ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

ТОМСКИЙ ИНСТИТУТ ПЕРЕПОДГОТОВКИ КАДРОВ И АГРОБИЗНЕСА

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Техническая защита информации, не содержащей сведений, составляющих государственную тайну».

Рассмотрено и одобрено
на заседании Ученого совета
(Протокол № 6 от 01.07.2021г.)

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат:
00E262DA75537E587101FC3D70D93C40C1
Владелец: Дорошенко Ольга Петровна
Действителен: с 05.04.2023 до 28.06.2024

Томск 2021

1. Общая характеристика дополнительной профессиональной программы повышения квалификации

1.1. Нормативно-методические основы разработки программы

Программа разработана с учетом требований следующих нормативных документов:

- ФЗ от 29.12.2012 г. № 273 «Об Образовании в Российской Федерации»;
- ФЗ от 27.07.2006 г. № 149 «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями);
- ФЗ № от 15.08.1996 г. № 114 «О порядке выезда из Российской Федерации и въезда в Российскую Федерацию» (с изменениями и дополнениями);
- ФЗ от 28.12.2010 г. № 390 «О безопасности» (с изменениями и дополнениями);
- ФЗ от 04.05.2011 г. № 99 «О лицензировании отдельных видов деятельности» (с изменениями и дополнениями);
- Указ Президента РФ от 14.01.1992 г. № 20 «О защите государственных секретов РФ»;
- Указ Президента РФ от 06.10 2004 г. № 1286 «Вопросы межведомственной комиссии по защите государственной тайны» (с изменениями и дополнениями);
- Указ Президента РФ от 26.02.2009 г. «Вопросы межведомственной комиссии по защите государственной тайны»;
- Указ Президента РФ от 02.06.2021 г. № 400 «О стратегии национальной безопасности Российской Федерации;
- Постановление Правительства РФ от 26.06. 1995 г. № 608 «О сертификации средств защиты информации» (с изменениями и дополнениями);
- Устав ФГБОУ ТИПКиА.

1.2 Цель реализации данной дополнительной профессиональной программы повышения квалификации.

Цель – получение новых компетенций, необходимых для осуществления профессиональной деятельности и (или) повышение профессионального уровня в рамках имеющейся квалификации служащих, работающих в области технической защиты информации (ТЗИ), в части организации защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее – информация ограниченного доступа).

1.3. Планируемые результаты обучения.

Программа направлена на освоение следующих профессиональных компетенций.

Вид компетенции	В результате изучения учебной дисциплины слушатели должны		
	Знать:	Уметь:	Владеть:
Общепрофессиональные компетенции			
понимание сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности;	средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля	оценивать качество готового программного обеспечения;	методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации;

	эффективности защиты информации;		
Профессиональные компетенции			
способность обеспечивать безопасность и целостность данных информационных систем и технологий;	принципы и общие методы обеспечения информационной безопасности; критерии, условия и принципы отнесения информации к защищаемой; теоретические и методические основы рационального построения защищенного документооборота; принципы и методы обработки конфиденциальных документов; методы и приемы защиты документированной информации от несанкционированного	разрабатывать и оформлять нормативно-методические материалы по регламентации процессов обработки, хранения и защиты конфиденциальных документов; практически выполнять технологические операции по защите и обработке конфиденциальных документов	методами и формами защиты информации;

В результате повышения квалификации слушатели должны

Знать:

- нормативные правовые акты Российской Федерации, нормативные и методические документы в области ТЗИ (в том числе по защите информации от ее утечки по техническим каналам, защите информации от несанкционированного доступа (НСД));

основы построения информационных систем и формирования информационных ресурсов ограниченного доступа;

