

**НИИ статистики Росстата**

**НАУЧНО-ОБРАЗОВАТЕЛЬНЫЙ ЦЕНТР «КОРПОРАТИВНЫЙ УНИВЕРСИТЕТ РОССТАТА»**

**Утверждаю**

**Директор НИИ статистики Росстата**

**Р.А. Хамзин**

«*05*» *июня* 2021 года



**ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА  
ПОВЫШЕНИЯ КВАЛИФИКАЦИИ**

**ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ФЕДЕРАЛЬНОЙ СЛУЖБЕ  
ГОСУДАРСТВЕННОЙ СТАТИСТИКИ**

Руководитель Научно-образовательного Центра  
«Корпоративный университет Росстата»

*[Signature]*  
В.И. Швей

**МОСКВА, 2021**

## **1. Общая характеристика программы**

### **1.1.Цель реализации программы.**

Целью реализации дополнительной общеразвивающей программы «Обеспечение безопасности информации в Федеральной службе государственной статистики» является получение слушателями новых компетенций и базовых знаний, умений и навыков в области информационной безопасности, необходимых для осуществления профессиональной деятельности; подготовка слушателей к самостоятельному принятию решений, связанных с безопасной работой в сети Интернет, защитой своих персональных данных и финансовых интересов.

### **Планируемые результаты обучения**

В результате обучения по программе слушатель должен знать:

- российское законодательство, регулирующие отношения в области информационной безопасности;
- угрозы и риски, возникающие в процессе использования современных информационных технологий;
- основные тенденции развития киберпреступности;
- правила безопасной работы в Интернете

уметь:

- определять и выявлять признаки вредоносных программ;
- правильно строить защиту конфиденциальной информации, включая персональные данные;
- анализировать и толковать нормы законодательства и судебную практику в сфере информационной безопасности.

владеть:

- навыками безопасной работы в сети Интернет;
- организацией защиты персональных данных

### **1.2.Категория слушателей**

К освоению программы допускаются лица, имеющие или получающие среднее профессиональное или высшее образование.

### **1.3.Трудоемкость обучения**

Нормативная трудоемкость обучения по программе – 18 часов.

#### 1.4. Форма обучения

Очная, с использованием средств удаленного доступа.

## 2. Содержание Программы

### 2.1. Учебный план программы «Обеспечение безопасности информации в Федеральной службе государственной статистики».

№	Наименование разделов, дисциплин	Общая трудоемкость час	Всего ауд час	Аудиторные занятия, ч			СРС <sup>1</sup> , в т.ч. КСР <sup>2</sup> , ч	Форма контроля
				Лекции	Лабораторные работы	Практические и семинарские занятия		
1	2	3	4	5	6	7	8	9
1.	Тема 1.	6	6	4	–	2	–	
2.	Тема 2.	6	6	4	–	2	–	
3.	Тема 3.	4	4	4	–	-	–	
4.	Итоговая аттестация	2			–		–	зачет
	<b>Итого:</b>	<b>18</b>	<b>16</b>	<b>12</b>	<b>–</b>	<b>4</b>	<b>–</b>	<b>2</b>

### Перечень планируемых результатов обучения по дисциплине

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций (код и наименование индикатора)	Результаты обучения (знания, умения)
ПК-1. Автоматизированная информационно-аналитическая поддержка процессов принятия решений	ПК-1.1. Осуществляет формализацию задач автоматизированной информационно-аналитической поддержки процессов принятия решений в сфере безопасности в конкретной предметной области	ПК-1.1. З-1. Знает роль и место информационно-аналитической деятельности в системах организационного управления; методологические основы информационно-аналитической деятельности; принципы организации информационно-аналитической деятельности
		ПК-1.1. У-1. Умеет использовать современные модели и методы измерения, прогнозирования,

