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

Утверждено:
на заседании кафедры
протокол № 9 от 24.04.2020
Зав. кафедрой / А.С. Исмагилова

Согласовано:
Председ тель УМК института
/Р.А. Гильмутдинова

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Техническая защита информации

Б1.Б.18 базовая

программа бакалавриата

Направление подготовки
10.03.01 Информационная безопасность

Профиль подготовки
Организация и технология защиты информации

Квалификация
бакалавр

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

Для приема: 2020 г.

Уфа 2020 г.

Составитель: Ф.Т. Байрушин.

Рабочая программа дисциплины утверждена на заседании кафедры управления информационной безопасностью протокол № 9 от 24.04.2020

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

Заведующий кафедрой ____________________/ _____________Ф.И.О/

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

Заведующий кафедрой ____________________/ _____________Ф.И.О/

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

Заведующий кафедрой ____________________/ _____________Ф.И.О/

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

Заведующий кафедрой ____________________/ _____________Ф.И.О/

Список документов и материалов

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми 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 задачи своей профессии в соответствии с нормами морали, профессиональной этики и служебного этикета	ОК-5 способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	
	Знать политику информационной безопасности, применение комплексного подхода к обеспечению информационной безопасности объекта защиты	ПК-4 способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	
	Знать основные принципы организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ПК-6 способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	
Умения	Уметь понимать социальную значимость своей будущей профессии, цели и смысл государственной службы находить баланс между интересами личности, общества и государства соблюдать нормы профессиональной этики	ОК-5 способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	
	Уметь реализовывать на практике принципы политики информационной безопасности, применять	ПК-4 способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к	

	комплексный подход к обеспечению информационной безопасности объекта защиты	обеспечению информационной безопасности объекта защиты	
	Уметь применять навыки организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ПК-6 способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	
Владения (навыки / опыт деятельности)	Владеть высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	ОК-5 способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	
	Владеть навыками работы по реализации политики информационной безопасности, применения комплексного подхода к обеспечению информационной безопасности объекта защиты	ПК-4 способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	
	Владеть навыками организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ПК-6 способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Техническая защита информации» относится к дисциплинам базовой части профессионального цикла.
Дисциплина изучается на 3 курсе в 5,6 семестрах

Цель изучения дисциплины: формирование у бакалавров целостного представления о технической защите информации.

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

Содержание рабочей программы представлено в Приложении А.

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

ОК-5 -способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения для зачета	
		Не зачтено	Зачтено
Первый этап (уровень)	Знать основные задачи своей профессии в соответствии с нормами морали, профессиональной этики и служебного этикета	Не знает или имеет фрагментарные знания об основных задачах своей профессии в соответствии с нормами морали, профессиональной этики и служебного этикета	В целом знает основные задачи своей профессии в соответствии с нормами морали, профессиональной этики и служебного этикета
Второй этап (уровень)	Уметь понимать социальную значимость своей будущей профессии, цели и смысл государственной службы находить баланс между	Не умеет или не способен понимать социальную значимость своей будущей профессии, цели и смысл государственной службы находить баланс между интересами личности, общества и государства соблюдать	В целом умеет понимать социальную значимость своей будущей профессии, цели и смысл государственной службы находить баланс между интересами личности, общества и государства соблюдать нормы

	интересами личности, общества и государства соблюдать нормы профессиональной этики	нормы профессиональной этики	профессиональной этики
Третий этап (уровень)	Владеть мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Не владеет мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Способен владеть высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики

ПК-4 способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения для зачета	
		Не зачтено	Зачтено
Первый этап (уровень)	Знать политику информационной безопасности, применение комплексного подхода к обеспечению информационной безопасности объекта защиты	Не знает или имеет фрагментарные знания о политике информационной безопасности, применение комплексного подхода к обеспечению информационной безопасности объекта защиты	В целом знает основные задачи политики информационной безопасности, применение комплексного подхода к обеспечению информационной безопасности объекта защиты
Второй этап (уровень)	Уметь применять реализацию политики информационной безопасности, применять	Не умеет или не способен применять реализацию политики информационной безопасности, применять комплексный подход к	В целом умеет применять реализацию политики информационной безопасности, применять комплексный подход к обеспечению

	комплексный подход к обеспечению информационной безопасности объекта защиты	обеспечению информационной безопасности объекта защиты	информационной безопасности объекта защиты
Третий этап (уровень)	Владеть представлениями о применении реализации политики информационной безопасности, применении комплексного подхода к обеспечению информационной безопасности объекта защиты	Не владеет представлениями о применении реализации политики информационной безопасности, применении комплексного подхода к обеспечению информационной безопасности объекта защиты	Способен представлять положения о применении реализации политики информационной безопасности, применении комплексного подхода к обеспечению информационной безопасности объекта защиты

ПК-6 способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения для зачета	
		Не зачтено	Зачтено
Первый этап (уровень)	Знать основные принципы организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Не знает или имеет фрагментарные знания об основных принципах организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	В целом знает положения об основных принципах организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации

Второй этап (уровень)	Уметь применять навыки организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Не умеет или не способен применять навыки организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	В целом умеет применять навыки организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации
Третий этап (уровень)	Владеть навыками организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Не владеет навыками организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Способен применять навыки организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей, перечисленных в рейтинг-плане дисциплины (для зачета: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).

Шкала оценивания для зачета:

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

не зачтено – от 0 до 59 рейтинговых баллов).

ОК-5. Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики.

Этап (уровень) освоения компетенции	**Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций**	**Критерии оценивания результатов защиты курсового проекта и экзамена**			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)

	)				
Первый этап (уровень)	Знать: основные задачи своей профессии в соответствии с нормами морали, профессиональной этики и служебного этикета	Не способен разбираться в задачах своей профессии в соответствии с нормами морали, профессиональной этики и служебного этикета .	Способен разбираться в задачах своей профессии в соответствии с нормами морали, профессиональной этики и служебного этикета, однако допускает значительные ошибки	Способен разбираться в задачах своей профессии в соответствии с нормами морали, профессиональной этики и служебного этикета, но допускает незначительные ошибки	Способен детально и подробно разбираться в задачах своей профессии в соответствии с нормами морали, профессиональной этики и служебного этикета
Второй этап (уровень)	Уметь: понимать социальную значимость своей будущей профессии, цели и смысл государственной службы находить баланс между интересами личности, общества и государства соблюдать нормы профессиональной этики	Не понимает социальную значимость своей будущей профессии, цели и смысл государственной службы находить баланс между интересами личности, общества и государства соблюдать нормы профессиональной этики	Испытывает сложности в понимании социальной значимости своей будущей профессии, целях и смысле государственной службы находить баланс между интересами личности, общества и государства соблюдать нормы профессиональной этики	Понимает социальную значимость своей будущей профессии, цели и смысл государственной службы находить баланс между интересами личности, общества и государства соблюдать нормы профессиональной этики. Однако испытывает сложности со связью теории и конкретной задачи	Отчетливо понимает социальную значимость своей будущей профессии, цели и смысл государственной службы находить баланс между интересами личности, общества и государства соблюдать нормы профессиональной этики
Третий этап (уровень)	Владеть: навыками принятия решений в условиях информационной неопределенности навыками творческого	Не владеет навыками принятия решений в условиях информационной неопределенности навыками творческого	Владеет общими навыками принятия решений в условиях информационной неопределенности навыками творческого	Владеет навыками принятия решений в условиях информационной неопределенности навыками творческого	В совершенстве владеет навыками принятия решений в условиях информационной неопределенности

	мышления для выполнения профессиональных задач в области обеспечения информационной безопасности и защиты интересов личности, общества и государства	мышления для выполнения профессиональных задач в области обеспечения информационной безопасности и защиты интересов личности, общества и государства	мышления для выполнения профессиональных задач в области обеспечения информационной безопасности и защиты интересов личности, общества и государства	мышления для выполнения профессиональных задач в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, однако допускает незначительные ошибки.	навыками творческого мышления для выполнения профессиональных задач в области обеспечения информационной безопасности и защиты интересов личности, общества и государства