- виды конфиденциальной информации;
- перечни сведений конфиденциального характера, основные требования и рекомендации по их защите;
- действующую систему сертификации средств защиты информации по требованиям безопасности информации;
- основы лицензирования деятельности по ТЗКИ (техническая защита конфиденциальной информации) и (или) деятельности по разработке и производству средств защиты информации;
- возможные ТКУИ (технические каналы утечки информации) на объектах информатизации и угрозы безопасности информации в автоматизированных (информационных) системах;
- организацию и содержание проведения работ по ТЗКИ, состав и содержание необходимых документов (в том числе по защите информации от утечки по техническим каналам, защиты информации от НСД и по защите информации от специальных воздействий);
- организационные и технические мероприятия по ТЗКИ и контролю защищенности информации;
- общие требования по ТЗКИ (в том числе по защите информации от ее утечки по техническим каналам, защиты информации от НСД), нормы, требования и рекомендации по защите объектов информатизации, методы и методики контроля их выполнения;
- требования к средствам ТЗКИ и контроля защищенности информации;

- средства ТЗКИ и контроля защищенности информации;
- показатели оценки защищенности информации, методы их расчета и анализа, методы и средства контроля защищенности информации, в том числе при использовании открытых каналов радиосвязи;
- порядок организации взаимодействия структурных подразделений по ТЗИ при решении вопросов ТЗКИ, организационного и технического контроля в организации или в органах государственной власти;
- структуру, назначение, задачи, полномочия, техническую оснащенность и возможности структурных подразделений по ТЗИ в организации или в органах государственной власти;
сертифицированные по требованиям безопасности информации основные технические средства и системы (ОТСС) и вспомогательные технические средства и системы (ВТСС), порядок оснащения ими подразделений по ТЗИ;
- порядок проведения аттестации объектов информатизации по требованиям безопасности информации;
- основы проведения научных исследований и разработок в области ТЗКИ;
- достижения науки и техники в стране и за рубежом в области технических разведок, перспективные направления развития технических методов и средств защиты информации ограниченного доступа, программно-аппаратных средств защиты информации от НСД.

Уметь:
- применять на практике требования нормативных правовых актов, нормативных и методических документов в области ТЗКИ;
- организовывать работы по ТЗКИ на объектах информатизации и автоматизированных (информационных) системах;
- разрабатывать нормативные, методические и плановые документы по ТЗКИ;
- руководить деятельностью подразделений по ТЗИ при решении задач ТЗКИ;
- планировать и организовывать мероприятия организационного и технического контроля защищенности информации;
- определять возможные ТКУИ на объектах информатизации и угрозы безопасности информации в автоматизированных (информационных) системах;
- формировать требования по ТЗКИ (в том числе по защите информации от ее утечки по техническим каналам, защиты информации от НСД);
- формировать требования к средствам ТЗКИ и контроля защищенности информации;
применять средства ТЗКИ и контроля защищенности информации.

Владеть навыками:
- работы с действующими нормативными правовыми актами, нормативными и методическими документами в области ТКУИ;
- организации разработки необходимой документации по вопросам ТЗКИ;
- руководства работами по выявлению ТКУИ и определению угроз безопасности информации применительно к объектам защиты, определению требований по ТЗКИ объектов защиты, контролю защищенности информации на объектах защиты;
- организации и проведения научных исследований и разработок в области ТЗКИ;
- руководства деятельностью подразделений по ТЗКИ в организации или в органе государственной власти при решении задач ТЗКИ;
- организации проведения контроля защищенности информации ограниченного доступа в организации или в органе государственной власти при решении задач ТЗКИ;
- организации аттестации объектов информатизации, проведения специальных исследований, лицензирования и сертификации в области ТЗКИ;
- работы с действующими нормативными правовыми актами, нормативными и методическими документами в области защиты государственной тайны;
- организации разработки необходимой документации по вопросам по защите государственной тайны;

- руководства работами по выявлению и определению угроз безопасности информации применительно к объектам защиты, определению требований к объектам защиты, контролю защищенности информации на объектах защиты;
- организации аттестации объектов информатизации, проведения специальных исследований, лицензирования и сертификации в области защиты государственной тайны.

