 баллов.

Типовые вопросы для тестирования

1. Событие ИБ – это…

а) идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики ИБ или аварию защитных мер (средств), а также возникновение ранее неизвестной ситуации, которая может быт
ь связана с безопасностью;

б) идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики ИБ или аварию защитных мер (средств);

в) нарушение политики ИБ или авария защитных мер (средств) системы.

2. Инцидент ИБ - это…

а) одно или серия нежелательных событий ИБ, которые имеют значительную вероятность компрометации бизнес-операций (бизнес-функций) и угрожают информационной безопасности;

б) события ИБ, которые угрожают информационной безопасности;

в) нежелательные события ИБ, которые компрометируют бизнес-операции.

3. Входит ли установление причин инцидентов в жизненный цикл управления событиями и инцидентами ИБ?

а) входит;

б) нет.

4. Контроль за реализацией единых правил эксплуатации средств обнаружения

компьютерных атак на информационные ресурсы входит в деятельность:
а) анализа данных о событиях безопасности;
б) обнаружения компьютерных атак;
в) по регистрации инцидентов.

5. Деятельность по обнаружению компьютерных атак включает в себя:
а) контроль за централизованным обновлением баз решающих правил для средств обнаружения компьютерных атак;
б) выявление ранее неизвестных компьютерных атак сетевого уровня, в том числе с применением средств анализа сетевого трафика на каналах связи;
в) оба вышеперечисленных процесса.

Критерии оценки теста

Показатель оценки	Распределение баллов
Обучающийся выполнил задание лишь частично	5
Обучающийся с ошибками выполнил задание	20
Обучающийся выполнил задание	30

Контрольная работа №1 (Модуль 1)

Построить возможные сценарии инцидента внедрения вредоносного кода.

Критерии оценки

Показатель оценки	Распределение баллов
Обучающийся выполнил задание лишь частично	5
Обучающийся с ошибками выполнил задание	10
Обучающийся выполнил задание	15

Контрольная работа №2 (Модуль 2)

Построить возможные сценарии инцидента сбора информации.

Критерии оценки

Показатель оценки	Распределение баллов
Обучающийся выполнил задание лишь частично	5
Обучающийся с ошибками выполнил задание	10
Обучающийся выполнил задание	15

Практические занятия

№	Наименование практических занятий	Трудоёмкость (час.)
1	Обнаружение событий ИБ, которые могут быть причиной инцидента ИБ с помощью программных средств: система обнаружения вторжений Snort, антивирусное программное обеспечение «Антивирус Касперского 6.0», утилита проверки целостности файлов «GFI LANguard System Integrity Monitor», записи журналов системы защиты Secret Net.	6

	Заполнение формы «Отчет о событии ИБ»	
2	Анализ и реагирование на инциденты ИБ: неавторизованный доступ; сбор информации. Анализ и реагирование на инциденты ИБ: несоответствующее использование (Проведение практических занятий в форме групповых дискуссий, деловой игры).	
3	Выработка стратегии сдерживания инцидентов ИБ. Выработка стратегии по устранению инцидентов ИБ. Формирование итоговой отчётности об инциденте ИБ. (Проведение практических занятий в форме групповых дискуссий, деловой игры)	8

Выполнение практического задания - 5 баллов, частичное выполнение практического задания - от 3 до 4 баллов.

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Башкирского государственного университета. Текущая аттестация проводится в форме аудиторной, лабораторной, письменной контрольной, практической работы. Критерии оценивания приведены выше.

Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования.

При оценивании используются количественные шкалы оценок. Критерии оценивания приведены выше.

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература:

1. 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. Электронная библиотечная система «Университетская библиотека онлайн» – https://biblioclub.ru.
2. Электронная библиотечная система издательства «Лань» – https://e.lanbook.com/
3. Электронный каталог Библиотеки БашГУ – http://www.bashlib.ru/catalogi/
4. http://window.edu.ru/ – Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам»;
5. 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);
6. www.newlibrary.ru – Новая электронная библиотека;
7. www. edu.ru – Федеральный портал российского образования;
8. www.elibrary.ru – Научная электронная библиотека;
9. www.nehudlit.ru – Электронная библиотека учебных материалов.
10. 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.
11. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
12. Система централизованного тестирования БашГУ (Moodle).GNU General Public License.

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

Наименование специальных помещений и помещений для самостоятельной работы	*Вид занятий*	*Наименование оборудования, программного обеспечения*
1	**2**	**3**
Аудитория № 516	Лекции, семинары, практические занятия.	Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное

		оборудование.
Аудитория № 610	Лекции, семинары, практические занятия.	Учебная мебель, доска, LED Телевизор TCLL55P6 USBLACK – 1 шт., кронштейн для телевизора NBP 5 – 1 шт., Кабель HDMI (m)-HDH(m)ver14,10м.
Аудитория № 609	Лекции, семинары, практические занятия.	Учебная мебель, доска, мобильное мультимедийное оборудование.
Аудитория № 608	Лекции, семинары, практические занятия.	Учебная мебель, доска, мобильное мультимедийное оборудование
Аудитория № 613	Практические занятия, лабораторные работы.	Учебная мебель, доска, моноблок стационарный – 12 шт. с возможностью подключения к сети Интернет и доступа в электронную информационно-образовательную среду. Windows 8 Russian Windows Professional 8 Russian Up-grade. Договор №104 от 17.06.2013 г. Лицензии бессрочные. Microsoft Office Standard 2013 Russian. Договор №114 от 12.11.2014 г. Лицензии бессрочные.