ПК-4. Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты

Этап (уровень) освоения компетенции	**Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)**	**Критерии оценивания результатов защиты курсового проекта и экзамена**			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать: политику, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации; понятие системы управления, основные виды структур, принципы	Фрагментарные представления о современных принципах и методах обеспечения информационной безопасности и защиты информации, возможностях организационных, аппаратных и программных средств безопасности и защиты информации;	В целом сформированные, но неполные знания о политиках, стратегиях и технологиях информационной безопасности и защиты информации, основных понятиях в области информационной безопасности, возможностях организационн	Сформированные, но содержащие отдельные пробелы знания о политиках, стратегиях и технологиях информационной безопасности и защиты информации, способах их организации и оптимизации; понятиях системы управления,	Сформированные систематические знания о политиках, стратегиях и технологиях информационной безопасности и защиты информации, способах их организации и оптимизации; понятиях системы управления,

	системного подхода к анализу структур; общеметодологические принципы теории информационной безопасности; возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации; состояние законодательной базы и стандарты в области информационной безопасности, общеметодологические принципы теории информационной безопасности; состояние законодательной базы и стандарты в области информационной безопасности;	состоянии законодательной базы и стандартов в области информационной безопасности, неточные знания об основных понятиях в области информационной безопасности, общеметодологических принципах теории информационной безопасности; состоянии законодательной базы и стандарты в области информационной безопасности	ых, аппаратных и программных средств безопасности и защиты информации; состоянии законодательной базы и стандартов в области информационной безопасности, общеметодологических принципах теории информационной безопасности; состоянии законодательной базы и стандарты в области информационной безопасности	основных видах структур, принципах системного подхода к анализу структур; общеметодологических принципах теории информационной безопасности; возможностях и особенностях организационных, аппаратных и программных средств безопасности и защиты информации; состоянии законодательной базы и стандартов в области информационной безопасности, общеметодологических принципах теории информационной безопасности; состоянии законодательной базы и стандарты в области информационной безопасности	основных видах структур, принципах системного подхода к анализу структур; общеметодологических принципах теории информационной безопасности; возможностях и особенностях организационных, аппаратных и программных средств безопасности и защиты информации; состоянии законодательной базы и стандартов в области информационной безопасности, общеметодологических принципах теории информационной безопасности; состоянии законодательной базы и стандарты в области информационной безопасности
Второй этап (уровень)	Уметь: реализовывать на практике принципы политики безопасности; использовать закономерности преобразования	Фрагментарные умения применять принципы политики безопасности; закономерности преобразования данных в	В целом успешное, но не систематическое умение применять принципы политики безопасности; закономерности	Успешное, но содержащее отдельные пробелы умение применять принципы политики безопасности;	Сформированное умение применять принципы политики безопасности; закономерности преобразования данных в

	данных в каналах при выполнении комплекса мер по информационной безопасности; обосновывать организационно-технические мероприятия по защите информации; использовать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации.	каналах при выполнении комплекса мер по информационной безопасности; обосновывать организационно-технические мероприятия по защите информации; использовать возможности организационных, аппаратных и программных средств безопасности и защиты информации	преобразования данных в каналах при выполнении комплекса мер по информационной безопасности; обосновывать организационно-технические мероприятия по защите информации; использовать возможности организационных, аппаратных и программных средств безопасности и защиты информации	закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности; обосновывать организационно-технические мероприятия по защите информации; использовать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации	каналах при выполнении комплекса мер по информационной безопасности; обосновывать организационно-технические мероприятия по защите информации; использовать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации
Третий этап (уровень)	Владеть: навыками анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью; навыками организации комплекса мероприятий по защите информации в	Фрагментарное владение навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью; навыками выявления и устранения угроз информационной безопасности; навыками эксплуатации современного электронного оборудования и информационно-коммуникацион	В целом успешное, но не полное владение навыками анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками формирования комплекса мер для управления информационной безопасностью; навыками организации комплекса мероприятий по защите информации в процессах	Успешное, но содержащее отдельные пробелы владение навыками анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью; навыками организации	Сформированное владение навыками анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью; навыками организации комплекса мероприятий по защите

	процессах автоматизированной обработки информации; навыками выявления и устранения угроз информационной безопасности; навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий; навыками во внедрении, адаптации и настройке средств защиты прикладных ИС.	ных технологий; навыками во внедрении, адаптации и настройке средств защиты прикладных ИС,	автоматизированной обработки информации; навыками выявления и устранения угроз информационной безопасности; навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий; навыками во внедрении, адаптации и настройке средств защиты прикладных ИС.	комплекса мероприятий по защите информации в процессах автоматизированной обработки информации; навыками выявления и устранения угроз информационной безопасности; навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий; навыками во внедрении, адаптации и настройке средств защиты прикладных ИС.	информации в процессах автоматизированной обработки информации; навыками выявления и устранения угроз информационной безопасности; навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий; навыками во внедрении, адаптации и настройке средств защиты прикладных ИС.

ПК-6. Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации

Этап (уровень) освоения компетенции	**Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)**	**Критерии оценивания результатов защиты курсового проекта и экзамена**			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать: основные принципы оценки работоспособности и тестирования оборудования	Имеет фрагментарные знания об основных принципах оценки работоспособности и	В целом знает: об основных принципах оценки работоспособности и тестирования оборудования	Знает: об основных принципах оценки работоспособности и тестирования оборудования	Демонстрирует целостность знания об основных принципах оценки работоспособности и

	обработки и передачи данных; критерии и меры надежности, возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации	тестирования оборудования обработки и передачи данных; критерии и меры надежности, возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации	обработки и передачи данных, но не знает критерии и меры надежности, возможности и особенности организационно, аппаратных и программных средств безопасности и защиты информации.	обработки и передачи данных; критерии и меры надежности, возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации, но допускает незначительные ошибки.	тестирования оборудования обработки и передачи данных; критерии и меры надежности, возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации
Второй этап (уровень)	Уметь: использовать возможности и особенности организационных, аппаратных и программных средств обеспечения безопасности и защиты информации; составлять и реализовывать планы тестирующих мероприятий, в том числе имитирующих внешние и внутренние атаки, нарушающие систему информационной безопасности.	Умеет использовать возможности и особенности организационных, аппаратных и программных средств обеспечения безопасности и защиты информации.	Умеет использовать возможности и особенности организационно, аппаратных и программных средств обеспечения безопасности и защиты информации, но не умеет составлять и реализовывать планы тестирующих мероприятий, в том числе имитирующих внешние и внутренние атаки, нарушающие систему информационной безопасности.	Уверенно использует возможности и особенности организационных, аппаратных и программных средств обеспечения безопасности и защиты информации; составлять и реализовывать планы тестирующих мероприятий, в том числе имитирующих внешние и внутренние атаки, нарушающие систему информационной безопасности, но допускает незначительные ошибки.	Уверенно использует возможности и особенности организационных, аппаратных и программных средств обеспечения безопасности и защиты информации; составлять и реализовывать планы тестирующих мероприятий, в том числе имитирующих внешние и внутренние атаки, нарушающие систему информационной безопасности.
Третий этап (уровень)	Владеть: навыками эксплуатации современного электронного оборудования	Не способен эксплуатировать современного электронного обор и информационн	Владеет навыками эксплуатации современного электронного оборудования и	Владеет навыками эксплуатации современного электронного оборудования	Владеет навыками эксплуатации современного электронного оборудования

	и информационно-коммуникационных технологий; использования методов тестирования коммуникационного оборудования и аппаратуры обработки данных, криптографических систем	о-коммуникационных технологий.	информационно-коммуникационных технологий, но не использует методов тестирования коммуникационного оборудования и аппаратуры обработки данных, криптографических систем.	и информационно-коммуникационных технологий; использования методов тестирования коммуникационного оборудования и аппаратуры обработки данных, криптографических систем, но испытывает незначительные трудности	и информационно-коммуникационных технологий; использования методов тестирования коммуникационного оборудования и аппаратуры обработки данных, криптографических систем