2. Содержание дополнительной профессиональной программы повышения квалификации

2.1. Учебный план

Категория слушателей - служащие, работающие в области ТЗИ в части организации работ по защите информации ограниченного доступа.

Срок обучения: 40 часов
Форма обучения: очная.

№ п/п	Наименование разделов и тем	Всего	Аудиторные занятия		Самост. работа	Форма контроля
			Лекции	Практ. занятия		
1	Планирование и организация и работ по ТЗКИ. Цели и задачи ТЗКИ.	4	4			
2	Правовые основы ТЗКИ.	4	4			
3	Определение угроз безопасности информации ограниченного доступа.	4	4			
4	Защищаемые информация и информационные ресурсы. Объекты защиты.	4	4			
5	Требования по защите информации и создание системы защиты информации.	6	6			
6	Аттестация объектов информатизации по требованиям безопасности информации.	6	6			
7	Сертификация средств защиты информации	6	6			опрос
8	Методы и средства контроля защищенности информации	2	2			
9	Основы организации контроля состояния ТЗКИ	2	2			
Итоговый контроль		**2**				**зачет**
ИТОГО		**40**	**38**			2

2.2. Календарный учебный график

№	Наименование дисциплин, разделов и тем	Всего аудиторных часов	Дни				
			1	2	3	4	5
1	Планирование и организация и работ по ТЗКИ. Цели и задачи ТЗКИ.	4	4				
2	Правовые основы ТЗКИ.	4	4				
3	Определение угроз безопасности информации ограниченного доступа.	4		4			
4	Защищаемые информация и информационные ресурсы. Объекты защиты	4		4			
5	Требования по защите информации и создание системы защиты информации.	6			6		
6	Аттестация объектов информатизации по требованиям безопасности информации.	6			2	4	
7	Сертификация средств защиты информации.	6				4	2
8	Методы и средства контроля защищенности информации	2					2
9	Основы организации контроля состояния ТЗКИ	2					2
Итоговая аттестация (зачет)		**2**					2
Итого		**40**	**8**	**8**	**8**	**8**	**8**

3. Тематический план дополнительной профессиональной программы повышения квалификации

Тема 1. Планирование и организация и работ по ТЗКИ. Цели и задачи ТЗКИ. (4 часа)
- основные термины и определения в области ТЗИ;
- место ТЗИ в системе мероприятий по обеспечению информационной безопасности в Российской Федерации;
- цели и задачи ТЗИ;
- объекты информатизации: классификация и характеристика;
- организация научных исследований и разработок в области ТЗИ;
- защищаемые информация и информационные ресурсы;
- объекты защиты;
- защищаемые информация и информационные ресурсы;
- объекты защиты информации;
- объекты информатизации, их классификация и характеристика;
- государственные информационные ресурсы, негосударственные информационные ресурсы, находящиеся в ведении органов государственной власти и организаций.

Тема 2. Правовые основы ТЗКИ. (4 часа)
- правовые основы защиты информации;
- система документов в области ТЗИ, а также ТЗКИ;
- нормативные правовые акты Российской Федерации;

- 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;
- организационно-правовые основы лицензирования деятельности в области защиты информации, аттестации объектов информатизации по требованиям безопасности информации;
- система сертификации средств защиты информации;
- ответственность за правонарушения в области защиты информации.

Тема 3. Определение угроз безопасности информации ограниченного доступа. (4 часа)
- угрозы безопасности информации ограниченного доступа;
- классификация ТКУИ;
- классификация и характеристики угроз безопасности информации, связанных с НСД;
- модель угроз безопасности информации;
- методы выявления и анализа угроз безопасности информации;
- методы выявления и анализа уязвимостей программного обеспечения, используемые в информационных системах;
- банк данных угроз безопасности информации, включающий базу данных уязвимостей программного обеспечения, используемые в информационных системах;
- описание уязвимостей программного обеспечения, включенных в базу данных уязвимостей программного обеспечения, используемые в информационных системах;
- международный подход к выявлению и анализу уязвимостей, базы данных, содержащие уязвимости, в том числе CVE;
- общая система.

