УДК 621.391

С.П. Евсеев, Э.А. Линд, О.Г. Король, О.М. Носик

Харьковский национальный экономический университет, Харьков

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Рассматриваются основные законодательные акты о защите персональных данных стран Евросоюза, США и стран постсоветского пространства. Проводится анализ основных требований, выдвигаемых к программным и аппаратно-программным средствам защиты персональных данных.

Ключевые слова: *персональные данные, защита персональных данных, законодательные акты.*

Постановка проблемы

Сегодня практически каждый человек обладает ценной электронной информацией, будь то ваши личные данные, например, файл с логинами и паролями к различным онлайн-сервисам, или рабочие документы – финансовый отчет, план работы с перспективным клиентом или стратегия развития предлагаемой компанией услуги. Такая информация нуждается в надежной защите: от несанкционированного доступа и распространения, случайного удаления или изменения. Все развитые страны Европы и постсоветского пространства обеспокоены проблемой информационной безопасности, а также защитой персональных данных граждан страны. Это обусловлено тем, что информатизация и оцифровка информации получили широкое распространение во всех сферах деятельности человека, в том числе и хранении личных и рабочих данных. Принятие законов о защите персональных данных обоснованы статистическими данными о краже личной информации. Для примера: в 2010 году число жертв хищения персональных данных превысило 8,1 млн. человек только в США [5; 6].

Целью статьи является анализ законодательной базы стран Евросоюза, США и стран постсоветского пространства о защите персональных данных, оценка основных требований, выдвигаемых к программным и программно-аппаратным средствам обеспечения защиты персональных данных (ПД).

Необходимость обеспечения безопасности персональных данных в наше время – объективная реальность. Современный человек не может самостоятельно противодействовать посягательству на его частную жизнь. Возросшие технические возможности по сбору и обработке персональной информации, развитие средств электронной коммерции и социальных сетей делают необходимым принятие мер по защите персональных данных. Кража персональных данных может нанести правообладателю ощутимый материальный ущерб, если речь идет о кредитных картах или информации о сбережениях в банке. Злоумышленники, обладающие достаточными техническими знаниями, похищают реквизиты банковских карт (скимминг) или имитируют сайты финансовых учреждений, чтобы заставить пользователя показать свою личную информацию (фишинг). На самом деле зачастую даже трудно установить источник утечки персональных данных вследствие высокой информатизации современного общества. Основные виды ПД представлены на рис. 1.

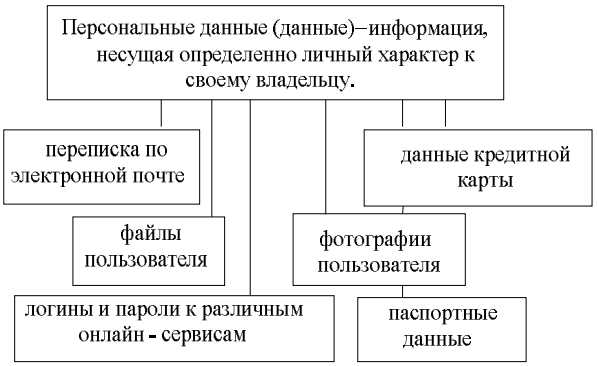

Рис. 1. Виды персональных данных

Кража персональных данных может нанести правообладателю ощутимый, как моральный, так и материальный ущерб, организовать спам-рассылку, изменить статус в социальных сетях и т.д.

Злоумышленники, обладающие дос-таточными техническими знаниями, похищают реквизиты банковских карт (скиминг) или имитируют сайты финансовых учреждений, чтобы заставить пользователя показать свою личную информацию (фишинг). На самом деле зачастую даже трудно установить источник утечки персональных данных вследствие высокой информатизации современного общества.

Проведенные исследования показали, что основными ”свободными” точками доступа к персональным данным являются социальные сети. Наибольшей популярностью пользуются сети Одноклассники.ru, В Контакте, Мой Мир@mail.ru. Опрос активных пользователей Интернета в возрасте от 16 до 45 (и старше) лет показал, что наиболее часто посещаемой является сеть Одноклассники.ru (37,8 %).

Ядро пользователей данной социальной сети составляют люди среднего возраста (30 – 44 года), а

наиболее частыми посетителями являются женщины.

Не менее популярной является социальная сеть В Контакте – ей отдают предпочтение около 29 % интернет-пользователей; ядро пользователей данной социальной сети составляет молодёжь (16-29 лет). Проект Мой Мир@mail.ru занимает третье по популярности место, а основными посетителями являются пользователи в возрасте от 45 и старше. Около 55 % пользователей посещают социальные сети ежедневно, а около 31 % активных пользователей Интернета делают это несколько раз в неделю.

Социальные сети также представляют большой интерес для фишеров, позволяя собирать личные данные пользователей:

в 2006 году компьютерный червь разместил на MySpace множество ссылок на фишинговые сайты, нацеленные на кражу регистрационных данных;

в мае 2008 года первый подобный червь распространился и в популярной российской сети ВКонтакте. По оценкам специалистов, более 70 % фишинговых атак в социальных сетях – успешны.

Основные средства проникновения и кражи ПД представлены на рис. 2.