<sup>1</sup> СРС – САМОСТОЯТЕЛЬНАЯ РАБОТА СЛУШАТЕЛЯ

<sup>2</sup> КСР – КОНТРОЛЬНО-САМОСТОЯТЕЛЬНАЯ РАБОТА СЛУШАТЕЛЯ

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций (код и наименование индикатора)	Результаты обучения (знания, умения)
		планирования, принятия решений при решении задач поддержки процессов принятия решений
ПК-4. Настройка ИАС для решения задач в сфере профессиональной деятельности	ПК-4.1. Настраивает ИАС для решения информационно-аналитических задач	<p>ПК-4.1. З-4. Знает методологические основы информационно-аналитической деятельности; роль и место информационно-аналитической деятельности в системах организационного управления</p> <p>ПК-4.1. У-4. Умеет применять ИАС в информационно-аналитической деятельности; применять ИАС в процессах организационного управления</p>
ПК-5. Обеспечение функционирования ИАС	ПК-5.1. Осуществляет обслуживание ИАС на всех этапах их жизненного цикла	<p>ПК-5.1. З-5. Знает назначение и классификация информационных и аналитических систем, систем управления; принципы эксплуатации и сопровождения ИАС; программные и программно-аппаратные средства защиты информации</p> <p>ПК-5.1. У-5. Умеет осуществлять меры противодействия нарушениям сетевой безопасности с использованием программных и программно-аппаратных средств защиты информации; применять защищенные протоколы, межсетевые экраны, средства обнаружения вторжений в компьютерные сети</p>

**2.2. Учебно-тематический план «Обеспечение безопасности информации в  
Федеральной службе государственной статистики»**

Наименование разделов, дисциплин	Общ. труд оемк ость, час	Всего ауд, час	Аудиторные занятия, час			Компет енция	Форма контро ля
			Лекц ии	Лаб .	Се ми нар		
2	3	4	5	6	7	8	9
<b>Тема 1</b>	6	6	4		2	ПК-1	
1.1. Цифровая экономика. Влияние новых информационных технологий на развитие цифрового общества. Стратегия развития Росстата и системы государственной статистики в России до 2024 г. Государственная политика РФ в области обеспечения ИБ.	2	2	2	-		-	ТЕСТ
1.2. Концепция национальной безопасности. Доктрина Информационной Безопасности РФ. Государственная система защиты информации (ФСБ РФ, ФСТЭК, МВД РФ и др.). Основные положения федеральных законов РФ в области ИБ («Об информации, информационных технологиях и защите информации», «О государственной тайне», «О безопасности критической информационной инфраструктуры Российской Федерации» и др.	2	2	-	-	2	-	-
1.3. Концепция информационной безопасности Федеральной службы государственной статистики РФ. Информационные системы Росстата. Классификация угроз безопасности в ИС органов государственной власти.	2	2	2	-		-	
<b>Тема 2.</b>	6	4	4	-	2	ПК-4	
2.1 Законы РФ «О коммерческой тайне», «О персональных данных» и др. Российские и международные стандарты ИБ	2	2	2				ТЕСТ
2.2 КСЗИ. Угрозы и риски ИБ. Модели злоумышленника. Компьютерные преступления. Типы вредоносных программ и антивирусы. ПДТР.	2	2		-	2	-	
2.3. Основные требования и рекомендации по защите информации. Организационные методы защиты информации. Инженерно-технические СЗИ. Режим и охрана. СКУД.	2	2	2	-		-	
<b>Тема 3.</b>	6	6	4	-		ПК-5	
3.1. Защита информации от НСД. Парольные системы защиты. Программно-аппаратные, физические и биометрические средства	2	2	2	-		-	ТЕСТ

Наименование разделов, дисциплин	Общ. труд оемк ость, час	Всего ауд, час	Аудиторные занятия, час			Компет енция	Форма контро ля
			Лекц ии	Лаб .	Се ми на р		
2	3	4	5	6	7	8	9
защиты. Антивирусы. Обзор аппаратно-программных СЗИ. Системы ДЛП. Аудит ИБ. Лицензирование ИБ.							
3.2. Влияние человеческого фактора на ИБ организации. Инсайдеры. Методы «социальной инженерии». Информационный терроризм. Кибертерроризм в сети.	2	2	2	–		–	
3.3. Влияние COVID-19 на информационную безопасность организации. Практические советы по организации защиты информации на рабочем месте. Зачет.	2	2	2	–		–	2, зачет
<b>Итого:</b>	<b>18</b>	<b>18</b>	<b>16</b>				<b>2</b>

## **2.3. РАБОЧАЯ УЧЕБНАЯ ПРОГРАММА**

### **Тема 1.**

**1.1.** Цифровая экономика. Влияние новых информационных технологий на развитие цифрового общества. Стратегия развития Росстата и системы государственной статистики в России до 2024 г. Государственная политика РФ в области обеспечения ИБ. Угрозы и риски, связанные с новыми информационными технологиями.

