СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Современное стремительное развитие информационных технологий предъявляет новые требования к хранению и обработке данных, в том числе конфиденциальных. От традиционных носителей информации и от выделенных серверов компании и частные лица постепенно переходят к дистанционным технологиям. Однако переход к распределенному хранению данных в глобальной сети требует построения системы эффективной защиты данных.

Кроме того, проблема защиты конфиденциальных данных приобрела особую значимость с вступлением в силу в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Информационные системы сбора, хранения, обработки иди передачи данных должны строго соответствовать требованиям, обозначенным в Положении об обеспечении безопасности конфиденциальных данных при их обработке в информационных системах, совместном Приказе ФСТЭК России, ФСБ России, Мининформсвязи России 2008 г. № 55/86/20, а также в методических документах ФСТЭК России и ФСБ России.

Исследование вопросов безопасности конфиденциальных данных и разработка системы их защиты приобретают особую важность и актуальность, так как информации, обрабатываемая российскими компаниями, стремительно растет, а отсутствие строго контроля может привести к высоким рискам утечки персональных данных.

Объект исследования – конфиденциальные данные СРО «РусСтрой», функционирующих в глобальной сети Интернет.

Предмет исследования – процесс защиты конфиденциальных данных СРО «РусСтрой», функционирующих в глобальной сети Интернет.

Цель исследования - на основе анализа методов информационной безопасности и исследования исходной защищенности информационной

среды разработать систему защиты конфиденциальных данных СРО, функционирующих в глобальной сети Интернет.

Для достижения цели исследования необходимо решения ряда задач:

1. Провести обзор литературы и Интернет-источников по вопросам организации защиты персональных данных.
2. На основе анализа особенностей защиты конфиденциальных данных в Интернете и информационной системы обработки и хранения конфиденциальных данных построить модель нарушителя.
3. Провести анализ возможных мер по обеспечению безопасности конфиденциальных данных СРО, функционирующих в глобальной сети Интернет.
4. Разработать систему по обеспечению безопасности конфиденциальных данных СРО, функционирующих в глобальной сети Интернет.
5. Дать экономическое обоснование проекта.

Методы исследования: анализ, синтез, изучение источников информации, диагностика.

Вопросам защиты конфиденциальных данных, в том числе распространяемых посредством сети Интернет, посвящены работы многих авторов. Например, вопросы утечки информации по техническим каналам рассмотрены в учебном пособии «Техническая защита информации» автора Хорев А.А. Такими угрозами могут стать внедрение вредоносного программного обеспечения от неблагонадежных сайтов, задержка коммуникаций в связи с перегрузкой канала, утечка информации, атаки на вычислительную систему и т.д. [1]

В учебном пособии Барабаш П.А. «Безопасность персональных данных» раскрываются аспекты правовой, организационной и инженерно-технической защиты конфиденциальных данных[2].

---

[1] Хорев А.А. Технические каналы утечки информации. – М.:Аналитика, 2012. – 435с.
[2] Барабаш П.А. Безопасность персональных данных. Учебное пособие. – СПб.: Политехника, 2012. – 167с.

Вопросам построения систем защиты при доступе к Интернет-ресурсам посвящены работы таких авторов, как Бородакий В.Ю. (рассматривает вариант безопасного хранения ресурсов средствами облачных технологий)[3]; Щеглов А.Ю. (проводит анализ методов и средств защиты компьютерной информации от несанкционированного доступа)[4], Хореев П.В. (анализирует технические меры защиты информации)[5].

Данное исследование отличается тем, что включает в себя построение модели нарушителя безопасности конфиденциальных данных, которая может стать основой для выбора эффективных средств защиты. Кроме того, в работе раскрываются вопросы применения технических и организационных мер по обеспечению безопасности персональных данных СРО, функционирующих в глобальной сети Интернет.

Практическое применение результаты исследования могут найти при построении системы эффективной защиты персональных данных в СРО «РусСтрой», а также в других организациях, функционирующих в глобальной сети Интернет.

Диплом состоит из введения, трех глав и заключения. Первая глава – теоретическая, посвящена вопросам определения конфиденциальных данных и методов их защиты. Вторая глава – практическая, содержит анализ возможных мер по защите конфиденциальных данных и описание возможной системы их защиты. Третья глава – экономическая, включает экономическое обоснование проекта.

---

[3] Бородакий В.Ю. Практика и перспективы создания защищенного информационно-вычислительного облака на основе МСС ОГВ / В.Ю. Бородакий, А.Ю. Добродеев, П.А. Нащекин // Актуальные проблемы развития технологических систем государственной охраны, специальной связи и специального информационного обеспечения: VIII Всероссийская межведомственная научная конференция: материалы и доклады (Орел, 13–14 февраля 2013 г.). – В 10 ч. Ч.4 / Под общ. ред. В.В. Мизерова. – Орел: Академия ФСО России, 2013.

[4] Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. — СПб.: Наука и техника, 2014. — 384 с.

[5] Хореев П.В. Методы и средства защиты информации в компьютерных системах. – М.: Издательский центр «Академия», 2013. –205с.

ЗАКЛЮЧЕНИЕ

Вопросы безопасности при обработке конфиденциальных данных, хранение которых организовано средствами сервисов глобальной сети Интернет, остаются актуальными, так как распределенная среда предоставляет широкий круг возможностей реализации атак.

При решении размещения конфиденциальных данных в сети Интернет руководители предприятий должные обязательно учитывать проблему защиты информации. Значимость данного вопроса обусловлена и критической важностью информационных ресурсов, и необходимость строго соответствия нормативно-правовым актам, регулирующих отношения в этой сфере.

