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

Актуализировано:
на заседании кафедры
протокол № 10 от «07» июня 2018 г.

Зав. кафедрой _____/А.С.Исмагилова

Согласовано:
Председатель УМК института

_____/ Р.А. Гильмутдинова

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина
Информационная безопасность

Вариативная часть

Направление подготовки
38.03.06 Торговое дело

Направленность (профиль) подготовки
Государственные и муниципальные закупки

Квалификация
Бакалавр

Разработчик (составитель) к.б.н.	_____/Ф.Т.Байрушин

Для приема: 2016 г.

Уфа 2018 г.

Составитель: Ф.Т. Байрушин

Рабочая программа дисциплины актуализирована на заседании кафедры государственного управления протокол № 12 от«07»июня 2018г.

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 спланируемыми результатами освоения образовательной программы

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

Результаты обучения		Формируемая компетенция (с указанием кода)	Примечание
Знания	Знать основные понятия и задачи в области информационно-коммуникационных технологий для решения стандартных задач профессиональной деятельности	ОПК-1: способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	
	Знать нормативные документы для решения профессиональных проблем	ОПК-3: умением пользоваться нормативными документами в своей профессиональной деятельности, готовностью к соблюдению действующего законодательства и требований нормативных документов.	
	Знать порядок выбора деловых партнеров, проведения деловых переговоров, заключения договоров и контроля их выполнения	ПК-6: способность выбирать деловых партнеров, проводить с ними деловые переговоры, заключать договоры и контролировать их выполнение.	
Умения	Уметь работать с офисными программами, проводить поиск информации, осуществлять сбор и анализ данных, необходимых для проведения конкретных расчетов; обрабатывать массивы данных в соответствии с поставленной задачей.	ОПК-1: способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	
	Умеет пользоваться нормативными документамипри решении профессиональных проблем.	ОПК-3: умением пользоваться нормативными документами в своей профессиональной деятельности, готовностью к соблюдению действующего законодательства и требований	

		нормативных документов.	
	Уметь выбирать деловых партнеров, проводить с ними деловые переговоры, заключать договоры и контролировать их выполнение	ПК-6: способность выбирать деловых партнеров, проводить с ними деловые переговоры, заключать договоры и контролировать их выполнение.	
Владения (навыки / опыт деятельности)	Владеть информационно-коммуникационными технологиями с учетом основных требований информационной безопасности.	ОПК-1: способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	
	Владеть навыками соблюдения действующего законодательства и требований нормативных документов в профессиональной деятельности	ОПК-3: умением пользоваться нормативными документами в своей профессиональной деятельности, готовностью к соблюдению действующего законодательства и требований нормативных документов.	
	Владеть способностью выбирать деловых партнеров, проводить с ними деловые переговоры, заключать договоры и контролировать их выполнение	ПК-6: способность выбирать деловых партнеров, проводить с ними деловые переговоры, заключать договоры и контролировать их выполнение.	

2. Цель и место дисциплины в структуре образовательной программы

Цель изучения дисциплины: формирование у бакалавров целостного представления об информационной безопасности.

Дисциплина «Информационная безопасность» относится к дисциплинам вариативной части профессионального цикла.

Дисциплина изучается на 2 курсе.

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 с указанием этапов их формирования в процессе освоения образовательной программы. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

ОПК-1: способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
Первый этап (уровень)	Знаетосновные понятия и задачи в области информационно-коммуникационных технологий для решения стандартных задач профессиональной деятельности	Не знает или имеет фрагментарных знаний об основных понятиях в области информационно-коммуникационных технологий для решения стандартных задач профессиональной деятельности	В целом основные понятия и задачи в области информационно-коммуникационных технологий для решения стандартных задач профессиональной деятельности
Второй этап (уровень)	Уметьработать с офисными программами, проводить поиск информации, осуществлять сбор и анализ данных, необходимых для проведения конкретных расчетов; обрабатывать массивы данных в соответствии с поставленной задачей.	Не умеет или не способенпроводить поиск информации, осуществлять сбор и анализ данных, необходимых для проведения конкретных расчетов; обрабатывать массивы данных в соответствии с поставленной задачей	В целом уверенно работает с офисными программами, проводить поиск информации, осуществлять сбор и анализ данных, необходимых для проведения конкретных расчетов; обрабатывать массивы данных в соответствии с поставленной задачей.
Третий этап (уровень)	Владеть способностью выбора и использования информационно-коммуникационны	Не способен выбрать необходимые для работы информационно-коммуникационные технологии	Владеет способностью выбора и использования информационно-коммуникационными технологиями с учетом основных требований

	ми технологиями с учетом основных требований информационной безопасности.		информационной безопасности.