Тема 4. Защищаемые информация и информационные ресурсы. Объекты защиты. (4 часа)
- 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.

Тема 5. Требования по защите информации и создание системы защиты информации. (6 часов)
- требования по защите информации, содержащейся в информационной системе (на объекте информатизации);
- требования по защите информации, обрабатываемой техническими средствами, от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН);
- требования по защите акустической речевой информации;
- требования по защите информации от НСД;
- требования национальных и международных стандартов по защите информации;
- создание и функционирование системы защиты информации ограниченного доступа, как составные части работ по созданию и эксплуатации объектов информатизации учреждений и предприятий;
- стадии и этапы создания системы защиты информации ограниченного доступа;
- порядок выполнения работ по защите информации о создаваемой автоматизированной системе в защищенном исполнении;

- 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 по требованиям безопасности информации и ввод его в действие; сопровождение системы защиты информации в ходе эксплуатации объекта информатизации);
- разработка эксплуатационной документации на систему защиты информации;
- особенности организации защиты персональных данных.

Тема 6. Аттестация объектов информатизации по требованиям безопасности информации. (6 часов)
- 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 7. Сертификация средств защиты информации. (6 часов)
- порядок сертификации продукции, используемой в целях защиты конфиденциальной информации: технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля защищенности информации, программных, программно-технических средств защиты информации, программных средств контроля защищенности информации.

Тема 8. Методы и средства контроля защищенности информации. (2 часа)
- методы и средства контроля защищенности информации;
- методы и средства контроля защищенности информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН;
- методы и средства контроля защищенности акустической речевой информации от утечки по техническим каналам;
- методы и средства контроля защищенности информации от НСД;
- документирование результатов контроля;
- требования к средствам контроля защищенности информации.

Тема 9. Основы организации контроля состояния ТЗКИ. (2 часа)
- основные задачи контроля состояния ТЗКИ;
- классификация видов контроля состояния ТЗКИ;
- система документов по контролю состояния ТЗКИ;
- вопросы, подлежащие проверке при контроле состояния ТЗКИ в организации;
- организационный и технический контроль состояния ТЗКИ.

4. Организационно-педагогические условия реализации программы.

4.1. Учебно-методическое обеспечение

4.1.1. Рекомендуемые источники и литература:

1. Афонин А.А, Сибикин В.И. Правовые акты РФ по вопросам защиты государственной тайны [Текст]: сборник ФГБОУ ДПО «Томский институт переподготовки кадров и аанробизнеса», 2014-243 с.;
2. Афонин А.А, Кизилова Е.А., Пономарчук М.Ю., Сибикин В.И Защита государственной тайны [Текст]: сборник ФГБОУ ДПО «Томский институт переподготовки кадров и аанробизнеса» ,2010-65 с;
3. Баранова, Е.К. Информационная безопасность и защита информации: [Текст]: Учебное пособие/Е.К.Баранова,А.В.Бабаш.-М.:Риор,2017.476с.
4. Баранова, Е.К. Информационная безопасность и защита информации: [Текст]: Учебное

пособие/Е.К.Баранова,А.В.Бабаш.М.:Риор,2018.-400с.
5. Баранова, Е.К. Информационная безопасность и защита информации: [Текст]: Учебное пособие/Е.К.Баранова,А.В.Бабаш.-М.:Риор,2017.-400с.
6. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам[Текст]:Г.А.Бузов.-М.:ГЛТ,2016.-586с.
7. Емельянова, Н.З. Защита информации в персональном компьютере: [Текст]:Уч.пос / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. - М.: Форум, 2017. - 352 с. Тимофеев С.Е. Защита информации ограниченного доступа [Текст]: учебно-методическое пособие ФГБОУ ДПО «Томский институт переподготовки кадров и агробизнеса»,2009-10 с;
8. Пономарчук М.Ю.,Тимофеев С.Е Обеспечение режима секретности в организации [Текст]: учебно-методическое пособие ФГБОУ ДПО «Томский институт переподготовки кадров и агробизнеса»,2021-21 с;

4.1.2. Материалы для организации работы слушателей:

- презентации;
- опорные слайды;
- раздаточный печатный материал.

