

Приложение № 5

к приказу от 19.12.2018 № 225-аб

**Санкт-Петербургское государственное автономное учреждение
«Центр занятости населения Санкт-Петербурга»**

«СОГЛАСОВАНО»

На заседании рабочей группы по организации
и осуществлению образовательной
деятельности СПб ГАУ ЦЗН

19.12.2018
Протокол № 3

«УТВЕРЖДАЮ»

Директор СПб ГАУ ЦЗН

Горохова Ю.А. Горохова



**ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
повышения квалификации**

«Защита персональных данных»
(наименование программы)

Санкт-Петербург
2019

Настоящая программа не может быть использована без разрешения разработчиков программ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Область применения и нормативные ссылки

Программа повышения квалификации «Защита персональных данных» (далее – программа) нацелена на подготовку специалистов различных категорий, от руководителей структурных подразделений СПб ГАУ ЦЗН до работников, непосредственно занятых работой с персональными данными граждан.

В последнее время в Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных», другие российские законы, регулирующие работу с персональными данными, внесены значительные изменения, принят ряд новых федеральных законов, постановлений Правительства РФ и нормативно-методических документов уполномоченных органов власти, затрагивающих эту сферу деятельности. Требования этих документов и организация работ по их реализации в организации детально рассматриваются в учебном курсе.

Программа регламентирует цели, планируемые результаты, содержание, условия и технологии реализации образовательного процесса, оценку качества подготовки выпускника и включает в себя: учебный план, программы учебных модулей, календарный учебный график, а также оценочные и методические материалы, обеспечивающие реализацию соответствующей образовательной технологии.

Программа разработана в соответствии с:

- Федеральным законом от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
- Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
- Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
- Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне»;
- Федеральным законом от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности»;
- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры российской федерации»;
- Федеральным законом от 28.12.2010 № 390-ФЗ «О безопасности»;
- Федеральным законом от 30.12.2001 № 195-ФЗ «Кодекс российской федерации об административных правонарушениях»;
- Федеральным законом от 13.12.1996 № 63-ФЗ «Уголовный кодекс российской федерации»;
- Постановление Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
- Постановление Правительства Российской Федерации 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»);

- Постановление Правительства Российской Федерации от 24.05.2010 № 365 «О координации мероприятий по использованию информационно-коммуникационных технологий в деятельности государственных органов»;

- Постановление Правительства Российской Федерации от 25.04.2012 № 394 «О мерах по совершенствованию использования информационно-коммуникационных технологий в деятельности государственных органов»;

- Постановление Правительства Российской Федерации от 06.06.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

- Постановление Правительства Российской Федерации от 26.06.1995 № 608 «О сертификации средств защиты информации»;

- Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- Постановление Правительства Российской Федерации от 14.09.2012 № 928 «О базовых государственных информационных ресурсах»;

- Постановление Правительства Российской Федерации от 21.11.2011 № 957 «Об организации лицензирования отдельных видов деятельности»;

- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

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

- Приказом Министерства образования и науки РФ от 01.07.2013 № 499 «Порядок организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;

- Приказом Министерства труда и соцзащиты РФ от 28.11.2016 № 676н «Об утверждении профессионального стандарта «Специалист по оказанию услуг в области занятости населения» (регистрационный номер 860);

- Письмом Министерства образования и науки РФ от 22.04.2015 №ВК-1032/06 «О направлении методических рекомендаций»;

- Письмом Министерства образования и науки РФ от 21.04.2015 №ВК-1013/06 «О направлении методических рекомендаций по реализации дополнительных профессиональных программ»;

- Приказом Министерства образования и науки РФ от 23.08.2017 № 816 «Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ».

1.2. Цель и результаты реализации программы

Цели освоения программы:

- Повышение осведомленности сотрудников в вопросах информационной безопасности и мобилизация на сознательное и неукоснительное выполнение правил обеспечения безопасности.

- Информирование о месте и роли пользователей информационных систем в общей системе обеспечения информационной безопасности организации.

- Информирование о типовых ошибках конечных пользователей автоматизированных

информационных систем при работе с критичной информацией на серверах и рабочих станциях, при использовании электронной почты, при работе в Интернет, при использовании мобильных компьютеров, при удаленном доступе в сеть организации и способах предотвращения инцидентов (противодействия нарушениям безопасности со стороны пользователей).

- Информирование о последствиях ошибочных действий пользователей и рекомендации по противодействию угрозам.

Категория слушателей:

- Руководители структурных подразделений СПб ГАУ ЦЗН, в ведении которых находится организация обработки персональных данных и ее осуществление.

- Руководители и специалисты СПб ГАУ ЦЗН, непосредственно отвечающие за обеспечение информационной безопасности, охрану конфиденциальности информации и реализующие мероприятия по технической защите конфиденциальной информации.

- Рядовые сотрудники СПб ГАУ ЦЗН, работающие со средствами автоматизированной обработки информации.

Таблица 1. Связь программы с профессиональными стандартами

В основу обучения ДПП повышения квалификации положен профессиональный стандарт №860 «Специалист по оказанию услуг в области занятости населения».			
Планируемые результаты обучения направлены на выполнение слушателем:			
обобщенных трудовых функций (ОТФ)	трудовых функций (ТФ)	трудовых действий (ТД)	на уровне квалификации
Содействие гражданам в поиске подходящей работы, работодателям в подборе необходимых работников и осуществление социальных выплат и финансовой поддержки (А)	Содействие гражданам в поиске подходящей работы, работодателям в подборе необходимых работников и осуществление социальных выплат и финансовой поддержки (А/01.6)	Соблюдение конфиденциальности в отношении информации, полученной от граждан	6
	Содействие работодателям в подборе необходимых работников; реализация дополнительных мероприятий в сфере занятости населения (А/02.6)	Соблюдение конфиденциальности в отношении информации, полученной от граждан	6
	Организация оплачиваемых общественных работ и временного трудоустройства граждан (А/03.6)	Соблюдение конфиденциальности в отношении информации, полученной от граждан	6
	Содействие самозанятости	Соблюдение конфиденциальности в	6

	безработных граждан (А/04.6)	отношении информации, полученной от граждан	
	Осуществление социальных выплат и финансовой поддержки гражданам, признанным в установленном порядке безработными (А/05.6)	Соблюдение конфиденциальности в отношении информации, полученной от граждан	6
	Информирование об услугах, оказываемых ЦЗН, и о положении на рынке труда в субъектах Российской Федерации (А/06.6)	Соблюдение конфиденциальности в отношении информации, полученной от граждан	6
	Формирование и ведение регистров получателей государственных услуг в сфере занятости населения (физических лиц и работодателей) (А/07.6)	Соблюдение конфиденциальности в отношении информации, полученной от граждан	6
Организация профессиональной ориентации, психологической поддержки и социальной адаптации безработных граждан на рынке труда (В)	Организация профессиональной ориентации граждан (В/01.6)	Соблюдение конфиденциальности в отношении информации, полученной от граждан	6
	Оказание психологической поддержки безработным гражданам (В/02.6)	Соблюдение конфиденциальности в отношении информации, полученной от граждан	6
	Организация социальной адаптации безработных граждан на рынке труда (В/03.6)	Соблюдение конфиденциальности в отношении информации, полученной от граждан	6
Организация профессионального обучения и дополнительного профессионального образования граждан по направлению органов службы занятости (С)	Организация взаимодействия с образовательными организациями по организации профессионального обучения и дополнительного профессионального образования	Соблюдение конфиденциальности в отношении информации, полученной от граждан	6

