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

Дисциплина
Основы управления информационной безопасностью

Обязательная часть (Б1.О.29)

программа бакалавриата

Направление подготовки
10.03.01 Информационная безопасность

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

Квалификация
бакалавр

Разработчик (составитель) . _____ .	_____ / Салов И.В.

Для приема: 2022г.

Уфа 2022 г.

Составитель: Салов Игорь Владимирович

Рабочая программа дисциплины *утверждена* на заседании кафедры 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 / 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

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**
	ОПК-2.3 Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности.	ОПК-2.3.1 Знает меры, методы и средства обеспечения безопасности объекта защиты информации с применением локальных нормативных актов и стандартов информационной безопасности.	Знать меры, методы и средства обеспечения безопасности объекта защиты информации с применением локальных нормативных актов и стандартов информационной безопасности..
		ОПК-2.3.2 Умеет разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности.	Уметь разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности..
		ОПК-2.3.3 Владеет методами и принципами разработки, внедрения и сопровождения комплекса мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности.	Владеть методами и принципами разработки, внедрения и сопровождения комплекса мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности..

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Основы управления информационной безопасностью» относится к обязательной части.

Дисциплина изучается на 4 курсе в 8 семестре.

Целью учебной дисциплины «Основы управления информационной безопасностью», является формирование навыков определения основных угроз безопасности информации, разработки и реализации политики управления доступом на объекте информатизации.

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

ОПК-2.3. Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
ОПК-2.3.1 Знает меры, методы и средства обеспечения безопасности объекта защиты информации с применением локальных нормативных актов и стандартов информационной безопасности.	Знать меры, методы и средства обеспечения безопасности объекта защиты информации с применением локальных нормативных актов и стандартов информационной безопасности..	Не знает или показывает очень слабые знания.	Знает меры, методы и средства обеспечения безопасности объекта защиты информации с применением локальных нормативных актов и стандартов информационной безопасности.
ОПК-2.3.2 Умеет разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности.	Уметь разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности..	Не умеет.	Умеет разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности.

ОПК-2.3.3 Владеет методами и принципами разработки, внедрения и сопровождения комплекса мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности.	Владеть методами и принципами разработки, внедрения и сопровождения комплекса мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности..	Не владеет.	Владеет методами и принципами разработки, внедрения и сопровождения комплекса мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности.

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

ОПК-2.3. Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности.

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
ОПК-2.3.1 Знает меры, методы и средства обеспечения безопасности объекта защиты информации с применением локальных нормативных актов и стандартов информационной безопасности.	Знать меры, методы и средства обеспечения безопасности объекта защиты информации с применением локальных нормативных актов и стандартов информационной безопасности..	тестирование, практическое задание
ОПК-2.3.2 Умеет разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности.	Уметь разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности..	тестирование, практическое задание
ОПК-2.3.3 Владеет методами и принципами разработки, внедрения и сопровождения комплекса мер по обеспечению безопасности	Владеть методами и принципами разработки, внедрения и сопровождения комплекса мер по обеспечению безопасности объекта защиты с	тестирование, практическое задание

объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности.	применением локальных нормативных актов и стандартов информационной безопасности..	

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; для зачета: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).
Шкалы оценивания:

(для зачета:

зачтено – от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),

не зачтено – от 0 до 59 рейтинговых баллов).

Рейтинг – план дисциплины
«Основы управления информационной безопасностью»

Направление подготовки: 10.03.01 Информационная безопасность

курс 4, семестр8

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Создание СУИБ на предприятии				
Текущий контроль			0	
Практическая работа	8	5	0	40
Рубежный контроль				
Тест	10	1	0	10
Всего		4	0	50
Модуль 2. Особенности реализации СМИБ.				
Текущий контроль				
Практическая работа	8	5	0	40
Рубежный контроль				
Тест	10	1	0	10
Всего		5	0	50
Поощрительные баллы				
1. Участие в студенческой олимпиаде по дисциплине	3	1	0	3
2.Публикация научной статьи	4	1	0	4
3.Участие в научно-практической конференции по профилю	3	1	0	3
Всего		3	0	10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			0	-6
2. Посещение практических (семинарских, лабораторных занятий)			0	-10

Итоговый контроль				
1. Зачет	60	1	60	100

Зачет

Вопросы для зачета:

