Автономная некоммерческая организация
дополнительного профессионального образования

«Техническая академия Росатома»
(АНО ДПО «Техническая академия Росатома»)

УТВЕРЖДАЮ

Заместитель директора
Департамента основной
деятельности по сопровождению
отраслевой деятельности

Д.И. Сучков

20.12.2019
дата

ПРОГРАММА

повышения квалификации

Основы информационной безопасности компьютерных систем, применяемых в организациях атомной отрасли

Обнинск
2019

Автономная некоммерческая организация
дополнительного профессионального образования

«Техническая академия Росатома»
(АНО ДПО «Техническая академия Росатома»)

УТВЕРЖДАЮ

Заместитель директора
Департамента основной
деятельности по сопровождению
отраслевой деятельности

Д.И. Сучков

20.12.2019
дата

УЧЕБНЫЙ ПЛАН

Основы информационной безопасности компьютерных систем, применяемых в организациях атомной отрасли

Цель обучения: Развитие у слушателей компетенций необходимых для выполнения профессиональной деятельности в области обеспечения информационной безопасности информационных систем Госкорпорации «Росатом» и ее организаций

Продолжительность обучения по программе 110 часов *Режим очного обучения* 8 час/день

Форма обучения дистанционно-очная

Номер раздела	Наименование раздела	Количество часов обучения[1]					Виды и форма контроля
		всего	очно		заочно		
			Л	ПЗ	СДО	СР	
1	Введение в информационную безопасность	38	22	6	10		текущий (опрос)
2	Администрирование средств защиты информации	30	5	15	10		текущий (опрос)
3	Мониторинг и диагностика информационной безопасности	14	4	5	5		текущий (опрос)
4	Безопасное использование информационных технологий	25	4		21		текущий (опрос)
		3					итоговая аттестация (тестирование)

[1] Л – лекции, ПЗ – практические занятия, СР – самостоятельная работа по изучению предоставленного материала, СДО – обучение в системе дистанционного обучения.

Номер раз-дела	Наименование раздела	Количество часов обучения[1]					Виды и форма контроля
		всего	очно		заочно		
			Л	ПЗ	СДО	СР	
Итого		110	35	26	46		

Планируемые результаты обучения

по программе: Основы информационной безопасности компьютерных систем, применяемых в организациях атомной отрасли

Номер раздела учебного плана программы	Профессиональные компетенции, на которые направлено обучение			Код и наименование ОТФ/ТФ[2] (в соотв-ии с ПС)
	Наименование компетенции	Умения	Знания	
1	Администрирование систем защиты информации автоматизированных систем;	Планировать политику безопасности программных компонентов автоматизированных систем	Принципы формирования политики информационной безопасности в автоматизированных системах; основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах; основные меры по защите информации в автоматизированных системах	B/02.6 Администрирование систем защиты информации автоматизированных систем
	Диагностика систем защиты информации автоматизированных систем		Нормативные правовые акты в области защиты информации; национальные, межгосударственные и международные стандарты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите	B/01.6 Диагностика систем защиты информации автоматизированных систем

[2] Графа заполняется при наличии утвержденного ПС.

Номер раздела учебного плана программы	Профессиональные компетенции, на которые направлено обучение			Код и наименование ОТФ/ТФ[2] (в соотв-ии с ПС)
	Наименование компетенции	Умения	Знания	
			информации; организационные меры по защите информации; основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в автоматизированных системах; принципы построения средств защиты информации от утечки по техническим каналам	
	Мониторинг защищенности информации в автоматизированных системах	Классифицировать и оценивать угрозы информационной безопасности; анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах; применять нормативные документы по противодействию технической разведке	НПА в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; организационные меры по защите информации; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных систе-	B/05.6 Мониторинг защищенности информации в автоматизированных системах

Номер раздела учебного плана программы	Профессиональные компетенции, на которые направлено обучение			Код и наименование ОТФ/ТФ[2] (в соотв-ии с ПС)
	Наименование компетенции	Умения	Знания	
			мах; методы защиты информации от утечки по техническим каналам	
2	Администрирование систем защиты информации автоматизированных систем	Создавать, удалять и изменять учетные записи пользователей автоматизированной системы; устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации; использовать криптографические методы и средства защиты информации в автоматизированных системах	Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем безопасности автоматизированных систем; программно-аппаратные средства защиты информации автоматизированных систем; принципы организации и структура систем защиты программного обеспечения автоматизированных систем	B/02.6 Администрирование систем защиты информации автоматизированных систем
	Диагностика систем защиты информации автоматизированных систем	Использовать криптографические методы и средства защиты информации в автоматизированных системах		B/01.6 Диагностика систем защиты информации автоматизированных систем
	Мониторинг защищенности информации в автоматизированных системах		Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем; программно-аппаратные средства	B/05.6 Мониторинг защищенности информации в автоматизированных системах

