

Мир науки. Педагогика и психология / World of Science. Pedagogy and psychology <https://mir-nauki.com>

2023, Том 11, № 1 / 2023, Vol. 11, Iss. 1 <https://mir-nauki.com/issue-1-2023.html>

URL статьи: <https://mir-nauki.com/PDF/20PDMN123.pdf>

Ссылка для цитирования этой статьи:

Сиротский, А. А. Разработка и реализация дистанционной практикоориентированной программы повышения квалификации специалистов по защите персональных данных / А. А. Сиротский // Мир науки. Педагогика и психология. — 2023. — Т. 11. — № 1. — URL: <https://mir-nauki.com/PDF/20PDMN123.pdf>

For citation:

Sirotskiy A.A. Development and implementation of a remote practice-oriented professional development program for personal data protection specialists. *World of Science. Pedagogy and psychology*. 2023; 11(1): 20PDMN123. Available at: <https://mir-nauki.com/PDF/20PDMN123.pdf>. (In Russ., abstract in Eng.)

Сиротский Алексей Александрович

ФГБОУ ВО «Национальный исследовательский Московский государственный строительный университет»,
Москва, Россия

Доцент

Кандидат технических наук, доцент

E-mail: hotwater2009@yandex.ru

ORCID: <https://orcid.org/0000-0002-9343-7185>

РИНЦ: https://www.elibrary.ru/author_profile.asp?id=525833

Разработка и реализация дистанционной практикоориентированной программы повышения квалификации специалистов по защите персональных данных

Аннотация. В статье рассматривается задача создания ориентированной на формирование практических навыков дистанционной учебной программы повышения квалификации специалистов в области защиты персональных данных. Отмечается, что в настоящее время на рынке труда специалисты с компетенциями в данной области востребованы, а соответствующие учебные программы актуальны.

Описываются методы исследований и разработки учебной программы, характеризующейся максимально возможной для дистанционного формата содержательной насыщенностью и прямыми интерактивными формами взаимодействия преподавателя со слушателями. Представлена структурно-логическая модель программы, состав трудовых функций выпускника программы, описание совершенствуемых компетенций, а также приведены примеры отдельных элементов её содержательной части, включающей в себя видеолекции, вебинары, тестовые задания и практическую работу. В результате исследований, выделена и описана минимально необходимая изучаемая база, освоение которой требуется для формирования нужных знаний и навыков. В качестве примеров приведены компоненты изучаемой базы.

Раскрыто содержание и логика построения практического задания, состоящего из 30 действий, и подробно изложено выполнение первого действия, представляющего собой многофакторный анализ среды организации с выявлением и определением характеристик, непосредственно влияющих на решения, принимаемые при создании систем защиты персональных данных.

Также приведены реальные фрагменты иллюстративного материала с лекций и вебинаров и примеры выверенных тестовых вопросов, не допускающих неоднозначностей трактовки при выборе верных вариантов ответа.

Приведённая схема аттестационных мероприятий, включающая промежуточные и итоговые аттестации как по практической, так и по теоретической части, на практике прошедших обучение нескольких сотен слушателей, показала свою эффективность и целесообразность.

Модульная структура компонентов программы, основанная на принципах декомпозиции, имеет высокую адаптивную гибкость и может быть адаптирована, откорректирована, обновлена и дополнена в соответствии с динамикой изменения законодательства о персональных данных и подзаконной нормативно-правовой базы.

Ключевые слова: повышение квалификации; дистанционное обучение; персональные данные; оператор; информационная безопасность; практические навыки; специалисты; модель

Введение

Наряду с задачами повышения экономической, финансовой и правовой грамотности специалистов различных отраслей, в настоящее время одной из актуальных задач является подготовка кадров в области обеспечения защиты персональных данных в организациях. В силу обязательных требований законодательства к защите персональных данных граждан, специалисты по данному направлению востребованы в организациях всех видов деятельности и всех форм собственности. Несмотря на то, что информационная безопасность является одним из приоритетных направлений научно-технического развития [1], специалистов, имеющих базовое или дополнительное образование по соответствующему направлению явно недостаточно, в связи с чем имеют достаточно высокую востребованность программы повышения квалификации для специалистов смежных специализаций, ориентированные на совершенствование компетенций в области защиты персональных данных. Более того, не все специалисты, имеющие базовое профильное образование, достаточно глубоко знают нормы и требования по защите персональных данных и владеют соответствующими методологиями, необходимыми для квалифицированного выполнения данных профессиональных задач. В этой связи дополнительное обучение профильных специалистов позволяет предметно сориентировать их на решение специализированных задач по обеспечению защищенности персональных данных в компаниях.

Некоторые компании на подобные программы обучения направляют своих сотрудников, высвобождающихся с других должностей, которых планируют привлечь к работе в подразделениях по защите персональных данных, и которые пока ещё не имеют соответствующих знаний и навыков. Знания в области требований по защите персональных данных, методов и средств их реализации также являются крайне полезными при исполнении своих прямых служебных обязанностей сотрудниками отделов кадров, бухгалтерии, менеджерами по работе с клиентами, и другими сотрудниками компании, — это позволяет предупреждать возможные неумышленные нарушения, которые могут быть допущены ими в своей профессиональной сфере ввиду незнания специфических законодательных норм и требований.

Программы повышения квалификации по защите персональных данных также оказались весьма востребованы в национальных проектах («Демография», обучение по направлениям службы занятости населения, «Персональные цифровые сертификаты», «Цифровые профессии»), что позволяет подготовить соискателей к возможности трудоустройства по новым востребованным профессиям. По подготовленным и реализованным программам уже

проведено обучение нескольких сотен граждан, как из числа находящихся в поиске работы, так и из числа работающих в различных сферах, в том числе в организациях образования, культуры, социального обслуживания, центров оказания государственных и муниципальных услуг.

В целом, актуальность повышения квалификации специалистов в области защиты персональных данных является общепризнанной и подробно исследовалась в ряде научно-методологических работ, например в [2–4].

Методы исследования

Разработка и реализация программы повышения квалификации по защите персональных данных проводилась на базе института цифровых компетенций финансового университета при правительстве РФ.

Исходя из возможного контингента граждан, которые имеют законное право поступать и обучаться на программах повышения квалификации, а также открытости и доступности программы, следует, что на данную программу могут поступить лица, как имеющие базовое образование в области защиты информации, так и граждане из иных сфер деятельности. В этой связи одним из ключевых требований к разрабатываемой и реализуемой программе определено, что данная программа должна обеспечивать возможность качественного обучения как лиц, уже имеющих базовое образование и/или какой-либо опыт деятельности по защите информации, так и не имеющих оных, но при этом обладающих базовыми компетенциями в своей профессиональной деятельности.

Соответственно, целью программы повышения квалификации по защите персональных данных является совершенствование профессиональных компетенций руководителей и сотрудников коммерческих предприятий всех форм собственности и различных видов деятельности в сфере обеспечения комплексной защиты персональных данных сотрудников и клиентов в условиях интенсивного развития цифровой экономики [5] в соответствии с требованиями законодательства, нормативно-правовыми требованиями, обычаями делового оборота, условиями цифровой среды и информационного общества, сформировавшейся практикой и с учётом зарубежного и российского опыта; формирование теоретических знаний и практических умений воплотить полученные знания в конкретные формы и механизмы в действующем и организующемся бизнесе.

