Составители: И.В.Салов, Ф.Т.Байрушин

Рабочая программа дисциплины актуализирована на заседании кафедры управления информационной безопасностью протокол №10от «7» июня 2018 г.

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

Заведующий кафедрой _____/ _____Ф.И.О/

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

Заведующий кафедрой _____/ __Ф.И.О/

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

Заведующий кафедрой _____/ _____Ф.И.О/

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

Заведующий кафедрой _____/ _____Ф.И.О/

Список документов и материалов

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных спланируемыми результатами освоения образовательной программы

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

Результаты обучения		Формируемая компетенция (с указанием кода)	Примечание
Знания	Знать место и роль профессии в системе национальной безопасности РФ, социальные ценности общества и их связь с социальной значимостью своей будущей профессии, основные виды социальных организаций и способы взаимодействия в них, основные задачи своей профессии в соответствии с нормами морали, профессиональной этики и служебного этикета	ОК-4: Способность выполнять профессиональные задачи в соответствии с нормами морали, профессиональной этики и служебного этикета	Контроль-тестирование, экзамен
	Знать аппаратные средства вычислительной техники; операционные системы персональных ЭВМ; основы администрирования вычислительных сетей; системы управления БД, эксплуатационные и технико-экономические характеристики программных и технических средств защиты информации и обеспечения информационной безопасности, типы технических и программно-аппаратных средств обработки и защиты информации, основные направления политик защиты информации на предприятии (организации)	ПК-2: Способность применять технические и программно-аппаратные средства обработки и защиты информации	Контроль-тестирование, экзамен

	Знать правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, системы организации бумажного и электронного конфиденциального делопроизводства	ПК-4: Способность участвовать в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации	Контроль-тестирование, экзамен
	Знать аппаратные средства вычислительной техники; операционные системы персональных ЭВМ; основы администрирования вычислительных сетей; системы управления БД, эксплуатационные и технико-экономические характеристики технических средств защиты информации и обеспечения информационной безопасности, типы технических средств обработки и защиты информации, основные направления политик защиты информации на предприятии (организации)	ПК-5: Способность осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния	Контроль-тестирование, экзамен
	Знать нормативно-правовые документы по обеспечению информационной безопасности в нашей стране и за рубежом, стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов,	ПСК-3: Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	Контроль-тестирование, экзамен

	методики анализа рисков информационных систем		
Умения	Уметь осознавать социальную значимость своей профессии,находить баланс между интересами личности, общества и государства,соблюдать нормы профессиональной этики	ОК-4: Способность выполнять профессиональные задачи в соответствии с нормами морали, профессиональной этики и служебного этикета	Контроль-тестирование, экзамен
	Уметь формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе,осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты,выполнять работы по установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации	ПК-2: Способность применять технические и программно-аппаратные средства обработки и защиты информации	Контроль-тестирование, экзамен
	Уметь выбирать тип необходимых средств для выявления наличия электронных средств перехвата информации,применять на практике методы локальной и комплексной автоматизации процессов обработки документов в документационной службе,разрабатывать организационно-распорядительные документы по вопросам защиты информации	ПК-4: Способность участвовать в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации	Контроль-тестирование, экзамен

	Уметь формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе,осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных аппаратных средств защиты информации,выполнять работы по установке, конфигурированию и эксплуатации компонентов технических систем обеспечения информационной безопасности и защиты информации	ПК-5: Способность осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния	Контроль-тестирование, экзамен
	Уметьинтерпретировать и обобщать данные, формулировать выводы и рекомендации,применять на практике методы обработки данных,разрабатывать и реализовывать решения, направленные на поддержку социально-значимых проектов и развитие компьютерного творчества	ПСК-3: Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	Контроль-тестирование, экзамен
Владения (навыки / опыт деятельности)	Владеть пониманием социологического аспекта профессионализации и высокой мотивацией к выполнению профессиональной деятельности, навыками творческого мышления для выполнения профессиональных задач в области обеспечения безопасности информационных технологий и защиты	ОК-4: Способность выполнять профессиональные задачи в соответствии с нормами морали, профессиональной этики и служебного этикета	Контроль-тестирование, экзамен

	интересов личности, общества и государства		
	Владеть методами оценки, тестирования. настройки на применение средств программно-технического обеспечения защиты информации	ПК-2: Способность применять технические и программно-аппаратные средства обработки и защиты информации	Контроль-тестирование, экзамен
	Владеть навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации,методами сбора и анализа исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности	ПК-4: Способность участвовать в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации	Контроль-тестирование, экзамен
	Владетьметодами оценки, тестирования. настройки и применения компонентов технических систем обеспечения защиты информации	ПК-5: Способность осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния	Контроль-тестирование, экзамен
	Владетьинтерпретации и обобщения результатов, формулирования рекомендаций и принятия решений,методологией и навыками решения научных и практических задач	ПСК-3: Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	Контроль-тестирование, экзамен

2. Место дисциплины в структуре образовательной программы

Дисциплина «Программно-аппаратная защита информации» относится к дисциплинам базовой частиобразовательной программы.

Дисциплина изучается на 3-емкурсе в 6 семестре.

Цель изучения дисциплины: формирование у специалистов целостного представления об программно-аппаратных средствахзащиты информации.

Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин:

Математика,

Средства вычислительной техники,

Аппаратные средства вычислительной техники,

Средства и системы технического обеспечения обработки, хранения и передачи информации.

Эти дисциплины направлены на формирование компетенций ОК-4, ПК-2, ПК-4, ПК-5, ПСК-3.

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

Содержание рабочей программы представлено в Приложении 1.

