Тип работы: ВКР (Выпускная квалификационная работа)

Предмет: Информационные технологии

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В настоящее время широкое развитие получают технологии, связанные с возможностями проведения финансовых операций, сделок, получения государственных услуг в дистанционном режиме с использованием Интернет-технологий. В качестве идентификатора для автоматизации в системах Банков, сервисов государственных услуг, систем оплаты услуг ЖКХ и связи выступают персональные данные. Таким образом, для исключения несанкционированного использования персональных данных необходимо принимать меры по обеспечению их защищенности. Накопление массивов персональных данных осуществляется в информационных системах кадрового учета предприятий, банковских системах, системах образовательных и медицинских учреждений. Современные системы документооборота позволяют совершать юридически значимые действия с использованием электронной подписи, для выдачи которой необходимо предъявлять документы, в которых содержатся персональные данные. Таким образом, для исключения нанесения ущерба необходимо обеспечить защиту при проведении операций в дистанционном режиме.
Обеспечение конфиденциальности персональных данных предполагает необходимость защиты от несанкционированного доступа, модификации, удаления, копирования массивов данных. Механизмы защиты персональных данных включают проведение настроек программных комплексов, проведение организационных мероприятий, принятие мер по физическому укреплению зданий и помещений организаций, что позволит защитить носители информации от краж и несанкционированного копирования. В некоторых случаях для предотвращения утечек принимаются меры по защите физических каналов.
Целью работы является определение порядка организационных и технических мер по обеспечению конфиденциальной информации от взлома и утечек в условиях ООО «СДЭК».
Задачи работы:
 анализ законодательной базы в области обеспечения защиты персональных данных (ПДн);

 анализ структуры информационной системы организации, определение объектов защиты ПДн;
 определение перечня актуальных угроз конфиденциальности ПДн;
 анализ текущего состояния обеспечения защиты ПДн в условиях компании и определение направлений их совершенствования;
 выбор программных и аппаратных решений по защите информационной системы компании от взлома и утечек.
Объект исследования: информационная система ООО «СДЭК».
Предмет исследования: технологические и организационные методы по обеспечению защиты информации от взлома и утечек.

ГЛАВА 1. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ. ОСНОВЫ ОРГАНИЗАЦИИ ЗАЩИТЫ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1.1 Понятие персональных данных в информационной системе предприятия

К категории персональных данных относятся сведения о физических лицах, посредством которых можно провести их однозначную идентификацию. Персональные данные могут включать:
 анкетные данные, включающие ФИО, данные о дате и месте рождения;
 реквизиты документов, удостоверяющих личность субъекта (серия и номер паспорта, СНИЛС, ИНН, военный билет, водительское удостоверение и др.);
 адрес электронной почты, номера телефонов;
 информация о полученной квалификации, трудовой деятельности;
 информация о вероисповедании;
 идентификаторы в информационных системах банов и государственных учреждений;
 медицинская документация.
В качестве субъектов ПДн выступают физические лица, которые могут быть однозначно определены посредством информации, являющейся носителем ПДн.
Проблематика обеспечения защиты ПДн является предметом обсуждения международных форумов в области информационной безопасности, экономического развития, обороны, информационных технологий. По данным [3], несанкционированное использование персональных данных, сетевые атаки, используемые для получения несанкционированного доступа к информационным ресурсам, содержагщим ПДн, входят в первую пятерку актуальных рисков, с которыми сталкиваются компании – операторы информационных систем, в которых осуществляется обработка конфиденциальных сведений, включающих ПДн. На рисунке 1 приведена диаграмма количества инцидентов, связанных с утечками ПДн в 2019 г в сравнении с 2018 г.г.

Рисунок 1 - Диаграмма количества инцидентов, связанных с утечками ПДн в 2019 г в сравнении с 2018 г.г.

Как показано на рисунке 1, для современного состояния информационных систем предприятий характерно наличие тренда, связанного с увеличением количества инцидентов информационной безопасности, связанных несанкционированным использованием ПДн, что приводит к негативным последствиям для субъектов ПДн. Статистика инцидентов, связанных с несанкционированным использованием ПДн в условиях Российских операторов за 2020г., приведена на рис.2.

Рисунок 2 – Статистика инцидентов, связанных с несанкционированным использованием ПДн в условиях Российских операторов за 2020г.

Причинами инцидентов, связанных с утечками ПДн, могут являться как халатность сотрудников компании – оператора ПДн, а также преднамеренная активность сторонних лиц, направленная на получение доступа к защищаемым информационным ресурсам.
В организациях, являющихся операторами по обработке ПДн, в соответствии с действующим законодательством, необходимо принятие ряда мер по обеспечению защищенности информационных ресурсов, нарушение которых может приводить к санкциям в виде штрафов, уголовной ответственности руководства и приостановки деятельности организации.
В рамках своей деятельности организации осуществляют обработку данных о сотрудниках в деятельности отдела кадров и бухгалтерского учета, о клиентах (в рамках деятельности компаний, предоставляющих услуги различного вида). В настоящее время также сбор персональных данных осуществляется в рамках маркетинговой деятельности и работы программ лояльности. Обработка ПДн возможна только при наличии

согласия, поданного субъектом в письменной форме.

