УДК 004.056

Д. И. Сачков
кандидат экономических наук, доцент,
Байкальский государственный университет экономики и права
В. Н. Быкова
Байкальский государственный университет экономики и права

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ ДЛЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ*

Прошлое столетие характеризуется бурным развитием информационных технологий. В настоящее время информационное пространство с применением компьютерных систем, позволяющих упростить ежедневный быт, основательно вошло в повседневную жизнь рядового человека, но вместе с этим стало негативным фактором, связанным с безопасностью данных. Использование персональных данных в информационных системах, начиная с социальных сетей и заканчивая поликлиникой, несет в себе опасность разгласить личную информацию. В рамках решения этих проблем был принят Федеральный закон «О персональных данных» № 152-ФЗ. В данной статье рассмотрены вопросы в части процедуры внедрения и трудоемкости процесса приведения персональных данных к требованиям законодательства, а также проведен анализ существующих решений (автоматизированных систем), предназначенных для мониторинга защиты персональных данных. Выявлены причины, по которым компании не выполняют требования законодательства; проанализированы методические рекомендации контролирующих органов (Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации, Роскомнадзор) в области защищенной обработки персональных данных; выделены основные этапы по приведению защиты персональных данных к требованиям законодательства.

Ключевые слова: персональные данные; закон; защита информации; информационные системы; безопасность.

D. I. Sachkov
PhD in Economics, Associate Professor,
Baikal State University of Economics and Law
V. N. Bykova
Baikal State University of Economics and Law

USE OF INFORMATION SYSTEMS FOR PERSONAL DATA PROTECTION*

The last century was characterized by rapid development of information technologies. Currently, the information space with use of computer systems that allow to simplify everyday life has fundamentally entered into day-to-day living of common people, but at the same time it has become a negative factor related to date security. The use of personal data in information systems, beginning from social networks and finishing with a health clinic, comes laden with a danger of disclosing private information. Solution of these problems resulted in enacting the Federal Law «On Personal Data» № 152-ФЗ. This article considers the items in regard to implementation procedures and labor input of process in leading personal data to legislation requirements, as well as makes an analysis of existing solutions (automated systems) designed for monitoring personal data protection. Identifications are given for the reasons why companies do not fulfill the legislation requirements; analysis is made of methodical recommendations of the supervisory bodies (Federal Service for Technical and Export Control, Federal Security Department of the Russian Federation, Federal Service for Supervision

* Статья подготовлена при финансовой поддержке государственного задания № 2014/52 на выполнение работ в сфере научной деятельности в рамках базовой части проекта № 326 «Финансово-бюджетное проектирование как основа управления социально-экономическим развитием ресурсного региона Сибири» (номер госрегистрации в ФГАНУ ЦИТиС 01201458898).

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
2014. № 3
http://eizvestia.isea.ru

in the Sphere of Telecom, Information Technologies and Mass Communications) in the sphere of protected processing of personal data; the stages are outlined for leading personal data protection to legislation requirements.

Keywords: personal data; law; information protection; information systems; security.

Стремительное развитие телекоммуникационных и информационных технологий, а также повсеместное применение вычислительной техники привели к тому, что Интернет прочно вошел в жизнь современного человека. Социальные сети, интернет-магазины, развлекательные игры, портал государственных услуг, интернет-банкинг — вот далеко не полный перечень информационных продуктов, используемых сегодня [7; 8]. Одна из сторон медали, позволяющая современному человеку экономить время при оплате товаров и услуг, получать образование, не выходя из дома, а также находить информацию, необходимую в процессе его жизнедеятельности, с помощью нескольких щелчков мыши. Как известно, есть и другая сторона медали — это информационная безопасность человека, использующего телекоммуникационные технологии. Регистрируясь на различных информационных ресурсах, пользователи вводят сведения о себе (паспортные данные, номера банковских счетов и др.), которые, попадая в руки злоумышленников, могут нанести вред их владельцу.

В настоящее время информация — это очень дорогой продукт, и компании тратят огромные денежные средства и на ее поиск (так называемый промышленный шпионаж), и на организацию собственной безопасности (коммерческая тайна, персональные данные (ПДн), сведения о клиентах и поставщиках и др.). На законодательном уровне государство четко определило, что сбор, хранение и распространение информации о частной жизни лица без его согласия не допускается, в связи с чем требует от организаций и индивидуальных предпринимателей, обрабатывающих ПДн, обеспечить их защиту[1]. Активная деятельность по защите ПДн началась с принятия Федерального закона «О персональных данных» № 152-ФЗ[2] и продолжается до сих пор.

