Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»

ДОПОЛНИТЕЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА «ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ НА ПРЕДПРИЯТИИ»

Выпускная квалификационная работа
по направлению подготовки 44.03.04 Профессиональное обучение
(по отраслям)
профилю подготовки «Информатика и вычислительная техника»
профилизации «Информационная безопасность»

Идентификационный номер ВКР: 562

Екатеринбург 2019

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»
Институт инженерно-педагогического образования
Кафедра информационных систем и технологий

К ЗАЩИТЕ ДОПУСКАЮ
Заведующий кафедрой ИС
_____ И. А. Суслова
«____« _____ 2019 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

ДОПОЛНИТЕЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА «ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ НА ПРЕДПРИЯТИИ»

Исполнитель:
обучающаяся группы № ЗИБ–501 А. В. Олькова
Руководитель:
старший преподаватель А. Г. Окуловская
Нормоконтролер: С. Ю. Ярина

Екатеринбург 2019

АННОТАЦИЯ

Выпускная квалификационная работа состоит из электронного учебного пособия «Защита персональных данных на предприятии» и пояснительной записки на 59 страницах, содержащей 16 рисунков, 7 таблиц, 31 источник литературы и 1 приложение.

Ключевые слова: ДОПОЛНИТЕЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА, ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ, ЭЛЕКТРОННОЕ УЧЕБНОЕ ПОСОБИЕ.

Олькова, А. В., Дополнительная образовательная программа «Защита персональных данных на предприятии»**:** выпускная квалификационная работа / А. В. Олькова; Рос. гос. проф.-пед. ун-т, Ин-т инж.-пед. образования, Каф. информ. систем и технологий. — Екатеринбург, 2019. — 59 с.

Объект исследования: процесс обучения по дополнительной профессиональной программе.

Предмет исследования: обучение и учебные материалы по курсу «Защита персональных данных на предприятии».

Целью работы является разработка дополнительной образовательной программы «Защита персональных данных на предприятии». Для достижения цели были проанализированы печатные и интернет источники по теме. На основе сотрудничества с заказчиком, были разработаны дополнительная образовательная программа, интерфейс и структура электронного учебного пособия. После интерфейс был наполнен блоками теории, практических заданий и итогового контроля.

Хоть в целом требования к защите персональных данных ужесточаются, но информация всё ещё подвергается утечке. Поэтому данное направление в наше время очень актуально.

СОДЕРЖАНИЕ

Введение 5
1 Анализ источников по курсу «Защита персональных данных на предприятии» 7
1.1 Характеристика учебного центра 7
1.2 Анализ печатных изданий по защите персональных данных на предприятии 12
1.3 Анализ интернет источников 16
1.4 Обзор курсов схожей тематики других компаний 17
1.5 Дополнительная образовательная программа «Защита персональных данных на предприятии» 19
2 Описание электронного учебного пособия «Защита персональных данных на предприятии» 25
2.1 Понятие электронного учебного пособия и требования, предъявляемые к нему 25
2.2 Назначение и структура электронного учебного пособия 27
2.3 Интерфейс электронного учебного пособия 29
2.4 Содержание электронного учебного пособия 36
2.4.1 Блок теории 36
2.4.2 Блок дополнительных источников информации 39
2.4.3 Блок практических заданий 40
2.4.4 Блок контроля знаний 44
2.5 Методические указания для использования электронного учебного пособия 49
2.5.1 Технические требования 49
2.5.2 Инструкция по использованию пособия для преподавателя 49
2.5.3 Инструкция по использованию пособия для обучающегося 50
Заключение 52

Список использованных источников 54
Приложение 58

ВВЕДЕНИЕ

Актуальность темы защиты персональных данных на предприятиях обусловлена тем, что каждый работник на каждом предприятии предоставляет свои персональные данные работодателю. Так же существуют права и свободы граждан, защищаемые государством. Такие как «Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени» — пункт 1 ст.23 гл.2 Конституции РФ, «Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются» — пункт 1 ст.24 гл.2 Конституции РФ.

Но с появлением новых технологий обработки информации, а так же с повышением ценности информации существуют существенные риски утечки персональных данных, использования их в корыстных целях.

По данным глобального исследования утечек конфиденциальной информации в I полугодии 2018 года от компании InfoWatch, 69% утечек информации приходится на персональные данные, в I полугодии 2017 года на утечку персональных данных приходится 65,5%, как мы видим, процент утечек персональных данных к общему числу утечек информации растет. Виновниками в 53,5% случаев становятся сотрудники предприятия.

Так как большая часть утечек персональных данных происходит при участии сотрудников предприятия, целесообразно, наряду со штрафами и мотивациями, ввести обучение сотрудников работе с персональными данными. В связи с этим, в Обществе с ограниченной ответственностью Учебно-экспертном центре «Концепция безопасности труда» уместно разработать новую дополнительную образовательную программу «Защита персональных данных на предприятии».

А одним из самых лучших способов повышения результативности обучения в современном мире является внедрение в образовательный про-

цесс электронного учебного пособия. Поэтому, разработка электронного учебного пособия по программе «Защита персональных данных на предприятии» становится особенно актуальной.

Объект исследования: процесс обучения по дополнительной профессиональной программе.

Предмет исследования: обучение и учебные материалы по курсу «Защита персональных данных на предприятии».

Цель работы: разработать дополнительную образовательную программу «Защита персональных данных на предприятии».

Для достижения цели необходимо выполнить следующие задачи:

1. Проанализировать материал по теме «Защита персональных данных на предприятии».
2. Разработать дополнительную образовательную программу «Защита персональных данных на предприятии»
3. Разработать структуру и интерфейс электронного учебного пособия по дополнительной образовательной программе «Защита персональных данных на предприятии».
4. Наполнить электронное учебное пособие.

1 АНАЛИЗ ИСТОЧНИКОВ ПО КУРСУ «ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ НА ПРЕДПРИЯТИИ»

1.1 Характеристика учебного центра

Общество с ограниченной ответственностью Учебно-экспертный центр «Концепция безопасности труда» создан в соответствии с действующим на территории Российской Федерации законодательством 06 марта 2018 года. Общество с ограниченной ответственностью действует на основании Устава. Место нахождения предприятия: г. Екатеринбург, ул. Машиностроителей, дом 29, офис 233.

Общество с ограниченной ответственностью Учебно-экспертный центр «Концепция безопасности труда» предоставляет услуги в области охраны труда, пожарной безопасности, промышленной безопасности, экологии. Также имеет подразделение «Учебный центр», который оказывает услуги по обучению сотрудников компаний по направлениям: охрана труда для руководителей и специалистов, пожарная безопасность, гражданская оборона и защита от чрезвычайных происшествий.

Учебно-экспертный центр имеет в своём распоряжении 3 кабинета. В одном находятся все работники центра: директор, менеджер по работе с клиентами, специалисты по охране труда, специалисты по пожарной безопасности, руководитель учебного направления, методисты и преподаватели.

Два других кабинета это аудитории учебного центра. Первая аудитория вмещает группу до 14 человек. Для размещения такой группы, аудитории оснащена следующим:

- 7 парт;
- 14 стульев;
- магнитно-маркерная доска, размером 120 см х 90 см;

- подключаемый к компьютеру преподавателя, телевизор с диагональю 40 дюймов;
- рабочее место преподавателя: стол, кресло, персональный компьютер, канцелярские принадлежности;
- стеллажи со справочной литературой.

Вторая аудитория вмещает до 30 человек, можно частично увидеть, как она выглядит на фотографии (рисунок 1).

Рисунок 1 — Фотография аудитории учебного центра

У нее в оснащении:

- 15 парт разной высоты (для удобного размещения обучаемых разного роста);
- 30 стульев, также разной высоты;
- магнитно-маркерная доска, размером 180 см х 120 см;
- рабочее место преподавателя: стол, кресло, персональный компьютер, канцелярские принадлежности;

- проектор;
- персональные компьютеры для обучающихся в количестве 5 штук.

Так же в распоряжении учебного центра находятся планшеты Irbis HIT (TZ49) в количестве 10 шт. Ими могут пользоваться обучающиеся в любой из аудиторий.

Организационная структура предприятия показана на схеме ниже (Рисунок 2).

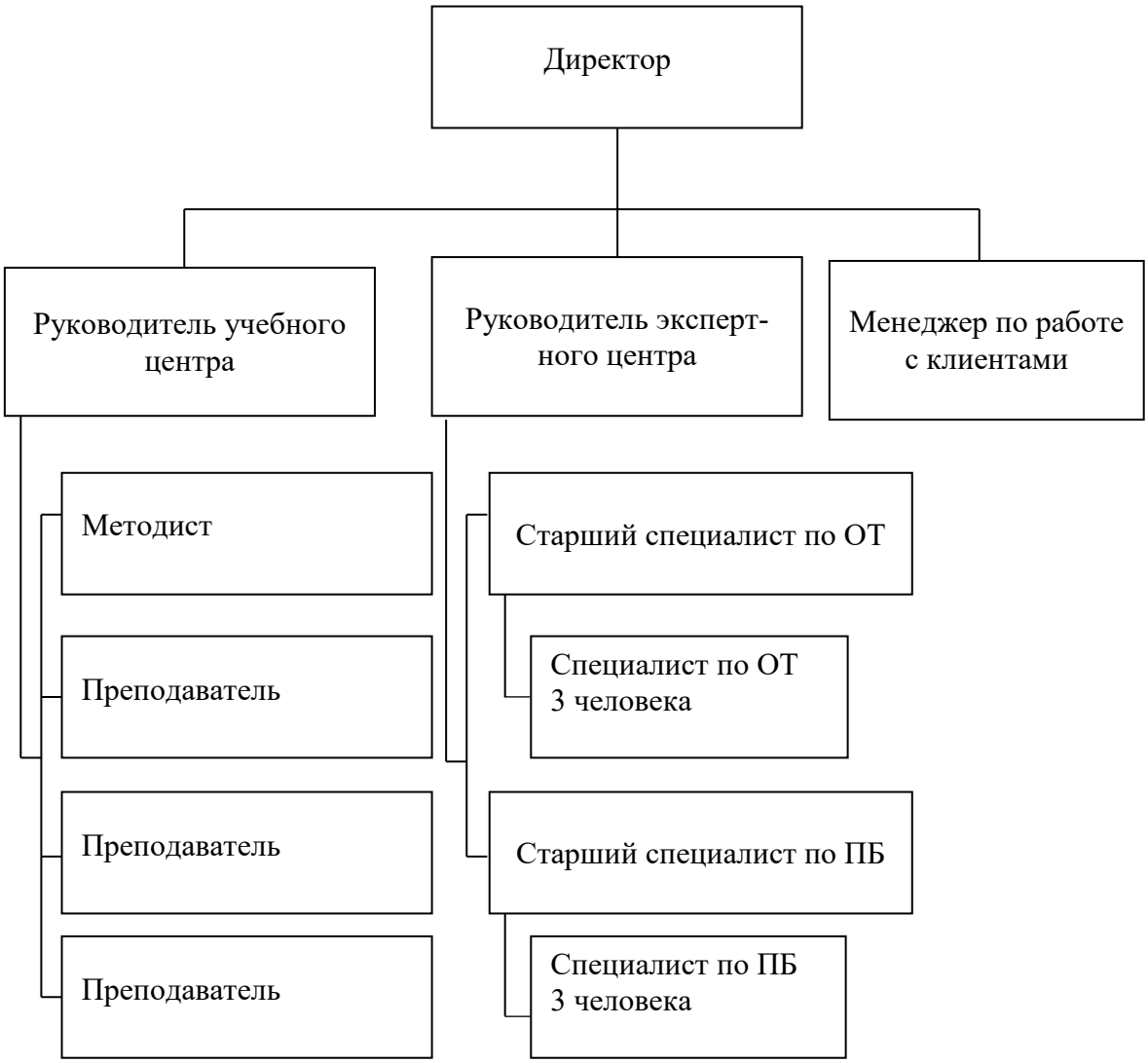

Рисунок 2 — Организационная структура Общества с ограниченной ответственностью Учебно-экспертного центра «Концепция безопасности труда»