4. Фонд оценочных средств по дисциплине

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

ОК-4: Способность выполнять профессиональные задачи в соответствии с нормами морали, профессиональной этики и служебного этикета.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать место и роль профессии в системе национальной безопасности РФ	Не знает	Имеет фрагментарные знания о месте и роли профессии в системе национальной безопасности РФ	В целом знает основные понятия о месте и роли профессии в системе национальной безопасности РФ	Демонстрирует целостные знания о месте и роли профессии в системе национальной безопасности РФ
	Знать социальные ценности общества и их связь с социальной значимостью своей будущей профессии	Не знает	Имеет фрагментарные знания о социальных ценностях общества и их связи с социальной значимостью своей будущей профессии	В целом знает основные социальные ценности общества и их связь с социальной значимостью своей будущей профессии	Демонстрирует целостные знания о социальных ценностях общества и их связи с социальной значимостью своей будущей профессии
	Знать основные виды социальных организаций и способы взаимодействия в них	Не знает	Имеет фрагментарные знания о основных видах социальных организаций и способы взаимодействия в них	В целом знает некоторые элементы основных видов социальных организаций и способы взаимодействия в них	Демонстрирует целостные знания о основных видах социальных организаций и способы взаимодействия в них
	Знать основные задачи своей профессии в соответствии с нормами морали, профессиональной этики и служебного этикета	Не знает	Имеет фрагментарные знания о основных задачах своей профессии в соответствии с нормами морали, профессиональной этики и служебного этикета	В целом знает некоторые элементы основных задач своей профессии в соответствии с нормами морали, профессиональной этики и служебного этикета	Демонстрирует целостные знания о основных задачах своей профессии в соответствии с нормами морали, профессиональной этики и служебного этикета
Второй этап (уровень)	Уметь осознавать социальную значимость своей профессии	Не умеет	Умеет осознавать социальную значимость своей профессии, но допускает значительные ошибки	Умеет осознавать социальную значимость своей профессии, но допускает незначительные ошибки	Умеет осознавать социальную значимость своей профессии
	Уметь находить баланс между интересами личности, общества и государства	Не умеет	Умеет находить баланс между интересами личности, общества и государства, но допускает значительные ошибки	Умеет находить баланс между интересами личности, общества и государства, но допускает незначительные ошибки	Умеет находить баланс между интересами личности, общества и государства

	Уметь соблюдать нормы профессиональной этики	Не умеет	Умеет соблюдать нормы профессиональной этики, но допускает значительные ошибки	Умеет соблюдать нормы профессиональной этики, но допускает незначительные ошибки	Умеет соблюдать нормы профессиональной этики
Третий этап (уровень)	Владеть пониманием социологического аспекта профессионализации и высокой мотивацией к выполнению профессиональной деятельности	Не владеет	Недостаточно понимает социологический аспект профессионализации и высокой мотивацией к выполнению профессиональной деятельности	Понимает основные моменты социологического аспекта профессионализации и высокой мотивацией к выполнению профессиональной деятельности	Способен использовать социологический аспект профессионализации и высокой мотивацией к выполнению профессиональной деятельности
	Владеть навыками творческого мышления для выполнения профессиональных задач в области обеспечения безопасности информационных технологий и защиты интересов личности, общества и государства	Не владеет	Недостаточно владеет навыками творческого мышления для выполнения профессиональных задач в области обеспечения безопасности информационных технологий и защиты интересов личности, общества и государства	Владеет отдельными навыками творческого мышления для выполнения профессиональных задач в области обеспечения безопасности информационных технологий и защиты интересов личности, общества и государства	Способен использовать навыки творческого мышления для выполнения профессиональных задач в области обеспечения безопасности информационных технологий и защиты интересов личности, общества и государства

ПК-2: Способность применять технические и программно-аппаратные средства обработки и защиты информации.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать аппаратные средства вычислительной техники; операционные системы персональных ЭВМ, администрирования вычислительных сетей; системы управления БД	Не знает	Имеет фрагментарные знания оаппаратных средствах вычислительной техники; операционных системах персональных ЭВМ; основах администрирования вычислительных сетей; системы управления БД	Знает основы аппаратных средств вычислительной техники; операционных систем персональных ЭВМ, администрирования вычислительных сетей; системы	Знает аппаратные средства вычислительной техники; операционные системы персональных ЭВМ, администрирования вычислительных сетей; системы управления БД

	Знать эксплуатационные и технико-экономические характеристики программных и технических средств защиты информации и обеспечения информационной безопасности	Не знает	Имеет фрагментарные знания оэксплуатационных и технико-экономических характеристиках программных и технических средств защиты информации и обеспечения информационной безопасности	Знает основыэксплуатационных и технико-экономических характеристик программных и технических средств защиты информации и обеспечения информационной безопасности	Знает эксплуатационные и технико-экономические характеристики программных и технических средств защиты информации и обеспечения информационной безопасности
	Знать типы технических и программно-аппаратных средств обработки и защиты информации	Не знает	Имеет фрагментарные знания о типах технических и программно-аппаратных средств обработки и защиты информации	Знает основныетипы технических и программно-аппаратных средств обработки и защиты информации	Знает типы технических и программно-аппаратных средств обработки и защиты информации
	Знать основные направления политик защиты информации на предприятии (организации)	Не знает	Имеет фрагментарные знания оосновных направлениях политик защиты информации на предприятии (организации)	Знает некоторыеосновные направления политик защиты информации на предприятии (организации)	Знает основные направления политик защиты информации на предприятии (организации)
Второй этап (уровень)	Уметь формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе	Не умеет	Допускает значительные ошибки при формулировании и настройке политик безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе	Допускает незначительные ошибки при формулировании и настройке политик безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе	Имеет навыки формулировании и настройки политик безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе
	Уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	Не умеет	Допускает значительные ошибки при осуществлении мер противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	Допускает незначительные ошибки при осуществлении мер противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	Имеет навыки осуществления мер противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты
	Уметь выполнять работы по установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации	Не умеет	Допускает значительные ошибки при выполнении работ по установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации	Допускает незначительные ошибки при выполнении работ по установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации	Имеет навыки выполнения работ по установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации

Третий этап (уровень)	Владеть методами оценки, тестирования, настройки на применение средств программно-технического обеспечения защиты информации	Не владеет	Недостаточно владеет методами оценки, тестирования, настройки на применение средств программно-технического обеспечения защиты информации	Владеет отдельными методами оценки, тестирования, настройки на применение средств программно-технического обеспечения защиты информации	Владеет методами оценки, тестирования, настройки на применение средств программно-технического обеспечения защиты информации