**1.2.** Концепция национальной безопасности. Доктрина Информационной Безопасности РФ. Государственная система защиты информации (ФСБ РФ, ФСТЭК, МВД РФ и др.). Основные положения федеральных законов РФ в области ИБ («Об информации, информационных технологиях и защите информации», «О государственной тайне», «О безопасности критической информационной инфраструктуры Российской Федерации» и др.

**1.3.** Концепция информационной безопасности Федеральной службы государственной статистики РФ. Информационные системы Росстата. Классификация угроз безопасности в ИС органов государственной власти.

### **Тема 2.**

**2.1.** Законы РФ «О коммерческой тайне», «О персональных данных» и др. Российские и международные стандарты ИБ.

**2.2.** КСЗИ. Угрозы и риски ИБ. Модели злоумышленника. Компьютерные преступления. Типы вредоносных программ и антивирусы. ПДТР.

**2.3.** Основные требования и рекомендации по защите информации. Организационные методы защиты информации. Инженерно-технические СЗИ. Режим и охрана. СКУД.

### **Тема 3.**

**3.1.** Защита информации от НСД. Парольные системы защиты. Программно-аппаратные, физические и биометрические средства защиты. Антивирусы. Обзор аппаратно-программных СЗИ. Системы DLP. Аудит ИБ. Лицензирование ИБ.

**3.2.** Влияние человеческого фактора на ИБ организации. Инсайдеры. Методы «социальной инженерии». Информационный терроризм. Кибертерроризм в сети.

**3.3.** Влияние COVID-19 на информационную безопасность организации. Практические советы по организации защиты информации на рабочем месте.

## Учебно-методическое и информационное обеспечение программы

### Рекомендуемая литература

#### Базовые учебники:

1. Баяндин Н.И. Информационно-аналитическое обеспечение безопасности бизнеса. Учебник. СПб.: ИЦ Интермедия, 2016 – 263 с.
2. Баяндин Н.И., Куликова С.В. Подготовка кадров для решения задач информационного противоборства в бизнес-среде. Монография. М.: РУСайнс, 2016, 103 с.
3. Бражников А.Е. Практические рекомендации по безопасной работе в Интернете. М. 2017 – 93 с.
4. Раздаточные материалы к семинару. Составитель Баяндин Н.И., 2020 г. 100 с.
5. Журнал Директор по безопасности. 2014 – 2020 гг.

#### Рекомендуемые Интернет-ресурсы и другие электронные информационные источники:

1. Официальный интернет-портал правовой информации [Электронный ресурс] // URL: <http://pravo.gov.ru/>
2. Справочно-правовая система Консультант Плюс [Электронный ресурс] // URL: <http://www.consultant.ru/>
3. Справочно-правовая система ГАРАНТ [Электронный ресурс] // URL: <http://www.garant.ru/>



## **ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ**

Операционная система Windows 10, Microsoft Office Professional Plus: 2019 год (MS Word, MS Excel, MS Power Point, MS Access)

Антивирус Dr.Web Desktop Security Suite Комплексная защита

Браузер Google Chrome

### **МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

Для реализации программы, дисциплина обеспечена:

- учебной аудиторией для проведения занятий лекционного типа в дистанционном режиме, оборудованной мультимедийными средствами обучения для демонстрации лекций-презентаций, учебно-наглядными пособиями, набором демонстрационного оборудования; с комплектом лицензионного программного обеспечения, операционной системой Microsoft Windows, 10 Pro; пакетом прикладных программ Microsoft Office: 2016 (MS Word, MS Excel, MS Power Point, MS Access); Google Chrome; Microsoft Project;
- помещениями для самостоятельной работы слушателей, оснащенными компьютерной техникой с возможностью подключения к сети «Интернет» и обеспеченной доступом в электронную информационно-образовательную среду Университета;
- помещениями для профилактического обслуживания учебного оборудования, укомплектованными специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации.

