ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И МАТЕМАТИЧЕСКИЕ МЕТОДЫ КАК ИНСТУМЕНТАЛЬНАЯ ОСНОВА ФИНАНСОВЫХ ОПЕРАЦИЙ НА РАЗНЫХ УРОВНЯХ УПРАВЛЕНИЯ

УДК 004.056

Е.А. Житникова, И.И.Сергеева

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Защита личной информации является предметом всеобщего обсуждения в последние несколько лет. Этот вопрос заслуживает особого внимания, поскольку он касается многих аспектов как бизнеса, так и частной жизни. Для многих компаний сбор конфиденциальных данных о потребителях и информации о сотрудниках является неотъемлемой частью ведения бизнеса. Если вы собираете такого рода информацию, то ваша юридическая ответственность заключается в принятии мер для надежной защиты этих данных. Компания должна разработать строгие меры безопасности для предотвращения потери, уничтожения, изменения, утечки и несанкционированного доступа к личной информации в соответствии с действующими законами и правилами. Именно данной проблематике посвящена статья. Кроме того, в ней расмотрены основные программные продукты, которые могут быть использованы.

Ключевые слова. Информационные технологии, персональные данные, информационные системы.

UDC 004.056

E.A.Zhitnikova, I.I.Sergeeva

PERSONAL DATA PROTECTION IN THE INFORMATION SYSTEMS

Protection of personal data has been a matter of considerable debates over the last few years. This problem needs special attention because it deals with many aspects both of business and private life. For many companies confidential information gathering about the employees is an integral part of its business. The Companies should elaborate rigorous security measures to prevent loss, destruction, modification, leaks and illegal access to the personal information, according to the applicable laws and regulations. The article is devoted to this problem. Moreover the author enumerates the principal software products that can be used in the protection of personal information

Keywords. Information technology, personal data information systems.

Необходимость обеспечения безопасности персональных данных (ПД) в наше время объективная реальность. Информация о человеке всегда имела большую ценность, но сегодня она превратилась в самый дорогой товар. Информация в руках мошенника превращается в орудие преступления, в руках уволенного сотрудника – в средство мщения, в руках инсайдера – товар для продажи конкуренту… Именно поэтому персональные данные нуждаются в самой серьезной защите.

Сегодня вряд ли можно представить деятельность организации без обработки информации о человеке. В любом случае организация хранит и обрабатывает данные о сотрудниках, клиентах, партнерах, поставщиках и других физических лицах. Утечка, потеря или несанкционированное изменение персональных данных приводит к невосполнимому ущербу, а порой и к полной остановке деятельности организации.

По определению Конвенции Совета Европы о защите частных лиц в отношении автоматизированной обработки данных личного характера, персональные данные означают любую информацию об определенном или поддающемся определению физическом лице [1].

По Федеральному закону «О персональных данных», к персональным данным относится любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация. Защита персональных данных — это комплекс организационных и технических мер исключающих доступ к информации, содержащей персональные данные, лиц, не обладающих соответствующими полномочиями, а также исключающих возможность неправомерного использования такой информации [1].

В соответствии с законом все данные должны быть теперь защищены, однако для этого можно использовать разные уровни защиты. Подзаконные акты Федеральной службы по техническому и экспортному контролю РФ и ФСБ выделяют четыре категории персональных данных (рисунок 1).

Данные самой высокой категории, предоставляемые в Пенсионный фонд, имеются в любой компании (ведомости о зарплате с указанием ФИО, сведения о социальном положении сотрудника, наличие

Рисунок 1 - Категории персональных данных

инвалидности, семейное положение, количество детей и др.) [2].

Чем выше категория персональных данных, тем более сложные механизмы требуются для их защиты. Для самой низкой категории – К4 – достаточно обеспечить только целостность данных, причем подбор технологических решений остается на совести компании. Данные категории К1 необходимо в том числе, защитить от утечек по визуальным и звуковым каналам, а также по побочному электромагнитному излучению, что организовать довольно сложно, поскольку потребуется специальное помещение и компьютерное оборудование, а используемые для защиты решения должны иметь соответствующие сертификаты ФСТЭК и ФСБ [3]. Последнее ведомство контролирует использование криптографии, однако без шифрования в системе такого уровня вряд ли удастся обойтись. К тому же при использовании сертифицированных ФСБ криптобиблиотек нужно еще иметь заключение на корректность их встраивания в продукт.