1. Понятие информационной безопасности. Термины и определения.
2. Система информационной безопасности.
3. Проверка безопасности информационных систем. Аудит систем.
4. Общие сведения об информационной безопасности.
5. Проверка безопасности информационных систем. Мониторинг систем.
6. Основные составляющие информационной безопасности.
7. Внешний аудит.
8. Обоснование необходимости рассмотрения вопросов информационной безопасности.
9. Внутренний аудит.
10. Процессный подход в рамках управления ИБ.
11. Проблемы построения современных систем безопасности.
12. Слежение за доступом к системам и их использованием.
13. Стандарты информационной безопасности ISO/IEC серии 27000.
14. Отраслевые стандарты информационной безопасности
15. Стандарты и нормативные акты РФ в области информационной безопасности.
16. Оценка рисков нарушения безопасности.
17. Средства управления информационной безопасностью.
18. Защита от вредоносного программного обеспечения.
19. Ключевые средства контроля информационной безопасности.
20. Ответственность за информационные ресурсы.
21. Требование бизнеса по обеспечению контроля доступа.
22. Факторы, необходимые для успешной реализации системы информационной безопасности в организации.
23. Управление доступом пользователей. Обязанности пользователей.
24. Группы требований к информационной безопасности организации.
25. Система планирования бесперебойной работы организации.
26. Политика информационной безопасности.
27. Классификация информации.
28. Инфраструктура информационной безопасности.
29. Безопасность информации в должностных инструкциях.
30. Обучение пользователей правилам информационной безопасности.
31. Реагирование на события, таящие угрозу безопасности.
32. Оперирование с носителями информации и их защита.
33. Термины и определения информационной безопасности.
34. Понятие информационной безопасности.
35. Циклическая модель улучшения процессов.
36. Системный подход к управлению организацией.
37. Процессный подход к управлению организацией.
38. Планирование СУИБ.
39. Совершенствование СУИБ.
40. Стратегии построения и внедрения СУИБ.
41. Построение и внедрение процессов СУИБ по отдельности.
42. Идентификация процессов СУИБ организации.
43. Документирование и описание процесса СУИБ.
44. Работа с процессами СУИБ организации.

45. Задание процесса СУИБ.
46. Метод оценки рисков на основе модели информационных потоков.
47. Расчет рисков по угрозе целостности.
48. Управление безопасностью как элемент системы управления рисками.
49. Качественные методики управления рисками.
50. Программное обеспечение управление рисками COBRA.
51. Программное обеспечение управление рисками RA SoftwareTool.
52. Количественные методики управления рисками.
53. Метод управления рисками CRAMM.
54. Метод оценки рисков на основе модели угроз и уязвимостей.
55. Расчет рисков по угрозе информационной безопасности.
56. Методика оценки рисков информационной безопасности компании DigitalSecurity.
57. Деятельность по обеспечению ИБ организации как процесс.
58. Управление ИБ информационно-телекоммуникационных технологий организации.
59. Система управления ИБ организации.
60. Область действия СУИБ.
61. Документальное обеспечение СУИБ.
62. Поддержка СУИБ со стороны руководства организации.
63. Контроль сетевого доступа.

Примерная тематика курсовых проектов (работ)

Курсовое проектирование не предусмотрено

Тестовые задания

При изучении дисциплины используются тестовые задания закрытого типа. Каждое тестовое задание включает вопрос и варианты ответов к нему. Тестирование выполняется в письменной форме.
Необходимо выбрать один ответ из предложенных вариантов.

Модуль 1. Создание СУИБ на предприятии.

1. Цель информационной безопасности:

а) обеспечить комфортную работу организации и свести к минимуму финансовые затраты, посредством разработки комплекса нормативно-правовых документов;

б) обеспечить бесперебойную работу организации и свести к минимуму ущерб от событий, таящих угрозу безопасности, посредством разработки комплекса нормативно-правовых документов;

в) обеспечить бесперебойную работу организации и свести к минимуму ущерб от событий, таящих угрозу безопасности, посредством их предотвращения и сведения последствий к минимуму;

г) обеспечить комфортную работу организации и свести к минимуму финансовые затраты, посредством предотвращения событий, таящих угрозу безопасности и сведения последствий к минимуму.

2. Что **не входит** в основные задачи ИБ:

а) обеспечение невозможности отказа от авторства информационных ресурсов и поддерживающей инфраструктуры;

б) обеспечение доступности информационных ресурсов и поддерживающей инфраструктуры;

в) обеспечение целостности информационных ресурсов и поддерживающей инфраструктуры;

г) обеспечение конфиденциальности информационных ресурсов и поддерживающей инфраструктуры.

3. В случае, когда информация служит «руководством к действию» (Рецептура лекарств, предписанные медицинские процедуры, набор и характеристики комплектующих изделий, ход технологического процесса), в качестве основной задачи ИБ рассматривается обеспечение:

а) Целостности;

б) Конфиденциальности;

в) Доступности;

г) Документируемости.

4. Процессорная модель СУИБ описывается:

а) циклом ПРПД (планирование, реализация, проверка, действие);

б) цикломДеминга;

в) циклом PDCA (Plan-Do-Check-Act);

г) Все вышеуказанное.

5. Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется:

а) форточкой безопасности;

б) дверью угрозы;

в) окном опасности;

г) окном уязвимости.

6. Действие, которое потенциально может привести к нарушению информационной безопасности называется:

а) Источником угрозы;

б) Атакой;

в) Уязвимостью;

г) Угрозой.