	граждан по направлению органов службы занятости (С/01.6)		
	Организация и контроль процесса профессионального обучения и дополнительного (С/02.6)	Соблюдение конфиденциальности в отношении информации, полученной от граждан	6
Организация работы подразделения ЦЗН и руководство им (D)	Руководство деятельностью подразделения ЦЗН и контроль его деятельности в соответствии со специализацией (D/01.7)	Соблюдение конфиденциальности в отношении информации, полученной от граждан	7
	Организация работы по предоставлению услуг в ЦЗН, его контроль (D/02.7)	Соблюдение конфиденциальности в отношении информации, полученной от граждан	7
	Мониторинг услуг, организация информирования граждан по вопросам занятости населения и о положении на рынке труда (D/03.7)	Соблюдение конфиденциальности в отношении информации, полученной от граждан	7
	Контроль работы по оформлению, комплектованию и передаче в архив документов подразделения ЦЗН (D/04.7)	Соблюдение конфиденциальности в отношении информации, полученной от граждан	7
Управление деятельностью ЦЗН, планирование и контроль деятельности ЦЗН (E)	Планирование и контроль деятельности ЦЗН (E/01.8)	Соблюдение конфиденциальности в отношении информации, полученной от граждан	8
	Мониторинг рынка труда и организация работы по информированию граждан о положении на рынке труда (E/02.8)	Соблюдение конфиденциальности в отношении информации, полученной от граждан	8
	Организация совместных мероприятий с органами исполнительной	Соблюдение конфиденциальности в отношении информации, полученной от граждан	8

	власти, местного самоуправления, внебюджетными фондами, учреждениями (МСЭ) и социальными партнерами по вопросам занятости населения (Е/03.8)		
	Управление персоналом ЦЗН (Е/04.8)	Соблюдение конфиденциальности в отношении информации, полученной от граждан	8
	Организация ведения финансово-хозяйственной деятельности ЦЗН (Е/05.8)	Соблюдение конфиденциальности в отношении информации, полученной от граждан	8

Таблица 2. Планируемые результаты обучения

Модуль ДПП	Задачи профессиональной деятельности ¹ (ЗПД)	Профессиональные компетенции, подлежащие формированию (ПК)	Профессиональные компетенции, подлежащие развитию (ПК)
Модуль 1. Обеспечение безопасности персональных данных при их обработке	Соблюдение конфиденциальности в отношении информации, полученной от граждан, посредством обеспечения безопасности персональных данных при их обработке (ЗПД.1)	Способность использовать нормативные правовые документы в своей профессиональной деятельности в части обеспечения безопасности персональных данных при их обработке (ПК.1.1).	
Модуль 2. Криптографические средства защиты информации. Требования по технической защите информации	Соблюдение конфиденциальности в отношении информации, полученной от граждан, средствами криптографической защиты информации (ЗПД.2)	Способность использовать нормативные правовые документы в своей профессиональной деятельности в части защиты персональных данных средствами криптографической защиты информации (ПК.2.1)	
Модуль 3.	Соблюдение	Способность	

¹ Формулируются с учетом ТД.

Модуль ДПП	Задачи профессиональной деятельности ¹ (ЗПД)	Профессиональные компетенции, подлежащие формированию (ПК)	Профессиональные компетенции, подлежащие развитию (ПК)
Криптографические средства защиты информации CryptoPro. Общие сведения	конфиденциальности в отношении информации, полученной от граждан, средствами CryptoPro (ЗПД.3)	использовать нормативные правовые документы в своей профессиональной деятельности в части защиты персональных данных средствами CryptoPro (ПК.3.1)	
Модуль 4. Криптографические средства защиты информации VipNet. Общие сведения	Соблюдение конфиденциальности в отношении информации, полученной от граждан, средствами VipNet (ЗПД.4)	Способность использовать нормативные правовые документы в своей профессиональной деятельности в части защиты персональных данных средствами VipNet (ПК.4.1)	

1.3. Требования к уровню подготовки поступающего на обучение, необходимому для освоения программы

Высшее или среднее профессиональное образование.

1.4. Трудоемкость обучения

Трудоемкость обучения:

- 1 категория – 16 часов (защита ПДн);
- 2 категория – 24 часа (защита ПДн, + СКЗИ + CryptoPro);
- 3 категория – 24 часа (защита ПДн, + СКЗИ + VipNet);
- 4 категория – 28 часов (защита ПДн, СКЗИ + CryptoPro + VipNet).

1.5. Форма обучения

Форма обучения - заочная форма с применением электронного обучения.

1.6. Режим занятий

Максимальная учебная нагрузка 2-4 часа в день.

2. СОДЕРЖАНИЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

2.1. Учебный план

Таблица 3. Учебный план

№ п/п	Наименование модулей	Общая трудоем- кость, час.	Дистанционные занятия, час.		Форма контроля
			Лек- ции	Практичес- кие занятия	
1	2	3	5	6	7
1.	Модуль 1. Обеспечение безопасности персональных данных при их обработке (для всех категорий)	14	10,5	3,5	Тестирование
2.	Криптографические средства защиты информации. Требования по технической защите информации (для категории 2, 3, 4)	4	3	1	Тестирование
3.	Криптографические средства защиты информации CryptoPro. Общие сведения (для категории 2, 4)	4	3	1	Тестирование
4.	Криптографические средства защиты информации VipNet. Общие сведения (для категории 3, 4)	4	3	1	Тестирование
	Итоговый контроль	2		2	Тестирование
	Итого для:				
	1 категории	16	10,5	5,5	
	2 категории	24	16,5	7,5	
	3 категории	24	16,5	7,5	
	4 категории	28	19,5	8,5	

2.2. Учебно-тематический план

Таблица 4. Учебно-тематический план

№ п/п	Наименование модулей	Общая трудоем- кость, час.	Дистанционные занятия, час.		Форма контроля
			Лек- ции	Практичес- кие занятия	
1	2	3	5	6	7
1.	Модуль 1. Обеспечение безопасности персональных данных при их обработке (для всех категорий)	14	10,5	3,5	Тестирование
1.1.	Основные понятия и нормативно-правовое обеспечение защиты персональных данных в Российской Федерации	2	1,5	0,5	Тестирование
1.2.	Персональные данные	2	1,5	0,5	Тестирование
1.3.	Работа с персональными данными в службе занятости без средств автоматизации	2	1,5	0,5	Тестирование
1.4.	Работа с персональными данными в службе занятости с использованием средств автоматизации	2	1,5	0,5	Тестирование
1.5.	Безопасность информации при работе на ПЭВМ. Типичные ошибки операторов при работе с критичной информацией	2	1,5	0,5	Тестирование
1.6.	Безопасная работа с информацией при использовании электронной почты и ресурсов сети Интернет. Типичные ошибки конечных пользователей	2	1,5	0,5	Тестирование
1.7.	Контроль и надзор за соблюдением законодательства о защите информации и персональных данных	2	1,5	0,5	Тестирование
2.	Криптографические средства защиты информации. Требования по технической защите информации (для категории 2, 3, 4)	4	3	1	Тестирование
3.	Криптографические средства защиты информации CryptoPro. Общие сведения (для категории 2, 4)	4	3	1	Тестирование
4.	Криптографические средства защиты информации VipNet. Общие сведения (для категории 3, 4)	4	3	1	Тестирование
	Итоговый контроль	2		2	Тестирование
	Итого для:				
	1 категории	16	10,5	5,5	
	2 категории	24	16,5	7,5	
	3 категории	24	16,5	7,5	
	4 категории	28	19,5	8,5	

2.3. Календарный учебный график

Таблица 5. Календарный учебный график (для категории 1)

