УДК 004.056

Т.Т. Газизов, А.А. Мытник, А.Н. Бутаков

Типовая модель угроз безопасности персональных данных для информационных систем автоматизации учебного процесса

Рассмотрены информационные системы автоматизации учебного процесса ТГПУ: ИС E-Decanat и ИС Абитуриент. Выявлены типовые уязвимости и угрозы, сопряженные с обработкой персональных данных. Предложены анализ выявления угроз и методы решения по обеспечению безопасности персональных данных для каждой из рассмотренных систем.
Ключевые слова: информационная безопасность, уязвимость информационных систем, защита данных.

Сегодня обработка персональных данных является повседневной задачей, с которой сталкивается большинство работников всех сфер науки и образования [1, 2]. Работа приемной комиссии, кафедр, деканатов любого вуза всегда связана с обработкой и хранением персональных данных студентов. Как правило, для автоматизации действий обработки данных создаются информационные системы. Опыт внедрения и эксплуатации информационных систем показывает, что успешное использование программы для управления учебным процессом позволяет увеличить скорость принятия управленческих решений для большинства задач подразделения [3]. При этом одной из наиболее актуальных задач при проектировании автоматизированных информационных систем является обеспечение безопасности персональных данных при их обработке и защита от несанкционированного вмешательства. Цель данной работы – рассмотреть типовую модель угроз безопасности персональных данных для двух информационных систем автоматизации учебного процесса на примере Томского государственного педагогического университета (ТГПУ). Для описания типовой модели угроз рассмотрим описание и схему работы информационных систем автоматизации учебного процесса ТГПУ: ИС E-Decanat и ИС Абитуриент.

Информационная система E-DECANAT 2.0 предназначена для автоматизации управления учебным процессом ТГПУ. Целью разработки информационной системы E-Decanat является совершенствование деятельности учебных подразделений вуза – деканатов по учету и анализу движения контингента студентов для обеспечения эффективности управленческих решений. ИС E-Decanat 2.0 разработана в соответствие с построенной информационной моделью деканата и реализована с использованием технологии Java на основе клиент-серверной архитектуры. При разработке были использованы: IDE NetBeans, MS SQL Express Edition, СУБД MySQL. Предложенное решение является кроссплатформенным и опирается на открытые стандарты свободного программного обеспечения, что заметно расширяет сферу его применения для нужд высшего профессионального образования.

Совокупность данных в информационной системе подразделена на общие данные, т.е. те, которые обрабатывают различные подразделения вуза, и локальные, которые необходимы только для отдельного деканата с целью достижения баланса нагрузки при обработке и передаче данных. При решении этих задач используются две базы данных, одна из которых размещена в деканате, а другая – на одном из центральных серверов вуза. В центральной базе данных хранится общая информация, необходимая для работы всех факультетов вуза. В локальной базе данных хранится информация, необходимая для работы самого деканата: академические ведомости, учебные планы и другая сопутствующая информация. В роли СУБД используются два решения: MS SQL Server для общей БД и MySQL для локальной БД. Для обработки документов реализована интеграция с офисным пакетом OpenOffice.org с использованием экспорта данных в шаблоны.

Информационная система E-Decanat предназначена для автоматизации учебного процесса и не затрагивает экономическую и хозяйственную деятельность вуза. Информационная система не является изолированной от внешних систем и интегрирована в общую информационную инфраструктуру вуза (рис. 1), где взаимодействует с такими информационными системами, как «Электронная ка-

федра», «Абитуриент», информационная система учета студенческих кадров «A-Cadry», система автоматизации документооборота «A-Delo» [4].