Существенные различия в требованиях защиты персональных данных для разных категорий информации неизбежно приведут к необходимости вносить изменения в имеющиеся архитектуры ИТ-систем, однако это относительно просто выполнить лишь для небольших баз данных, но не для всей системы целиком. Как следствие, компаниям придется выделять отдельные системы, отвечающие за работу с персональными данными высоких категорий, а для экономии средств защиту остальной информации обеспечивать на других, относительно недорогих конфигурациях [4]. В результате могут потребоваться изменения архитектуры в таких системах, как CRM, центры обработки телефонных вызовов и т. д., требующих вынесения персональных данных контрагентов в отдельную базу данных с высоким уровнем защиты.

Архитектура решения должна позволять выносить персональные данные не только в отдельный сегмент сети, но и вообще во внешнюю компанию, поскольку, скорее всего, защитой этих баз будут заниматься специализированные компании, имеющие необходимый набор лицензий на разработку, продажу и предоставление услуг в области шифрования. Возможно, что организации просто не захотят самостоятельно выполнять требования закона и подзаконных актов, а будут передавать защиту своих данных на аутсорсинг [5]. При этом используемые в компаниях программные продукты, такие как CRM, телефонные справочники и т. д., которые содержат персональные данные клиентов и партнеров, скорее всего, придется модифицировать.

Субъект ПД самостоятельно решает вопрос передачи кому-либо своих ПД, документально оформляя свое намерение [6]. В соответствии со статьей 9 ФЗ-№152 обработка персональных данных осуществляется только при условии согласия в письменной форме с указанием данных (рисунок 2).

Лица, виновные в нарушении требований обработки и хранения ПД, несут гражданскую, уголовную, дисциплинарную и иную, предусмотренную законодательством РФ, ответственность.

Защиту персональных данных можно обеспечить только в той информационной системе, где злоумышленник не может вмешаться в работу ее базовых элементов – сетевых устройств, операционных систем, приложений и СУБД [7].

Защита от вирусов является одним из средств предотвращения утечек конфиденциальной информации, в том числе и персональных данных, – вирусы, черви и другие вредоносные программы часто занимаются воровством информации и организуют скрытые каналы утечки [8]. Современные антивирусные решения включают в себя не только сигнатурную защиту, но и более современные средства, такие как поведенческий анализ программ, экраны уровня приложений, контроль целостности критических для операционной системы данных и другие методы защиты рабочих мест и серверов.

Корпоративная сеть целиком и каждое отдельное рабочее место должны быть защищены не только от