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
1-й этап Знания	основных задач своей профессии в соответствии с нормами морали, профессиональной этики и служебного этикета	ОК-5 способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Опрос, практические задания, тестирование, лабораторные задания
	политики информационной безопасности, применение комплексного подхода к обеспечению информационной безопасности объекта защиты	ПК-4 способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Опрос, практические задания, тестирование, лабораторные задания
	основных принципов организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ПК-6 способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Опрос, практические задания, тестирование, лабораторные задания
2-й этап Умения	понимать социальную значимость своей будущей профессии, цели и смысл государственной	ОК-5 способность понимать социальную значимость своей будущей профессии, обладать	Опрос, практические задания, тестирование, лабораторные задания

	службы находить баланс между интересами личности, общества и государства соблюдать нормы профессиональной этики	высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	
	реализовывать на практике принципы политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	ПК-4 способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Опрос, практические задания, тестирование, лабораторные задания
	применять навыки организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ПК-6 способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Опрос, практические задания, тестирование, лабораторные задания
3-й этап Владения навыками	высокой мотивации к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	ОК-5 способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Опрос, практические задания, тестирование, лабораторные задания
	работы по реализации политики	ПК-4 способность участвовать в работах по реализации политики	Опрос, практические задания, тестирование, лабораторные задания

	информационной безопасности, применения комплексного подхода к обеспечению информационной безопасности объекта защиты	информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	
	организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ПК-6 способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Опрос, практические задания, тестирование, лабораторные задания

Устный опрос (аудиторная работа)

Устный индивидуальный опрос проводится после изучения новой темы с целью выяснения наиболее сложных вопросов, степени усвоения информации. Студент излагает содержание вопроса изученной темы и делает доклад по одной из тем.

Примерная тематика занятий

Модуль 1

1.Основные свойства информации как предмета технической защиты
2.Источники и носители конфиденциальной информации
3.Виды угроз безопасности информации
4.Способы и средства инженерной защиты и технической охраны

Модуль 2.

1.Способы и средства предотвращения утечки информации через побочные электромагнитные излучения и наводки
2.Способы предотвращения утечки информации по материально-вещественному каналу
3.Общие положения по технической защите информации в организации
4.Организационные и технические меры по технической защите информации в организации

Модуль 3

1.Принципы построения системы СТЗИ: многозональность и многорубежность
2.Одноразовые пароли
3.Ролевое управление доступом
4.Низкочастотные и высокочастотные излучения технических средств

Модуль 4

1.Цифровые сертификаты
2.Шифрование заменой(подстановка
3.Типовая структура технического канала утечки информации
4.Система распределения ключей Диффи-Хелмана

Критерии и методика оценивания:

Студенту предлагается 4 аудиторных заданий в каждом из 4 модулей в процессе изучения материала курса. За каждое задание начисляется:

Модуль 1,2

- 3 балла, если ответы на вопросы даны верно и достаточно полно.
- 2 балла выставляется студенту, если в логическом рассуждении нет существенных ошибок; правильно сделан выбор формулировок, но допущено не более двух несущественных ошибок,
- 1 балл , если в ответах нет определенной логической последовательности, неточно используется специализированная терминология;
- 0 баллов если ответ на устный вопрос не дан или дан неверно.

Модуль 3,4

- 2,5 балла, если ответы на вопросы даны верно и достаточно полно.
- 2 балла выставляется студенту, если в логическом рассуждении нет существенных ошибок; правильно сделан выбор формулировок, но допущено не более двух несущественных ошибок,
- 1 балл , если в ответах нет определенной логической последовательности, неточно используется специализированная терминология;
- 0 баллов если ответ на устный вопрос не дан или дан неверно.

Темы лабораторных работ

Модуль 1

1. Анализ демаскирующих признаков, методы и способы защиты демаскирующих признаков на объекте защиты (предлагается до 5 видов объектов защиты).
2. – Составление модели поведения внешнего нарушителя на этапах реализации угроз безопасности информации, методы и способы противодействия от утечки информации по техническим каналам.
3. – Составление модели поведения инсайдера на этапах реализации угроз безопасности информации, методы и способы противодействия от утечки информации по техническим каналам.
4. – Определение и анализ условий и факторов, способствующие утечки информации по техническим каналам, методы и способы противодействия утечке информации.
5. – Разработка и анализ методов защиты видовых демаскирующих признаков от технических средств разведок.
6. – Разработка и анализ методов защиты сигнальных демаскирующих признаков от технических средств разведок.

7. – Разработка и анализ методов защиты радиосигналов от перехвата техническими средствами разведок.

Модуль 2

1. – Разработка и анализ методов защиты электрических сигналов от перехвата техническими средствами разведок.
2. – Разработка и анализ методов защиты материальных и вещественных демаскирующих признаков от технических средств разведок.
3. – Анализ возможностей технических средств наблюдения в видимом и ИК диапазонах за объектом защиты, методы и средства противодействия средствам наблюдения.
4. – Анализ возможностей технических средств наблюдения в радио диапазонах за объектом защиты, методы и средства противодействия средствам наблюдения.
5. – Анализ возможностей технических средств перехвата конфиденциальной информации передаваемой по линии связи, методы и средства противодействия перехвата конфиденциальной информации.
6. – Анализ возможностей технических средств съема конфиденциальной речевой информации с использованием вторичных переизлучателей.
7. – Анализ возможностей технических средств съема конфиденциальной речевой информации с использованием опто-волоконных линий связи.

Модуль 3

1. – Анализ возможностей технических средств съема конфиденциальной речевой информации с использованием средств высокочастотного навязывания.
2. – Анализ возможностей технических средств подслушивания, методы и средства противодействия средствам подслушивания.
3. – Анализ возможностей технических средств демаскирующих признаков веществ, методы и средства нейтрализации (утилизации) отходов производства.
4. – Анализ возможностей технических средств контроля, обнаружения, уничтожение закладных устройств, порядок проведения поисковых мероприятий на предлагаемом объекте (до 5 объектов).
5. – Анализ возможностей технических средств контроля, обнаружения, уничтожение закладных устройств, в слаботочных линиях связи, порядок проведения поисковых мероприятий (до 5 видов линий и их архитектур построения).
6. – Анализ возможностей технических средств контроля, обнаружения, уничтожение закладных устройств в телефонных линиях связи, порядок проведения поисковых мероприятий (до 5 видов линий и их архитектур построения).
7. – Анализ возможностей технических средств контроля, обнаружения, уничтожение 11 закладных устройств, в электросетях, цепях заземления, порядок проведения поисковых мероприятий.

Модуль 4

1. – Моделирование вербального объекта защиты, возможных угроз безопасности информации для оптических каналов утечки информации в видимом и ИК диапазонах, разработка способов, методов и технических средств защиты информации.
2. – Моделирование вербального объекта защиты, где ведутся конфиденциальные переговоры, возможных угроз безопасности информации для акустических каналов утечки информации, разработка методов и технические средств защиты информации.
3. – Моделирование вербального объекта защиты, где ведутся конфиденциальные переговоры, возможных угроз безопасности информации для акустикорадиоэлектронных каналов утечки информации, разработка методов и технических средств защиты информации.
4. – Моделирование вербального объекта защиты, где ведутся конфиденциальные переговоры, возможных угроз безопасности информации для акустико-оптических

каналов утечки информации, разработка методов и технических средств защиты информации.

5. – Моделирование вербального объекта защиты, где производится обработка информации с использованием СВТ (АС), возможных угроз безопасности информации и технических каналов утечки информации, разработка методов и технических средств защиты информации.
6. – Моделирование вербального объекта защиты, где производится обработка информации с использованием технических средств обработки информации, возможных угроз безопасности информации и технических каналов утечки информации, разработка методов и технических средств защиты информации.
7. – Моделирование вербального объекта защиты, возможных угроз безопасности информации для материально-вещественных каналов утечки информации, разработка методов и технических средств защиты информации.

