Министерство науки и высшего образования Российской Федерации

ИВАНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Институт профессионального развития

УТВЕРЖДАЮ:

ВРИО ректора ФГБОУ ВО "ИвГУ"

_____ А.А. Малыгин

«14» 10 2020 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Техническая защита информации. Способы и средства защиты информации от несанкционированного доступа»

Категория слушателей	*лица, имеющие высшее образование*
Трудоемкость	*72 часа*
Нормативный срок освоения программы	*4 недели*

Иваново

ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1. Цель программы

Целью программы является совершенствование компетенций, необходимых для осуществления профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации специалистов, работающих в области технической защиты информации, в части разработки и применения способов и средств защиты информации от несанкционированного доступа**.**

2. Планируемые результаты обучения

Перечень профессиональных компетенций, качественное изменение которых осуществляется в результате обучения:

- способность разрабатывать и применять способы и средства защиты информации от несанкционированного доступа**.**

2.1. Знать (осведомленность в областях)

- нормативные правовые акты Российской Федерации, нормативные и методические документы в области ТЗИ (защиты информации от НСД);
- основы функционирования государственной системы противодействия (ПД) иностранным техническим разведкам (ИТР) и ТЗИ;
- основные понятия в области ТЗИ;
- основы лицензирования деятельности в части ТЗИ (лицензирование деятельности по проведению работ, связанных с созданием средств защиты информации, осуществлением мероприятий и (или) оказанием услуг в области защиты государственной тайны, а также лицензирование деятельности по технической защите конфиденциальной информации и деятельности по разработке и производству средств защиты конфиденциальной информации);
- порядок проведения работ по сертификации средств защиты информации по требованиям безопасности информации;
- систему организации защиты информации, действующей в органе государственной власти, организации;
- основы методологии и методики проведения ТЗИ от НСД в органе государственной власти, организации;
- способы и средства обработки и передачи информации;
- процедуры выявления угроз безопасности информации на объектах информатизации, организации;
- общие требования по ТЗИ (по защите информации от НСД), требования и рекомендации по защите объектов информатизации;
- способы и средства защиты информации от НСД;
- требования к средствам защиты информации от НСД;
- правила разработки, утверждения, обновления и отмены документов в области ТЗИ;
- цели, задачи, основные принципы организации, методы и средства ведения контроля состояния защищенности информации в органе государственной власти, организации;
- порядок оформления технической документации по защите информации;

- порядок обработки результатов контроля, анализа и оценки защищенности объектов информатизации, порядок подготовки актов по результатам специальных исследований, специальных проверок, протоколов измерений, предписаний на право эксплуатации объектов, систем и средств в защищенном исполнении и других документов по результатам контроля.

2.2. Уметь (способность к деятельности)

- анализировать угрозы безопасности информации;
- определять требования к средствам защиты информации от НСД;
- проводить обоснование выбора современных способов и средств защиты информации от НСД;
- проводить мероприятия по защите информации от НСД;
- устанавливать, применять и настраивать средства защиты информации от НСД;
- разрабатывать проекты нормативных и методических документов по защите объектов информатизации от НСД к информации;
- разрабатывать технические задания на проведение научно-исследовательских и опытно-конструкторских работ в части ТЗИ от НСД;
- осуществлять проверку выполнения требований нормативных документов по защите информации от НСД;
- осуществлять контроль защищенности информации от НСД; проводить работы при осуществлении лицензируемых видов деятельности в области ТЗИ;
- проводить работы по классификации защищенности автоматизированных (информационных) систем от НСД к информации.

2.3. Навыки (использование конкретных инструментов)

- работы с нормативными правовыми актами, методическими документами, национальными и международными стандартами в области ТЗИ;
- работы с базами данных, содержащих информацию по угрозам и уязвимостям безопасности информации, в том числе зарубежными информационными ресурсами;
- разработки необходимых документов в интересах организации работ по защите информации от НСД;
- проведения работ, связанных с защитой информации от НСД, проектирования, построения и эксплуатации системы защиты информации;
- выявления угроз безопасности информации в автоматизированных (информационных) системах;
- участия в разработке организационных и технических мероприятий по защите объектов информатизации от НСД к информации, контроля их выполнения;
- установки, применения и настройки современных средств защиты информации от НСД;
- проведения работ по контролю защищенности информации от НСД.

3. Категория слушателей

Лица, имеющие высшее образование

Квалификация: не требуется

Наличие опыта профессиональной деятельности: не требуется

Предварительное освоение иных дисциплин/курсов /модулей: не требуется.

