Тип работы: ВКР (Выпускная квалификационная работа)

Предмет: Юриспруденция

2. Проблемы реализации информационных прав личности в России

2.1 Защита персональных данных

Сегодня невозможно представить деятельность какой-либо организации без хранения и обработки данных о человеке. Организация может хранить данные о своих сотрудниках, о клиентах или контрагентах. Защита персональных данных является на сегодняшний день одним из важных направлений в обеспечении информационной безопасности большинства организаций. Личные данные могут представлять большую ценность. Они могут служить и орудием преступления или использоваться в конкурентной борьбе между компаниями. Поэтому персональные данные нуждаются в профессиональной защите.
К персональным данным относится информация, которую человек может предоставить о себе сам или данные, которые позволяют однозначно идентифицировать человека. Это могут быть: фамилия, имя, отчество, дата рождения, место рождения, адрес, семейное положение, данные о владении имуществом, образовании, доходах и т.д.
Персональные данные разделяются на следующие категории:
- 1 группа. Информация о расовой и национальной принадлежности, о религиозных и политических убеждениях, о состоянии здоровья.
- 2 группа – биометрические данные. Данные характеризующие физические данные человека. Это могут быть фотографии, отпечатки пальцев.
- 3 группа – общедоступные данные. Это сведения о человеке, которые предоставлены самим человеком.
- 4 группа – иные категории данных, которые не попадают в первые три группы.
Уровень защищенности персональных данных – это комплексный показатель, который отражает выполнение требований по нейтрализации угроз безопасности информационных систем, хранящих персональные данных
Требования к защите персональных данных в информационных системах установлены Постановлением правительства РФ от 01.11.2012 №119. Согласно постановлению, существует три типа угроз:
- Угрозы 1-го типа. Связаны с наличием в системном программном обеспечении возможностей, которые не оговорены в документации к нему.
- Угрозы 2-го типа. Связаны с наличием в прикладном программном обеспечении возможностей, которые не оговорены в документации к нему.
- Угрозы 3-го типа. Не связаны с наличием недокументированных возможностей в прикладном ПО.
Оценку уровня угроз осуществляют эксперты в области информационной безопасности. Сначала необходимо определить для информационной системы уровень актуальных угроз. Далее в зависимости от выявленного уровня необходимо выполнить ряд мер по организации защиты. Меры по организации защиты персональных данных условно можно разделить на три уровня:
- Административный уровень – назначение должностных лиц, разграничение ответственности, утверждение документов.
- Прикладной уровень – меры, которые осуществляются программными методами внутри самой информационной системы.
- Системный уровень – меры, которые осуществляются программными и аппаратными методами на уровне сети и операционной системы.

Административные меры:
1. Обеспечить безопасность помещений.
2. Обеспечить сохранность носителей с данными.
3. Утвердить документально перечень лиц, которые могут иметь доступ к данным, хранящимся в информационной системе, с целью выполнения служебных обязанностей.
4. Проверить сертифицированы ли используемые средства защиты информации.
5. Назначить должностных лиц или отдельную структуру (отдел безопасности), ответственных за обеспечение безопасности персональных данных.
В информационных системах должны применяться следующие способы защиты информации:
- Пароли при записи в базу данных шифруются. Чаще всего для этого используется метод md5. Например, вместо пароля «abs32» в базу запишется строка «d912d688926b43c9d0a2bd9dd9946bb5». Даже если злоумышленник получит доступ к базе данных пользователей с паролями, то восстановить пароль по шифру практически невозможно.
- Ограничение минимальной длины пароля и проверка надежности пароля с целью исключения подбора пароля. Единственным способом получить пароль по шифру md5 является получение баз данных стандартных паролей. Допустим, шифр пароля «12345» давно известен злоумышленникам. Поэтому с целью повышения надежности нужно создавать нестандартные пароли. Они должны быть не короче определенной длины, содержать буквы в разных регистрах и цифры.
- Информационная система должна быть снабжена средствами защиты от подбора пароля.
- Должна быть запрещена на техническом уровне работа нескольких пользователей в системе под одним и тем же логином.
- Права доступа пользователей должны настраиваться лично уполномоченным администратором системы.
- Пользователи не должны иметь прямого доступа в систему управления базами данных.
- Должна быть продумана политика управления сеансами пользователей. Например, при отсутствии активности в течении определенного времени сеанс автоматически завершается.
- Диапазона IP-адресов, с которых разрешен вход в систему, должен быть ограничен.
- Объекты системы должны храниться исключительно на серверах. Хранение на персональном компьютере пользователя должно быть исключено.
На системном уровне для защиты информации следует пользоваться сертифицированными межсетевыми экранами и антивирусным ПО. Межсетевой экран (файрвол, брандмауэр) это аппаратный и программный комплекс, который осуществляет контроль и фильтрацию проходящих через него сетевых пакетов. Контроль и фильтрация проводятся в соответствии с настраиваемыми правилами.
Основная функция межсетевого экрана – защита узлов сети от несанкционированного доступа. Типичными функциями межсетевого экрана являются:
- Фильтрация доступа к различным службам.
- Препятствование получению информации из подсети.
- Препятствование внедрению в защищенную подсеть несанкционированных данных.
- Контроль доступа к узлам сети.
- Регистрация всех попыток доступа извне и изнутри.
- Регламентирование порядка доступа к сети.
- Уведомление о подозрительной деятельности, попытках атак на узлы сети или сам межсетевой экран.
Федеральная служба по техническому и экспортному контролю (ФСТЭК) разработала и утвердила реестр сертифицированных межсетевых экранов, которым следует руководствоваться при выборе средств информационной защиты.
Другим важным средством предотвращения утечки личных данных является защита от вирусов. Именно вирусные программы часто занимаются воровством информации и организацией скрытых каналов утечки. Современные антивирусные программы включают в себя следующие функции:
- Сигнатурная защита – быстрое реагирование на вторжение.
- Поведенческий анализ программ.
- Экраны на уровне приложений.
- Контроль целостности важных для операционной системы данных.
Вопросы охраны тайной информации, допускаемые для сотрудников предприятия, можно найти в Трудовом кодексе РФ.
Стоит обратить внимание и на обязанности работника в соответствии ТК РФ: ознакомление работника с его трудовыми обязанностями под расписку, если сотрудник имеет доступ к закрытой информацией