Учебный центр реализует несколько рабочих программ дополнительного профессионального образования. Все они, так или иначе, связанны с безопасностью: охрана труда, пожарная безопасность, гражданская оборона и защита от чрезвычайных ситуаций. О чем и говорит название учебно-

экспертного центра «Концепция безопасности труда». Реализуемые программы, представлены в таблице ниже (Таблица 1):

Таблица 1 — Реализуемые программы в учебном центре

Наименование образовательной программы (направления подготовки специальности профессии)	Уровень (ступень) образования	Вид образовательной программы (основная, дополнительная)	Нормативный срок усвоения
Охрана труда для руководителей и специалистов организаций (Руководители, специалисты, ИТР)	профессиональное образование	дополнительная	40 часов
Охрана труда для руководителей и специалистов организаций (Члены аттестационных комиссий)	профессиональное образование	дополнительная	40 часов
Гражданская оборона и защита от чрезвычайных ситуаций для рабочих и служащих	Профессиональное образование	дополнительная	36 часов
Пожарно-технический минимум для ответственных лиц	Профессиональное образование	Дополнительная	18 часов

Учебный центр создан приказом №02-УЦ от 1 октября 2018 года. В приложении к приказу размещено положение об учебном центре ООО УЭЦ «Концепция безопасности труда».

Согласно положению, основная цель учебного центра – это управление учебной работой, методическим обеспечением, совершенствованием, модернизацией и оптимизацией образовательного процесса в учебно-экспертном центре.

Положение об учебном центре также определяет основные его задачи:

1. Повышение эффективности и качества образовательной деятельности учебного центра.

2. Разработка основ совершенствования и модернизации учебного процесса.

3. Обеспечение условий для реализации учебных программ, а также для внедрения новых образовательных технологий и средств обучения.

4. Разработка, внедрение и поддержание функционирования системы менеджмента качества, в соответствии образовательным стандартам.

5. Мониторинг новой информации по образовательным процессам.

6. Формирование баз данных обучающихся, контроль качества освоения программ.

7. Ведение документации, связанной с вопросами образовательной деятельности.

8. Учет материально-технического обеспечения учебного процесса.

Для реализации вышеизложенных задач, учебный центр выполняет следующие функции:

- планово-аналитическую;
- методическую.

В планово-аналитическую функцию входят следующие направления:

- формирование дополнительных профессиональных образовательных программ;
- определение планируемых образовательных результатов освоения программ;
- обновление существующих образовательных программ;
- разработка учебных планов, годового план-графика;
- составление расписания занятий, консультаций, итоговых аттестаций, семинаров;
- разработка требований к привлекаемому преподавательскому составу, контроль соблюдения требований;
- реализация мероприятий для эффективного функционирования системы менеджмента качества;
- разработка документов для прохождения процедур лицензирования, аккредитации.

Теперь обратим внимание на методическую функцию учебного центра:

- разработка структуры методической работы центра;
- разработка проектов нормативных локальных актов, которые регламентируют организацию, осуществление, контроль и анализ методической работы в учебном центре.

1.2 Анализ печатных изданий по защите персональных данных на предприятии

Рассмотрение защиты персональных данных на предприятии возможно произвести с разных сторон. Во-первых, со стороны нормативно-правовой базы. Есть множество документации регулирующей права субъектов персональных данных, а предприятия, в свою очередь, обязаны действовать только следуя этим правилам. Во-вторых, защита персональных данных на предприятии это комплекс организационно-технических мер. В-третьих, безопасность информации — это вопрос знаний персонала, как взаимодействовать с персональными данными, то есть вопрос инструктажей и обучения.

Общее определение персональных данных дано в ст. 3 закона о персональных данных. Согласно этой статье к персональным данным относится любая информация, прямо или косвенно относящаяся к определяемому или определенному физическому лицу (субъекту персональных данных).

Это может быть: имя, отчество, фамилия; место, год, месяц и день рождения вместе или отдельно взятые; адрес проживания или местонахождения; семейное или социальное положение; сведенья об имуществе; образование, профессия, доходы; контактная информация: личный номер телефона, электронная почта, личный блог; аудио- и видеофайлы и т. д.

Персональные данные как информацию (зафиксированную на любом материальном носителе) о конкретном человеке, которая отождествлена или может быть отождествлена с ним определяет Лушников А. М. в своей статье «Защита персональных данных работника: сравнительно-правовой комментарий гл.14 Трудового Кодекса РФ».

Лушников А. М. в своей другой статье «Неприкосновенность частной жизни и персональные данные в сфере трудовых отношений: стратегия правотворчества в контексте мирового опыта» [10] поднимает вопрос законотворчества в области защиты персональных данных в рамках трудовых отношений. Как есть коммерческая тайна, которую не может распространять работник, так и должна быть персональная профессиональная тайна конкретного работника, которую должен охранять работодатель.

В своих исследованиях Лушников А. М. отмечает основные положения стратегии в данной сфере:

1. Отнесение персональных данных к конфиденциальной информации, уточнение «конфиденциальной информации».

2. Российское законодательство в вопросах защиты персональных данных трудящихся должно соответствовать международным стандартам. Перенимать зарубежный опыт, а также подстраиваться на основе этого опыта под российские реалии.

3. Создание сбалансированной нормативной базы в вопросах охраны персональных данных в трудовых отношениях. Начиная Федеральным законом, продолжая главой в трудовом кодексе и заканчивая нормативными актами. А также создание типовых локальных нормативных актов.

В своей статье «К вопросу о защите персональных данных в сфере бизнеса» Эмиров М. Б. рассматривает проблемы защиты, сохранности и использования персональных данных в сфере бизнеса. А также даёт рекомендации по устранению данных проблем [30].

Наиболее значимыми проблемами в практике защиты персональных данных на предприятии Эмиров М. Б. выделяет следующие:

1. Что отнести к категории персональных данных.
2. Как защитить эти данные.
3. Как ими можно пользоваться в бизнес среде.
4. Кто и в какой форме несет ответственность за правонарушения, связанные с персональными данными.

Среди рекомендаций по решению данных проблем перечислены следующие меры:

- совершенствование механизмов защиты персональных данных, то есть контроля со стороны федеральных и региональных органов власти;
- информирование населения о его правах, методах их защиты;
- конкретное определение обязанностей операторов персональных данных.

В «Вестнике научного общества студентов, аспирантов и молодых ученых» Шерпетис Е. И. в своей работе «Угрозы безопасности персональных данных в учреждении» [28] даёт широкую и чёткую классификацию угроз, которым подвержены персональные данные на любом предприятии.

Все угрозы безопасности персональных данных он разделяет на:

1. Угрозы утечки по техническим каналам. Утечка может быть акустической (речь), видовой (просмотр) и ПЭМИН (Побочные Электро-Магнитные Излучения и Наводки).
2. Угрозы несанкционированного доступа. Несанкционированный доступ может привести к нарушению конфиденциальности, целостности и доступности.
3. Угрозы уничтожения, хищения аппаратных средств путём физического доступа.
4. Угрозы хищения, несанкционированной модификации и блокировки информации. Действие вредоносных программ, не декларированных возможностей системного ПО и ПО для обработки персональных данных.
5. Угрозы непреднамеренных действий пользователей.
6. Угрозы преднамеренных действий пользователей.
7. Угрозы несанкционированного доступа по каналам связи. Атаки с использованием протоколов межсетевого взаимодействия.

В этой работе очень широко и ёмко рассмотрены угрозы безопасности персональных данных на предприятии.

Для того чтобы устранить возникшие угрозы безопасности персональных данных в учреждении необходимо провести ряд организационно-технических мер, а именно:

- ввести пропускной режим в учреждение;
- защитить помещение в соответствии с СТР-к;
- проинструктировать пользователей ИСПДн о порядке работы с персональными данными;
- подключить источники бесперебойного питания;
- осуществить резервное копирование» [28].

Так как данная работа, направленная на исследование вопроса защиты персональных данных на любых предприятиях целесообразно упомянуть об учебном пособии «Защита персональных данных в организациях здравоохранения» А. Г. Сабанова [18].

В данном учебном пособии рассмотрены такие основные положения:

- требования, предъявляемые к защите персональных данных;
- подготовительные этапы по защите персональных данных: выявление потоков информации, определение и организация мероприятий по защите персональных данных;
- формирование перечня угроз, определение уровня защищенности, определение опасности и реализуемости угроз;
- построение системы защиты персональных данных.

Жукова В. В. в «Вестнике научного общества студентов, аспирантов и молодых ученых» в своей статье «Обеспечение защиты персональных данных в информационных системах» утверждает: «Основной задачей обеспечения безопасности персональных данных при их обработке в информационных системах является предотвращение утечки персональных данных по техническим каналам, несанкционированного доступа к ним, предупреждение преднамеренных программно-технических воздействий с целью их разрушения (уничтожения) или искажения в процессе обработки, передачи и хранения». В ходе своего исследования она так же установила, что: «без-

опасность персональных данных при обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные и технические меры защиты» [3].

1.3 Анализ интернет источников

Алексей Парфентьев, автор статьи «Обзор методов защиты корпоративной информации», опубликованной в интернет-журнале «Information Security/ Информационная безопасность» №5, 2017, считает, что: «Защита конфиденциальной информации — цикличный процесс, который в большей степени зависит от организационных, а не технических методов. Обучение пользователей правилам информационной безопасности, мониторинг и разграничение прав доступа, шифрование данных, внедрение DLP-системы — все перечисленные методы обеспечивают надежную защиту только при разумном и комплексном подходе. Грамотное сочетание основных методов способно многократно увеличить безопасность корпоративных данных и не допустить саму возможность случайных утечек данных или намеренного разглашения конфиденциальной информации» [12].

К. Саматов в своей статье «Комплексная защита информации ограниченного доступа в корпоративных информационных системах» выделяет следующие меры защиты персональных данных:

1. Организационные (организационно-юридические). Подготовка организационно-распорядительной документации по вопросам защиты информации: инструкции, регламенты, приказы, методические указания.
2. Технические меры:
    - инженерно-техническая защита;
    - защита от несанкционированного доступа к информации;
    - защита от утечек по техническим каналам;
    - криптографическая защита информации.

3. Морально-этические меры. Обучение и воспитание внутренних пользователей.

Также К. Саматов сообщает: «Еще одним трендом в вопросе кадровой безопасности, появившимся буквально несколько месяцев назад, являются системы мониторинга и выявления отклоняющегося от нормы поведения пользователей — User and Entity Behavior Analytics (UEBA). Данные системы предназначены для анализа поведения пользователей и выявления на его основе актуальных угроз кадровой и информационной безопасности» [8].

В общем и целом, тема защиты персональных данных на предприятии очень актуальна. Вопрос обучения работников стоит остро.

1.4 Обзор курсов схожей тематики других компаний

Для разработки конкурентоспособной, отвечающей запросам рынка и, действительно, полезной для повышения квалификации дополнительной образовательной программы «Защита персональных данных на предприятии», сравним курсы схожей тематике сторонних организаций, учебных центров и высших учебных заведений, осуществляющих обучение специалистов и руководителей по дополнительным образовательным программам.

