ББК 32.97-018.2я73
П 30

Петренко В. И., Мандрица И. В.

П 30 Защита персональных данных в информационных системах. Практикум: Учебное пособие. — СПб.: Издательство «Лань», 2019. — 108 с.: ил. — (Учебники для вузов. Специальная литература).

ISBN 978-5-8114-3311-7

В практикуме приводятся краткие теоретические сведения и методические пояснения и рекомендации по выполнению практических занятий по учебной дисциплине «Защита персональных данных в информационных системах», а также порядок их оформления. Практикум составлен в соответствии с учебным планом по направлению подготовки «Информационная безопасность» и Федеральным государственным образовательным стандартом высшего образования по направлению подготовки «Информационная безопасность» (уровень бакалавриата).

Практикум предназначен для студентов, обучающихся по указанному направлению подготовки.

ББК 32.97-018.2я73

Рецензенты:

Ф. Б. ТЕБУЕВА — доктор физико-математических наук, доцент, зав. кафедрой прикладной математики и компьютерной безопасности Института информационнных технологий и телекоммуникаций Северо-Кавказского федерального университета;

Н. Г. ДЕМУРЧЕВ — кандидат технических наук, доцент, директор ООО «СГУ-Инфоком».

Обложка
Е. А. ВЛАСОВА

ВВЕДЕНИЕ

Учебная дисциплина «Защита персональных данных в информационных системах» относится к области современных знаний о способах и средствах защиты персональных данных в информационных системах.

Целью изучения дисциплины «Защита персональных данных в информационных системах» является теоретическая и практическая подготовленность бакалавра для проведения работ по обеспечению безопасности персональных данных (ПДн) при их обработке в информационных системах (ИС) в соответствии с современными требованиями, а также приобретение набора компетенций будущего бакалавра по направлению подготовки 10.03.01 «Информационная безопасность».

Задачами дисциплины являются:

1) изучение федеральных законов, постановлений Правительства РФ, приказов ФСТЭК РФ и ФСБ РФ в области защиты персональных данных при их обработке в ИС;

2) изучение методов и процедур определения актуальных угроз и уязвимостей безопасности персональных данных при их обработке в ИС;

3) изучение методов и порядка проведения мероприятий по техническому обеспечению безопасности ПДн при их обработке в ИС;

4) развитие умений, навыков и способностей разрабатывать организационно-распорядительные документы, необходимые для безопасного функционирования информационной системы персональных данных (ИСПДн);

5) ознакомление со средствами и методами защиты информации.

Дисциплина «Защита персональных данных в информационных системах» относится к обязательным дисциплинам вариативной части профессионального цикла.

Она является базовой для изучения дисциплин по комплексным системам защиты информации на предприятии.

Учебное пособие содержит тринадцать практических занятий, подлежащих выполнению студентами.

Каждое практическое занятие состоит из следующих разделов:

— наименование занятия;

— цели занятия;

— формируемые компетенции;

— учебные вопросы занятия;

— теоретическая часть;

— оборудование и материалы;

— методические пояснения и рекомендации по выполнению практического занятия;

— задания базового и повышенного уровней;

— содержание отчета;

— контрольные вопросы.

Учебное пособие содержит список литературы, общий для всех практических занятий.

Задания по практическим занятиям построены по уровням:

1-й уровень — выполнение заданий базового уровня;

2-й уровень — решение заданий повышенного уровня.

Лекционный материал достаточно подробно изложен в учебном пособии [1].

УКАЗАНИЯ ПО ТЕХНИКЕ БЕЗОПАСНОСТИ ПРИ ВЫПОЛНЕНИИ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Требования безопасности перед началом работ.

1. ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.

2. Убедиться в отсутствии видимых повреждений на рабочем месте.

3. Разместить на столе тетради, учебные пособия так, чтобы они не мешали работе на компьютере.

4. Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или сотрудника лаборатории.

Требования безопасности во время работы.

1. ЗАПРЕЩАЕТСЯ: присоединять или отсоединять кабели, трогать разъемы, провода и розетки, открывать системный блок, пытаться самостоятельно устранять неисправности в работе оборудования, приносить и запускать компьютерные игры.

2. Выполняя практическое занятие, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данной работе.

3. Подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса.

4. При обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или сотруднику лаборатории.

Требования безопасности по окончании работы.

1. Доложить руководителю занятий или сотруднику лаборатории о завершении работ.

2. Привести в порядок и сдать рабочее место сотруднику лаборатории, доложить руководителю занятий о сдаче.