В рамках поставленных условий на разработку программы, применительно к реализации программы, необходимо было решить следующие задачи:

- формирование в краткой, сжатой и лаконичной форме чётких и ясных представлений о предмете профессиональной деятельности по защите персональных данных и месте этой деятельности в предметной области информационной безопасности, что в свою очередь направлено на адаптацию и профессиональное ориентирование слушателей, пока не имеющих специфического опыта или специфической подготовки;
- возможность реализации программы в полностью дистанционном формате, что обеспечит географическую независимость слушателей;
- максимизировать прямое взаимодействие слушателей с преподавателем;
- представить учебный материал в чёткой логической последовательности;
- обеспечить высокий уровень практической ориентированности программы, направленный не только на формирование теоретических знаний, но и практических навыков, необходимых для реальной деятельности.

Методы исследований и проектирования программы были направлены на поиск наиболее оптимальных:

- форматов и технологий дистанционного обучения [6];
- состава учебных модулей, дидактической системы [7; 8];
- содержательных компонентов учебных модулей [9];
- методов взаимодействия со слушателями;
- методов донесения знаний и формирования навыков;
- способов и средств промежуточной и итоговой аттестации слушателей [10].

Поскольку любые виды профессионального обучения направлены на формирование навыков и умений для выполнения оплачиваемой профессиональной деятельности, то одним из ключевых направлений исследований являлось поиск и выбор методов отработки практических навыков в условиях дистанционного взаимодействия.

Принципиальными методологическими направлениями исследований являлись исследования, направленные на обеспечение наглядности и информативности учебных материалов, адаптивности, позволяющей обеспечить наиболее благоприятный процесс обучения, компенсаторности, позволяющей минимизировать затраты сил и энергии слушателей на достижение целей обучения, интегративности, направленной на восприятие изучаемых модулей и тем как единое целое, определяющее успешность реализации процессов защиты персональных данных в организациях.

При разработке учебного плана и учебных материалов методы исследований также опирались на соответствие нормам и требованиям нормативно-правовой базы как в самой образовательной сфере, так и в сфере предметной области, а также на выявлении и исполнении требований образовательных и профессиональных стандартов.

Создание учебных материалов, планов занятий, лекционных презентаций, диалоговых моделей вебинаров опирались на исследования педагогических, а точнее андрагогических (андрагогика — раздел теории обучения, раскрывающий специфические закономерности освоения знаний и умений взрослым субъектом учебной деятельности) процессов и соответствующих им проблемно-ориентированных средств и методов обучения.

В данной части методической проблемы создания эффективной дистанционной программы обучения по заданным условиям включили в себя исследования:

- собственных имеющихся научно-методических разработок;
- методологии декомпозиции учебного процесса [11];
- средств и методов предметного обучения в дистанционном формате;
- способов организации совместной учебно-познавательной деятельности взрослых слушателей, в том числе руководителей организаций [12];
- методов мотивации и адаптации слушателей к новым или относительно новым видам профессиональной деятельности [13];
- методов организации активного обучения и активных форм проведения занятий [14; 15] в дистанционном формате;

- перспективных способов познавательного изложения учебного материала (проблемная лекция, лекция-визуализация, лекция-повторение, лекция формирования опорных понятий, лекция трактовки и альтернативного изложения, вебинар-дискуссия, вебинар-инструкция, вебинар-презентация, вебинар-обсуждение и др.).

Новизной проведённых исследований и разработок, положенных в основу созданного курса повышения квалификации, являются:

- структурно-логическая модель формирования содержательности и последовательности обучения на основе системы формируемых знаний и навыков;
- выделенный минимально необходимый перечень базовых сущностей, изучение которых необходимо для формирования возможности практической деятельности специалиста по защите персональных данных, а также определение минимальной глубины их изучения;
- выделенная система ключевых характеристик объекта защиты, на основе анализа которых производится выполнение практического задания;
- практико-ориентированное модульное взаимосвязанное проектное задание, состоящее из последовательности выполняемых действий;
- методика проведения интерактивной диалоговой формы вебинаров в режиме реального времени, опирающаяся на элементарные и легко воспринимаемые примеры жизненных ситуаций.

Результаты

Поскольку деятельность по защите персональных данных является частным случаем более обширной профессиональной области, то разработка образовательной программы опиралась на Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 10.03.01 «Информационная безопасность» (Утв. Приказом министерства образования и науки РФ от 01.12.2016 г. № 1515).

При разработке программы за основу был выбран профессиональный стандарт 06.033 "Специалист по защите информации в автоматизированных системах" (Утв. приказом Министерства труда и социальной защиты Российской Федерации от 15.09.2016 года № 522н) в части обобщенных трудовых и трудовых функций:

- обслуживание систем защиты информации в автоматизированных системах, код «А», уровень квалификации 5;
- обеспечение защиты информации в автоматизированных системах, код «В», уровень квалификации 6;
- внедрение систем защиты информации автоматизированных систем, код «С», уровень квалификации 6.

Трудовые функции выпускника программы повышения квалификации, с кодами согласно профессиональному стандарту:

- А/02.5, ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем;

- А/03.5, обеспечение защиты информации при выводе из эксплуатации автоматизированных систем;
- В/03.6, управление защитой информации в автоматизированных системах;
- С/02.6, разработка организационно-распорядительных документов по защите информации в автоматизированных системах;
- С/04.6, внедрение организационных мер по защите информации в автоматизированных системах.

Профессиональные компетенции, совершенствуемые и приобретаемые слушателями в процессе освоения программы:

1. **Общепрофессиональная (ОПК-1):** способность оценивать факторы, влияющие на безопасность обработки персональных данных в организации, анализировать требования нормативно-правовой базы в разрезе цифровой экономики и информационного общества в условиях постоянно изменяющейся внешней среды.
2. **Профессиональная (ПК-1):** готовность применять различные методы и технологии защиты персональных данных, осуществлять планирование, организацию и контроль мероприятий по защите персональных данных в условиях развития цифровой экономики.
3. **Профессиональная (ПК-2):** способность оценивать риски при эксплуатации информационных систем персональных данных, эффективно организовывать процесс обработки персональных данных, оценивать эффективность защитных мероприятий, разрабатывать предложения по их совершенствованию, осуществлять управление информационной безопасностью организации с применением информационных технологий.
4. **Профессиональная (ПК-3):** способность принимать участие в обследовании информационных систем персональных данных, определять требования к построению систем защиты персональных данных в цифровой экономике, выявлять угрозы безопасности персональных данных в организации, выявлять и обрабатывать инциденты информационной безопасности персональных данных, определять требуемые уровни защищённости персональных данных, обрабатываемых в информационных системах персональных данных, осуществлять выбор и обосновывать необходимость применения средств защиты персональных данных, разрабатывать организационно-распорядительную документацию, руководить процессами обеспечения защищённости персональных данных на предприятии.

Важным этапом проектирования программы является формирование совокупности знаний, умений и владений, которыми должны будут обладать слушатели, успешно окончившие программу обучения. Сложность данного этапа определяется весьма ограниченным количеством учебных часов, отводимых на программы повышения квалификации, в отличие от более обширных программ профессиональной переподготовки. При этом, как уже отмечалось, одной из принципиальных задач является ориентация программы на практическую деятельность, что должно выражаться в развитии практических навыков слушателей по выстраиванию безопасной системы обработки персональных данных в организации.