США была первой страной, которая озаботилась проблемой защиты персональных данных. **«Закон о конфиденциальности» (Privacy Act)** был принят 31 декабря 1974. Он гласит, что все учреждения обязаны сообщить публичным уведомлением о своих базах данных и зарегистрироваться в Федеральном реестре. «Закон о конфиденциальности» запрещает разглашение информации из баз данных при отсутствии письменного согласия субъекта информации за исключением случаев, являющихся одним из двенадцати уставных исключений.

Следующим законом о защите персональных данных был **Safe Harbour Act**. Он вступил в силу в октябре 1998 года. Департамент торговли США запустил сертифицированную программу, которая называется **Safe Harbor** и которая направлена на закрепление правил обмена конфиденциальными данными при торговле между Соединенными Штатами Америки и Европейским Союзом.

Патриотический Акт США(Patriot Act) - гарант правовой защиты информации, вступил в действие с 26 октября 2001 года. Закон о правовой защите информации вносит поправки в 15 положений других законов, включая федеральные законы. Помимо других положений Патриотический Акт США содержит два положения, касающиеся компьютерного шпионажа и правовой защиты информации:

- Закон о правовой защите информации предоставляет правительству более широкие полномочия на проведение расследований и связанных с ними наблюдений, что вызвало беспокойство многих борцов за права на неприкосновенность частной жизни.
- В соответствии с новым законом предусматриваются более суровые меры наказания за ряд действий, связанных с компьютерным шпионажем.

Такие организации, как Центр демократии и технологий, Организация электронных границ, Союз американских гражданских свобод и Информационный Центр правовой защиты электронной информации, выступили за пересмотр закона в Конгрессе, поскольку многие положения Закона были сформулированы под влиянием эмоциональной атмосферы, царившей в стране после событий 11 сентября.

Патриотический Акт США имеет объем более 300 страниц и содержит огромное количество поправок для действующих законов [4; 6].

«Закон о защите персональных данных» был принят в Калифорнии в июле 2003 года. В соответствии с законом, все организации, предоставляющие коммерческие услуги, обязаны информировать своих клиентов в случае утечки их персональных данных, как то ФИО, номера социального страхования или номера кредитных карт. Закон помог выявить степень уязвимости защиты данных и побудил другие штаты последовать их примеру. Новый закон о защите персональных медицинских данных Калифорнии - первый в США, его рассматривают и остальные штаты.

Последовав примеру США, Европа также при-

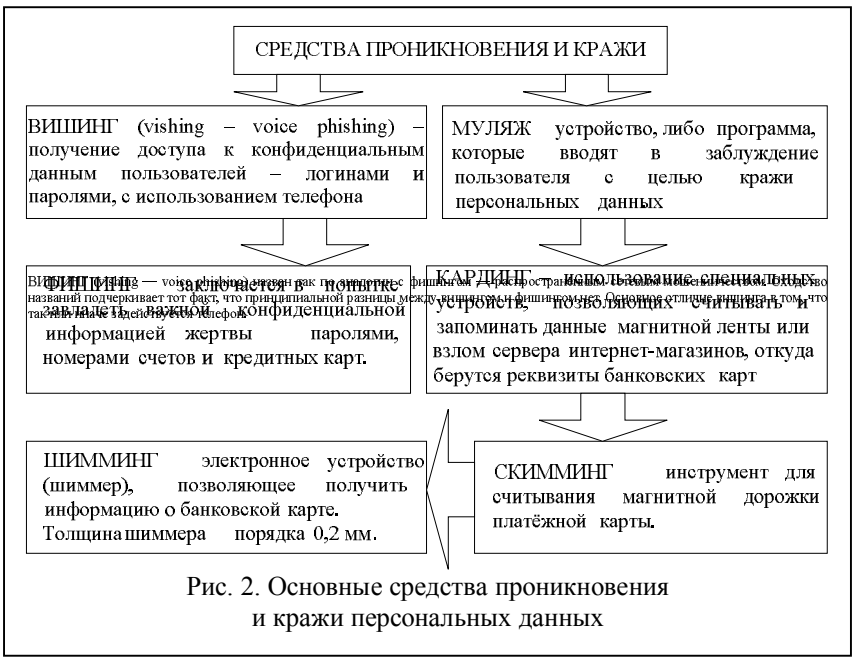

Рис. 2. Основные средства проникновения и кражи персональных данных

ступила к разработке ряда законов о защите персональной информации. К концу 70-х годов защита персональных данных в Совете Европы выделилась в самостоятельный вид деятельности. Комитетом экспертов Совета Европы по вопросам защиты персональных данных были сформулированы принципы защиты от неправомерных сбора, обработки, хранения и распространения сведений о физических лицах. Эти принципы 28 января 1981 года получили официальное закрепление в первом и единственном на сегодняшний день международном соглашении – Конвенции "**О защите (прав) физических лиц при автоматизированной обработке персональных данных**" (известна как Конвенция № 108, согласно порядку в серии Европейских договоров) [4].

В 1995 году Европейский Парламент и Совет Европейского Союза на основании положений Договора об учреждении Европейского Союза приняли **Директиву 95/46/ЕС** Европейского Парламента и Совета от 24 октября 1995 года "О защите физических лиц при обработке персональных данных и свободного обращения этих данных".

Основные законодательные акты о защите персональных данных представлены на рис. 3.