Стоить отметить, что далеко не все организации в полной мере обеспокоились необходимостью применения закона, это подтверждается результатами проверок. В 2012 г. Роскомнадзор передал 5 359 дел в суд на общую сумму 8,9 млн р. Помимо простого невыполнения законодательства в области защиты персональных данных имеет место быть неквалифицированное применение требований закона, но самые негативные последствия влечет за собой формальное применение федерального закона, без включения механизмов защиты в деятельность организации. В связи с этим, защита ПДн является актуальной задачей, а порядок их защиты остается серьезным вопросом, требующим внимательного к себе отношения.

В России более 7 млн юридических лиц и индивидуальных предпринимателей, на которые распространяется действие данного закона. Требования законодательства сейчас практически полностью выполнили организации, относящиеся к крупному бизнесу, а также государственные и муниципальные учреждения (больницы, школы, учреждения социальной защиты и прочие). Большая часть компаний, относящихся к среднему и малому бизнесу, до сих пор серьезно не задумались о выполнении данного закона и не подготовили документацию, отвечающую требованиям закона.

Основными причинами, по которым компании не выполняют требования законодательства и не спешат их реализовать, являются:

– постоянно меняющиеся нормативные акты, запутанность терминологии, юридические коллизии;

[1] Конституция Российской Федерации : принята всенар. голосованием 12 дек. 1993 г. Ст. 23–24.
[2] О персональных данных : федер. закон РФ от 27 июля 2006 г. № 152-ФЗ.

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
2014. № 3
http://eizvestia.isea.ru

– отсутствие в штате квалифицированного юриста по вопросам использования персональных данных;

– высокая стоимость аппаратно-программных средств, обеспечивающих качественную защиту персональных данных;

– отсутствие технических работников (программистов, системных администраторов), которые могут настроить автоматизированную систему в соответствии с требованиями законодательства;

– завышенная цена услуг сторонних организаций (аутсорсинг) по приведению документации и технических средств ко всем требованиям законодательства;

– несоизмеримость штрафов и затрат на подготовку и внедрение системы защиты персональных данных.

Федеральный закон «О персональных данных» был принят в 2006 г., но его вступление в силу откладывалось до 2011 г. За это время разработали множество нормативных актов, которые должны были помочь операторам организовать защиту ПДн в своих автоматизированных системах. Только в 2008 г. появляются следующие документы:

1. Приказ ФСТЭК России, ФСБ России и Министерства информационных технологий и связи Российской Федерации «Об утверждении порядка проведения классификации информационных систем персональных данных»[1] (так называемый «Закон трех»).

2. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, разработанная ФСТЭК России[2].

3. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, разработанных ФСТЭК России[3].

Количество документов, регламентирующих защиту ПДн, увеличивается с каждым годом. Стоить выделить обязательные документы, с которыми должны быть знакомы все операторы ПДн: 2010 г. — приказ ФСБ России и ФСТЭК России № 416/489; 2012 г. — постановление Правительства РФ № 1119; 2013 г. — приказ ФСТЭК России № 21, приказы Роскомнадзора № 274 и № 996, федеральный закон № 99-ФЗ, информационное сообщение ФСТЭК России и др. В 2014 г. планируется принятие новых нормативных документов (проект изменений в ФЗ «О персональных данных» и в Кодексе об административных правонарушениях), ужесточение требований закона, а также увеличение максимального размера штрафа до 700 тыс. р. за невыполнение требований закона «О персональных данных». Таким образом, каждый оператор ПДн обязан соблюдать требования законодательства и отслеживать соответствующие изменения. Вполне логично, что не каждое предприятие среднего и малого бизнеса, а также индивидуальные предприниматели могут позволить себе отдельного юриста, который занимался бы вопросами защиты ПДн работников и клиентов компании.

Анализируя методические рекомендации контролирующих органов (ФСТЭК, ФСБ, Роскомнадзор) в области защищенной обработки ПДн, можно сделать вывод, что выполнить требования законодательства можно, разбив эти требования на несколько этапов [3]. В соответствии с приказом № 21 ФСТЭК России утвердила Состав и содержание организационных и техниче-

[1] Об утверждении порядка проведения классификации информационных систем пер-сональных данных : приказ ФСТЭК России, ФСБ России и Министерства информационных технологий и связи Российской Федерации от 13 февр. 2008 г. № 55/86/20.

[2] Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных : методика ФСТЭК России от 14 февр. 2008 г.