Прежде всего было необходимо чётко определить состав формируемых у слушателей знаний, навыков и владений изучаемой предметной областью. Общий принцип избранного подхода к моделированию показан на рисунке 1. Каждая формируемая трудовая функция сопоставляется с одной или несколькими (наиболее принципиальными для её формирования) компетенциями, на основе чего определяются учебные действия. Одновременно с этим выявляется необходимая база. Под базой здесь понимаются любые сущности, с которыми должен быть знаком специалист, и которые он должен уметь использовать и применять в большей или меньшей степени. Применительно к рассматриваемой предметной области учебной программы, базой являются:

- совокупность законодательных и иных нормативно-правовых актов (НПА), определяющих основные требования по защите персональных данных, и которыми необходимо руководствоваться такому специалисту;
- совокупность аналитических методов, применяемых в практике работ по обеспечению информационной безопасности;
- конкретные методики оценки рисков безопасности;
- конкретные приёмы проведения обследования и оценки защищённости информационной инфраструктуры организации [16];
- существующие информационные средства и информационные ресурсы, которые необходимы или как минимум полезны при реализации задач по защите персональных данных;
- программные средства построения и реализации информационных систем персональных данных (системы хранения и обработки информации);
- программные и технические средства защиты информации, наиболее часто применяемые при создании систем защиты информационных систем персональных данных;
- система стандартов и практик управления информационной безопасностью.

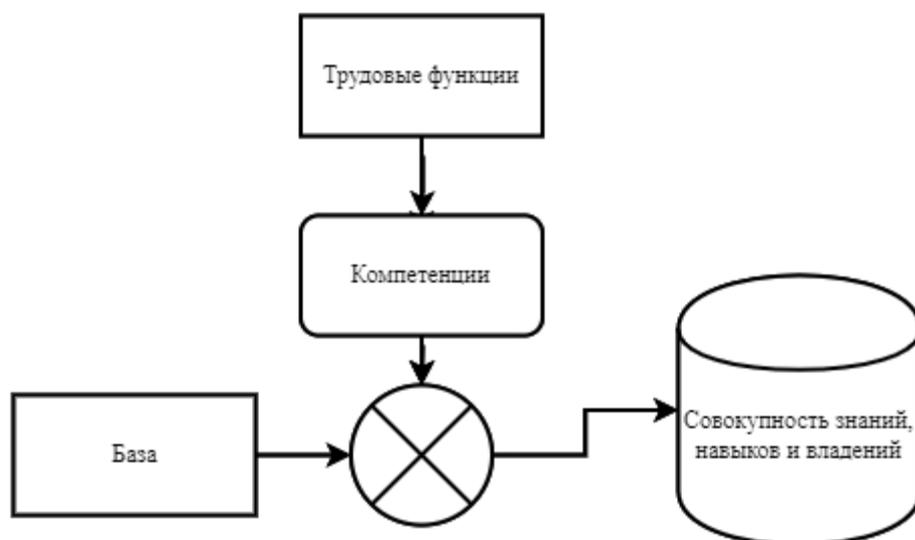


Рисунок 1. Общий принцип структурно-логического моделирования состава учебной программы (составлено автором)

Модель, составленная с использованием рассмотренного подхода, приведена на рисунке 2. Каждая трудовая функция (ТФ) находит отражение через одну, две или три компетенции, в контексте которых она преимущественно рассматривается. В свою очередь, каждая компетенция направлена на реализацию как минимум двух трудовых функций. Как видно, наиболее ёмкой оказывается компетенция ПК-3, включающая в себя самый широкий спектр действий, а значит и умений.

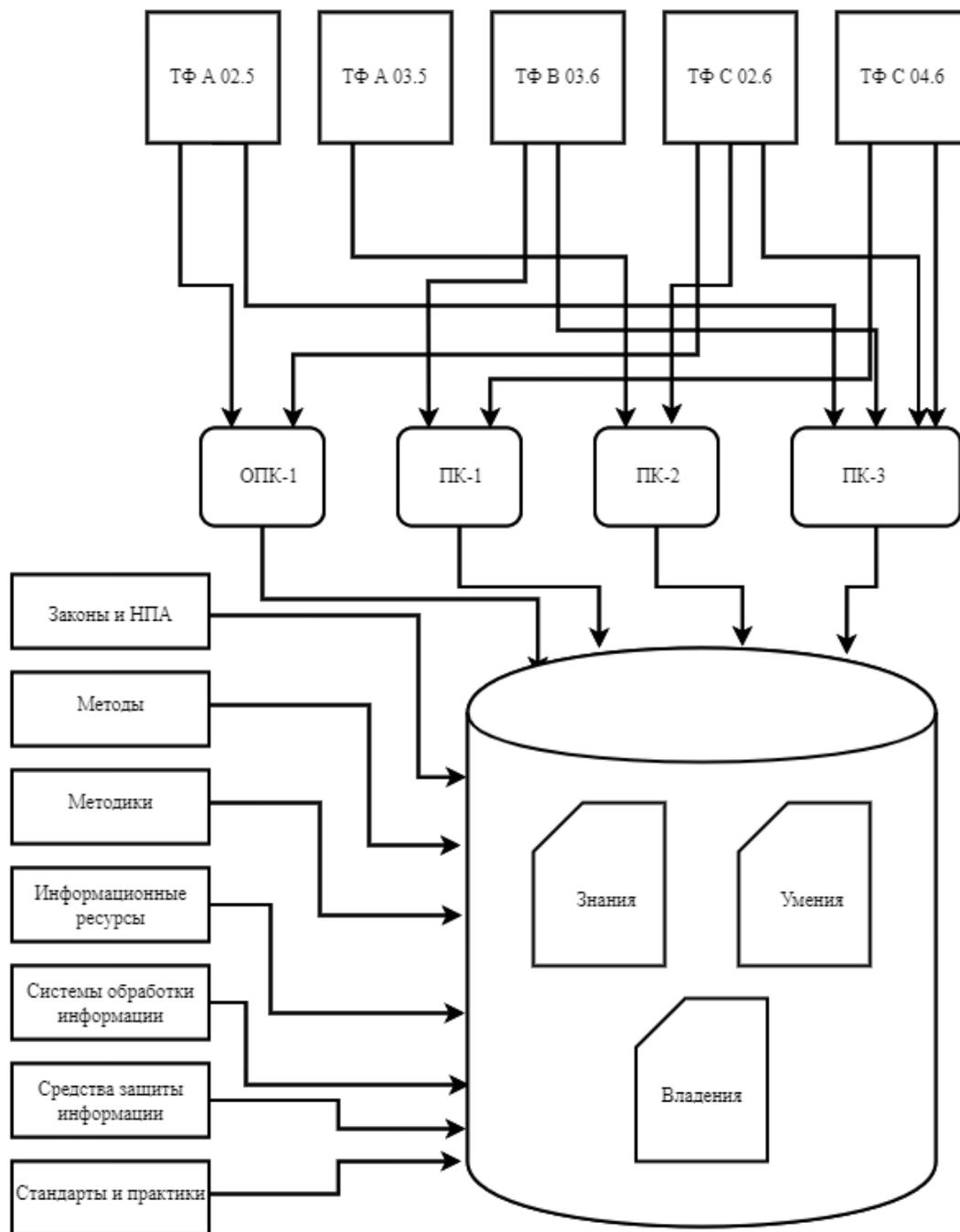


Рисунок 2. Структурно-логическая модель состава учебной программы повышения квалификации по защите персональных данных (составлено автором)