4.2. Материально - технические условия реализации программы.

Материально-технические ресурсы института обеспечивают проведение аудиторных занятий (лекций, практических и семинарских занятий, консультаций и т.п). Слушателям предоставлена возможность пользования оборудованными аудиториями и компьютерными классами с выходом в интернет и доступом к электронно-библиотечной системе, а также возможность использования оргтехники (копировально-множительные аппараты, сканеры, принтеры).

Для проведения лекций, практических занятий с использованием активных форм и методов обучения учебные аудитории оборудованы техническими средствами.

Наименование специализированных аудиторий, кабинетов, лабораторий	**Вид занятий**	**Наименование оборудования, программного обеспечения**
Аудитория № 1	лекции, практические занятия	компьютер, мультимедийный проектор, экран, маркерная доска

4.3. Кадровое обеспечение программы повышения квалификации.

Образовательный процесс обеспечивается научно-педагогическими кадрами, имеющими базовое образование, соответствующее преподаваемому учебному курсу, и ученую степень или имеющими дополнительное профессиональное образование, профессиональную переподготовку, направленность которой соответствует преподаваемому учебному курсу, или опыт деятельности в соответствующей профессиональной сфере (стаж научно-педагогической работы не менее трех лет, при наличии ученого звания без предъявления к стажу работы) и систематически занимающимися научной и/или научно-методической деятельностью или иной практической деятельностью, соответствующей направленности образовательной программы.

К образовательному процессу могут привлекаться специалисты из числа действующих руководителей и ведущих специалистов профильных организаций, учреждений.

Состав преподавателей и экспертов приведен в приложении 1.

4.4. Организация образовательного процесса.

Реализация дополнительной профессиональной программы повышения квалификации «Техническая защита информации, не содержащей сведений, составляющих государственную тайну» предусматривает проведение теоретических занятий.

Продолжительность занятий – 8 часов в день с перерывами 5-10 мин., кофе-паузой и обедом продолжительностью 1 час.

5. Оценка качества освоения программы.

5.1. Формы контроля и аттестации.

Оценка качества проводится в отношении соответствия результатов освоения программы повышения квалификации заявленным целям и планируемым результатам обучения.

Учебным планом дополнительной профессиональной программы повышения квалификации предусмотрена промежуточная аттестация по завершении каждого блока курса обучения, которая проводится в форме **зачета**, организованного в виде тестовых заданий.

Для реализации программы предусмотрено создание оценочных материалов, которые включают вопросы тестирования, позволяющие оценивать уровень освоения профессиональных компетенций.

По результатам аттестационных испытаний выставляется оценка по двухбалльной системе: «зачтено», «не зачтено».

Описание шкалы оценивания уровня овладения слушателями компетенций на этапе зачета с использованием теста.

Оценка	Характеристика ответа слушателя (количество правильных ответов)
Зачтено	60 - 100 % правильных ответов
Не зачтено	Менее 60 % правильных ответов

5.2. Оценочные материалы для проведения аттестации.
Примерные тесты для проведения аттестации.

1) К правовым методам, обеспечивающим информационную безопасность, относятся:
- Разработка аппаратных средств обеспечения правовых данных.
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий.
- Разработка и конкретизация правовых нормативных актов обеспечения безопасности.

2) Основными источниками угроз информационной безопасности являются все указанное в списке:
- Хищение жестких дисков, подключение к сети, инсайдерство.
- Перехват данных, хищение данных, изменение архитектуры системы.
- Хищение данных, подкуп системных администраторов, нарушение регламента работы.