ОПК-3: умением пользоваться нормативными документами в своей профессиональной деятельности, готовностью к соблюдению действующего законодательства и требований нормативных документов**.**

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
Первый этап (уровень)	Знает нормативные документы для решения профессиональных проблем	Не знает или имеет фрагментарных знаний о нормативных документов для решения профессиональных проблем	Демонстрирует целостные знания нормативных документов для решения профессиональных проблем.
Второй этап (уровень)	Умеет пользоваться нормативными документами при решении профессиональных проблем.	Не умеет или не способеннормативными документами при решении профессиональных проблем	Умеет выбирать и применять нормативные документы при решении профессиональных проблем
Третий этап (уровень)	Владеть : навыками соблюдения действующего законодательства и требований нормативных документов в профессиональной деятельности	Не способен выбрать о нормативные документы действующего законодательства и требований профессиональной деятельности	Способен выбирать и применять оптимальные нормативные документы; владеет действующим законодательством при решении профессиональных проблем.

ПК-6: способность выбирать деловых партнеров, проводить с ними деловые переговоры, заключать договоры и контролировать их выполнение**.**

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено

	заданного уровня освоения компетенций)		
Первый этап (уровень)	Знает порядок выбора деловых партнеров, проведения деловых переговоров, заключения договоров и контроля их выполнения	Не знает или имеет фрагментарные знания по выбору деловых партнеров, проведению деловых переговоров, заключению договоров и контролю их выполнения	Демонстрирует систематизированные знания о выборе деловых партнеров, проведении деловых переговоров, заключении договоров и контроле их выполнения
Второй этап (уровень)	Умеет выбирать деловых партнеров, проводить с ними деловые переговоры, заключать договоры и контролировать их выполнение	Демонстрирует фрагментарные умения выбора деловых партнеров, проведения с ними деловых переговоров, заключения договоров и контроля их выполнения	Демонстрирует сформированное умениевыбирать деловых партнеров, проводить с ними деловые переговоры, заключать договоры и контролировать их выполнение
Третий этап (уровень)	Владеть способностью выбирать деловых партнеров, проводить с ними деловые переговоры, заключать договоры и контролировать их выполнение	Не способен выбирать деловых партнеров, проводить с ними деловые переговоры, заключать договоры и контролировать их выполнение	Успешное и систематическое применение способности выбирать деловых партнеров, проводить деловые переговоры, заключать договоры и контролировать ихвыполнение

Студенты заочной формы обучения сдают зачет в форме тестовых заданий, которые составляются по вопросам зачета. Порог прохождения итогового тестирования – 60% правильных ответов.

–«Зачтено» выставляется студенту, если 15 ответов правильных;

–«Не зачтено» выставляется студенту, если 10 и более ответовнеправильных.

Если обучающийся не преодолел установленный порог, то он направляется на пересдачу дисциплины.

4.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций

Этапы освоения	Результаты обучения	Компетенция	Оценочные средства
Знает	основные понятия и задачи в области информационно-коммуникационных технологий для решения стандартных задач профессиональной деятельности	**ОПК-1:** способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	устный индивидуальный опрос, контрольная работа,
	нормативные документы для решения профессиональных проблем	**ОПК-3:** умением пользоваться нормативными документами в своей профессиональной деятельности, готовностью к соблюдению действующего законодательства и требований нормативных документов**.**	устный индивидуальный опрос, контрольная работа,
	порядок выбора деловых партнеров, проведения деловых переговоров, заключения договоров и контроля их выполнения	**ПК-6:** способность выбирать деловых партнеров, проводить с ними деловые переговоры, заключать договоры и контролировать их выполнение**.**	устный индивидуальный опрос, контрольная работа,
2-й этап Умеет	работать с офисными программами, проводить поиск информации, осуществлять сбор и анализ данных, необходимых для проведения конкретных расчетов; обрабатывать массивы данных в соответствии с поставленной задачей.	**ОПК-1:** способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных	Тестирование, контрольная работа

		технологий и с учетом основных требований информационной безопасности.	
	пользоваться нормативными документамипри решении профессиональных проблем.	**ОПК-3:** умением пользоваться нормативными документами в своей профессиональной деятельности, готовностью к соблюдению действующего законодательства и требований нормативных документов**.**	Тестирование, контрольная работа
	выбирать деловых партнеров, проводить с ними деловые переговоры, заключать договоры и контролировать их выполнение	**ПК-6:** способность выбирать деловых партнеров, проводить с ними деловые переговоры, заключать договоры и контролировать их выполнение**.**	Тестирование, контрольная работа
3-й этап Владеть	информационно-коммуникационными технологиями с учетом основных требований информационной безопасности.	**ОПК-1:** способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Тестирование, контрольная работа
	навыками соблюдения действующего законодательства и требований нормативных документов в профессиональной деятельности	**ОПК-3:** умением пользоваться нормативными документами в своей профессиональной деятельности, готовностью к соблюдению	Тестирование, контрольная работа