Не вдаваясь в детализацию, приведём перечень знаний, умений и владений, которые сформулированы в рамках данной программы с учётом тенденций по активной информатизации и цифровизации всех сфер общественных и деловых отношений. Таким образом, выпускники программы повышения квалификации должны:

а) Знать:

- основные характеристики и тенденции развития современной цифровой экономики, информационно-коммуникативные процессы и механизмы общественных и корпоративных коммуникаций;
- формы представления, хранения и обработки персональных данных в цифровой среде;
- основные положения нормативных правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных;
- основные виды угроз безопасности персональных данных в информационных системах персональных данных;
- содержание и порядок организации работ по выявлению угроз безопасности персональных данных;
- процедуры задания и реализации требований по защите информации в информационных системах персональных данных;
- меры обеспечения безопасности персональных данных;
- требования по обеспечению безопасности персональных данных;
- порядок применения организационных мер и технических средств обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных.

б) Уметь:

- создавать организационно-распорядительные документы в интересах организации по обеспечению безопасности персональных данных;
- планировать мероприятия по обеспечению безопасности персональных данных;
- обосновывать и задавать требования по обеспечению безопасности персональных данных в информационных системах персональных данных;
- проводить оценки актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- определять состав и содержание мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для блокирования угроз безопасности персональных данных.

в) Владеть:

- навыками анализа деловых процессов в цифровой экономике;
- навыками работы с правовыми базами данных;
- навыками определения уровней защищённости персональных данных;
- навыками выявления угроз безопасности персональных данных в информационных системах персональных данных;
- навыками разработки необходимых документов в интересах организации по обеспечению безопасности персональных данных;

- навыками применения сертифицированных средств защиты информации.

Важной составной частью проектирования программы является конкретизация изучаемой базы (базовых сущностей), а также определение глубины их изучения (поскольку в рамках ограниченной по времени программы повышения квалификации детальное изучение, например, специализированных программных средств не представляется возможным).

Для конкретизации, приведём (в сокращённом варианте) отдельные составные компоненты изучаемой базы с оценкой минимально необходимой (с учётом ограничений программ повышения квалификации) глубины изучения (табл. 1). По соображениям объективности и неаффилированности, названия конкретных средств, программных продуктов и информационных ресурсов в таблице не приводятся. На учебных занятиях называются и обсуждаются конкретные средства, которые могут быть применены как при защите персональных данных в небольших, локальных, так и в довольно крупных распределённых информационных системах [17], выстраиваемых в больших компаниях.

При этом учебный курс построен таким образом, чтобы дать по возможности максимальные знания по защите персональных данных с учётом особенностей различных видов экономической и хозяйственной деятельности. Хотя, безусловно, до сведения слушателей доводится, что существуют такие виды деятельности, в которых присутствует ряд обособленных отраслевых требований, которые выходят за рамки общего курса и требуют отдельного изучения. К таким отраслям, в частности, относится финансово-кредитная сфера [18].

Таблица 1

Перечень компонентов изучаемой базы с оценкой глубины изучения

База	Компоненты базы	Глубина изучения
Законы	Федеральный закон от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации"	Ключевые нормы информационных отношений и основные требования к защите информации
	Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"	Детально — все нормы и требования применительно к операторам персональных данных, обзорно — нормы и требования применительно к государственным регуляторам
	Гражданский кодекс Российской Федерации (ГК РФ)	Отдельные нормы применительно к информационным технологиям
	Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ	Детально — состав правонарушений, предусмотренных ст. 13.11, обзорно — состав иных правонарушений, предусмотренных главой 13
НПА	Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК) России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»	Подробно и детально
	Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»	Подробно и детально

База	Компоненты базы	Глубина изучения
Методики	Методика оценки угроз безопасности информации (утв. ФСТЭК России 05.02.2021 г.)	Подробно, детально, с практическими примерами и практической работой
Информационные ресурсы	Электронная информационно-правовая система	Формирование способности самостоятельной работы с системой и поиска документов
	Банк данных угроз информации	Подробное изучение атрибутов угроз, обзорный анализ угроз и формирование способности самостоятельного поиска, анализа и сопоставления угроз
	Банк данных уязвимостей программного обеспечения	Подробное изучение атрибутов уязвимостей, обзорный анализ уязвимостей и формирование способности самостоятельного анализа информационной инфраструктуры на предмет возможного наличия уязвимостей в рамках практической работы
Системы обработки информации	Программные средства автоматизации деятельности предприятий	Обзорное знакомство с функциональными особенностями и областью применения
Системное и прикладное программное обеспечение	Операционная система	Компоненты безопасности и интерфейсы доступа к настройкам безопасности
	Средства доступа к сетевым сервисам (браузеры)	Детальное изучение настроек механизмов, функций и сервисов безопасности
Средства защиты информации	Программный комплекс защиты от несанкционированного доступа	Обзор функциональных возможностей и областей применения
	Аппаратно-программный комплекс доверенной загрузки	
	Межсетевой экран	
	Сетевой сканер	
	Антивирусное программное обеспечение	Детальное изучение функционала и механизмов настройки функций безопасности

Составлено автором

Для формирования в рамках учебных задач практического подхода и практических навыков была сформирована практическая работа, выполняемая по единой методике и состоящая из 30 действий. В практической работе за основу выбирается условный объект (организация), на примере которой выполняется планирование решений по организации системы защиты персональных данных. Свойства и характеристики организации являются определяющими факторами, влияющими на принятие соответствующих решений в рамках создания системы защиты персональных данных. Поэтому первым действием практической работы является анализ среды организации по ряду факторов и показателей, от которых непосредственно зависит исполнение обязательных нормативно-правовых требований по защите персональных данных. Примеры некоторых характеристик и показателей, которые выявляются, определяются и анализируются в первом действии, приведены в таблице 2.

Важно, что каждый фактор и показатель, подвергающийся анализу в первом действии практической работы, находит своё отражение в последующих действиях. В целом, результаты, полученные в одном действии, являются основой для выполнения одного или нескольких последующих действий. Таким образом формируется понимание взаимосвязи между зависимыми факторами и принимаемыми решениями. Однако при этом есть и такие ситуации, которые требуют при необходимости скорректировать предварительно принятые решения на предыдущих действиях, что в целом соответствует обычной реальной инженерной проектной практике.

