Автономная некоммерческая организация
дополнительного профессионального образования

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

УТВЕРЖДАЮ

Заместитель директора
Департамента основной
деятельности по сопровождению
отраслевой деятельности

Автономная некоммерческая организация дополнительного профессионального образования * Техническая академия Росатома * ОГРН 1174027012830 * Техническая академия * РОСАТОМ * Обнинск *

Д.И. Сучков

20.12.2019
дата

ПРОГРАММА

повышения квалификации

Деятельность органа криптографической
защиты информации предприятий Госкорпорации «Росатом»

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

Деятельность органа криптографической защиты информации предприятий Госкорпорации «Росатом»

Цель обучения: Развитие у слушателей компетенций, необходимых для выполнения профессиональной деятельности по эксплуатации органа криптографической защиты информации предприятий Госкорпорации «Росатом»

Продолжительность обучения по программе 40 часа

Режим очного обучения 8 час/день

Форма обучения очное

Номер раздела	Наименование раздела	Количество часов обучения[1]					Виды и форма контроля
		всего	очно		заочно		
			Л	ПЗ	СДО	СР	
1	Введение в криптографическую защиту информации	8	6	2			текущий (опрос)
2	Правовое регулирование деятельности органа криптографической защиты информации предприятий ГК Росатом	4	4				текущий (опрос)
3	Организационное и техническое обеспечение органа криптографической защиты информации предприятий ГК Росатом	4	4				текущий (опрос)

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

Номер раздела	Наименование раздела	Количество часов обучения[1]					Виды и форма контроля
		всего	очно		заочно		
			Л	ПЗ	СДО	СР	
4	Деятельность органа криптографической защиты информации предприятий ГК Росатом	22	3	19			текущий (опрос)
		2					итоговая аттестация (тестирование)
	Итого	40	17	21			

Планируемые результаты обучения

по программе: Деятельность органа криптографической защиты информации предприятий Госкорпорации «Росатом»

Номер раздела учебного плана программы	Профессиональные компетенции, на которые направлено обучение			Код и наименование ОТФ/ТФ[2] (в соответствии с ПС)
	Наименование компетенции	Умения	Знания	
1	Администрирование систем защиты информации автоматизированных систем;		Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах	B/02.6 Администрирование систем защиты информации автоматизированных систем
	Диагностика систем защиты информации автоматизированных систем		Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в автоматизированных системах	B/01.6 Диагностика систем защиты информации автоматизированных систем
	Мониторинг защищенности информации в автоматизированных системах	Классифицировать и оценивать угрозы информационной безопасности	Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах	B/05.6 Мониторинг защищенности информации в автоматизированных системах

[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 соответствии с ПС)
	Наименование компетенции	Умения	Знания	
2	Диагностика систем защиты информации автоматизированных систем		Нормативные правовые акты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	B/01.6 Диагностика систем защиты информации автоматизированных систем
	Мониторинг защищенности информации в автоматизированных системах		Нормативные правовые акты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	B/05.6 Мониторинг защищенности информации в автоматизированных системах
3	Администрирование систем защиты информации автоматизированных систем		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	B/02.6 Администрирование систем защиты информации автоматизированных систем

Номер раздела учебного плана программы	Профессиональные компетенции, на которые направлено обучение			Код и наименование ОТФ/ТФ[2] (в соответствии с ПС)
	Наименование компетенции	Умения	Знания	
			систем; основные меры по защите информации в автоматизированных системах	
	Диагностика систем защиты информации автоматизированных систем		Организационные меры по защите информации	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 обеспечения защиты информации автоматизированных систем; организационные меры по защите информации	B/05.6 Мониторинг защищенности информации в автоматизированных системах
4	Администрирование систем защиты информации автоматизированных систем	Использовать криптографические методы и средства защиты информации в автоматизированных системах; регистрировать и анализировать события, связанные с защитой информации в автоматизированных системах.	Средства защиты информации в автоматизированных системах	B/02.6 Администрирование систем защиты информации автоматизированных систем

Номер раздела учебного плана программы	Профессиональные компетенции, на которые направлено обучение			Код и наименование ОТФ/ТФ[2] (в соответствии с ПС)
	Наименование компетенции	Умения	Знания	
	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	Контролировать события безопасности и действия пользователей автоматизированных систем		B/05.6 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

Деятельность органа криптографической
защиты информации предприятий Госкорпорации «Росатом»