[3] Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных : утв. ФСТЭК России 15 февр. 2008 г.

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
2014. № 3
http://eizvestia.isea.ru

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
2014. № 3
http://eizvestia.isea.ru

ских мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных[1]. Документ позволяет выделить несколько этапов [3; 4] по приведению защиты ПДн к требованиям законодательства:

1. *Организационные мероприятия*. Целью данного этапа является назначение ответственного лица, в обязанности которого входят взаимодействие с субъектами, третьими лицами и регулирующими органами по вопросам передачи и получения, обработки и обеспечения безопасности ПДн. Результатом выполнения данного этапа служат внутренние документы компании (например, приказ о назначении ответственного за организацию работ по защите ПДн).

2. *Определение класса информационной системы персональных данных* (ИСПДн). На этом этапе в зависимости от структуры информационной системы, категорий и объема обрабатываемых ПДн определяется класс информационной системы. Результатом данного этапа является сформированный акт классификации, в котором отражены категория, объем, класс, а также характеристики ИСПДн.

3. *Формирование модели угроз*. Обеспечение безопасности ПДн достигается, в частности, определением угроз безопасности ПДн при их обработке в ИСПДн и формированием на их основе моделей угроз с целью их последующей нейтрализации [5]. Для формирования требований к системе защиты ПДн необходимо построить частные модели угроз безопасности ПДн для каждой из выделенных в компании ИСПДн. Результат этапа — документы «Частные модели угроз» и «Модели нарушителя безопасности ПДн».

4. *Техническая реализация требований по защите ПДн*. На этом этапе особое внимание удаляется внедрению аппаратно-программных средств, позволяющих нейтрализовать актуальные угрозы. При проектировании системы безопасности требуется рассмотреть различные угрозы, которые могут возникнуть (например, угроза загрузки с внешних носителей информации; выявление уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационной системы; угроза несанкционированного доступа и др.).

Стоит заметить, что для организации защиты ПДн первые 3 пункта методических рекомендаций требуют только организационных решений без затрат на материальные ресурсы, чего нельзя сказать о п. 4 «Техническая реализация требований по защите ПДн». Таким образом определяется целесообразность внедрения/установки аппаратных средств защиты ПНд (например, Secret Net, который поддерживает процедуры идентификации и аутентификации; электронный замок «Соболь») и программных средств (например, средства антивирусной защиты, защиты от вторжений и средств имитации, межсетевые экраны и пр.).

Принятие данного закона повлияло также на то, что многие компании, разрабатывающие программное обеспечение, начали внедрение программных продуктов (решений), позволяющих при небольших денежных и временных затратах выполнить требования законодательства (по сравнению с услугами, которые оказывают компании-лицензиаты по защите информации). Разработчики программ для защиты ПДн предлагают различный функционал, от которого зависит уровень защищенности ИСПДн: в некоторых решениях — это только скрытие и/или блокировка файлов и папок или разработка полного комплекта документов, регламентирующих выполнение требований закона; у других — полноценное шифрование, у третьих — от разработки организационно-распорядительных документов до настройки внедрения и страхования финансовых рисков.

[1] Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : приказ ФСТЭК России от 18 февр. 2013 г. № 21.

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
2014. № 3
http://eizvestia.isea.ru

Программное обеспечение, обеспечивающее безопасность ИСПДн, обязано пройти сертификацию на соответствие требованиям закона «О персональных данных» и получить сертификат соответствия ФСТЭК России.

Программные решения, которые обеспечивают выполнение требований законодательства, можно разделить на следующие группы:

1. Документированные — позволяют подготовить организационно-распорядительную документацию, которую запрашивает регулятор (Роскомнадзор) при документарной проверке. Как правило, это веб-сервисы, позволяющие пользователю в режиме онлайн решить вопрос подготовки документации. Такие сервисы реализованы по принципу анкетирования с дальнейшим формированием перечня необходимых документов (приказов, положений, планов работ, журналов учета и т. д.).

2. Программно-аппаратные — рекомендуют программные средства для защиты ПДн, исходя из особенностей ИСПДн. Функционал автоматизированных систем данной группы значительно отличается от функционала веб-решений первой группы. Данные системы, работающие также по принципу анкетирования, разрабатывают комплект документов, регламентирующих вопросы обработки и защиты ПДн, но кроме этого и формируют рекомендации по выбору аппаратно-технических средств защиты информации.