		Плановый период реализации программы – 16 час, режим занятий – 2 часа в день															
		1 день		2 день		3 день		4 день		5 день		6 день		7 день		8 день	
Модуль 1. Обеспечение безопасности персональных данных при их обработке	Форма	Д		Д		Д		Д		Д		Д		Д			
	Вид УД	Л	П	Л	П	Л	П	Л	П	Л	П	Л	П	Л	П		
	часов	1,5	0,5	1,5	0,5	1,5	0,5	1,5	0,5	1,5	0,5	1,5	0,5	1,5	0,5		
Итоговый контроль	Форма															Д	
	Вид УД															К	
	часов															2	

Таблица 6. Календарный учебный график (для категории 2)

		Плановый период реализации программы – 24 час, режим занятий – 2-4 часа в день															
		1 день		2 день		3 день		4 день		5 день		6 день		7 день		8 день	
Модуль 1. Обеспечение безопасности персональных данных при их обработке (для всех категорий)	Форма	Д		Д		Д		Д		Д							
	Вид УД	Л	П	Л	П	Л	П	Л	П	Л	П						
	часов	3	1	3	1	1,5	0,5	1,5	0,5	1,5	0,5						
Модуль 2. Криптографические средства защиты информации. Требования по технической защите информации (для категории 2, 3, 4)	Форма											Д					
	Вид УД											Л	П				
	часов											3	1				
Модуль 3. Криптографические средства защиты информации CryptoPro. Общие сведения (для категории 2, 4)	Форма													Д			
	Вид УД													Л	П		
	часов													3	1		
Итоговый контроль	Форма															Д	
	Вид УД															К	
	часов															2	

Таблица 7. Календарный учебный график (для категории 3)

		Плановый период реализации программы – 24 час, режим занятий – 2-4 часа в день															
		1 день		2 день		3 день		4 день		5 день		6 день		7 день		8 день	
Модуль 1. Обеспечение безопасности персональных данных при их обработке (для всех категорий)	Форма	Д		Д		Д		Д		Д							
	Вид УД	Л	П	Л	П	Л	П	Л	П	Л	П						
	часов	3	1	3	1	1,5	0,5	1,5	0,5	1,5	0,5						
Модуль 2. Криптографические средства защиты информации. Требования по технической защите информации (для категории 2, 3, 4)	Форма											Д					
	Вид УД											Л	П				
	часов											3	1				
Модуль 4. Криптографические средства защиты ин-формации VipNet. Общие сведения (для категории 3, 4)	Форма													Д			
	Вид УД													Л	П		
	часов													3	1		
Итоговый контроль	Форма															Д	
	Вид УД															К	
	часов															2	

		Плановый период реализации программы – 28 час, режим занятий – 2-4 часа в день															
		1 день		2 день		3 день		4 день		5 день		6 день		7 день		8 день	
Модуль 1. Обеспечение безопасности персональных данных при их обработке (для всех категорий)	Форма	Д		Д		Д		Д									
	Вид УД	Л	П	Л	П	Л	П	Л	П								
	часов	3	1	3	1	1,5	0,5	3	1								
Модуль 2. Криптографические средства защиты информации. Требования по технической защите информации (для категории 2, 3, 4)	Форма									Д							
	Вид УД									Л	П						
	часов									3	1						
Модуль 3. Криптографические средства защиты ин-формации	Форма											Д					
	Вид УД											Л	П				
	часов											3	1				

СryptoPro. Общие сведения (для категории 2, 4)										
Модуль 4. Криптографические средства защиты информации VipNet. Общие сведения (для категории 3, 4)	Форма							Д		
	Вид УД							Л	П	
	часов							3	1	
Итоговый контроль	Форма									Д
	Вид УД									К
	часов									2

Условные обозначения:

А – аудиторные.

Д – дистанционные.

К – контроль.

Л – лекционное занятие.

П – практическое занятие.

СР – самостоятельная работа.

2.3. Тематическое содержание программы

Модуль 1. Обеспечение безопасности персональных данных при их обработке

Таблица 8. Планируемые результаты обучения

Задача профессиональной деятельности	Соблюдение конфиденциальности в отношении информации, полученной от граждан, посредством обеспечения безопасности персональных данных при их обработке (ЗПД.1)		
Профессиональные компетенции	Слушатель должен знать	Слушатель должен уметь	Слушатель должен владеть (приобрести опыт деятельности)
ПК.1.1	3.1.1.1. содержание основных нормативных правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных 3.1.1.2. меры обеспечения безопасности персональных данных при их обработке без средств автоматизации и при их обработке в информационных системах 3.1.1.3. основные виды угроз безопасности персональных данных при их обработке без средств автоматизации 3.1.1.4. порядок применения организационных мер обеспечения персональных данных при их обработке без средств автоматизации 3.1.1.5. основные виды угроз безопасности персональных данных при их обработке в информационных системах 3.1.1.6. порядок применения организационных мер обеспечения персональных данных при их обработке в информационных	У.1.1.1. осуществлять мероприятия в своей профессиональной деятельности по обеспечению безопасности персональных данных без средств автоматизации У.1.1.2. определять состав и содержание мер по обеспечению безопасности персональных данных при их обработке без средств автоматизации, необходимых для блокирования угроз безопасности персональных данных У.1.1.3. осуществлять мероприятия в своей профессиональной деятельности по обеспечению безопасности персональных данных в информационных системах У.1.1.4. определять состав и содержание мер по обеспечению безопасности персональных данных при их	О.1.1.1. навыком определения уровня защиты персональных данных при их обработке без средств автоматизации О.1.1.2. навыком выявления угроз безопасности персональных данных при их обработке без средств автоматизации и в информационных системах О.1.1.3. навыком определения уровня защиты персональных данных при их обработке в информационных системах

	системах 3.1.1.7. основные виды угроз безопасности персональных данных	обработке в информационных системах, необходимых для блокирования угроз безопасности персональных данных У.1.1.5. применять правила безопасности информации при работе на ПЭВМ У.1.1.6. применять правила безопасности информации при использовании электронной почты и ресурсов сети Интернет	
--	---	--	--

Таблица 9. Описание образовательного процесса

№ п/п	Тема занятия	Коли- чество часов	Форма организации учебного занятия	Основные элементы содержания	Формируемые элементы профессиона- льной компетенции
1.	Основные понятия и нормативно- правовое обеспечение защиты персональных данных в Российской Федерации	2	Л 1,5 П 0,5	Цель и задачи обучения. Содержание учебной программы. Основные понятия, термины, определения (информация, персональные данные, конфиденциальная информация, защита информации и т.д.). Актуальность проблемы защиты информации. Защита персональных данных как реализация конституционных прав граждан на неприкосновенность частной жизни. Законодательная и нормативная база регламентирующая вопросы защиты информации и персональных данных. Основные понятия в	3.1.1.1

				Федеральном законе от 27 июля 2006 года № 152-ФЗ «О персональных данных» и Трудовом кодексе РФ (Глава 14). Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года N 149-ФЗ.	
2.	Персональные данные	2	Л 1,5 П 0,5	Классификация персональных данных. Персональные данные в системе документооборота службы занятости. Персональные данные в автоматизированных системах и приложениях. Обработка персональных данных: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение. Принципы обработки персональных данных. Условия обработки персональных данных. Согласие субъекта. Особенности обработки персональных данных в государственных или муниципальных информационных системах персональных данных (ИСПДн). Права субъектов персональных данных и их соблюдение при обработке. Обязанности оператора персональных данных в ходе сбора и обработки персональных данных, ответы на запросы	3.1.1.2