1.2 Законодательные и нормативные акты, регулирующие отношения, связанные с защитой и обработкой персональных данных

Проведем обзор законодательства, регламентирующего вопросы обеспечения защиты ПДн. Перечень правовых актов, в которых определены требования в области защиты ПДн, включает [4]:
- 152- ФЗ «О Персональных данных» от 27.07.2006;
- Статьи Трудового кодекса;
- Указы, постановления и ГОСТы, применяемые для решения задач защиты ПДн в системах определенного вида.

В соответствии с 152-ФЗ «О персональных данных», компании, осуществляющие обработку ПДн, должны принимать меры, исключающие возможности несанкционированного доступа к ПДн. Определение комплекса мер по защите осуществляется в соответствии с классом защищенности, объемами обрабатываемых сведений.
В Постановлении 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»/ 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. Проведена детальная классификация ИСПДн, в которой определены классы защищенности ПДн по типам [6]:
- общедоступные ПДн;
- ПДн, позволяющие однозначно идентифицировать субъекта;
- ПДн, при утечке которых не наступает негативных последствий для субъекта;
- ПДн, утечка которых может приводить к негативным последствиям для их субъекта.

Для каждого из уровней защищенности определен перечень мероприятий по защите от утечек. Класс защищенности присваивается системе по результатам аудита, который проводится или сторонними сертифицированными организациями или силами специалистов компании, имеющих соответствующие компетенции.

1.3 Система защиты персональных данных. Анализ и средства защиты персональных данных

При проектировании системы защиты информации необходимо выполнить:
- создать организационную структуру в компании, в компетенцию которой входят вопросы разработки регламентов информационной безопасности, технической поддержки программных и инженерных систем, аудит соблюдения требований сотрудниками;
- инвентаризация информационных ресурсов, определение перечня конфиденциальных сведений;
- определение списка сотрудников, имеющих доступ к работе с ПДн, ознакомление их с требованиями соблюдения конфиденциальности, особенностями работы с информационными ресурсами, содержащими ПДн;
- создание ролевой модели доступа, разработка регламентов документооборота в рамках предоставления доступа к информационным ресурсам в части утверждения заявок руководством, соответствия должностных обязанностей и имеющихся полномочий в ИСПДн, приведение их в соответствие;
- создание комиссий по разбору инцидентов в области информационной безопасности.

Пакет локальных нормативных актов в области защиты ПДн должен включать [10]:
- Положение об организации защиты информации;
- Список информационных систем, содержащих персональные данные;
- Согласия субъектов на проведение обработки ПДн;
- Обязательства о неразглашении конфиденциальных сведений, работа с которыми производится в рамках выполнения должностных обязанностей;
- Инструкции пользователей и администраторов программных комплексов, используемых для обработки ПДн;
- Таблицы разграничения пользователей к ИСПДн.

Работа сотрудников с защищаемыми информационными ресурсами должна производиться в соответствии с приказами руководства.

В Положении о работе с персональными данными в условиях информационных систем организаций указывается порядок получения, обработки ПДн, с которыми осуществляется взаимодействие, определяются технологии обеспечения их конфиденциальности, регламентируются операции резервирования данных, размещения резервных копий на электронных и бумажных носителях, возможность передачи в сторонние организации или третьим лицам.
Локальными нормативными актами в организациях регламентируются вопросы [8]:
- цель и задачи обработки ПДн;
- определение видов обрабатываемых ПДн, источники их получения;
- перечень отделов и сотрудников, имеющих допуск к работе с ПДн;
- перечень программных продуктов, в которых производится обработка ПДн (с указанием способов защиты на уровне приложения);
- ответственность операторов за нарушение регламентов обработки ПДн и при возникновении инцидентов, связанных с их утечками.

Защита ПДн на уровне программного обеспечения осуществляется через разграничение доступа, парольную защиту, мониторинг активности пользователей. Также должны быть исключены прецеденты работы пользователей под чужими учетными данными.
За нарушения требований к защите ПДн при их обработке в информационных системах компаний предусмотрены санкции в форме дисциплинарной, материальной, административной и уголовной ответственности (ст. 90 ТК РФ, ч. 1 ст. 24 Федерального закона от 27.07.2006 № 152-ФЗ).
Наступление дисциплинарной ответственности происходит в случаях, когда разглашение персональных данных проводится сотрудниками, задействованными в обработке ПДн в информационных системах.
Нарушения требований к обеспечению защиты информации могут приводить в зависимости от типа нарушения от дисциплинарного взыскания до увольнения, санкций в виде денежных штрафов, административной и уголовной ответственности.
Причинами утечек конфиденциальной информации могут являться [10]:
- действия сотрудников, нарушающие требования по защите информации, связанные либо с халатностью, либо с направленной работой злоумышленников;
- активность посторонних лиц – посетителей офиса компании;
- неэффективная организация контроля за состоянием защищенности информационных ресурсов.