Сравнение проведем по следующим критериям:

1. Название курса.
2. Сокращенное название организации.
3. Форма обучения.
4. Срок обучения.
5. Количество часов, приходящихся на лекционные занятия.
6. Количество часов, приходящихся на практические занятия.
7. Форма контроля знаний.

Для удобства восприятия информации и сравнения данные сформированы в таблицу 2.

Таблица 2 — Сравнительная таблица курсов по защите персональных данных на предприятии

№ п/п	Название курса	Сокращенное название организации	Форма обучения	Срок обучения	Количество часов		Форма контроля полученных знаний.
					Лекционные занятия	Практические занятия	
1	Обеспечение безопасности персональных данных на предприятии	НОУ ДПО «ЦПР»	очная	5 рабочих дней, 40 часов	26	12	Зачет без оценки (устный опрос)
2	Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных	Академия АйТи	очная дистанционная	9 рабочих дней / 72 часа	40	28	Зачет без оценки (тестирование)
3	Защита информационных систем обработки персональных данных	ВНИИПВТИ	очная дистанционная	5 рабочих дней / 40 часов	28	10	Зачет без оценки (тестирование)
4	Защита персональных данных	НГУ	очно	5 рабочих дней / 40 часов	12	28	Тест по курсу
5	Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных	ФГБОУ ВО «ТУСУР»	Заочно, с использованием дистанционных образовательных технологий	2 месяца / 72 часа	40	28	Тест

Из таблицы ясно, что более половины предприятий стараются курс по данной тематике сузить до 40 часов в одну рабочую пятидневную неделю. С одной стороны, это может говорить о «выжимке» воды из курса, узкой, но «глубокой» специализации. Но и может означать, что темы курса будут пройдены «поверхностно», без углубления, или будут рассмотрено мало нюансов по данной тематике обучения.

Так же, из сравнительной таблицы видно, что предпочтение в итоговом контроле отдают тестированию. В случае качественной разработки, апробирования, корректировки теста, это серьезный, пригодный инструмент для измерения полученных знаний, усвояемости конкретным слушателем курса, и усвояемости группой в целом. Но не стоит забывать о том, что зачастую тесты пишутся «на коленке». Такой продукт не способен дать реальную оценку знаниям, усвоенным человеком.

1.5 Дополнительная образовательная программа «Защита персональных данных на предприятии»

Проанализировав источники по теме «Защита персональных данных на предприятии», мы совместно с преподавателями учебного центра разработали дополнительную профессиональную программу «Защита персональных данных».

Дополнительная профессиональная программа «Защита персональных данных на предприятии» была утверждена директором ООО УЭЦ «Концепция безопасности труда» Симоновой Оксаной Владимировной 10 декабря 2018 года.

Рабочая программа курса состоит из 7-ми разделов:

1. Цели и задачи освоения рабочей программы.
2. Перечень планируемых результатов обучения по программе, соотнесенных с планируемыми результатами освоения программы.
3. Место программы в структуре дополнительного профессионального образования.
4. Объем программы и тематический план.
5. Содержание программы.
6. Методические рекомендации по реализации учебной программы.
7. Список основной литературы.

В пояснительной записке указано, что данная программа предполагает очную форму обучения, нормативный срок для освоения 72 часа, сам процесс обучения составляет 9 дней по 8 часов, включая все виды аудиторных и внеаудиторных (самостоятельных) работ.

Слушателями курса являются руководители и специалисты кадровых служб, отделов продаж и работы с контрагентами.

Также, говорится, что слушатели курса, в ходе освоения программы, изучают правовые и организационные основы обеспечения безопасности персональных данных, методы и процедуры выявления угроз безопасности персональных данных.

Формой итогового контроля являются тестовые задания.

В первом разделе «Цели и задачи освоения рабочей программы» рабочая программа курса ставит следующие цели: формирование знаний и навыков, необходимых для организации и обеспечения безопасности персональных данных, обрабатываемых в информационных системах.

Далее в этом разделе программы рассматриваются задачи для выполнения поставленной цели. К ним относятся следующие:

- изучение правовых и организационных основ обеспечения безопасности персональных данных в информационных системах персональных данных;
- изучение методов и процедур выявления угроз безопасности персональных данных в информационных системах персональных данных и оценки степени их опасности;
- практическая отработка ведения и составления документации по обеспечению безопасности персональных данных.

Во втором разделе имеется перечень планируемых результатов по спискам «Быть ознакомлены», «Знать», «Уметь» и «Владеть». Таким образом, вследствие освоения программы, обучающиеся должны приобрести и улучшить следующие знания и умения:

- выявление потенциальных и реальных угроз информационной безопасности, умение выстраивать их в порядок по возможности реализации и возможной величине ущерба;
- осуществление организационно-правового обеспечения информационной безопасности на предприятии;
- организация работы коллектива предприятия с учетом требований защиты информации;
- совершенствование системы управления безопасностью конфиденциальной информации;
- изучение и обобщение опыта работы других учреждений, организаций и предприятий в области повышения эффективности защиты персональных данных;
- контроль эффективности реализации политики защиты персональных данных на предприятии;
- знание методов выявления угроз безопасности автоматизированных систем обработки персональных данных;
- знание методов технической защиты информации, методов формирование требования по защите информации, методов организации и управления деятельностью служб защиты персональных данных на предприятии;
- знание методик проверки защищенности объектов информатизации на соответствие требованиям нормативных документов;
- изучение технических каналов утечки информации, возможностей технических разведок, способов и средств защиты информации от утечки по техническим каналам, методов и средств контроля эффективности технической защиты информации;
- изучение принципов и методов противодействия несанкционированному информационному воздействию на вычислительные системы и си
-

стемы передачи информации, принципов организации информационных систем в соответствии с требованиями по защите информации.

В третьем разделе программы мы видим место программы в структуре образования. То есть это отсылка к нормативным актам, стандартам, по которым составлена данная программа. Программа была составлена в соответствии с нормативными актами в области информационной безопасности. За основу взяты документы, регламентирующие защиту персональных данных. При разработке выполнены требования к содержанию программы, утвержденные Приказом Министерства образования и науки РФ от 5 декабря 2013 г. № 1310 «Об утверждении Порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности».

В разделе «Объем программы и тематический план» рассматривается тематический план проводимых занятий и количество часов, отводимых на каждую тему, род занятий — лекция или практическое занятие (таблица 3).

Таблица 3 — Тематический план курса «Защита персональных данных на предприятии»

№ тем п/п	Наименование тем	Количество часов на курс подготовки			
		Всего	В том числе		
			Лекции (очно)	Практические занятия (очно)	Контроль
1	2	3	4	5	6
1	Общие положения по обеспечению безопасности персональных данных на предприятии	8	8		
2	Нормативная правовая база по обеспечению безопасности персональных данных	8	8		
3	Основные направления деятельности должностных лиц, отделов и служб предприятия по обеспечению безопасности персональных данных	9	5	4	
4	Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных	10	5	5	

Окончание таблицы 2

5	Обеспечение безопасности персональных данных при их обработке без использования средств автоматизации	10	5	5	
6	Методы и средства контроля безопасности персональных данных	11	6	5	
7	Изучение, подбор и расстановка кадров, принимающих участие в обеспечении безопасности персональных данных	12	6	6	
Зачет		4			4
Итого по программе		72	43	25	4

В разделе «Содержание программы» содержится подробное понятийное описание каждой темы.

В шестом разделе «Методические рекомендации по реализации учебной программы» подробно рассматривается процесс реализации программы. Рекомендуется использовать действующие нормативные, законодательные акты, документы национальной системы стандартов, нормативные документы Федеральной службы по техническому и экспортному надзору и Федеральной службы безопасности Российской Федерации. Также учебные пособия, иллюстративные материалы. В процессе аудиторной работы, а также при планировании самостоятельной работы слушателей курса применять компьютерные технологии.

Наиболее важные и сложные моменты, являющиеся теоретической основой, подаются слушателям в форме лекций. Во время лекций тему можно излагать с помощью проблемного метода, метода «Кейса», с привлечением слушателей для решения поставленной проблемы, задачи, ситуации.

Для практических заданий рекомендуются методические разработки, отвечающие следующим требованиям: ориентирование на предприятие, являющиеся работодателем слушателя, с учетом специфики ситуации на конкретных предприятиях, с различными моделями информационных систем персональных данных, с набором конкретных действий.

В качестве итогового контроля рекомендуется зачет с использованием компьютерных технологий методом тестирования.

В разделе со списком основной литературы прописаны основные материалы для освоения программы. Содержит в себе 32 пункта. Всё это регламенты, акты, законы, ГОСТы, Специальные требования, рекомендации в области защиты персональных данных.

Теперь, после разработки дополнительной образовательной программы «Защита персональных данных на предприятии», можно перейти к разработке учебного материала. Так как рекомендуется данную программу реализовывать с помощью компьютерных технологий, решено создать электронное учебное пособие «Защита персональных данных на предприятии».

2 ОПИСАНИЕ ЭЛЕКТРОННОГО УЧЕБНОГО ПОСОБИЯ «ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ НА ПРЕДПРИЯТИИ»

2.1 Понятие электронного учебного пособия и требования, предъявляемые к нему

В обучении широко используется такое средство как электронное учебное пособие. Электронное учебное пособие относят к разновидностям компьютерных средств обучения.

Компьютерное средство обучения (КСО) — это программное средство (программный комплекс) или программно-технический комплекс, предназначенный для решения определенных педагогических задач, имеющий предметное содержание и ориентированный на взаимодействие с обучаемыми [6].

Педагогические задачи, решаемые компьютерными средствами обучения:

1. Начальное ознакомление с предметной областью, освоение ее базовых понятий и концепций.
2. Базовая подготовка на разных уровнях глубины и детальности.
3. Выработка умений и навыков решения типовых практических задач в данной предметной области.
4. Выработка умений анализа и принятия решений в нестандартных (нетиповых) проблемных ситуациях.
5. Развитие способностей к определенным видам деятельности.
6. Проведение учебно-исследовательских экспериментов с моделями изучаемых объектов, процессов и среды деятельности.
7. Восстановление знаний, умений и навыков (для редко встречающихся ситуаций, задач и технологических операций).

8. Контроль и оценивание уровней знаний и умений [5].

Электронное учебное пособие может являться как программным средством представления информации, знаний, так и программным средством контроля полученных знаний. Это вытекает из того, что в электронном учебном пособии могут «соседствовать» лабораторные работы, лекции, тренажеры, интерактивное иллюстрирование тем, тестовые задания и много другое.

Построенный таким образом процесс познания материала, даёт возможность быстрого усвоения знаний, и такой же быстрый контроль понимания информации, полученных умений и навыков.

В литературе есть множество определений электронного учебного пособия. Приведу несколько из них:

Электронное учебное пособие (ЭУП) — это программно-методический обучающий комплекс, предназначенный для самостоятельного изучения студентом учебного материала по определенным дисциплинам [6].

Электронное учебное пособие (ЭУП) — это электронное учебное издание, частично или полностью заменяющее или дополняющее учебник и официально утвержденное в качестве данного вида издания [2].

Электронное учебное пособие — программно-методический комплекс, обеспечивающий возможность самостоятельно освоить учебный курс или его раздел. Соединяет в себе свойства обычного учебника, справочника, задачника и лабораторного практикума [5].