		действующего законодательства и требований нормативных документов**.**	
	способностью выбирать деловых партнеров, проводить с ними деловые переговоры, заключать договоры и контролировать их выполнение	**ПК-6:** способность выбирать деловых партнеров, проводить с ними деловые переговоры, заключать договоры и контролировать их выполнение**.**	Тестирование, контрольная работа

Устный индивидуальный опрос

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

Студент излагает содержание вопроса изученной темы.

1. Информационные процессы в сфере государственных закупок.
2. Задача устойчивого развития информационной сферы государственных закупок.
3. Виды защищаемой информации в сфере государственных закупок
4. Состояние и перспективы информатизации сферы тендерных закупок.
5. Обеспечение информационной безопасности организации тендерных закупок.
6. Применение Федерального Закона РФ «Об информации, информационных технологиях и защите информации» в сфере государственных закупок.
7. Профессиональные тайны в сфере государственных закупок, их виды.
8. Объекты коммерческой тайны на предприятии.
9. Информационные угрозы для государства, их виды и причины возникновения
10. Информационные угрозы для компании.
11. Информационные угрозы для личности (физического лица).
12. Действия и события, нарушающие информационную безопасность.
13. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз.
14. Способы воздействия информационных угроз на объекты.
15. Внешние и внутренние субъекты информационных угроз.
16. Компьютерные преступления и их классификация.
17. Исторические аспекты компьютерных преступлений и современность.
18. Субъекты и причины совершения компьютерных преступлений.
19. Вредоносные программы, их виды.
20. История компьютерных вирусов и современность.
21. Государственное регулирование информационной безопасности.
22. Деятельность международных организаций в сфере информационной безопасности.
23. Нормативно-правовые аспекты в области информационной безопасности в Российской Федерации.
24. Доктрина информационной безопасности России.
25. Федеральные законы по ИБ в РФ
27. Политика безопасности и ее принципы.
28. Фрагментарный и системный подход к защите информации.

29. Методы и средства защиты информации.
30. Организационное обеспечение ИБ.

Студент излагает содержание вопроса изученной темы, в соответствии с тематикой практических занятий. Критерии и методика оценивания:

- «отлично» выставляется студенту, если точно используется специализированная терминология, показано уверенное владение нормативной базой;
- «хорошо» выставляется студенту, допущены один-два недочета при освещении основного содержания ответа, нет определенной логической последовательности, неточно используется специализированная терминология;
- «удовлетворительно» выставляется студенту, нет общего понимания вопроса, имеются затруднения или допущены ошибки в определении понятий, использовании терминологии;
- «неудовлетворительно»ставится при незнании и непонимании вопроса, при полном отсутствии ответа на дополнительный вопрос.

Типовые тесты

Тестирование студентов проводится с целью осуществления текущего контроля. В каждом варианте 25 вопросов закрытого типа.

Вариант 1

1. Защита информации это:
   1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
   2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
   3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
   4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
   5. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

2. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:
   1. активный перехват;
   2. пассивный перехват;
   3. аудиоперехват;
   4. видеоперехват;
   5. просмотр мусора.

3. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:
   1. активный перехват;
   2. пассивный перехват;
   3. аудиоперехват;
   4. видеоперехват;

4. Под replay-атакой понимается:

1. модификация передаваемого сообщения
2. повторное использование переданного ранее сообщения
3. невозможность получения сервиса законным пользователем

5. Уровень секретности - это
1. ответственность за модификацию и НСД информации
2. административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю конкретной секретной информации, регламентируемой специальным документом, с учетом государственных, военно-стратегических, коммерческих, служебных или частных интересов

6. Что такое несанкционированный доступ (нсд)?
1. Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа
2.Создание резервных копий в организации
3. Правила и положения, выработанные в организации для обхода парольной защиты
4. Вход в систему без согласования с руководителем организации

6. К посторонним лицам нарушителям информационной безопасностиотносится:
а) персонал, обслуживающий технические средства;
б) технический персонал, обслуживающий здание;
в) сотрудники службы безопасности.
г) представители конкурирующих организаций.

8. Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом?
а) Безопасная OECD
2. ISO\IEC
3. OECD
4. CPTED

9. Перехват, который осуществляется путем использования оптической техники называется:
а) активный перехват;
б) пассивный перехват;
в) аудиоперехват;
г) видеоперехват;
д) просмотр мусора.