Занятие № 1

РАЗРАБОТКА ПРИКАЗОВ ОБ ОРГАНИЗАЦИИ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Цели занятия

В результате настоящего занятия и последующей самостоятельной работы студенты должны:

1) знать содержание и порядок разработки приказа об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, приказа о назначении ответственного за обработку персональных данных и приказа о создании комиссии по организации и проведению работ по защите персональных данных;

2) уметь разрабатывать организационно-распорядительные документы, необходимые для эффективной защиты персональных данных в соответствии с требованиями действующего законодательства;

3) приобрести навыки разработки необходимых документов в интересах организации работ по обеспечению безопасности ИСПДн;

4) приобрести навыки анализа и обобщения полученных результатов.

Формируемые компетенции

ОПК-5 — способность использовать нормативные правовые акты в профессиональной деятельности.

Учебные вопросы занятия

1. Разработка приказа об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

2. Разработка приказа о назначении ответственного за обработку персональных данных.

3. Разработка приказа о создании комиссии по организации и проведению работ по защите персональных данных.

Теоретическая часть

Основополагающим законом в области защиты персональных данных является Федеральный закон № 152 от 27 июля 2006 г. «О персональных данных» [2].

Закон определяет:

— основные понятия, связанные с обработкой персональных данных;

— принципы и условия обработки персональных данных;

— обязанности оператора персональных данных;

— права субъекта персональных данных;

— виды ответственности за нарушение требований ФЗ № 152;

— государственные органы, осуществляющие контроль за соблюдением требований ФЗ № 152.

Статья 18.1 ФЗ № 152 определяет меры, направленные на обеспечение выполнения оператором обязанностей по защите персональных данных. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено данным федеральным законом или другими федеральными законами. К таким мерам относятся:

1) назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;

2) издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со ст. 19 ФЗ № 152;

4) осуществление внутреннего контроля и/или аудита соответствия обработки персональных данных ФЗ № 152 и принятым в соот-

ветствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения ФЗ № 152, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим федеральным законом;

6) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и/или обучение указанных работников.

Статья 22.1 закона определяет порядок назначения лиц, ответственных за обработку персональных данных, и их обязанности:

— оператор, являющийся юридическим лицом, назначает лицо, ответственное за организацию обработки персональных данных;

— лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от исполнительного органа организации, являющейся оператором, и подотчетно ему;

— оператор обязан предоставлять лицу, ответственному за организацию обработки персональных данных, следующие сведения:

1) наименование (фамилия, имя, отчество), адрес оператора;

2) цель обработки персональных данных;

3) категории персональных данных;

4) категории субъектов, персональные данные которых обрабатываются;

5) правовое основание обработки персональных данных;

6) перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;

7) описание мер, предусмотренных ФЗ № 152, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

8) фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;

9) дата начала обработки персональных данных;

10) срок или условие прекращения обработки персональных данных;

11) сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

12) сведения об обеспечении безопасности персональных данных в соответствии с требованиями;

— лицо, ответственное за организацию обработки персональных данных, в частности, обязано:

1) осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

2) доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

3) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и/или осуществлять контроль за приемом и обработкой таких обращений и запросов.

Принципы правового регулирования отношений в сфере информации определяются Федеральным законом № 149 от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации» [3].

Оборудование и материалы

Персональные ЭВМ с подключением к сети Интернет.

Текстовый редактор Microsoft Office или аналогичный.

Защита персональных данных в информационных системах: электронный учебно-методический комплекс. Свидетельство о государственной регистрации базы данных № 2012620964.

Информационно-справочная система «Защита персональных данных в информационных системах». Свидетельство о государственной регистрации базы данных № 2012620913.

ЗАДАНИЯ

Методические пояснения и рекомендации по выполнению первого вопроса

В ходе отработки первого вопроса обучаемые должны, для заданного варианта исходных данных (Задания базового уровня) разработать приказ об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Методические пояснения и рекомендации по выполнению второго вопроса

В ходе отработки второго вопроса обучаемые должны для заданного варианта исходных данных (Задания базового уровня) разработать приказ о назначении ответственного за обработку персональных данных.

Методические пояснения и рекомендации по выполнению третьего вопроса

В ходе отработки третьего вопроса обучаемые должны для заданного варианта исходных данных (Задания базового уровня) разработать приказ о создании комиссии по организации и проведению работ по защите персональных данных.

Для получения максимальной оценки обучаемый должен для заданного варианта исходных данных отработать вопросы из заданий повышенного уровня.

Задания базового уровня

1. Разработать приказ об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных для дошкольной образовательной организации.

2. Разработать приказ об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных для общеобразовательной организации.

3. Разработать приказ об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных для профессиональной образовательной организации.