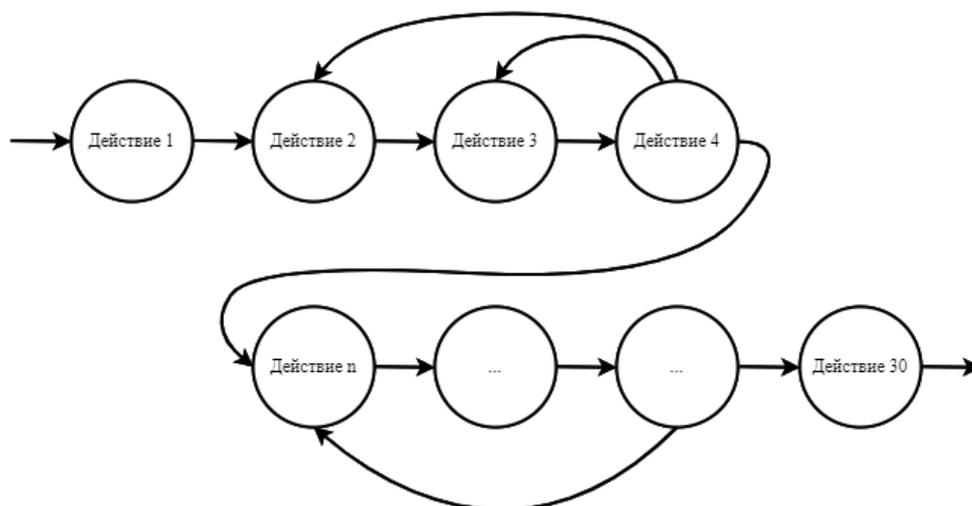
Таблица 2

**Примеры характеристик и показателей,
выявляемых в первом действии практического задания**

№ п/п	Характеристика или показатель	Примеры возможных определений
1	Организационно-правовой статус организации	Индивидуальный предприниматель, общество с ограниченной ответственностью, автономная некоммерческая организация, муниципальная организация, орган местного самоуправления и др.
2	Юридическое местонахождение организации	Город, область, село и т. п.
3	Физическое местонахождение организации	Офисное помещение в бизнес-центре, отдельно стоящее здание и т. п.
4	Правовой статус занимаемого помещения	В собственности, аренда, субаренда и т. п.
5	Предмет деятельности	Оптовые или розничные продажи, оказание образовательных услуг, оказание услуг по строительству или ремонту, оказание государственных услуг, общественная деятельность и т. п.
6	Количество собственных сотрудников	Ориентировочное значение, с точностью до порядка числа
7	Состав сотрудников по должностным функциям	Руководители, бухгалтеры, менеджеры, рабочие, тренеры и т. п.
8	Количество сторонних лиц (клиентов), персональные данные которых могут запрашиваться и обрабатываться	Ориентировочное значение, с точностью до порядка числа
9	Состав целевой аудитории клиентов	Клиенты автосервиса, посетители спортивного клуба и т. п.
10	Масштаб организации	Наличие или отсутствие филиалов
11	Место физического и географического размещения хранилищ персональных данных	Собственная инфраструктура, арендованная инфраструктура, заимствованный сервис и т. п.
12	Текущее состояние деятельности по защите персональных данных	Ведётся (требуется коррекция, улучшение) или не ведётся (организация создаётся)

Составлено автором

Данный принцип выполнения практической работы схематически показан на рисунке 3 моделью в виде ориентированного графа. Визуализация и формализация процессов с помощью графовых моделей [19; 20] представляется одной из наиболее удобных для отображения и анализа последовательности выполнения действий рассматриваемой учебной практической работы.



**Рисунок 3. Модель выполнения практической
работы в виде ориентированного графа (составлено автором)**

Преподнесение материалов учебного курса производится на:

- предварительно записанных видеолекциях, состоящих из модулей по 10–20 минут, причём наиболее принципиальные для осознания положения, изложенные в одном из более ранних модулей, при необходимости, акцентируются в ином контексте в последующих модулях;
- интерактивных вебинарах в режиме реального времени, на которых преподнесение материала выстраивается в чёткой последовательности и с обязательным диалогом со слушателями, обеспечивающим их полноценное погружение в изучаемую область.

Лекционный материал строится преимущественно не трансляционным, а иллюстративно-трактующим способом, подразумевающим не только изложение теоретических норм и понятий, но и максимальное количество примеров, пояснений, альтернативных изложений и иллюстраций. Иллюстрации применяются как ассоциативные, направленные на установление визуальных ассоциаций для наилучшего запоминания изложенного материала, так и предметные, в виде графических схем, диаграмм, форм документов, фотографий, скриншотов окон программных систем и т. д. Пример лекционного слайда по теме «категории персональных данных» с разбором примеров по определению категорий обрабатываемых персональных данных в различных организациях, приведён на рисунке 4. Основу слайда составляет предметная схема, а в нижнем правом углу размещена ассоциативная иллюстрация.

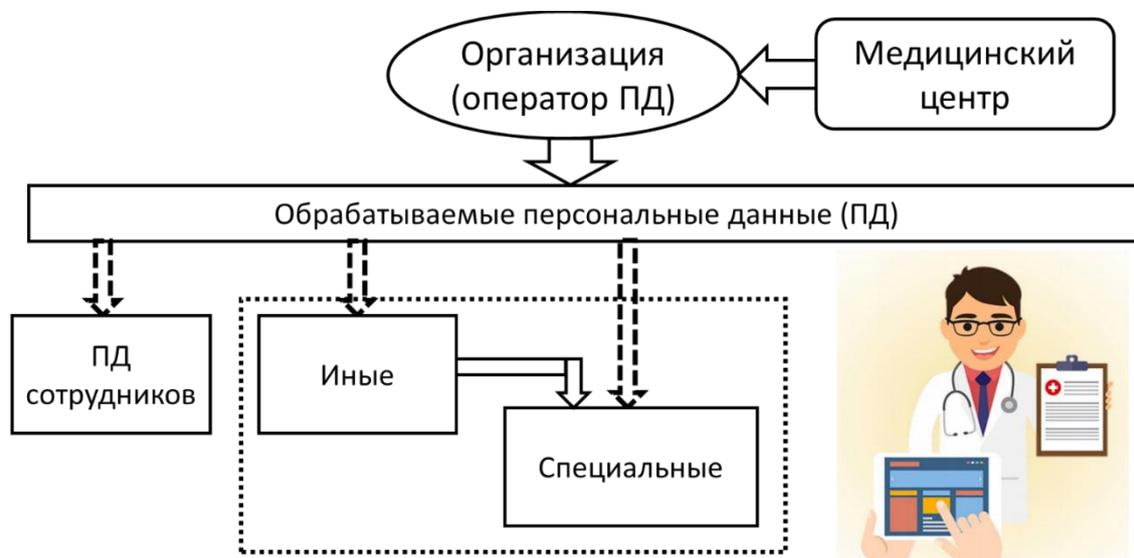


Рисунок 4. Слайд из лекции по теме «категории персональных данных» (составлено автором)

Вебинары в режиме реального времени занимают не менее 40 % всего объёма учебного курса. Именно на вебинарах разбираются и обсуждаются практические ситуации, которые могут с высокой вероятностью встретиться в реальной деятельности. Интерактивный диалог строится с возможностью каждому слушателю написать в чате вебинара своё восприятие ситуации, своё решение, которое он принял бы в разбираемом примере, своё мнение, а также задать обратные вопросы. Результатом обсуждения является наглядное разрешение обсуждаемой ситуации и возникших при этом сопутствующих вопросов. Важно также заметить, что в рамках проблематики защиты персональных данных существуют и неоднозначно разрешаемые задачи (чаще всего, из-за отсутствия соответствующих прямых нормативно-правовых указаний), в подобных примерах совместно обсуждается возможная

практика и вырабатывается возможный сценарий действий специалиста по защите персональных данных.