10. К внутренним нарушителям информационной безопасности относится:
а) любые лица, находящиеся внутри контролируемой территории;
б) персонал, обслуживающий технические средства.
в) сотрудники отделов разработки и сопровождения ПО;
г) технический персонал, обслуживающий здание

11. Собственником информации не может быть:
а) государство;
б) юридическое лицо;
в) группа физических лиц;
г) физическое лицо;
д) ответы а – г правильны;
е) нет правильного ответа.

12. Терминология в сфере защиты информации регулируется
а) ГОСТ Р 6.30 – 2003
б) ГОСТ 51141 – 98
в) ГОСТ 50922 – 96
г) Гражданским кодексом.

13. Заранее намеченный результат защиты информации – это
а) замысел защиты информации;
б) цель защиты информации;
в) уровень эффективности защиты информации.

14.Кто является основным ответственным за определение уровня классификации информации?
а) Руководитель среднего звена
б) Высшее руководство
в) Владелец
г) Пользователь

15.Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
Варианты ответа:
а) Сотрудники
б) Хакеры
в) Атакующие
г) Контрагенты (лица, работающие по договору)

16.Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
Варианты ответа:
а) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
б) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
в) Улучшить контроль за безопасностью этой информации
г) Снизить уровень классификации этой информации

17.Что самое главное должно продумать руководство при классификации данных?
Варианты ответа:
а) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
б) Необходимый уровень доступности, целостности и конфиденциальности
в) Оценить уровень риска и отменить контрмеры
г) Управление доступом, которое должно защищать данные

18.Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
а) Владельцы данных
б) Пользователи
в) Администраторы
г) Руководство

19.Что такое процедура?
а) Правила использования программного и аппаратного обеспечения в компании
б) Пошаговая инструкция по выполнению задачи
в) Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

г) Обязательные действия

20.Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

Варианты ответа:

а) Поддержка высшего руководства
б) Эффективные защитные меры и методы их внедрения
в) Актуальные и адекватные политики и процедуры безопасности
г) Проведение тренингов по безопасности для всех сотрудников

21.Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

Варианты ответа:

а) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
б) Когда риски не могут быть приняты во внимание по политическим соображениям
в) Когда необходимые защитные меры слишком сложны
г) Когда стоимость контрмер превышает ценность актива и потенциальные потери

22.Что такое политики безопасности?

а) Пошаговые инструкции по выполнению задач безопасности
б) Общие руководящие требования по достижению определенного уровня безопасности
в) Широкие, высокоуровневые заявления руководства
г) Детализированные документы по обработке инцидентов безопасности

23.Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

а) Анализ рисков
б) Анализ затрат / выгоды
в) Результаты ALE
г) Выявление уязвимостей и угроз, являющихся причиной риска

24.Что лучше всего описывает цель расчета ALE?

а) Количественно оценить уровень безопасности среды
б) Оценить возможные потери для каждой контрмеры
в) Количественно оценить затраты / выгоды
г) Оценить потенциальные потери от угрозы в год

25.Тактическое планирование – это:

а) Среднесрочное планирование
б) Долгосрочное планирование
в) Ежедневное планирование
г) Планирование на 6 месяцев

Вариант 2

1.Что является определением воздействия (exposure) на безопасность?

а) Нечто, приводящее к ущербу от угрозы
б) Любая потенциальная опасность для информации или систем
в) Любой недостаток или отсутствие информационной безопасности
г) Потенциальные потери от угрозы

2.Эффективная программа безопасности требует сбалансированного применения:

а) Технических и нетехнических методов
б) Контрмер и защитных механизмов
в) Физической безопасности и технических средств защиты
г) Процедур безопасности и шифрования

3.Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

а) Внедрение управления механизмами безопасности
б) Классификацию данных после внедрения механизмов безопасности

в) Уровень доверия, обеспечиваемый механизмом безопасности
г) Соотношение затрат / выгод

4.Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?

а) Только военные имеют настоящую безопасность
б) Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности
в) Военным требуется больший уровень безопасности, т.к. их риски существенно выше
г) Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

5.Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?

а) Поддержка
б) Выполнение анализа рисков
в) Определение цели и границ
г) Делегирование полномочий

6.Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?

а) Чтобы убедиться, что проводится справедливая оценка
б) Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
в) Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа
г) Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

7.Что является наилучшим описанием количественного анализа рисков?

а) Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности
б) Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков
в) Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков
г) Метод, основанный на суждениях и интуиции

8.Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств?