4. **Учебный план программы "Техническая защита информации. Способы и средства защиты информации от несанкционированного доступа"**

№ п/п	Модуль	Всего, час	Виды учебных занятий		
			лекции	практические занятия	самостоятельная работа
1	Учебный модуль № 1. Организация работ по ТЗИ	16	2	6	8
2	Учебный модуль № 2. Защита информации от НСД	20	2	14	4
3	Учебный модуль № 3. Контроль состояния ТЗИ от НСД	20	6	6	8
4	Учебный модуль №4. Защита персональных данных	14	2	4	8
5	Итоговая аттестация	2	Экзамен в форме тестирования		

5. Календарный учебный график проведения учебных занятий по дополнительной профессиональной программе повышения квалификации "Техническая защита информации. Способы и средства защиты информации от несанкционированного доступа "

периодичность набора групп - 1 группа в месяц

№ п/п	Наименование учебных модулей	Трудоёмкость (час)	Сроки обучения
1	Учебный модуль № 1. Организация работ по ТЗИ	16	01.11.2020 - 05.11.2020
2	Учебный модуль № 2. Защита информации от НСД	20	06.11.2020 - 12.11.2020
3	Учебный модуль № 3. Контроль состояния ТЗИ от НСД	20	13.11.2020 - 19.11.2020
4	Учебный модуль №4. Защита персональных данных	14	20.11.2020 -23.11.2020
5	Итоговая аттестация	2	24.11.2020 - 25.11.2020
Всего:		72	

1. Учебно-тематический план программы «Техническая защита информации. Способы и средства защиты информации от несанкционированного доступа»

Трудоемкость программы - 72 академических часа. Продолжительность академического часа 45 минут.

№ п/п	Модуль	Всего, час	Виды учебных занятий		
			лекции	практические занятия	самостоятельная работа по выполнению практико-ориентированных заданий
1	**Учебный модуль № 1. Организация работ по ТЗИ**	**16**	**2**	**6**	**8**
	Тема № 1. Цели и задачи ТЗИ	3	1		2
	Тема № 2. Защищаемые информация и информационные ресурсы. Объекты защиты	2		2	
	Тема № 3. Угрозы безопасности информации, связанные с НСД	4		2	2
	Тема № 4. Правовые основы ТЗИ	3	1		2
	Тема № 5. Формирование требований по защите информации и создание системы защиты информации от НСД	4		2	2
2.	**Учебный модуль № 2. Защита информации от НСД**	**20**	**2**	**14**	**4**
	Тема № 1. Организационно-технические основы выполнения мероприятий по ТЗИ от НСД	6	2	2	2
	Тема № 2. Меры и средства защиты информации от НСД	14		12 (лабораторные работы практико-ориентированного характера)	2
3.	**Учебный модуль № 3. Контроль состояния**	**20**	**6**	**6**	**8**

	ТЗИ от НСД				
	Тема № 1. Основные задачи контроля состояния ТЗИ от НСД	4	2		2
	Тема № 2. Методы и средства контроля защищенности информации от НСД	6		4 (лабораторные работы практико-ориентированного характера)	2
	Тема № 3. Аттестация объектов информатизации по требованиям безопасности информации	6	2	2	2
	Тема № 4. Сертификация средств защиты информации от НСД	4	2		2
4.	**Учебный модуль №4 Защита персональных данных**	**14**	**2**	**4**	**8**
	Тема № 1. Законодательство Российской Федерации о персональных данных	3	1		2
	Тема № 2. Правовые, организационные и технические меры для защиты персональных данных	4		2	2
4	Тема № 3. Формирование требований по защите персональных данных и создание системы защиты для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных	4		2	2
	Тема № 4 Ответственность за нарушение требований законодательства Российской Федерации в области персональных данных	3	1		2
Итоговая аттестация		**2**	Итоговый экзамен в форме тестирования		

Методы, формы, технологии, применяемые при реализации программы:

- смешанная технология,
- дистанционные образовательные технологии,
- электронное обучение.

В рамках программы повышения квалификации предусмотрено проведение практических занятий с привлечением специалистов высшего уровня квалификации в области ТЗИ, имеющих опыт работы в данной области, представителей российских компаний, государственных и общественных организаций.

Программа повышения квалификации предусматривает проведение онлайн-занятий в соответствии с целевыми установками программы, которые обеспечивают требуемый уровень усвоения учебного материала. Знания приобретаются в основном проведением лекций, практических занятий и самостоятельной работы. Умения и навыки достигаются проведением ряда взаимосвязанных лабораторных и практических занятий, компьютерного моделирования последствий принимаемых решений, деловых и ролевых игр, разбором конкретных ситуаций, тренингов и др.

2. Учебная (рабочая) программа повышения квалификации «Техническая защита информации. Способы и средства защиты информации от несанкционированного доступа»

Учебный модуль № 1. Организация работ по ТЗИ.

Тема № 1. Цели и задачи ТЗИ.