Таким образом, электронное учебное пособие — это современный программно-методический обучающий комплекс, ориентированный на самостоятельную работу студента, по изучению материала по определённой дисциплине, может дополнять или заменять учебник или другое учебное издание.

Со стороны студентов, электронное учебное пособие используется для таких моделей обучения, как изучение теоретической составляющей дисциплины, выполнение практических работ, самоконтроля получаемых знаний.

К достоинствам электронных учебных пособий можно отнести:

- приспособляемость графика обучения к возможностям студента;

- возможность обучаться в соответствии со своими возможностями и потребностями, то есть по собственному плану;
- независимость и объективность оценки полученных знаний;
- возможность дистанционной консультации с преподавателем;
- возможность использования мультимедийных и интерактивных элементов обучения;
- простое и быстрое обновление информации в пособии;
- низкие затраты на публикацию и распространение;
- возможность устанавливать связь, средствами ссылок на другие учебные пособия, литературу.

Основное же назначение электронного учебного пособия — это систематизация получаемых студентами знаний по изучаемой дисциплине.

В связи с этим, очень актуально создать электронное учебное пособие по курсу «Защита персональных данных на предприятии». Для этого нужно определиться с назначением, применением и структурой пособия.

2.2 Назначение и структура электронного учебного пособия

Электронное учебное пособие по курсу «Защита персональных данных на предприятии» по первоначальному замыслу создаётся для помощи преподавателю при проведении курса. Курс преподаётся исключительно очно. Группа набирается не более 12 человек, в среднем — 8 слушателей. Преподаватель выводит демонстрационные материалы на доску при помощи проектора. Так же планирует показ данного пособия. Во время очных занятий, слушатели пользуются планшетами, выдаваемыми преподавателем или своим личным устройством. Поэтому, желательно, чтобы пособие было мобильно, чтобы можно было пользоваться на большом количестве устройств.

Структура электронного учебного пособия должна соответствовать тематическому плану преподаваемого курса. Поэтому содержит блоки для 7

теоретических тем и 4 практических заданий, а для контроля используются тестовые задания.

Блок для раскрытия теоретического материала содержит темы:

1. Общие положения по обеспечению безопасности персональных данных на предприятии.

2. Нормативная правовая база по обеспечению безопасности персональных данных.

3. Основные направления деятельности должностных лиц, отделов и служб предприятия по обеспечению безопасности персональных данных.

4. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных.

5. Обеспечение безопасности персональных данных при их обработке без использования средств автоматизации.

6. Методы и средства контроля безопасности персональных данных.

7. Изучение, подбор и расстановка кадров, принимающих участие в обеспечении безопасности персональных данных.

Блок для практических заданий содержит следующие темы:

1. Типовые формы журналов по защите персональных данных на предприятии.

2. Определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

3. Определение уровня защищенности персональных данных.

4. Определение состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах.

Итоговый контроль представлен в виде двух ступеней:

1. Перечень тестовых заданий, отражающих усвоение студентами знаний по курсу «Защита персональных данных на предприятии»

2. Проект пакета локальных актов, регулирующих обращение с персональными данными на предприятии слушателя курса.

Для наглядности, структуру электронного учебного пособия можно изобразить в виде схемы (рисунок 3).

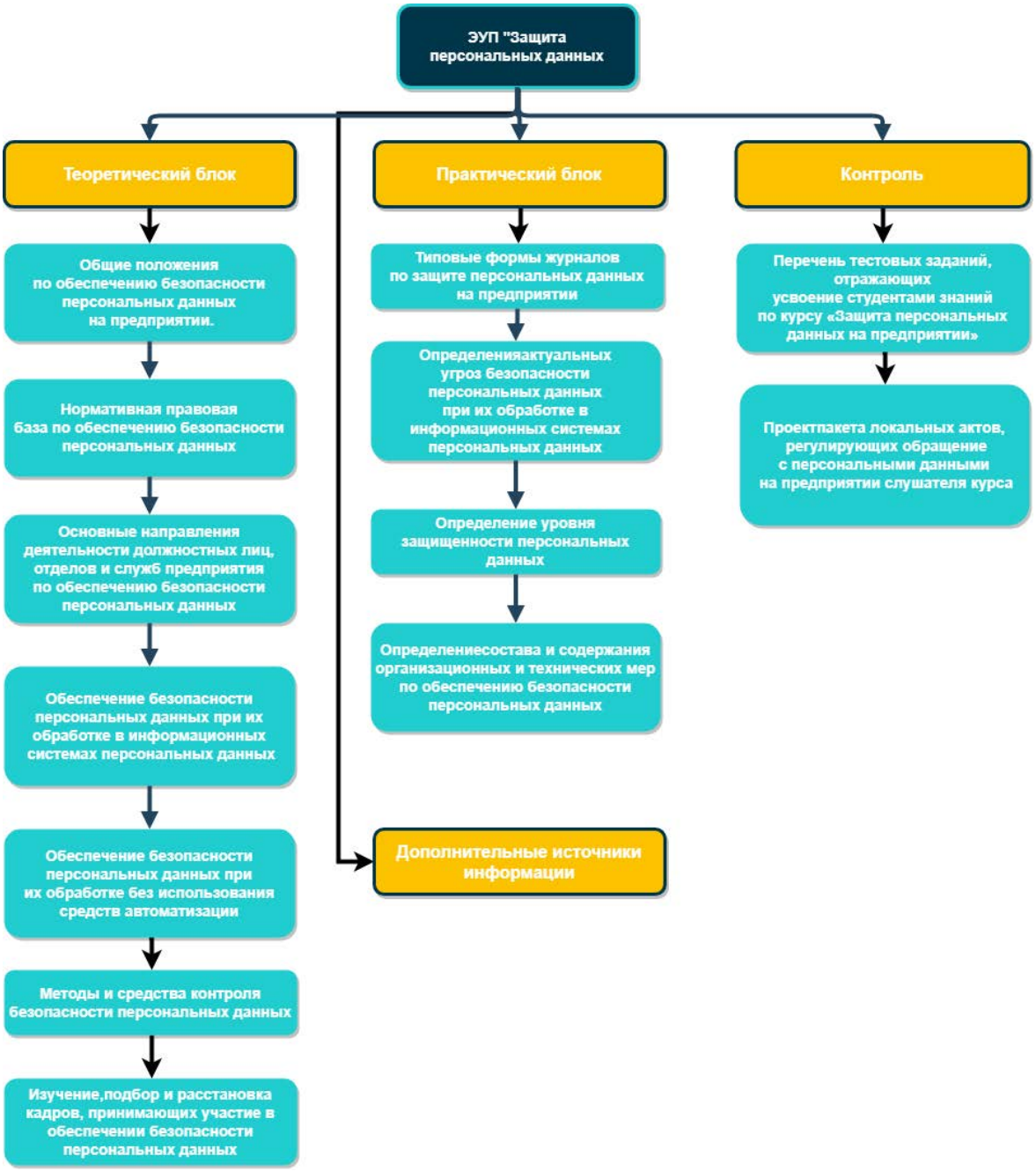

Рисунок 3 — Структура электронного учебного пособия

2.3 Интерфейс электронного учебного пособия

Электронное учебное пособие реализовано с использованием таких web-технологий как разметка гипертекста (HTML), каскадной таблицы стилей (CSS) и JavaScript.

Данные технологии можно представить, как слоёный торт (Рисунок 4).

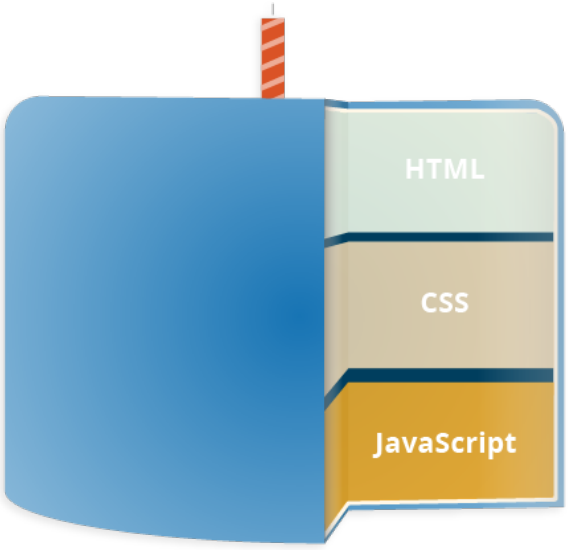

Рисунок 4 — Web-технологии

HTML — это язык разметки, который мы используем для визуального и смыслового структурирования нашего web-контента, например, определяем параграфы, заголовки, таблицы данных, или вставляем изображения и видео на страницу.

CSS — это язык стилей с помощью которого мы придаем стиль отображения нашего HTML контента, например, придаем цвет фону (background) и шрифту, придаем контенту многоколоночный вид.

JavaScript язык программирования, который позволяет Вам создать динамически обновляемый контент, управляет мультимедиа, анимирует изображения, впрочем, делает всё, что угодно.

Три слоя прекрасно выстраиваются друг над другом [30].

JavaScript в данном продукте используется для плавного появления объектов, привлекательного проявления заставки с названием электронного учебного пособия, для открытия и скрытия модальных окон.

Представлено пособие в виде Лендинг-пейдж или ещё называемой «посадочная страница». Лендинг-пейдж — это одностраничный сайт.

Цветовая гамма интерфейса состоит из следующих цветов:

- основной фон — белый;

- фон заставки — сине-зелёный (#00364A);
- элементы навигации, выделение основных понятий, шкала содержания — ярко бирюзовый (#20cdcf);
- ссылки и заголовок на заставке — оранжевый (#fcc200).

Выбор данных цветов обусловлен фирменным стилем Общества с ограниченной ответственность Учебно-экспертного центра «Концепция безопасности труда». Гамма фирменного стиля компании изображена ниже (Рисунок 5).

Рисунок 5 — Палитра цветов фирменного стиля

Для того, чтобы воспользоваться данным электронным учебным пособием, пользователю нужен любой браузер. И, так как, Google Chrome установлен как основной на всех компьютерах и девайсах учебного центра, разрабатывалось пособие именно под этот браузер. Но, так как слушатели могут приходить со своими девайсами, для их удобства, реализована возможность запуска из любого другого браузера. Главное, чтобы версия была как можно новее.

Именно поэтому электронное учебное пособие сделано в виде сайта. Чтобы быть доступным, практически, с любого устройства.

Для доступа к электронному учебному пособию, слушатель курса набирает в адресной строке браузера адрес размещенного на бесплатном хостинге пособия.

Так как учебный центр коммерческий, были озвучены пожелания, что у электронного учебного пособия должна быть презентативная открывающая заставка. Поэтому, при открытии сайта, первой появляется заставка, с большим, стильным заголовком (рисунок 6).