(работодатель - сотрудник); изучение и соблюдение режима коммерческой, тайны и мер ответственности за несоблюдение (для сотрудника); создать работнику необходимые условия для соблюдения, им установленного работодателем режима коммерческой тайны (для работодателя).
Конфиденциальное делопроизводство требует особой организации работы по сравнению с открытым. Рассмотрим некоторые аспекты работы с конфиденциальными документами.
• Во-первых, приказом руководителя назначается должностное лицо, отвечающее за работу с документами, содержащими конфиденциальные сведения. Если в организации большой поток документов конфиденциального характера, то создается целое подразделение, отвечающее за работу с ними.
• Во-вторых, работники

1. Окинавская хартия глобального информационного общества, принятая главами государств и правительств 22 июля 2000 года // Официальный сайт Президента России. Режим доступа: http://archive.-kremlin.ru/te- xt/docs/2000/07/123786.shtml
2. Женевская Декларация принципов построения информационного общества 12 декабря 2003 года // Официальный сайт Межрегионального Центра библиотечного содружества. Режим доступа: http://mcbs.rn-/documents/5/45
3. Об информации, информационных технологиях и о защите информации: федеральный закон: принят Государственной думой 8.07.2006 г. № 149-ФЗ // Собрание законодательства Российской Федерации. 2006. № 31. Ст. 3448.
4. О государственной тайне: закон РФ от 21.07.1993 г. № 5485-1 // Собрание законодательства Российской Федерации. 1997. № 41. Ст. 4637.
5. О персональных данных: федеральный закон от 27.07.2006 г. № 152-ФЗ // Собрание законодательства Российской Федерации. 2006. № 31. Ст. 3448.
6. О коммерческой тайне: федеральный закон: принят Государственной думой 9.07.2004 г. № 98-ФЗ // Собрание законодательства Российской Федерации. 2004. № 32. Ст. 3283.
7. О банках и банковской деятельности: федеральный закон от 03.02.1996 г. № 17-ФЗ // Собрание законодательства Российской Федерации. 1996. № 6. Ст. 492.
8. Об аудиторской деятельности: федеральный закон: принят Государственной Думой 24.12.2008 г. № 1502-5-ФЗ // Собрание законодательства Российской Федерации. 2009. № 1. Ст. 15.
9. О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства: федеральный закон № 119-ФЗ от 20.08.2004 г. // Собрание законодательства Российской Федерации. 2004. № 34. Ст. 3534.
10. Об адвокатской деятельности и адвокатуре Российской Федерации: федеральный закон от 31.05.2002 № 63-ФЗ // Собрание законодательства Российской Федерации. 2002. № 23. Ст. 2102.
11. Об основах охраны здоровья граждан в Российской Федерации: федеральный закон от 21.11.2011 г. № 323-ФЗ // Собрание законодательства Российской Федерации. 2011. № 48. Ст. 6724.
12. О средствах массовой информации: закон РФ от 27.12.1991 № 2124-1 // Российская газета. 1992. № 32.
13. Доктрина информационной безопасности РФ, утверждена Президентом РФ № Пр-1895 от 09.09.2000
14. Распоряжение Правительства РФ «Об утверждении Концепции открытости федеральных органов исполнительной власти» № 93р от 30.01.2014
15. Распоряжение Правительства РФ «Об утверждении Стратегии развития отрасли информационных технологий в РФ на 2014 - 2020 годы и на перспективу до 2025 года» № 2036-р от 01.11.2013
16. Указ Президента РФ «О дополнительных гарантиях прав граждан на информацию» № 2334 от 31.12.1993 (ред. от 01.09.2000).
17. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (ред. от 21.07.2014).
18. Федеральный закон «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» от 09.02.2009 № 8-ФЗ (ред. от 28.12.2013).
19. Федеральный закон «Об организации предоставления государственных и муниципальных услуг» № 210-ФЗ от 27.07.2010 (ред. от 21.07.2014).
20. Протокол Правительственной комиссии «Об утверждении методических рекомендаций по реализации принципов открытости в федеральных органах исполнительной власти» № АМ-П36-89пр. от 26.12.2013
21. Автаева Н.О., Зудин Д.И. Государственная информационная политика в области СМИ // Вестник Нижегород. ун-та им. Н.И. Лобачевского. Сер.: Социальные науки. - 2010. - № 3(19). - С. 17.
22. Брекендридж Д. PR 2.0: Новые медиа, новые аудитории, новые инструменты. - М.: Эксмо, 2009. - 56 с.

23. Быков И.А., Филатова О.Г. Технологии Веб 2.0 и связи с общественностью: смена парадигмы или дополнительные возможности? // Вестник Санкт-Петерб. ун-та. - 2011. - Сер. 9, № 2. - С. 233.
24. Василенко И. Связь с общественностью в государственных организациях и местных органах власти: западный опыт // Проблемы теории и практики управления. - 2003. - № 4.- С. 2-4.
25. Лекторова Ю.Ю. Официальный сайт органа власти в системе государственной информационной политики // Информационное общество. - 2016. - № 3. - С. 20.