Содержание темы

Основные термины и определения в области ТЗИ. Государственная система ПД ИТР и ТЗИ. Место ТЗИ в системе мероприятий по обеспечению информационной безопасности в Российской Федерации. Цели и задачи ТЗИ.

Тема № 2. Защищаемые информация и информационные ресурсы. Объекты защиты.

Содержание темы

Объекты защиты информации. Защищаемые информация и информационные ресурсы. Объекты информатизации, их классификация и характеристика.

Государственные информационные ресурсы, негосударственные информационные ресурсы, находящиеся в ведении органов государственной власти и организаций.

Понятие, классификация и технологии построения информационных систем. Информационные системы как объекты защиты от НСД. Стандартная модель взаимодействия открытых систем и протоколы межсетевого взаимодействия.

Тема № 3. Угрозы безопасности информации, связанные с НСД.

Содержание темы

Понятие и классификация угроз безопасности информации, связанных с НСД. Источники угроз безопасности информации от НСД.

Модели угроз безопасности информации от НСД.

Методы выявления и анализа угроз безопасности информации, уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах.

Банк данных угроз безопасности информации, включающий базу данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах.

Описание уязвимостей программного обеспечения, включенных в базу данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах.

Международный подход к выявлению и анализу уязвимостей, базы данных, содержащие уязвимости, в том числе CVE. Общая система оценки уязвимостей (стандарт CVSS).

Тема № 4. Правовые основы ВИ.

Содержание темы

Правовые основы защиты информации. Система документов в области ТЗИ. Нормативные правовые акты. Нормативные правовые акты ФСТЭК России. Методические документы. Технические документы (документация). Плановые документы. Информационные документы. Документы в области технического регулирования и стандартизации. Система стандартов в области защиты информации. Общие вопросы организации лицензирования деятельности в области ТЗИ, сертификации средств защиты информации, аттестации объектов информатизации по требованиям безопасности информации. Ответственность за правонарушения в области защиты информации.

Тема № 5. Формирование требований по защите информации и создание системы защиты информации от НСД.

Содержание темы

Формирование требований по защите информации от НСД, содержащейся в информационной системе (на объекте информатизации).

Требования по защите информации от НСД.

Требования международных стандартов по защите информации от НСД.

Создание и функционирование системы защиты информации как составные части работ по созданию и эксплуатации объектов информатизации учреждений и предприятий.

Стадии и этапы создания системы защиты информации.

Комплекс работ по созданию системы защиты информации (формирование требований к системе защиты информации; разработка (проектирование) системы защиты информации; внедрение системы защиты информации; аттестация объекта информатизации на соответствие требованиям безопасности информации и ввод его в действие; сопровождение системы защиты информации в ходе эксплуатации объекта информатизации).

<u>Учебный модуль № 2. Защита информации от НСД.</u>

Тема № 1. Организационно-технические основы выполнения мероприятий по ТЗИ от НСД.

Содержание темы

Комплекс мероприятий по ТЗИ от НСД.

Особенности защиты информации от НСД при использовании современных информационных технологий (мобильных, беспроводных, грид, суперкомпьютерных, виртуализации, облачных, больших данных и др.).

Обеспечение защиты информации от НСД в ходе эксплуатации аттестованной информационной системы.

Обеспечение защиты информации от НСД при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

Тема № 2. Меры и средства защиты информации от НСД.

Содержание темы

Общая характеристика и классификация мер и средств защиты информации от НСД.

Требования к мерам защиты информации от НСД, реализуемым в автоматизированной (информационной) системе. Меры защиты информации от НСД. Особенности создания системы защиты информации от НСД как обеспечивающей подсистемы автоматизированной (информационной) системы. Системные и документальные части системы защиты информации от НСД.

Средства защиты информации от НСД. Межсетевые экраны, требования к ним и способы применения. Системы обнаружения вторжений, требования к ним и способы применения. Средства антивирусной защиты, требования к ним и способы применения. Специальные программно-аппаратные и программные комплексы доверенной загрузки и разграничения контроля доступа. Средства регистрации и учета. Средства (механизмы) обеспечения целостности информации. Криптографические средства защиты информации. Перспективные технологии биометрической аутентификации. DLP-системы, их возможности и перспективы применения.

Установка и настройка средств защиты информации от НСД.

Общий порядок разработки и производства средств защиты информации от НСД.

Мероприятия по физической защите объекта информатизации и отдельных технических средств, исключающих НСД к техническим средствам, их хищение и нарушение работоспособности.

<u>Учебный модуль № 3. Контроль состояния ТЗИ от НСД.</u>

Тема № 1. Основные задачи контроля состояния ТЗИ от НСД.

