

уровне) виртуальной средой расхода ресурсов, который включает один или более накопителей информации, доступных для машинного считывания, а также программные инструкции, сохраненные на хотя бы одном или более накопителе информации ...»).

В пунктах 7-12 этого же патента уже патентуется компьютерная система, но в данной формуле на первом месте стоит всё-таки программа, а реализующая её аппаратура – на втором.

Что же касается патентов, где в формулах изобретений на первом месте стоят способ и аппаратура для его реализации, а на втором – патентуемый программный продукт, то таких патентов много. Пример – американский патент [12], формула изобретения которого состоит из двадцати пунктов, а в пунктах 20 и 21 указано, что «...What is claimed is:

20. A computer program product, which comprises a plurality of program commands for controlling a program development system, the plurality of program commands being stored on a physical medium, ... (патентуется программный продукт, включающий в себя множество программных команд для управления системой разработки программ, где множество программных команд сохраняется на физическом носителе ...).

21. A computer program product, which comprises a plurality of program commands for controlling a portable data carrier, the plurality of program commands being stored on a physical medium, the program commands being set up so as to cause the portable data carrier... (патентуется программный продукт, включающий в себя множество программных команд для управления переносным носителем информации, где множество программных команд хранится на физическом носителе, будучи настроенными так, что бы заставить переносной носитель информации...).

В докладе сравниваются и обсуждаются возможности патентования баз данных и компьютерных программ в США и в Республике Беларусь и поддерживается предложение автора [13] рассмотреть вопрос о создании вспомогательной системы правовой охраны компьютерных программ и баз данных, которая бы учитывала их специфику, а также недостатки и недостаточность охраны средствами как патентного, так и авторского права.

Список использованных источников:

1. Крюкова, Э. П., Швед П. Я. Обзор законодательства Республики Беларусь в области защиты прав в отношении информации // Компьютерная преступность и информационная безопасность / Под общ. ред. А. П. Леонова – Мн.: Арил, 2000. – Гл. 2. – С. 143-184.
2. Авторское право в Internet: виртуальная реальность ... [Электронный ресурс] – Режим доступа: idea.rinet.by/?opinion&id=3. – Дата доступа: 15.03.2015.
3. Сайт НЦИС [Электронный ресурс] – Режим доступа: http://www.belgopatent.org.by/index.php?option=com_content&view=article&id=186&Itemid=74. – Дата доступа: 15.03.2015.
4. Виды объектов интеллектуальной собственности. Правовое регулирование и охрана в сети интернет... [Электронный ресурс] – Режим доступа: pravovedenie.by/vidy-obektov-intellektualnoj-sobstvennosti-pravovoe-g-... – Дата доступа: 15.03.2015.
5. Мамяофа, И. Э. Проблема охраны алгоритмов и вычислительных программ в зарубежном патентном праве // Вопросы изобретательства. / И. Э. Мамяофа. – 1968. - № 1. – С. 25-30.
6. Титов, А. П. Правовая охрана программного обеспечения ЭВМ : дис. ... канд. юрид. наук: 12.00.03 / А. П.Титов ; Ин-т государства и права Нац. акад. наук Беларуси. – Минск, 2001. – 117 л.
7. Попова, И. В. Программа для ЭВМ в системе объектов авторского права : дис. ... канд. юрид. наук: 12.00.03 / И. В.Попова ; Ин-т философии и права Нац. акад. наук Беларуси. – Минск, 1999. – 115л.
8. Виталиев, Г. В. Правовая охрана программ для ЭВМ и баз данных ... [Электронный ресурс] – Режим доступа: www.relcom.ru/Archive/1997/ComputerLaw/Soft_law.htm. – Дата доступа: 15.03.2015.
9. Карелина, М. М. Судебная защита прав авторов программ для ЭВМ и баз данных [Электронный ресурс] – Режим доступа: www.internet-law.ru/intlaw/avtpravo.html. – Дата доступа: 15.03.2015.
10. Симкин, Л. С. Программы для ЭВМ: правовая охрана. Правовые средства против компьютерного пиратства / Л. С. Симкин. – М.: Городец, 1998. – 207 с.
11. United States Patent 8,327,376. Using smart objects in a virtual universe to conserve computing resources (Использование интеллектуальных объектов в виртуальной среде для для сохранения уровня расхода вычислительных ресурсов), дата публикации December 4, 2012.
12. United States Patent 8,296,719. Software factory readiness review (Обзор готовности программной фабрики (билд-машины)), дата публикации January 11, 2013.
13. Правовая охрана компьютерных программ: проблемы и и пути их решения. Дубицкий В. М. [Электронный ресурс] – Режим доступа: center.gov.by/articleDubitski.html. – Дата доступа: 15.03.2015.