Приложение 1

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

Содержание рабочей программы
дисциплины «Расследование инцидентов информационной безопасности»
на 7 семестр ОФО

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	3 ЗЕТ / 108 часов
Учебных часов на контактную работу с преподавателем:	37,2
лекций	12
практических/ семинарских	24
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	36
Учебных часов на самостоятельную работу обучающихся (СР)	20

Форма контроля:
экзамен 5 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 / Сем	ЛР	СР		
1	2	3	4	5	6	7	8
1.	**Модуль 1. Система менеджмента инцидентов ИБ защищенных телекоммуникационных систем и её планирование** **Раздел 1.** **Общие положения:** 1.1. Термины и определения: событие информационной безопасности (ИБ); инцидент ИБ; менеджмент инцидентов ИБ; группа реагирования на инциденты ИБ. Виды инцидентов ИБ защищенных телекоммуникационных систем: неавторизованный доступ; отказ в обслуживании;	6	12	-	10	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Аудиторная работа, тесты

	вредоносный код; несоответствующее использование; сбор информации. 1.2. Причины возникновения инцидентов ИБ защищенных телекоммуникационных систем: остаточные риски, изменения внутренней и внешней среды (появление новых угроз), появление новых уязвимостей. Последствия инцидентов ИБ. 1.3. Цели менеджмента инцидентов ИБ. Система менеджмента инцидентов ИБ защищенных телекоммуникационных систем. Процессы менеджмента инцидентов ИБ защищенных телекоммуникационных систем. **Раздел 2. Планирование системы менеджмента инцидентов ИБ защищенных телекоммуникационных систем:**						

	2.1. Политика менеджмента инцидентов ИБ. Содержание политики менеджмента инцидентов ИБ. Документационное обеспечение системы менеджмента инцидентов ИБ. Процедуры менеджмента инцидентов ИБ защищенных телекоммуникационных систем. 2.2. Группа реагирования на инциденты ИБ (ГРИИБ). Назначение. Члены группы реагирования и её структура. Взаимодействие с другими подразделениями организации. Отношения со сторонними лицами и организациями. 2.3. Техническая поддержка обработки инцидентов ИБ и восстановления после них. 2.4. Обеспечение осведомленности сотрудников об обнаружении и						

	оповещении об инцидентах ИБ защищенных телекоммуникационных систем. Обучение персонала ГРИИБ менеджменту инцидентов ИБ защищенных телекоммуникационных систем. 2.5. Контрольный перечень действий по обработке инцидентов ИБ защищенных телекоммуникационных систем. 2.6. Приоритетный порядок обработки инцидентов ИБ на основе классификации инцидентов защищенных телекоммуникационных систем						
2.	**Модуль 2. Использование, анализ и улучшение системы менеджмента инцидентов ИБ защищенных телекоммуникационных систем. Менеджмент конкретных видов инцидентов телекоммуникационных**	6	12	-	10	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Аудиторная работа, тесты

	систем **Раздел 3. Использование системы менеджмента инцидентов ИБ защищенных телекоммуникационных систем:** 3.1. Обнаружение и оповещение об Инциденте ИБ защищенных телекоммуникационных систем. Средства обнаружения инцидентов ИБ. Предвестники и указатели инцидентов ИБ защищенных телекоммуникационных систем. 3.2. Анализ инцидентов ИБ защищенных телекоммуникационных систем. Порядок анализа событий ИБ и инцидентов ИБ. Первичная оценка. Отчётность о событии ИБ. Вторичная оценка. Отчётность об инциденте ИБ. 3.3 Сдерживание инцидента ИБ защищенных						

	телекоммуникационных систем. Принятие решения о сдерживании. Стратегии сдерживания инцидента ИБ. 3.4. Устранение инцидента ИБ защищенных телекоммуникационных систем и восстановление после него. Действия по устранению инцидента и восстановлению после него. Резервное копирование данных. Резервный фонд оборудования. 3.5. Сбор и обработка данных об инцидентах ИБ защищенных телекоммуникационных систем. Цель сбора данных. Статистические данные об инцидентах ИБ. Итоговая отчётность об инцидентах ИБ. Срок хранения данных об инцидентах ИБ. **Раздел 4.** **Анализ и улучшение системы менеджмента инцидентов ИБ защищенных телекоммуникационных**						

	систем: 4.1. Изучение полученного опыта. 4.2. Определение и осуществление улучшений оценки риска и управления информационной безопасностью. 4.3. Определение и осуществление улучшений системы менеджмента инцидентов ИБ защищенных телекоммуникационных систем. **Раздел 5. Менеджмент конкретных видов инцидентов телекоммуникационных систем:** 5.1. Определение инцидента неавторизованного доступом. Примеры инцидентов неавторизованного доступа. Менеджмент инцидентов неавторизованного доступа. 5.2. Определение инцидента отказа в						

	обслуживании. Примеры инцидентов отказа в обслуживании: рефлекторные атаки, усилительные атаки, атаки распределенного отказа в обслуживании. Менеджмент инцидентов отказа в обслуживании. 5.3. Определение инцидента, связанного с применением вредоносного кода. Примеры инцидентов, связанных с применением вредоносного кода. Менеджмент инцидентов, связанных с применением вредоносного кода. 5.4. Определение инцидента, связанного с несоответствующим использованием. Примеры инцидентов, связанных с несоответствующим использованием. Менеджмент инцидентов, связанных с несоответствующим использованием. 5.5. Определение инцидента сбора информации. Примеры						

	инцидентов сбора информации. Менеджмент инцидентов сбора информации.						
	Всего часов	12	24	-	20		