ПК-4: Способность участвовать в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации	Не знает	Имеет фрагментарные знания о правовых нормах и стандартах по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации	Знает основные правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации	Знает правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации
	Знать правовые основы организации защиты государственной тайны и конфиденциальной информации, системы организации бумажного и электронного конфиденциального делопроизводства	Не знает	Имеет фрагментарные знания оправовых основах организации защиты государственной тайны и конфиденциальной информации, системы организации бумажного и электронного конфиденциального делопроизводства	Знает основные правовые основы организации защиты государственной тайны и конфиденциальной информации, системы организации бумажного и электронного конфиденциального делопроизводства	Знает правовые основы организации защиты государственной тайны и конфиденциальной информации, системы организации бумажного и электронного конфиденциального делопроизводства
Второй этап (уровень)	Уметь выбирать тип необходимых средств для выявления наличия электронных средств перехвата информации	Не умеет	Допускает значительные ошибки при выборе типа необходимых средств для выявления наличия электронных средств перехвата информации	Допускает незначительные ошибки при выборе типа необходимых средств для выявления наличия электронных средств перехвата информации	Имеет навыки выбора типа необходимых средств для выявления наличия электронных средств перехвата информации
	Уметь применять на практике методы локальной и комплексной автоматизации процессов обработки документов в документационной службе	Не умеет	Допускает значительные ошибки при применении на практике методов локальной и комплексной автоматизации процессов обработки документов в документационной службе	Допускает незначительные ошибки при применении на практике методов локальной и комплексной автоматизации процессов обработки документов в документационной службе	Умеет применять на практике методы локальной и комплексной автоматизации процессов обработки документов в документационной службе

	Уметь разрабатывать организационно-распорядительные документы по вопросам защиты информации	Не умеет	Допускает значительные ошибки при разработке организационно-распорядительных документов по вопросам защиты информации	Допускает незначительные ошибки при разработке организационно-распорядительных документов по вопросам защиты информации	Имеет навыки работы по разработке организационно-распорядительных документов по вопросам защиты информации
Третий этап (уровень)	Владеть навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации	Не владеет	Недостаточно владеет навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации	Владеет отдельными навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации	Владеет навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации
	Владеть методами сбора и анализа исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности	Не владеет	Недостаточно владеетметодами сбора и анализа исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности	Владеет отдельными методами сбора и анализа исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности	Владеетметодами сбора и анализа исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности

ПК-5: Способность осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать аппаратные средства вычислительной техники; операционные системы персональных ЭВМ; основы администрирования вычислительных сетей; системы управления БД	Не знает	Имеет фрагментарные знания оаппаратных средствах вычислительной техники; операционных системах персональных ЭВМ	Знает основные аппаратные средства вычислительной техники; операционные системы персональных ЭВМ	Знает аппаратные средства вычислительной техники; операционные системы персональных ЭВМ; основы администрирования вычислительных сетей; системы управления БД

	Знать эксплуатационные и технико-экономические характеристики программных и технических средств защиты информации и обеспечения информационной безопасности	Не знает	Имеетфрагментарные знания о эксплуатационных и технико-экономических характеристик программных и технических средств защиты информации и обеспечения информационной безопасности	Знает основные эксплуатационные и технико-экономические характеристики программных и технических средств защиты информации и обеспечения информационной безопасности;	Знает эксплуатационные и технико-экономические характеристики программных и технических средств защиты информации и обеспечения информационной безопасности;
	Знать типы технических и программно-аппаратных средств обработки и защиты информации	Не знает	Имеетфрагментарные знания отипахтехнических и программно-аппаратных средств обработки и защиты информации	Знает основные типы технических и программно-аппаратных средств обработки и защиты информации	Знает типы технических и программно-аппаратных средств обработки и защиты информации
	Знать основные направления политик защиты информации на предприятии (организации)	Не знает	Имеетфрагментарные знания о основных направлениях политик защиты информации на предприятии (организации)	Знает основные направления политик защиты информации на предприятии (организации)	Знает направления политик защиты информации на предприятии (организации)
Второй этап (уровень)	Уметь формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе	Не умеет	Допускает значительные ошибкипри разработке инновационных методов, средств и технологий в области логистической деятельности	Допускает незначительные ошибки при разработке инновационных методов, средств и технологий в области логистической деятельности	Имеет навыки разработки инновационных методов, средств и технологий в области логистической деятельности
	Уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	Не умеет	Допускает значительные ошибкиприосуществлении мер противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	Допускает незначительные ошибки приосуществлении мер противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	Имеет навыкиосуществлении мер противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты
	Уметь выполнять работы по установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации	Не умеет	Допускает значительные ошибкипривыполнении работ по установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации	Допускает незначительные ошибки привыполнении работ по установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации	Имеет навыкиработы по установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации
Третий этап (уровень)	Владеть методами оценки, тестирования.настройки на применение средств программно-технического обеспечения защиты информации	Не владеет	Недостаточно владеет методами оценки, тестирования.настройки на применение средств программно-технического обеспечения защиты информации	Владеет отдельными методами оценки, тестирования.настройки на применение средств программно-технического обеспечения защиты информации	Владеет методами оценки, тестирования.настройки на применение средств программно-технического обеспечения защиты информации

ПСК-3: Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно	4 («Хорошо»)	5 («Отлично»)

	достижения заданного уровня освоения компетенций)		»)		
Первый этап (уровень)	Знать нормативно-правовые документы по обеспечению информационной безопасности в нашей стране и за рубежом	Не знает	Имеет фрагментарные знания о нормативно-правовых документах по обеспечению информационной безопасности в нашей стране и за рубежом	Знает основные нормативно-правовые документы по обеспечению информационной безопасности в нашей стране и за рубежом	Знает нормативно-правовые документы по обеспечению информационной безопасности в нашей стране и за рубежом
	Знать стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов	Не знает	Имеет фрагментарные знания о стандартах построения систем информационной безопасности и стандартах оценки степени защиты систем информационной безопасности объектов	Знает основные стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов	Знает стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов
	Знать методики анализа рисков информационных систем	Не знает	Имеет фрагментарные знания о методиках анализа рисков информационных систем	Знает основныеметодики анализа рисков информационных систем	Знает методики анализа рисков информационных систем
Второй этап (уровень)	Уметь интерпретировать и обобщать данные, формулировать выводы и рекомендации	Не умеет	Допускает значительные ошибки при интерпретации и обобщении данных, формулировании выводов и рекомендаций	Допускает незначительные ошибки при интерпретации и обобщении данных, формулировании выводов и рекомендаций	Имеет навыки интерпретации и обобщения данных, формулирования выводов и рекомендаций
	Уметь применять на практике методы обработки данных	Не умеет	Допускает значительные ошибки при применении на практике методов обработки данных	Допускает незначительные ошибки при применении на практике методов обработки данных	Умеет применять на практике методы обработки данных
	Уметь разрабатывать и реализовывать решения, направленные на поддержку социально-значимых проектов и развитие компьютерного творчества	Не умеет	Допускает значительные ошибки при разработке и реализации решений, направленных на поддержку социально-значимых проектов и развитие компьютерного творчества	Допускает незначительные ошибки при разработке и реализации решений, направленных на поддержку социально-значимых проектов и развитие компьютерного творчества	Имеет навыки работы по разработке и реализации решений, направленных на поддержку социально-значимых проектов и развитие компьютерного творчества
Третий этап (уровень)	Владеть навыками интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений	Не владеет	Недостаточно владеет навыками интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений	Владеет отдельными навыками интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений	Владеет навыками интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений
	Владеть методологией и навыками решения научных и практических задач	Не владеет	Недостаточно владеетметодологией и навыками решения научных и практических задач	Владеет отдельными методами и навыками решения научных и практических задач	Владеетметодами и навыками решения научных и практических задач