Одной из частных задач вебинаров является разбор практических проблемных ситуаций и реальных профессиональных задач. Поэтому на вебинарах большое значение уделяется подготовке к выполнению практикоориентированной самостоятельной работы как основы будущей самостоятельной профессиональной деятельности.

Одним из действий в рамках практической работы, и одним из важнейших действий в реальной практике является определение целей обработки персональных данных и соответственного минимально необходимого, но достаточного состава обрабатываемых персональных данных. Определение целей обработки и состава персональных данных является не только одной из первейших практических задач, но должно выполняться мотивированно, обоснованно, аргументированно и быть в организации должным образом задокументировано. Практическая отработка этого навыка и формирование соответствующих знаний проводится на вебинаре, и как правило, сопровождается большим интересом слушателей, а также их активным участием в выстраивании логических цепочек «цель → задача → необходимые данные → достаточные данные → аргументация → обоснование». Пример слайда с соответствующего вебинара приведён на рисунке 5.



Рисунок 5. Слайд с вебинара по теме «взаимосвязь целей обработки и объёма персональных данных» (составлено автором)

По итогам обучения каждый слушатель в рамках выполнения практической работы формирует прообраз профессионального портфолио, включающего в себя:

- отчёт по обследованию организации — оператора персональных данных;
- решение задачи по определению целей и состава обрабатываемых персональных данных;
- проект политики безопасности организации в области обработки персональных данных;
- проект внутреннего режима конфиденциальности для сотрудников, имеющих доступ к персональным данным;
- проект «согласия на обработку персональных данных» для клиентов;

- отчёт по моделированию и оценке угроз безопасности персональным данным в организации;
- определение необходимого уровня защищённости персональных данных для рассматриваемой организации;
- выбор средств обработки информации;
- проект системы программно-технической защиты персональных данных;
- план организационных действий, направленных на обеспечение защищённости персональных данных в организации;
- план работ по подготовке организации к обработке персональных данных в соответствии с нормативными требованиями.

Для консультаций слушателей по возникающим у них в процессе выполнения практического задания вопросам был организован ещё один компонент учебного процесса — форум, интегрированный в систему дистанционного обучения и доступный в личном кабинете каждого слушателя. При возникновении вопросов, каждый слушатель может создать либо свою отдельную тему, либо написать вопрос в уже имеющейся ветке форума (теме). Возникшие вопросы таким образом могут обсуждаться совместно всеми слушателями, и кроме того, на вопросы отвечают преподаватели и руководители образовательной организации.

Схема аттестации слушателей (рис. 6) — многофакторная, она включает в себя тестирования по теоретической части, зачёты по блокам (модулям) практической работы и итоговую защиту практической работы.

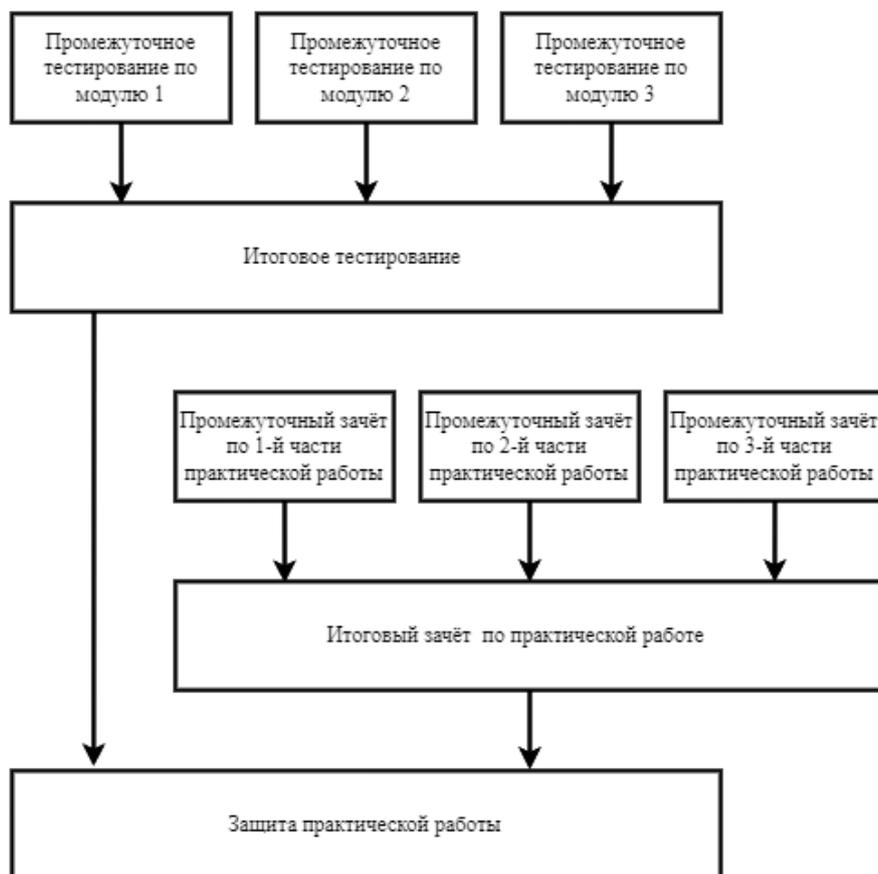


Рисунок 6. Схема аттестации по учебной программе «защита персональных данных в организации» (составлено автором)

Поскольку учебная программа условно подразделяется на три модуля, то промежуточные тестирования проводятся по каждому из трёх укрупнённых модулей учебной программы, а в заключение проводится и итоговое тестирование. Как промежуточное, так и итоговое тестирования преследуют цель контроля усвоения теоретических знаний. Вопросы итогового теста в целом соответствуют выборке вопросов из промежуточных тестов. Все тестовые вопросы направлены на контроль не просто теоретических, а наиболее важных и принципиальных знаний. Причём, тестовые вопросы сформулированы таким образом, чтобы исключить возможности неоднозначных трактовок. Ниже для примера приведены несколько вопросов.

Вопрос № 1. Кто может стать оператором персональных данных? (выберите все верные варианты ответов):

- А) Физическое лицо.
- Б) Индивидуальный предприниматель.
- В) Юридическое лицо.
- Г) Государственная организация.

Вопрос № 2. Какие из перечисленных документов отменены и больше не действуют? (выберите все верные варианты ответов):

А) Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Б) Совместный приказ ФСТЭК, Федеральной Службы Безопасности и Мининформсвязи РФ от 13.02.2008 № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных».

В) Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Г) Постановление Правительства РФ от 13.02.2019 г. № 146 «Об утверждении Правил организации и осуществления государственного контроля и надзора за обработкой персональных данных».

Вопрос № 3. Комплекс программных или аппаратных средств, которые выявляют факты и предотвращают попытки несанкционированного доступа в корпоративную систему, называется (выберите один верный ответ):

- А) Система обеспечения информационной безопасности.
- Б) Система разграничения сетевого трафика.
- В) Система авторизации и аутентификации.
- Г) Система контроля доступа.
- Д) Система обнаружения и предотвращения вторжений.

Вопрос № 4. Угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе, относятся к угрозам (выберите один верный ответ):

- А) 1-го типа.
- Б) 2-го типа.
- В) 3-го типа.
- Г) 4-го типа.