Номер раздела учебного плана программы	Профессиональные компетенции, на которые направлено обучение			Код и наименование ОТФ/ТФ[2] (в соотв-ии с ПС)
	Наименование компетенции	Умения	Знания	
			обеспечения защиты информации автоматизированных систем	
3 3 3	Администрирование систем защиты информации автоматизированных систем	Регистрировать и анализировать события, связанные с защитой информации в автоматизированных системах	Методы контроля эффективности защиты информации от «утечки» по техническим каналам; технические средства контроля эффективности мер защиты информации; критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем	B/02.6 Администрирование систем защиты информации автоматизированных систем
	Диагностика систем защиты информации автоматизированных систем	Определять источники и причины возникновения инцидентов; оценивать последствия выявленных инцидентов; осуществлять контроль обеспечения уровня защищенности в автоматизированных системах; обнаруживать нарушения правил разграничения доступа; устранять нарушения правил разграничения доступа	Технические средства контроля эффективности мер защиты информации; регламент информирования персонала автоматизированной системы о выявленных инцидентах; регламент учета выявленных инцидентов; регламент устранения инцидентов; критерии оценки защищенности автоматизированной системы	B/01.6 Диагностика систем защиты информации автоматизированных систем
	Мониторинг защищенности информации в автоматизированных системах	Контролировать события безопасности и действия пользователей автоматизированных	Технические средства контроля эффективности мер защиты информации	B/05.6

Номер раздела учебного плана программы	Профессиональные компетенции, на которые направлено обучение			Код и наименование ОТФ/ТФ[2] (в соотв-ии с ПС)
	Наименование компетенции	Умения	Знания	
		систем; применять технические средства контроля эффективности мер защиты информации; контролировать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем; документировать процедуры и результаты контроля функционирования системы защиты информации автоматизированной системы		Мониторинг защищенности информации в автоматизированных системах

При разработке программы учитывался профессиональный стандарт:

№ ПС	Наименование ПС	Дата введения в действие ПС
843	Специалист по защите информации в автоматизированных системах	15.09.2016

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН

Основы информационной безопасности компьютерных систем, применяемых в организациях атомной отрасли

Номер раздела, темы	Наименование разделов, тем	Количество часов обучения[3]					Виды и форма контроля
		всего	очно		заочно		
			Л	ПЗ	СДО	СР	
1	Введение в информационную безопасность	38	22	6	10		текущий (опрос)
1.1	Основные определения. Цели и задачи информационной безопасности	2	2				
1.2	Защищаемые информация и информационные ресурсы. Объекты защиты	1	1				
1.3	Правовые основы информационной безопасности	14	6		8		
1.4	Национальные, межгосударственные и международные стандарты в области информационной безопасности	4	2		2		
1.5	Определение угроз безопасности информации ограниченного доступа	4	2	2			
1.6	Требования по защите информации и созданию системы защиты информации	4	3	1			
1.7	Основы технической защиты информации	5	2	3			
1.8	Основы криптографической защиты информации	2	2				
1.9	Организационные меры по защите информации	2	2				
2	Администрирование средств защиты информации	30	5	15	10		текущий (опрос)
2.1	Содержание и порядок деятельности персонала по эксплуатации защищенных информационных систем	3	1	2			
2.2	Администрирование средств защиты информации от несанкционированного доступа	21	3	10	8		
2.3	Администрирование средств криптографической защиты информации	6	1	3	2		

[3] Л – лекции, ПЗ – практические занятия, СР – самостоятельная работа по изучению предоставленного материала, СДО – обучение в системе дистанционного обучения.