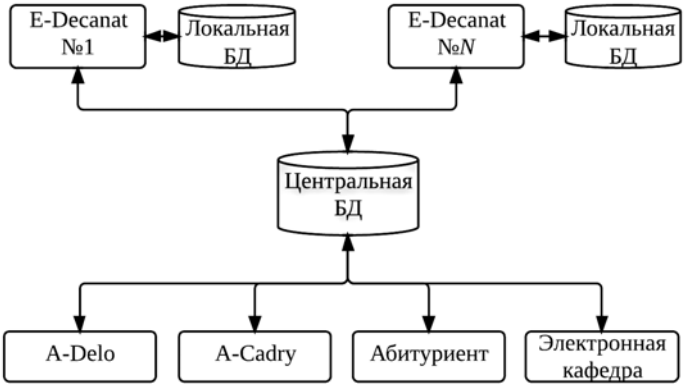

Рис. 1. Функциональная схема «E-Decanat» и «Абитуриент»

Информационная система «Абитуриент» предназначена для контроля знаний студентов ТГПУ. Целью создания информационной системы «Абитуриент» является автоматизация деятельности приемной комиссии ТГПУ [5]. Система располагает возможностями учета личных данных абитуриента и результатов вступительных испытаний, обеспечивает возможность выборки данных с использованием типовых запросов, генерацию отчетов в формате офисных приложений (например, таких, как OpenOffice.Org) [6], автоматическое зачисление и т.д. При разработке системы использовалось следующее программное обеспечение: MS Visual Studio 2008, СУБД MS SQL 2005. Информационная система обеспечивает гибкую настройку профилей и направлений подготовки на факультетах ТГПУ, различные формы конкурсных испытаний без внесения изменения в исходные модули системы. Обеспечивает механизм многопользовательского доступа к данным в соответствии с предопределенными привилегиями. База данных этой системы разделена на две части: информационную и наполняемую. Информационная часть используется для хранения наименований направлений и профилей, количества выделенных бюджетных и целевых мест, конкурсных предметов для каждого профиля. Наполняемая часть состоит из личных данных абитуриента и его конкурсной информации. Система «Абитуриент» интегрирована в общую информационную систему вуза, а также имеет связь с внешней информационной системой «ФИС ЕГЭ» (предназначенной для регистрации пользователей в информационных системах Федеральной службы по надзору в сфере образования и науки).

Рассмотренные информационные системы работают с персональными данными студентов. При обработке ПДн на автоматизированном рабочем месте, имеющем подключения к сетям связи общего пользования и (или) сетям международного информационного обмена, в соответствии с положением ФСТЭК России от 15 февраля 2008 г., возможна реализация следующих угроз безопасности ПД (УБПДн) [7–9]: угрозы утечки информации по техническим каналам; угрозы несанкционированного доступа (НСД) к ПДн, обрабатываемым на автоматизированном рабочем месте. Угрозы утечки информации по техническим каналам включают в себя: угрозы утечки акустической (речевой) информации; угрозы утечки видовой информации; угрозы утечки информации по каналу ПЭМИН. Угрозы НСД в ИСПДн связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн, а также нарушителей, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена. Угрозы из внешних сетей включают в себя: угрозы «Анализа сетевого трафика» с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации; угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.; угрозы выявления паролей; угрозы получения НСД путем подмены доверенного объекта; угрозы типа «Отказ в обслуживании»; угрозы удаленного запуска приложений; угрозы внедрения по сети вредоносных программ.

Функционирование рассмотренных выше информационных систем связано с обработкой персональных данных, отсюда возникает необходимость обеспечения безопасности информации о пер-

сональных данных. При этом, анализируя функциональные схемы представленных ИС, можем выделить наиболее типичные угрозы из типовой модели угроз: sql injection, разглашение служебной информации пользователями; получение удаленного доступа к СУБД; получение физического доступа к серверу СУБД; несанкционированный доступ к данным при передаче по сети. Проведя анализ построения и эксплуатации представленных ИС, а также исследуя особенности их использования в вузе, составим сводную таблицу возможных угроз, методов борьбы с ними а также зонами ответственности (таблица).