Критерии и методика оценивания:

Студенту предлагается 7 заданий в каждом из 4 модулей в процессе изучения материала курса. За каждое задание начисляется:

Модуль 1, 2

- 3,25 балла выставляется студенту, если практическое задание решено верно, показано уверенное владение учебным материалом;

- 2 балла выставляется студенту, если в логическом рассуждении нет существенных ошибок; правильно сделан выбор формулировок, но допущено не более двух несущественных ошибок,

1 балл выставляется студенту, нет определенной логической последовательности, неточно используется специализированная терминология;

- 0 баллов выставляется студенту, если студент не дал ни одного правильного ответа

Модуль 3,4

- 2,5 балла выставляется студенту, если практическое задание решено верно, показано уверенное владение учебным материалом;

- 2 балла выставляется студенту, если в логическом рассуждении нет существенных ошибок; правильно сделан выбор формулировок, но допущено не более двух несущественных ошибок,

1 балл выставляется студенту, нет определенной логической последовательности, неточно используется специализированная терминология;

- 0 баллов выставляется студенту, если студент не дал ни одного правильного ответа

Типовые тесты

Модуль 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

7К посторонним лицам нарушителям информационной безопасностиотносится:

1. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
2. персонал, обслуживающий технические средства;
3. технический персонал, обслуживающий здание;
4. пользователи;
5. сотрудники службы безопасности.
6. представители конкурирующих организаций.

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

9. Перехват, который осуществляется путем использования оптической техники называется:
1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

10. К внутренним нарушителям информационной безопасности относится:
1. клиенты;
2. пользователи системы;
3. посетители;
4. любые лица, находящиеся внутри контролируемой территории;
5. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации.
6. персонал, обслуживающий технические средства.
7. сотрудники отделов разработки и сопровождения ПО;
8. технический персонал, обслуживающий здание

11. Анализ протоколируемой информации с целью оперативного выявления и предотвращения нарушений режима информационной безопасности – это?
1. Протоколирование
2. Экранирование
3. Аудит

12. Хронологически упорядоченная совокупность записей результатов деятельности субъектов АС, достаточная для восстановления, просмотра и анализа последовательности действий с целью контроля конечного результата – это?
1. Политика безопасности
2. Журнал аудита
3. Регистрационный журнал

13. К какому классу межсетевых экранов относится CISCO PIX?
1. Межсетевые экраны экспертного уровня
2. Шлюзы прикладного уровня

14. Активный перехват информации это перехват, который:
1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;
4. осуществляется путем использования оптической техники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

15. Защита информации от утечки это деятельность по предотвращению:
1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;

2. 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;
3. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

16.Длина исходного ключа у алгоритма шифрования DES (бит)
56
128
64
256

17.Компьютер — это:
а) устройство для работы с текстами;
б) электронное вычислительное устройство для обработки чисел;
в) устройство для хранения информации любого вида;
г) многофункциональное электронное устройство для работы с информацией;
д) устройство для обработки аналоговых сигналов.
е) другое

18. Постоянное запоминающее устройство служит для:
а) хранения программ начальной загрузки компьютера и тестирования его узлов;
б) хранения программы пользователя во время работы;
в) записи особо ценных прикладных программ;
г) хранения постоянно используемых программ;
д) постоянного хранения особо ценных документов.
е) другое

19. Процесс хранения информации на внешних носителях принципиально отличается от процесса хранения информации в оперативной памяти:
а) тем, что на внешних носителях информация может храниться после отключения питания компьютера;
б) объемом хранимой информации;
в) различной скоростью доступа к хранимой информации;
г) возможностью защиты информации;
д) способами доступа к хранимой информации.
е) другое

20. Манипулятор “мышь” — это устройство:
а) модуляции и демодуляции;
б) считывания инфоромации;
в) долговременного хранения информации;
г) ввода информации;
д) для подключения принтера к компьютеру.
е) другое

21. С использованием команды MD в MS DOS создается:
а) текстовый файл;
б) командный файл;
в) пустой каталог;
г) совокупность каталогов;
д) файл IO.SYS.
е) другое

22. Одной из основных характеристик компьютера является быстродействие, которое характеризуется:

а) количеством операций в секунду;
б) количеством выполняемых одновременно программ;
в) временем организации связи между АЛУ и ОЗУ;
г) количеством вводимых символов;
д) количеством подключенных устройств;
е) другое

23. Имя и тип файла разделяются между собой:
а) символом “ . ”;
б) символом “ - ”;
в) пробелом
г) символом “*”
д) символом « _ »
е) другое

24Скорость работы компьютера зависит от:
а) тактовой частоты обработки информации в процессоре;
б) наличия или отсутствия подключенного принтера;
в) организации интерфейса операционной системы;
г) объема внешнего запоминающего устройства;
д) объема обрабатываемой информации.
е) другое

25 Во время исполнения прикладная программа хранится:
а) в видеопамяти;
б) в процессоре;
в) в оперативной памяти;
г) на жестком диске;
д)в ПЗУ.
е) другое

Модуль 2

1.Компьютер — это:
а) устройство для работы с текстами;
б) электронное вычислительное устройство для обработки чисел;
в) устройство для хранения информации любого вида;
г) многофункциональное электронное устройство для работы с информацией;
д) устройство для обработки аналоговых сигналов.
е) другое

2. Постоянное запоминающее устройство служит для:
а) хранения программ начальной загрузки компьютера и тестирования его узлов;

б) хранения программы пользователя во время работы;
в) записи особо ценных прикладных программ;
г) хранения постоянно используемых программ;
д) постоянного хранения особо ценных документов.
е) другое

3. Процесс хранения информации на внешних носителях принципиально отличается от процесса хранения информации в оперативной памяти:
а) тем, что на внешних носителях информация может храниться после отключения питания компьютера;
б) объемом хранимой информации;
в) различной скоростью доступа к хранимой информации;
г) возможностью защиты информации;
д) способами доступа к хранимой информации.
е) другое

4. Манипулятор “мышь” — это устройство:
а) модуляции и демодуляции;
б) считывания инфоромации;
в) долговременного хранения информации;
г) ввода информации;
д) для подключения принтера к компьютеру.
е) другое

5. С использованием команды MD в MS DOS создается:
а) текстовый файл;
б) командный файл;
в) пустой каталог;
г) совокупность каталогов;
д) файл IO.SYS.
е) другое

6. Одной из основных характеристик компьютера является быстродействие, которое характеризуется:

а) количеством операций в секунду;
б) количеством выполняемых одновременно программ;
в) временем организации связи между АЛУ и ОЗУ;
г) количеством вводимых символов;
д) количеством подключенных устройств;
е) другое

7. Имя и тип файла разделяются между собой:
а) символом “ . ”;
б) символом “ - ”;
в) пробелом
г) символом “*”
д) символом « _ »
е) другое

8Скорость работы компьютера зависит от:
а) тактовой частоты обработки информации в процессоре;
б) наличия или отсутствия подключенного принтера;

в) организации интерфейса операционной системы;
г) объема внешнего запоминающего устройства;
д) объема обрабатываемой информации.
е) другое

9 Во время исполнения прикладная программа хранится:
а) в видеопамяти;
б) в процессоре;
в) в оперативной памяти;
г) на жестком диске;
д)в ПЗУ.
е) другое

10Для подключения компьютера к телефонной сети используется:
а) модем;
б) факс;
в) сканер;
г) принтер;
д) монитор.
е) другое

11Расширение имени файла, как правило, характеризует:
а) время создания файла;
б) объем файла;
в) место, занимаемое файлом на диске;
г) тип информации, содержащейся в файле;
д) место создания файла.
е) другое

12 Команда COPY предназначена для копирования в MS DOS:
а) файлов и каталогов;
б) только текстовых файлов;
в) только каталогов;
г) только командных файлов;
д) утилит MSDOS.
е) другое

13 . Максимальная длина двоичного кода, который может обрабатываться или передаваться процессором целиком:
а) Кэш;
б) BIOS;
в) Разрядность;
г) Тактовая частота
д) Контроллер;
е) другое

14 . В какой из последовательностей единицы измерения информации указаны в порядке возрастания:
а)байт, килобайт, мегабайт, бит;
б)килобайт, байт, бит, мегабайт;
в)байт, мегабайт, килобайт, гигабайт;
г)мегабайт, килобайт, гигабайт, байт;
д)байт, килобайт, мегабайт, гигабайт. е) другое.