3. Комплексные — позволяют выполнить технические требования законодательства для ИСПДн любого класса. Следует отметить, что данные решения имеют обязательную сертификацию ФСТЭК России или ФСБ России. И здесь функционал различных аппаратно-программных комплексов существенно различается в зависимости от целей и задач [1; 2].

Если с программными решениями, относящимися к первым двум группам, все понятно, так как их использование рассчитано на пользователей, не обладающих высокими компетенциями в области информационной безопасности, то решения третьей группы необходимо детально проанализировать. Здесь стоит обратиться к приказу ФСТЭК России «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18 февраля 2013 г. № 21. Данный документ направлен на реализацию нормы ч. 4 ст. 19 Федерального закона «О персональных данных», определяет 15 мер и дает их детальное содержание.

В данной статье на основе приказа ФСТЭК России № 21 выполнен анализ наиболее распространенных систем защиты информации от несанкционированного доступа и утечки информации: *Secret Net 7.0*[1] (разработчик ООО «Код безопасности» г. Москва), *Dallas Lock 8.0*[2] (разработчик ООО «Конфидент» г. Санкт-Петербург). Кроме основных мер по обеспечению безопасности ПДн, взяты еще следующие параметры: наличие сертификатов ФСТЭК, количество клиентов, среда функционирования, техническая поддержка [6]. Данные средства защиты имеют все необходимые лицензии ФСТЭК России, которые позволяют использовать их для защиты информации в автоматизированных системах класса до 1Б включительно и в ИСПДн до 1-го класса включительно. *Secret Net 7.0* и *Dallas Lock 8.0* могут функционировать на любом компьютере под управлением операционных систем семейства *Windows*, поддерживают 32-х и 64-х битные версии операционных систем[3]. Средства защиты информации (СЗИ) могут действовать в двух режимах (автономный и сетевой), обеспечивая защиту от несанкционированного доступа через локальный, сетевой и терминальный входы (табл.).

[1] URL : http://www.securitycode.ru/company.
[2] URL : http://www.dallaslock.ru.
[3] Следует учесть, что архитектура IA64 (Itanium) не поддерживается системой Dallas Lock 8.0-C.

ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
2014. № 3
http://eizvestia.isea.ru

Сравнительный анализ средств защиты информации Secret Net 7.0 и Dallas Lock 8.0 от несанкционированного доступа

Меры по обеспечению безопасности персональных данных	Secret Net 7.0[1]	Dallas Lock 8.0[2]
Идентификация и аутентификация субъектов доступа и объектов доступа	Реализован механизм парольной аутентификации пользователей средствами СЗИ. Идентификация и аутентификация пользователя совместно с операционной системой Windows с помощью программно-аппаратных средств (iButton; eToken Pro, eToken PRO Java (USB, смарт-карты); Rutoken, Rutoken ЭЦП и Rutoken Lite), а также усиленная аутентификация пользователей с использованием аппаратной поддержки ПАК «Соболь» и Secret Net Card	Обеспечивает идентификацию и аутентификацию локальных, доменных, терминальных и удаленных пользователей на этапе входа в операционную систему. Осуществляет работу с различными типами аппаратных идентификаторов
Ограничение программной среды	Для каждого пользователя компьютера формируется определенный перечень программ, разрешенных для запуска. Он может быть задан как индивидуально для каждого пользователя, так и определен на уровне групп пользователей	Существует механизм «замкнутой программной среды», который позволяет явно указать с какими программами пользователь может взаимодействовать
Защита машинных носителей информации	Поддерживается контроль следующих устройств: основные параметры рабочей станции (процессор, память); диски (физические, оптические, сменные и виртуальные); сетевые интерфейсы (Ethernet, 1394 FireWire, Bluetooth, IrDA, Wi-Fi); USB-устройства	Предотвращает утечки информации с использованием сменных накопителей (таких как CD-диск, USB-Flash-диск, внешний жесткий диск и др.). Система позволяет разграничивать доступ как к отдельным типам накопителей, так и к конкретным экземплярам
Управление доступом субъектов доступа к объектам доступа	Каждому информационному ресурсу назначается один из трех уровней конфиденциальности: «неконфиденциально», «конфиденциально», «строго конфиденциально», а каждому пользователю — уровень допуска. Доступ осуществляется по результатам сравнения уровня допуска с категорией конфиденциальности информации. Реализован контроль подключения и изменения устройств, а также разграничения доступа к устройствам, отслеживается неизменность (целостность) аппаратной конфигурации компьютера и контролируется использование отчуждаемых носителей	Возможно ограничение круга доступных для пользователя объектов файловой системы (дисков, папок и файлов под FAT и NTFS). Применяется полностью независимый от операционной системы механизм. Используются два принципа контроля доступа: – мандатный — каждому пользователю присваивается уровень доступа (пользователь будет иметь доступ к объектам, уровень доступа которых не превышает его собственный); – дискреционный — обеспечивает доступ к защищаемым объектам (дискам, каталогам, файлам) в соответствии со списками пользователей (групп) и их правами доступа (матрица доступа). В соответствии с содержимым списка вычисляются права на доступ к объекту для каждого пользователя (чтение, запись, выполнение и др.)
Регистрация событий безопасности	Регистрирует все события, происходящие на компьютере: включение/выключение компьютера, вход/выход пользователей, события НСД, запуск приложений, обращения к конфиденциальной информации, контроль вывода конфиденциальной информации на печать и отчуждаемые носители и т. п.	Реализовано ведение 6 электронных журналов (журнал входов; журнал доступа к ресурсам, журнал запуска процессов, журнал управления политиками безопасности, журнал управления учетными записями, журнал печати)
Антивирусная защита	Данный функционал не реализован	
Обнаружение вторжений	Данный функционал не реализован	
Выявление инцидентов и реагирование на них	Реализована возможность обнаружения, идентификации и регистрации инцидентов с последующим информированием ответственных лиц	