7. Попытка реализации действия, которое потенциально может привести к нарушению информационной безопасности, называется:

а) Угрозой;

б) Уязвимостью;

в) Источником угрозы;

г) Атакой.

8. Тот, кто предпринимает попытку реализации действия, которое потенциально может привести к нарушению информационной безопасности, называется:

а) Злоумышленником;

б) Источником угрозы;

в) Источником атаки;

г) Уязвимостью.

9. Слабое место в информационной системе, которое может привести к нарушению безопасности путем реализации некоторой угрозы, называется:

а) Источником угрозы;

б) Окном опасности;

в) Уязвимость;

г) Критичностью реализации угрозы.

10. Критичностью реализации угрозы называется:

а) слабое место в информационной системе, которое может привести к нарушению безопасности путем реализации некоторой угрозы;

б) степень возможности реализации угрозы через данную уязвимость в тех или иных условиях. Указывается в процентах;

в) степень влияния реализации угрозы на ресурс, т.е. как сильно реализация угрозы повлияет на работу ресурса. Задается в процентах. Состоит из критичности реализации угрозы по конфиденциальности, целостности и доступности (ER_c, ER_i, ER_a);

г) действие, которое потенциально может привести к нарушению информационной безопасности.

11. Что не относится к этапам управления рисками:

а) инвентаризация анализируемых объектов;

б) оценка рисков;

в) определение политики ИБ;

г) анализ угроз и их последствий.

12. Для определения основных рисков необходимо следовать следующей цепочке:

а) источник угрозы > фактор (уязвимость) > угроза (действие) > последствия (атака);

б) источник угрозы > угроза (действие) > фактор (уязвимость) > последствия (атака);

в) источник угрозы > фактор (уязвимость) > последствия (атака) > угроза (действие) ;

г) угроза (действие) > фактор (уязвимость) > источник угрозы > последствия (атака).

13. Модель угроз это :

а) документ, определяющий перечень и характеристики основных (актуальных) угроз безопасности и уязвимостей при их обработке в ИС, которые должны учитываться в процессе организации защиты информации, проектирования и разработки систем защиты информации, проведения проверок (контроля) защищенности ИС;

б) совокупность документированных руководящих принципов, правил, процедур и практических приёмов в области ИБ, которые регулируют управление, защиту и распределение ценной информации;

в) комплекс политических, правовых, экономических, социально-культурных и организационных мероприятий государства, направленный на обеспечение конституционного права граждан на доступ к информации;

г) Нет правильного ответа.

14. Угрозы можно классифицировать по:

а) Все перечисленное;

б) по аспекту информационной безопасности (доступность, целостность, конфиденциальность), против которых угрозы направлены в первую очередь;

в) по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);

г) по происхождению и способу осуществления (непреднамеренные/преднамеренные действия природного/техногенного характера).

15. Через уязвимость «Отсутствие разграничения доступа к базе данных и файлам» можно реализовать угрозу :

а) Уязвимость конфиденциальности;

б) Уязвимость целостности;

в) Все указанные уязвимости;

г) Уязвимость доступности.

16. Обеспечения ИБ предприятия включают в себя сочетание следующих уровней:

а) конфиденциальности, целостности и доступности информации;

б) законодательного, научно-технического и физического;

в) реализуемого, гибкого, гарантируемого и универсального;

г) законодательного, административного, процедурного и программно-технического.

17. Политика ИБ предприятия относится к :

а) процедурному уровню;

б) законодательному уровню;

в) административному уровню;

г) программно-техническому уровню.

18. Управление персоналом, физическая защита, поддержание работоспособности, реагирование на нарушения режима безопасности, планирование восстановительных работ, относятся к :

а) процедурному уровню;

б) законодательному уровню;

в) административному уровню;

г) программно-техническому уровню.

19. Идентификация и аутентификация пользователей, управление доступом, протоколирование и аудит, криптография, экранирование и обеспечение высокой доступности:

а) процедурному уровню;

б) законодательному уровню;

в) административному уровню;

г) программно-техническому уровню.

20. Что входит в методы защиты информации:

а) правовые методы защиты;

б) методы защиты от случайных угроз;

в) методы защиты от традиционного шпионажа и диверсий;

г) Все перечисленное, а еще организационные методы защиты, методы защиты от электромагнитных излучений и наводок, методы защиты от несанкционированного доступа, криптографические методы защиты и методы защиты от компьютерных вирусов.

21. ГОСТ Р ИСО/МЭК 27002-2012 это:

а) Международный стандарт качества;

б) Российский стандарт качества;

в) Международный стандарт – Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности;

г) Национальный стандарт РФ – Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

22. ISO/IEC 27002:2005 это:

а) Международный стандарт качества;

б) Российский стандарт качества;

в) Международный стандарт – Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности;

г) Национальный стандарт РФ – Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

23. ГОСТ Р ИСО/МЭК 27007-2014 является:

а) Руководством по обеспечению защиты информационного обмена между подразделениями и организациями;

б) Руководством по реализации системы менеджмента информационной безопасности;

в) Руководством по аудиту систем менеджмента информационной безопасности;

г) Руководством по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1.