На защите практической работы от каждого слушателя требуется представить сообщение о результатах проведённого анализа, выбранных решениях и соответствующих основаниях проведённых действий. С учётом того, что письменная работа уже просматривалась, и при наличии существенных замечаний, отправлялась на доработку, сама итоговая защита занимает всего несколько минут и преследует цель краткого формулирования выбранных решений и полученных результатов.

Таким образом, используя научно-методическую основу, в рамках ограниченного объёма учебного времени создана и реализована информативно насыщенная и практикоориентированная программа для дистанционного формата повышения квалификации специалистов по защите персональных данных.

Обсуждение

На текущий момент по данной программе обучено уже несколько сотен слушателей. По окончании обучения от слушателей получали обратную связь, так называемую «рефлексию». Важно отметить, что слушатели весьма положительно охарактеризовали как процесс обучения, так и качество и объём полученных знаний и навыков. Первоначально некоторые слушатели выражали обеспокоенность довольно большим количеством аттестационных мероприятий, однако в процессе обучения данная обеспокоенность исчезала, тому способствовали несколько факторов:

- во-первых, все аттестационные мероприятия направлены именно на контроль сформированных знаний и их закрепление;
- во-вторых, все вопросы тестирования поставлены предельно чётко, а варианты ответов сформулированы таким образом, чтобы не допускать сомнительные неоднозначности;
- в-третьих, на вебинарах подробно проводился разбор всех необходимых тем и учебных вопросов, с тем чтобы слушатели, участвовавшие в вебинарах, были способны успешно пройти аттестационные мероприятия;
- в-четвёртых, слушатели имели возможность просмотреть повторно записи вебинаров любое количество раз.

Следует также отметить принципиальную особенность самой предметной области, связанной с информационной безопасностью в целом и защитой персональных данных в частности. Она заключается в очень высокой динамичности — нормативно-правовые основы и требования постоянно изменяются, дополняются, совершенствуются. Это объясняется как относительной молодостью как самого предметного направления информационной безопасности и защиты персональных данных, так и высокими темпами информатизации и цифровизации деловых и общественных процессов. И первое, и второе получили активное развитие в течении нескольких последних десятилетий. Сам Федеральный Закон «О защите персональных данных» был принят в России в 2006 году, т. е. по историческим меркам развития и формирования научных направлений — совсем недавно.

За период с момента принятия, в Федеральный Закон «О защите персональных данных» вносились изменения и дополнения 28 раз [21], а количество подзаконных нормативно-правовых и регламентирующих документов, которыми необходимо руководствоваться в процессах организации и управления защитой персональных данных, исчисляется десятками [22–24]. Они также претерпевают изменения, некоторые нормы и принципы изменяются, соответственно изменяется и состав актуальных документов. Всё это требует возможности максимально оперативной коррекции учебной программы, которая должна по возможности максимально быстро отражать в себе все происходящие изменения. Такая возможность в структуру программы заложена на этапе её проектирования:

- модули видеолекций, длительностью по 10–20 минут, и консолидированные по отдельным предметным темам и вопросам, могут быть относительно быстро перезаписаны и заменены;
- могут быть созданы (и периодически создаются) новые модули видеолекций, которые интегрируются к уже существующим;
- вебинары, как компонент прямого интерактивного взаимодействия слушателей с преподавателем, принимают на себя основную задачу по изучению новой содержательной части, для этого производится переработка содержания визуальных материалов (слайдов презентаций), демонстрируемых на вебинарах;
- тестовые вопросы проходят периодическую проверку на актуальность и корректность, при необходимости они заменяются полностью или в части вариантов правильных ответов.

Заключение

В связи с планомерно усложняющимися нормативными и законодательными требованиями к защите персональных данных, планируемым ужесточением штрафных санкций за нарушения, а также имеющим место случаям неправомерного распространения персональных данных, перед организациями — операторами персональных данных стоит задача обеспечения надлежащей защищённости обрабатываемых персональных данных в соответствии с требованиями законодательства и нормативно-правовых актов.

Практикоориентированные программы, предоставляющие соответствующие знания и навыки, освоение которых даёт возможность непосредственно погрузиться в рабочий процесс, имеют высокую востребованность. Мониторинг рынка труда и вакансий показывает, что практически постоянно присутствует спрос на сотрудников, имеющих компетенции в области обеспечения защиты персональных данных, и способных работать в команде служб информационной безопасности компаний различного уровня.

В рамках проведённого исследования были выделены критерии построения практикоориентированной программы повышения квалификации по защите персональных данных, построена модель программы, сформирована её структура и выполнено содержательное наполнение.

В качестве методологии обучения были выбраны приёмы, обеспечивающие максимально возможное прямое учебное взаимодействие в дистанционном формате, а практическая часть работы с поэтапными заданиями выстроена в максимальном приближении к последовательности процедур, которые присутствуют в деятельности реальной организации.

Модульное построение программы позволяет быстро и оперативно вносить изменения и коррективы в соответствии с трансформацией деловых процессов и динамикой изменения нормативно-правовой базы.

Анализ востребованности программы показал высокую мотивацию слушателей, а также целесообразность дальнейшего развития как данной программы, так аналогичных программ по смежным задачам обеспечения информационной безопасности.

ЛИТЕРАТУРА

1. Белянкова, Е.И. Информационная безопасность как приоритетное направление работы органов государственной власти в сети Интернет / Е.И. Белянкова, М.Ю. Александрова // Молодой ученый. — 2018. — № 7(193). — С. 124–126. — EDN YPPLDG.
2. Насыров, А.Р. Актуальность курсов повышения квалификации операторов ЭВМ, обрабатывающих персональные данные средствами вычислительной техники / А.Р. Насыров, А.С. Сафиуллин // Современные проблемы социально-гуманитарных наук: Сборник докладов I Всероссийской научно-практической заочной конференции (с международным участием), Казань, 06 июня — 06 2015 года / Научный ред. А.В. Гумеров. — Казань: Отечество, 2015. — С. 86–89. — EDN UJATXN.
3. Зейналов, Д.Т. Повышение квалификации специалистов организаций и предприятий в области защиты информации и персональных данных / Д.Т. Зейналов, А.Р. Шахмаева, Г.И. Качаева // Неделя науки-2017: сборник материалов XXXVIII итоговой научно-технической конференции преподавателей, сотрудников, аспирантов и студентов Дагестанского государственного технического университета, Махачкала, 17–22 апреля 2017 года. — Махачкала: Дагестанский государственный технический университет, 2017. — С. 419–421. — EDN ZANFRT.
4. Казыханов, А.А. Необходимость повышения квалификации сотрудников, занимающихся обработкой персональных данных / А.А. Казыханов, К.Г. Попов // Символ науки: международный научный журнал. — 2016. — № 5-2(17). — С. 46–47. — EDN WAFRCX.
5. Сиротский, А.А. Тенденции развития информационных сервисов в структуре цифровой экономики / А.А. Сиротский, А.Э. Самадуров // Современные информационные технологии в образовании, науке и промышленности: XI Международная конференция, IX Международный конкурс научных и научно-методических работ, Москва, 02–03 ноября 2018 года / Ответственные редакторы: Т.В. Пирязева, В.В. Серов. — Москва: ООО "Издательство "Спутник+", 2018. — С. 169–172. — EDN YWFBJB.
6. Гулая, Т.М. Специфика взаимодействия преподавателя и студентов в условиях формата онлайн обучения с использованием дистанционных образовательных технологий / Т.М. Гулая, С.А. Романова // Современное педагогическое образование. — 2022. — № 8. — С. 42–45. — EDN QWZXRВ.