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В БИБЛИОТЕКАХ БЕЛОРУССКОЙ ЖЕЛЕЗНОЙ ДОРОГИ

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Зайкина И.С.

Рассматриваются меры по защите информации и персональных данных в научно-технических библиотеках Белорусской железной дороги.

Одним из главных приоритетов работы любой информационной системы является обеспечение информационной безопасности для обрабатываемых данных. Информационная система, объединяющая все научно-технические библиотеки дороги в единое информационное пространство (далее – информационная система библиотек БелЖД), дает доступ предприятиям дороги к своим программам через централизованный сервер персональных данных.

Проблема персональных данных, которую породило бурное развитие информационных технологий, заключается в несанкционированном использовании персональных данных граждан (в данном случае читателей научно-технических библиотек дороги) в различных целях, начиная от рассылки спама и телефонного маркетинга, заканчивая несанкционированным дебетованием средств с пластиковых карточек и различных форм мошенничества [1]. Информационная система библиотек БелЖД обеспечивает все необходимые меры по защите информации и персональных данных [2-3], в том числе:

1. Система и программные средства имеют фрагментарную архитектуру построения, при которой учетные данные, библиографическая информация и персональные данные хранятся в различных местах. Доступ к системе осуществляется кластерным способом – через единую точку входа в рамках корпоративной сети. В целях минимизации угроз безопасности обработки данных в системе существует возможность выбора одной из схем развертывания (её исполнения), отличающихся по месту расположения демографического сервера и иной информации, а также каналов подключения.

2. Для использования программного обеспечения требуется ввод имени пользователя и пароля. При регистрации пользователя в системе указываются его роли. В соответствии с ролью пользователя определяется объем прав по работе в программе, в том числе и объем предоставляемых сведений.

3. Ведется учет количества пользователей, допущенных к работе с персональными данными. Возможен мониторинг действий с персональными данными и просмотр результатов действий в журналах событий.

4. Программа представляет собой единую платформу для работы нескольких операторов, однако сведения, занесенные одним из них, могут быть переданы другому только при наличии согласия на то основного оператора. В зависимости от решаемой задачи и роли пользователя, сведения предоставляются либо в неизменном, либо в обезличенном виде.

5. В программе отсутствуют средства разработки и отладки, что гарантирует отсутствие возможности третьих лиц повлиять на среду обработки персональных данных.

6. Система настроена так, что у лиц, работающих в программе, будет отсутствовать возможность пользования программой с автоматизированного рабочего места, находящегося вне контролируемой зоны. Такими гибкими настройками возможно разрешение только такого входящего и исходящего трафика, который является необходимым для работы (с блокированием любого входящего и исходящего трафика, не разрешенного явно). Разграничение доступа на уровне межсетевое взаимодействие выполняется с помощью настроек одного или каскада демографических серверов.

7. Основная точка входа в программу использует защищенные протоколы HTTPS и SSL для предотвращения доступа третьих лиц к передаваемой по каналам информации. SSL является стандартом обеспечения безопасности передаваемых данных между компьютером пользователя и просматриваемым веб-сайтом. Сайты, использующие SSL, предоставляют браузерам сертификаты безопасности для подтверждения их идентификационных данных.

8. Сохранность информации обеспечивается хранением её на серверах платформы Amazon EC2, обеспечивающих доступность и бесперебойность на 99,95% и хранящей до 100 резервных копий обрабатываемой информации. В используемых ресурсах реализуются современные способы обеспечения безопасности.

Опыт эксплуатации информационной системы библиотек БелЖД показал, что утечек персональных данных из системы за последние три года не было.

Список использованных источников:

1. Защита персональных данных: опыт правового ... [Электронный ресурс] – Режим доступа: <http://statut.by/lichnyj-jurist/14-i-have-a-right/184-18-09-2011>. – Дата доступа: 15.03.2015.
2. Корниенко, А. А. Информационная безопасность и защита информации на железнодорожном транспорте: учебник в 2-х частях. Ч. 1. Методология и система обеспечения информационной безопасности на железнодорожном транспорте. / А. А. Корниенко. – М.: УМЦ ИСТ, 2014. – 440 с.
3. Яковлев, В. В. Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта: учебник для вузов ж.-д. транспорта. / В. В. Яковлев, А. А. Корниенко. – М.: УМК МПС России, 2002. – 328 с.

ВЕБ-СЕРВИС МОНИТОРИНГА СОСТОЯНИЯ СЕРВЕРОВ И СЕТЕВОГО ОБОРУДОВАНИЯ КОМПЬЮТЕРНОЙ СЕТИ

*Институт информационных технологий БГУИР,
г. Минск, Республика Беларусь*

Зыцкич М.А.

Лашкевич Е.М. - м.т.н., ст. преподаватель