В рамках дипломного исследования были рассмотрены особенности защиты конфиденциальных данных, хранимых средствами сети Интернет. Выявлены такие проблемы, как необходимость строгого контроля и управления удаленными серверами, выполнение обязательств по охране данных поставщиками услуг. Названные проблемы усугубляются еще и тем фактором, что размещая информацию в публичном сервисе, пользователи не всегда могут контролировать уровень ее безопасности.

В работе проведен анализ возможных способов удаленного хранения данных. Так, определено, что организация хранения данных возможна на виртуальных серверах (тогда обеспечение безопасности становится обязанностью поставщика услуг) или на выделенных корпоративных серверах (в этом случае безопасность ресурсов обеспечивают специалисты компании). Так же рассмотрены возможные атаки на сетевые ресурсы и выявлены элементы, являющиеся наиболее уязвимыми. К ним можно отнести канал связи, Web-сервер, клиентские компьютеры, серверы баз данных, корпоративные серверы и т.д. Проведен анализ и оценка рисков при доступе к Интернет-ресурсам и даны рекомендации по определению областей доверия.

Для разработки системы защиты при конфиденциальных данных проведено тестирование некоторых программных продуктов с целью выбора оптимального решения по защите информации. Объектами экспериментального исследования стали сетевые экраны и антивирусные программы. По результатам тестирования были даны рекомендации по установке Comodo или Bitdefender в качестве брандмауэра и Kaspersky Internet Security, Dr.Web Security Space или Bit Defender Internet Security в качестве антивирусной программы. На основе обзора предлагаемых решений по организации идентификации и аутентификации было внесено предложение о покупке и дальнейшем использовании USB-ключей или смарт-карт eToken. Рассмотрены также принципы построения систем обнаружения и предотвращения вторжений и утечки информации с целью их дальнейшей реализации.

Таким образом, можно сделать вывод о достижении цели и решении задач, определенных во введении.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Источники

1. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) «О персональных данных» (с изм. и доп., вступ. в силу с 01.09.2015)
2. 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»

Литература

3. Хорев А.А. Технические каналы утечки информации. – М.:Аналитика, 2012. – 435с.
4. Барабаш П.А. Безопасность персональных данных. Учебное пособие. – СПб.: Политехника, 2012. – 167с.
5. Бородакий В.Ю. Практика и перспективы создания защищенного информационно-вычислительного облака на основе МСС ОГВ / В.Ю. Бородакий, А.Ю. Добродеев, П.А. Нащекин // Актуальные проблемы развития технологических систем государственной охраны, специальной связи и специального информационного обеспечения: VIII Всероссийская межведомственная научная конференция: материалы и доклады (Орел, 13–14 февраля 2013 г.). – В 10 ч. Ч.4 / Под общ. ред. В.В. Мизерова. – Орел: Академия ФСО России, 2013.
6. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. — СПб.: Наука и техника, 2014. — 384 с.
7. Хореев П.В. Методы и средства защиты информации в компьютерных системах. – М.: Издательский центр «Академия», 2013. –205с.
8. Формирование информационного общества в XXI веке./Сост.: Е.И.Кузьмин, В.Р.Фирсов - СПб.: РНБ, 2010. - 640 с.

9. Букин С.О. Безопасность банковской деятельности: Учебное пособие. – СПб.: Питер, 2011. – 288с.

10. Молдовян А.А., Молдовян А.Н. Безопасность глобальных сетевых технологий. — СПб.: БХВ-Петербург, 2011. — 320 с.

11. Скиба В. Ю., Курбатов В. А. Руководство по защите от внутренних угроз информационной безопасности, СпБ, Питер, 2011 г.- 320 с.

12. Лебедь С. В., Межсетевое экранирование: Теория и практика защиты внешнего периметра, Издательство Московского технического университета им. Баумана, 2012. - 304 с.

13. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах. – М.: Форум, Инфра-М, 2010. – 592 с.

14. Дудихин В.В., Дудихина О.В. Конкурентная разведка в Internet. Советы аналитика – М:. ДМК Пресс, 2012. – 192 с.

15. Малюк А.А, Пазизин С.В, Погожин Н.С. Введение в защиту информации в автоматизированных системах. – М.: Горячая Линия - Телеком, 2011. – 146 с.

16. Исаев А.С., Хлюпина Е.А. «Правовые основы организации защиты персональных данных» – СПб: НИУ ИТМО, 2014. – 106 с.

17. Стефаров А.П., Жуков В.Г., Жукова М.Н. Модель нарушителя прав доступа в автоматизированной системе // Прогр. продукты и системы. – 2012. – № 2. – С. 51-54.

18. Гришина Н. В. Организация комплексной системы защиты информации. -- М.: Гелиос АРВ, 2009. - 256 с.

19. Платонов В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей. Учебное пособие. — М.: Академия, 2012. — 240 с.

Электронные ресурсы

20. Аверченков В.И. Защита персональных данных в организации: монография [Электронный ресурс]/ В.И.Аверченков, М.Ю.Рытов, Т.Р.Гайнулин. – 2-е изд., стереотип. – М.:Флинта, 2011. – 124с.

21. «Способ удобного шифрования данных в облаке (собственными средствами)» [Электронный ресурс]. URL: http://habrahabr.ru/post/241720/

22. «Стандарты информационной безопасности» [Электронный ресурс]. URL: http://www.arinteg.ru/articles/standarty-informatsionnoy-bezopasnosti-27697.html

23. Комплексная система защиты персональных данных в распределенной информационной системе [Электронный ресурс]. URL: http://knowledge.allbest.ru/programming/2c0a65635a2ad78b4c43a88521206d37_2.html