а) Стандарты
б) Должный процесс (Dueprocess)
в) Должная забота (Duecare)
г) Снижение обязательств

9.Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?

а) Список стандартов, процедур и политик для разработки программы безопасности
б) Текущая версия ISO 17799
в) Структура, которая была разработана для снижения внутреннего мошенничества в компаниях
г) Открытый стандарт, определяющий цели контроля

10.Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод:

а) гаммирования;
б) подстановки;
в) кодирования;

г) перестановки;
д) аналитических преобразований.

11.Защита информации от утечки это деятельность по предотвращению:

а) воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;

б) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;

в) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;

г) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

12.Защита информации это:

а) процесс сбора, накопления, обработки, хранения, распределения и поиска информации;

б) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;

в) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;

г) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;

д) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

13.Естественные угрозы безопасности информации вызваны:

а) деятельностью человека;

б) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;

в) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;

г) корыстными устремлениями злоумышленников;

д) ошибками при действиях персонала.

14. Искусственные угрозы безопасности информации вызваны:

а) деятельностью человека;

б) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;

в) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;

г) корыстными устремлениями злоумышленников;

д) ошибками при действиях персонала.

15. К основным непреднамеренным искусственным угрозам АСОИ относится:

а) физическое разрушение системы путем взрыва, поджога и т.п.;

б) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;

в) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;

г) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

16.К посторонним лицам нарушителям информационной безопасности относится:

а) персонал, обслуживающий технические средства;

б) технический персонал, обслуживающий здание;

в) представители конкурирующих организаций.
г) лица, нарушившие пропускной режим;

17.Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п:
а) черный пиар;
б) фишинг;
в) нигерийские письма;
г) источник слухов;

18.Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:
а) черный пиар;
б) фишинг;
в) нигерийские письма;
г) источник слухов;

19.Субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и (или) собственником информации – это
а) носитель информации
б) собственник информации
в) владелец информации
д) пользователь информации

20. Содержание и порядок действий, направленных на обеспечение защиты информации – это
а) мероприятие по защите информации;
б) система защиты информации
в) организация защиты информации.

21. В настоящее время по степени конфиденциальности можно классифицировать информацию,
а) составляющую коммерческую тайну;
б) составляющую государственную тайну;
в) составляющую служебную тайну;
г) составляющую профессиональную тайну.

22. В каких областях деятельности может быть государственная тайна
а) военной
б) образовательной
в) экономической
г) контрразведывательной
д) внешнеполитической

23.. К внутренним нарушителям информационной безопасности относится:
а) пользователи системы;.
б) персонал, обслуживающий технические средства.
в) сотрудники отделов разработки и сопровождения ПО;
г) технический персонал, обслуживающий здание

24.. Собственником информации не может быть:
а) государство;
б) юридическое лицо;
в) нет правильного ответа
г) физическое лицо;

25. Терминология в сфере защиты информации регулируется

а) ГОСТ Р 6.30 – 2003
б) ГОСТ 51141 – 98
в) ГОСТ 50922 – 96
г) Гражданским кодексом.

Для студентов заочной формы обучения порог прохождения тестирования – 60% правильных ответов.

–«Зачтено» выставляется студенту, если 15 ответов правильных;

–«Не зачтено» выставляется студенту, если 10 и более ответовнеправильных.

Если обучающийся не преодолел установленный порог, то ему предоставляется еще одна попытка.

Типовые материалы к зачету

9. Информационные процессы в сфере государственных закупок.
10. Задача устойчивого развития информационной сферы государственных закупок.
11. Виды защищаемой информации в сфере государственного и муниципального управления.
12. Состояние и перспективы информатизации сферы торговых закупок.
13. Обеспечение информационной безопасности организации торговых закупок.
14. Применение Федерального Закона РФ «Об информации, информационных технологиях и защите информации» в сфере государственных закупок.
15. Сущность и понятие информационной безопасности. Связь информационной безопасности с информатизацией общества.
16. Понятие и назначение доктрины информационной безопасности. Основные положения доктрины информационной безопасности Российской Федерации и их реализация.
17. Сущность и понятие защиты информации. Уязвимость информации. Цели защиты информации.
18. Законодательная база защиты документированной информации в РФ.
19. Подзаконные нормативно-правовые акты в сфере защиты информации.
20. Понятие и виды конфиденциальной информации в современном российском законодательстве.
21. Государственная тайна, ее нормативное регулирование.
22. Правовой режим персональных данных. Общая характеристика Федерального закона «О персональных данных»
23. Понятие коммерческой тайны. Общая характеристика Федерального закона «О коммерческой тайне».
24. Понятие и разновидности служебной и профессиональной тайн.
25. Перечень конфиденциальных сведений и Перечень конфиденциальных документов, методика их формирования.
26. Служба конфиденциального делопроизводства, ее статус в структуре организации. Квалификационные характеристики и требования к сотрудникам службы КД.
27. Цели и задачи, права и обязанности, нормативно-методическая база службы КД
28. Анализ угроз несанкционированного получения документированной информации, хищения или уничтожения документов, их фальсификации или подмены. Предполагаемые рубежи и уровни защиты документопотоков
29. Понятие «защищенный документооборот», его цели и задачи.
30. Гриф ограничения доступа к документу: понятие, назначение, виды.
31. Избирательность и разрешительная система доступа к конфиденциальным документам.