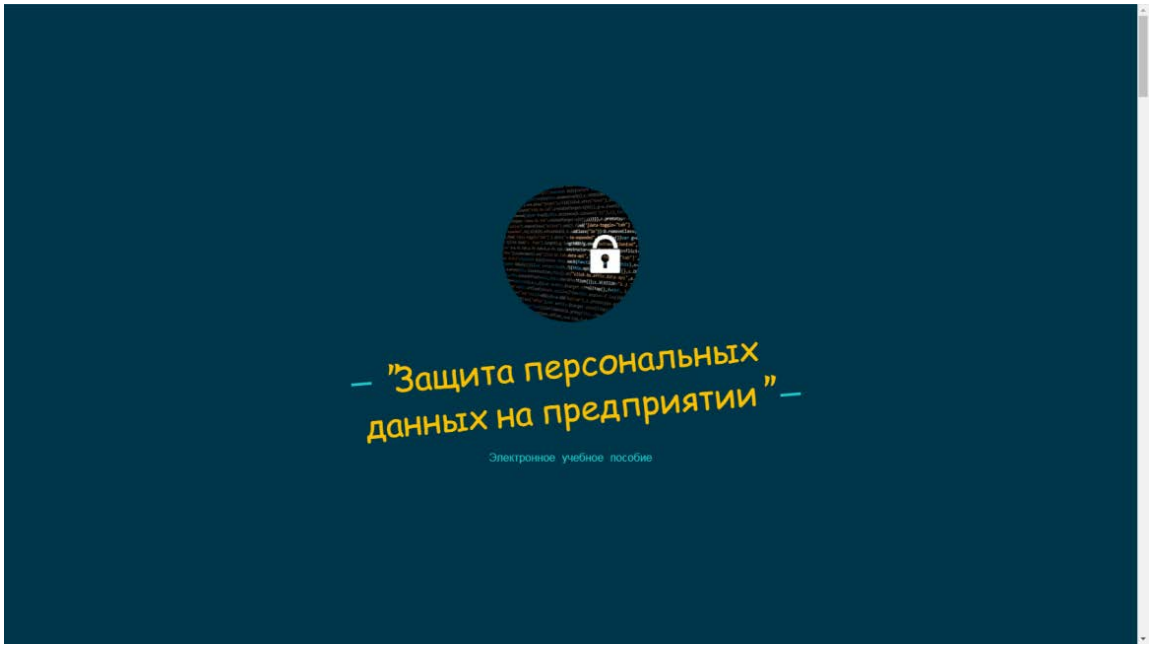

Рисунок 6 — Заставка с названием пособия

При прокручивании вниз, пользователю открывается следующий блок — приветствие (рисунок 7). Здесь кратко описывается, о чем данное электронное учебное пособие.

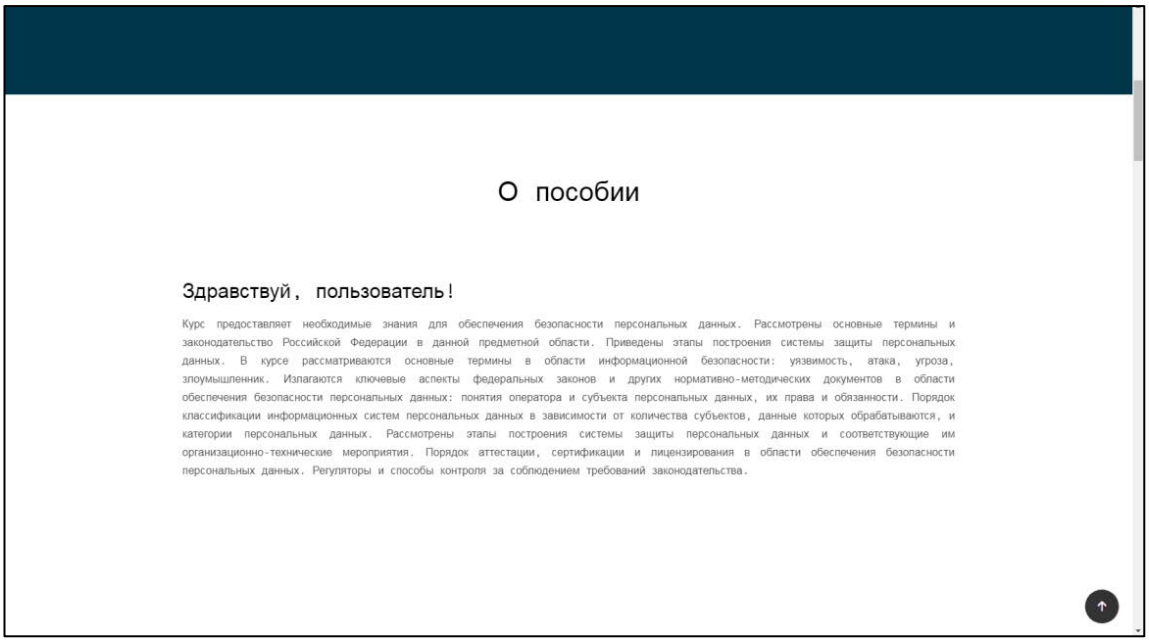

Рисунок 7 — Блок «Приветствие»

Далее пользователю открывается шкала, в которой по порядку располагаются блоки: теория (рисунок 8), дополнительные источники информации (рисунок 9), практические задания (рисунок 10) и контроль (рисунок 11). По бокам от шкалы расположены названия тем.

Хронологическая шкала даёт понять обучающемуся, сколько времени он затратит, примерно, на каждую тему или задание. Это удобно, тем, что слушатель курса сможет скорректировать свой график ознакомления с материалом. Засечь время на занятия.

В заголовках тем встроена кнопка, при нажатии на нее открывается модальное окно. Это реализовано с помощью JavaScript.

Рисунок 8 — Шкала — Содержание и блок «Теория»

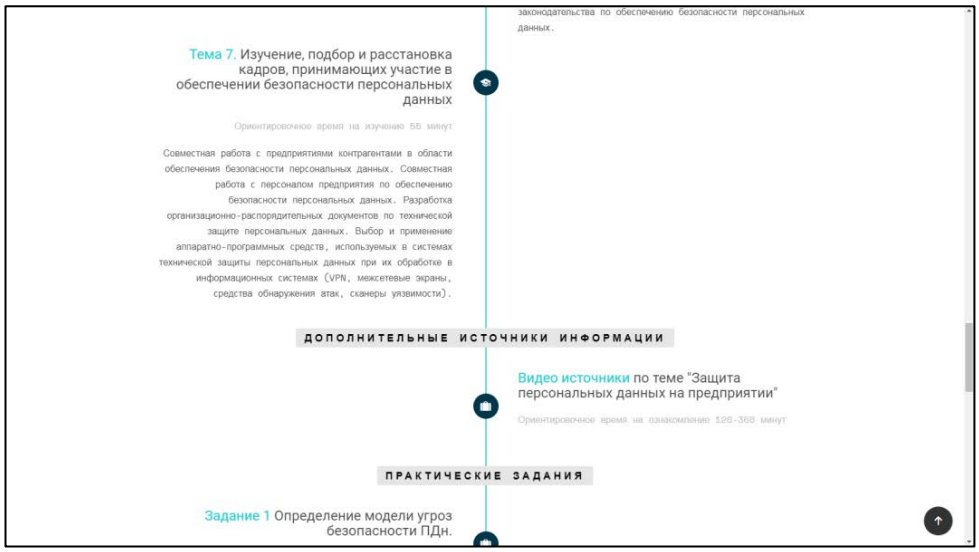

Рисунок 9 — Шкала с блоком «Дополнительные источники информации»

Рисунок 10 — Шкала с блоком «Практические задания»

Рисунок 11 — Шкала с блоком «Контроль»

В нижней части страницы, после прокрутки первой заставки появляется кружочек со стрелочкой «вверх», при нажатии прокручивает страницу на самый верх, он так же реализован с помощью JavaScript.

Как видно на рисунке 12, в верхней части модального окна распологается заголовок, якорные ссылки оранжевого цвета на разделы темы и крестик — кнопка закрытия модального окна.

В нижней же части есть ссылки на открытие предидущей и следующей темы, а так же выход к содержанию, то есть закрытие окна.

В самой большой части модального окна, в середине, находится основной контент, он сопровожден полосой прокрутки, основные понятия в контенте выделены ярко-бирюзовым цветом, как отметка «Тема 1» на скриншоте.

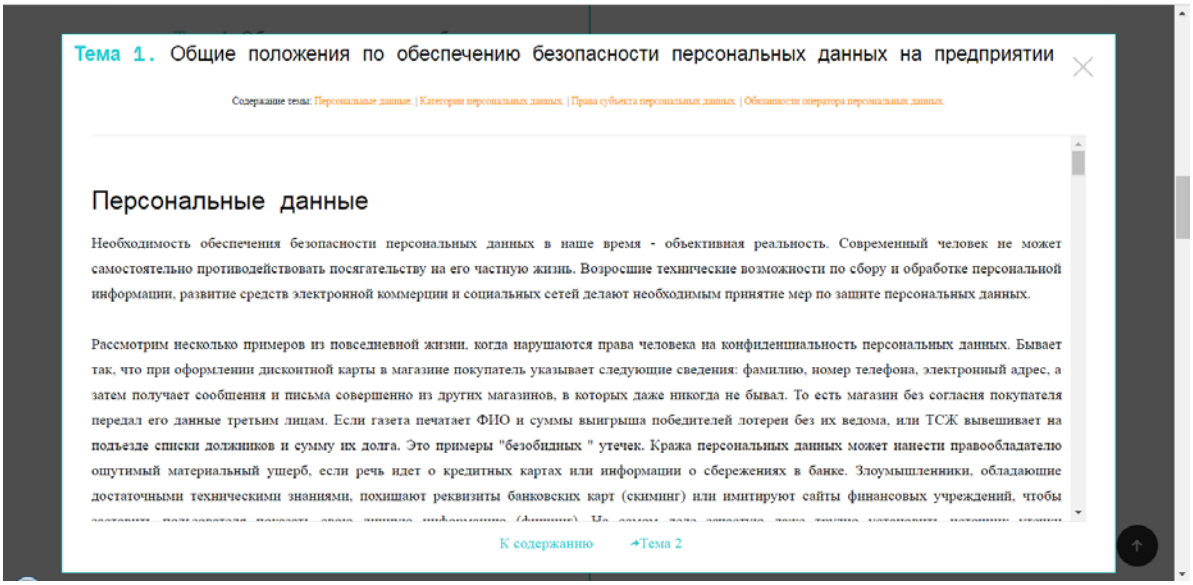

Рисунок 12 — Модальное окно

Итоговый контроль по курсу реализован с помощью тестовых заданий. Тестовые задания сформированы с помощью инструмента Google — Формы (Рисунок 13).

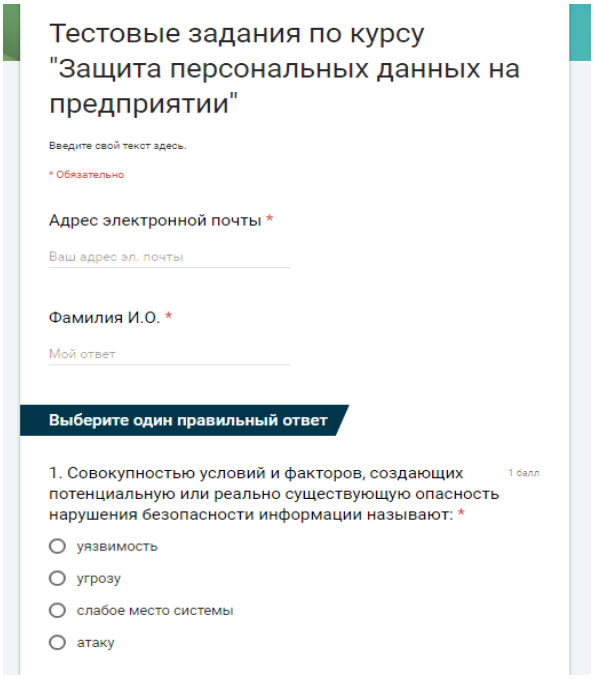

Рисунок 13 — Тестовые задания на Google формах.