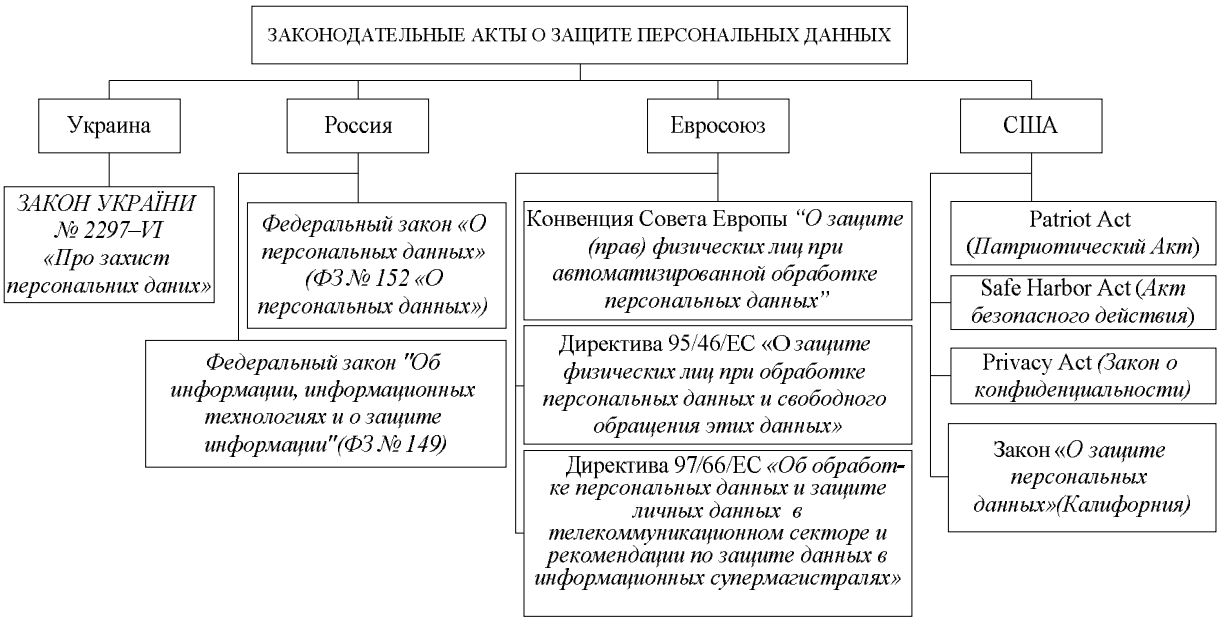

Рис. 3. Законы о защите персональных данных

Основная причина, побудившая ввести дополнительные к Конвенции 1981 года указания, вызвана тем, что защита персональных данных в государствах-участниках осуществлялась на разных уровнях. Это обуславливалось отсутствием единого уровня нормативно-правовой регламентации и несоответствием степени защиты персональных данных, которая предоставлялась национальными законодательными, регулятивными и административными положениями [4].

В дополнение к этой Директиве 15 декабря 1997 году была также утверждена **Директива 97/66/ЕС "Об обработке персональных данных и защите собственности в телекоммуникационном секторе**". Она дополняет и конкретизирует правила обработки операционных данных, которые собираются операторами во время предоставления телекоммуникационных услуг. В настоящее время это в большей степени касается телекоммуникационной интерсети Интернет [4].

Украина и Россия приняли законы о защите персональных данных относительно недавно, поэтому законодательная база этих стран касательно защиты личных данных только начала развиваться.

Первыми шагами России в отношении защиты персональных данных стали законы "О персональных данных" и "Об информации, информационных технологиях и о защите информации".

Федеральный закон "Об информации, информационных технологиях и о защите информации"" (ФЗ № 149 "Об информации, информационных технологиях и о защите информации") принятый 27 июля 2006, является базовым законом в области защиты информации.

Федеральный закон "О персональных данных" (ФЗ № 152 "О персональных данных") был принят 27 июля 2006 года и вступил в законную силу 26 января 2007 г. Целью закона является защита прав и свобод человека при обработке его персональных данных. Принятие данного федерального закона явилось триггером в создании правовых условий для защиты прав субъектов персональных данных в РФ [2].

Необходимость принятия Закона в Украине пе-

резрела. В стране существуют, возможно, миллионы баз данных, в которых накапливается информация о гражданах. Во многих случаях граждане никак не защищены. На сегодняшний день в Украине принят только один закон о защите персональных данных, принятие которого, к сожалению, обусловлено скорее желанием вступить в Европейский Союз, нежели желанием защитить своих граждан от несанкцион-ированного доступа к их личным данным.

Закон Украины № 2297-VI "О защите персональных данных" был подписан Президентом Украины 1 июня 2010. Он регулирует отношения, связанные с защитой персональных данных при их обработке. Закон содержит вполне пристойно написанные и понятные базовые положения, которое во многих аспектах схожи с Конвенцией Совета Европы [3].

