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

12. 2019

ПРОГРАММА

повышения квалификации

Культура информационной безопасности

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
30.12.2019
дата

УЧЕБНЫЙ ПЛАН

Культура информационной безопасности

Цель обучения: Повысить уровень осведомлённости сотрудников предприятий в вопросах информационной безопасности, познакомиться с основными правилами обеспечения информационной безопасности при работе с современными информационными системами.

Продолжительность обучения по программе 16 час

Режим очного обучения 4-8 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 информационную безопасность	2	2				текущий (опрос)
2	Основные угрозы информационной безопасности при использовании информационных и компьютерных систем в системах управления.	6	4	2			текущий (опрос)
3	Основные правила безопасного взаимодействия с информационными и компьютерными системами.	5		5			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	Деловая игра «Правила безопасного взаимодействия с киберсредой».	1		1			текущий (опрос)
5	Круглый стол по проблемным вопросам обеспечения информационной безопасности.	1		1			
		1					итоговая аттестация (тестирование)
	Итого	16	6	9			

Планируемые результаты обучения

по программе: Культура информационной безопасности

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	
1,2	Выявлять угрозы информационной безопасности	Определять основные признаки типовых угроз нарушений против информационной безопасности;	Основные понятия в области информационной безопасности. Основные угрозы безопасности информации в информационных системах.	
3,4,5	Подбирать организационные меры защиты при выявлении угроз информационной безопасности	Применять типовые политики от реализации типовых угроз информационной безопасности;	Организационные меры по защите информации.	

При разработке программы учитывался профессиональный стандарт:

Регистрационный номер ПС	Наименование ПС	Дата введения в действие ПС

[2] Графа заполняется при наличии утвержденного ПС.

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН

Культура информационной безопасности

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.	2	1				текущий (опрос)
1.1	Основные понятия в области информационной безопасности.		1				
1.2	Основные требования к системам защиты, обеспечивающим информационную безопасность		1				
2	Основные угрозы информационной безопасности при использовании информационных и компьютерных систем в системах управления.	6	4	2			текущий (опрос)
2.1	Угрозы безопасности при аутентификации в информационных и управляющих системах.		1	1			
2.2	Угрозы безопасности автоматизированному рабочему месту и при взаимодействии через проводные сети передачи данных.		1				
2.3	Угрозы безопасности при обмене документами в электронном виде через съемные носители или накопители информации и при работе с электронной почтой.		1	1			
2.4	Угрозы безопасности при использовании мобильных устройств обработки информации и беспроводных сетей передачи данных.		1				
3	Основные правила безопасного взаимодействия с информационными и компьютерными системами.	5		5			текущий (опрос)
3.1	Правила безопасной аутентификации в			1			

[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	
	информационных и управляющих системах						
3.2	Правила безопасного использования автоматизированного рабочего места и взаимодействия через проводные сети передачи данных.			1			
3.3	Правила безопасного обмена документами в электронном виде через съемные носители или накопители информации и при работе с электронной почтой.			2			
3.4	Правила безопасного использования мобильных устройств обработки информации и беспроводных сетей передачи данных.			1			
4	Деловая игра «Правила безопасного взаимодействия с киберсредой».	1		1			текущий (опрос)
5	Круглый стол по проблемным вопросам обеспечения информационной безопасности.	1		1			
		1					итоговая аттестация (тестирование)
	Итого	16	6	9			

УЧЕБНАЯ ПРОГРАММА

Культура информационной безопасности

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.

Данная программа предназначена для повышения уровня осведомленности сотрудников обслуживающих подразделений предприятий и организаций, эксплуатирующие средства вычислительной техники в обеспечении работы ядерных объектов, в области информационной безопасности.

Основная цель учебного курса - повысить уровень осведомлённости сотрудников предприятий в вопросах информационной безопасности, познакомиться с основными правилами обеспечения информационной безопасности при работе с современными информационными системами.

Результатом обучения является формирование у сотрудников ядерных объектов основных знаний и практических навыков, обеспечивающих безопасное использование современных информационных систем различного уровня и назначения.

1.1 Требования к слушателям программы

Сотрудники обслуживающих подразделений предприятий и организаций, использующие средства вычислительной техники в обеспечении работы ядерных объектов

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	НИЗКИЙ

1.3 Характеристика программы в системе обучения Госкорпорации «Росатом»

Значение приоритета обучения	ОБЯЗАТЕЛЬНОЕ
Сертификат, подтверждающий определенный уровень развития ПТЗиН и/или квалификации	Тип сертификата: Управление информационной безопасностью и защита государства Подтип сертификата: Другое (управление инф. безопасностью и защита гостайны), удостоверение о повышении квалификации «Культура информационной безопасности» Обязательное, периодичность 1 раз в 3 года
Нормативные ссылки (для «**обязательного**» обучения)	Приказ ГК «Росатом» от 09.01.2019 № 1/4-П-дсп Приказ ФСТЭК России от 21.12.2017 № 235 п.15

2. Содержание программы

Номер раздела, темы	Наименование раздела, темы	Краткое содержание
1	Введение в информационную безопасность.	