Содержание темы

Классификация видов контроля состояния ТЗИ от НСД.

Система документов по контролю состояния ТЗИ от НСД.

Вопросы, подлежащие проверке при контроле состояния ТЗИ от НСД в организации.

Организационный и технический контроль состояния ТЗИ от НСД.

Тема 2. Методы и средства контроля защищенности информации от НСД.

Содержание темы

Классификация методов контроля защищенности информации от НСД и их характеристика. Сканеры безопасности и их характеристика. Средства анализа программных кодов и их характеристика. Средства антивирусной защиты и их характеристика.

Тема № 3. Аттестация объектов информатизации по требованиям безопасности информации.

Содержание темы

Порядок проведения аттестации объектов информатизации по требованиям безопасности информации. Программы и методики аттестационных испытаний. Заключение по результатам аттестации объекта информатизации. Аттестат соответствия объекта информатизации.

Тема № 4. Сертификация средств защиты информации от НСД.

Содержание темы

Порядок проведения работ по сертификации продукции, используемой в целях защиты информации от НСД.

Учебный модуль №4. Защита персональных данных.

Тема № 1. Законодательство Российской Федерации о персональных данных

Содержание темы

Правовые основы защиты персональных данных. Нормативные правовые акты Российской Федерации в области персональных данных. Нормативные правовые документы Правительства Российской Федерации, Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, устанавливающие требования по обеспечению безопасности персональных данных при их обработке в информационных системах.

Тема № 2. Правовые, организационные и технические меры для защиты персональных данных

Содержание темы

Правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Обязанность оператора по принятию мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

Тема № 3. Формирование требований по защите персональных данных и создание системы защиты для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных

Содержание темы

Создание информационной системы и формирование требований по защите персональных данных. Создание системы защиты для обеспечения безопасности персональных данных при их обработке в информационной системе персональных данных.

Комплекс работ по созданию системы защиты персональных данных (формирование требований к системе защиты персональных данных; разработка (проектирование) системы защиты персональных данных; внедрение системы зашиты персональных данных; оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных; ввод в эксплуатацию информационной системы и обеспечение защиты персональных данных в ходе эксплуатации информационной системы персональных данных.

Тема № 4. Ответственность за нарушение требований законодательства Российской Федерации в области персональных данных

Содержание темы

Виды ответственности за нарушение требований законодательства Российской Федерации в области персональных данных.

Описание лабораторных работ

№ п/п	Номер (наименование) учебного модуля, темы	Описание
1	Модуль № 2, Тема № 2	Восстановление системного и прикладного программного обеспечения после сбоев и отказов оборудования и программно-математического воздействия
2	Модуль № 2, Тема № 2	Установка и настройка антивирусных программ
3	Модуль № 2, Тема № 2	Установка программно-аппаратного комплекса защиты и его настройка по соответствующему классу защищенности
4	Модуль № 2, Тема № 2	Установка и настройка программно-аппаратного комплекса доверенной загрузки
5	Модуль № 2, Тема № 2	Установка средств сетевой безопасности и их настройка по классу защищенности
6	Модуль № 3, Тема № 2	Инструментальный контроль защищенности автоматизированной системы на соответствие требований по защите информации от НСД
7	Модуль № 3, Тема № 2	Контроль сетевой безопасности (системы обнаружения вторжений и анализа защищённости. Сетевые сканеры)

Описание практико-ориентированных заданий

№ п/п	Номер (наименование) учебного модуля, темы	Тематика практико-ориентированных заданий
1	Модуль № 1, Тема № 5	Разработка технического задания (разделов технического задания) на создание системы защиты информации
2	Модуль № 1, Тема № 3	Разработка модели угроз безопасности информации, обрабатываемой в автоматизированной системе
3	Модуль № 3, Тема № 2	Порядок проведения работ, выполняемых при осуществлении контроля защищенности информации от НСД
4	Модуль № 3, Тема № 3	Программы и методики аттестационных испытаний
5	Модуль № 3, Тема № 4	Программы и методики сертификационных испытаний

3. Оценочные материалы по образовательной программе

Система контроля качества обучения по дополнительной профессиональной программе предусматривает решение задачи соответствия результатов освоения заявленным целям и планируемым результатам обучения. В соответствие с этим оценка качества реализации программы включает в себя:

– аттестацию слушателей на предмет соответствия их персональных достижений поэтапным требованиям программы;

– использование современных оценочных технологий;

– организацию самостоятельной работы с учетом их индивидуальных способностей по решению практико-ориентированных задач;

– поддержание постоянной обратной связи и принятие оптимальных решений в управлении качеством обучения на уровне преподавателя.

Устанавливаются следующие типы контроля образовательных достижений слушателей: **текущая**, **промежуточная** и **итоговая** аттестация.