[1] URL : http://www.securitycode.ru/products/secret_net/scope_auto_edition.

[2] URL : http://www.dallaslock.ru/sub-doc.html.

Анализ существующих решений (автоматизированных систем) показывает, что для создания комплексной защиты ПДн есть все необходимые инструменты, позволяющие обеспечить безопасность информации на высоком уровне. Выбор в пользу того или иного СЗИ зависит от ценовой политики компании, от требований заказчика и частных особенностей объекта (персональный компьютер, сеть, здание и другие факторы), но не смотря на доступность готовых решений в области защиты ПДн, аналитики констатируют с каждым годом рост нарушений в этой области. Большинство утечек информации происходит через каналы, которые могут быть перекрыты техническими средствами.

Результаты исследования аналитического центра *InfoWatch*[1] говорят о критически низком уровне использования средств защиты от утечек для обеспечения безопасности персональных данных в РФ. Это подтверждает существующее мнение, что большинство компаний занимаются «бумажной» безопасностью ПДн, выполняя требования регуляторов лишь формально. Реальной работы по повышению уровня безопасности ПДн не ведется. Судя по характеру утечек (выброшенные документы, публикации в базе данных в Интернете), можно говорить также о невысокой компетенции сотрудников, отвечающих за безопасность ПДн в России. Так, по статистике каждая пятая утечка ПДн происходит из государственных органов. Наиболее часто встречается раскрытие ПДн граждан неопределенному кругу лиц. Госслужащие, нарушая требования законодательства о защите ПДн, исходят из благих побуждений, например, удобство граждан, ведут к нарушению законодательства.

Основными нарушителями являются малые и средние компании — на них выпадает две трети утечек (или 66 % всех утечек) ПДн. При этом утечки ПДн в среднем бизнесе приводят к более критичным последствиям (доля крупных материальных потерь вследствие утечки в небольших компаниях даже выше, чем в сегменте крупных организаций). Следует констатировать серьезные недостатки систем защиты ПДн в небольших организациях, а часто даже полное отсутствие каких-либо усилий в деле обеспечения безопасности ПДн. На наш взгляд, пока в России законодательно не установят норму обязательного информирования пострадавших граждан об утечке ПДн, не будет существенных сдвигов в области защиты ПДн. Граждане, чьи персональные данные утекут из страховой компании, оператора связи, госоргана, допустивших утечку, не будут знать о данном факте и, соответственно, не смогут прореагировать на случившееся судебным иском к виновнику с последующей компенсацией ущерба.

Список использованной литературы

1. Аверченков В. И. Оценка рисков безопасности информационных систем персональных данных / В. И. Аверченков, М. Ю. Рытов, О. М. Голембиовская // Информация и безопасность. — 2012. — № 3. — С. 321–328.

2. Голембиовская О. М. Автоматизация выбора средств защиты персональных данных на основе анализа их защищенности : автореф. дис. ... канд. техн. наук : 05.13.19 / О. М. Голембиовская. — СПб., 2013. — 17 с.

3. Ефремов А. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн / А. Ефремов // Защита информации. INSIDE. — 2013. — № 4. — С. 12–14.

4. Журавлев В. Правила игры в 21 / В. Журавлев // Защита информации. INSIDE. — 2013. — № 4. — С. 15–17.