Номер раздела, темы	Наименование разделов, тем	Количество часов обучения[3]					Виды и форма контроля
		всего	очно		заочно		
			Л	ПЗ	СДО	СР	
1	Введение в криптографическую защиту информации	8	6	2			текущий (опрос)
1.1	Основные понятия криптографической защиты информации	2	2				
1.2	Методы и средства криптографической защиты информации	2	2				
1.3	Определение актуальных угроз безопасности информации, при использовании средств криптографической защиты информации	4	2	2			
2	Правовое регулирование деятельности органа криптографической защиты информации предприятий ГК Росатом	4	4				текущий (опрос)
2.1	Система нормативных правовых документов в области криптографической защиты информации	2	2				
2.2	Системы сертификации и лицензирования в области криптографической защиты информации	2	2				
3	Организационное и техническое обеспечение органа криптографической защиты информации предприятий ГК Росатом	4	4				текущий (опрос)
3.1	Организационно-распорядительные документы органа криптографической защиты информации	1	1				
3.2	Размещение и техническое оснащение органа криптографической защиты	1	1				
3.3	Меры и средства обеспечения информационной без-	2	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	
	опасности органа криптографической защиты информации						
4	Деятельность органа криптографической защиты информации предприятий ГК Росатом	22	3	19			
4.1	Делопроизводство органа криптографической защиты информации	8	1	7			
4.2	Установка, настройка и эксплуатация средств криптографической защиты информации	12	1	11			
4.3	Типовые нарушения в работе органа криптографической защиты информации	2	1	1			
		2					итоговая аттестация (тестирование)
	Итого	40	17	21			

УЧЕБНАЯ ПРОГРАММА

Деятельность органа криптографической
защиты информации предприятий Госкорпорации «Росатом»

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, осуществляющие деятельность органа криптографической защиты информации, либо реализующие функции обеспечения информационной безопасности автоматизированных (информационных) систем, администрирования и (или) диагностики систем защиты информации автоматизированных (информационных) систем, и (или) мониторинга защищенности информации в автоматизированных (информационных) системах, использующих криптографические методы и средства защиты информации.

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 по программе «Деятельность органа криптографической защиты информации предприятий Госкорпорации "Росатом"» Срок действия – 3 года
Нормативные ссылки (для «**обязательного**» обучения)	Приказ Госкорпорации «Росатом» от 09.01.2019 № 1/4-П-дсп. Приказ ФАПСИ от 13.06.2001 № 152

2 Содержание программы

№ раздела, темы	Наименование раздела, темы	Краткое содержание
1	Введение в криптографическую защиту информации	Основные понятия криптографической защиты информации. Методы и средства криптографической защиты информации. Определение актуальных угроз безопасности информации, при использовании СКЗИ
1.1	Основные понятия криптографической защиты информации	Л: Криптографическая защита информации, криптографическое средство защиты информации, криптографическое преобразование, алгоритм криптографического пре-

№ раздела, темы	Наименование раздела, темы	Краткое содержание
		образования, 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, 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, средства криптографической защиты информации и другие
1.2	Методы и средства криптографической защиты информации	Л: Национальные криптографические стандарты: алгоритм криптографического преобразования; функция хэширования; процессы формирования и проверки электронной цифровой подписи. Модель криптографической системы защиты информации ГК Росатом. Средства криптографической защиты информации, применяемые в Госкорпорации «Росатом»
1.3	Определение актуальных угроз безопасности информации, при использовании средств криптографической защиты информации	Л: Уровни криптографической защиты информации. Условия применение средств криптографической защиты информации в автоматизированных (информационных) системах. Выбор объектов для защиты информации. Угрозы информационной безопасности. ПЗ: Оценка актуальности угроз безопасности информации, при использовании средств криптографической защиты информации
2	Правовое регулирование деятельности органа криптографической защиты информации предприятий ГК Росатом	Система нормативно-правовых документов в области криптографической защиты информации. Системы сертификации и лицензирования в области криптографической защиты информации
2.1	Система нормативных правовых документов в области криптографической защиты информации	Л: Федеральные законы, указы президента, постановления правительства, документы уполномоченных федеральных органов, документы Госкорпорации «Росатом»
2.2	Системы сертификации и лицензирования в области криптографической защиты информации	Л: Понятия сертификации, аттестации, лицензирования, лицензии, сертификата (аттестата) соответствия, системы сертификации (аттестации, лицензирования). Формы подтверждения соответствия. Системы сертификации средств защиты информации. Системы сертификации и лицензирования ФСБ России
3	Организационное и техническое обеспечение органа криптогра-	Организационно-распорядительные документы органа криптографической защиты информации предприятий ГК «Росатом». Размещение и техническое оснащение органа криптографической защиты информации предприя-