Текущая аттестация учебной работы обучающихся позволяет преподавателю составить представление о том, как слушатели воспринимают и осмысливают изучаемый материал, каковы их учебные склонности, интересы и способности. Накопленные наблюдения позволяют более объективно подходить к проверке и оценке знаний учащихся, своевременно принимать необходимые меры для предупреждения неуспеваемости.

Текущая аттестация оперативна и разнообразна по методам, при помощи которых она проводится, она обеспечивает своевременное усвоение и закрепление учебного материала на каждом этапе обучения, поэтому проводится на каждом занятии при рассмотрении первого же кейса следующим образом: после короткой лекции обучающиеся под руководством преподавателя приступают к отработке соответствующих практических навыков, задания для которой включают в себя элементы предыдущей темы.

Оценивание текущего контроля преподавателем не производится. Освоение обучающимся темы производится через многократное закрепление практических навыков, контрапунктом проходящее через весь календарно-тематический план.

Промежуточная аттестация должна определять уровень освоения слушателями теоретического и практического материала (углубленное изучение актуальных проблем, приобретение практических навыков) и охватывать все содержание модулей.

Текущая и промежуточная аттестация проводится в виде тестирования во время практических занятий и не требует выделения отдельных часов в учебном плане для ее прохождения.

Итоговая аттестация слушателей происходит в форме тестирования.

Шкала оценивания - «зачтено/незачтено».

8.1. Вопросы тестирования по модулям, итоговое тестирование

№	Вопросы входного тестирования	Вопросы промежуточного, итогового тестирования
1	**Не предусмотрено**	1. Основные термины и определения в области ТЗИ. 2. Цели и задачи ТЗИ. 3. Объекты информатизации: классификация и характеристика. 4. Система документов в области ТЗИ. 5. Система стандартов в области защиты информации. 6. Ответственность за правонарушения в области защиты информации. 7. Требования по защите информации от НСД. 8. Требования международных стандартов по защите информации от НСД. 9. Стадии и этапы создания системы защиты информации. 10. Государственные информационные ресурсы. 11.Понятие и общая классификация угроз безопасности информации, связанных с НСД. 12.Методы выявления и анализа угроз безопасности информации. 13.Методы выявления и анализа уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах. 14.Обеспечение защиты информации от НСД в ходе эксплуатации аттестованной информационной системы. 15.Обеспечение защиты информации от НСД при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации. 16.Требования к мерам защиты информации от НСД, реализуемым в информационной системе. Меры защиты информации от НСД. 17.Средства защиты информации от НСД. 18.Общий порядок разработки и производства средств защиты информации от НСД. 19.Классификация видов контроля состояния ТЗИ от НСД. 20.Система документов по контролю состояния ТЗИ от НСД. 21.Классификация методов контроля защищенности информации от НСД и их характеристика. 22.Сканеры безопасности и их характеристика. 23.Средства анализа программных кодов и их характеристика. Средства антивирусной защиты и их характеристика. 24.Порядок проведения аттестации объектов информатизации по требованиям безопасности информации. 25.Угрозы безопасности персональных данных при их обработке

		в информационной системе персональных данных. 26.Определение состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных. 27. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных с использованием средств криптографической защиты информации.
2		Экзамен в форме тестирования

8.2. Описание показателей и критериев оценивания, шкалы оценивания

Уровень сформированности компетенции	**Показатели**
Начальный	Компетенция недостаточно развита. Частично проявляет навыки, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается
Базовый	Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределённости, сложности
Продвинутый	Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности
Профессиональный	Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействующими факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности

Шкала оценивания итогового задания:

Оценка «зачтено» - выполненное задание соответствует всем критериям, достижение уровня не менее базового.

Оценка «незачтено» - выполненное задание не соответствует хотя бы одному критерию.