15 .Винчестер предназначен для:

а) подключения периферийных узлов к магистрали;
б) управления работой ЭВМ по заданной программе;
в)хранения информации;

16 Память, используемая для хранения ьольших объемов информации:

а) оперативная память;
б) гибкий магнитный диск;
в) постоянная память (ПЗУ);

17 Микропроцессор имеет в своем составе:

а) устройство ввода;
б) внутренние регистры;
в) арифметико-логическое устройство;

18. Как называется умышленно искаженная информация?
а)Дезинформация
б)Информативный поток
в) Достоверная информация
г) Перестает быть информацией
19. Как называется информация, к которой ограничен доступ?
а Конфиденциальная
б Противозаконная
в Открытая
г Недоступная
20. Какими путями может быть получена информация?
а. проведением, покупкой и противоправным добыванием информации научных исследований
б. захватом и взломом ПК информации научных исследований
в. добыванием информации из внешних источников и скремблированием информации научных исследовании
г. захватом и взломом защитной системы для информации научных исследований
21. Как называются компьютерные системы, в которых обеспечивается безопасность информации?
а. защищенные КС
б.небезопасные КС
в. Само достаточные КС
г.Саморегулирующиеся КС
22.Основной документ, на основе которого проводится политика информационной безопасности?
а. программа информационной безопасности
Б. регламент информационной безопасности
в. политическая информационная безопасность
г. Протекторат
В зависимости от формы представления информация может быть разделена на?
а. Речевую, документированную и телекоммуникационную
б. Мысль, слово и речь
в. цифровая, звуковая и тайная
г. цифровая, звуковая

23. К каким процессам относят процессы сбора, обработки, накопления, хранения, поиска и распространения информации
а. Информационным процессам
б. Мыслительным процессам
в. Машинным процессам
г. Микропроцессам
24.Что называют защитой информации?
а. Все ответы верны
б. Называют деятельность по предотвращению утечки защищаемой информации
в. Называют деятельность по предотвращению несанкционированных воздействий на защищаемую информацию
г. Называют деятельность по предотвращению непреднамеренных воздействий на защищаемую информацию
25. Под непреднамеренным воздействием на защищаемую информацию понимают?
а. Воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств и воздействие природных явлений
б. Процесс ее преобразования, при котором содержание информации изменяется на ложную
в. Возможности ее преобразования, при котором содержание информации изменяется на ложную информацию
г. Не ограничения доступа в отдельные отрасли экономики или на конкретные производства

Модуль 3

1.Шифрование информации это
а. Процесс ее преобразования, при котором содержание информации становится непонятным для не обладающих соответствующими полномочиями субъектов
б. Процесс преобразования, при котором информация удаляется
в. Процесс ее преобразования, при котором содержание информации изменяется на ложную
г. Процесс преобразования информации в машинный код

2.Основные предметные направления Защиты Информации?
а. охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности
б. Охрана золотого фонда страны
в.Определение ценности информации
г. Усовершенствование скорости передачи информации

3. 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 страны
б. ограничения доступа в отдельные отрасли экономики или на конкретные производства
в. защищаемые банками и иными кредитными организациями сведения о банковских операциях
г. защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

4. Коммерческая тайна это….
а. защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны
б. ограничения доступа в отдельные отрасли экономики или на конкретные производства

в.. защищаемые банками и иными кредитными организациями сведения о банковских операциях
г. защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

5.Как называется тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений?
а. Тайна связи
б. Нотариальная тайна
в. Адвокатская тайна
г. Тайна страхования

6.Элемент аппаратной защиты, где используется установка источников бесперебойного питания (UPS)?
а. защита от сбоев в электропитании
б. защита от сбоев серверов, рабочих станций и локальных компьютеров
в. защита от сбоев устройств для хранения информации
г. защита от утечек информации электромагнитных излучений

7.Функция защиты информационной системы, гарантирующая то, что доступ к информации, хранящейся в системе может быть осуществлен только тем лицам, которые на это имеют право
а. управление доступом
б. конфиденциальность
в. аутентичность
г. целостность

8. Элемент аппаратной защиты, где используется резервирование особо важных компьютерных подсистем
а. защита от сбоев в электропитании
б. защита от сбоев серверов, рабочих станций и локальных компьютеров
в. защита от сбоев устройств для хранения информации
г. защита от утечек информации электромагнитных излучений

9.Элемент аппаратной защиты, где используется организация надежной и эффективной системы резервного копирования и дублирования данных
а. защита от сбоев в электропитании
б. защита от сбоев серверов, рабочих станций и локальных компьютеров
в. защита от сбоев устройств для хранения информации
г. защита от утечек информации электромагнитных излучений

10. Элемент аппаратной защиты, где используется экранирование, фильтрацию, заземление, электромагнитное зашумление, а также средства ослабления уровней нежелательных электромагнитных излучений.
а. защита от сбоев в электропитании
б. защита от сбоев серверов, рабочих станций и локальных компьютеров
в. защита от сбоев устройств для хранения информации
г. защита от утечек информации электромагнитных излучений

11.Какая из перечисленных атак на поток информации является пассивной:
а. перехват.
б. имитация.

в. модификация.
г. фальсификация.
д. прерывание.

12.Технические каналы утечки информации делятся на…
а. Все перечисленное
б. Акустические и виброакустические
в. Электрические
г. Оптические

13. Какой технический канал утечки отвечает за распространение звуковых колебаний в любом звукопроводящем материале или среде?
а. Акустические и виброакустические
б. Электрические
в. Оптические
г. Радиоканалы

14. Какой технический канал утечки отвечает за напряжение и токи в различных токопроводящих коммуникациях?
а. Акустические и виброакустические
б. Электрические
в. Оптические
г. Радиоканалы

15. Какой технический канал утечки отвечает за электромагнитные излучения радиодиапазона?
а. Акустические и виброакустические
б. Электрические
в. Оптические
г. Радиоканалы

16.Какой технический канал утечки отвечает за электромагнитные излучения в видимой, инфракрасной и ультрафиолетовой частях спектра?
а. Акустические и виброакустические
б. Электрические
в. Оптические
г. Радиоканалы

17.По сведениям Media и PricewaterhouseCoopers, на чью долю приходится 60% всех инцидентов IT-безопасности?
а. Хакерские атаки
б. Различные незаконные проникновения
в. Инсайдеры
г. Технические компании

18. Учет всех возможных коммуникационных каналов, обеспечения физической безопасности, шифрования резервных копий и информации, покидающей корпоративный периметр, и других организационных мероприятий это?
а. Индивидуальный подход к защите
б. Комплексный подход к защите
в. Смешанный подход к защите
г. Рациональный подход к защите

19.Меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе
а. Информационная безопасность
б. Защитные технологии
в. Заземление
г. Конфиденциальность

20.Можно выделить следующие направления мер информационной безопасности
а. Правовые
б. Организационные
в. Все ответы верны
г. Технические

21.Что можно отнести к правовым мерам ИБ?
а. Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства
б. охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра итд
в. Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, установку оборудования обнаружения и тушения пожара, оборудования обнаружения воды, принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое
г. охрану вычислительного центра, установку сигнализации и многое другое

22.Что можно отнести к организационным мерам ИБ?
а. Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства.
б.Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.
в. Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем.
г. Охрану работоспособности отдельных звеньев и организацию вычислительных сетей с возможностью перераспределения ресурсов.
д.Принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

23.Что можно отнести к техническим мерам ИБ?
а. Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства
б. Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.

в. Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев и многое другое
г. Простые и доступные меры защиты от хищений, саботажа, диверсий, взрывов.

