Тип работы: Дипломная работа

Предмет: Информатика основы

Содержание

Введение

В рамках данной работы проведен анализ организации работ по управлению персональными данными. Стандарты, регулирующие технологию работы со сведениями, содержащими персональные данные, должны содержать:

- порядок доступа сотрудников к работе в информационных системах, в которых проводится обработка персональных данных;
- технологию разграничения доступа к информационным системам;
- технологии копирования и хранения информации, в которой содержатся персональные данные;
- использование средств информационной безопасности при обработке персональных данных.

Для определения требований к обеспечению безопасности обработки персональных данных необходимо классифицировать их по типам и объемам.

Классификация персональных данных проведена как в федеральных законах (152-ФЗ «О персональных данных»), так и в нормативных актах ФСБ и других федеральных, а также отраслевых стандартах, соответствующими ГОСТами.

Цель выпускной квалификационной работы заключается в разработке информационной системы управления персональными данными сотрудников предприятий.

Задачи работы:

- анализ нормативно-правовых актов и основных требований к защите персональных данных;
- анализ специфики работы с персональными данными в условиях исследуемой компании;
- построение модели угроз конфиденциальности персональных данных;
- анализ бизнес-процессов управления персональными данными;
- анализ используемых программных и аппаратных средств защиты персональных данных;
- анализ недостатков существующей системы защиты персональных данных;

- разработка рекомендаций по совершенствованию системы защиты персональных данных;
- технико-экономическое обоснование проекта.

Объект исследования: технология по обеспечению защиты информации Управления ПФР.
Предмет исследования: технология обеспечения защиты персональных данных Управления ПФР.

1.Аналитическая часть

1.1. Обзор законодательных актов в области защиты персональных данных

Персональные данные - любая информация, имеющая отношение к определенному или определяемому на основании такой информации физическому лицу, позволяющая его идентифицировать включающая реквизиты:

- фамилия, имя, отчество;
- дату и место рождения;
- контактные данные;
- данные об образовании, месте работы;
- иные данные (о состоянии здоровья, биометрические данные, реквизиты документов, данные идентификации субъекта в банковских системах и др.)

Субъект персональных данных – физическое лицо, идентифицируемое посредством персональных данных (владелец персональных данных).
Согласно докладу о глобальных рисках Всемирного экономического форума 2019 года, мошенничество с данными и кибератаки являются четвертым и пятым глобальными рисками, с которыми сталкиваются организации, использующие автоматизированные системы для обработки информации. По своей значимости эти риски приравниваются к экологическим проблемам. На рисунке 1 приведены статистические данные по нарушениям персональных данных в странах мира на 2019 г. (красный столбец) в сравнении с 2018г. (серый столбец).

Рисунок 1 - Статистические данные по нарушениям персональных данных в странах мира на 2019 г. в сравнении с 2018г.

Как показано на рисунке 1, в настоящее время наблюдается тенденция к росту инцидентов, связанных с утечками персональных данных, которые несут значительный ущерб для субъектов. В Российской Федерации также отмечаются случаи утечки персональных данных, содержащихся в информационных базах различных ведомств (рисунок 2).

Рисунок 2 – Утечки персональных данных в РФ за 2019г.

Утечки персональных данных могут происходить как непреднамеренно из-за нарушения требований к защите информации, так и вследствие направленных действий злоумышленников.
Таким образом, для обеспечения защиты персональных данных необходимо принимать ряд технологических и организационных мер, позволяющих обеспечить требования работы с конфиденциальной информацией.
Одной из наиболее часто встречающихся категорий персональных данных, с которой работают специалисты различных компаний, являются данные о сотрудниках. Специалистам отделов по работе с персоналом приходится работать со сканированными копиями документов сотрудников, что предполагает необходимость ограничения доступа к ним. Запросы на предоставление персональных данных могут подаваться со стороны различных ведомств, при этом их направление не всегда является правомерным. Таким образом, специалисту по кадрам необходимо знать, какие данные можно предоставлять в конкретное ведомство. Автоматизация разграничения доступа по типам документов позволяет выполнить требования законодательства о защите персональных данных, так как позволит создать возможности определения типов документов, которые могут быть предоставлены в ответ на запросы и автоматизировать рассылку данных в защищенном виде.
Нормативная база в области защиты персональных данных включает:

- 152- ФЗ «О Персональных данных» от 27.07.2006;
- Статьи Трудового кодекса;
- Локальные нормативные акты.