Занятия могут проводиться очно.

### **3. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ**

**по дисциплине «Обеспечение безопасности информации в Федеральной службе государственной статистики»,**

**Тема 1. (промежуточное тестирование)**

1. Влияние новых информационных технологий на развитие цифрового общества.
2. Стратегия развития Росстата и системы государственной статистики в России до 2024 г.
3. Государственная политика РФ в области обеспечения ИБ.
4. Концепция национальной безопасности.
5. Доктрина Информационной Безопасности РФ.

6. Государственная система защиты информации (ФСБ РФ, ФСТЭК, МВД РФ и др.).
7. Основные положения федеральных законов РФ в области ИБ («Об информации, информационных технологиях и защите информации», «О государственной тайне», «О безопасности критической информационной инфраструктуры Российской Федерации» и др.
8. Концепция информационной безопасности Федеральной службы государственной статистики РФ.
9. Информационные системы Росстата.
10. Классификация угроз безопасности в ИС органов государственной власти.

### **Тема 2. (промежуточное тестирование)**

1. Законодательство РФ «О коммерческой тайне», «О персональных данных».
2. Российские и международные стандарты информационной безопасности.
3. Угрозы и риски информационной безопасности.
4. Естественные и искусственные технические каналы утечки информации, классификация и способы реализации.
5. Компьютерные преступления.
6. Типы вредоносных программ и антивирусы.
7. Противодействие техническим разведкам.
8. Основные требования и рекомендации по защите информации.
9. Организационные методы защиты информации.
10. Инженерно-технические средства защиты информации.

### **Тема 3. (промежуточное тестирование)**

1. Защита информации от несанкционированного доступа.
2. Парольные системы защиты.
3. Программно-аппаратные, физические и биометрические средства защиты.
4. Системы ДЛП.
5. Аудит ИБ.
6. Влияние человеческого фактора на ИБ организации.
7. Методы «социальной инженерии».
8. Информационный терроризм
9. Влияние COVID-19 на информационную безопасность организации.
10. Практические советы по организации защиты информации на рабочем месте.



**Формирование балльной оценки по дисциплине  
«Обеспечение безопасности информации в Федеральной службе государственной  
статистики»,**

Рейтинговая оценка работы слушателя, осуществляется следующим образом:

Виды работ	Максимальное количество баллов
Посещаемость	40
Текущий и рубежный контроль	30
Зачет	30
<b>ИТОГО</b>	<b>100</b>

**1. Посещаемость**

В соответствии с утвержденным учебным планом по дисциплине «Обеспечение безопасности информации в Федеральной службе государственной статистики», предусмотрено:

3 лекционных и практических занятий, 1 занятие продолжается 6 уч. часов, За посещение 1 занятия назначается 10 баллов. Максимальное количество баллов 40, если слушатель посетил все занятия.

**2. Текущий и рубежный контроль**

Расчет баллов по результатам текущего и рубежного контроля:

Форма контроля	Наименование раздела/ темы, выносимых на контроль	Форма проведения контроля (тест, контр. работа и др. виды контроля в соответствии с Положением)	Количество баллов, максимально
Текущий контроль	Тема 1 – Тема 3	Тестирование	30
<b>Всего</b>			<b>30</b>

При использовании балльно-рейтинговой системы оценивания знаний слушателей ( БРС) - количество баллов, которые может набрать слушатель при соответствующем выполнении задания: минимальная оценка – 4 баллов, максимальная оценка - 10 баллов.(по одной теме)

### **Итоговое тестирование**

Итоговое тестирование проводится по окончанию программы и заключается в ответе слушателя на три вопроса из тестов тем 1-3, выбираемых преподавателем случайным образом.

Программу разработал  
Старший преподаватель-консультант

Н.И. Баяндин