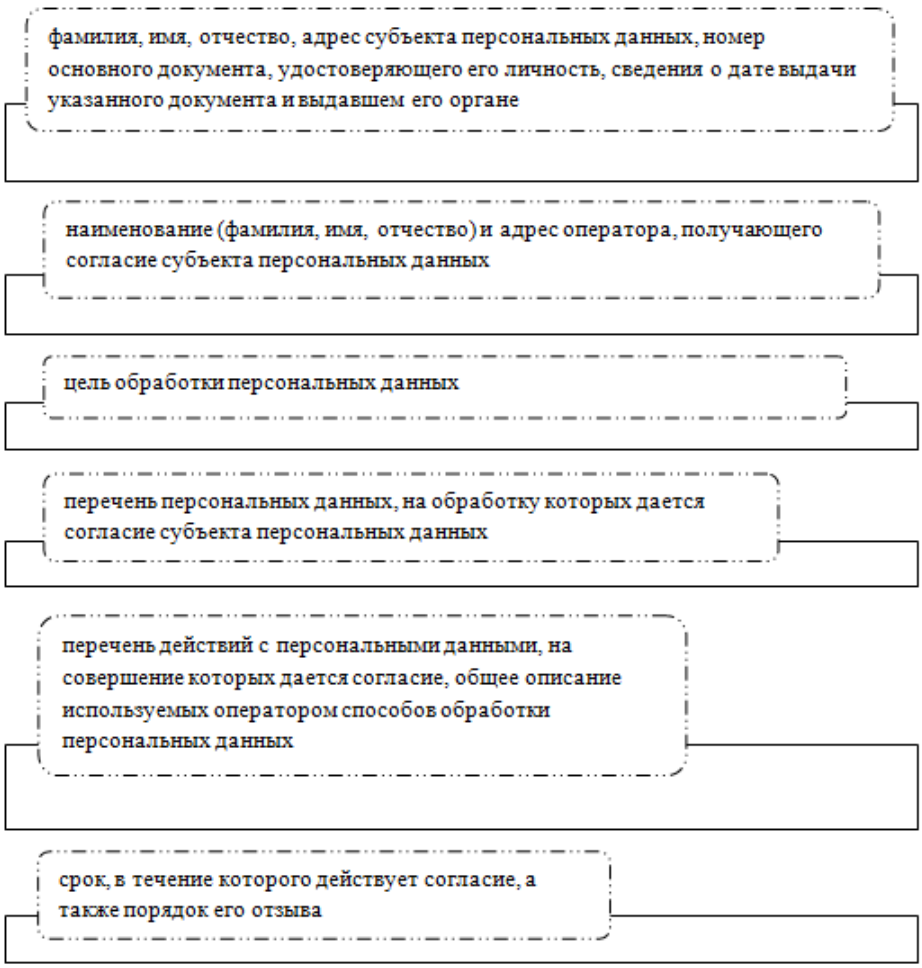

Рисунок 2 - Схема обработки персональных данных.

массовых атак с помощью вирусов, но и от целенаправленных сетевых атак. Для этого достаточно поставить систему блокировки неиспользуемых сетевых протоколов и сервисов, что и делает межсетевой экран. Часто к функциональности межсетевых экранов добавляют и средства организации виртуальных частных сетей – VPN.

В некоторых антивирусных решениях класса Internet Security (например, «Лаборатории Касперского», Symantec, Eset, McAfee и Trend Micro) уже встроены персональные межсетевые экраны, фиксирующие атаки по сетевым протоколам и попытки сетевых червей проникнуть на защищаемую машину. Кроме того, межсетевые экраны должны быть активированы на шлюзовом маршрутизаторе (такой функционал, как правило, имеется в сетевых устройствах), что позволит создать так называемую демилитаризованную зону (DMZ) для внешних Web-приложений и систем электронной почты. Собственно, в DMZ, для доступа к которой в межсетевом экране используются более жесткие правила, размещаются сетевые ресурсы, доступные извне, и защитные механизмы для них [9].

Системы предотвращения вторжений (Intrusion Prevention System, IPS) устанавливаются в разрыв сети и служат для выявления в проходящем трафике признаков нападения и для блокировки обнаруженной наиболее популярной атаки. В отличие от шлюзовых антивирусов, IPS анализируют не только содержимое IP-пакетов, но и используемые протоколы и корректность их использования. Спектр атак, от которых могут защитить системы предотвращения вторжений, несколько шире, чем у шлюзовых антивирусов [10]. Системы IPS производят как компании, специализирующиеся на сетевой защите, такие как Check Point и McAfee (продукт Network Security Platform), так и производители сетевого оборудования – Juniper и Cisco.

К общим средствам защиты относятся также сканеры уязвимостей, которые проверяют информационную систему на наличие различных «брешей» в операционных системах и программном обеспечении. Как правило, это отдельные программы или устройства, тестирующие систему путем посылки специальных запросов, имитирующих атаку на протокол или приложение. Наиболее популярными продуктами этого класса являются MaxPatrol, семейство продуктов IBM ISS, Symantec и McAfee (Vulnerability Manager). Впрочем, сейчас появляются пассивные сканеры, которые просто контролируют сетевой трафик и выявляют в нем наличие тех или иных признаков уязвимости. Такие сканеры только появились и еще не завоевали достаточно большой доли рынка. Сканеры уязвимостей можно использовать для проведения внутреннего аудита защиты, который предусмотрен в требованиях ФСТЭК.