Таким образом, проведенный анализ законодательных актов о защите персональных данных свидетельствует о значимости данного вопроса и решения его не только на уровне пользователей, но и на государственном уровне. Законодательные акты во многом схожи между собой и преследуют единую цель – обеспечить максимальную защиту и юридическую поддержку согражданам при решении вопросов защиты своих персональных данных в современных условиях резкого возрастания вычислительных возможностей, возникновения и роста кибертерроризма, появления новых более ухищренных угроз и атак на персональные данные пользователей локальных и глобальных сетей. На наш взгляд, наиболее полным и структурированным документом по описанию защиты персональных данных является Директива 95/46/ЕС. Она достаточно подробно описывает обязанности государства по защите персональных данных в законодательной сфере, права и обязанности владельцев баз данных, а также права субъектов персональных данных. Помимо этого есть ряд исключений, при которых государство имеет право на обработку и разглашение (или наоборот – неразглашение) персональных данных. Именно на основе Директивы 95/46/ЕС были созданы законы о защите персональных данных во всех странах Европы, а также практически полностью директива (с некоторыми поправками) была взята в качестве Федерального Закона России ФЗ № 152 "О персональных данных" и, конечно же, была основой для принятия в Украине закона № 2297-VI "О защите персональных данных". Все законодательные акты в одинаковой степени обязывают сообщать субъектам персональных данных об обработке их данных, а также защищать их на должном уровне во избежание распространения этих данных несанкционирован-ными лицами. Таким образом, проведенный анализ показал, что законы о персональных данных устанавливают общие подходы к обеспечению защиты ПД, права и обязанности субъектов, владеющих ими, а также обязательную регистрацию и защиту баз персональных данных в специальном государственном реестре [1].

Вместе с тем, проведенный анализ законодательной базы Украины показал, что главным отличием Закона Украины № 2297-VI "О защите персональных данных" является то, что при правильно составленном запросе к владельцу базы персональных данных любое третье лицо может получить доступ к персональным данным человека. Помимо этого в законе Украины не оговорен вопрос об удалении данных в случае, если они больше не нужны, оговорены лишь случаи разрывов отношений субъекта персональных данных и владельца баз персональных данных, или же в случае истечения срока пользования персональными данными. В законодательных базах стран Евросоюза и России отдельным пунктом прописан механизм уничтожения базы персональных данных по завершении цели, с которой эти данные собирались. Кроме этого, на взгляд авторов, существенным недостатком закона Украины является отсутствие четкой политики государства по использованию, а главное по обеспечению защиты персональных данных граждан Украины в своих целях (в Законе говорится о том, что государство может накапливать эти данные и использовать их без ведома субъектов этих персональных данных).

Отличительной особенностью Директивы 95/46/ЕС является создание «Рабочей группы по защите индивидуумов в отношении обработки их персональных данных». Она имеет статус консультативного органа и действует в качестве независимой структуры. Таким образом, помимо органа надзора существует независимая группа экспертов, регулирующая нормативно-правовые отношения всех субъектов отношений, связанных с базами данных [1].

Сравнительный анализ законодательных актов России (ФЗ № 152) с европейскими законами показал, что к фундаментальным отличиям относятся:

1. Независимость уполномоченного органа (ЕС);

2.Саморегуляция и невмешательство государства (ЕС);

3. Определение персональных данных;

4.Идентифицируемость субъекта ПД;

5.Принципы обработки;

6. Исключения из получения согласия:

а) преддоговорная работа;

б) баланс интересов;

в) Обязанность оператора перед законом.

7. Директ-маркетинг;

8. Предоставление сведений субъекту персональных данных;

9. Уведомление уполномоченного органа;

Сравнительная характеристика законодательных актов разных стран приведена в табл. 1.

Таблица 1

Сравнительная характеристика законодательных актов разных стран

Особенности законодательных актов	Страны			
	США	Евросоюз	Украина	Россия
Регистрация владельцами баз данных в государственном реестре	+	+	+	+
Специальный орган надзора	+	+	+	+
Рабочая группа по защите индивидуумов в отношении обработки их персональных данных	-	+	-	-
Реестр операций по обработке персональных данных	+	+	-	-
Обеспечение владельцами баз персональных данных надлежащего уровня защиты этих данных	+	+	+	+
Необходимо согласие субъекта данных на обработку его персональных данных	+	+	+	+
Передача данных третьим лицам	+	-	+	-
Уведомление субъекта данных об обработке его персональных данных	+	+	+	+
Предоставление субъекту персональных данных информации относительно владельца базы персональных данных	+	+	+	+
Субъект данных имеет право получить сведения о том, какая информация о нем хранится в базе персональных данных	+	+	+	+
Информация, хранящаяся в базе данных, не должна быть избыточной и должна соответствовать целям обработки персональных данных, заявленным ранее	+	+	+	+
Гласность операций по обработке данных и их хранению	+	+	-	-
Передача данных в третьи страны (при согласии субъекта персональных данных)	+	+	+	+
Особенности обработки персональных данных в государственных или муниципальных информационных системах персональных данных	-	-	+	+
Оплата доступа к персональным данным (кроме случаев доступа субъекта персональных данных к своим данным)	-	-	+	-
Возможность в отказе доступа к персональным данным субъекту этих данных	-	-	-	+
Формирование внутренних Кодексов владельцев баз данных	+	+	+/-	+/-

Проведенные исследования показали, что в законодательных актах России и стран Евросоюза/США существуют отличия в обеспечении безопасности персональных данных.

Так в законодательных актах России:

•требования определяют регуляторы (для обработки средствами автоматизации);

•отсутствует привязка к природе персональных данных, технологиям обработки, адекватности затрат [2].