3) Виды информационной безопасности:
- Персональная, корпоративная, государственная.
- Клиентская, серверная, сетевая.
- Локальная, глобальная, смешанная.

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
- Несанкционированного доступа, воздействия в сети.
- Инсайдерства в организации.
- Чрезвычайных ситуаций.

5) Основные объекты информационной безопасности:
- Компьютерные сети, базы данных.
- Информационные системы, психологическое состояние пользователей.
- Бизнес-ориентированные, коммерческие системы.

6) Основными рисками информационной безопасности являются:
- Искажение, уменьшение объема, перекодировка информации.
- Техническое вмешательство, выведение из строя оборудования сети.
- Потеря, искажение, утечка информации.

7) К основным принципам обеспечения информационной безопасности относится:
-Экономической эффективности системы безопасности.
- Многоплатформенной реализации системы.
- Усиления защищенности всех звеньев системы.

8) Основными субъектами информационной безопасности являются:
- Руководители, менеджеры, администраторы компаний.
- Органы права, государства, бизнеса.
- Сетевые базы данных, фаерволлы.

9) Принципом информационной безопасности является принцип недопущения:
- Неоправданных ограничений при работе в сети (системе).
- Рисков безопасности сети, системы.
- Презумпции секретности.

10) Принципом политики информационной безопасности является принцип:
- Невозможности миновать защитные средства сети (системы).
- Усиления основного звена сети, системы.
- Полного блокирования доступа при риск-ситуациях.

11) К основным типам средств воздействия на компьютерную сеть относится:
- Компьютерный сбой.
- Логические закладки («мины»).
- Аварийное отключение питания.

12) Когда получен спам по e-mail с приложенным файлом, следует:
- Прочитать приложение, если оно не содержит ничего ценного – удалить.
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама.
- Удалить письмо с приложением, не раскрывая (не читая) его.

13) Наиболее распространены угрозы информационной безопасности корпоративной системы:
- Покупка нелицензионного ПО.
- Ошибки эксплуатации и неумышленного изменения режима работы системы.
- Сознательного внедрения сетевых вирусов.

14) Наиболее распространены угрозы информационной безопасности сети:
- Распределенный доступ клиент, отказ оборудования.
- Моральный износ сети, инсайдерство.
- Сбой (отказ) оборудования, нелегальное копирование данных.

15) Утечкой информации в системе называется ситуация, характеризуемая:
- Потерей данных в системе.
- Изменением формы информации.
- Изменением содержания информации.

16) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
- Целостность.
- Доступность.
- Актуальность.

5.3 Условия актуализации программы повышения квалификации

Высокий уровень качества подготовки слушателей по данной программе обеспечивается путем использования современных образовательных технологий:
- электронного и мультимедийного обучения;
- практико-ориентированного подхода;
- интерактивных форм и методов обучения (круглых столов, форумов, дискуссий и т.п.);
- экспертно-консультационного сопровождения слушателей на протяжении всего периода обучения.

6. Оценка качества реализации программы.

Оценочная анкета, предлагаемая слушателям, обеспечивает оценочную экспертизу реализованной дополнительной профессиональной программы повышения квалификации (см. Приложение 2).

Разработчик: Важенин Сергей Константинович,
старший преподаватель КМиА ФГБОУ ТИПКиА,

Чусова Татьяна Павловна, начальник отдела развития.

СОГЛАСОВАНО:

Врио проректора по УМР	Е.Е. Бугаева
Зав. УМО	Е.Н. Михайлаки
Заведующий кафедрой	Ж.А. Ермушко
Начальник отдела развития	Т.П. Чусова

Кадровое обеспечение образовательного процесса

№ п/п	Фамилия, имя, отчество,	Ученая степень, ученое звание	Основное место работы, должность	Место работы и должность по совместительству
1	Артеменко Александр Алексеевич		Зам. Директора РУНЦ ВС и ДВ «Информационная безопасность» ТУСУР	
2	Афонин Александр Анатольевич		Председатель комитета муниципальных услуг управления и информатизации Администрации г. Томска.	
3	Степанов Игорь Витальевич		Директор РУНЦ ВС и ДВ «Информационная безопасность» ТУСУР.	