8.3. Примеры контрольных заданий по модулям или всей образовательной программе

Контрольное вопросы, выносящееся на защиту по итогу прохождения курса

1. Основные термины и определения в области ТЗИ.
2. Цели и задачи ТЗИ.
3. Объекты информатизации: классификация и характеристика.
4. Система документов в области ТЗИ.
5. Система стандартов в области защиты информации.
6. Ответственность за правонарушения в области защиты информации.
7. Требования по защите информации от НСД.
8. Требования международных стандартов по защите информации от НСД.
9. Стадии и этапы создания системы защиты информации.
10. Государственные информационные ресурсы.
11. Понятие и общая классификация угроз безопасности информации, связанных с НСД.
12. Методы выявления и анализа угроз безопасности информации.
13. Методы выявления и анализа уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах.
14. Обеспечение защиты информации от НСД в ходе эксплуатации аттестованной информационной системы.
15. Обеспечение защиты информации от НСД при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.
16. Требования к мерам защиты информации от НСД, реализуемым в информационной системе. Меры защиты информации от НСД.
17. Средства защиты информации от НСД.
18. Общий порядок разработки и производства средств защиты информации от НСД.
19. Классификация видов контроля состояния ТЗИ от НСД.
20. Система документов по контролю состояния ТЗИ от НСД.
21. Классификация методов контроля защищенности информации от НСД и их характеристика.
22. Сканеры безопасности и их характеристика.
23. Средства анализа программных кодов и их характеристика. Средства антивирусной защиты и их характеристика.
24. Порядок проведения аттестации объектов информатизации по требованиям безопасности информации.
25. Угрозы безопасности персональных данных при их обработке в информационной системе персональных данных.
26. Определение состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных.
27. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных с использованием средств криптографической защиты информации.

8.4. Тесты и обучающие задачи (кейсы), иные практико-ориентированные формы заданий

Итоговое тестирование после прохождения курса:
https://sdo.ivanovo.ac.ru/course/view.php?id=2178

8.5. Описание процедуры оценивания результатов обучения.

Формы аттестации

Форма итоговой аттестации обучающихся (в том числе для обучающихся из числа государственных гражданских служащих), освоивших программу повышения квалификации, - экзамен в форме тестирования.

Перечень тестов, используемых для проведения экзамена, сформирован на основе перечней тестов, выносимых для контроля знаний обучающихся при проведении промежуточных аттестаций по учебным модулям, представленным в рабочей программе курса повышения квалификации.

Описание процедуры оценивания

Слушатель проходит тестирование в системе дистанционного обучения ИвГУ, прикрепляет отчеты по выполнению лабораторных работ практико-ориентированного характера. Преподаватель оценивает задания в соответствии с критериями и шкалой оценки, заполняет чек-лист.

9. Организационно-педагогические условия реализации программы

9.1. Кадровое обеспечение программы

№ п/п	Фамилия, имя, отчество (при наличии)	Место основной работы и должность, ученая степень и ученое звание (при наличии)	Ссылки на веб-страницы с портфолио (при наличии)	Фото в формате jpeg	Отметка о полученном согласии на обработку персональных данных
1	Васенев Андрей Николаевич	начальник управления развития инфраструктуры, кандидат экономических наук, доцент	отсутствует		имеется

9.2. Учебно-методическое обеспечение и информационное сопровождение

<table>
<tr><th colspan="2">Учебно-методические материалы</th></tr>
<tr><th>Методы, формы и технологии</th><th>Методические разработки, материалы курса, учебная литература</th></tr>
<tr><td>Дополнительная профессиональная программа является сугубо практико-ориентированной, и предполагает проведение лабораторных работ.
При проведении занятий рекомендуется использовать методы активного обучения и элементы проектной технологии.</td><td>Гультяева, Т.А. Основы защиты информации : учебное пособие : [16+] / Т.А. Гультяева ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2018. – 83 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=574730 (дата обращения: 21.10.2020). – Библиогр. в кн. – ISBN 978-5-7782-3641-7. – Текст : электронный.
Введение в информационную безопасность и защиту информации : учебное пособие : [16+] / В.А. Трушин, Ю.А. Котов, Л.С. Левин, К.А. Донской ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2017. – 132 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=575113 (дата обращения: 21.10.2020). – Библиогр.: с. 49-50. – ISBN 978-5-7782-3233-4. – Текст : электронный.</td></tr>
<tr><th colspan="2">Информационное сопровождение</th></tr>
<tr><th>Учебно-методические материалы/Электронные образовательные ресурсы</th><th>Электронные информационные ресурсы</th></tr>
<tr><td>система дистанционного обучения Moodle https://sdo.ivanovo.ac.ru/course/view.php?id=2178</td><td>базы данных, банк данных угроз безопасности информации www.bdu.fstec.ru; http://www.fsb.ru, информационно-справочные и поисковые системы: www.pravo.gov.ru, www.fstec.ru, www.gost.ru/wps/portal/tk362/; правовые справочно-поисковые системы («Гарант», «Консультант Плюс»)</td></tr>
<tr><td>Система электронной поддержки образовательного процесса «Мой университет» (ЭИОС) https://uni.ivanovo.ac.ru</td><td>ЭБС «Университетская библиотека онлайн» www.biblioclub.ru
Электронная библиотека ИвГУ http://lib.ivanovo.ac.ru
Электронный каталог НБ ИвГУ http://lib.ivanovo.ac.ru/index.php/ek</td></tr>
</table>