24. СТО ВР ИББС-1.0 относится к :

а) Международным стандартам;

б) Национальным стандартам РФ;

в) Отраслевым стандартам РФ;

г) Ведомственным стандартам РФ.

25. В основные этапы разработки системы управления не входит:

а) инвентаризация активов;

б) категорирование активов;

в) оценка защищенности информационной системы;

г) Не правда, все эти этапы входят.

Модуль 2. Особенности реализация СМИБ

1. Категорирование активов компании заключается в:

а) оценки их критичности для обеспечения обороноспособности страны, так как бизнес-процессы вашей компания, не представляют ценности;

б) оценки их стоимости в случае ликвидации предприятия;

в) оценки их критичности, путем проведения референдума на предприятии;

г) оценки их критичности для бизнес-процессов предприятия.

2.Оценка критичности активов производится:

а) Только в условных денежных единицах;

б) Только в долларах США;

в) Только в рублях;

г) Как в денежных единицах, так и в уровнях.

3. Классическая формула оценки информационных рисков:

а) R=D P(V);

б) $E=MC^2$;

в) U=IR;

г) S=VT.

4. К видам гражданско-правовых режимов не относится:

а) правовой режим собственности;

б) режим исключительных прав;

в) режим обязательственного права;

г) Все перечисленные виды относятся к гражданско-правовым режимам.

5. Согласно Указа Президента РФ от 6 марта 1997 г. N 188 « Об утверждении перечня сведений конфиденциального характера», к видам конфиденциальной информации не относится:

а) Сведения, составляющие тайну следствия и судопроизводства, сведения о лицах, в отношении которых в соответствии с федеральными законами от 20 апреля 1995 г. N 45-ФЗ "О государственной защите судей, должностных лиц правоохранительных и контролирующих органов" и от 20 августа 2004 г. N 119-ФЗ "О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства", другими нормативными правовыми актами Российской Федерации принято решение о применении мер государственной защиты, а также сведения о мерах государственной защиты указанных лиц, если законодательством Российской Федерации такие сведения не отнесены к сведениям, составляющим государственную тайну;

б) Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

в) Информация, размещаемая ее обладателями в сети "Интернет" в формате, допускающем автоматизированную обработку без предварительных изменений человеком в целях повторного ее использования;

г) Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

6. Федеральный закон от 27 июля 2006 года №152-ФЗ называется:

а) О персональных данных;

б) О государственной тайне;

в) О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях;

г) Об информации, информационных технологиях и о защите информации.

7. Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными, называется :

а) Оператором;

б) Хранителем;

в) Сервером;

г) Обработчиком.

8. Действия, направленные на раскрытие персональных данных неопределенному кругу лиц называются:

а) Обработкой персональных данных;

б) Блокированием персональных данных;

в) Распространением персональных данных;

г) Хранением персональных данных.

9. Какое утверждение не соответствует требованиям Федерального закона «О персональных данных»:

а) Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

б) Обработке подлежат персональные данные, вне зависимости от целей их обработки;

в) Обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

г) Обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных.

10. Какой случай обработки персональных данных не допускается в соответствии с Федеральным законом «О персональных данных»:

а) Субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

б) Обработка персональных данных о судимости может осуществляться государственными органами или муниципальными органами в пределах полномочий, предоставленных им в соответствии с законодательством Российской Федерации, а также иными лицами в случаях и в порядке, которые определяются в соответствии с федеральными законами, вне зависимости от устранения причины, вследствие которых осуществлялась обработка;

в) Персональные данные сделаны общедоступными субъектом персональных данных;

г) Обработка персональных данных осуществляется в соответствии с Федеральным законом от 25 января 2002 года N 8-ФЗ «О Всероссийской переписи населения».

11. Закон РФ от 21.07.1993 N 5485-1 называется:

а) О персональных данных;

б) О государственной тайне;

в) О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях;

г) Об информации, информационных технологиях и о защите информации.

12. Субъектами правоотношений в соответствии с законом «О государственной тайне» являются:

а) Предприятия, учреждения и организации, независимо от их организационно-правовых форм деятельности и видов собственности;

б) Все указанные лица;

в) Любые юридические лица;

г) Органы государственного управления.

13. Государственная тайна это:

а) Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности государства;

б) Защищаемые государством сведения в области его военной, внешнеполитической, экономической, инженерно-технической, научной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности государства;

в) Защищаемые государством сведения в области его научной, политической, финансовой, разведывательной, контрразведывательной и спортивной, распространение которых может нанести ущерб безопасности государства;

г) Защищаемые государством сведения в области его научно-технической, спортивной, экономической, экологической, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности государства.