Кадровое обеспечение образовательного процесса

№ п/п	Фамилия, имя, отчество,	Ученая степень, ученое звание	Основное место работы, должность	Место работы и должность по совместительству
1	Афонин Александр Анатольевич		Председатель комитета муниципальных услуг управления и информатизации Администрации г. Томска.	
2	Муратов Валерий Михайлович		Заместитель генерального директора по режиму АО «НПФ»Микран».	
3	Степанов Игорь Витальевич		Директор РУНЦ ВС и ДВ «Информационная безопасность» ТУСУР.	Специалист по технической защиты информации ФГБОУ ДПО ТИПКиА

Приложение 2

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

ТОМСКИЙ ИНСТИТУТ ПЕРЕПОДГОТОВКИ КАДРОВ И АГРОБИЗНЕСА

Оценочная анкета слушателя

Программа

1. Открытость и доступность информации об организации, осуществляющей образовательную деятельность

№	Показатели	Да	Нет
1	Информация о деятельности организации, осуществляющей образовательный процесс, размещена на стендах в помещении организации		
2	Информация о ТИПКиА размещена на официальном сайте организации в информационно-телекоммуникационной сети «Интернет»		
3	На сайте организации присутствует информация о дистанционных способах обратной связи с получателями услуг		
4	Наличие на сайте организации сведений о контактных телефонах, адресах электронной почты, электронных сервисах (форма для подачи электронного обращения)		
5	Наличие технической возможности выражения получателем услуг мнения о качестве условий оказания услуг организацией		

2. Комфортность условий, в которых осуществляется образовательная деятельность

№	Показатели	Да	Нет
1	Наличие комфортной зоны отдыха, оборудованной соответствующей мебелью		
2	Наличие и понятность навигации внутри организации		
3	Наличие и доступность питьевой воды, санитарно-гигиенических помещений		
4	Санитарное состояние помещений организации		
5	Транспортная доступность (возможность доехать до организации на общественном транспорте, наличие парковки)		

3. Доброжелательность, вежливость работников

№	Показатели	Да	Нет
1	Удовлетворенны ли Вы доброжелательностью, вежливостью работников организации, обеспечивающих первичный контакт и информирование при обращении в организацию		
2	Удовлетворенны ли Вы доброжелательностью, вежливостью работников организации, обеспечивающих непосредственное оказание образовательных услуг		
3	Удовлетворенны ли Вы доброжелательностью, вежливостью работников организации при использовании дистанционных форм		

	взаимодействия		

4. Удовлетворенность условиями ведения образовательной деятельности организации

№	Показатели	Да	Нет
1	Удовлетворенны ли Вы организационными условиями предоставляемых услуг		
2	Удовлетворенны ли Вы в целом условиями оказания услуг в организации		
3	Готовы ли Вы рекомендовать организацию родственникам и знакомым		

5. Организация обучения

№	Показатели	Да	Нет
1	Информацию о проведении обучения я получил(а) на сайте организации		
2	Расписание, информация о программе обучения и преподавателях мне были доступны на информационных ресурсах организации		
3	Я получил(а) все ответы на вопросы, касающиеся обучения		
4	Я считаю, что организацию обучения можно было сделать лучше		

6. Содержание программы

№	Показатели	Да	Нет
1	Вся информация по программе мне была интересна		
2	Часть тем я бы убрал(а) из программы		
3	Я считаю, что необходимо добавить некоторые важные темы		

Мнение по содержанию:
Какие важные темы стоит добавить в программу

_____
_____

Какие темы можно убрать из программы обучения

_____
_____