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

перечисленных в рейтинг-плане дисциплины, для экзамена:текущий контроль – максимум 40 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10.

Шкалы оцениваниядля экзамена:

от 45 до 59 баллов – «удовлетворительно»;

от 60 до 79 баллов – «хорошо»;

от 80 баллов – «отлично».

4.2. Типовые контрольные задания или иные материалы, необходимые для 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	Знать место и роль профессии в системе национальной безопасности РФ, социальные ценности общества и их связь с социальной значимостью своей будущей профессии, основные виды социальных организаций и способы взаимодействия в них, основные задачи своей профессии в соответствии с нормами морали, профессиональной этики и служебного этикета	ОК-4: Способность выполнять профессиональные задачи в соответствии с нормами морали, профессиональной этики и служебного этикета	тестирование, практическое задание
	Знать аппаратные средства вычислительной техники; операционные системы персональных ЭВМ; основы администрирования вычислительных сетей; системы управления БД, эксплуатационные и технико-экономические характеристики программных и технических средств защиты информации и обеспечения	ПК-2: Способность применять технические и программно-аппаратные средства обработки и защиты информации	тестирование, практическое задание

	информационной безопасности, типы технических и программно-аппаратных средств обработки и защиты информации, основные направления политик защиты информации на предприятии (организации)		
	Знать правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, системы организации бумажного и электронного конфиденциального делопроизводства	ПК-4: Способность участвовать в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации	тестирование, практическое задание
	Знать аппаратные средства вычислительной техники; операционные системы персональных ЭВМ; основы администрирования вычислительных сетей; системы управления БД, эксплуатационные и технико-экономические характеристики технических средств защиты информации и обеспечения информационной безопасности, типы технических средств обработки и защиты информации, основные направления политик защиты информации на предприятии (организации)	ПК-5: Способность осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния	тестирование, практическое задание
	Знать нормативно-	ПСК-3: Способность	тестирование,

	правовые документы по обеспечению информационной безопасности в нашей стране и за рубежом, стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов, методики анализа рисков информационных систем	проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	практическое задание
2-й этап Умения	Уметь осознавать социальную значимость своей профессии,находить баланс между интересами личности, общества и государства,соблюдать нормы профессиональной этики	ОК-4: Способность выполнять профессиональные задачи в соответствии с нормами морали, профессиональной этики и служебного этикета	тестирование, практическое задание
	Уметь формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе,осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты,выполнять работы по установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации	ПК-2: Способность применять технические и программно-аппаратные средства обработки и защиты информации	тестирование, практическое задание
	Уметь выбирать тип необходимых средств для выявления наличия электронных средств перехвата	ПК-4: Способность участвовать в аттестационных испытаниях и аттестации объектов, помещений,	тестирование, практическое задание

	информации,применять на практике методы локальной и комплексной автоматизации процессов обработки документов в документационной службе,разрабатывать организационно-распорядительные документы по вопросам защиты информации	технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации	
	Уметь формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе,осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных аппаратных средств защиты информации,выполнять работы по установке, конфигурированию и эксплуатации компонентов технических систем обеспечения информационной безопасности и защиты информации	ПК-5: Способность осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния	тестирование, практическое задание
	Уметьинтерпретировать и обобщать данные, формулировать выводы и рекомендации,применять на практике методы обработки данных,разрабатывать и реализовывать решения, направленные на поддержку социально-значимых проектов и развитие компьютерного творчества	ПСК-3: Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	тестирование, практическое задание

3-й этап Владения навыками	Владеть пониманием социологического аспекта профессионализации и высокой мотивацией к выполнению профессиональной деятельности, навыками творческого мышления для выполнения профессиональных задач в области обеспечения безопасности информационных технологий и защиты интересов личности, общества и государства	ОК-4: Способность выполнять профессиональные задачи в соответствии с нормами морали, профессиональной этики и служебного этикета	тестирование, практическое задание
	Владеть методами оценки, тестирования. настройки на применение средств программно-технического обеспечения защиты информации	ПК-2: Способность применять технические и программно-аппаратные средства обработки и защиты информации	тестирование, практическое задание
	Владеть навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации,методами сбора и анализа исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности	ПК-4: Способность участвовать в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации	тестирование, практическое задание
	Владетьметодами оценки, тестирования. настройки и применения компонентов технических систем обеспечения защиты информации	ПК-5: Способность осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния	тестирование, практическое задание

	Владетьинтерпретации и обобщения результатов, формулирования рекомендаций и принятия решений,методологией и навыками решения научных и практических задач	ПСК-3: Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	тестирование, практическое задание

Экзамен

Структура экзаменационного билета

Экзаменационный билет состоит из двух вопросов, отражающих соответственно материал первого и второго модуля.