32. Прием и регистрация конфиденциальных документов.
33. Принципы и этапы документирования конфиденциальных сведений.
34. Учетные формы: виды, правила оформления и ведения.
35. Составление, учет и уничтожение проектов конфиденциальных документов.
36. Особенности оформления реквизитов конфиденциальных документов.
37. Правила издания, копирования и тиражирования конфиденциальных документов
38. Экспедиционная обработка исходящих конфиденциальных документов.
39. Организация и контроль исполнения конфиденциальных документов. Правила работы исполнителя.
40. Экспертиза ценности конфиденциальных документов
41. Номенклатура конфиденциальных дел. Установление сроков конфиденциальности при составлении номенклатуры дел.
42. Правила формирования и оформления конфиденциальных дел.
43. Учет выдачи дел во временное пользование.
44. Подготовка конфиденциальных дел и документов для архивного хранения.

Зачет сдается в форме тестирования. Для студентов заочной формы обучения порог прохождения тестирования:

–«Зачтено» выставляется студенту, если 15 ответов правильных;

–«Не зачтено» выставляется студенту, если 10 и более ответовнеправильных.

Если обучающийся не преодолел установленный порог, то ему предоставляется еще одна попытка.

Типовые задания для контрольной работы

Учебным планом для студентов, обучающихся по заочной форме, предусмотрено выполнение контрольной работы. Она должна быть представлена в письменной форме. Для этого студент знакомится с методическими указаниями по выполнению и выбирает тему контрольной работы. Работа выполняется в соответствии с Методическими указаниями по написанию и оформлению контрольных работ ИИГУ (http://www.bashedu.ru/ru/organizatsiya-uchebnoi-raboty).

Темы контрольных работ

Вариант 1

1. Информационные процессы в сфере государственных закупок.
2. Понятие доступа к данным со стороны процесса; отличия от доступа со стороны пользователя. Понятие и примеры скрытого доступа. Надежность систем ограничения доступа.

Вариант 2

1. Субъекты и объекты информационных отношений в сфере государственных закупок.
2. Несанкционированное копирование программ как тип несанкционированного доступа. Юридические аспекты несанкционированного копирования программ. Способы защиты от копирования.

Вариант 3

1. Задача устойчивого развития в информационной сфере государственных закупок.
2. Особенности построения защиты информации в телекоммуникационных сетях УИС.

Вариант 4

1. Виды защищаемой информации в сфере государственных закупок.
2. Направления по защите от враждебных воздействий на безопасность компьютерных сетей.

Вариант 5
1. Применение Федерального Закона РФ «Об информации, информационных технологиях и защите информации» в сфере государственных закупок
2. Угрозы безопасности современных информационно-вычислительных и телекоммуникационных сетей. Классификация угроз безопасности.
Вариант 6
1. Аппаратные и программно-аппаратные средства криптозащиты данных.
2. Вирусы как особый класс разрушающих программных воздействий. Защита от разрушающих программных воздействий.
Вариант 7
1. Понятие атрибутов доступа к файлам. Организация доступа к файлам в различных операционных системах
2. Способы фиксации фактов доступа. Журналы доступа. Выявление следов несанкционированного доступа к файлам
Вариант 8
1. Методы и средства защиты данных от несанкционированного доступа.
2. Понятие и содержание информационной безопасности.
Вариант 9
1. Необходимость, назначение и общее содержание организационно- правового обеспечения информационной безопасности.
2. Методы и специальные технические средства, используемые в ходе поисковой операции в целях обеспечения защиты информации.
Вариант 10
1. Понятие и цели проведения специальных проверок объектов информатизации; основные этапы проведения проверки
2. Уязвимость компьютерных систем. Понятие несанкционированного доступа (НСД). Классы и виды НСД
Вариант 11
1. Основные направления инженерно-технической защиты информации: физическая защита, скрытие информации, поиск и нейтрализация источников утечки
2. Распространённые способы блокирования каналов утечки информации и виды специальных технических средств защиты
Вариант 12
1. Требования и показатели защищенности автоматизированных средств обработки информации.
2. Условия и факторы, способствующие утечке информации ограниченного доступа.
Вариант 13
1. Технические методы защиты информации.
2. Общая характеристика технических средств несанкционированного получения информации и технологий их применения
Вариант 14
1. Понятие и виды каналов утечки информации
2. Основные угрозы безопасности информации.
Вариант 15
1. Обеспечение безопасности ведомственной информации, информационных ресурсов, средств и систем информатизации.
2. Краткий обзор современных методов защиты информации
Вариант 16
1. Обеспечение информационной безопасности в каналах связи.
2. Меры противодействия информационной безопасности в автоматизированных системах обработки данных.
Вариант 17