Нормативной базой технологии систем информационной безопасности являются: федеральное

законодательство, нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации, а также руководящие документы Федеральной службы по техническому и экспортному контролю (ФСТЭК России) и ФСБ России, регулирующие вопросы безопасности информации.
В соответствии с нормативными документами в области защиты информации, каждое предприятие и организация, в которой производится обработка персональных данных, обязано принять ряд организационных и технологических мер по обеспечению защиты информации.
Приведем основные положения законодательных актов в области информационной безопасности.
Защита информации, содержащейся в информационной системе, является составной частью работ по созданию и эксплуатации информационных систем персональных данных (ИСПДн) и обеспечивается на всех стадиях (этапах) ее создания и в ходе эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в информационной системе.
Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным
Согласно Федеральному закону от 27 июля 2006г. № 152-ФЗ, оператор в рамках обработки персональных данных должен обеспечивать комплекс необходимых правовых, организационных и технических мер по обеспечению конфиденциальности персональных данных, что достигается путем определения угроз безопасности, оценки эффективности мероприятий по обеспечению безопасности, контроля за принимаемыми мерами по защите информации [8].
Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
Постановление № 1119 содержит довольно подробную классификацию информационных систем персональных данных, угроз безопасности таких систем (п. 6), уровней защищенности информационных систем от указанных угроз
Так, в постановлении № 1119 выделено пять типов информационных систем персональных данных в зависимости от того, какие именно данные обрабатываются в рамках такой системы[7, с.58]:
1. информационные системы, обрабатывающие специальные категории персональных данных (данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений и т.д.);
2. информационные системы, обрабатывающие биометрические данные (данные, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность);
3. информационные системы, обрабатывающие общедоступные персональные данные;
4. информационные системы, обрабатывающие иные категории персональных данных (данные, не перечисленные выше);
5. информационные системы, обрабатывающие данные о сотрудниках оператора информационной системы.
В соответствии с требованиями к защите персональных данных при их обработке в информационной системе персональных данных (постановлении № 1119), под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным[12, с.88].
В настоящее время согласно методологии информационной безопасности, определены три типа угроз безопасности информационных систем персональных данных[11, с.78]:
1. Угрозы, связанные с наличием недокументированных возможностей в системном программном обеспечении, используемом в информационной системе;
2. Угрозы, связанные с наличием недокументированных возможностей в прикладном программном обеспечении, используемом в информационной системе;
3. Угрозы, не связанные с наличием недокументированных возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.
Приказ ФСТЭК России № 21 от 18.02.2013 определяет принципы классификации систем персональных данных. Согласно приказу ФСБ от 10.07.2014 № 378 определены четыре уровня защищенности персональных данных.
Каждый из присвоенных уровней защищенности предполагает применение соответствующих мер по обеспечению информационной безопасности.

В зависимости от соотношения типа информационной системы и характерных для нее угроз выделены четыре уровня защищенности персональных данных, необходимых для конкретной информационной системы.
Формирование требований к защите информации, содержащейся в информационной системе, осуществляется обладателем информации.
Общие требования к обеспечению информационной безопасности включают в себя [9, с.58]:
- принятие решения о необходимости защиты информации, содержащейся в информационной системе;
- определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе, и разработку на их основе модели угроз безопасности информации;
- определение требований к системе защиты информации информационной системы;
- классификацию информационной системы по требованиям защиты информации (далее - классификация информационной системы).
В рамках данной работы проведен анализ вопросов обеспечения защиты информации в информационных системах через построение методики оценки эффективности защиты персональных данных.
Этапами построения архитектуры системы информационной безопасности на предприятиях являются:
- аудит информационной системы, определение класса информационной системы;
- приведение базы локальных нормативных актов предприятия в соответствие с требованиями уровня защищённости информационной системы;
- проектирование технологической компоненты информационной безопасности в соответствии с уровнем защищенности информационной системы;
- установка технических средств защиты информации (системы видеонаблюдения, контроля управления доступом, систем охранно-пожарной сигнализации) в соответствии с моделью угроз безопасности.
Также за нарушения требований защиты персональных данных возможно наступление административной и уголовной ответственности.
Проблематика обеспечения защиты личных персональных данных рассматривается как в существующих законодательных актах, так и в исследовательских работах, посвящённых указанной тематике.
В работе Овчинниковой Т. А. «Ответственность за нарушение требований законодательства РФ о персональных данных» рассмотрены законодательные аспекты обеспечения защиты персональных данных, описан порядок привлечения к ответственности в зависимости от тяжести обнаруженного нарушения (от дисциплинарного взыскания до уголовной ответственности).
В работе Родичева Ю. А. «Правовая защита персональных данных» проведен анализ нормативных актов в области обеспечения защиты персональных данных – от федеральных законов до отраслевых стандартов. В работе Воробьева Е. Г. «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных» проведено описание требований к классам защищённости информационных систем персональных данных в зависимости от их категории.
Внесение персональных данных субъекта в общедоступные источники производится при наличии письменного согласия и ограничивается: фамилией, именем, отчеством, годом и местом рождения, адресом, абонентскими номерами и иной информацией, распространение которой не может нанести вреда субъекту.
Персональные данные являются информацией ограниченного доступа и являются объектом защиты в соответствии с требованиями законодательства РФ. При разработке требований к защите персональных данных производится их разделение на 4 категории, включающие:
- категория 4 - обезличенная и (или) общедоступная информация;
- категория 3 - персональные данные, с помощью которых проводится однозначная идентификация субъекта персональных данных;
- категория 2 - персональные данные, с помощью которых проводится идентификация субъекта персональных данных и возможно получение о нем дополнительных данных, за исключением персональных данных, отнесенных к категории 1;
- категория 1 - персональные данные, описывающие расовую, национальную принадлежность, политические взгляды, религиозные и философские убеждения, данные о состоянии здоровья, интимной жизни.
Классы информационных систем, обрабатывающих персональные данные, определяются их категорией и количеством ПДн.
 В ИСПДн класса 4 (К4) при нарушении параметров обработки персональных данных, отсутствуют