Упомянутые средства защиты являются общими для всей сети и не связаны непосредственно с защитой

собственно персональных данных, однако в требованиях ФСТЭК их наличие специально оговаривается, поэтому эти базовые средства должны быть у каждого оператора персональных данных, причем даже для минимального уровня К4, где выбор средств защиты предоставляется самому оператору [11].

Набор средств для защиты конфиденциальных данных от утечек находится сейчас в стадии формирования. Имеется три класса таких продуктов: системы контроля над периферийными устройствами, системы защиты от утечек (Data Leak Prevention, DLP) и средства шифрования, причем каждый из производителей считает, что именно его продукт защищает от утечек. Скорее всего, для полной безопасности имеет смысл сочетать все три типа продуктов, но пока таких комплексных решений на рынке нет. Продукты для предотвращения утечек конфиденциальной информации можно использовать не только для защиты персональных данных, но и для предотвращения разглашения любых критических для работы предприятия сведений [12]. С помощью этих средств компания может не только формально удовлетворить требования ФСТЭК по защите персональных данных, но и попутно решить задачи по защите других видов конфиденциальной информации.

Нередко утечка данных происходит через съемные носители информации и несанкционированные каналы связи: флэш-память, USB-диски, Bluetooth или Wi-Fi, поэтому контроль за использованием USB-портов и другого периферийного оборудования также является одним из способов контроля утечек. На рынке имеется несколько решений этого класса, например от компаний SmartLine и SecureIT.

Системы защиты от утечек позволяют с помощью специальных алгоритмов выделить из потока данных конфиденциальные и заблокировать их несанкционированную передачу. В DLP-системах предусмотрены механизмы контроля разнообразных каналов передачи информации: электронной почты, мгновенных сообщений, Web-почты, печати на принтере, сохранения на съемном диске и др. Причем модули DLP блокируют утечку только конфиденциальных данных, поскольку имеют встроенные механизмы для определения того, насколько та или иная информация является секретной. В этом случае используется три технологии: по ключевым словам и регулярным выражениям, по отпечаткам эталонных конфиденциальных документов или по меткам секретности [13]. Продукты разных производителей до недавнего времени использовали один из этих методов, однако в последнее время ведутся разработки комплексного механизма контроля конфиденциальности, который использовал бы несколько перечисленных методов.

Защита данных от утечек так или иначе использует механизмы шифрования, а эта отрасль всегда контролировалась ФСБ, и все требования по сертификации систем шифрования публикуются и проверяются этим ведомством [14]. Следует отметить, что шифровать нужно не только сами базы персональных данных, но и их передачу по сети, а также резервные копии баз данных. Можно использовать механизмы шифрования, встроенные в базы данных, однако для их законного применения требуется интегрировать в них российские алгоритмы шифрования, что не всегда возможно, поэтому некоторые российские компании разрабатывают собственные продукты, в частности продукт Aladdin eToken SafeData. Впрочем, для защиты персональных данных можно шифровать целые разделы файловой системы, которые используются для хранения данных, такие решения предлагаются в России несколькими компаниями. Наиболее активны в этой сфере Aladdin, SecureIT, InfoWatch и «Физтех-Софт», однако на больших базах данных продукты этих компаний могут сильно замедлять производительность, поэтому для них можно либо использовать специализированные продукты, либо выделять их в отдельные базы, которые шифруются отдельно.

Шифрование используется и при передаче персональных данных по сети в распределенной системе. С этой целью можно применять предлагаемые различными разработчиками продукты класса VPN, которые, как правило, базируются на шифровании, однако подобные системы должны быть сертифицированы и тесно интегрированы с базами данных, в которых хранятся персональные данные.

Системы класса RMS (Right Management System) базируются на алгоритмах шифрования, однако управляют не процессом шифрования документов, а ключами дешифрации. Эти ключи хранятся на центральном сервере системы, и доступ к ним разрешается после прохождения процедуры строгой аутентификации пользователя, что означает – расшифровать документ может только тот пользователь, у которого есть на это права. Решения класса RMS предлагают пока в основном зарубежные компании – Microsoft (Microsoft RMS), Oracle (Oracle IRM) и ряд других, поэтому при использовании в российских условиях этих продуктов могут возникнуть проблемы с сертификацией в ФСБ. Кроме того, в существующих продуктах права доступа к ключам определяют авторы документов, что не позволяет защититься от внутренних угроз, как это делается в DLP-системах. Поэтому пока системы RMS не получили должного распространения в качестве средств защиты от утечек информации.