24. Потенциальные угрозы, против которых направлены технические меры защиты информации
а. Потери информации из-за сбоев оборудования, некорректной работы программ и ошибки обслуживающего персонала и пользователей
а. Потери информации из-за халатности обслуживающего персонала и не ведения системы наблюдения
б. Потери информации из-за не достаточной установки резервных систем электропитании и оснащение помещений замками.
в. Потери информации из-за не достаточной установки сигнализации в помещении.
г. Процессы преобразования, при котором информация удаляется

25.Шифрование информации это
а. Процесс ее преобразования, при котором содержание информации становится непонятным для не обладающих соответствующими полномочиями субъектов
б. Процесс преобразования, при котором информация удаляется
в. Процесс ее преобразования, при котором содержание информации изменяется на ложную
г. Процесс преобразования информации в машинный код

Модуль 4

1.Для подключения компьютера к телефонной сети используется:
а) модем;
б) факс;
в) сканер;
г) принтер;
д) монитор.
е) другое

2.Расширение имени файла, как правило, характеризует:
а) время создания файла;
б) объем файла;
в) место, занимаемое файлом на диске;
г) тип информации, содержащейся в файле;
д) место создания файла.
е) другое

3. Команда COPY предназначена для копирования в MS DOS:
а) файлов и каталогов;
б) только текстовых файлов;
в) только каталогов;
г) только командных файлов;
д) утилит MS DOS.
е) другое
4 . Максимальная длина двоичного кода, который может обрабатываться или передаваться процессором целиком:

а) Кэш;
б) BIOS;
в) Разрядность;
г) Тактовая частота
д) Контроллер;
е) другое

5. В какой из последовательностей единицы измерения информации указаны в порядке возрастания:
а)байт, килобайт, мегабайт, бит;
б)килобайт, байт, бит, мегабайт;
в)байт, мегабайт, килобайт, гигабайт;
г)мегабайт, килобайт, гигабайт, байт;
д)байт, килобайт, мегабайт, гигабайт. е) другое.

6 .Винчестер предназначен для:

а) подключения периферийных узлов к магистрали;
б) управления работой ЭВМ по заданной программе;
в)хранения информации;

7 Память, используемая для хранения ьольших объемов информации:

а) оперативная память;
б) гибкий магнитный диск;
в) постоянная память (ПЗУ);

8. Микропроцессор имеет в своем составе:

а) устройство ввода;
б) внутренние регистры;
в) арифметико-логическое устройство;

9.Что можно отнести к правовым мерам ИБ?
а. Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства
б. охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра итд
в. Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, установку оборудования обнаружения и тушения пожара, оборудования обнаружения воды, принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое
г. охрану вычислительного центра, установку сигнализации и многое другое

10.Что можно отнести к организационным мерам ИБ?
а. Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского

законодательства, а также судопроизводства.
б.Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.
в. Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем.
г. Охрану работоспособности отдельных звеньев и организацию вычислительных сетей с возможностью перераспределения ресурсов.
д.Принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.
11. Под replay-атакой понимается:
1. модификация передаваемого сообщения
2. повторное использование переданного ранее сообщения
3. невозможность получения сервиса законным пользователем

12. 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

13К посторонним лицам нарушителям информационной безопасностиотносится:
1. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
2. персонал, обслуживающий технические средства;
3. технический персонал, обслуживающий здание;
4. пользователи;
5. сотрудники службы безопасности.
6. представители конкурирующих организаций.

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

15.. Перехват, который осуществляется путем использования оптической техники называется:
1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

16. К внутренним нарушителям информационной безопасности относится:

1. клиенты;
2. пользователи системы;
3. посетители;
4. любые лица, находящиеся внутри контролируемой территории;
5. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации.
6. персонал, обслуживающий технические средства.
7. сотрудники отделов разработки и сопровождения ПО;
8. технический персонал, обслуживающий здание

17. Анализ протоколируемой информации с целью оперативного выявления и предотвращения нарушений режима информационной безопасности – это?
1. Протоколирование
2. Экранирование
3. Аудит

18. Элемент аппаратной защиты, где используется экранирование, фильтрацию, заземление, электромагнитное зашумление, а также средства ослабления уровней нежелательных электромагнитных излучений.
а. защита от сбоев в электропитании
б. защита от сбоев серверов, рабочих станций и локальных компьютеров
в. защита от сбоев устройств для хранения информации
г. защита от утечек информации электромагнитных излучений

19.Какая из перечисленных атак на поток информации является пассивной:
а. перехват.
б. имитация.
в. модификация.
г. фальсификация.
д. прерывание.

20.Технические каналы утечки информации делятся на…
а. Все перечисленное
б. Акустические и виброакустические
в. Электрические
г. Оптические

21. Какой технический канал утечки отвечает за распространение звуковых колебаний в любом звукопроводящем материале или среде?
а. Акустические и виброакустические
б. Электрические
в. Оптические
г. Радиоканалы

22. Какой технический канал утечки отвечает за напряжение и токи в различных токопроводящих коммуникациях?
а. Акустические и виброакустические
б. Электрические
в. Оптические
г. Радиоканалы

23. Какой технический канал утечки отвечает за электромагнитные излучения радиодиапазона?
а. Акустические и виброакустические
б. Электрические
в. Оптические
г. Радиоканалы

24.Какой технический канал утечки отвечает за электромагнитные излучения в видимой,

инфракрасной и ультрафиолетовой частях спектра?
а. Акустические и виброакустические
б. Электрические
в. Оптические
г. Радиоканалы
25.По сведениям Media и PricewaterhouseCoopers, на чью долю приходится 60% всех инцидентов IT-безопасности?
а. Хакерские атаки
б. Различные незаконные проникновения
в. Инсайдеры
г. Технические компании

Критерии и методика оценивания:
Один тестовый вопрос (25 вопросов).
Модуль 1,2

- 1 балл выставляется студенту, если ответ правильный;
- 0 баллов выставляется студенту, если ответ неправильный.

Модуль 3,4

- 0,6 балла выставляется студенту, если ответ правильный;
- 0 баллов выставляется студенту, если ответ неправильный.

Типовые материалы к зачету

1. Системный подход как основа создания эффективной технической защиты информации
2. Использование физических эффектов в технических системах
3. Закономерности проявления физических эффектов
4. Закономерности технической реализации физических эффектов
5. Особенности построения физических схем
6. Базы данных по физическим эффектам
7. Классификация технических каналов утечки информации. Роль физических эффектов в образовании каналов утечки информации.
8. Классификация акустических каналов утечки информации
9. Прямой акустический канал
10. Акустовибрационный канал
11. Акустоэлектрический канал утечки информации
12. Акусторадиоэлектронный канал
13. Акустопараметрический канал
14. Акустооптический канал
15. Классификация электрических каналов утечки информации
16. Канал утечки информации по телефонной линии
17. Канал утечки информации по цепям электропитания
18. Канал утечки информации по цепям заземления
19. Классификация оптических каналов утечки информации

20. Системы обнаружения оптических устройств. Средства противодействия утечке информации по оптическим каналам.
21. Классификация электромагнитных каналов утечки информации
22. Методы и средства предотвращения утечки информации по радиотехническим каналам
23. Методы и средства контроля утечки информации по радиоканалам
24. Источники электромагнитных излучений и наводок
25. Использование эффектов: паразитных связей, электромагнитных наводок, с целью образования случайных антенн
26. Методы пассивной защиты информации от утечки через ПЭМИН
27. Методы активной защиты информации от утечки через ПЭМИН
28. Методы средства и контроля побочных электромагнитных излучений и наводок
29. Передача информации с помощью лазера
30. Структурные схемы образования комплексных каналов утечки информации

Критерии оценки (в баллах):

- «Зачтено» выставляется студенту, если он набрал по результатам изучения дисциплины 60 баллов;

- «Не зачтено» выставляется студенту, если он набрал менее 59 баллов.