В актах стран Евросоюза/ США:

•учитывает природу ПД, возможности нарушителя, технологии обработки, адекватность стоимости системы защиты наносимому ущербу;

•гибкий подход к созданию системы защиты баз персональных данных.

Перспективы развития законодатель-ной базы защиты персональных данных

На сегодняшний день интерес к развитию законов о защите персональных данных проявляют не только Европа и США, а также и Украина. В странах Европы и США весьма обеспокоены проблемой защиты персональных данных.

На данный момент в американский сенат внесен очередной законопроект по усилению защиты частных лиц от хищения и утери личных данных в Сети. В случае, если новый закон будет принят, фишерам-рецидивистам, атакующим американских граждан, грозят штрафы до 1 млн дол. либо тюремный срок до 5 лет. Personal Data Protection and

Breach Accountability Act (Закон "О защите персональных данных и ответственности в отношении утечек") запрещает также инсталляцию ПО для сбора информации, идентифицирующей пользователя, без его ведома и согласия. Вне закона окажутся и черные оптимизаторы, которые подтасовкой результатов поисковой выдачи заманивают посетителей на коммерческие сайты, поддельные страницы и целевую рекламу, получая за это вознаграждение.

Организациям, клиентские онлайн-базы которых превышают объем в 10 тыс. записей, во избежание утечек закон предписывает соблюдать определенные правила хранения данных в Сети.

Власти Европейского союза планируют ужесточить закон о защите данных. В новых поправках к закону о защите информации особое внимание уделяется компаниям, которые пострадали от взлома и кражи данных.

Согласно проекту поправок, в таких случаях они будут обязаны уведомлять власти и заинтересованных лиц в течение суток после "утечки". Кроме того, у пользователей появится возможность потребовать от компаний полного удаления своих данных, а также легко переносить персональную информацию от одной организации к другой.

На компании, нарушившие новый закон о защите информации, будет налагаться штраф в размере 1 процента от их общей выручки. Как ожидается, нововведения в законодательстве ЕС будут иметь далеко идущие последствия для Facebook, Google, социальных сетей, облачных служб, систем электронного биллинга и других онлайн-сервисов. Тем не менее, новые правила могут быть пересмотрены в течение двух лет, а для интернет-компаний они вступят в силу не ранее 2014 или 2015 года.

Цель поправок – исключить случаи, подобным тем, которые произошли в прошлом году с Sony и Citigroup. Так, в апреле 2011 года 77 миллионов клиентов PlayStation Network узнали о краже своих данных только спустя неделю после взлома онлайн-сети. Аналогичная ситуация сложилась с Citigroup: в результате атаки 10 мая у 3,300 держателей ее банковских карт похитили 2,7 миллиона долларов, однако компания признала факт утечки только через месяц, 8 июня.

На сегодняшний день Евросоюз и США также активно сотрудничают между собой и хотят создать единое, унифицированное соглашение, это обусловлено тем, что возникли некоторые проблемы с защитой персональных данных европейских граждан. Речь идет о Директиве Евросоюза о защите пользовательских данных, а также о Законе о патриотизме.

Впервые о правовой коллизии заговорила Microsoft, которая в июле этого года уведомила своих европейских клиентов, в том числе и высокопоставленных, о том, что может возникнуть ситуация, когда американские власти затребуют у Microsoft, как у американской компании, данные о европейских пользователях облачных сервисов корпорации. Согласно Патриотическому закону Microsoft должна будет передать запрашиваемые сведения в Вашингтон, причем она не должна уведомлять об этом европейскую сторону. С другой стороны, это прямо противоречит европейской директиве, которая требует, чтобы перед отправкой данных в известность ставились владельцы этих данных. Ранее между ЕС и США уже было достигнуто соглашение, по которому компании могут передавать европейские данные в США, но лишь в том случае, если будет обеспечен «приемлемый уровень» их безопасности. Трансфер осуществляется в рамках соглашения Safe Harbor, куда входят семь основных принципов. Однако Safe Harbor имеет более низкий приоритет, в сравнении с Патриотическим законом [6].

Именно по этой причине Евросоюзу и США придется в ближайшее время тесно сотрудничать для устранения возникших трений между законодательствами и создания нового соглашения, удовлетворяющего обе стороны.

Россия и Украина более "равнодушны" относительно своих законов о защите персональных данных. На сегодняшний день в планах стран постсоветского пространства нет каких либо новых законодательных актов в этом направлении. В России происходит внесение изменений и поправок в ФЗ № 152 для его дальнейшего совершенствования.

Законодательная база Украины имеет в своем активе лишь вступивший в силу Закон Украины № 2297-VI "О защите персональных данных", содержащий только общие требования и положения в построении систем защиты персональных баз данных.

Таким образом, на сегодняшний день практически во всех государствах введены законы о защите персональных данных. Наиболее развитыми в этом направлении оказались США и Евросоюз, имеющие ряд законов, позволяющих защищать персональные данные этих граждан на достаточно высоком уровне и регулировать вопросы о персональных данных в международных отношениях. Законодательные базы стран постсоветского пространства практически отсутствуют за исключением России.