В качестве носителей информации, являющихся источниками конфиденциальных данных, могут выступать:
- трафик корпоративных приложений;
- файлы электронной почты;
- документация на бумажных носителях;

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ
2. Романов В. Г. Персональные данные: проблемы правовой охраны и защиты: монография / В. Г. Романов. - Чита : ЗабГУ, 2019. - 302 с.
3. Брауде-Золотарев М. Ю., Сербина Е.С., Негородов В. С., Волошкин И.Г. Персональные данные в государственных информационных ресурсах / М. Ю. Брауде-Золотарёв, Е.С. Сербина, В.С. Негородов, И.Г. Волошкин ; Российская акад. нар. хоз-ва и гос. службы при Президенте Российской Федерации (РАНХиГС). - Москва : Дело, 2016. – 53с.
4. Колованги С. В. Персональные данные: учебный курс / Колованги С.В. ; Санкт-Петербургский межрегиональный ресурсный центр. - Санкт-Петербург : СПб ГБОУ ДПО "Ресурсный центр", 2019. – 125с.
5. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации / Е. К. Баранова, А. В. Бабаш. - Москва: РИОР ИНФРА-М, 2018. – 334 с.
6. Бубнов А. А. Основы информационной безопасности: учебное пособие / А. А. Бубнов, В. Н. Пржегорлинский, О. А. Савинков. - Москва: Академия, 2017. – 252с.
7. Белобородова Н. А. Информационная безопасность и защита информации: учебное пособие / Н. А. Белобородова. - Ухта: УГТУ, 2016. - 69 с.
8. 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.
9. Вартанов А. А., Лоскутова И. В., Миронов С. Н. Основы администрирования программных средств защиты информации линейки QP: теория и практика: монография / А.А. Вартанов, И.В. Лоскутова, С.Н. Миронов. -

Москва: Радиотехника, 2018. - 163 с.
10. Ермаков А. В., Гойхман В. Ю. Информационная безопасность. Сетевая безопасность, Firewall, сетевые атаки, криптографическая защита информации: учебное пособие / А. В. Ермаков, В. Ю. Гойхман. - Якутск: СВФУ, 2019. - 75 с.
11. Ильин М. Е., Калинкина Т. И., Пржегорлинский В. Н. Криптографическая защита информации в объектах информационной инфраструктуры : учебник / М. Е. Ильин, Т. И. Калинкина, В. Н. Пржегорлинский. - Москва: Академия, 2020. – 283с.
12. Стреканова Д.С. Персональные данные: учебный курс / Колованги С.В.: СПб: Питер, 2020. – 239с.
13. Информационные технологии и защита персональных данных: общедоступная информация, распространение информации, документирование информации, порядок ограничения доступа к копиям заблокированных сайтов. - Москва : Профиздат, 2017. – 79с.
14. Королев Е. Н. Администрирование операционных систем: учебное пособие / Е. Н. Королев. - Воронеж: Воронежский государственный технический университет, 2017. - 85 с.
15. Крамаров С. О., Митясова О. Ю., Соколов С. В. Криптографическая защита информации : учебное пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов. - Москва: РИОР : ИНФРА-М, 2018. – 319 с.
16. Мазнин Д. Н., Баранкова И. И., Михайлова У. В., Илларионова Д. А. Организация обработки и защиты ПДн в : учебное пособие / Д. Н. Мазнин, И. И. Баранкова, У. В. Михайлова, Д. А. Илларионова. - Магнитогорск : ФГБОУ ВО "МГТУ им. Г. И. Носова", 2019. – 105с.
17. 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.- 564с.
18. Михалевич Е.В. Обработка персональных данных: анализ законодательства и судебной практики / Е.В. Михалевич. - Москва: ФГБУ "Редакция "Российской газеты", 2019. - 143 с.
19. 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
20. Никифоров С. Н. Защита информации: учебное пособие / С.Н. Никифоров. - Санкт-Петербург: СПбГАСУ, 2017. - 76 с.
21. 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.
22. Овчинникова Т. А. Ответственность за нарушение требований законодательства РФ о персональных данных: монография / Т. А. Овчинникова. - Хабаровск: Изд-во ТОГУ, 2018. – 81с.
23. Полегенько А. М. Защита информационных систем обработки персональных данных : учебное пособие / А. М. Полегенько. - Санкт-Петербург : Изд-во Санкт-Петербургского государственного экономического университета, 2018. - 72 с.
24. Романов В. Г. Персональные данные: проблемы правовой охраны и защиты: монография / В. Г. Романов. - Чита : ЗабГУ, 2019. - 302 с.