14. Засекречивание сведений и их носителей, это:

а) Определение в предусмотренном порядке категории, характеризующей важность информации, возможный ущерб вследствие ее разглашения, степень ограничения доступа к ней и уровень ее охраны государством;

б) Введение в предусмотренном порядке для сведений, составляющих государственную тайну, ограничений на их распространение;

в) Определение в предусмотренном порядке перечня сведений, составляющих государственную тайну;

г) Санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну.

15. Категория, характеризующая важность информации, возможный ущерб вследствие ее разглашения, степень ограничения доступа к ней и уровень ее охраны государством, это :

а) Гриф секретности;

б) Степень секретности;

в) Уровень секретности;

г) Степень конфиденциальности.

16. Улучшениям СУИБ бывают:

а) Условные;

б) Тактические;

в) Косметические;

г) Стратегические.

17. Не бывают аудита:

а) Внешнего;

б) Наружного;

в) Внутреннего;

г) Третьей стороной.

18. Основными способами обработки рисков являются:

а) уменьшение рисков

б) передача рисков

в) избежание рисков

г) принятие рисков

д) ликвидация рисков

19. «Записи» в системе СМИБ:

а) Выберите один или несколько ответов:

б) должны создаваться и поддерживаться в рабочем состоянии

в) должны храниться в архиве всю длительность жизненного цикла предприятия

г) должны обрабатываться ручным способом

д) должны быть защищены и должны управляться

е) должны быть отражены показатели процесса создания и менеджмента СМИБ, и все эпизоды значительных происшествий связанные с СМИБ

20. Что является активом для организации в СМИБ?

а) Выберите один или несколько ответов:

б) Квалификация персонала

в) Коллективные мероприятия

г) Программное обеспечение

д) Имидж

е) Корпоративная политика

21. Процесс планирования деятельности по управлению рисками ИБ состоит из:

а) Выберите один ответ:

б) Идентификации, консультирования, получения санкций

в) Анализа, внедрения, консультирования, оценки

г) Создания заявки, согласования, внедрения, консультирования

д) Идентификации, анализа, получения санкций, внедрения

22. Кто готовит План проведения аудита?

а) Выберите один ответ:

б) Экспертный совет аудиторов

в) Ведущий аудитор

г) Специалист ФСТЭК

д) Исполнитель

е) Заказчик

23. Для чего создается периметр безопасности?

а) Выберите один ответ:

б) Для создания системы СКУД

в) Для защиты участков, содержащих информацию и средства ее обработки

г) Для защиты всей контрольной зоны

д) Для защиты сейфа, в котором хранятся основные и резервные ключевые носители

е) Для защиты средств обработки информации

24. Количество этапов внедрения системы ИБ:

Выберите один ответ:

а) 6

б) 8

в) 4

г) 3

д) 5

е) 7

25. «Информация» по ГОСТ 27000 это:

а) совокупность содержащихся в базах данных сведений

б) сведения (сообщения, данные) воспроизводимые различными системами

в) актив, важный для бизнеса

г) сведения (сообщения, данные) независимо от формы их представления

Критерии оценки тестовых заданий

Структура работы	Критерии оценки	Распределение баллов
Один вопрос теста (25 вопросов в варианте) Модуль 1 Модуль 2	Неправильный ответ / Правильный ответ	 0,4 0,4

Практические работы

Цель проведения практических работ – практическое освоение материала дисциплины.

Темы практических работ

1. Разработка нормативных документов организации на основе стандартов ISO/IEC 27035:2011 - управление инцидентами ИБ и ISO/IEC 27037 - руководство по идентификации, сбору и/или получению и обеспечению сохранности свидетельств, представленных в электронной форме.
2. Метод оценки рисков на основе модели угроз и уязвимостей.
3. Расчет рисков по угрозе информационной безопасности. Методика оценки рисков информационной безопасности компании DigitalSecurity.
4. Использование средства полного анализа рисков экспертной системы «Авангард».
5. Журналы регистрации событий на примере ОС Windows.
6. Инструментальные средства проверки ИБ.
7. Виды проверок СУИБ.
8. Возможности системы управления событиями информационной безопасности (SIEM - системы).

Практическая работа № 1

Модуль 1. Создание СУИБ на предприятии.

Тема: Разработка нормативных документов организации на основе стандарта ГОСТ Р ИСО/МЭК 27037-2014 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме».

Цель: Практическое ознакомление с положением о порядке выявления и реагирования на инциденты информационной безопасности.

Задание: Разработать типовое положение о порядке выявления и реагирования на инциденты информационной безопасности.