				субъектов. Прекращение обработки. Уведомления об обработке персональных данных в уполномоченный орган по защите прав субъектов персональных данных.	
3.	Работа с персональным и данными в службе занятости без средств автоматизации	2	Л 1,5 П 0,5	Персональные данные сотрудников и субъектов персональных данных. Примерный перечень персональных данных, обрабатываемых в службе занятости. Ограничение доступа к персональным данным. Учет лиц, допущенных к персональным данным. Определение порядка обращения с персональными данными, контроль его соблюдения. Доступ лиц в помещения, где ведется обработка персональных данных. Понятие «контролируемой зоны». Лица, ответственные за организацию обработки и безопасность персональных данных в структурных подразделениях службы занятости. Хранение персональных данных. Учет хранилищ, носителей и операций (печать, копирование, тиражирование и т.п.). Особенности обработки персональных данных, осуществляемой без использования средств автоматизации. Документы, содержащие персональные данные. Передача документов, содержащих персональные данные, внутри структурного подразделения и между подразделениями. Порядок выноса	3.1.1.3, 3.1.1.4, 3.1.1.7, У.1.1.1, У.1.1.2, О.1.1.1, О.1.1.2

				персональных данных за пределы контролируемой зоны. Передача персональных данных третьим лицам. Ответы на запросы сторонних организаций.	
4.	Работа с персональным и данными в службе занятости с использованием средств автоматизации	2	Л 1,5 П 0,5	Информационные системы, используемые в службе занятости, в том числе информационные системы персональных данных (ИСПДн). Уровни защищенности персональных данных при их обработке в ИСПДн в зависимости от угроз безопасности этим данным и классификации ИСПДн. Каналы утечки информации при обработке в информационных системах. Организация доступа к информационным и автоматизированным системам. Обработка персональных данных, осуществляемая с использованием средств автоматизации. Требования по безопасности, обязательные для исполнения при обработке персональных данных (разделение полномочий, разрешительная система доступа, парольная защита, использование лицензионного ПО, применение антивирусной защиты, применение криптографических средств и межсетевых экранов, правило чистого стола, правила работы в электронной почте и интернет). Внутренние нормативные документы по обработке персональных данных и	3.1.1.2, 3.1.1.5, 3.1.1.6, 3.1.1.7, У.1.1.3, У.1.1.4, О.1.1.2, О.1.1.3

				обеспечению их безопасности (положения, инструкции, порядки и т.д.).	
5.	Безопасность информации при работе на ПЭВМ. Типичные ошибки операторов при работе с критичной информацией	2	Л 1,5 П 0,5	Использование ресурсов рабочих станций не по назначению. Порча и хищение оборудования, а также непринятие мер по их предотвращению. Использование сторонних средств вычислительной техники и отчуждаемых носителей информации. Самостоятельная установка и запуск сторонних программ. Изменение режимов, отключение или создание помех для работы антивирусных программ. Понятие о компьютерных вирусах. Как реагировать на вирусные атаки. Использование нелегального (пиратского) программного обеспечения. Ввод ошибочных данных, искажение или утрата важных файлов. Нарушение установленного порядка обращения с конфиденциальной информацией (создание, учет, хранение, передача, уничтожение). Нарушение правил использования паролей и средств усиленной аутентификации. Использование простых для подбора паролей, работа под чужими учетными записями. Меры предосторожности при работе с паролями.	У.1.1.5, О.1.1.2
6.	Безопасная работа с информацией при	2	Л 1,5 П 0,5	Личная (непроизводственная) переписка по электронной почте.	У.1.1.6, О.1.1.2

	использовани и электронной почты и ресурсов сети Интернет. Типичные ошибки конечных пользователей			Пересылка корпоративных конфиденциальных сведений по незащищенным каналам связи. Отправка конфиденциальных сведений по ошибочным адресам. Перегрузка серверов и каналов связи путем пересылки файлов больших объемов. Использование архивирования файлов для уменьшения объема пересылаемых сообщений. Непринятие мер в отношении СПАМа. Простейшие правила защиты от СПАМа. Опасность заражения вирусами через электронную почту. Использование доступа в Интернет в личных целях. Посещение хакерских или взломанных хакерами Интернет – сайтов.	
7.	Контроль и надзор за соблюдением законодательс тва о защите информации и персональных данных	2	Л 1,5 П 0,5	Система государственного контроля и надзора за обеспечением безопасности персональных данных. Контроль за обеспечением и соблюдением безопасности при работе с персональными данными в службе занятости. Ответственность за нарушение требований по обращению с персональными данными: гражданско-правовая, уголовная, административная, дисциплинарная, материальная. Практика правоприменения.	3.1.1.1

Модуль 2. Криптографические средства защиты информации. Требования по технической защите информации

Таблица 10. Планируемые результаты обучения

Задача профессиональной деятельности	Соблюдение конфиденциальности в отношении информации, полученной от граждан, средствами криптографической защиты информации (ЗПД.2)		
Профессиональные компетенции	Слушатель должен знать	Слушатель должен уметь	Слушатель должен владеть (приобрести опыт деятельности)
ПК.2.1	3.2.1.1. содержание основных нормативных правовых актов по технической защите информации 3.2.1.2. знать типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации 3.2.1.3. правила применения криптографических средств защиты информации	У.2.1.1. осуществлять мероприятия в своей профессиональной деятельности по обеспечению безопасности персональных данных криптографическими средствами защиты информации	О.2.1.1. навыком выявления угроз безопасности персональных данных при их обработке в информационных системах криптографическими средствами защиты информации

Таблица 11. Описание образовательного процесса

№ п/п	Тема занятия	Количество часов	Форма организации учебного занятия	Основные элементы содержания	Формируемые элементы профессиональной компетенции
1.	Криптографические средства защиты информации. Требования по технической защите информации	4	Л 3 П 1	Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения	3.2.1.1, 3.2.1.2, 3.2.1.3, У.2.1.1, О.2.1.1

				безопасности персональных данных при их обработке в информационных системах. Специальные требования и рекомендации по технической защите конфиденциальной информации. Организация и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну. Рекомендации по защите информации в органах исполнительной власти субъектов Российской Федерации, осуществляющих переданные полномочия в области содействия занятости населения и государственных учреждениях.	
--	--	--	--	---	--

Модуль 3. Криптографические средства защиты информации CryptoPro. Общие сведения

Таблица 12. Планируемые результаты обучения

Задача профессиональной деятельности	Соблюдение конфиденциальности в отношении информации, полученной от граждан, средствами CryptoPro (ЗПД.З)		
Профессиональные компетенции	Слушатель должен знать	Слушатель должен уметь	Слушатель должен владеть (приобрести опыт деятельности)
ПК.3.1	3.3.1.1. знать типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств CryptoPro,	У.3.1.1. осуществлять мероприятия в своей профессиональной деятельности по обеспечению безопасности персональных данных	О.3.1.1. навыком выявления угроз безопасности персональных данных при их обработке в информационных системах

	предназначенных для защиты информации 3.3.1.2. правила применения криптографических средств защиты информации CryptoPro	криптографическими средствами защиты информации CryptoPro	криптографическими средствами защиты информации CryptoPro
--	---	--	--

Таблица 13. Описание образовательного процесса

№ п/п	Тема занятия	Количество часов	Форма организации учебного занятия	Основные элементы содержания	Формируемые элементы профессиональной компетенции
1.	Криптографические средства защиты информации CryptoPro. Общие сведения	4	Л 3 П 1	Основные характеристики CryptoPro. Область применения. Правила и порядок использования CryptoPro. Правила безопасности.	3.3.1.1, 3.3.1.2, У.3.1.1, О.3.1.1

Модуль 4. Криптографические средства защиты информации VipNet. Общие сведения

Таблица 14. Планируемые результаты обучения

Задача профессиональной деятельности	Соблюдение конфиденциальности в отношении информации, полученной от граждан, средствами VipNet (ЗПД.4)		
Профессиональные компетенции	Слушатель должен знать	Слушатель должен уметь	Слушатель должен владеть (приобрести опыт деятельности)
ПК.4.1	3.4.1.1. знать типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств VipNet, предназначенных для защиты информации 3.3.1.2. правила применения криптографических средств защиты информации VipNet	У.4.1.1. осуществлять мероприятия в своей профессиональной деятельности по обеспечению безопасности персональных данных криптографическими средствами защиты информации VipNet	О.4.1.1. навыком выявления угроз безопасности персональных данных при их обработке в информационных системах криптографическими средствами защиты информации VipNet