9.3. Материально-технические условия реализации программы

Вид занятий	Наименование оборудования, программного обеспечения
лекции	операционная система MicrosoftWindows, пакет офисных программ MicrosoftOfficeи(или) LibreOffice, интернет-браузер MicrosoftEdge и(или) YandexBrowser
практические занятия	операционная система MicrosoftWindows, пакет офисных программ MicrosoftOfficeи(или) LibreOffice, интернет-браузер MicrosoftEdge и(или) YandexBrowser,
самостоятельная работа	операционная система MicrosoftWindows, пакет офисных программ MicrosoftOfficeи(или) LibreOffice, интернет-браузер MicrosoftEdge и(или) YandexBrowser,
Лаборатория «Технической защиты информации» Лабораторные работы	Операционная система. Офисные программы. Антивирусные программы. Программноеобеспечение для проведения компьютерных тестов. Учебный лабораторный комплекс для обеспечения исследованийспециальногопрограммного обеспечения и аппаратного СЗИ в составе: средства защиты информации от НСД; программно-аппаратный комплекс доверенной нагрузки; антивирусные пакеты; межсетевые экраны; средство создания модели разграничения доступа; программа контроля полномочий доступа к информационным ресурсам; программа фиксации и контроля исходного состояния программного комплекса: программа поиска и гарантированного уничтожения информации на дисках; системы обнаружения вторжений и анализа защищенности; сканеры безопасности

III. Паспорт компетенций (Приложение 2)

ПАСПОРТ КОМПЕТЕНЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Ивановский государственный университет»

дополнительная профессиональная образовательная программа повышения квалификации "Техническая защита информации. Способы и средства защиты информации от несанкционированного доступа"

1.	Наименование компетенции		Способность разрабатывать и применять способы и средства защиты информации от несанкционированного доступа.
2.	Указание типа компетенции	общекультурная/ универсальная	
		общепрофессиональная	
		профессиональная	**профессиональная**
		профессионально-специализированная	
3.	Определение, содержание и основные сущностные характеристики компетенции		- способность использовать нормативные правовые акты, методические документы, международные и национальные стандарты в области ТЗИ и обеспечения безопасности информационных технологий в своей профессиональной деятельности; - способность определять виды и формы информации, подверженной угрозам, возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов организации, целей и задач деятельности объекта защиты; - способность использовать достижения науки и техники в области ТЗИ, пользоваться реферативными и справочно-информационными изданиями в области

		ТЗИ; - способность определять угрозы безопасности информации, связанные с НСД, в автоматизированных (информационных) системах; - способность формировать требования по ТЗИ от НСД на объектах информатизации (формировать требования к системе защиты информации объекта информатизации); - способность разрабатывать способы и средства ТЗИ от НСД на объектах информатизации (разрабатывать системы защиты информации объектов информатизации); - способность внедрять способы и средства ТЗИ от НСД на объектах информатизации (внедрять системы защиты информации объекта информатизации).	
4.	Дескриптор знаний, умений и навыков по уровням	Уровни сформированности компетенции обучающегося	Индикаторы
	Знать - основные понятия в области ТЗИ; - нормативные правовые акты Российской Федерации, нормативные и методические документы в области ТЗИ (защиты информации от НСД). Уметь: - анализировать угрозы безопасности информации.	Начальный уровень	Компетенция недостаточно развита. Частично проявляет навыки, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается.
	Знать: - основы функционирования государственной системы противодействия (ПД) иностранным техническим разведкам (ИТР) и ТЗИ; - способы и средства обработки и передачи информации;	Базовый уровень	Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами

	- процедуры выявления угроз безопасности информации на объектах информатизации, организации; - общие требования по ТЗИ (по защите информации от НСД), требования и рекомендации по защите объектов информатизации; - способы и средства защиты информации от НСД; - требования к средствам защиты информации от НСД; - правила разработки, утверждения, обновления и отмены документов в области ТЗИ; - цели, задачи, основные принципы организации, методы и средства ведения контроля состояния защищенности информации в органе государственной власти, организации; - порядок оформления технической документации по защите информации; - порядок обработки результатов контроля, анализа и оценки защищенности объектов информатизации, порядок подготовки актов по результатам специальных исследований, специальных проверок, протоколов измерений, предписаний на право эксплуатации объектов, систем и средств в защищенном исполнении и других документов по результатам контроля. Уметь: - анализировать угрозы безопасности информации; - определять требования к средствам защиты информации от НСД; Навыки: - работы с нормативными правовыми актами, методическими документами, национальными и международными стандартами в области ТЗИ; - работы с базами данных, содержащих информацию по угрозам и уязвимостям безопасности		неопределённости, сложности.