То есть в названии «спрятанна» ссылка на форму с тестовыми заданиями. Google формы позволяют быстро и стильно оформить тестовые задания. Так же в них встроенна функция сохранения ответов в отдельный файл — что можно в дальнейшем оформлять как протокол итогового

контроля. Так же они (формы) могут дублировать ответы пользователя на его электронную почту, и сразу же дать информацию о результатах пройденного контроля. А для преподавателя становится возможным собрать статистику об усвояемости даваемых им материалов.

2.4 Содержание электронного учебного пособия

2.4.1 Блок теории

Блок теории составляют 7 тем по защите персональных данных на предприятии. Темы соответствуют тематическому плану рабочей программы по курсу. Предназначен теоретический блок для формирования знаний.

Тема №1. Общие положения по обеспечению безопасности персональных данных на предприятии.

В данной теме рассмотрены основные положения защиты персональных данных. В теме 4 раздела:

1. Персональные данные. В этом разделе представлены для изучения такие понятия, как «персональные данные», «оператор персональных данных», «обработка персональных данных», «информационная система персональных данных», «регуляторы».

2. Категории персональных данных. В этом разделе рассматриваются две категоризации персональных данных. Категории персональных данных по Федеральному закону «О персональных данных»: общедоступные, специальные, биометрические. Категории персональных данных по совместному приказу ФСТЭК, ФСБ и Министерства информационных технологий и связи РФ от 13 февраля 2008 года N 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»: 1 категория, 2 категория, 3 категория, 4 категорий.

3. Права субъекта персональных данных. Кто такой «субъект персональных данных». Рассмотрение основных его прав по Федеральному закону № 152 «О персональных данных».

4. Обязанности оператора персональных данных. Рассмотрение основных обязанностей операторов по Федеральному закону №152 «О персональных данных». Контроль со стороны Роскомнадзор, ФСБ и ФСТЭК.

Тема №2. Нормативная правовая база по обеспечению безопасности персональных данных.

В этой теме содержатся 3 раздела:

1. Нормативные акты в области персональных данных. Перечень основных регулирующих правовых и нормативных актов со ссылками на их текст в системе «Гарант».

2. Основные положения. Рассмотрены основные положения актов перечисленных в 1 разделе этой темы.

3. Ответственность за нарушение требований законодательства по обеспечению безопасности персональных данных. Административная ответственность: нарушения и наказания. Уголовная ответственность: типовые нарушения и наказания.

Тема №3. Основные направления деятельности должностных лиц, отделов и служб предприятия по обеспечению безопасности персональных данных.

Три раздела:

1. Цели системы защиты информации. Рассмотрены цели системы защиты. Принципы её применения, алгоритм создания, выполняемые задачи.

2. Должностные лица, отдела и службы. Руководитель системы защиты информации, его цели и задачи. Подразделения: программно-аппаратной защиты, инженерно-технической защиты, конфиденциального делопроизводства. Задачи подразделений. Требования к специалистам.

3. Нормативные акты на предприятии. Перечень необходимых локальных нормативных документов.

Тема №4. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных.

Включает в себя 4 раздела:

1. Особенности обеспечения безопасности персональных данных в автоматизированных системах. Классификация автоматизированных систем. Классы защищенности. Обеспечение безопасности в автоматизированных рабочих местах (АРМ) на базе автономных ПЭВМ при использовании съемных накопителей большой емкости. Обеспечение безопасности в локальных вычислительных сетях. Обеспечение безопасности при межсетевом взаимодействии.

2. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных. Обезличивание персональных данных. Информационная система персональных данных.

3. Мероприятия по обеспечению безопасности персональных данных при их обработке в ИСПДн. Перечень необходимых мероприятий.

4. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Тема №5. Обеспечение безопасности персональных данных при их обработке без использования средств автоматизации.

Разделы:

1. Защита персональных данных в кадровой документации. Принципы защиты персональных данных работников организации.

2. Журнал учета персональных данных и порядок его ведения.

3. Хранение и уничтожение материальных носителей с информацией о персональных данных. Сроки хранения. Порядок уничтожения.

4. Порядок реализации мер по обеспечению безопасности персональных данных.

Тема №6. Методы и средства контроля безопасности персональных данных.

Включается в себя следующие разделы;

1. Методы и средства контроля защищенности информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН.

2. Методы и средства контроля защищенности акустической речевой информации от утечки по техническим каналам.

3. Методы и средства контроля защищенности информации от несанкционированного доступа.

4. Регуляторы в области защиты персональных данных.

Тема №7. Организационные и технические меры защиты персональных данных.

Посвящено этой теме 2 раздела:

1. Разработка организационно-распорядительных документов по технической защите персональных данных.

2. Выбор и применение аппаратно-программных средств, используемых в системах технической защиты персональных данных при их обработке в информационных системах.

2.4.2 Блок дополнительных источников информации

В блоке дополнительных источников информации размещены видеоплееры с роликами из сервиса YouTube с записанными вебинарами от компаний, специализирующимися на информационной безопасности. Преподаватели, которые ведут данный курс, рекомендуют их к просмотру. Поэтому, для удобства преподавателей и слушателей курса, данные вебинары встроены в блок.

1. Вебинар «Защита персональных данных на социальном предприятии». Спикеры — специалисты компании «Дебевойз энд Плимптон». Эксперты рассказывают:

- о требованиях к сбору и обработке персональных данных;
- об особенностях сбора персональных данных через Интернет;

- о правах и обязанностях субъектов и операторов персональных данных;
- о нарушениях при обработке правовых персональных данных;
- о том, какая ответственность может за это наступить.

2. Вебинар «Персональные данные: что год грядущий нам готовит?» от Академия АйТи. Спикер Семенихин Игорь Викторович.

Прослушав вебинар, вы сможете:

- ознакомиться с перспективами нормативного правового и методического регулирования в области организации обработки и обеспечения безопасности персональных данных;
- получить подробную, пошаговую инструкцию, что и как правильно сделать в организации для реального обеспечения безопасности персональных данных и успешного прохождения проверок Роскомнадзора, ФСТЭК и ФСБ России;
- получить представление об обязательности требований нормативных правовых актов, руководящих и методических документов по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;
- ознакомиться с основными методами и способами решения проблем, возникающих у специалистов ИБ;
- уйти от частного и взглянуть на проблему организации безопасности персональных данных со стороны;
- ознакомиться с квалификационными требованиями к персоналу, занимающемуся вопросами организации обработки и обеспечения безопасности персональных данных.

2.4.3 Блок практических заданий

Блок практических заданий направлен на получение и улучшение навыков.

Практическое задание №1. Типовые формы журналов по защите персональных данных. Цель практического задания: научиться работать с нормативными документами по защите персональных данных.

Содержание: Коллективно восстановить типовые формы журналов по защите персональных данных. Для восстановления пользоваться нормативными документами.

Ход работы следующий: группа делится на подгруппы и каждой подгруппе выделяется одна из форм для заполнения. Каждый участник должен внести изменения в документ. Суть в том, что, скорее всего они не просто заполнят формы, но и сделают ошибки друг у друга. И вот так наглядно, поймут, что информации нужна защита.

Для работы нужно перейти по ссылке к файлу с общим доступом и заполнить его. Для заполнения предлагаются 4 формы типовых журналов: журнала учета установленных средств защиты информации (таблица 4), журнала учета машинных носителей информации (таблица 5), журнала учета пользователей, допущенных к информационным системам персональных данных (таблица 6), журнала проверок электронных журналов (таблица 7).

Таблица 4 — Форма журнала учета установленных средств защиты информации

№ п/п	Наименование средства защиты информации	Серийный (заводской) номер	Номер специального защитного знака	Место установки СЗИ	Организация, установившая СЗИ Ф.И.О. установившего СЗИ, дата, подпись	Отметка об изъятии СЗИ: Ф.И.О. производившего изъятие СЗИ, дата, подпись	Примечание
1	2	3	4	5	6	7	8
	Ввести пример заполнения	Ввести пример заполнения	Ввести пример заполнения	Ввести пример заполнения	Ввести пример заполнения	Ввести пример заполнения	Ввести пример заполнения

Таблица 5 — Форма журнала учета машинных носителей информации

№ п/п	Регистрационный (учетный) номер носителя	Вид носителя	Тип носителя и его емкость	Дата поступ ступления	Расписка в получении (ФИО, подпись, дата)	Расписка в обратном приеме (ФИО, подпись, дата)	Место хранения	Дата и номер акта об уничтожении	Примечание
1	2	3	4	5	6	7	8	9	10
	Ввести пример заполнения	Ввести пример заполполнения	Ввести пример заполнения	Ввести пример заполнения	Ввести пример заполнения	Ввести пример заполнения	Ввести пример заполнения	Ввести пример заполнения	Ввести пример заполнения

Таблица 6 — Форма журнала учета пользователей, допущенных к информационным системам персональных данных

№ п/п	Дата	Фамилия, имя, отчество пользователя	Наименование ИСПДн	Вписать заголовок столбца	Вписать заголовок столбца	Вписать заголовок столбца
1	2	3	4	5	6	7
	Ввести пример заполнения	Ввести пример заполнения	Ввести пример заполнения	Ввести пример заполнения	Ввести пример заполнения	Ввести пример заполнения

Таблица 7 — Форма журнала проверок электронных журналов

№ п/п	Дата проверки	Вписать заголовок столбца	Наименование проверяемого журнала	Вписать заголовок столбца	Подпись администратора безопасности	Примечание
1	2	3	4	5	6	7
	21.01.2018 …. ….	Ввести пример заполнения	Ввести пример заполнения	Ввести пример заполнения	Ввести пример заполнения	Ввести пример заполнения

Практическое задание №2. Определения перечня угроз безопасности персональных данных при их обработке в информационных системах.

Целью практического занятия является теоретическая и практическая подготовка слушателей в области изучения задач определения модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, научиться работать с нормативными документами по защите персональных данных.

Данное практическое задание предполагает использование документа «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России 15.02.2008 г. ДСП». На основе этого документа слушателю необходимо составить модель нарушителя и модель угроз безопасности персональных данных непосредственно с условиями и ситуацией на своем предприятии. Пошагово заполняются таблицы из документа.

Практическое задание №3. Определение уровня защищенности персональных данных.

Цель задания: изучение проблемы определения уровня защищенности персональных данных.

Задание предполагает изучение и анализ документа Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 г. Москва «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Слушатели курса на практическом занятии выполняют следующее задание: изучают документ, определяют уровень защищенности персональных данных для своего собственного предприятия, на основе данных своего места работы.

Практическое задание №4. Определение состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах.

Цель занятия: изучение проблемы определения состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах, навыки анализа документов.

Во время практического занятия слушатели курса изучают, анализируют, учатся применять следующий документ, регулирующий защиту персональных данных: Приказ ФСТЭК России от 18.02.2013 № 21» Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

2.4.4 Блок контроля знаний

После того, как слушатели курса изучат все теоретические темы, ознакомятся с дополнительными источниками информации, выполнят практические задания, они должны пройти контроль полученных знаний. Это нужно, чтобы понять самому обучающемуся, а также преподавателю успешность освоения программы.

Блок контроля полученных знаний состоит из двух частей.

Первая часть — это итоговый контроль средством заданий в тестовой форме. Почему заданий в тестовой форме, а не тест? А потому, что эти два понятия очень четко разделяются.

Итак, педагогический тест — это система параллельных заданий равномерно возрастающей трудности, специфической формы, определенного содержания, создаваемая с целью аргументированной оценки уровня и структуры подготовленности обучаемых [7].