Таблица 15. Описание образовательного процесса

№ п/п	Тема занятия	Количество часов	Форма организации учебного занятия	Основные элементы содержания	Формируемые элементы профессиональной компетенции
1.	Криптографические средства защиты информации VipNet. Общие сведения	4	Л 3 П 1	Что такое VipNet и зачем он нужен? Идентификация пользователя VipNet. Основные характеристики VipNet. Состав VipNet Клиент. О назначении и правилах работы с модулями VipNet Клиент: Контроль приложений, Монитор, Деловая почта.	3.4.1.1, 3.4.1.2, У.4.1.1, О.4.1.1

3. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

3.1. Требования к квалификации педагогических кадров, представителей предприятий и организаций, обеспечивающих реализацию образовательного процесса

Реализация образовательного процесса происходит с использованием электронного обучения без взаимодействия слушателей и педагогических работников. При необходимости проведения консультации могут привлекаться специалисты СПб ГАУ ЦЗН, ответственные за обеспечение защиты персональных данных. Для решения организационных вопросов для каждой группы назначается куратор из числа сотрудников учебно-методического отдела.

3.2. Требования к материально-техническим условиям

Проведение занятий по программе повышения квалификации не требует специализированных аудиторий и учебно-лабораторного оборудования. Обучение происходит на рабочем месте слушателя курса.

Для проведения занятий используется портал СДО для сотрудников СПб ГАУ ЦЗН <http://192.168.99.16>.

Каждый слушатель обеспечен доступом к электронно-библиотечной системе (электронной библиотеке) <http://biblioclub.ru>, которая содержит различные издания по основным темам. Электронная библиотека обеспечивает возможность индивидуального доступа каждого слушателя из любой точки, в которой имеется доступ к сети Интернет.

3.3. Требования к информационным и учебно-методическим условиям

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основная литература:

1. Фаронов А.Е. Основы информационной безопасности при работе на компьютере / А. Е. Фаронов. – Москва: Интернет-Университет Информационных Технологий, 2011 – 138 с.
2. Петренко В.И. Защита персональных данных в информационных системах: учебное пособие / В. И. Петренко. – Ставрополь: СКФУ, 2016 – 201 с.

Дополнительная литература:

1. Конфиденциальное делопроизводство и защищенный электронный документооборот: учебник / А. Г. Фабричнов, А. С. Дёмушкин, Т. В. Кондрашова, Н. Н. Куняев; под общей редакцией Н.Н. Куняева. - Москва: Логос, 2011 – 452 с. (Новая университетская библиотека).
2. Скрипник Д.А. Обеспечение безопасности персональных данных: курс / Д. А. Скрипник. – Москва: Интернет-Университет Информационных Технологий, 2011 – 109 с.

Сайты

Гарант <http://www.garant.ru>.

4. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

4.1. Текущий контроль успеваемости и промежуточная аттестация

Текущий контроль успеваемости и промежуточная аттестация по всем модулям предусмотрена в виде выполнения слушателями тестовых заданий.

4.2. Итоговая аттестация

Итоговая аттестация проводится в форме тестирования.

4.3. Формы контроля знаний слушателей

Тип контроля	Форма контроля
Текущий	Тестирование
Промежуточный	Тестирование
Итоговый	Тестирование

4.4. Порядок формирования оценок по программе повышения квалификации

Оценки по всем видам контроля выставляются по форме зачтено / не зачтено.

4.5. Оценочные материалы для проведения оценки качества освоения программы повышения квалификации

4.5.1. Паспорт комплекта оценочных средств

Предмет(ы) оценивания	Объект(ы) оценивания	Критерии оценки	Показатели оценки
ПК.1.1	Тест	Зачтено Не зачтено	от 85% и более менее 85 %
ПК.2.1	Тест	Зачтено Не зачтено	от 85% и более менее 85 %
ПК.3.1	Тест	Зачтено Не зачтено	от 85% и более менее 85 %
ПК.4.1	Тест	Зачтено Не зачтено	от 85% и более менее 85 %

4.5.2. Комплект оценочных средств

Модуль 1. Обеспечение безопасности персональных данных при их обработке (для всех категорий)

Тема 1. Основные понятия и нормативно-правовое обеспечение защиты персональных данных в Российской Федерации

Пример тестового задания:

1. Кем является СПб ГАУ ЦЗН в части обработки персональных данных?

Варианты ответа:

1. Оператор персональных данных
2. Субъект персональных данных
3. Регулятор персональных данных

4. Оператор ИСПДн
2. Какие действия относятся к обработке персональных данных?
Варианты ответа:
 1. Сбор, запись, систематизация, накопление и хранение
 2. Обновление, изменение и извлечение
 3. Использование
 4. Передача, распространение и предоставление
 5. Обезличивание
 6. Блокирование
 7. Удаление
3. Установите соответствие между понятиями и определениями
Понятие
 1. Блокирование персональных данных
 2. Несанкционированный доступ
 3. Обезличивание персональных данных
 Определение
 1. Временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).
 2. Доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации
 3. Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных

Тема 2. Персональные данные

Пример тестового задания:

1. Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных, называются:
Варианты ответа:
 1. Специальные категории персональных данных
 2. Биометрические персональные данные
 3. Иные персональные данные
 4. Общедоступные персональные данные
2. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не относятся к специальным категориям персональных данных, называются:
Варианты ответа:
 1. Специальные категории персональных данных
 2. Биометрические персональные данные
 3. Иные персональные данные
 4. Общедоступные персональные данные
3. Как называются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных?
Варианты ответа:
 1. Специальные категории персональных данных
 2. Биометрические персональные данные
 3. Иные персональные данные

4. Общедоступные персональные данные
4. В какой срок, с момента получения запроса, необходимо предоставить субъекту его персональные данные для ознакомления?
Варианты ответа:
 1. В момент обращения
 2. 7 дней
 3. 10 дней
 4. 30 дней
7. К какой категории относятся персональные данные, обрабатываемые в СПб ГАУ ЦЗН?
Варианты ответа:
 1. Специальные категории персональных данных
 2. Биометрические персональные данные
 3. Иные персональные данные
 4. Специальные данные
8. Кто поручает сотруднику СПб ГАУ ЦЗН обрабатывать персональные данные субъектов ПДн?
Варианты ответа:
 1. Директор СПб ГАУ ЦЗН
 2. Гражданин, обратившийся в СПб ГАУ ЦЗН за получением государственных услуг
 3. Начальник отдела
 4. Начальник службы безопасности
9. Укажите, условия допуска сотрудников СПб ГАУ ЦЗН к обработке персональных данных?
Варианты ответа:
 1. Сотрудник ознакомлен с необходимостью обработки персональных данных
 2. Сотрудник ознакомлен с перечнем обрабатываемых им ПДн
 3. Сотрудник ознакомлен с положениями законодательства РФ о ПДн
 4. Сотрудник подписал обязательство о неразглашении данных, к которым он допущен
 5. Сотрудник включен в список лиц, имеющих доступ к ПДн
 6. Издан Приказ о допуске сотрудника к обработке ПДн
 7. Получено разрешение контролирующего органа для сотрудника
10. Какое из утверждений является верным?
Варианты ответа:
 1. Возможно хранение конфиденциальной информации на отчуждаемых носителях, которые выдаются пользователям под роспись
 2. Хранение конфиденциальной информации на отчуждаемых носителях запрещено
11. Какое из утверждений является верным?
Варианты ответа:
 1. Допускается самостоятельное пребывание сотрудников, не являющихся уполномоченными лицами на обработку персональных данных, в помещениях для обработки ПДн
 2. Самостоятельное пребывание в помещениях для обработки ПДн не сотрудников СПб ГАУ ЦЗН запрещено
12. Что может потребовать субъект персональных данных от оператора персональных данных в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки?
Варианты ответа:
 1. Уточнения персональных данных
 2. Блокировки