Номер раздела, темы	Наименование разделов, тем	Количество часов обучения[3]					Виды и форма контроля
		всего	очно		заочно		
			Л	ПЗ	СДО	СР	
3	Мониторинг и диагностика информационной безопасности	14	4	5	5		текущий (опрос)
3.1	Мониторинг событий безопасности и контроль действий пользователей	3	1	2			
3.2	Контроль состояния технической защиты информации	6	2	2	2		
3.3	Обнаружение и устранение инцидентов, возникших в процессе эксплуатации информационных систем.	5	1	1	3		
4	Безопасное использование информационных технологий	25	4		21		
4.1	Культура информационной безопасности	11	2		9		
4.2	Атаки и методы противодействия им	8	1		7		
4.3	Типовые преступления против информационной безопасности	4	1		3		
4.4	Физическая безопасность при работе с информационными ресурсами	2			2		
		3					итоговая аттестация (тестирование)
	Итого	110	35	26	46		

УЧЕБНАЯ ПРОГРАММА

Основы информационной безопасности компьютерных систем, применяемых в организациях атомной отрасли

1 Общая характеристика программы

При разработке настоящей программы были учтены законодательные и нормативные правовые требования, содержащиеся в документах, которые приведены в разделе 5 настоящей учебной программы.

1.1 Требования к слушателям программы

Специалисты подразделений Госкорпорации «Росатом» и ее организаций, реализующие функции обеспечения информационной безопасности автоматизированных (информационных) систем, администрирования систем защиты информации автоматизированных систем, диагностики систем защиты информации автоматизированных систем, специалисты отделов информационных технологий.

1.2 Характеристика программы в системе ПТЗиН Госкорпорации «Росатом»

В системе производственно-технических знаний и навыков работников Госкорпорации «Росатом», программа:

направлена на развитие ПТЗиН	**Управление информационной безопасностью и защита государственной тайны**
по параметру «Вес», имеет значение	ВЫСОКИЙ

1.3 Характеристика программы в системе обучения Госкорпорации «Росатом»

Значение приоритета обучения	ОБЯЗАТЕЛЬНОЕ
Сертификат, подтверждающий определенный уровень развития ПТЗиН и/или квалификации	Удостоверение о повышении квалификации «Основы информационной безопасности компьютерных систем, применяемых в организациях атомной отрасли» Срок действия – 3 года
Нормативные ссылки (для «**обязательного**» обучения)	Приказ ГК «Росатом» от 09.01.2019 № 1/4-П-дсп

2 Содержание программы

№ раздела, темы	Наименование раздела, темы	Краткое содержание
1	Введение в информационную безопасность	Основные определения. Цели и задачи информационной безопасности. Защищаемые информация и информационные ресурсы. Объекты защиты. Правовые основы информационной безопасности. Национальные, межгосударственные и международные стандарты в области информационной безопасности. Определение угроз безопасности информации ограниченного доступа. Требования по защите информации и созданию системы защиты информации. Основы технической защиты информации. Основы криптографической защиты информации. Организационные меры по защите информации

№ раздела, темы	Наименование раздела, темы	Краткое содержание
1.1	Основные определения. Цели и задачи информационной безопасности	Л: Основные термины и определения в области информационной безопасности (ИБ). Цели и задачи ИБ. Техническая защита информации (ТЗИ). Государственная система противодействия иностранным техническим разведкам (ПД ИТР) и ТЗИ. Место ТЗИ в системе мероприятий по обеспечению информационной безопасности в Российской Федерации. Цели и задачи ТЗИ
1.2	Защищаемые информация и информационные ресурсы. Объекты защиты	Л: Объекты защиты информации. Защищаемые информация и информационные ресурсы. Автоматизированные системы (АС) и информационные системы (ИС), объекты информатизации (ОИ), их классификация и характеристика. Государственные информационные ресурсы, негосударственные информационные ресурсы, находящиеся в ведении органов государственной власти и организаций. Понятие, классификация и технологии построения ИС. ИС как объект защиты
1.3	Правовые основы информационной безопасности	Л: Правовые основы защиты информации. Основные требования федерального законодательства по вопросам защиты информации. Виды информации ограниченного доступа и правовые основы их защиты Нормативные правовые, организационно-распорядительные, нормативные, методические, плановые и информационные документы по защите информации. Ответственность за правонарушения в области защиты информации. Общие вопросы организации лицензирования деятельности в области ТЗИ, сертификации средств защиты информации, аттестации ОИ по требованиям безопасности информации. Доктрина информационной безопасности Российской Федерации. Федеральный закон №149-ФЗ. Федеральный закон №187-ФЗ. СДО: Основные требования федерального законодательства по вопросам защиты информации. Виды информации ограниченного доступа и правовые основы их защиты. Доктрина информационной безопасности Российской Федерации. Федеральный закон №149-ФЗ. Федеральный закон №187-ФЗ. Правовое обеспечение сертификации средств защиты информации. Ответственность за правонарушения в области защиты информации
1.4	Национальные, межгосударственные и международные стандарты в области информационной безопасности	Л: Обзор международных, межгосударственных и национальных стандартов в области защиты информации: серии Р 50k, 51k, 52k, 53k, 54k, 56k, ИСО/МЭК 27К, 15408 и другие. СДО: Международный стандарт ИСО/МЭК 27002
1.5	Определение угроз безопасности информации ограниченного доступа	Л: Понятие и классификация угроз безопасности информации. Модель угроз безопасности информации. Банк данных угроз безопасности информации, база данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах. Описание уязвимостей программного обеспечения,