Перечисленные продукты предотвращают утечки в том числе и персональных данных, хотя их можно использовать и для защиты другой критической для компании информации, однако следует помнить, что для выполнения требований закона «О персональных данных» надо пользоваться сертифицированными средствами защиты и при их установке следует проверить наличие сертификата ФСТЭК, а на средства шифрования и сертификата от ФСБ [12].

Следует отметить, что в подзаконных актах ФСТЭК имеется разделение на небольшие, средние и распределенные базы данных, требования к защите которых сильно различаются. Так, для защиты распределенных баз, как правило, нужны дополнительные инструменты защиты, что и понятно – распределенная база должна иметь каналы связи между своими частями, которые также необходимо защищать. Вообще, для защиты больших информационных систем есть несколько продуктов, позволяющих централизованно контролировать крупные установки защитных продуктов.

В большой информационной системе главной проблемой для администратора является правильная орга-

низация доступа сотрудников к различным ресурсам – от корректной настройки прав доступа часто зависит сохранность конфиденциальных данных, поэтому система управления правами доступа должна быть включена в систему защиты крупной информационной системы. Такая система обычно позволяет ввести ролевое управление правами доступа и контролирует соблюдение этих прав. Система также блокирует попытки изменить права доступа без разрешения администратора безопасности, что обеспечивает защиту от локальных администраторов. Типичными представителями этого семейства продуктов являются Oracle IAM и IBM Tivoli Access Manager, но можно назвать также и McAfee Unified Secure Access Solution [8]. Следует отметить, что методика защиты персональных данных предполагает управление правами доступа в системах любых размеров, обрабатывающих такую информацию, однако в небольших базах данных достаточно ручного управления правами доступа.

Крупная система защиты может генерировать множество сообщений о потенциальных нападениях, которые лишь потенциально способны привести к реализации той или иной угрозы. Часто такие сообщения являются лишь предупреждениями, однако у администраторов безопасности большой системы должен быть инструмент, который позволил бы им разобраться в сущности происходящего. Таким инструментом анализа может стать система корреляции событий, позволяющая связать несколько сообщений от устройств защиты в единую цепь событий и комплексно оценить опасность всей цепочки. Это позволяет привлечь внимание администраторов безопасности к наиболее опасным событиям. Примерами подобных систем являются Cisco MARS или netForensics, однако аналогичные модули есть и в Tivoli Security Operations Manager (TSOM).

Системы централизованного управления защитными механизмами позволяют полностью контролировать все события, связанные с безопасностью информационной системы [4]. Продукты этого уровня могут обнаруживать защитные механизмы, установленные на предприятии, управлять ими и получать от них отчеты о происходящих событиях. Эти же продукты могут автоматизировать решение наиболее простых проблем или помогать администраторам быстро разобраться в сложных атаках. Это, например, уже названный IBM TSOM, LANDesk Security Suite или McAfee Network Security Manager.

Все перечисленные продукты не являются обязательными для защиты крупных информационных систем, однако они позволяют автоматизировать большинство задач, решаемых администраторами безопасности, и минимизировать количество сотрудников, необходимых для защиты большой системы.

Фактически закон «О персональных данных» требует от компаний – участников рынка информационной безопасности построения современной системы защиты, которая может пригодиться не только для сохранения персональных данных, но и для полного контроля за всей информационной системой, предотвращения утечек конфиденциальной информации или других видов тайн, предотвращения вывода из строя наиболее важных частей информационной системы [13]. Поскольку в той или иной форме персональные данные имеются у всех компаний, этот закон можно воспринимать как требования государства по информационной защите любого вида деятельности и не следует игнорировать требования этого закона. К тому же большинство компаний уже выполнили часть работы по защите персональных данных, так как невозможно пользоваться Сетью без установки какого-либо антивируса и межсетевого экрана.