3. Уничтожения
4. Опубликования
13. От каких неправомерных или случайных действий должны быть защищены персональные данные при их обработке оператором персональных данных?
Варианты ответа:
 1. Доступ
 2. Уничтожение
 3. Изменение
 4. Блокировка
 5. Копирование
 6. Предоставление
 7. Распространение

Тема 3. Работа с персональными данными в службе занятости без средств автоматизации

Пример тестового задания:

1. Укажите, в каких системах СПб ГАУ ЦЗН обрабатываются персональные данные сотрудников
Варианты ответа:
 1. Единая автоматизированная информационная система
 2. АИС Парус-Бюджет
 3. Альфа-Банк Клиент
 4. АИС-БП Комитета финансов
 5. Система отчетности через Интернет (ПФР, ФНС, ФСС).
 6. Астра Клиент-Банк
2. Работодатель вправе обрабатывать персональные данные сотрудников СПб ГАУ ЦЗН только после
Варианты ответа:
 1. Письменного согласия сотрудника
 2. Устного согласия сотрудника
 3. Письменного согласия сотрудника, заверенного нотариально
3. В каких отделах СПб ГАУ ЦЗН осуществляется обработка персональных данных сотрудников СПб ГАУ ЦЗН?
Варианты ответа:
 1. Отдел бухгалтерской отчетности
 2. Отдел управления персоналом
 3. Материально-технический отдел
 4. Отдел ЕАИС
4. Укажите, какое из утверждений является верным?
Варианты ответа:
 1. ПДн в СПб ГАУ ЦЗН обрабатываются внутри контролируемых зон, в специально выделенных для этого помещениях
 2. ПДн в СПб ГАУ ЦЗН обрабатываются в специально выделенных для этого помещениях
5. Укажите, какое из утверждений в отношении бесконтрольного нахождения посторонних лиц в помещениях, в которых ведется обработка персональных данных является верным
Варианты ответа:
 1. Нахождение невозможно
 2. Нахождение возможно
 3. Нахождение возможно с разрешения начальника отдела
6. Укажите, какое из утверждений в отношении ответственности сотрудников СПб ГАУ ЦЗН, осуществляющих обработку персональных данных является верным

Варианты ответа:

1. Наличие ответственных за организацию обработки и безопасность персональных данных не снимает персональную ответственность с сотрудников СПб ГАУ ЦЗН за сохранность ПДн, целостность, достоверность и соблюдение режима конфиденциальности при их обработке
2. Наличие ответственных за организацию обработки и безопасность персональных данных снимает персональную ответственность с сотрудников СПб ГАУ ЦЗН за сохранность ПДн, целостность, достоверность и соблюдение режима конфиденциальности при их обработке
7. Какой способ обработки персональных данных используется в СПб ГАУ ЦЗН?
Варианты ответа:
 1. Автоматизированный
 2. Неавтоматизированный
 3. Смешанный (автоматизированный и неавтоматизированный)
8. Как называется физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных?
Варианты ответа:
 1. Оператор персональных данных
 2. Субъект персональных данных
 3. Клиент персональных данных
 4. Контрагент персональных данных
9. Укажите правила хранения персональных данных?
Варианты ответа:
 1. Хранятся только в установленных помещениях
 2. Определен круг лиц, допущенных к обработке ПДн
 3. Хранятся в специальных шкафах
 4. Хранятся в столах
 5. Хранятся отдельно от другой информации
 6. Хранятся совместно с другой информацией

Тема 4. Работа с персональными данными в службе занятости с использованием средств автоматизации

Пример тестового задания:

1. Укажите, какие системы используется в СПб ГАУ ЦЗН для обработки ПДн граждан субъектов ПДн и сотрудников СПб ГАУ ЦЗН
Варианты ответа:
 1. Единая автоматизированная информационная система
 2. АИС Парус-Бюджет
 3. Альфа-Банк Клиент
 4. Информационно-интерактивный ресурс для взаимодействия с гражданами и работодателями в сети Интернет
 5. АИС Регистры получателей государственных услуг Роструда
 6. АИС-БП Комитета финансов
 7. СЭД Сбербанка
 8. Система Межведомственного электронного взаимодействия исполнительных органов государственной власти
 9. Система отчетности через Интернет (ПФР, ФНС, ФМС и т.п.).
2. Укажите, с помощью чего может происходить утечка информации?
Варианты ответа:
 1. Электронная почта
 2. Чтение информации с экранов
 3. Вредоносное ПО

4. Интернет (блоги, форумы, социальные сети, Skype, ICQ)
 5. Внешние накопители данных
 6. Антивирусное ПО
 7. Голосовой ввод и вывод данных
3. Укажите, что относится к недокументированным возможностям программного обеспечения
- Варианты ответа:
1. Функции программного обеспечения, которые предназначены для пользователей, но не описанные в документации по недосмотру
 2. Функции программного обеспечения, которые не предназначены для конечных пользователей и не описанные в документации
 3. Функции программного обеспечения, которые не были предусмотрены изготовителем или были им умышленно скрыты
 4. Функции программного обеспечения, которые предназначены для пользователей и описанные в документации
4. Установите соответствие между требованием, направленным на безопасность персональных данных и его описанием
- Понятие
1. Разделение полномочий
 2. Разрешительная система доступа
- Определение
1. При работе с данными, документами каждый сотрудник должен выполнять заранее определенный перечень работ
 2. Доступ к информации предоставляется непосредственным руководителем либо лицом, выполняющим его обязанности
5. Установите соответствие между требованием, направленным на безопасность персональных данных и его описанием
- Понятие
1. Правило чистого стола
 2. Использование лицензионного ПО
- Определение
1. При работе с персональными данными необходимо убирать прочие документы из рабочей области (стола) для предотвращения случайной утери или порчи данных.
 2. Программное обеспечение, используемое для обработки персональных данных, должно быть получено из достоверных источников и иметь соответствующие документы, подтверждающие законность использования
6. Укажите, что относится к недокументированным возможностям программного обеспечения
- Варианты ответа:
1. Функции программного обеспечения, которые предназначены для пользователей, но не описанные в документации по недосмотру
 2. Функции программного обеспечения, которые не предназначены для конечных пользователей и не описанные в документации
 3. Функции программного обеспечения, которые не были предусмотрены изготовителем или были им умышленно скрыты
 4. Функции программного обеспечения, которые предназначены для пользователей и описанные в документации

Тема 5. Безопасность информации при работе на ПЭВМ. Типичные ошибки операторов при работе с критичной информацией

Пример тестового задания:

1. Какие действия помогут избежать заражения компьютерными вирусами?
Варианты ответа:
 1. Проверять все файлы, пришедшие по электронной почте
 2. Не отвечать на письма рекламного характера, пришедшие по электронной почте
 3. Не устанавливать сомнительное или неизвестное программное обеспечение
 4. Не указывать адреса своей почты на непроверенных сайтах
 5. Использовать простые и легко запоминающиеся пароли
 6. Проверять на наличие вирусов все внешние носители информации перед использованием
 7. Выключать компьютер во время рабочего перерыва
2. Укажите, какое из утверждений в части использования отчуждаемых носителей информации является верным
Варианты ответа:
 1. Допускается хранение конфиденциальной информации на отчуждаемых носителях информации
 2. Не допускается хранение конфиденциальной информации на отчуждаемых носителях информации
 3. Хранение конфиденциальной информации на отчуждаемых носителях информации допускается только с разрешения ответственного сотрудника
3. Укажите правила использования отчуждаемых носителей информации
Варианты ответа:
 1. Учитываются в специальном журнале
 2. Маркируются
 3. Выдаются под роспись
 4. Могут храниться другими сотрудниками
 5. Могут передаваться другим сотрудникам
4. Укажите, какое из утверждений в части использования неучтенных носителей информации является верным:
Варианты ответа:
 1. Использование неучтенных носителей информации запрещено
 2. Разрешено использование неучтенных носителей информации
 3. Использование неучтенных носителей информации разрешено только с разрешения ответственного сотрудника
5. Какая ответственность может наступить при использовании нелицензионных программ?
Варианты ответа:
 1. Уголовная
 2. Административная
 3. Гражданско-правовая
 4. Все перечисленные
6. Укажите основные признаки заражения компьютерным вирусом:
Варианты ответа:
 1. Сигналы антивирусной программы об обнаружении вирусного ПО
 2. Вывод на экран непредусмотренных сообщений или изображений
 3. Подача непредусмотренных звуковых сигналов
 4. Постоянное появление информации об ошибках
 5. Неправильная работа программ или медленная работа компьютера
 6. Невозможность загрузки ОС Windows
 7. Отключение монитора
 8. Отключение питания
7. Какие требования предъявляются к паролю?
Варианты ответа:
 1. Длина пароля должна быть не менее 6 символов

2. Длина пароля должна быть не менее 8 символов
3. Пароль должен состоять из букв английского алфавита в верхнем и нижнем регистрах, цифры и (или) специальных символов
4. Пароль должен состоять из букв английского алфавита в верхнем и нижнем регистрах

Тема 6. Безопасная работа с информацией при использовании электронной почты и ресурсов сети Интернет. Типичные ошибки конечных пользователей

Пример тестового задания:

1. Укажите, правила, предотвращающие получение нежелательных сообщений рекламного характера (СПАМ)?
Варианты ответа:
 1. Не указывать адрес почты в Интернете
 2. Не использовать адрес почты для регистрации на сомнительных ресурсах
 3. Не отвечать на письма рекламного характера, пришедшие по электронной почте
 4. Не загружать содержимое из СПАМ-писем, пришедших по электронной почте
 5. Архивировать СПАМ-письма перед удалением
2. Какие действия предотвратят отправку электронных писем по ошибочным адресам?
Варианты ответа:
 1. Использовать функцию «ответить» или адресную книгу почтового клиента
 2. Копировать адрес из достоверных источников
 3. Отвечать на письма с общедоступных почтовых серверов (Yandex, Google и т.п.)

Тема 7. Контроль и надзор за соблюдением законодательства о защите информации и персональных данных

Пример тестового задания:

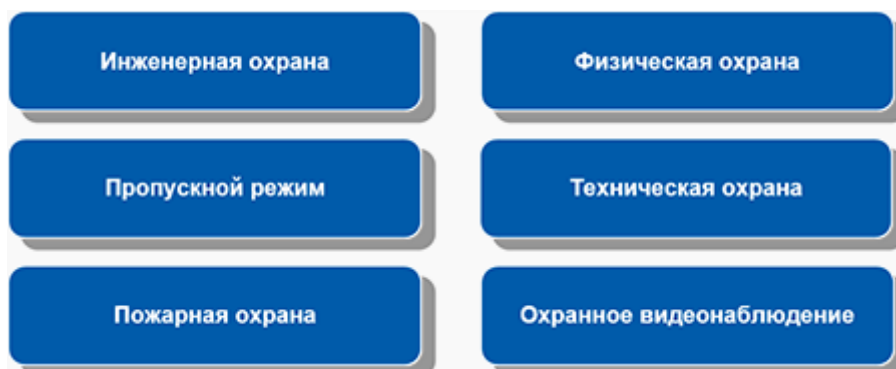
1. Укажите, кто является уполномоченным органом в области соблюдения норм и требований по обработке персональных данных и защиты прав субъектов персональных данных?
Варианты ответа:
 1. Роспотребнадзор
 2. ФСТЭК
 3. Роскомнадзор
 4. ФСБ
2. Какую ответственность, предусмотренную законодательством Российской Федерации, несут лица, виновные в нарушении требований Федерального закона «О персональных данных»?
Варианты ответа:
 1. Уголовную
 2. Дисциплинарную
 3. Административную
 4. Материальную

Пример тестового задания по модулю 1:

1. Укажите, кто является субъектом персональных данных СПб ГАУ ЦЗН
Варианты ответа:

1. Действующие сотрудники
 2. Бывшие сотрудники
 3. Кандидаты на замещение вакантных должностей
 4. Представители контрагентов СПб ГАУ ЦЗН
 5. Действующие клиенты СПб ГАУ ЦЗН, обратившиеся в за получением государственных услуг
 6. Бывшие клиенты СПб ГАУ ЦЗН, обратившиеся за получением государственных услуг
 7. Посетители СПб ГАУ ЦЗН
2. Что запрещено Трудовым кодексом РФ работодателю при обработке персональных данных?
- Варианты ответа:
1. Получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни
 2. Получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, если это не разрешено
 3. Получать и обрабатывать персональные данные работника о его образовании, научной степени и звания
 4. Получать и обрабатывать персональные данные работника о его семейном положении и составе семьи
3. В соответствии с Трудовым кодексом РФ работник должен быть ознакомлен с документами работодателя, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области
- Варианты ответа:
1. Под роспись
 2. Устно
 3. Устно в присутствии свидетелей
4. Работодатель вправе получать и обрабатывать данные о частной жизни работника только после
- Варианты ответа:
1. Письменного согласия работника
 2. Устного согласия работника
 3. Письменного согласия работника, заверенного нотариально
5. Кто может быть обладателем информации?
- Варианты ответа:
1. Гражданин (физическое лицо)
 2. Юридическое лицо
 3. Российская Федерация
 4. Субъект Российской Федерации
 5. Муниципальное образование
 6. Информационная система
 7. Система обработки персональных данных
6. Какое право имеет обладатель информации в части доступа к ней, если иное не предусмотрено Федеральными законами?
- Варианты ответа:
1. Разрешать доступ к информации
 2. Ограничивать доступ к информации
 3. Все выше перечисленное
7. К какой информации не может быть ограничен доступ?
- Варианты ответа:
1. Нормативно правовые акты, затрагивающим права, свободы и обязанности человека и гражданина
 2. Информация о состоянии окружающей среды

3. Информация о деятельности государственных органов и органов местного самоуправления
 4. Информация, накапливаемая в открытых фондах библиотек, музеев и архивов, в государственных, муниципальных и иных информационных системах, предназначенных для обеспечения граждан и организаций
 5. Интеллектуальная собственность
 6. Служебная информация
8. Укажите, какая конфиденциальная информация должна защищаться на объекте информатизации?
- Варианты ответа:
1. Речевая
 2. Передаваемая по каналам связи, выходящим за пределы контролируемой зоны
 3. Выводимая на экраны видеомониторов
 4. Обрабатываемая средствами вычислительной техники
 5. Представленная на бумажных носителях
9. К какому методу защиты относятся мероприятия, перечисленные на картинке?
- Варианты ответа:
1. Физический
 2. Организационный
 3. Технический
 4. Программно-аппаратный



10. К какому методу защиты относятся мероприятия, перечисленные на картинке?
- Варианты ответа:
1. Физический
 2. Организационный
 3. Технический
 4. Программно-аппаратный

Модуль 2. Криптографические средства защиты информации. Требования по технической защите информации (для категории 2, 3, 4)

Пример тестового задания по модулю 2:

1. Какое из определений СКЗИ является наиболее полным?
Варианты ответа:
 1. Средства криптографической защиты информации – это программное обеспечение или программно-аппаратный комплекс, с помощью которых происходит шифрование данных, и передача их по сети Интернет.
 2. Средства криптографической защиты информации – это программное обеспечение с помощью которого происходит шифрование данных, и передача их по сети Интернет.
2. Укажите, что запрещается пользователю криптосредств?