№ раз-дела, темы	Наименование раздела, темы	Краткое содержание
		включённых в базу данных уязвимостей. Международный подход к выявлению и анализу уязвимостей, базы данных, содержащие уязвимости, в том числе CVE. Решение практической задачи по общей системе оценки уязвимостей (стандарт CVSS). ПЗ: Разработка модели угроз безопасности информации и модели нарушителя в ИС
1.6	Требования по защите информации и созданию системы защиты информации	Л: Основные принципы построения систем защиты информации в ИС. Комплекс работ по созданию системы защиты информации (формирование требований к системе защиты информации; подготовка аналитического обоснования создания системы защиты информации; разработка (проектирование) системы защиты информации; внедрение системы защиты информации; аттестация объекта информатизации по требованиям безопасности информации и ввод его в эксплуатацию; сопровождение (поддержка) системы защиты информации в ходе эксплуатации объекта информатизации). Требования по защите информации, содержащейся в ИС. Требования приказов ФСТЭК к различным видам ИС. Требования по защите акустической речевой информации. Требования по защите информации от несанкционированного доступа (НСД). Принципы формирования политики информационной безопасности в информационных системах. ПЗ: Разработка требований по защите информации, обрабатываемой техническими средствами от утечки за счёт побочных электромагнитных излучений и наводок (ПЭМИН)
1.7	Основы технической защиты информации	Л: Основные способы и средства технической защиты информации от утечки по техническим каналам, защиты объектов информатизации от утечки информации по техническим каналам при её обработке с использованием технических средств, защиты акустической речевой информации от утечки по техническим каналам. Общие принципы построения средств защиты информации от утечки по техническим каналам. Общая характеристика и классификация мер и средств защиты информации от НСД. Защита информации на автоматизированных рабочих местах на базе автономных ПЭВМ. Защита информации в локальных вычислительных сетях. Защита информации при межсетевом взаимодействии. Защита информации при работе с системами управления базами данных. Особенности реализации требований по защите информации при взаимодействии абонентов с информационными сетями общего пользования. ПЗ: Решение и разбор ситуационной задачи по ТЗИ
1.8	Основы криптографической защиты информации	Л: Основные понятия криптографической защиты информации: криптографическая защита информации,

№ раз-дела, темы	Наименование раздела, темы	Краткое содержание
		криптографическое средство защиты информации, криптографическое преобразование, алгоритм криптографического преобразования, симметричные и ассиметричные криптографические алгоритмы, шифр, шифрование, зашифрование, расшифрование, ключ, имитовставка, имитозащита, хэш-функция, хэш-код, электронная цифровая подпись, процессы формирования и проверки подписи, ключ подписи, ключ проверки подписи, инфраструктура открытых ключей, простая и усиленная электронная подпись, неквалифицированная и квалифицированная электронная подпись, средства электронной подписи, сертификат ключа проверки электронной подписи, криптографический ключ, ключевая информация, ключевой носитель, компрометация криптоключей, орган криптографической защиты и другие. Методы и средства криптографической защиты информации, криптографические протоколы. Криптографические алгоритмы, национальные криптографические стандарты. Государственное регулирование в области криптографической защиты информации и сфере использования электронной подписи. СДО: Электронная цифровая подпись.
1.9	Организационные меры по защите информации	Л: Основные меры по защите информации в автоматизированных системах: основные меры защиты информации от утечки по техническим каналам, организационные меры защиты: временные ограничения, территориальные ограничения. Меры защиты информации от НСД
2	Администрирование средств защиты информации	Содержание и порядок деятельности персонала по эксплуатации защищенных информационных систем, администрирование средств защиты информации от несанкционированного доступа, администрирование средств криптографической защиты информации. Мониторинг и диагностика информационной безопасности
2.1	Содержание и порядок деятельности персонала по эксплуатации защищенных информационных систем	Л: Содержание и порядок деятельности персонала по эксплуатации защищенных информационных систем (ЗИС) и систем безопасности автоматизированных систем, обеспечение защиты информации при выводе из эксплуатации, аттестованной информационной системы или после принятия решения об окончании обработки информации. ПЗ: Решение и разбор ситуационной задачи по взаимодействию персонала ЗИС
2.2	Администрирование средств защиты информации от несанкционированного доступа	Л: Принципы организации и структура систем защиты программного обеспечения автоматизированных систем. Создание, удаление и изменение учетных записей пользователей автоматизированной системы; настройки механизмов безопасности операционных систем, систем управления базами данных, обеспечение безопасности