Типовые материалы к экзамену

Вопросы к экзамену

1. Угрозы безопасности информации и меры по их предотвращению.
2. Видовые демаскирующие признаки объектов в видимом и инфракрасном диапазонах света.
3. Демаскирующие признаки аналоговых сигналов
4. Типовая структура технического канала утечки информации.
5. 1 Концепция и методы инженерно-технической защиты информации
6. Понятие экранирования. Основные положения
7. Контроль защищенности информации на объекте ВТ от утечки по каналу ПЭМИ.
8. Демаскирующие признаки дискретных сигналов
9. Технический контроль акустической защищенности выделенного помещения.
10. Материально-вещественный канал утечки информации. Способы восстановления информации на магнитных носителях.
11. Аттестация объектов информатизации. Мероприятия по выявлению и оценке свойств каналов утечки .
12. Технический контроль акустической защищенности выделенного помещения. Контроль технических средств и систем .
13. Принципы построения системы ТЗИ: равнопрочность рубежей, непрерывность, подконтрольность и гибкость системы защиты
14. Утечка информации по цепям электропитания
15. Технический контроль акустической защищенности выделенного помещения. Акустический и виброакустический контроль
16. Низкочастотные и высокочастотные излучения технических средств
17. Виды технических каналов утечки информации
18. Оптические каналы утечки информации

19. Скрытие и защита от утечки информации по акустическому и виброакустическому каналам.
20. Анализаторы линий и устройства контроля проводных линий
21. Демаскирующие признаки дискретных сигналов .
22. Электромагнитные излучения распределенных источников.
23. Виды технических каналов утечки информации
24. Оптические каналы утечки информации
25. Принципы построения системы ТЗИ: равнопрочность рубежей, непрерывность, подконтрольность и гибкость системы защиты
26. Утечка информации по цепям электропитания
27. Технический контроль акустической защищенности выделенного помещения.
28. Аттестация объектов информатизации
29. Концепция и методы инженерно-технической защиты информации
30. Понятие экранирования. Основные положения
31. Демаскирующие признаки аналоговых сигналов
32. Типовая структура технического канала утечки информации.
33. Принципы построения системы ТЗИ: многозональность и многорубежность
34. Способы защиты информации с помощью технологии Proximity и смарт-карт
35. Технические каналы утечки информации. Структура и классификация.
36. Электромагнитный канал утечки информации .
37. Методы выявления закладных устройств.
38. Пассивные методы защиты речевой информации от её утечки через ограждающие конструкции. Рекомендации по выбору ограждающих конструкций.
39. Активные методы и средства защиты речевой информации от утечки по техническим каналам, Характеристика генераторов шума.
40. Методы и средства защиты информации в телефонных линиях связи.

Экзаменационные билеты

Федеральное государственное бюджетное образовательное учреждение высшего образования
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Институт истории и государственного управления

Направление подготовки 10.03.01 «Информационная безопасность»
Дисциплина Техническая защита информации

1 Угрозы безопасности информации и меры по их предотвращению.
2 Видовые демаскирующие признаки объектов в видимом и инфракрасном диапазонах света.

Зав. кафедрой УИБ А.С. Исмагилова

Критерии оценивания компетенций (результатов)
и описание шкалы оценивания

При выставлении баллов за экзамен экзаменатор руководствуется следующими критериями:

25-30 баллов - студент дал полные, развернутые ответы на все теоретические вопросы билета, продемонстрировал знание функциональных возможностей, терминологии, основных элементов, умение применять теоретические знания. Студент без затруднений ответил на все дополнительные вопросы.

17-24 баллов - студент раскрыл в основном теоретические вопросы, однако допущены неточности в определении основных понятий. При ответе на дополнительные вопросы допущены небольшие неточности.

10-16 баллов - при ответе на теоретические вопросы студентом допущено несколько существенных ошибок в толковании основных понятий. Логика и полнота ответа страдают заметными изъянами. Заметны пробелы в знании основных методов. Теоретические вопросы в целом изложены достаточно, но с пропусками материала. Имеются принципиальные ошибки в логике построения ответа на вопрос

1-10 баллов - ответ на теоретические вопросы свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Обнаруживается отсутствие навыков применения теоретических знаний. Студент не смог ответить ни на один дополнительный вопрос.

.

Шкалы оценивания для экзамена:
от 45 до 59 баллов – «удовлетворительно»;
от 60 до 79 баллов – «хорошо»;
от 80 баллов – «отлично».

Тематика курсовых проектов

1. Разработка статистического классификатора системы обнаружения атак.
2. Принципы построения и функционирования аппаратных антивирусных средств.
3. Построение модели ситуационного управления защищенности информации в организации
4. Технические каналы утечки информации «типовых» объектов информатизации
5. Основные угрозы и меры по обеспечению безопасности информации по акустическому каналу утечки
6. Защита служебных кабинетов от утечки информации по акустическому каналу
7. Защита служебных кабинетов от утечки информации по виброакустическому каналу
8. Выявление акустических каналов утечки информации служебных кабинетов
9. Основные угрозы безопасности информации по электрическому каналу утечки
10. Выявление электрических каналов утечки информации служебных кабинетов
11. Защита служебных кабинетов от утечки информации по электрическому каналу
12. Основные угрозы безопасности информации по электромагнитному каналу утечки
13. Защита служебных кабинетов от утечки информации по электромагнитному каналу
14. Демаскирующие признаки применения специальной техники разведывательного назначения и методы их выявления
15. Поисковые приборы, используемые в сфере защиты информации
16. Контроль радиоэфира объекта информатизации Д
17. Поиск закладных устройств технических систем разведывательного назначения, находящихся в выключенном состоянии
18. Защита речевой информации в сетях оперативной связи ОВД
19. Основные методы и технические средства блокирования утечки информации по техническим каналам
20. Защита информации от несанкционированных воздействий
21. Защита информации от непреднамеренных воздействий
22. Методика проектирования систем ИТЗИ объектов информатизации

23. Система ИТЗИ «типового» служебного кабинета
24. Информационная безопасность и оборот технических средств разведывательного назначения и защиты информации
25. Методы повышение скрытности передачи информации в организации.
26. Методы защиты информации от утечки при передаче по открытым каналам.
27. Проектирование системы управления средствами защиты информации информационно-телекоммуникационных систем.
28. Оценка информационных рисков объекта информатизации и ее влияние на систему защиты информации.
29. Инженерно-техническая защита информации как сфера научной и практической деятельности.
30. Защита информации с помощью интегрированных систем охраны
31. Защита информации с помощью технических систем охранного телевидения
32. Защита информации с помощью технических систем управления доступом.
33. Защита информации с помощью технических систем охранно-пожарной сигнализации.
34. Защита информации с помощью инженерных средств

Критерии оценивания курсовой работы

Оценка «отлично»:

работа выполнена в полном объеме и изложена грамотным языком в определенной логической последовательности с точным использованием специализированной терминологии; показано уверенное владение прикладными программами.

Оценка «хорошо»:

работа выполнена в полном объеме, но имеет один из недостатков: в работе допущены один-два недочета при освещении основного содержания ответа; нет определенной логической последовательности, неточно используется специализированная терминология;

Оценка «удовлетворительно»:

работа выполнена неполно, не показано общее понимание вопроса, имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, при знании теоретического материала выявлена недостаточная сформированность основных умений и навыков.

Оценка «неудовлетворительно»

работа не выполнена или выполнена с грубейшими ошибками.

4.3. Рейтинг-план дисциплины (при необходимости)

Рейтинг–план дисциплины представлен в приложении 2.

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература:

1. Скрипник Д. А. Общие вопросы технической защиты информации: Учебная литература для ВУЗов [Электронный ресурс/ Москва: Национальный Открытый Университет «ИНТУИТ», 2016.- 425 стр. Режим доступа // http:// http://biblioclub.ru/index.php?page=book_red&id=429070&sr=1

2. Голиков А. М. Защита информации от утечки по техническим каналам: учебное пособие[Электронный ресурс] Томский государственный университет систем управления и радиоэлектроники, 2015. -256с. Режим доступа //http:/ http://biblioclub.ru/index.php?page=book_red&id=480636&sr=1

Дополнительная литература

3. Голиков А. М. Защита информации в инфокоммуникационных системах и сетях: учебное пособие [Электронный ресурс] Томский государственный университет систем управления и радиоэлектроники, 2015. -256с. Режим доступа //http:/ http://biblioclub.ru/index.php?page=book_red&id=480636&sr=1
4. Сердюк В. А. Организация и технологии защиты информации : обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие[Электронный ресурс] Москва: Издательский дом Высшей школы экономики, 2015 .-574с. -Режим доступа http://biblioclub.ru/index.php?page=book_red&id=440285&sr=1

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

1. Справочная правовая система «КонсультантПлюс» – http://www.consultant-plus.ru.
2. Электронная библиотечная система «Университетская библиотека онлайн» – https://biblioclub.ru.
3. Электронная библиотечная система издательства «Лань» – https://e.lanbook.com/
4. Электронный каталог Библиотеки БашГУ – http://www.bashlib.ru/catalogi/
5. www.fstec.ru –сайт ФСТЭК России
6. www.fsb.ru – сайт ФСБ России
7. http://window.edu.ru/ – Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам»;
8. http://univertv.ru/video/matematika/ – Открытый образовательный видеопортал UniverTV.ru. Образовательные фильмы на различные темы. Лекции в ведущих российских и зарубежных вузах. Научная конференция или научно-популярная лекция по интересующему вопросу);
9. www.newlibrary.ru – Новая электронная библиотека;
10. www. edu.ru – Федеральный портал российского образования;
11. www.elibrary.ru – Научная электронная библиотека;
12. www.nehudlit.ru – Электронная библиотека учебных материалов.
13. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные.
14. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
15. Система централизованного тестирования БашГУ (Moodle).GNU General Public License.