В первой редакции Закона «О персональных данных» было указано, что информационные системы персональных данных, созданные до дня вступления в силу Федерального закона РФ № 152 «О персональных данных», должны были приведены в соответствие с требованиями данного Федерального закона не позднее 1 января 2010 года.

В настоящее время, по разным объективным и субъективным причинам, срок действия закона ФЗ-152 в части разработанных ранее информационных систем персональных данных перенесен сначала до 1 января 2011 года, а затем и до 1 июля 2011 года (закон № 444277-5). Однако все разрабатываемые (модернизированные) с начала 2011 года информационные системы персональных данных уже должны соответствовать закону [15].

На этой почве открывается большое поле деятельности для предприятий, способных оперативно построить корпоративную систему защиты информации и подготовить необходимый пакет документов для проверяющих органов. Другим вариантом решения проблемы соответствия закону «О персональных данных» является передача функции защиты персональных данных сторонним организациям, и такие компании-аутсорсеры уже начинают появляться в России. Тем не менее этот вариант может быть связан с изменением ИТ-архитектуры и потребует времени и дополнительных расходов.

Список литературы:

1. Волчинская, Е.К. Персональные данные в России 2010 [Текст] / Е.К. Волчинская // Защита персональных данных. Опыт правового регулирования. - 2010. - N6. - С. 5-7.

2. Fersko-Weis H. Projekt management software [Text] / Fersko-Weis H. //Hardware IBM PC. - Addison-Wesley. -2008. - November 15. - P. 178-226.

3. Марков, А.П. Проблемы и решения по защите персональных данных в информационных системах персональных данных [Текст] / А.П. Марков, Б. И. Сухинин // Компьютерная безопасность. - Улан-Уде: ВСГТУ. - 2009. - №5. – с. 20-27.

4. Баймакова, И.А. Обеспечение защиты персональных данных [Текст] / И.А. Баймакова // Персональная информационная система. - Книга 2. // 2011, №2 - С. 155-164.

5. Йошида, Х. Будущее систем хранения [Текст] / Х. Йошида // PC Magazine Russian Edition. – 2010. - № 5. - С. 34.

6. Федотов, Н.К. Обременительная защита [Текст]/ Н.К. Федотов // Компьютерра. – 2010. - № 18. - С. 28-

30.

7. Черняк, Л.С. Барьеры на пути утечек данных [Текст]/ Л.С. Черняк // Ежемесячный компьютерный журнал «CompUnity». – 2010. - № 9. - С. 12-14.

8. Круглова, Н.А. Программный круговорот [Текст] / Н.А. Круглова // Информационные технологии и вычислительные системы. – 2010. - №5. - С. 4.

9. Коржов, В.В. Защита персональных данных: проблемы и пути решения [Текст] / В.В. Коржов // Открытые системы. – 2010. - №10 . - С. 11.

10. Долакова, Е.П. Средства массовой информации и соблюдение конфиденциальности [Текст] / Е.П. Долакова // Information Security. – 2010. - №7. - С. 6-7.

11. Астахов, А.В. Защита информации. Инсайд [Электронный ресурс] / А.В. Астахов // Мир ПК. - Режим доступа: http://www.osp.ru/.

12. Сергеев, Р.П. Защищая свои права [Электронный ресурс] / Р.П. Сергеев // LAN. - Режим доступа: http://www.osp.ru/.

13. Лушников, А.К. Мера и средства защиты персональных данных [Электронный ресурс] / А.К. Лушников // ComputerWorld Россия. - Режим доступа: http://www.osp.ru/.

14. Башотов, И.Л. Операторы персональных данных [Электронный ресурс] / И.Л. Башотов // PC Week Russian Edition. - Режим доступа: http://www.osp.ru/.

15. Хватков, В.Н. Информзащита [Электронный ресурс] / В.Н. Хватков // ComputerWeek Moscow. - Режим доступа: http://www.osp.ru/.

Житникова Екатерина Александровна
студентка 4 курса финансово-экономического факультета
Орловского государственного института экономики и торговли
e-mail: kate2479@mail.ru

Сергеева Инна Ивановна
к.э.н., доцент кафедры ИТЭ
Орловского государственного института экономики и торговли
e-mail: inchiksergeeva@yandexl.ru