Варианты ответа:

1. Разглашать информации о ключевых документах
 2. Снимать копии с носителей ключевой информации
 3. Выводить ключевые документы на дисплей компьютера или принтер
 4. Записывать постороннюю информацию на носители ключевой информации
 5. Хранить носители ключевой информации в сейфе
 6. Устанавливать ключевые документы в другие компьютеры
 7. Устанавливать антивирусное программное обеспечение
3. Необходимо ли держать в тайне информацию о криптоключе?
- Варианты ответа:
1. Нет, обязательно
 2. Да, конечно
 3. Ее все знают
4. Что должен делать сотрудник, если ему стало известно, что информация о криптоключе известна посторонним?
- Варианты ответа:
1. Немедленно доложить начальнику отдела
 2. Уничтожить криптоключ
 3. Ничего не предпринимать
5. Непосредственно к работе со СКЗИ допускаются сотрудники:
- Варианты ответа:
1. Прошедшие соответствующее обучение
 2. Получившие разрешение от контролирующего органа
 3. Самостоятельно изучившие техническую документацию СКЗИ
6. Укажите, какое средство криптографической защиты информации используется в СПб ГАУ ЦЗН в качестве персонального сетевого экрана, позволяющего контролировать IP-трафик компьютера?
- Варианты ответа:
1. КриптоПро
 2. SBERSIGN
 3. БиКрипт
 4. VipNet
 5. Контейнер
 6. Крипто-Ком
 7. Крипто-Си

Модуль 3. Криптографические средства защиты информации CryptoPro. Общие сведения (для категории 2, 4)

Пример тестового задания по модулю 3:

1. Можно ли записывать стороннюю информацию на ключевой носитель?
- Варианты ответа:
1. Да
 2. Нет
 3. Только с разрешения ответственного должностного лица
2. Укажите, какие функции не выполняются КриптоПро?
- Варианты ответа:
1. Авторизации и обеспечения контроля подлинности электронных документов
 2. Обеспечения конфиденциальности и контроля целостности информации
 3. Защиты программного обеспечения от несанкционированного доступа
 4. Антивирусная защита
 5. Обмен мгновенными защищенными сообщениями

3. Можно, ли оставлять носитель с ключами ЭЦП подключенными к ПК после подписания платежных документов?
Варианты ответа:
 1. Допускается
 2. Не допускается
 3. Допускается с разрешения ответственного должностного лица
4. Укажите, в каких случаях необходимо выполнить блокировку и смену ключей ЭЦП?
Варианты ответа:
 1. Кража
 2. Истечение срока действия
 3. Потеря
 4. Смена руководителей юридического лица, подписывавших распоряжения о предоставлении сотрудникам полномочий подписания ЭЦП
 5. Командировка руководителей юридического лица, подписывавших распоряжения о предоставлении сотрудникам полномочий подписания ЭЦП
5. Что должно происходить с компьютером, на котором установлены технические средства СКЗИ КriptoПро, при уходе пользователя с рабочего места?
Варианты ответа:
 1. Автоматическое выключение компьютера
 2. Автоматическое включение парольной заставки
 3. Автоматическая перезагрузка компьютера

Модуль 4. Криптографические средства защиты информации VipNet. Общие сведения (для категории 3, 4)

Пример тестового задания по модулю 4:

1. Укажите, какие программы входят в состав ViPNet Client?
Варианты ответа:
 1. ViPNet Монитор
 2. ViPNet Контроль приложений
 3. ViPNet Деловая Почта
 4. ViPNet Транспортный модуль
 5. ViPNet Криптопровайдер
 6. ViPNet Координатор
 7. ViPNet Администратор
 8. ViPNet Терминал
2. Укажите, какие программные модули ViPNet Client запускаются автоматически при старте ОС Windows и работают в фоновом режиме?
Варианты ответа:
 1. ViPNet Монитор
 2. ViPNet Контроль приложений
 3. ViPNet Деловая Почта
 4. ViPNet Транспортный модуль
 5. ViPNet Криптопровайдер
3. Укажите, какая программа из состава ViPNet Client обеспечивает обмен защищенными сообщениями?
Варианты ответа:
 1. ViPNet Монитор
 2. ViPNet Контроль приложений
 3. ViPNet Деловая Почта
 4. ViPNet Транспортный модуль
 5. ViPNet Криптопровайдер

4. Укажите, какая программа из состава ViPNet Client обеспечивает обмен электронными письмами?

Варианты ответа:

1. ViPNet Монитор
2. ViPNet Контроль приложений
3. ViPNet Деловая Почта
4. ViPNet Транспортный модуль
5. ViPNet Криптопровайдер

5. Укажите, какая программа из состава ViPNet Client позволяет обнаружить сетевую активность приложений?

Варианты ответа:

1. ViPNet Монитор
2. ViPNet Контроль приложений
3. ViPNet Деловая Почта
4. ViPNet Транспортный модуль
5. ViPNet Криптопровайдер

6. Укажите, какой значок в панели задач соответствует программе ViPNet Контроль приложений?



Варианты ответа:

1. 1
2. 2
3. 3

7. Укажите, какой значок в панели задач соответствует программе ViPNet Монитор?



Варианты ответа:

1. 1
2. 2
3. 3

8. Укажите, какой значок в панели задач соответствует программе ViPNet Транспортный модуль?



Варианты ответа:

1. 1
2. 2
3. 3

9. С помощью каких программ можно осуществить передачу файлов внутри защищенной сети VipNet?

Варианты ответа:

1. ViPNet Монитор.
2. ViPNet Контроль приложений.
3. Проводник Windows.
4. Средство переноса данных Windows.

10. С помощью каких программ можно осуществить выбор и передачу файлов внутри защищенной сети VipNet?

Варианты ответа:

1. ViPNet Монитор.
2. ViPNet Контроль приложений.

3. Проводник Windows.
 4. Средство переноса данных Windows.
 5. ViPNet Транспортный модуль.
11. Укажите возможные способы открытия окна программы VipNet Контроль приложений?
- Варианты ответа:
1. Кликнуть мышкой по значку программы, расположенному в панели задач.
 2. Выполнить команду Программы→ViPNet→Client→ViPNet Контроль приложений.
 3. Нажать кнопку «ViPNet Контроль приложений» в окне ViPNet Монитор.
 4. Нажать кнопку «ViPNet Контроль приложений» в окне Транспортный модуль.
 5. Выбрать пункт контекстного меню «ViPNet Контроль приложений» в проводнике Windows.

Пример тестового задания для итогового контроля:

1. Для чего нужен пароль пользователя VipNet Client?
 1. Для защиты данных на ключевой дискете и аутентификации пользователя.
 2. Для выхода в интернет.
 3. Для осуществления тонкой настройки клиента.
2. Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно - программные СКЗИ должны быть:
 1. Оборудованы средствами контроля за их вскрытием (опечатаны).
 2. Свободно вывозиться за границу.
 3. Доступны посторонним лицам.
3. Электронный документ это
 1. Документ, в котором информация представлена в электронно-цифровой форме.
 2. Документ, напечатанный с носителя информации (дискеты, жесткого диска) .
 3. Бумажный документ, но имеющий электронную цифровую подпись.
4. Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат:
 1. Налоговому учету.
 2. Поэкземплярному учету.
 3. Бухгалтерскому учету.