Задание в тестовой форме — это педагогическое средство, к которому предъявляются следующие требования:

- краткость;
- технологичность;

- правильность формы;
- логическая форма высказывания;
- одинаковость правил оценки ответов;
- наличие определенного места для ответов;
- правильность расположения элементов задания;
- одинаковость инструкции для всех испытуемых;
- адекватность инструкции форме и содержанию задания.

Состоит наш контроль из 28 заданий в тестовой форме.

Тестовые задания бывают открытой формы и закрытой.

Открытая форма тестового задания — это, когда обучающемуся не дают правильного ответа, а только оставляют место для ответа. Такие задания дают самую точную информацию о знаниях обучающегося, но очень сложны в конструировании и проверке.

Задания в открытой форме имеют следующую конструкцию: инструкция, формулировка задания, эталон ответа.

Пример тестового задания в открытой форме в нашем итоговом контроле (рисунок 14).

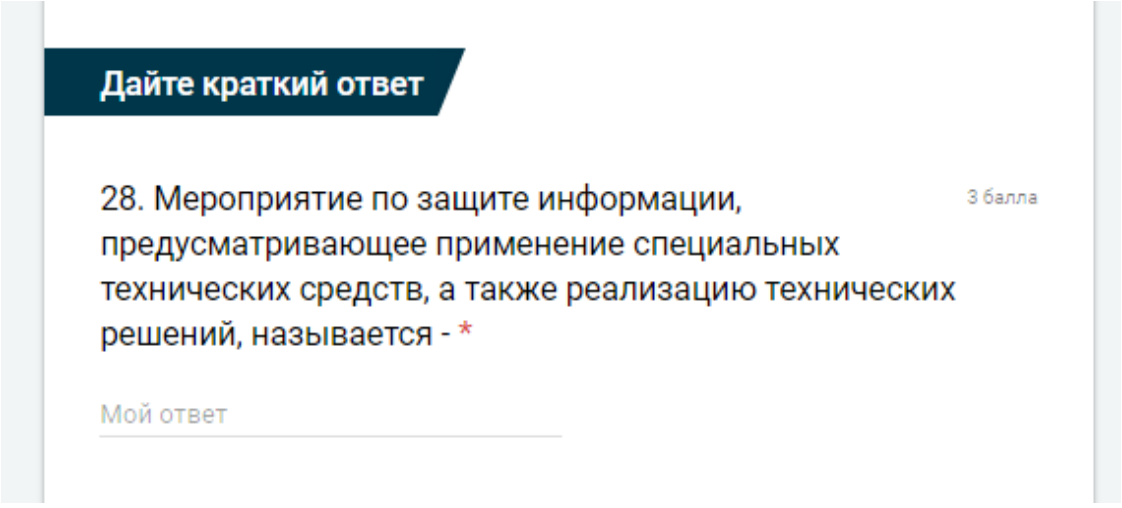

Рисунок 14 — Пример тестового задания открытой формы

Закрытая форма тестового задания — легко конструируются, быстро понимаются испытуемыми. Имеют следующую конструкцию: инструкция,

формулировка задания, варианты ответа, эталон. Задания в закрытой форме имеют разную внутреннюю конструкцию.

Пример задания с одним правильным ответом можно увидеть ниже (Рисунок 15).

Рисунок 15 — Задание с одним правильным ответом

Пример задания с несколькими возможными правильными ответами (Рисунок 16). Такие задания используются для проверки классификационных и номенклатурных знаний.

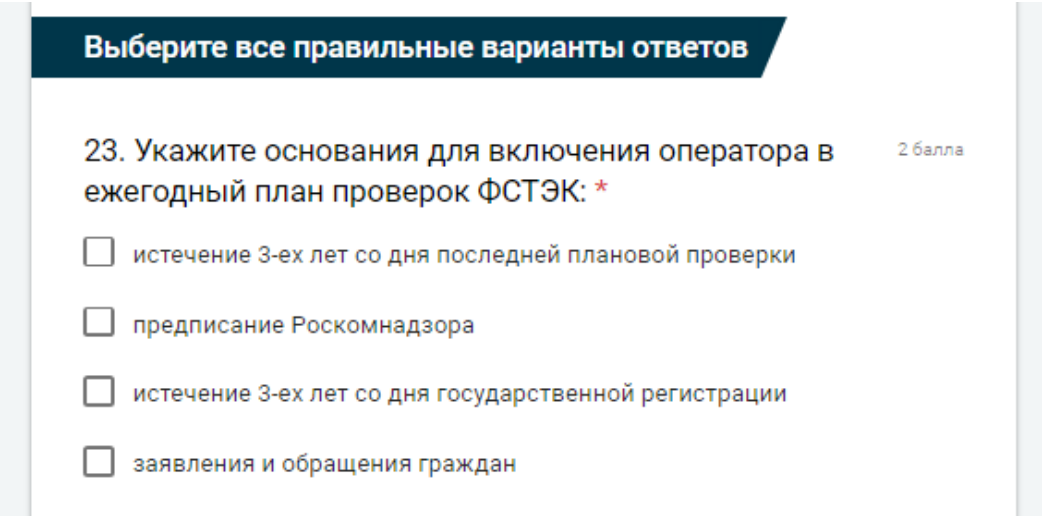

Рисунок 16 — Задание с множественным выбором

После успешного прохождения заданий в тестовой форме, обучающимся предстоит выполнить заключительный объемный проект.

Разработать пакет документов по защите персональных данных для своего собственного предприятия.

В пакет документов входят:

1. Положение по обработке персональных данных, включающее следующие формы:

- согласия субъекта на обработку персональных данных (ПД)
- уведомления оператора об обработке ПД
- поручения третьей стороне на обработку ПД
- акта уничтожения персональных данных
- уведомления о прекращении обработки и уничтожении ПД
- отзыва согласия субъекта на обработку персональных данных
- запроса субъекта на предоставление сведений об обработке ПД
- запроса субъекта на уточнение ПД
- уведомления субъекта об обработке персональных данных
- уведомления о внесении изменений в персональные данные
- уведомления о прекращении обработки персональных данных оператором и др.

2. Приказ об организации работ по защите персональных данных, содержащий сведения о назначении (утверждении):

- ответственного за обработку персональных данных в информационных системах персональных данных;
- ответственного за обеспечение функционирования средств защиты информации;
- списка лиц, допущенных к работе со средствами защиты информации;
- списка лиц, допущенных к работе с персональными данными, обрабатываемыми в информационной системе, для выполнения служебных (трудовых) обязанностей;

- списка помещений, в которых разрешается обработка персональных данных.

3. Политика обеспечения безопасности персональных данных.
4. Перечень персональных данных, обрабатываемых в ИСПДн.
5. Перечень защищаемых информационных ресурсов.
6. Акт классификации ИСПДн.
7. Инструкция по учёту носителей персональных данных.
8. Инструкция администратору ИСПДн.
9. Инструкция о порядке допуска лиц к информационным ресурсам ИСПДн.
10. Инструкция по внесению изменений в ИСПДн.
11. Инструкция по организации антивирусной защиты в ИСПДн.
12. Инструкция по организации парольной защиты.
13. Инструкция по резервному копированию и восстановлению персональных данных.
14. Инструкция пользователю ИСПДн.
15. Инструкция по использованию ресурсов сети Интернет.
16. Обязательство о неразглашении сведений.
17. План внутренних проверок состояния защиты персональных данных.
18. Заключение о возможности использования СЗИ.

Проверяется данный проект преподавателем, преподаватель после проверки даёт свои рекомендации по введению данного пакета документов в процессы предприятия.

2.5 Методические указания для использования электронного учебного пособия

2.5.1 Технические требования

Электронное учебное пособие предназначено для работы в аудитории. Так как теоретический материал имеет форму конспекта, основную информацию доводит преподаватель. А практические задания требуют консультаций с преподавателем и защиты проделанной работы.

Но всё-таки, пособие может быть использовано для самостоятельного изучения слушателями курса. Информация в теоретическом блоке достаточна для освоения тем, так же имеются рекомендуемые дополнительные источники информации. Практические задания также возможно сделать самостоятельно.

Требования к аппаратному обеспечению: разрешение экрана устройства не менее 1024 x 768;

Требования к программному обеспечению:

- веб-браузер с поддержкой веб-технологий HTML5, CSS3 (Internet Explorer (не ниже 9) Chrome, Firefox, Opera);
- доступ в глобальную сеть интернет.

2.5.2 Инструкция по использованию пособия для преподавателя

Для работы с данным электронным пособием, преподаватель должен обеспечить аудиторное занятие для группы. Убедитесь, что для каждого слушателя найдется устройство для работы с пособием. Либо это один из 4 компьютеров, либо планшет. Проверьте, что устройства имеют доступ к сети Интернет, иначе пособие не будет работать.

Допускается использованием слушателем курса собственного устройства. Для этого, предупредите слушателей о программных и аппаратных требованиях данного пособия.

Слушатели курса проходят блоки теории и практических заданий по рекомендованной последовательности. Конечно, пособие даёт возможность индивидуального пути изучения.

Прохождение курса очно, и следовательно, изучение пособия заканчивается итоговым контролем в виде заданий в тестовой форме. После проверки знаний, слушатели выполняют итоговый проект по подготовке пакета документов. Проект защищают в аудитории перед группой и преподавателем.

2.5.3 Инструкция по использованию пособия для обучающегося

Для работы с пособием:

1. Откройте браузер (Chrome, Internet Explorer (не ниже 9), Opera, Mozilla Firefox).
2. Введите адрес электронного учебного пособия.
3. Прокрутите вниз до шкалы с содержанием.
4. Выберите тему или задание.
5. В открывшемся окне изучите материал. Для навигации внутри темы используйте ссылки под заголовком.
6. Для общей навигацией по пособию пользуйтесь либо хронологической шкалой, либо кнопкой слева «Содержание» (выезжающее содержание с ссылками).
7. После изучения всего материала и выполнения заданий можете приступить к контролю знаний.
8. Для этого спуститесь к блоку «Контроль» и нажмите на «Тестовые задания по курсу». В открывшейся рядом вкладке, выполните задания. Обязательно впишите Ваши имя, фамилию, адрес электронной почты. После за-

полнения, нажмите «Отправить». Ответы на задания отправятся преподавателю, а копия Ваших ответов Вам.

9. После успешного выполнения заданий в тестовой форме, приступайте к выполнению проекта по разработке пакета документов по защите персональных данных на Вашем предприятии.

10. Защитите Ваш проект в аудитории.

11. Поздравляю: вы успешно закончили курс!

ЗАКЛЮЧЕНИЕ

Результатом выполнения выпускной квалификационной работы стали дополнительная образовательная программа «Защита персональных данных на предприятии» и электронное учебное пособие к ней. Разработана данная программа для Общества с ограниченной ответственностью учебно-экспертного центра «Концепция безопасности труда».

В процессе выполнения работы были проанализированы источники по теме защиты персональных данных на предприятии. На основе анализа разработана дополнительная образовательная программа «Защита персональных данных на предприятии». И электронное учебное пособие к данной дополнительной образовательной программе.

Проблема защиты персональных данных с каждым годом всё актуальнее, количество утечек информации растет, а требования регламентов ужесточаются. Исходя из этого обучение по дополнительной образовательной программе «Защита персональных данных на предприятии» остаётся востребованной.

В свою очередь, обучение повысит осознанность сотрудников предприятий при работе с персональными данными. Что приведет к снижению утечек, нарушений. Обучение должно быть направленным на получение и улучшение знаний и навыков. Использование электронного учебного пособия при проведении занятий положительно влияет на формирование и приобретение знаний и навыков.