	информации, в том числе зарубежными информационными ресурсами.		
	Знать: - основы лицензирования деятельности в части ТЗИ (лицензирование деятельности по проведению работ, связанных с созданием средств защиты информации, осуществлением мероприятий и (или) оказанием услуг в области защиты государственной тайны, а также лицензирование деятельности по технической защите конфиденциальной информации и деятельности по разработке и производству средств защиты конфиденциальной информации); - порядок проведения работ по сертификации средств защиты информации по требованиям безопасности информации; Уметь: - проводить обоснование выбора современных способов и средств защиты информации от НСД; - проводить мероприятия по защите информации от НСД; - устанавливать, применять и настраивать средства защиты информации от НСД; Навыки: - разработки необходимых документов в интересах организации работ по защите информации от НСД; - проведения работ, связанных с защитой информации от НСД; проектирования, построения и эксплуатации системы защиты информации.	Продвинутый	Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.

	Знать: - систему организации защиты информации, действующей в органе государственной власти, организации; - основы методологии и методики проведения ТЗИ от НСД в органе государственной власти, организации; Уметь: - разрабатывать проекты нормативных и методических документов по защите объектов информатизации от НСД к информации; - разрабатывать технические задания на проведение научно-исследовательских и опытно-конструкторских работ в части ТЗИ от НСД; - осуществлять проверку выполнения требований нормативных документов по защите информации от НСД; - осуществлять контроль защищенности информации от НСД; проводить работы при осуществлении лицензируемых видов деятельности в области ТЗИ; - проводить работы по классификации защищенности автоматизированных (информационных) систем от НСД к информации. Навыки: - выявления угроз безопасности информации в автоматизированных (информационных) системах; - участия в разработке организационных и технических мероприятий по защите объектов информатизации от НСД к информации, контроля их выполнения; - установки, применения и настройки современных средств защиты информации от НСД; - проведения работ по контролю защищенности информации от НСД.	Профессиональный	Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействующими факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.

5.	Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции	Базовые навыки информационной компетентности
6.	Средства и технологии оценки	Продолжительность тестирования – 60 минут. Дополнительные информационные материалы не предполагаются. Приоритетным при анализе и оценке выполнения задания студентом является констатация ожидаемых действий (в соответствии с выделенными показателями) и их обоснованность, а не установление правильности (неправильности) предложенных студентом решений.

Документ составлен в соответствии с требованиями профессиональных стандартов:

- профессионального стандарта «Специалист по технической защите информации» (утв. приказом Министерства труда и социальной защиты РФ от 1 ноября 2016 г. № 599н);

- профессионального стандарта «Специалист по защите информации в автоматизированных системах» (утв. Приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 года № 522н);

- профессионального стандарта «Специалист по защите информации в телекоммуникационных системах и сетях (утв. Приказом Министерства труда и социальной защиты РФ от 03 ноября 2016 г. № 608н).

- методических рекомендаций по разработке программ профессиональной переподготовки и повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, противодействия иностранным техническим разведкам и технической защиты информации (утв. ФСТЭК России 16 апреля 2018 г.);

- примерной программы повышения квалификации «Техническая защита информации. Способы и средства защиты информации от несанкционированного доступа» (утв. ФСТЭК России 30 марта 2016 г. (изменения утв. ФСТЭК России 30 мая 2018 г.)).

IV.Иная информация о качестве и востребованности образовательной программы

Информация о качестве и востребованности программы отражена в рекомендательных письмах ООО «Инвольта», ООО «АПКОМ ПАРТНЕРЗ»

V. Рекомендаций к программе от работодателей:

наличие двух писем от работодателей ООО «Инвольта», ООО «АПКОМ ПАРТНЕРЗ» о рекомендации образовательной программы для реализации в рамках Государственной системы предоставления ПЦС на формирование у трудоспособного населения компетенций цифровой экономики, указана востребованность результатов освоения программы в сфере деятельности соответствующих компаний и готовности к рассмотрению заявок наиболее успешно освоивших образовательную программу граждан на прохождение стажировки и (или) собеседования на предмет трудоустройства путем проставления отметки в профиле программы.

VI.Указание на возможные сценарии профессиональной траектории граждан по итогам освоения образовательной программы

Сценарии профессиональной траектории граждан, освоивших дополнительную профессиональную программу повышения квалификации «Техническая защита информации. Способы и средства защиты информации от несанкционированного доступа»:

- развитие профессиональных качеств, повышение заработной платы, сохранение и развитие квалификации, работающего по найму гражданина в организации текущей сферы занятости;

- трудоустройство для граждан, состоящих на учете в Центре занятости, а также безработных.

VII.Дополнительная информация

Указание на область реализации компетенций цифровой экономики, к которой в большей степени относится образовательная программа, в соответствии с Перечнем областей

п. 5. Кибербезопасность и защита данных

VIII.Приложенные Скан-копии

Утвержденной рабочей программа (подпись, печать, в формате pdf)