Возможные угрозы и методы борьбы с ними

Угроза	Меры предотвращения	Зона ответственности
SQL injection	Использование безопасных запросов, использование хранимых процедур	Разработчик
Разглашение служебной информации пользователями	Профилактическая беседа	Пользователь
Получение удаленного доступа к СУБД	Настройка сервера, ограничение сетевых подключений	Администратор БД, администратор сети
Получение физического доступа к серверу СУБД	Защита от несанкционированного доступа к оборудованию	Служба безопасности
Несанкционированный доступ к данным при передаче по сети	Защищенное соединение между клиентом и СУБД	Разработчик, поставщик СУБД, доверенный центр сертификации

В данной работе была рассмотрена типовая модель угроз безопасности персональных данных применительно к информационным системам автоматизации учебного процесса подразделений вуза, применяемых в автоматизации бизнес-процессов Томского государственного педагогического университета. Были выявлены типовые уязвимости и угрозы, сопряженные с обработкой персональных данных в рассмотренных информационных системах, выбраны методы борьбы с ними, указаны зоны ответственности. Результаты анализа представлены в виде таблицы. В этой связи цель данной работы была достигнута и применены соответствующие решения по обеспечению безопасности персональных данных для каждой из рассмотренных систем.

Литература

1. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»), устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_149747/, свободный (дата обращения: 24.04.2014).

2. Давыдова Е.М. Модель образовательного процесса с учетом требований работодателя // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2013. – № 4 (30). – С. 177–181.

3. Mytnik A.A. Business process automation in university using E-Decanat 2.0 software / A.A. Mytnik, A.P Klishin // The 1th International Global Virtual Conference–Workshop, April 2013. – Zilina: EDIS, 2013. – P. 308–310.

4. Мытник А.А. Опыт внедрения информационной системы E-Decanat для автоматизации управления учебным процессом в ТГПУ / А.А. Мытник, А.П. Клишин // Вестник ТГПУ. – 2013. – Вып. 1 (129). – С. 184–187.

5. Стась А.Н. Информационные системы. – Томск: Изд-во ТГПУ, 2010. – 186 с.

6. Пьяных Е.Г. Проектирование баз данных в среде OpenOffice.org (ПО для управления базами данных): учеб. пособие. – М., 2008. – 62 с.

7. Миронова В.Г. Модель нарушителя безопасности конфиденциальной информации / В.Г. Миронова, А.А. Шелупанов // Информатика и системы управления. – 2012. – № 1. – С. 28–35.

8. Шелупанов А.А., Миронова В.Г., Ерохин С.С., Мицель А.А. Автоматизированная система предпроектного обследования информационной системы персональных данных АИСТ-П // Доклады ТУСУРа. – 2010. –№ 1. – С. 14–22.

9. Авсентьев О.С. Принципы моделирования механизмов воздействия вредоносных программ на защищенные информационные системы в интересах оценки угроз их безопасности / О.С. Авсентьев, В.В. Александров, Г.И. Рябинин, С.В. Скрыль, Р.В. Мещеряков // Доклады ТУСУРа. – 2008. – Т. 2. – № 1. – С. 135–136.

Газизов Тимур Тальгатович
Доцент каф. информатики Томского государственного педагогического университета (ТГПУ)
Тел.: 8 (382-2) 52-11-26
Эл. почта: gtt@tspu.edu.ru

Мытник Антон Александрович
Магистрант каф. информатики ТГПУ
Тел.: 8 (382-2) 52-11-26
Эл. почта: mytnikAA@gmail.com

Бутаков Алексей Николаевич
Аспирант каф. информатики ТГПУ
Тел.: 8 (382-2) 52-11-26
Эл. почта: butakovan@tspu.edu.ru

Gazizov T.T. , Mytnik A.A., Butakov A.N.
Generic Model of Security Threats for Personal Data in regard of Information Systems Dedicated to Academic Planning

Information systems dedicated to automation of academic planning in TSPU called E-Decanat and IS Abiturient are reviewed in the article. Generic vulnerabilities and threats related to processing of personal data are revealed. Ways of analysis related to identifying threats and solutions related to security of personal data for each examined system suggested.
Keywords: Information security, vulnerability of information systems, protection of data.