5. Карпычев В. Ю. Новые подходы к определению актуальных угроз безопасности персональных данных / В. Ю. Карпычев // Информация и безопасность. — 2012. — № 1. — С. 93–96.

[1] Безопасность персональных данных в России в 2013 году. Статистика утечек. Отраслевые особенности // Аналитический Центр InfoWatch.

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
2014. № 3
http://eizvestia.isea.ru

6. Прокушев Я. Е. Сравнительный анализ средств программно-аппаратной защиты информации, применяемых в информационных системах персональных данных / Я. Е. Прокушев, С. В. Пономаренко // Информация и безопасность. — 2012. — № 1. — С. 31–36.

7. Сачков Д. И. Оценка эффективности информационно-телекоммуникационных систем на основе свободного программного обеспечения: монография / Д. И. Сачков, В. В. Братищенко, З. В. Архипова. — Иркутск : Изд-во БГУЭП, 2013. — 156 с.

8. Сачков Д. И. Современные информационно-телекоммуникационные технологии в управлении социально-экономическими системами / Д. И. Сачков, З. В. Архипова, В. В. Братищенко. — Иркутск : Изд-во БГУЭП, 2013. — 193 с.

References

1. Averchenkov V. I., Rytov M. Yu., Golembiovskaya O. M. Security risk estimation for personal data information systems. *Informatsiya i bezopasnost – Information and Security*, 2012, no. 3, pp. 321–328 (in Russian).

2. Golembiovskaya O. M. *Avtomatizatsiya vybora sredstv zashchity personalnykh dannykh na osnove analiza ikh zashchishchennosti. Avtoref. Kand. Diss.* [Automation of selecting protection means for personal data in terms of their security analysis. Cand. Diss.]. Saint Petersburg, 2013. 17 p.

3. Efremov A. Structure and content of organizational and technical measures for providing security of personal data while their processing in ISPDn. *Zashchita informatsii. INSIDE – Information Protection. INSIDE*, 2013, no. 4, pp. 12–14 (in Russian).

4. Zhuravlev V. Rules of playing 21. Zashchita informatsii. INSIDE – Information Protection. INSIDE, 2013, no. 4, pp. 15–17 (in Russian).

5. Karpychev V. Yu. New approaches to identification of immediate threads to personal data security. *Informatsiya i bezopasnost – Information and Security*, 2012, no. 1, pp. 93–96 (in Russian).

6. Prokushev Ya. E., Ponomarenko S. V. Comparative analysis of means of software-hardware information protection used in personal data information systems. *Informatsiya i bezopasnost – Information and Security*, 2012, no. 1, pp. 31–36 (in Russian).

7. Sachkov D. I., Bratishchenko V. V., Arkhipova Z. V. *Otsenka effektivnosti informatsionno-telekommunikatsionnykh sistem na osnove svobodnogo programmnogo obespecheniya* [Efficiency estimation for information and telecommunication systems on the basis of free software]. Irkutsk, Baikal State University of Economics and Law Publ., 2013. 156 p.

8. Sachkov D. I., Bratishchenko V. V., Arkhipova Z. V. *Sovremennye informatsionno-telekommunikatsionnye tekhnologii v upravlenii sotsialno-ekonomicheskimi sistemami* [Modern information and telecommunication technologies in management of socio-economic systems]. Irkutsk, Baikal State University of Economics and Law Publ., 2013. 193 p.

Информация об авторах

Сачков Дмитрий Иванович — кандидат экономических наук, доцент, кафедра информатики и кибернетики, Байкальский государственный университет экономики и права, 664003, г. Иркутск, ул. Ленина, 11, e-mail: leninb@yandex.ru.

Быкова Вера Николаевна — магистрант, кафедра информатики и кибернетики, Байкальский государственный университет экономики и права, 664003, г. Иркутск, ул. Ленина, 11, e-mail: Bykova.vn@yandex.ru.

Authors

Dmitry I. Sachkov — PhD in Economics, Associate Professor, Chair of Computer Science and Cybernetics, Baikal State University of Economics and Law, 11 Lenin St., 664003, Irkutsk, Russia, e-mail: leninb@yandex.ru.

Vera N. Bykova — Master Degree Student, Chair of Computer Science and Cybernetics, Baikal State University of Economics and Law, 11 Lenin St., 664003, Irkutsk, Russia, e-mail: Bykova.vn@yandex.ru.

http://eizvestia.isea.ru
2014. № 3
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