Порядок выполнения:

1. Ознакомиться с ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности, ISO/IEC 27035:2011 - управление инцидентами ИБ и ISO/IEC 27037 - Руководство по идентификации, сбору и/или получению и обеспечению сохранности свидетельств, представленных в электронной форме.
2. Ознакомиться типовым Положением о реагирования на инциденты информационной безопасности.
3. Назовите основные разделы Положения о реагирования на инциденты информационной безопасности.
4. Ответить на контрольные вопросы:
   a) Назовите этапы менеджмента инцидентов ИБ.
   b) Какие мероприятия включает в себя этап «Планирование и подготовка»?
   c) Какие процессы необходимо осуществить при использовании системы менеджмента инцидентов ИБ?
   d) Какие действия по анализу состояния ИБ необходимо предпринять после разрешения/закрытия инцидентов ИБ?
   e) В чем заключаются преимущества структурного подхода менеджмента инцидентов информационной безопасности?
5. Защита практической работы. Проводится в форме устного опроса после выполнения работы.

Критерии оценки практической работы

Структура работы	Критерии оценки	Распределение баллов
Одно практическое задание Модуль 1 Модуль 2	работа выполнена с ошибками и не получены ответы на все контрольные вопросы/ работа выполнена, но не получены ответы на все контрольные вопросы/ работа выполнена и	 0/4/8 0/4/8

	получены ответы на все контрольные вопросы	

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература

1. Шаньгин, В.Ф. Информационная безопасность [Электронный ресурс] : учебное пособие / В.Ф. Шаньгин. — Электрон. дан. — Москва : ДМК Пресс, 2014. — 702 с. — Режим доступа: https://e.lanbook.com/book/50578. — Загл. с экрана.

Дополнительная литература

2. Шаньгин, В.Ф. Защита компьютерной информации [Электронный ресурс] : учебное пособие / В.Ф. Шаньгин. — Электрон. дан. — Москва : ДМК Пресс, 2010. — 544 с. — Режим доступа: https://e.lanbook.com/book/1122. — Загл. с экрана.
3. Малюк, А.А. Защита информации в информационном обществе : учебное пособие / А.А. Малюк. - Москва : Горячая линия-Телеком, 2015. - 229 с. : ил., схем., табл. - Библиогр. в кн. - ISBN 978-5-9912-0481-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=457170
4. 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

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 «ЭБ БашГУ» - https://elib.bashedu.ru
3. Электронная библиотечная система БашГУ – www.bashlib.ru
4. Электронная библиотечная система издательства «Лань» - https://e.lanbook.com
5. Антиплагиат.ВУЗ. Договор № 81 от 27.04.2018 г. Срок действия лицензии до 04.05.2019 г., договор № 1104 от 18.04.2019 г. Срок действия лицензии до 04.05.2020 г
6. Банк нормативно-правовых актов РФ Министерства юстиции РФ - http://zakon.scli.ru/ru/legal_texts/index.php
7. Справочная правовая система Консультант Плюс. Договор №31705775411 от 07.12.2017 г. http://www.consultant-plus.ru
8. Национальные стандарты РФ в области информационной безопасности: http://www.iso27000.ru/standarty/gost-r-nacionalnye-standarty-rossiiskoi-federacii-v-oblasti-zaschity-informacii
9. Нормативные документы и материалы сайта ФСТЭК России (Федеральной службы по техническому и экспортному контролю России): https://fstec.ru/ Раздел «Национальные старты информационной безопасности» (https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/113-gosudarstvennye-standarty/377-gosudarstvennye-standarty)

Государственные информационно-правовые системы:

1. Научный центр правовой информации при министерстве Юстиций РФ - http://www.scli.ru
2. Официальный интернет-портал правовой информации - http://pravo.gov.ru
3. Информационно-правовая система «Законодательство России» - http://pravo.fso.gov.ru
4. Модуль «Документы - Президент России» - http://www.kremlin.ru/acts
5. Банк документов, подписанных Президентом России - http://kremlin.ru/acts/bank
6. База данных «Федеральные законы» - http://graph.garant.ru:8080/SESSION/PILOT/main.htm
7. Автоматизированная система обеспечения законодательной деятельности государственной думы (законопроекты и законодательные инициативы) - http://asozd.duma.gov.ru/
8. База данных «Издания по общественным и гуманитарным наукам» (на платформе EastView) - Ссылка http://www.ebiblioteka.ru(вход из сети вуза без регистрации).
9. Банк данных "Библиотека копий официальных публикаций правовых актов» при ассоциации юристов России - http://alrf.consultant.ru/
10. Банк данных "Копии правовых актов: Российская Федерация» - http://giod.consultant.ru/
11. Банк данных "Нормативно-правовые акты Федерального Собрания Российской Федерации - http://duma.consultant.ru/

Другие профессиональные базы данных и информационно-справочные системы:

1. Электронная база данных диссертаций РГБ (авторизованный доступ по паролю в сети вуза) – Ссылка: http://dvs.rsl.ru
2. База данных «Вестники Московского университета» (на платформе EastView) (вход без регистрации). - Ссылка http://www.ebiblioteka.ru/browse/udb/12.
3. AnnualReviews – обзор журналов по общественно-научной тематике и др. – доступ из сети вуза. – Ссылка: http://www.annualreviews.org/
4. Computers & Applied Sciences Complete (EBSCO) - доступвсетивуза, языканглийский. - Ссылка: http://search.ebscohost.com/
5. SCOPUS - наукометрическая, библиографическая и реферативная база данных издательской корпорации Elsevier. Язык английский, вход после регистрации или из сети вуза. – Ссылка: http://www.scopus.com/
6. TaylorandFrancis – База полнотекстовых научных журналов, книг. Язык английский. – доступ из сети вуза. – Ссылка: http://www.tandf
7. WebofScience - наукометрическая, библиографическая и реферативная база данных издательской корпорации ThomsonReuters. Язык английский, вход после регистрации или из сети вуза. – Ссылка: http://apps.webofknowledge.com/
8. Wiley - Полнотекстовая база данных статей из 1400 журналов издательства Wiley по всем отраслям знаний. Язык английский. Доступ из сети вуза без регистрации. – Ссылка: http://onlinelibrary.wiley.com/
9. Сайт по информационной безопасности: http://securitypolicy.ru/; его раздел: «Документы, стандарты и методики по информационной безопасности»: http://securitypolicy.ru/
10. Докипедия: http://dokipedia.ru
11. Словари и энциклопедии On-Line- http://www.dic.academic.ru

Программноеобеспечение

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. Лицензиибессрочные.
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).GNUGeneralPublicLicense. Лицензии бессрочные.

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

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
1	2	3
1. ***учебная аудитория для проведения занятий лекционного типа:*** аудитория № 403 (гуманитарный корпус),аудитория № 405 (гуманитарный корпус), аудитория № 413 (гуманитарный корпус),аудитория № 415 (гуманитарный корпус),аудитория № 416 (гуманитарный корпус),аудитория № 418 (гуманитарный корпус),аудитория № 419 (гуманитарный корпус),аудитория № 515 (гуманитарный корпус), аудитория № 516 (гуманитарный корпус). **2.** ***учебная аудитория для проведения занятий семинарского типа:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус). **3.** ***учебная аудитория для курсового проектирования (выполнения курсовых работ):***аудитория № 613(гуманитарный корпус). **4.** ***учебная аудитория для проведения групповых и индивидуальных консультаций:***аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **5.** ***учебная аудитория для текущего контроля и промежуточной***	Лекции, практические занятия, текущий контроль, промежуточная аттестация, экзамен	**Аудитория № 403** Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный ClassicNorma 244*183 – 1 шт.,учебно-наглядные пособия. **Аудитория № 405** Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром PrometheanActivBoard 387 RPOMOUNTEST -1 шт., Ком-ер встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H – 1 шт. , Мультимедиа-проектор PanasonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт. , Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт. **Аудитория № 413** Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт APAPT MA1225 – 1 шт. **Аудитория № 415** Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт APAPT MA1225 – 1 шт. **Аудитория № 416** Учебная мебель, доска, проектор Optoma Ex542 i-1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 418** Учебная мебель, доска, Экран настенный LumienMasterPikture 153*203 MatteWhiteFiberClas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт. **Аудитория № 419** Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 515** Учебная мебель, доска, терминал видео конференц-связи LifeSizeIcon 600-камера, интер-ая система со встроенным короткофокусным проектором PrometheanActivBoard 387 RPO MOUNT EST, профес-сиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса

аттестации:аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **6.*помещения для самостоятельной работы:***аудитория № 613 (гуманитарный корпус), читальный зал библиотеки аудитория 402 (гуманитарный корпус).		HDMI CMPRO 4H4H, интер-ая напольная кафедра докладчика, ком-ер встраиваемый в кафедру IN-TEL Core i3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/Thermaltake VL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром. **Аудитория № 516** Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран. **Аудитория № 509** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 608** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 609** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 610** Учебная мебель, доска, учебно-наглядные пособия, LED Телевизор TCLL55P6 USBLACK – 1 шт., кронштейн для телевизора NBP 5 – 1 шт., Кабель HDMI (m)-HDH(m)ver14,10м. **Аудитория № 613** Учебная мебель, доска, моноблок стационарный – 15 шт. **Компьютерный класс аудитория № 420** Учебная мебель, моноблоки стационарные 15 шт. **Компьютерный класс аудитория № 404** Учебная мебель, компьютеры -15 штук. **Аудитория 402 читальный зал библиотеки** Учебная мебель, доска, компьютеры в комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура, мышь, стеллажи, шкафы картотечные, комбинированные. **Аудитория № 523** Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт.