Экзаменационные материалы

1. Основные понятия и определения в области создания ПАСОИБ.
2. Нормативно-правовая база создания ПАСОИБ.
3. Анализ угроз информационной безопасности.
4. Анализ сетевых угроз информационной безопасности.
5. Классификация ПАСОИБ.
6. Функциональные возможности ПАСОИБ.
7. Принципы разработки ПАСОИБ.
8. Концепция диспетчера доступа.
9. Основные этапы проектирования ПАСОИБ.
10. Классификация функциональных требований по защите информации и данных.
11. Принципы действия и технологические особенности программно-аппаратных средств, реализующих отдельные функциональные требования по защите информации и данных и их взаимодействие с общесистемными компонентами вычислительных систем.
12. Методы обеспечения идентификации и аутентификации.
13. Методы криптографической защиты.
14. Методы и средства хранения ключевой информации.
15. Методы и средства ограничения доступа к компонентам вычислительных систем.
16. Характеристика методов и средства привязки программного обеспечения к аппаратному кружению и физическим носителям.
17. Методы аудита безопасности.
18. Методы обеспечения доступа к системе защиты и управления безопасностью.
19. Методы обеспечения целостности системы защиты.
20. Классификация аппаратных компонентов средств защиты программ.
21. Классификация программных компонентов средств защиты программ.
22. Структура программного обеспечения.
23. Способы встраивания средств защиты в программное обеспечение.
24. Способы определения факта незаконного использования программ.
25. Способы защиты программ от незаконного использования.
26. Способы изучения кода программ.
27. Способы защиты программ от изучения кода.
28. Основные принципы обеспечения безопасности программ.
29. Изолированная программная среда.

30. Классификация программно-аппаратных средств защиты от несанкционированного доступа к информации, хранимой в ПЭВМ.
31. Характеристики программно-аппаратных средств защиты от несанкционированного доступа к информации, хранимой в ПЭВМ.
32. Понятие электронного замка.
33. Принципы построения и функционирования электронных замков.
34. Механизмы контроля аппаратной конфигурации ПЭВМ.
35. Общие принципы разграничения доступа пользователей к устройствам ПЭВМ.
36. Основные принципы криптографической защиты информации.
37. Классификация программно-аппаратных средств защиты информации в сетях передачи данных.
38. Принципы построения и функционирования межсетевых экранов в сетях передачи данных.
39. Программно-аппаратные средства межсетевого экранирования.
40. Основные принципы защиты информации при передаче по каналам связи.
41. Программно-аппаратные средства защиты информации при передаче по каналам связи.
42. Основные принципы разграничения доступа к сетевым ресурсам.
43. Основные принципы обнаружения сетевых атак.
44. Программно-аппаратные средства обнаружения сетевых атак.
45. Основные принципы защиты от сетевых атак.
46. Программно-аппаратные средства защиты от сетевых атак.
47. Основные принципы управления безопасностью сети.
48. Программно-аппаратные средства управления безопасностью сети.
49. Обзор штатных средств сетевого оборудования, предназначенных для защиты информации при передаче по каналам связи.
50. Способы применения штатных средств сетевого оборудования, предназначенных для защиты информации при передаче по каналам связи.
51. Основные требования к информационной безопасности.
52. Задачи сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности.
53. Технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности.
54. Классификация требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности.
55. Проверка ОИ на базе вычислительной техники.
56. Электронный документ (ЭД). Понятие ЭД. Типы ЭД.
57. Виды информации в КС. Информационные потоки в КС. Понятие исполняемого модуля.
58. Уязвимость компьютерных систем. Понятие доступа, субъект и объект доступа.
59. Понятие несанкционированного доступа (НСД), классы и виды НСД. Несанкционированное копирование программ как особый вид НСД.
60. Понятие злоумышленника; злоумышленник в криптографии и при решении проблем компьютерной безопасности (КБ).
61. Политика безопасности в компьютерных системах. Оценка защищенности.
62. Способы защиты конфиденциальности, целостности и доступности в КС.
63. Руководящие документы Гостехкомиссии по оценке защищенности от НСД.
64. Понятие идентификации пользователя. Задача идентификации пользователя. Понятие протокола идентификации. Локальная и удаленная

идентификация. Идентифицирующая информация (понятие, способы хранения, связь с ключевыми системами).

65. Файл как объект доступа. Оценка надежности систем ограничения доступа – сведение к задаче оценки стойкости.
66. Организация доступа к файлам. Иерархический доступ к файлам. Понятие атрибутов доступа. Организация доступа к файлам различных ОС.
67. Защита сетевого файлового ресурса на примерах организации доступа в различных ОС.
68. Способы фиксации факторов доступа. Журналы доступа и критерии их информативности.
69. Выявление следов несанкционированного доступа к файлам, метод инициированного НСД.
70. Доступ данных со стороны процесса (понятие; отличия от доступа со стороны пользователя).
71. Построение программно-аппаратных комплексов шифрования.
72. Аппаратные и программно-аппаратные средства криптозащиты данных. Построение аппаратных компонент криптозащиты данных, специализированные СБИС как носителя алгоритма шифрования.
73. Защита алгоритма шифрования; принцип чувствительной области и принцип главного ключа.
74. Необходимые и достаточные функции аппаратного средства криптозащиты. Проектирование модулей криптопреобразований на основе сигнальных процессов.
75. Классификация защищаемых компонент ПЭВМ: отчуждаемые и неотчуждаемые компоненты ПЭВМ.
76. Процесс начальной загрузки ПЭВМ, взаимодействие аппаратной и программной частей. Механизмы расширения BIOS. Преимущества и недостатки программных и аппаратных средств.
77. Способы защиты информации на съемных дисках. Организация прозрачного режима шифрования.
78. Магнитные диски прямого доступа.
79. Магнитные и интеллектуальные карты.
80. Средство TouchMemory.
81. Способы изучения ПО: статистическое и динамическое изучение. Роль программной и аппаратной среды.
82. Временная надежность (невозможность обеспечения гарантированной надежности).
83. Задачи защиты от изучения и способы их решения.
84. Защита от отладки: итеративный программный замок.
85. Защита от отладки: принцип ловушек и избыточного кода.
86. Защита от дизассемблирования. Принцип внешней загрузки файлов.
87. Динамическая модификация программы. Защита от трассировки по прерываниям.
88. Способы ассоциирования защиты и программного обеспечения. Оценка надежности защиты от отладки.
89. Ключи на базе перепрограммируемой постоянной памяти.
90. Ключи на базе заказных чипов.
91. Примеры реализации ключей (Aktivator, HASP, Alladin и другие).
92. Ключи на базе микропроцессоров.
93. Модели взаимодействия прикладной программы и программы злоумышленника, компьютерные вирусы как особый класс РПВ, активная и пассивная защита, необходимые и достаточные условия недопущения

разрушающего воздействия; понятие изолированной программной среды, защита программ от изменения и контроль целостности.

94. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; программно-аппаратные средства обеспечения информационной безопасности в типовых ОС, СУБД, вычислительных сетях.

Структура экзаменационного билета.
Экзаменационный билет включает в себя два теоретических вопроса и одну задачу.
Примерные вопросы для экзамена:
1. Теоретический вопрос.
2.Теоретический вопрос.

Форма 1.4.-33

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Специальность10.05.05«Безопасность информационных технологий в правоохранительной сфере»
Дисциплина Программно-аппаратнаязащитаинформации

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Уязвимость компьютерных систем. Понятие доступа, субъект и объект доступа.
2. Классификация ПАСОИБ.

Зав. кафедрой управления информационной безопасностью А.С.Исмагилова

Кафедра управления информационной безопасностью

Устанавливается следующая градация перевода оценки из многобалльной в четырехбалльную:

Экзамены:
- отлично – от 80 до 110 баллов (включая 10 поощрительных баллов),
- хорошо – от 60 до 79 баллов,
- удовлетворительно – от 45 до 59 баллов,
- неудовлетворительно – менее 45 баллов.

Критерии оценивания результатов экзамена для ОФО:
Критерии оценки (в баллах):
- 25-30 баллов выставляется студенту, если студент дал полные, развернутые ответы на все теоретические вопросы билета, продемонстрировал знание терминологии, основных понятий, умение применять теоретические знания при выполнении практических заданий. Студент без затруднений ответил на все дополнительные вопросы.

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

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

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

Перевод оценки из 100-балльной в четырехбалльную производится следующим образом:

- отлично – от 80 до 110 баллов (включая 10 поощрительных баллов);
- хорошо – от 60 до 79 баллов;
- удовлетворительно – от 45 до 59 баллов;
- неудовлетворительно – менее 45 баллов.

Тестирование

Задание №1 (***Образец***)

Незаконный сбор, присвоение и передача сведений составляющих коммерческую тайну, наносящий ее владельцу ущерб, - это...

а) политическая разведка;
б) промышленный шпионаж;
в) добросовестная конкуренция;
г) конфиденциальная информация;
д) правильного ответа нет.

Задание №2

Какая информация является охраняемой внутригосударственным законодательством или международными соглашениями как объект интеллектуальной собственности:

а) любая информация;
б) только открытая информация;
в) запатентованная информация;
г) закрываемая собственником информация;
д) коммерческая тайна.
е) Метод записи чисел, представление чисел с помощью письменных знаков;
ж) Система измерения, сбора, анализа, представления и интерпретации информации о посетителях веб-сайтов с целью их улучшения и оптимизации.

Задание №3

Кто может быть владельцем защищаемой информации

а) только государство и его структуры;
б) предприятия акционерные общества, фирмы;
в) общественные организации;
г) только вышеперечисленные;
д) кто угодно.

Задание №4

Какие сведения на территории РФ могут составлять коммерческую тайну

1) учредительные документы и устав предприятия;
2) сведенья о численности работающих, их заработной плате и условиях труда;

3) документы о платежеспособности, об уплате налогов, о финансово-хозяйственной деятельности;

4) другие;

5) любые.

Задание № 5

Какие секретные сведения входят в понятие «коммерческая тайна»?

1) связанные с производством;

2) связанные с планированием производства и сбытом продукции;

3) технические и технологические решения предприятия;

4) только первый и второй вариант ответа;

5) три первых варианта ответа.

Критерии оценки тестовых заданий

Структура работы	Критерии оценки	Распределение баллов
6 семестр Модуль 1. Основные принципы программно-аппаратных средств обеспечения информационной безопасности, Модуль 2. Программно-аппаратные средства защиты информации		
Один тестовый вопрос (всего в тесте 25 вопросов)	Не правильный ответ/	0/0,6
Тест (все 25 вопросов)	Правильный ответ	0/15

Темы лабораторных работ

1) Анализ угроз информационной безопасности. Анализ сетевых угроз информационной безопасности.
2) Методы и средства ограничения доступа к компонентам вычислительных систем.
3) Основные принципы криптографической защиты информации.
4) Проверка ОИ на базе вычислительной техники.

Типовая лабораторная работа

Модуль 2. Программно-аппаратные средства защиты информации.

Тема: Основные принципы криптографической защиты информации.

Цель: Практическое ознакомление с программой TrueCrypt, обеспечивающей шифрование разделов диска на персональном компьютере.

Задание: Ознакомиться с основными возможностями программы TrueCrypt 7.0.

Порядок выполнения:

1) Создайте с помощью приложения TrueCrypt простой том (зашифрованный файловый контейнер). Опишите свои действия. В качестве иллюстраций используйте скриншоты. Опишите назначение простого тома приложения TrueCrypt.

2) Защитите с помощью приложения TrueCryptфлеш-носитель паролем. Опишите свои действия. В качестве иллюстраций используйте скриншоты.

3) Создайте с помощью приложения TrueCrypt скрытый том (зашифрованный файловый контейнер). Опишите свои действия. В качестве иллюстраций используйте скриншоты. Опишите назначение зашифрованного тома приложения TrueCrypt.

4) Опишите назначение шифрования с помощью приложения TrueCrypt системного раздела.

Критерии оценки лабораторной работы

Структура работы	Критерии оценки	Распределение баллов
6 семестр	работа выполнена неполно, не показано общее понимание вопроса, имелись затруднения или допущены ошибки в определении понятий, использовании терминологии /работа выполнена в полном объеме, но допущены один-два недочета при освещении основного содержания ответа, нет определенной логической последовательности, неточно используется специализированная терминология/ работа выполнена в полном объеме и изложена грамотным языком в определенной логической последовательности с точным использованием специализированной терминологии; показано уверенное владение прикладными программами	0/1/2

Темы практических работ

1) Анализ угроз информационной безопасности.
2) Классификация ПАСОИБ.
3) Методы криптографической защиты.
4) Журналы регистрации событий на примере ОС Windows.
5) Программно-аппаратные средства защиты от несанкционированного доступа к информации, хранимой в ПЭВМ.
6) Система контроля и управления доступом (СКУД) на примере гуманитарного корпуса БашГУ.
7) Системы сигнализации на примере гуманитарного корпуса БашГУ.
8) Штатные средства сетевого оборудования, предназначенные для защиты информации при передаче по каналам связи.