1. Современное состояние и перспективы развития информационной безопасности в телекоммуникационных системах информации.
2. Принципы государственной политики обеспеченияинформационной безопасности Российской Федерации.
Вариант 18
1. Методы закрытия речевых сигналов в телефонных каналах связи.
2. Особенности проблем защиты конфиденциальной информации.
Вариант 19
1. Деятельность международных организаций в сфере информационной безопасности
2. Достоверность и целостность информации при передаче по каналам связи
Вариант 20
1. Основные составляющие национальных интересов в информационной сфере; виды и источники угроз информационной безопасности Российской Федерации.
2. Назначение и краткий анализ общих моделей процесса защиты информации.

Защита контрольной работы

Проводится в форме устного опроса после выполнения работы. Критерии и методика оценивания:

Критерии оценки	Распределение баллов
нет контрольной работы / существенные замечания и ошибки в ответе / имеются некоторые несущественные замечания и ошибки, точный ответ	Не допущен к зачету / доработка / зачтено

4.3.Рейтинг-план дисциплины (при необходимости)

Рейтинг–план дисциплины не предусмотрен для студентов заочной формы обучения.

5 Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература:

1. Ковалев, Д.В. Информационная безопасность : учебное пособие / Д.В. Ковалев, Е.А. Богданова ; Министерство образования и науки РФ, Южный федеральный университет. - Ростов-на-Дону : Издательство Южного федерального университета, 2016. - 74 с. : схем., табл., ил. - Библиогр. в кн. - ISBN 978-5-9275-2364-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=493175.
2. Шилов, А.К. Управление информационной безопасностью : учебное пособие / А.К. Шилов ; Министерство науки и высшего образования РФ, Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет», Институт компьютерных технологий и информационной безопасности. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. - 121 с. : ил. - Библиогр.: с. 81 - 82 - ISBN 978-5-9275-2742-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=500065

Дополнительная литература

1. Пелешенко, В.С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления : учебное пособие / В.С. Пелешенко, С.В. Говорова, М.А. Лапина ; Министерство образования и науки РФ, Федеральное государственное автономное образовательное учреждение высшего образования «Северо-Кавказский федеральный университет». - Ставрополь : СКФУ, 2017. - 86 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=467139 .

2. Аудит информационной безопасности органов исполнительной власти : учебное пособие / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, М.В. Рудановский. - 4-е изд., стер. - Москва : Издательство «Флинта», 2016. - 100 с. - (Организация и технология защиты информации). - Библиогр.: с. 83-84 - ISBN 978-5-9765-1277-1 ; То же [Электронный ресурс].- URL: http://biblioclub.ru/index.php?page=book&id=93259.

5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины

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. Справочная правовая система «КонсультантПлюс» – http://www.consultant-plus.ru

Программное обеспечение:

1. Windows 8 Russian Windows Professional 8 Russian Upgrade. Договор №104 от 17.06.2013 г. Лицензии бессрочные.
2. MicrosoftOfficeStandard 2013 Russian. Договор №114 от 12.11.2014 г. Лицензии бессрочные.

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

Наименование специальныхпомещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
1	2	3
1. учебная аудитория для проведения занятий лекционного типа: аудитория № 515 (гуманитарный корпус), аудитория № 516 (гуманитарный корпус). **2. учебная аудитория для проведения занятий семинарского типа:** аудитория № 413 (гуманитарный корпус), лаборатория информационных технологий № 420	**Аудитория № 515** Учебная мебель, доска, терминал видео конференц-связи LifeSizeIcon 600-камера, интер-ая 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, интер-ая напольная кафедра докладчика, ком-ер встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/ThermaltakeVL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром.	1. Windows 8 Russian Windows Professional 8 Russian Upgrade. Договор №104 от 17.06.2013 г. Лицензии бессрочные. 2. MicrosoftOfficeStandard 2013 Russian. Договор №114 от 12.11.2014 г. Лицензии бессрочные.