Электронное учебное пособие было разработано с помощью таких технологий, как HTML5, CSS, JavaScript. Поддерживаются эти технологии в любом современном браузере. Следовательно, можно сказать, что, получившееся в результате пособие, весьма доступно практически на любом устройстве. Имеет современный интерфейс, приятно глазу и, значит, с ним хочется учиться.

В ходе выполнения работы были решены следующие задачи:

1. Проанализировать материал по теме «Защита персональных данных на предприятии».
2. Разработать дополнительную образовательную программу «Защита персональных данных на предприятии»
3. Разработать структуру и интерфейс электронного учебного пособия по дополнительной образовательной программе «Защита персональных данных на предприятии».
4. Наполнить электронное учебное пособие.

Цель была следующая: разработать дополнительную образовательную программу «Защита персональных данных на предприятии». Таким образом, цель достигнута.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Алексеев Г. В. Основы разработки электронных учебных изданий [Текст]: учебно-методическое пособие / Г. В. Алексеев. — Санкт-Петербург: Лань, 2016. — 144 с.

2. Девяткин Е. М. Комплекс электронных лабораторных установок по общей физике [Электронный ресурс] / Е. М. Девяткин, С. Л. Хасанова, Н. В. Чиганова // Современные проблемы науки и образования. — 2016. — № 4. — Режим доступа: http://www.science-education.ru/ru/article/view?id=24956/ (дата обращения: 10.12.2018)

3. Жукова В. В. Обеспечение защиты персональных данных в информационной системе [Текст] / В. В. Жукова // Вестник научного общества студентов, аспирантов и молодых ученых. — 2015. — № 3. — С. 68–71.

4. Иллюстрированный самоучитель по HTML [Электронный ресурс]. — Режим доступа: http://ru.html.net/ (дата обращения: 17.12.2018).

5. Ильина М. А. Электронные учебные пособия, и их важность в учебном процессе [Текст] / М. А. Ильина // Информационно-коммуникационные технологии в педагогическом образовании. — 2012. — № 3. — С. 102–103.

6. Козлова Е. И. Электронные учебные издания в современном вузе: учебно-методическое пособие [Текст] / Е. И. Козлова. — Москва: Форум, 2013. — 207 с.

7. Колясникова Л. В. Современные средства оценивания результатов обучения [Текст]: учебное пособие / Л. В. Колясникова — Екатеринбург, 2017. — 203 с.

8. Комплексная защита информации ограниченного доступа в корпоративных информационных системах [Электронный ресурс]. — Режим доступа: http://itsec.ru/articles2/Inf_security/kompleksnaya-zaschita-informatsii-

ogranichennogo-dostupa-v-korporativnyh-informatsionnyh-sistemah/ (дата обращения: 12.12.2018).

9. Лушников А. М. Защита персональных данных работника: сравнительно-правовой комментарий гл.14 Трудового Кодекса РФ. [Электронный ресурс]. — Режим доступа: http://www.top-personal.ru/issue.html?2150 (дата обращения: 29.11.2018).

10. Лушников А. М. Неприкосновенность частной жизни и персональные данные в сфере трудовых отношений: стратегия правотворчества в контексте мирового опыта. [Текст] / А. М. Лушников // Юридическая техника. — 2015. — № 9. — С. 410–417.

11. Макаров А. М. Организация защиты персональных данных [Текст]: учебное пособие / А. М. Макаров, И. В. Калиберда, К. О. Бондаренко. — Ставрополь: СКФУ, 2015. — 102 с.

12. Обзор методов защиты корпоративной информации — Информационная безопасность [Электронный ресурс]. — Режим доступа: http://itsec.ru/articles2/Inf_security/obzor-metodov-zaschity-korporativnoy-informatsii/ (дата обращения 12.12.2018).

13. Петюшкин А. В. HTML в Web-дизайне [Текст] / А. В. Петюшкин. — под ред. Е. Кондукова. — Санкт-Петербург: БХВ-Петербург, 2004. — 400 с.

14. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. — Режим доступа: http://base.garant.ru/70252506/#ixzz5fYD91RtG (дата обращения: 29.11.2018).

15. Приказ Министерства образования и науки РФ от 5 декабря 2013 г. № 1310 «Об утверждении Порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности» [Электронный ресурс]. — Режим доступа:

http://rulaws.ru/acts/Prikaz-Minobrnauki-Rossii-ot-05.12.2013-N-1310/ (дата обращения: 29.11.2018).

16. Приказ Федеральной службы по техническому и экспортному контролю 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» (с изменениями и дополнениями) [Электронный ресурс]. — Режим доступа: http://base.garant.ru/70380924/ (дата обращения: 10.12.2018).

17. Руднев А. Ю. Разработка и использование электронных учебных изданий [Текст] / А. Ю. Руднев, В. А. Тегин. — Москва: Lennex Corp, 2012. — 168 с.

18. Сабанов А. Г. Защита персональных данных в организациях здравоохранения [Текст]: учебное пособие / А. Г. Сабанов, В. Д. Зыков, Р. В. Мещеряков. — Москва: Горячая линия-Телеком, 2012. — 206 с.

19. Современный учебник по JavaScript [Электронный ресурс]. — Режим доступа: https://learn.javascript.ru/ (дата обращения: 29.11.2018).

20. Справочник по CSS [Электронный ресурс]. — Режим доступа: http://htmlbook.ru/css (дата обращения: 22.11.2018).

21. Справочник по HTML [Электронный ресурс]. — Режим доступа: http://htmbook.ru/html (дата обращения: 11.12.2018).

22. Федеральная служба по техническому и экспортному контролю приказ от 23 марта 2017 г. № 49 «о внесении изменений в состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. — Режим доступа: https://fstec.ru/component/attachments/download/1694 (дата обращения: 29.11.2018).

23. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и

дополнениями) [Электронный ресурс]. — Режим доступа: http://base.garant.ru/12148555/#ixzz5fYDKzx2B (дата обращения: 29.11.2018).

24. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (с изменениями и дополнениями) Актуальная ред. 30.06.2018 [Электронный ресурс]. — Режим доступа: http://ivo.garant.ru/#/document/12148567/-paragraph/24880:0 (дата обращения: 29.11.2018).

25. Флэнаган Д. JavaScript: карманный справочник [Текст]: справочник / Д. Флэнаган. — под. ред. Тригуб С. Н. — пер. с англ. Сысонюк А. Г. — 3-е издание. — Москва: ООО «И. Д. Вильямс», 2013. — 320 с.

26. Халяпина Л. П. Новые информационные технологии в профессиональной педагогической деятельности: учебное пособие / Л. П. Халяпина, Н. В. Анохина. — Кемерово: Кемеровский государственный университет, 2011. — 118 с.

27. Что такое Bootstrap [Электронный ресурс]. — Режим доступа: https://webformyself.com/chto-takoe-bootstrap/ (дата обращения: 25.11.2018).

28. Шерпетис Е. И. Угрозы безопасности персональных данных в учреждении [Текст] / Е. И. Шерпетис // Вестник научного общества студентов, аспирантов и молодых ученых. — 2015. — № 3. — С. 230–235.

29. Шмитт К. CSS. Рецепты программирования [Текст] / К. Шмит. — пер. с англ. Т. Коротяева. — Санкт-Петербург: БХВ-Петербург, 2011. — 672 с.

30. Эмиров М. Б. К вопросу о защите персональных данных в сфере бизнеса [Текст] / М. Б. Эмиров, А. Г. Саидов, Д. А. Рагимханова // Юридический вестник ДГУ. — 2011. — № 1. — С. 58–61.

31. Mozilla и отдельные соучастники. [Электронный ресурс] — Режим доступа: https://developer.mozilla.org/ru/docs/Learn/JavaScript (дата обращения: 05.12.2018).

ПРИЛОЖЕНИЕ

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»

Институт инженерно-педагогического образования

Кафедра информационных систем и технологий

Направление подготовки 44.03.04 Профессиональное обучение (по отраслям)

Профиль «Информатика и вычислительная техника»

Профилизация «Информационная безопасность»

УТВЕРЖДАЮ
И.о. заведующего кафедрой

_____ И.А. Суслова
подпись и.о. фамилия

« ___ » _____ 2018 г.

ЗАДАНИЕ
на выполнение выпускной квалификационной работы бакалавра

студента (ки) *5* курса группы *ЗИБ-501*

Ольковой Аделины Викторовны
фамилия, имя, отчество полностью

1. Тема ***Дополнительная образовательная программа «Защита персональных данных на предприятии»***

утверждена распоряжением по институту от «_____» _____ 20 г. № ___

2. Руководитель ***Окуловская Анастасия Георгиевна***
фамилия, имя, отчество полностью

_____ _____ *ст. преподаватель* *РГППУ*
ученая степень ученое звание должность место работы

3. Место преддипломной практики *ООО УЭЦ «Концепция безопасности труда»*

4. Исходные данные к ВКР: Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (с изменениями и дополнениями) Актуальная ред. 30.06.2018.
Алексеев Г. В. Основы разработки электронных учебных изданий [Текст]: учебно-методическое пособие / Г. В. Алексеев. — Санкт-Петербург: Лань, 2016. — 144 с.

5. Содержание текстовой части ВКР (перечень подлежащих разработке вопросов):
проанализировать материал по теме «Защита персональных данных на предприятии»;

разработать дополнительную образовательную программу «Защита персональных данных на предприятии»;
разработать структуру и интерфейс электронного учебного пособия по дополнительной образовательной программе «Защита персональных данных на предприятии»;
наполнить электронное учебное пособие.

6. Перечень демонстрационных материалов *презентация, выполненная в MS Power Point*

7. Календарный план выполнения выпускной квалификационной работы

№ п/п	Наименование этапа дипломной работы	Срок выполнения этапа	Процент выполнения ВКР	Отметка руководителя о выполнении
1	Сбор информации по выпускной квалификационной работе	12.12.2018	10%	подпись
2	Выполнение работ по разрабатываемым вопросам и их изложение в пояснительной записке:		60%	подпись
2.1	Анализ источников по теме	22.12.2018	10%	подпись
2.2	Разработка дополнительной образовательной программы «Защита персональных данных на предприятии»	24.12.2018	20%	подпись
2.3	Разработка структуры и интерфейса электронного учебного пособия по дополнительной образовательной программе «Защита персональных данных на предприятии»	26.12.2018	15%	подпись
2.4	Наполнение электронного учебного пособия	28.12.2018	15%	подпись
3	Оформление текстовой части ВКР	03.01.2019	10%	подпись
4	Выполнение демонстрационных материалов к ВКР	07.01.2019	10%	подпись
5	Нормоконтроль	15.01.2019	5%	подпись
6	Подготовка доклада к защите в ГЭК	18.01.2019	5%	подпись

8. Консультанты по разделам выпускной квалификационной работы

Наименование раздела	Консультант	Задание выдал		Задание принял	
		подпись	дата	подпись	дата

Руководитель _____ _____ *Задание получил* _____ _____
подпись дата подпись студента дата

9. Дипломная работа и все материалы проанализированы.
Считаю возможным допустить ***Олькову А.В.*** к защите выпускной квалификационной работы в государственной экзаменационной комиссии.
Руководитель _____ _____
подпись дата

10. Допустить ***Олькову А.В.*** к защите выпускной квалификационной работы
фамилия и. о. студента
в государственной экзаменационной комиссии (протокол заседания кафедры от «___» _____ 20___г., № _____)
И.о. заведующего кафедрой _____ _____
подпись дата