Анализ основных требований по созданию систем защиты персональных данных

Неотъемлемой частью любой законодательной базы о защите персональных данных является положение о создании систем защиты персональных баз данных. Так в ФЗ России №152 рассмотрены общие принципы и меры по защите персональных данных:

"*Статья 19*. Меры по обеспечению безопасности персональных данных при их обработке (в ред. Федерального закона от 25.07.2011 N 261-ФЗ):

1. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

2. Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональ-ных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контроль над принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных" [2].

Таким образом, выделяются три основных типа мер по обеспечению безопасности персональных баз данных (ПБД): организационные, технические и правовые, представленных на рис. 4.

Под *правовыми мерами безопасности персональных данных* подразумеваются действующие законодательные акты государства о защите ПБД. Правовые меры позволяют субъекту персональных данных защищать свои данные от сторонних лиц, а также требовать защиты этих данных со стороны всех владельцев баз данных, в которых находятся персональные данные субъекта. Таким образом, государство непосредственно обеспечивает правовую защиту данных, и косвенно, с помощью законов и постановлений о защите персональных данных, обеспечивает другие меры по защите персональных данных.

Организационные меры по защите персональных данных подразделяются на общие и внутренние. Под общими мерами подразумевается ряд рекомендаций общего характера для всех видов владельцев персональных баз данных. Внутренние меры по защите информации включают в себя внутренние кодексы и положения владельцев баз персональных данных, которые обусловлены спецификой организации, в которой находятся ПБД. Иными словами, внутренние меры по защите разрабатываются индивидуально каждым владельцем баз персональных данных с учетом специфики этих данных, работы с ними, а также их важности. Зачастую такие внутренние меры являются коммерческой тайной и не подлежат распространению. К внутренним мерам относят:

введение внутренних руководящих указаний или принципов;

принятие Кодексов практики или поведения;

учреждение некой должности специального ответственного. Так, для реализации общих организационных мер по защите ПБД законодательной базой России определено, что обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных должно предусматривать:

оценку обстановки;

обоснование требований по обеспечению безопасности персональных данных и формулирование задач их защиты;

разработку плана обеспечения безопасности персональных данных;

выбор целесообразных способов (мер и средств) защиты персональных данных в соответствии с задачами и замыслом защиты;

решение вопросов управления обеспечением безопасности персональных данных в динамике изменения обстановки и контроля эффективности защиты;

обеспечение реализации принятого замысла защиты;

планирование мероприятий по защите персональных данных;

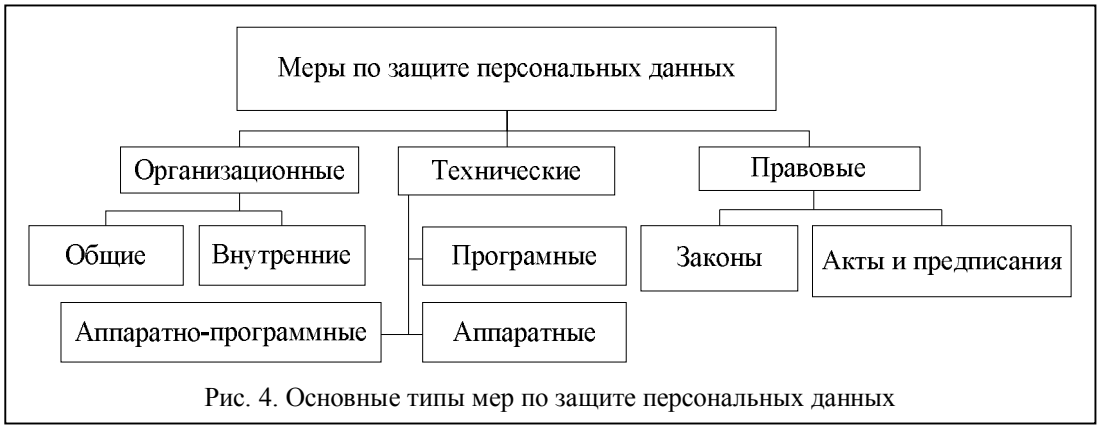

Рис. 4. Основные типы мер по защите персональных данных

организацию и проведение работ по созданию системы защиты персональных данных в рамках разработки (модернизации) информационных систем персональных данных, разработка и развертывание средств защиты персональных данных или ее элементов в информационных системах персональных данных, решение основных задач взаимодействия, определение их задач и функций на различных стадиях создания и эксплуатации информационных систем;

разработку документов, регламентирующих вопросы организации обеспечения безопасности персональных данных и эксплуатации средств защиты персональных данных в информационных системах персональных данных;

развертывание и ввод в опытную эксплуатацию средств защиты персональных данных в информационных системах персональных данных;

доработку средств защиты персональных данных по результатам опытной эксплуатации [9].

Законодательные акты стран Евросоюза в свою очередь уделяют больше внимания внутренним мерам организационной безопасности, таким как Кодексы практики или поведения. Так, в Германии Федеральный закон о защите данных требует от фирм и компаний иметь Кодексы практики. Более того, когда некая компания использует более 4 человек для автоматизированной обработки персональных данных (или более 19 человек для обработки данных неэлектронными средствами), эта компания должна назначить своего внутреннего

уполномоченного по защите данных в качестве узаконенного средства саморегулирования [1; 4].

В Ирландском законе 1988 г. о защите данных сказано: “Уполномоченный по защите данных может поощрять профессиональные ассоциации или другие представительные организации к принятию Кодексов практики”.