№ раз-дела, темы	Наименование раздела, темы	Краткое содержание
		компьютерных сетей и программных систем; программно-аппаратные средства защиты информации автоматизированных систем. ПЗ: Администрирование средств защиты информации от несанкционированного доступа. СДО: Парольная защита. Средства управления доступом, средства идентификации и аутентификации. Защита информации при работе с системами управления базами данных. Антивирусная защита.
2.3	Администрирование средств криптографической защиты информации	Л: Криптографические функции в операционных системах и наложенных средствах защиты информации. ПЗ: Использование криптографических методов и средств защиты информации в автоматизированных системах
3	Мониторинг и диагностика информационной безопасности	Мониторинг событий безопасности и контроль действий пользователей информационных систем, контроль состояния технической защиты информации, обнаружение и устранение инцидентов, возникших в процессе эксплуатации информационных систем
3.1	Мониторинг событий безопасности и контроль действий пользователей	Л: Средства мониторинга событий безопасности. Регистрация и анализ событий, связанных с защитой информации в автоматизированных системах. Контроль действий пользователей информационных систем. Категории журналов событий. Способы построения, дополнительные компоненты и реализация инфраструктуры управления журналами событий. Технология обнаружения атак. Классификация систем обнаружения атак. Специализированные системы обнаружения атак. ПЗ: Решение и разбор ситуационной задачи по мониторингу событий безопасности
3.2	Контроль состояния технической защиты информации	Л: Основы организации контроля состояния технической защиты информации. Методы и средства контроля защищенности информации от несанкционированного доступа информационных системах. Методы и средства контроля защищенности информации от «утечки» по техническим каналам в информационных системах. Технические средства контроля эффективности мер защиты информации. Критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем, критерии оценки защищенности автоматизированной системы. Аттестация объектов информатизации по требованиям безопасности информации. ПЗ: Документирование процедур и результатов контроля функционирования системы защиты информации информационной системы. СДО: Контроль состояния технической защиты информации от несанкционированного доступа

№ раздела, темы	Наименование раздела, темы	Краткое содержание
3.3	Обнаружение и устранение инцидентов, возникших в процессе эксплуатации информационных систем.	Л: Определение источников и причин возникновения инцидентов, оценка последствий выявленных инцидентов, контроль обеспечения уровня защищенности в автоматизированных системах, выявление нарушений правил разграничения доступа и устранение выявленных нарушений. Регламент информирования персонала информационной системы о выявленных инцидентах; регламент учета выявленных инцидентов; регламент устранения инцидентов. ПЗ: Решение и разбор ситуационной задачи по обнаружению и устранению инцидентов. СДО: Инциденты информационной безопасности
4	Безопасное использование информационных технологий	Методы и средства идентификации и процессы аутентификации, основные способы и методы осуществления угроз безопасности
4.1	Культура информационной безопасности	Л: Понятие культуры информационной. Документы МАГАТЭ. Роль человеческого фактора в обеспечении информационной безопасности СДО: Безопасная работа в сети Интернет. Безопасная работа с электронной почтой. Безопасная работа с мобильными устройствами. Безопасная работа с персональными данными
4.2	Атаки и методы противодействия им	Л: Понятия целевой и массированной (массовой) атаки. Возможные последствия атак. Примеры целевых атак. Последовательность проведения целевых атак. Меры и средства защиты от атак. СДО: Целевые атаки и методы противодействия им. Социальная инженерия. Спам и защита от него. Защита от фишинга
4.3	Типовые преступления против информационной безопасности	Л: Типовые преступления против информационной безопасности. Преступления, связанные с нарушением авторских прав. Преступление связанные с нарушением неприкосновенности (тайны) частой жизни. Преступление, связанные с нарушением безопасности информации. Преступления, связанные с неправомерным доступом к компьютерной информации (ст. 272 УК РФ). Преступления, связанные с создание вредоносных программ (ст. 273 УК РФ). Преступления, связанные с нарушением правил хранения компьютерной информации (ст. 274 УК РФ). СДО: Типовые преступления против информационной безопасности
4.4	Физическая безопасность при работе с информационными ресурсами	СДО: Физическая безопасность при работе с информационными ресурсами