Приложение № 1

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

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины **Основы управления информационной безопасностью** на 8 семестр
___очная_ф/о___

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	3 ЗЕТ / 108 часа
Учебных часов на контактную работу с преподавателем:	44,2
лекций	22
практических/ семинарских	22
лабораторных	–
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0,2
из них, предусмотренные на выполнение курсовой работы / курсового проекта	–
Учебных часов на самостоятельную работу обучающихся (СР)	63,8
из них, предусмотренные на выполнение курсовой работы / курсового проекта	–
Учебных часов на подготовку к зачету (Контроль)	–

Форма контроля
Зачет8 семестр

Семестр 8

№	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР / СЕМ	ЛР	СР		
1	2	3	4	5	6	8	9
1	Модуль 1. Создание СУИБ на предприятии. Тема: Стандартизация систем и процессов управления информационной безопасностью. Серия стандартов ISO/IEC 27000 «Информационные технологии. Методы обеспечения безопасности». ISO/IEC 27000:2009 -СУИБ: определения и основные принципы. ISO/IEC 27001:2005 и ГОСТ Р ИСО/МЭК 27001-2006 -Требования к СУИБ. ISO/IEC 27002:2005 и ГОСТ Р ИСО/МЭК 17799-2005 - практические правила управления ИБ. ISO/IEC 27003:2010 – руководство по внедрению СУИБ. ISO/IEC 27004:2009 и ГОСТ Р ИСО/МЭК 27004-2011 - оценка функционирования СУИБ. ISO/IEC 27005:2011 и ГОСТ Р ИСО/МЭК 27005-2010 - управление рисками ИБ. ISO/IEC 27006:2011 и ГОСТ Р ИСО/МЭК 27006-2008 - требования к органам, осуществляющим аудит и сертификацию СУИБ. ISO/IEC 27007:2011 и ISO/IEC 27008:2011 - руководства по аудиту СУИБ и средств управления ИБ, реализованных в СУИБ. Тема: Серия стандартов ISO/IEC 27011:2008 - руководство по управлению ИБ для	4 4	4 4		8 8	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	лабораторная работа, тест

	телекоммуникационных компаний на основе ISO/IEC 27002. ISO/IEC 27013 -руководство по интегрированному внедрению стандартов ISO/IEC 20000 и 27001. ISO/IEC 27014 - инфраструктура руководства ИБ. ISO/IEC 27015 - руководство но управлению ИБ для финансовых сервисов. ISO/IEC 27031:2011 - руководство по готовности информационных и телекоммуникационных технологий для обеспечения непрерывности бизнеса. ISO/IEC 27033 - управление безопасностью сетей.						
	Тема: Серия стандартов ISO/IEC 27035:2011 - управление инцидентами ИБ. ISO/IEC 27037 - руководство по идентификации, сбору и/или получению и обеспечению сохранности свидетельств, представленных в электронной форме. Стандарты на отдельные процессы управления ИБ и оценку безопасности ИТ. ISO/IEC 13335 - методы и средства обеспечения безопасности информационных технологий. ISO/IEC 15408 и ISO/IEC 18045:2008 - общие критерии и методология оценки безопасности информационных технологий. ISO 19011:2011 и ГОСТ Р ИСО 19011-2003 - рекомендации по аудиту систем менеджмента. BS 25999 и ГОСТ Р 53647 – управление непрерывностью бизнеса.	4	4		8		
	Тема: Отраслевые стандарты в области управления ИБ - стандарты банковской системы Российской Федерации. СТО БР ИББС-1.0 - общие положения в области обеспечения ИБ организаций банковской системы Российской Федерации. СТО БР ИББС-1.1- аудит ИБ. СТО БР ИББС-1.2 - методика оценки соответствия ИБ организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0.	2	2		8		

2	Модуль 2. Особенности реализация СМИБ. Тема: Методика определения угроз безопасности информации в информационных системах. Оценка возможностей нарушителей по реализации угроз безопасности информации. Типы нарушителя. Мотивация нарушителя. Виды и потенциал нарушителя. Возможные способы реализации угроз безопасности информации. Тема: Определение актуальных угроз безопасности информации в информационной системе. Оценка вероятности (возможности) реализации угрозы безопасности информации. Показатели, характеризующие проектную защищенность информационной системы. Оценка степени возможного ущерба от реализации угрозы безопасности информации. Возможные негативные последствия от нарушения конфиденциальности, целостности, доступности информации. Характеристика степени ущерба. Тема: Определение актуальности угрозы безопасности информации. Рекомендации по формированию экспертной группы и проведению экспертной оценки при определении угроз безопасности информации. Структура модели угроз безопасности информации. Определение потенциала нарушителя, необходимого для реализации угрозы безопасности информации в информационной системе.	2 2 2	2 2 2		8 8 8	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	лабораторная работа, тест

	Тема: Инструментальные средства проверки ИБ. Национальный стандарт Российской Федерации «Информационная технология. Методы и средства обеспечения безопасности. Рекомендации для аудиторов в отношении мер и средств контроля и управления информационной безопасностью.» Тестирование «вслепую». «Дважды слепое» тестирование. Тестирование методом «серого ящика». Тестирование методом «двойного серого ящика». Тестирование методом «тандема». Реверсивное тестирование. Системы анализа защищенности. Системы обнаружения вторжения. Системы предотвращения вторжения.	2	2		7,8		
Всего часов		22	22	–	63,8		