Типовая практическая работа

Модуль 2. Программно-аппаратные средства защиты информации.

Тема: Журналы регистрации событий на примере ОС Windows.

Цель: Практическое ознакомление с системой журналирования, применяемой в ОС Windows.

Задание: Ознакомиться с системой журналирования ОС Windows.

Порядок выполнения:

1) Ознакомиться с системой журналирования ОС Windows.

2) Показать ключевые журналы ОС Windows.
3) Указать типичные проблемы, возникающие при обработке указанных журналов.
4) Перечислить типовые пути решения возникающих проблем.

Критерии оценки практической работы

Структура работы	Критерии оценки	Распределение баллов
6 семестр	работа выполнена неполно, не показано общее понимание вопроса, имелись затруднения или допущены ошибки в определении понятий, использовании терминологии /работа выполнена в полном объеме, но допущены один-два недочета при освещении основного содержания ответа, нет определенной логической последовательности, неточно используется специализированная терминология/ работа выполнена в полном объеме и изложена грамотным языком в определенной логической последовательности с точным использованием специализированной терминологии; показано уверенное владение прикладными программами	0/2/4

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. Долозов, Н.Л. Программные средства защиты информации : конспект лекций / Н.Л. Долозов, Т.А. Гультяева ; Министерство образования и науки Российской Федерации, Новосибирский государственный технический университет. - Новосибирск : НГТУ, 2015. - 63 с. : схем., ил. - Библиогр. в кн. - ISBN 978-5-7782-2753-8; То же [Электронный ресурс]. - URL:http://biblioclub.ru/index.php?page=book&id=438307

2. Программно-аппаратные средства обеспечения информационной безопасности: учебное пособие для вузов / А.В. Душкин, О.М. Барсуков, К.В. Славнов, Е.В. Кравцов ; под ред. А.В. Душкина. - Москва : Горячая линия - Телеком, 2016. - 248 с. : схем., табл., ил. - Библиогр.: с. 234-235 - ISBN 978-5-9912-0470-5 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=483768 (07.04.2019).

Дополнительная литература

3. Волкова, Т.В. Основы проектирования компонентов автоматизированных систем : учебное пособие [Электронный ресурс]/ / Т.В. Волкова ; Министерство образования и науки Российской Федерации, Оренбургский Государственный Университет, Кафедра программного обеспечения вычислительной техники и автоматизированных систем. - Оренбург : ОГУ, 2016. - 226 с. Режим доступа - URL: http://biblioclub.ru/index.php?page=book&id=471129 (13.01.2019).

4. Гухман, В.Б. Краткая история науки, техники и информатики : учебное пособие [Электронный ресурс]/ В.Б. Гухман. - Москва ; Берлин : Директ-Медиа, 2017. - 171с. [Электронный ресурс]/ URL: http://biblioclub.ru/index.php?page=book&id=474295 (13.01.2019).

5. Синицын, Ю.И. Сети и системы передачи информации : учебное пособие[Электронный ресурс]/ Ю.И. Синицын, Е. Ряполова, Р.Р. Галимов ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет». - Оренбург : ОГУ, 2017. - 190 с. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=485524 (13.01.2019).

6. Губарев, В.В. Введение в теоретическую информатику : учебное пособие / В.В. Губарев ; Министерство образования и науки Российской Федерации, Новосибирский государственный технический университет. - Новосибирск : НГТУ, 2014. - Ч. 1. - 420 с. : табл., граф., схем., ил. - Библиогр.: с. 452-457. - ISBN 978-5-7782-2477-3; То же [Электронный ресурс]. - URL:http://biblioclub.ru/index.php?page=book&id=436214

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 видеопорталUniverTV.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. Лицензиибессрочные.
14. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензиибессрочные.
15. Система централизованного тестирования БашГУ (Moodle). GNU General Public License.

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

Наименование специальных помещений и помещений для самостоятельной работы	**Вид Занятия**	**Оснащенность специальных помещений и помещений для самостоятельной работы**
1	2	3
1. ***учебная аудитория для проведения занятий лекционного типа:*** аудитория № 403 (гуманитарный корпус), аудитория № 405 (гуманитарный корпус), аудитория № 413 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 515 (гуманитарный корпус), аудитория № 516 (гуманитарный корпус). **2.** ***учебная аудитория для проведения лабораторных работ:*** компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс 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	Лекции, практические занятия, самостоятельные работы, групповые и индивидуальные опросы	**Аудитория № 403** Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный ClassicNorma 244*183 – 1 шт., учебно-наглядные пособия. **Аудитория № 405** Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром PrometheanActivBoard 387 RPOMOUNTEST -1 шт., Ком-ер встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H – 1 шт. , Мультимедиа-проектор PanasonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт. , Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт. **Аудитория № 413** Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт АРАРТ MA1225 – 1 шт.

(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). **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.*помещения для самостоятельной работы:*** читальный зал библиотеки аудитория 402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус). **6.*помещение для хранения и профилактического обслуживания учебного оборудования:***аудитория № 523 (гуманитарный корпус).		**Аудитория № 415** Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт APART MA1225 – 1 шт. **Аудитория № 416** Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 418** Учебная мебель, доска, Экран настенный LumienMasterPikture 153*203 MatteWhiteFiberClas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт. **Аудитория № 419** Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 515** Учебная мебель, доска, терминал видео конференц-связи LifeSizeIcon 600-камера, интер-ая система со встроенным короткофокусным проектором PrometheanActivBoard 387 RPO MOUNT EST, профес-сиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса HDMI CMPRO 4H4H, интер-ая напольная кафедра докладчика, ком-ер встраиваемый в кафедру IN-TEL Core i3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/Thermaltake VL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром. **Аудитория № 516** Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран. **Аудитория № 509** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 608** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 609** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 610** Учебная мебель, доска, учебно-наглядные пособия, LED Телевизор TCLL55P6 USBLACK – 1 шт., кронштейн для телевизора NBP 5 –

		1 шт., Кабель HDMI (m)-HDH(m)ver14,10м. **Аудитория № 613** Учебная мебель, доска, моноблок стационарный – 15 шт. **Компьютерный класс аудитория № 420** Учебная мебель, моноблоки стационарные 15 шт. **Компьютерный класс аудитория № 404** Учебная мебель, компьютеры -15 штук. **Аудитория 402 читальный зал библиотеки** Учебная мебель, доска, компьютеры в комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура, мышь, стеллажи, шкафы картотечные, комбинированные. **Аудитория № 523** Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт.