7. Нуриев, Н.К. Дидактическая инженерия: параметрическое проектирование дидактических систем / Н.К. Нуриев, С.Д. Старыгина. — Казань: Общество с ограниченной ответственностью "Редакционно-издательский центр "Школа", 2020. — 104 с. — ISBN 978-5-00162-266-6. — EDN SXPPWK.
8. Элибаева, Л.С. Особенности дидактической системы модульного обучения / Л.С. Элибаева, У.Г. Собиров // Вестник магистратуры. — 2019. — № 4-4(91). — С. 15–16. — EDN WKWELS.
9. Серик, М. Структурно-логическая схема в содержании информационно-дидактической системы / М. Серик, Г.Н. Нугманова, Н. Азиева // Международный журнал прикладных и фундаментальных исследований. — 2013. — № 11-2. — С. 82–83. — EDN RHDLDN.
10. Литвинов, В.А. К вопросу об автоматизации измерения умений по дисциплинам практической направленности / В.А. Литвинов, В.Э. Баумтрог // Современное образование. — 2017. — № 1. — С. 144–152. — EDN VZEYHJ.
11. Сиротский, А.А. Декомпозиция содержания учебного процесса как важный компонент качественного образования / А.А. Сиротский // Преподавание информационных технологий в Российской Федерации: Материалы Шестнадцатой открытой Всероссийской конференции, Москва, 14–15 мая 2018 года. — Москва: Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет), 2018. — С. 104–106. — EDN XUJESL.
12. Терехова, Т.А. Психолого-педагогические условия профессионального обучения руководителей / Т.А. Терехова, Л.Л. Михайлова // Baikal Research Journal. — 2022. — Т. 13. — № 1. — DOI 10.17150/2411-6262.2022.13(1).19. — EDN KOXAZI.
13. Ветошкина, Т.А. Людям нужно научиться быть профессионально мобильными, то есть способными к овладению новыми видами деятельности / Т.А. Ветошкина // Дискуссия. — 2016. — № 8(71). — С. 6–12. — EDN XVTNPT.
14. Тэттэр, А.Ю. Использование активных и интерактивных форм проведения занятий в европейских университетах / А.Ю. Тэттэр, В.Ю. Тэттэр, А.А. Коновальчук // Инновационное образование и экономика. — 2012. — № 10. — С. 46–48. — EDN OXPWBJ.
15. Исакова, М.К. Проведение лекционных занятий с применением активных форм обучения / М.К. Исакова, Р.Н. Жартыбаев, Р.С. Ибрагимова // Евразийский союз ученых. — 2014. — № 5-5(5). — С. 76–78. — EDN TSNLDX.
16. Сиротский, А.А. Формализованная модель аудита информационной безопасности организации на предмет соответствия требованиям стандартов / А.А. Сиротский, С.А. Резниченко // Безопасность информационных технологий. — 2021. — Т. 28. — № 3. — С. 103–117. — DOI 10.26583/bit.2021.3.09. — EDN LSDPLE.
17. Сиротский, А.А. Распределенные системы. Организация и типология / А.А. Сиротский // Техника машиностроения. — 2012. — № 2(82). — С. 34–37. — EDN RURSLL.

18. Сиротский, А.А. Некоторые особенности автоматизированных банковских процессов с позиций управления текущей операционной деятельностью / А.А. Сиротский // Вестник евразийской науки. — 2019. — Т. 11. — № 1. — С. 58. — EDN SMTQFR.
19. Исаев, Р.А. Визуализация графовых моделей: подход к построению метафор представления / Р.А. Исаев, А.Г. Подвесовский // Научная визуализация. — 2021. — Т. 13. — № 4. — С. 9–24. — DOI 10.26583/sv.13.4.02. — EDN SYGKVI.
20. Смоленцева, Т.Е. Графовая модель данных в задаче выбора направления дальнейшего обучения / Т.Е. Смоленцева, А.В. Калач, Р.С. Толмасов // Вестник Воронежского института ФСИИ России. — 2022. — № 3. — С. 116–120. — EDN VVIYUR.
21. Сиротский, А.А. Анализ изменений законодательства о персональных данных, вступающих в силу с 1 сентября 2022 г. / А.А. Сиротский // Безопасность информационных технологий. — 2022. — Т. 29. — № 4. — С. 67–81. — DOI 10.26583/bit.2022.4.06. — EDN MFRYWU.
22. Гильманшина, А.Л. Анализ литературы и нормативно-правовой базы в области защиты персональных данных / А.Л. Гильманшина // Вестник науки. — 2019. — Т. 2. — № 3(12). — С. 13–16. — EDN YZABTV.
23. Смаженков, Н.С. Нормативно-правовое регулирование защиты персональных данных в условиях использования цифровых технологий / Н.С. Смаженков // Вопросы российской юстиции. — 2020. — № 7. — С. 576–583. — EDN JHAVGN.
24. Лямчев, В.Е. Нормативно-правовое регулирование отношений в сфере защиты персональных данных / В.Е. Лямчев // Инновации. Наука. Образование. — 2021. — № 32. — С. 104–109. — EDN JWTEEZ.

Sirotskiy Alexei Alexandrovich

Moscow State University of Civil Engineering (National Research University), Moscow, Russia

E-mail: hotwater2009@yandex.ru

ORCID: <https://orcid.org/0000-0002-9343-7185>

RSCI: https://www.elibrary.ru/author_profile.asp?id=525833

Development and implementation of a remote practice-oriented professional development program for personal data protection specialists

Abstract. The article discusses the task of creating a distance training program aimed at the formation of practical skills for advanced training of specialists in the field of personal data protection. It is noted that at present, specialists with competencies in this area are in demand in the labor market, and the corresponding training programs are relevant.

Methods of research and development of a curriculum are described, characterized by content saturation as possible for remote format and direct interactive forms of interaction between a teacher and students. A structural logical model of the program, the composition of the labor functions of the graduate of the program, a description of the improved competencies, as well as examples of individual elements of its content part, including video lectures, webinars, test tasks and practical work, are presented. As a result of research, the minimum necessary studied base is identified and described, the development of which is required to form the necessary knowledge and skills. As examples, the components of the studied base are given.

The content and logic of constructing a practical task consisting of 30 actions are disclosed, and the implementation of the first action is described in detail, which is a multifactorial analysis of the organization's environment with the identification and determination of characteristics that directly affect decisions made when creating personal data protection systems.

There are also real fragments of illustrative material from lectures and webinars and examples of verified test questions that do not allow ambiguities in interpretations when choosing the correct answer options.

The given scheme of certification measures, including intermediate and final certifications both in practical and theoretical terms, in practice trained by several hundred students, showed its effectiveness and expediency.

The modular structure of the program components, based on the principles of decomposition, has high adaptive flexibility and can be adapted, adjusted, updated and supplemented in accordance to the dynamics of changes in the legislation on personal data and the by-law regulatory framework.

Keywords: advanced training; distance learning; personal data; operator; information security; practical skills; specialists; model