Законодательная политика США во многом схожа с политикой Евросоюза и в первую очередь направлена на создание внутренних Кодексов владельцев баз персональных данных. Помимо этого большое внимание уделяется подбору персонала службы безопасности, его обучению и тренингам. Службы безопасности в США зачастую обеспечивают как организационные меры безопасности персональных (и не только) данных, так и технические. Среди особенностей организационно-технических мер безопасности следует отметить досмотры личных вещей и машин въезжающих и выезжающих с территории организации.

В Украине на сегодняшний день, к сожалению, защита персональных данных организована на достаточно низком уровне, на “усмотрение и компетентность” системных администраторов или технических директоров компаний.

Таким образом, проведенный анализ показал, что общим для всех законодательных актов является признание необходимости организационных мер по защите персональных данных для предупреждения и предотвращения утечки информации. Все страны в той или иной мере реализуют принципы внешних и внутренних организационных мер безопасности персональ-ных данных, делая лишь акцент на те или иные методы. Вместе с тем, законодательная база России более направлена на организацию и планирование внешних организационных моментов защиты персональных данных, в то время как в США и Евросоюзе стремительно развивается практика введения внутренних Кодексов.

Технические средства защиты персональных данных являются важной составляющей при защите персональных данных. Существует три основных вида технических средств защиты данных, реализованных аппаратно, программно и аппаратно программно.

К *аппаратным средствам* относят комплексы электронных, электрических и механических устройств, которые обеспечивают защиту персональных данных на аппаратном (физическом) уровне. *Программные методы* защиты – это совокупность алгоритмов и программ, обеспечивающих разграничение доступа и исключение несанкционированного использования информации. Зачастую программные средства используются для защиты больших баз персональных данных и систем обработки. *Аппаратно-программными средствами* являются устройства, представляющие комплексную защиту данных и исключающие

возможность взлома программного кода (нелицензионного использования) программного продукта.

Ярким примером программной защиты данных является DLP-система. Под DLP подразумеваются такие продукты, которые позволяют обнаружить и/или блокировать несанкционированную передачу (утечку) конфиденциальной информации по какому-либо каналу, используя информационную инфраструктуру предприятия. Для сравнения рассмотрим 6 DLP-систем (из них 3 – Россия, 2 – США, 1 – Япония): InfoWatch Traffic Monitor Enterprise 3.5, SecurIT Zgate 3.0 и SecurIT Zlock 3.0, Дозор Джет 4.0.24, Symantec Data Loss Prevention 11.1, Websense Data Security Suite 7.5 , Trend Micro Data Loss Prevention 5.5 [8].

Сравнительная характеристика представлена в табл. 2.

Таблица 2

Сравнительная характеристика

	InfoWatch Traffic Monitor Enterprise	Дозор Джет	SecurIT Zgate и Zlock	Symantec DLP	Websense DSS	Trend Micro DLP
Контролируемые каналы передачи данных. Электронная почта (E-mail)						
SMTPS, ESMTP	Есть	Есть	Есть	Есть	Есть	Нет
Внутренняя Microsoft Exchange	Есть	Есть	Есть	Есть	Есть	Есть
Внутренняя IBM Lotus Domino	Есть	Есть	Есть	Есть	Есть	Есть
POP3	Нет	Есть	Есть	Есть	Есть	Нет
IMAP4	Нет	Нет	Есть	Нет	Есть	Нет
Интернет-пейджеры						
ICQ, Miranda (OSCAR)	Есть	Есть	Есть	Нет	Нет	Есть)
Windows Live Messenger	Нет	Есть	Есть	Есть	Есть	Есть
Microsoft Office Communicator	Есть	Нет	Есть	Есть	Есть	Нет
Перехват файлов IM	Есть (OSCAR)	Есть	Есть	Есть	Есть	Есть
HTTP, FTP и иные протоколы						
Входящий HTTP-трафик	Нет	Нет	Есть	Есть	Нет	Есть
Исходящий HTTP-трафик	Есть	Есть	Есть	Есть	Есть	Есть
Возможность сканирования почтового и веб-трафика в облаке	Нет	Нет	Нет	Есть	Нет	Нет
Блокирование						
Протоколы, блокирование передачи данных по которых возможно	HTTP, HTTPS, SMTP, OSCAR (ICQ и другие агенты)	HTTP, FTP, SMTP, FTP over HTTP	HTTP, HTTPS, FTP, HTTP, FTPS, SMTP, POP3, IMAP4,	SMTP, HTTP, HTTPS FTP, AIM, AIM	HTTP, HTTPS, FTP, SMTP, ESMTP	HTTP, HTTPS, FTP, SMTP, ESMTP
Скорость анализа сетевого трафика	~100 Мб/с	~ 2 Гб/с	Нет ограничений	~330 Мб/с	Нет данных	~190 Мб/с
Возможности контроля подключаемых внешних устройств						
HDD, USB, COM/LPT, Wi-Fi	Есть	-	Есть	Есть	Есть	Есть
Локальные принтеры	Есть	-	Есть	Есть	Есть	Есть
Запрет доступа к файлам на PC для заданных приложений	Нет	-	Нет	Есть	Есть	Нет
Очистка диска PC (перемещение в карантин)	Нет	-	в разработке	Есть	Есть	Нет
Автоматическое определение реального владельца данных	Нет	-	в разработке	Есть	Нет	Нет
Контроль буфера обмена	Нет	-	Есть	Есть	Есть	Есть
Контроль копирования в общие папки	Нет	-	Нет	Есть	Есть	Есть
Интеграция с решениями сторонних производителей						
Интеграция с любыми утилитами посредством встроенных API	Нет	Есть	Есть	Есть	Нет	Нет
Интеграция со сторонними решениями	Oracle IRM, IBM TSOM, Alladdin eSafe, Cisco IronPort, Bluecoat	Lumension Device Control, ArcSight	Microsoft RMS, Oracle IRM, ABBYY FineReader,	Microsoft RMS, Oracle IRM, PGP	Websense Web security, Safend Protector,	отправка данных через syslog (SIEM)