Номер раздела, темы	Наименование раздела, темы	Краткое содержание
1.1	Основные понятия в области информационной безопасности.	Л: Основные понятия в области информационной безопасности. Основные методы и способы защиты от угроз информационной безопасности и противодействия компьютерным атакам.
1.2	Основные требования к системам защиты, обеспечивающим информационную безопасность	Требования федеральных уполномоченных органов регуляторов к системам защиты автоматизированных управляющих и информационных систем ядерных объектов.
2	Основные угрозы информационной безопасности при использовании информационных и компьютерных систем в системах управления.	Методы и средства идентификации и процессы аутентификации, основные способы и методы осуществления угроз безопасности.
2.1	Угрозы безопасности при аутентификации в информационных и управляющих системах.	Л: Состав автоматизированного рабочего места обработки информации, основные способы и методы осуществления угроз безопасности. ПЗ: «Основные угрозы информационной безопасности, обусловленные процессами аутентификации пользователей».
2.2	Угрозы безопасности автоматизированному рабочему месту и при взаимодействии через проводные сети передачи данных.	Л: Архитектура современных проводных сетей передачи данных, основные способы и методы осуществления угроз безопасности.
2.3	Угрозы безопасности при обмене документами в электронном виде через съемные носители или накопители информации и при работе с электронной почтой.	Л: Устройство съемные носители информации, основные способы и методы осуществления угроз безопасности. ПЗ: «Основные угрозы информационной безопасности при использовании флэш-накопителей»
2.4	Угрозы безопасности при использовании мобильных устройств обработки информации и беспроводных сетей передачи данных.	Л: Основные средства и технологии обмена документами в электронном виде, основные способы и методы осуществления угроз безопасности.
3	Основные правила безопасного взаимодействия с информационными и компьютерными системами.	
3.1	Правила безопасной аутентификации в информационных и управляющих системах	ПЗ: Основные политики безопасности аутентификации пользователей автоматизированных управляющих и информационных систем.

Номер раздела, темы	Наименование раздела, темы	Краткое содержание
3.2	Правила безопасного использования автоматизированного рабочего места и взаимодействия через проводные сети передачи данных.	ПЗ: Политики безопасности эксплуатации автоматизированного рабочего места и процессов коммуникации в сетях передачи данных.
3.3	Правила безопасного обмена документами в электронном виде через съемные носители или накопители информации и при работе с электронной почтой.	ПЗ: Политики безопасности использования съемных носителей информации. Политики безопасности обмена документами в электронном виде. Политики безопасности использования электронной почты.
3.4	Правила безопасного использования мобильных устройств обработки информации и беспроводных сетей передачи данных.	ПЗ: Политики безопасного использования мобильных устройств обработки информации и беспроводных сетей передачи данных.
4	Деловая игра «Правила безопасного взаимодействия с киберсредой».	ПЗ: «Анализ ситуационных задач взаимодействия с киберсредой»
5	Круглый стол по проблемным вопросам обеспечения информационной безопасности.	ПЗ. В рамках круглого стола рассматриваются проблемные вопросы обеспечения информационной безопасности при выполнении слушателями своих должностных обязанностей.

3. Контроль качества освоения программы

Метод контроля	Оценочные материалы
Текущий контроль	Осуществляется посредством проверки целей обучения на каждом занятии в форме устного опроса, а также выполнения контрольных практических заданий. Текст заданий практических работ приведен в раздаточном материале.
Итоговая аттестация	Проводится в виде тестирования, с использованием теста, содержащего вопросы по всем разделам (темам) курса. Вопросы теста приведены в контрольном блоке обучения.

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 75% – не зачтено; 75% и более – зачтено (успешное прохождение итоговой аттестации)

4. Условия реализации программы

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

- компьютер;
- мультимедийный проектор с экраном и акустической системой;
- флипчарт или маркерная доска с маркерами, либо меловая доска с мелом.

Практические занятия проводятся в учебной аудитории с использованием раздаточных методических материалов и следующих технических средств обучения:

- мультимедийный проектор с экраном.

5. Законодательные и нормативные правовые акты

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
2. Федеральный закон от 26.07.2017 года № 193-ФЗ «О внесении изменений в отдельные законодательные акты РФ в связи с принятием ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
3. Федеральный закон от 26.07.2017 № 194-ФЗ «О внесении изменений в Уголовный Кодекс РФ и Уголовно-процессуальный Кодекс РФ в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»
4. Указ Президента РФ №31с от 15.01.2013 «О создании ГосСОПКА»
5. Постановление правительства РФ № 127 от 08.02.2018 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».
6. Постановление правительства РФ № 162 от 17.02.2018 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности ЗО КИИ РФ»
7. Приказ ФСТЭК России № 229 от 11.12.2017 «Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов КИИ РФ»
8. Приказ ФСТЭК России № 235 от 21.12.2017 «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования»
9. Приказ ФСТЭК России № 236 от 21.12.2017 «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»
10. Приказ ФСТЭК России № 239 от 25.12.2017 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ»
11. Приказ ФСТЭК России № 138 от 09.08.2018 «О внесении изменений в Требования к обеспечению защиты информации в АСУ ТП на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом ФСТЭК от 14 марта 2014 г. N 31, и в Требования по обеспечению безопасности значимых объектов КИИ Российской Федерации, утвержденные приказом ФСТЭК от 25 декабря 2017 г. N 239»
12. Приказ ФСБ России от 24.07.2018 № 366 «О Национальном координационном центре по компьютерным инцидентам»
13. Приказ ФСБ России от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в ГосСОПКА и Порядка представления информации в ГосСОПКА»
14. Приказ ФСБ России от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами КИИ РФ, между субъектами КИИ РФ и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями,

осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами КИИ РФ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»

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

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

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

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