3 Контроль качества освоения программы

Метод контроля	Оценочные материалы
Устный опрос	Перечни контрольных вопросов по темам курса
Компьютерное тестирование	Перечень вопросов по курсу «Основы информационной безопасности компьютерных систем, применяемых в организациях атомной отрасли»

Система оценки достижения планируемых результатов:

Показатель (объект оценивания)	Критерии достижения показателя	Значение показателя
Количество правильных ответов по компьютерному тестированию (итоговая аттестация)	Процент правильных ответов	Менее 70% – не зачтено; 70% и более – зачтено (успешное прохождение итоговой аттестации)

4 Условия реализации программы

Лекционные занятия проводятся в учебной аудитории с использованием следующих средств обучения:

— ПЭВМ;

— мультимедийный проектор с экраном;

— флипчарт или маркерная доска с маркерами, либо меловая доска с мелом.

Практические занятия проводятся в компьютерном классе с использованием раздаточных методических материалов и следующих технических средств обучения:

— ПЭВМ (с учетом числа слушателей);

— локальная сеть с файловым сервером;

— мультимедийный проектор с экраном.

Дистанционное обучение проводится на ПЭВМ, имеющей доступ к Системе дистанционного обучения Технической академии Росатома. Для проведения дистанционного этапа слушателю необходимы следующие аппаратные и программные средства:

— ПЭВМ с доступом к сети Интернет;

— Логин и пароль к Системе дистанционного обучения Технической академии Росатома;

— Колонки или наушники.

5 Законодательные и нормативные правовые акты

1. Федеральный закон от 28.12.2010 №390-ФЗ «О безопасности».
2. Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 27.12.2002 №184-ФЗ «О техническом регулировании».
4. Федеральный закон от 29.06.2015 №162-ФЗ «О стандартизации в Российской Федерации».
5. Федеральный закон «О лицензировании отдельных видов деятельности» от 4 мая 2011 года № 99-ФЗ.
6. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации « от 26 июля 2017 года № 187-ФЗ.

7. Указ Президента Российской Федерации от 16.08.2004 №1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

8. Постановлением Правительства Российской Федерации от 15 сентября 1993 г. №912-51 «Об утверждении Положения о государственной системе защиты информации в Российской Федерации».

9. Постановление Правительства Российской Федерации от 26.06.1995 №608 «О сертификации средств защиты информации».

10. Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

11. «Положение о сертификации средств защиты информации по требованиям безопасности информации» (утв. Приказом Гостехкомиссии РФ от 27.10.1995 №199).

12. «Положение по аттестации объектов информатизации по требованиям безопасности информации» (утв. Гостехкомиссией РФ 25.11.1994).

13. Положение об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации (утв. председателем Гостехкомиссии России 25 ноября 1994 г).

14. Приказ ФСТЭК России от 20.07.2012 №89 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по исполнению государственной функции по контролю за соблюдением лицензионных требований при осуществлении деятельности по технической защите конфиденциальной информации».

15. Приказ ФСТЭК России от 20.07.2012 №90 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по исполнению государственной функции по контролю за соблюдением лицензионных требований при осуществлении деятельности по разработке и производству средств защиты конфиденциальной информации».

16. Приказ ФСТЭК России от 12.07.2012 №83 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации».

17. Приказ ФСТЭК России от 12.07.2012 №84 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации».

18. Стратегия национальной безопасности Российской Федерации (утв. Указом Президента РФ от 31 декабря 2015 г. N 683).

19. Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.).

20. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.

21. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

22. ГОСТ Р 53113.1-2008. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения.

23. ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.

24. ГОСТ РО 0043-003-2012. Защита информации. Аттестация объектов информатизации. Общие положения.

25. ГОСТ РО 0043-004-2013. Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний.

26. ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

27. ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности.

28. ГОСТ Р ИСО/МЭК 15408-3-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности.

29. ГОСТ Р 56545-2015. Защита информации. Уязвимости информационных систем. Правила описания уязвимости.

30. ГОСТ Р 56546-2015. Защита информации. Уязвимости информационных систем. Классификация уязвимости информационных систем.

31. ГОСТ Р ИСО/МЭК 27000-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология.

32. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

33. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента безопасности.

34. ГОСТ Р ИСО/МЭК 27003-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности.

35. ГОСТ Р ИСО/МЭК 27004-2011. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения.

36. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

37. ГОСТ Р ИСО/МЭК 27006-2008. Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности.

38. ГОСТ Р ИСО/МЭК 27007-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности.

39. ГОСТ Р ИСО/МЭК 27013-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1.

40. ГОСТ Р ИСО/МЭК 27033-1-2011. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции.

41. ГОСТ Р ИСО/МЭК 27033-3-2014. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления

42. ГОСТ Р ИСО/МЭК 27034-1-2014. Информационная технология. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия.

43. ГОСТ Р ИСО/МЭК 27037-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме.

44. Руководящий документ «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007).

45. Руководящий документ «Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007).

46. Руководящий документ «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007).

47. Руководящий документ «Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 19.11.2007).

48. Приказ ФСТЭК России №31 от 14.03.2014 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

49. Приказ ФСТЭК России от 11.02.2013 №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» с изменениями, внесёнными приказом ФСТЭК РФ №27 от 15.02.2017

50. Приказ ФСТЭК России от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

51. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК РФ 14.02.2008).

52. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК РФ 15.02.2008).

53. Положение о банке данных угроз безопасности информации (утв. Приказом ФСТЭК РФ от 16.02.2015 №9)

54. «Методический документ. Меры защиты информации в государственных информационных системах» (утв. ФСТЭК России 11.02.2014).

55. Нормативно-методический документ. Специальные требования и рекомендации по технической защите конфиденциальной информации. Утвержден приказом Гостехкомиссии России от 30 августа 2002 г. №282.

6 Список использованной литературы

1. Основы информационной безопасности: Учебное пособие / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2005Хорев А.А. Техническая защита информации: Учебное пособие для студентов. В 3 т. Т. 1. Технические каналы утечки информации. – М.: Аналитика, 2008.

2. Хорев А.А. Защита информации от утечки по техническим каналам: Учебное пособие. – Министерство обороны Российской Федерации, 2006. Форум, 2012. – 352 с.

3. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства: Учебное пособие. – М.: ДМК Пресс, 2008. –544 с.

4. Шаньгин В.Ф. Комплексная защита корпоративной информации: Учебное пособие. – М.: МИЭТ, 2009. – 404 с.

5. Аттестационные испытания автоматизированных систем от несанкционированного доступа по требованиям безопасности информации: Учебное пособие / В.С. Горбатов, С.В. Дворянкин, А.П. Дураковский под общей редакцией Ю.Н. Лаврухина. – НИЯУ МИФИ, 2014. – 560 с.

6. Контроль защищённости информации от утечки по техническим каналам за счёт побочных электромагнитных излучений и наводок. Аттестационные испытания по требованиям безопасности информации: Учебное пособие / А.А. Голяков, В.С. Горбатов, А.П. Дураковский, А.Е. Панин, М.С. Чистяков; под общей редакцией Ю.Н. Лаврухина. – НИЯУ МИФИ, 2014. – 208 с.: ил.

7. Контроль защищённости речевой информации в помещениях. Аттестационные испытания выделенных помещений по требованиям безопасности информации: Учебное пособие / В.С. Горбатов, А.П. Дураковский, И.В. Куницин, А.Е. Панин, под общей редакцией Ю.Н. Лаврухина. – НИЯУ МИФИ, 2014. – 248 с.: ил.

8. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. – М.:

9. Правовой режим лицензирования и сертификации в сфере информационной безопасности: Учебное пособие / Ю.Ю. Коваленко. – М.: Горячая линия – Телеком, 2012.

10. Концептуальные основы создания и применения системы защиты объектов / В.А. Воронов, В.А. Тихонов. – М.: Горячая линия – Телеком, 2013.

11. Гришина Н.В. Комплексная система защиты информации на предприятии: Учебное пособие. – М.: Форум, 2013.