Примерами реализации аппаратно-программных устройств, обеспечивающих защиту ПБД, являются Armorhino (Украина) и InfoWatch Crypto-Storage (Россия). Сравнительная характеристика Armorhino и InfoWatch Crypto-Storage представлена в табл. 3 [5, 7].

Таблица 3

Сравнительная характеристика Armorhino и InfoWatch Crypto-Storage (IWCS)

Характеристики	Armorhino	IWCS
Несколько разделов, выполняющих функцию типизации данных по степени необходимой защиты.	+	-
Аппаратное шифрование данных стойкими алгоритмами.	+	+
Устойчивость к ошибкам в процессе шифрования	+	+
Наличие учетных записей и возможность управления ими	+	-
Наличие различных ролей доступа (таких как «Пользователь», «Администратор» и.т.д.)	+	-
Поддержка работы со всеми типами и версиями операционных систем, актуальными на сегодняшний день.	+/-	+
Удобство и простота в использовании	+	+
Безвозвратное удаление	-	+
Восстановление данных	-	+

Решения представлены в виде флеш- устройства с вшитыми драйверами и возможностью переноса информации. Данные устройства – наиболее универсальное и стойкое решение по защите персональных данных, в случаях, использования и распространения ПБД на разных компьютерах.

Проведенный анализ технических мер защиты информации показал, что в условиях рынка информационных технологий России и Украины следует отдавать предпочтение аппаратно-программным средствам защиты информации, поскольку программные средства часто подвергаются взлому, а аппаратные средства не могут обеспечить достаточного уровня защиты данных.

Выводы

На сегодняшний день проблема защиты персональных данных стоит очень остро. Поэтому все государства разрабатывают, обновляют, дополняют свои законы о защите персональных данных. Вместе с законами совершенствуются и методы защиты персональных данных. Потребности в новых и надежных методах защиты растут, но вместе с тем растет и рынок предложений. На данный момент передовыми государствами в законодательной и организационной сфере защиты персональных данных являются страны Евросоюза и США, тем не менее, в сфере технических средств защиты достаточно сильную конкуренцию им составляют Россия и Украина.

Список литературы

1. Директива 95/46/ЕС Европейского Парламента и Совета от 24 октября 1995 года «О защите физических лиц при обработке персональных данных и свободного обращения этих данных».

2. Федеральный закон «О персональных данных» (ФЗ № 152 «О персональных данных»)

3. Закон Украины № 2297-VI «О защите персональных данных»

4. А.А. Баранов, В.М. Брыжко, Ю.К. Базанов. «Права человека и защита персональных данных»

5. InfoWatch CryptoStorage Enterprise [Електронний ресурс]. - Режим доступу до ресурсу: http://www.infowatch.ru/ products/cryptostorage_enterprise.

6. Столкновение законодательств о персональных данных США и Европейского Союза [Електронний ресурс]. - Режим доступу до ресурсу: http://www.pdp.net.ua/ stolknovenie-zakonodatelstv-o-personalnyx-dannyx-ssha-ievropejskogo-souzahttp://www.pravo. vuzlib.net/book_z137_page_28.html

7. Руководство пользователя «Захищений USB флеш-накопичувач-Armorhino.»

8. Сравнение систем защиты от утечек (DLP). [Електронний ресурс]. - Режим доступу до ресурсу: http://www.anti-malware.ru/comparisons/data_leak_ protection_2011_part1

9. Защита персональных данных. [Електронний ресурс]. - Режим доступу до ресурсу: http://www. iso27000.ru/ chitalnyi-zai/zaschita-personalnyh-dannyh/zaschita-personalnyh-dannyh.

Поступила в редколлегию 19.03.2012

Рецензент: д-р техн. наук, проф. В.О. Хорошко, Державний університет інформаційно-комунікаційних технологій, Київ.

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

С.П. Євсеєв, Е.О. Лінд, О.Г. Король, О.М.Носик

Розглядаються основні законодавчі акти про захист персональних даних країн Євросоюзу, США і країн пострадянського простору. Проводиться аналіз основних вимог, висунутих до програмних і апаратно-програмних засобів захисту персональних даних.

Ключові слова: персональні дані, захист персональних даних, законодавчі акти.

PERSONAL DATA PROTECTION

S.P. Evseev, E.A. Lind, O.G. Korol, A.M. Nosik

Main legislative acts about personal data protection in European Union, USA and post-soviet countries are considered. Analysis of the main requirements to software and hardware- software of personal data protection is made.

Keywords: *personal data, protection personal data, legislative acts.*