№ раз-дела, темы	Наименование раздела, темы	Краткое содержание
	фической защиты информации предприятий ГК Росатом	тий ГК «Росатом». Меры и средства обеспечения информационной безопасности органа криптографической защиты информации предприятий ГК «Росатом»
3.1	Организационно-распорядительные документы органа криптографической защиты информации	Л: Регламенты процессов. Типовые Инструкции и руководства пользователей органа криптографической защиты
3.2	Размещение и техническое оснащение органа криптографической защиты информации	Л: Требования к размещению, специальному оборудованию, охране и организации режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним. Отраслевые требования по информационной безопасности и использованию средств защиты информации для автоматизированных систем, обрабатывающих информацию, составляющую коммерческую тайну, служебную информацию ограниченного распространения (с пометкой «Для служебного пользования»), а также персональные данные в Госкорпорации «Росатом» и ее организациях. Техническое оснащение ОКЗ
3.3	Меры и средства обеспечения информационной безопасности органа криптографической защиты	Л: Защитные меры и рекомендованные средства криптографической защиты информации органа криптографической защиты информации предприятий Госкорпорации «Росатом»
4	Деятельность органа криптографической защиты информации предприятий ГК Росатом	Делопроизводство ОКЗ. Установка, настройка и эксплуатация СКЗИ ОКЗ. Типовые нарушения в работе ОКЗ
4.1	Делопроизводство органа криптографической защиты информации	Л: Заведение и ведение учетных форм ОКЗ. ПЗ: Ведение журнала учёта СКЗИ, журнала учета движения документов, журнала учета МНИ, журнала администратора безопасности
4.2	Установка, настройка и эксплуатация средств криптографической защиты информации	Л: Средства криптографической защиты, используемые в организациях Госкорпорации «Росатом». ПЗ: Установка, настройка и эксплуатация СКЗИ, используемым в организациях Госкорпорации «Росатом»
4.3	Типовые нарушения в работе органа криптографической защиты информации	Л: Обсуждение типовых нарушения в работе ОКЗ. Вопросы проведения расследований фактов нарушения условий использования средств криптографической защиты информации в организациях Госкорпорации «Росатом». ПЗ: Решение и разбор ситуационных задач по типовым нарушениям в работе отраслевого органа криптографической защиты информации.

3 Контроль качества освоения программы

Метод контроля	Оценочные материалы
Устный опрос	Перечни контрольных вопросов по темам курса.
Компьютерное тестирование	Перечень вопросов по курсу «Деятельность органа криптографической защиты информации предприятий ГК «Росатом»»

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.

5 Законодательные и нормативные правовые акты

1. Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности».
2. Федеральный закон от 03.04.1995 № 40-ФЗ «О федеральной службе безопасности».
3. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
4. Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании».
5. Федеральный закон «О лицензировании отдельных видов деятельности» от 4 мая 2011 года № 99-ФЗ.
6. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».
7. Федеральный закон от 06.04.2011 № 65-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «Об электронной подписи».
8. «Гражданский кодекс Российской Федерации (часть первая)» от 30.11.1994 № 51-ФЗ.
9. «Гражданский кодекс Российской Федерации (часть вторая)» от 26.01.1996 № 14-ФЗ.
10. Стратегия национальной безопасности Российской Федерации (утв. Указом Президента РФ от 31 декабря 2015 г. № 683).
11. Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.).

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

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

14. Постановление Правительства РФ от 16.04.2012 № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

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

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

17. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

18. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры».

19. ГОСТ Р 34.13-2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров.

20. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования.

21. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

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

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

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

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

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

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

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

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

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

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

32. 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.

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

34. 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

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

36. 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.

37. Приказ ФСБ РФ от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»

38. Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»

39. «Единые отраслевые методические указания по информационной безопасности и использованию средств защиты информации для автоматизированных систем, обрабатывающих информацию, составляющую коммерческую тайну, служебную информацию ограниченного распространения (с пометкой «Для служебного пользования»), а также персональные данные в Госкорпорации «Росатом» и ее организациях». Утверждён приказом Госкорпорации «Росатом» от 09.01.2019 № 1/4-П-дсп.

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, 2005.

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

3. Криптография: скоростные шифры / А. Молдовян и др. - М.: БХВ-Петербург, 2014.

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

5. https://crypto.rosatom.ru/dokumentatsiya/

6. https://support.cryptopro.ru/index.php?/Knowledgebase/List