негативные последствия для субъектов

Список литературы

1. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ
2. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ
3. Методический документ. Утвержден ФСТЭК России 5 февраля 2021 г.
4. Ажмухамедов И. М. Основы организационно-правового обеспечения информационной безопасности : курс лекций / И. М. Ажмухамедов, О. М. Князева, А. Н. Марьенков. - Астрахань : Изд-во АГТУ, 2015. - 183 с.
5. Андрианов В.В., Зефиров С.Л., Голованов В.Б., Голдуев Н.А. Обеспечение информационной безопасности бизнеса. – М.: Альпина Паблишерз, 2015. – 338с.
6. Андрианов В.В., Зефиров С.Л., Голованов В.Б., Голдуев Н.А. Обеспечение информационной безопасности бизнеса. – М.: Альпина Паблишерз, 2018 – 338с.
7. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации / Е. К. Баранова, А. В. Бабаш. - Москва: РИОР ИНФРА-М, 2018. – 334 с.
8. Белобородова Н. А. Информационная безопасность и защита информации: учебное пособие / Н. А. Белобородова. - Ухта: УГТУ, 2016. - 69 с.
9. Благодаров А. В. Алгоритмы категорирования персональных данных для систем автоматизированного проектирования баз данных информационных систем / А. В. Благодаров, В.С. Зияутдинов, П.А. Корнев, В.Н. Малыш. - Москва: Горячая линия-Телеком, 2015. - 115 с.
10. Бондарев В. В. Анализ защищенности и мониторинг компьютерных сетей: методы и средства : учебное пособие / В.В. Бондарев. - Москва: Изд-во МГТУ им. Н.Э. Баумана, 2017. – 225с.
11. Бубнов А. А. Основы информационной безопасности : учебное пособие / А. А. Бубнов, В. Н. Пржегорлинский, О. А. Савинков. - Москва: Академия, 2017. – 252с.
12. Герасименко В.А., Малюк А.А. Основы защиты информации. – СПб.: Питер, 2010. – 320с
13. Горев А. И., Симаков А. А. Обработка и защита информации в компьютерных системах : учебно-практическое пособие / А. И. Горев, А. А. Симаков. - Омск : ОмА МВД России, 2016. - 87 с.
14. ГОСТ Р 50922-96. Защита информации. Основные термины и определения. – М.: Госстандарт России, 1996. – 17 с.
15. Грибунин В.Г., Чудовский В.В. Реализация требований комплексной системы защиты информации. – М.: Академия, 2017. – 533 с.
16. Гришина Н.В. Аудит защиты персональных данных. – М.: Форум, 2015. – 240 с.
17. Гришина Н.В. Комплексная система защиты информации на предприятии. – М.: Форум, 2010. – 240 с.
18. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие. - Ст. Оскол: ТНТ, 2010. - 384 с.
19. Демин, Ю.М. Защита персональных данных во внутриорганизационном документообороте - С-Пб: Питер, 2015. – 331 с.
20. Емельянова Н.З., Партыка Т.Л., Попов И.И. Защита информации в персональном компьютере. – М.: Форум, 2009. – 368 с.
21. Ефимова, Л.Л. Информационная безопасность персональных данных. Российский и зарубежный опыт: Монография. - М.: ЮНИТИ-ДАНА, 2013. - 239 с.
22. Завгородний В.И. Комплексная защита в компьютерных системах: Учебное пособие. – М.: Логос; ПБОЮЛ. - 2017. - 264 с.
23. Зайцев А.В. Информационные системы в профессиональной деятельности [Электронный ресурс]: Учебное пособие. - М.: РАП, 2013. - 180 с.
24. Колдаев, В.Д. Структуры и алгоритмы обработки данных: Учебное пособие. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 296 с.
25. Кондратьев А. В. Техническая защита информации. Практика работ по оценке основных каналов утечки: [учебное пособие] / А. В. Кондратьев. - Москва: Горячая линия - Телеком, 2016. - 304 с.
26. Коннолли Т., Бегг К. Базы данных: проектирование, реализация и сопровождение: теория и практика. - Москва: Вильямс, 2017. - 1439 с.
27. Корнеев И.К, Степанов Е.А. Защита информации в офисе. – М.: ТК Велби, Проспект, 2008. – 336 с.
28. Королев Е. Н. Администрирование операционных систем : учебное пособие. - Воронеж : Воронежский государственный технический университет, 2017. - 85 с.
29. Королев Е. Н. Администрирование операционных систем: учебное пособие / Е. Н. Королев. - Воронеж:

Воронежский государственный технический университет, 2017. - 85 с.
30. Коряковский А.В. Информационные системы предприятия: Учебное пособие. - М.: НИЦ ИНФРА-М, 2016. - 283 с.
31. Круценюк К. Ю. Офисные информационные технологии : учебное пособие. - Норильск : редакционно-издательский отдел ФГБОУВПО "НГИИ", 2017. - 126 с.
32. Кузнецова Е. В. Правовые меры обеспечения информационной безопасности: методические рекомендации / Е. В. Кузнецова. - Москва: МАОРИ, 2016. - 53 с.
33. Лемешко Т. Б., Шурыгин В. Н. Современные информационные технологии : учебное пособие. - Москва : Росинформагротех, 2017. - 135 с.
34. Леоненков А.В. Объектно-ориентированный анализ и проектирование с использованием UML и IBM Rational Rose. Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. - 318 с
35. Летуновский А.В., Матюшичев И.Ю. UML моделирование информационных систем и бизнес-процессов. СПб.: Питер. - 2017. - 113 с.
36. Лопатин Д. В. Программно-аппаратная защита информации: учебное пособие. - Тамбов: ТГУ, 2014. – 254с.
37. Мелихова Н. В. Информационные технологии управления: учебное пособие. - Челябинск: Издательство Челябинского государственного университета, 2015. - 214 с.
38. Михайлова Е. М., Анурьева М. С. Организационная защита информации [Электронный ресурс]/ Михайлова Е. М., Анурьева М. С. - Тамбов: ФГБОУ ВО "Тамбовский государственный университет имени Г. Р. Державина", 2017.
39. Михалевич Е.В. Обработка персональных данных: анализ законодательства и судебной практики / Е.В. Михалевич. - Москва: ФГБУ "Редакция "Российской газеты", 2019. - 143 с.
40. Никифоров С. Н. Защита информации: защита от внешних вторжений: учебное пособие / С.Н. Никифоров. - Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный университет, 2017. - 82 с
41. Никифоров С. Н. Защита информации: учебное пособие / С.Н. Никифоров. - Санкт-Петербург: СПбГАСУ, 2017. - 76 с.
42. Никифоров С. Н., Ромаданова М. М. Защита информации. Пароли, скрытие, удаление данных: учебное пособие / С. Н. Никифоров, М. М. Ромаданова. - Санкт-Петербург: СПбГАСУ, 2017. - 107 с.
43. Овчинникова Т. А. Ответственность за нарушение требований законодательства РФ о персональных данных: монография / Т. А. Овчинникова. - Хабаровск: Изд-во ТОГУ, 2018. – 81с.
44. Смычёк М.А. Информационная безопасность и защита информации: учебное / М.А. Смычёк. - Нижний Новгород: Нижегородский государственный технический университет, 2016. – 125с.
45. Такатлы Д. А. Защита персональных данных / Д. А. Такатлы. - Петропавловск-Камчатский: Дальневосточный филиал Федерального государственного бюджетного образовательного учреждения высшего образования "Всероссийская академия внешней торговли Министерства экономического развития Российской Федерации", 2016. - 92 с.
46. Шалак М. Е. Архивное дело и делопроизводство: учебное пособие / М. Е. Шалак; РОСЖЕЛДОР. - Ростов-на-Дону: ФГБОУ ВО РГУПС, 2017. - 78 с.