Приложение 1

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

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ
дисциплины **Программно-аппаратные средства защиты информации**на 6 семестр

Вид работы	Объем дисциплины
	Очная форма обучения
Общая трудоемкость дисциплины (ЗЕТ / часов)	5 ЗЕТ / 180 часов
Учебных часов на контактную работу с преподавателем:	65,2
лекций	16
практических / семинарских	32
лабораторных	16
Других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем)	1,2
Учебных часов на самостоятельную работу обучающихся, включая подготовку к экзамену	35

Форма контроля:
Экзамен 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
1	Модуль 1. Основные принципы программно-аппаратных средств обеспечения информационной безопасности					Основная 1, 2 Дополнительная 3,4,5,6	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	тестирование, практическое задание
	Тема: Основные понятия и определения в области создания ПАСОИБ. Нормативно-правовая база создания ПАСОИБ. Анализ угроз информационной безопасности. Анализ сетевых угроз информационной безопасности. Классификация ПАСОИБ. Функциональные возможности ПАСОИБ. Принципы разработки ПАСОИБ. Концепция диспетчера доступа. Основные этапы проектирования ПАСОИБ.	2	4	4	4			
	Тема: Классификация функциональных требований по защите информации и данных. Принципы действия и технологические особенности программно-аппаратных средств, реализующих отдельные функциональные требования по защите информации и данных и их взаимодействие с общесистемными компонентами вычислительных систем. Методы обеспечения идентификации и аутентификации. Методы криптографической защиты. Методы и средства хранения ключевой информации.	2	4		4			
	Тема: Методы и средства ограничения доступа к компонентам вычислительных систем. Характеристика методов и средства привязки программного обеспечения к аппаратному кружению и физическим носителям.	2	4	4	4			
	Тема: Методы аудита безопасности. Методы обеспечения доступа к системе защиты и управления безопасностью. Методы	2	4		5			

	обеспечения целостности системы защиты.							
2	Модуль 2. Программно-аппаратные средства защиты информации Тема: Классификация аппаратных компонентов средств защиты программ. Классификация программных компонентов средств защиты программ. Структура программного обеспечения. Способы встраивания средств защиты в программное обеспечение. Способы определения факта незаконного использования программ. Способы защиты программ от незаконного использования. Способы изучения кода программ. Способы защиты программ от изучения кода. Основные принципы обеспечения безопасности программ. Изолированная программная среда. Тема:.Классификация программно-аппаратных средств защиты от несанкционированного доступа к информации, хранимой в ПЭВМ. Характеристики программно-аппаратных средств защиты от несанкционированного доступа к информации, хранимой в ПЭВМ. Понятие электронного замка. Принципы построения и функционирования электронных замков. Механизмы контроля аппаратной конфигурации ПЭВМ. Общие принципы разграничения доступа пользователей к устройствам ПЭВМ. Основные принципы криптографической защиты информации. Классификация программно-аппаратных средств защиты информации в сетях передачи данных. Принципы построения и функционирования межсетевых экранов в сетях передачи данных. Программно-аппаратные средства межсетевого экранирования. Основные принципы защиты информации при передаче по каналам связи.	2 2	4 4	0 4	4 4	Основная 1, 2 Дополнительная 3,4,5,6	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	тестирование, практическое задание
	Тема: Программно-аппаратные средства защиты информации при передаче по каналам связи. Основные принципы разграничения доступа к сетевым ресурсам. Основные принципы обнаружения сетевых атак. Программно-аппаратные средства обнаружения сетевых атак. Основные принципы защиты от сетевых атак. Программно-аппаратные средства защиты от сетевых атак. Основные принципы управления безопасностью сети. Программно-аппаратные средства управления безопасностью сети. Обзор штатных средств сетевого оборудования, предназначенных для защиты информации при передаче по каналам связи. Способы применения штатных средств сетевого оборудования, предназначенных для защиты информации при передаче по каналам связи. Тема: Основные требования к информационной безопасности. Задачи сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности.	2 2	4 4	0 4	5 5			

	Технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности.: Классификация требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности. Проверка ОИ на базе вычислительной техники.							
Всего:		16	32	16	35			

Приложение 2

Рейтинг – план дисциплины

Программно-аппаратные средства защиты информации

Специальность 10.05.05 Безопасность информационных технологий в правоохранительной сфере
Курс 3, семестр 6

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Основные принципы программно-аппаратных средств обеспечения информационной безопасности				
Текущий контроль				20
1. Лабораторная работа	2	2	0	4
2. Практическая работа	4	4	0	16
Рубежный контроль				
Тест	15	1	0	15
Всего		7	0	35
Модуль 2. Программно-аппаратные средства защиты информации				
Текущий контроль				20
1. Лабораторная работа	2	2	0	4
2. Практическая работа	4	4	0	16
Рубежный контроль				
Тест	15	1	0	15
Всего		7	0	35
Поощрительные баллы				
1. Участие в студенческой олимпиаде по дисциплине	3	1	0	3
2.Публикация научной статьи	4	1	0	4
3.Участие в научно-практической конференции по профилю	3	1	0	3
Всего		3	0	10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			0	-6
2. Посещение практических (семинарских, лабораторных занятий)			0	-10

Итоговый контроль				
1.Экзамен	30	1	0	30

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

Актуализировано:
на заседании кафедры
протокол № 10 от «7» июня 2018 г.
Зав. кафедрой / А.С. Исмагилова

Согласовано:
Председатель УМК института
/ Р.А. Гильмутдинова

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Программно-аппаратная защита информации
Б1.Б.24 (базовая)

Программа специалитета

Специальность
10.05.05 "Безопасность информационных технологий в правоохранительной сфере"

Специализация
"Технологии защиты информации в правоохранительной сфере"

Квалификация
Специалист по защите информации

Разработчики (составители)
Старший преподаватель / И.В. Салов

Доцент, канд.биол.наук / Ф.Т. Байрушин

Для приема: 2015 г.

Уфа 2018 г.