(гуманитарный корпус) **3. учебная аудитория для проведения групповых и индивидуальных консультаций:** аудитория № 609 (гуманитарный корпус), аудитория 509 (гуманитарный корпус). **4.учебная аудитория для текущего контроля и промежуточной аттестации:** аудитория № 609 (гуманитарный корпус), аудитория 509 (гуманитарный корпус). **5.помещения для самостоятельной работы:** аудитория № 613 (гуманитарный корпус), читальный зал аудитория 402 (гуманитарный корпус) 6. **помещение для хранения и профилактического обслуживания учебного оборудования:** аудитория 523 (гуманитарный корпус).	**Аудитория № 516** Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASKProxima, ноутбук HP, экран **Аудитория № 413** Учебная мебель, доска, Двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт АРАРТ MA1225 – 1 шт. **Аудитория № 420** Учебная мебель, моноблоки стационарные 15 шт. **Аудитория № 609** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 509** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 613** Учебная мебель, доска, моноблок стационарный – 15 шт. **Аудитория № 402** Учебная мебель, доска, компьютеры в комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура, мышь, стеллажи, шкафы картотечные, комбинированные. **Аудитория № 523** Шкаф-стеллаж, стол, стул, мобильное мультимедийное оборудование – ноутбук, проектор, экран	

Приложение 1

МИНОБРНАУКИ РОССИИ
ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ
Дисциплины «Информационная безопасность» на 2 курс
заочная форма обучения

Вид работы	**Объем дисциплины**
Общая трудоемкость дисциплины (ЗЕТ / часов)	4 ЗЕТ/144 часа
Учебных часов на контактную работу с преподавателем:	20,7
лекций	8
практических/ семинарских	4
лабораторных	8
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0,7
Учебных часов на самостоятельную работу обучающихся (СР)	119,3
Учебных часов на подготовку к зачету/ экзамену (Контроль)	4

Форма(ы) контроля:
экзамен_____-____ курс
зачет_____2_____ курс

	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)					Основная и дополнительная литература, рекомендуемая студентам (номера из списка)	Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
			ЛК	ПР / Сем	ЛР	СРС			
1	2		4	5	6	7	8	9	10
					Модуль1.				
	1.**Информационные процессы в сфере государственных закупок.** Стандарты в области информационной безопасности в сфере государственных и муниципальных закупок. Международные стандарты информационного обмена. Понятие угрозы, атаки в сфере государственных закупок. Глобальные сети и информационная безопасность сфере государственных закупок. 2. **Субъекты и объекты информационных отношений в сфере государственных закупок.**		4	2	4	19,3	Основная 1, 2 Дополнительная 1,2	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников. Выполнение контрольной работы	Тестирование, контрольная работа, устный индивидуальный опрос

	Основные субъекты - государственный или муниципальный заказчик и участники закупки -любое юридическое лицо независимо от его организационно-правовой формы, формы собственности, места нахождения и места происхождения капитала или любое физическое лицо, в том числе зарегистрированное в качестве индивидуального предпринимателя. Объекты- товары и услуги. Виды защищаемой информации в сфере государственных закупок								
Модуль 2									
	1.**Законодательство Российской Федерации о контрактной системе в сфере закупок.** Действующая российская нормативная правовая база в сфере государственных закупок, включая: Гражданский кодекс Российской Федерации;		4	2	4	100	Основная 1, 2 Дополнительная 1,2	Самостоятельное изучение рекомендуемой основной и дополнительной литературы. Выполнение контрольной работы	Тестирование, контрольная работа, устный индивидуальный опрос

	Бюджетный кодекс Российской Федерации; Федеральный закон от 5 апреля 2013 г. (с посл. изм.) № 44-ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд"; постановления и распоряжения Правительства Российской Федерации; нормативные и методические документы Минэкономразвития России и других федеральных органов исполнительной власти; другие нормативные акты, дополняющие законодательство Российской Федерации о контрактной системе. Общие представления об антимонопольном законодательстве. 2. **Мониторинг, контроль, аудит и защита прав и интересов участников закупок.** Общие вопросы мониторинга, аудита и контроля в сфере государственных и муниципальных закупок. Оценка								

	обоснованности и эффективности государственных и муниципальных закупок. Способы защиты прав и законных интересов участников процедуры закупки, порядок обжалования действий (бездействия) заказчика, уполномоченного органа, специализированной организации, комиссии по осуществлению закупок, должностного лица контрактной службы, контрактного управляющего, оператора электронной торговой площадки при осуществлении государственных и муниципальных закупок.								
	Всего часов		8	4	8	119,3			