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

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения	
1. ***учебная аудитория для проведения занятий лекционного типа:*** аудитория № 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 лабораторных работ*****:** Лаборатория полигон технической защиты информации № 508 (гуманитарный корпус), компьютерный класс, аудитория 404 (гуманитарный корпус), аудитория 420 (гуманитарный корпус). **3** ***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	Лекции, практические занятия, лабораторные занятия, курсовое проектирование (выполнение курсовых работ), групповые и индивидуальные консультации, текущий контроль, промежуточная аттестация	**Аудитория № 403** Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 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 Lumien Master Pikture 153*203 Matte White Fiber Clas(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 LifeSize Icon 600-камера, интер-ая система со встроенным короткофокусным проектором Promethean ActivBoard 387 RPO MOUNT EST, профес-сиональный LCD дисплей Flame 42ST,	1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные. 2.Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные. 3. Система централизованного тестирования БашГУ (Moodle).GNU General Public License.

(гуманитарный корпус). **4.** ***учебная аудитория для текущего контроля и промежуточной 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). **5.** ***учебная аудитория для курсового проектирования (выполнения курсовых работ):***аудитория №613 (гуманитарный корпус). **6.** ***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). **7.** ***помещения для самостоятельной работы:*** читальный зал библиотеки аудитория 402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус). **8.*помещение для хранения***		настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса 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/Therm altake 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. **Лаборатория полигон технической защиты информации № 508** Учебная мебель, учебно-наглядные пособия, аудиторная доска трехсекционная, плакаты с тематикой технической защиты информации, комплекс мониторинга WiFi сетей "Зодиак II", универсальный комплект инструментов для проведения работ по специальным проверкам и специальным обследованиям Калейдоскоп-П2, многофункциональный поисковый прибор ST-031M "Пиранья", нелинейный локатор «Лорнет», анализатор электромагнитного поля "Кордон". **Аудитория № 523** Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт.	

и профилактического обслуживания учебного оборудования: аудитория № 523 (гуманитарный корпус).			

Приложение 1

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ
дисциплины **Техническая защита информации**
на 5 семестр

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	3 ЗЕТ / 108 часов
Учебных часов на контактную работу с преподавателем:	72,2
лекций	18
практических / семинарских	18
лабораторных работ	36
Других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) ФКР	0,2
Учебных часов на самостоятельную работу обучающихся, включая подготовку к зачету	35,8

Форма контроля:
Зачет 5 семестр

на 6 семестр

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	4 ЗЕТ / 144 часов
Учебных часов на контактную работу с преподавателем:	67,2
лекций	16
практических / семинарских	32
лабораторных работ	16
Других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) ФКР	3,2

Учебных часов на самостоятельную работу обучающихся, включая подготовку к экзамену	33 43,8

Форма контроля:
Экзамен 6 семестр
В том числе: курсовой проект 6 семестр, контактных часов – 2.часов на самостоятельную работу - 20

5 семестр

	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	3	4	5	6	7	8	9
1	Модуль 1,2. Объекты информационной защиты	4	2	-	6	Основная 1, 2 Дополнительная 3,4	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Опрос, практические задания, тестирование
2	Нормативно-правовые аспекты технической защиты информации	4	4	6	6	Основная 1, 2 Дополнительная 3,4	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников. Выполнение практической работы	Опрос, практические задания, тестирование, лабораторные задания
3	Основные свойства информации как предмета технической	2	2	6	6	Основная 1, 2 Дополнительная 3,4	Самостоятельное изучение рекомендуемой основной и дополнительной	Опрос, практические задания, тестирование, лабораторные

	защиты						литературы, интернет-источников. Выполнение практической работы	задания
4	Источники и носители конфиденциальной информации	2	4	6	6	Основная 1, 2 Дополнительная 3,4	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников. Выполнение практической работы	Опрос, практические задания, тестирование, лабораторные задания
5	Виды угроз безопасности информации	2	2	6	3	Основная 1, 2 Дополнительная 3,4	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников. Выполнение практической работы	Опрос, практические задания, тестирование, лабораторные задания
6	Способы технической защиты информации	2	2	6	3	Основная 1, 2 Дополнительная 3,4	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников. Выполнение практической работы	Опрос, практические задания, тестирование, лабораторные задания
7	Средства технической защиты	2	2	6	5,8	Основная 1, 2 Дополнительная 3,4	Самостоятельное изучение рекомендуемой	Опрос, практические задания,

	информации						основной и дополнительной литературы, интернет-источников.	тестирование, лабораторные задания
	Всего	18	18	36	35,8			

6 семестр

	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	3	4	5	6	7	8	9
8	Модуль3,4 Способы и средства предотвращения утечки информации через побочные электромагнитные излучения и наводки	2	4	2	7	Основная 1, 2 Дополнительная 3,4	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников. Выполнение практической работы	Опрос, практические задания, тестирование, лабораторные задания
9	Способы предотвращения утечки информации по	4	8	4	7	Основная 1, 2 Дополнительная 3,4	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-	Опрос, практические задания, тестирование,

	материально-вещественному каналу						источников.	лабораторные задания
10	Общие положения по технической защите информации в организации информации в организации	2	4	2	7	Основная 1, 2 Дополнительная 3,4	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников. Выполнение практической работы	Опрос, практические задания, тестирование, лабораторные задания
11	Организационные меры по технической защите	4	8	4	7	Основная 1, 2 Дополнительная 3,4	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников. Выполнение практической работы	Опрос, практические задания, тестирование, лабораторные задания
12	Технические меры по технической защите информации в организации	4	8	4	5	Основная 1, 2 Дополнительная 3,4	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Опрос, практические задания, тестирование, лабораторные задания
	Всего	16	32	16	33			
	Курсовой проект					Основная 1, 2 Дополнительная 3,4	Структуризация и усвоение полученных во время изучения предмета, знаний, навыков и умений.	

Приложение 2

Рейтинг – план дисциплины
Техническая защита информации

Направление подготовки 10.03.01 «Информационная безопасность»
Курс 3, семестр 5

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1				
Текущий контроль			0	25
1. Аудиторная работа	3	4	0	12
2. Лабораторные работы	3,25	4	0	13
Рубежный контроль				25
1. Тестовые задания	1	25	0	25
Всего			0	50
Модуль 2				
Текущий контроль			0	25
1. Аудиторная работа	3	4	0	12
2. Лабораторные работы	3,25	4	0	13
Рубежный контроль				25
1. Тестовые задания	1	25	0	25
Всего			0	50
Поощрительные баллы				
1. Студенческая олимпиада			0	3
2. Публикация статей			0	3
3. Участие в конференции			0	4
Всего				10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий				-6
2. Посещение практических занятий				-10
Итоговый контроль				
Зачет			0	

Рейтинг – план дисциплины
Техническая защита информации

Направление подготовки 10.03.01 «Информационная безопасность»
Курс 3, семестр 6

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 3				
Текущий контроль			0	20
1. Аудиторная работа	2,5	4	0	10
2. Лабораторные работы	2,5	4	0	10
Рубежный контроль				15
1. Тестовые задания	0,6	25	0	15
Всего			0	35
Модуль 4				
Текущий контроль			0	20
1. Аудиторная работа	2,5	4	0	10
2. Лабораторные работы	2,5	4	0	10
Рубежный контроль				15
1. Тестовые задания	0,6	25	0	15
Всего			0	35
Поощрительные баллы				
1. Студенческая олимпиада			0	3
2. Публикация статей			0	3
3. Участие в конференции			0	4
Всего				10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
3. Посещение лекционных занятий				-6
4. Посещение практических занятий				-10
Итоговый контроль				
Экзамен			0	30