УДК 621.391

Евсеев С.П., Головашич С.О., Король О.Г.

ПОРТАТИВНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ

Рассматриваются основные законодательные акты в сфере защиты персональных данных стран Евросоюза, США и СНГ. Проводится анализ основных источников угроз конфиденциальности персональных данных. Рассматриваются возможности программно-аппаратных портативных средств обеспечения конфиденциальности информации, на примере устройства "Арморино".

Ключевые слова: персональные данные, защита конфиденциальных данных, средства хранения информации, "портативный офис", применение БСШ AES-256, аутентификация информации.

Постановка задачи. Сегодня практически каждый человек обладает ценной электронной информацией: личные данные, деловые документы, файлы с логинами и паролями к различным онлайн-сервисам, деловая переписка. 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 своих граждан. В соответствии с Законом Украины "О защите персональных данных" в ст. 2 под "*персональними даними* розуміються відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована", а в ст. 6 определено "*Первинними джерелами відомостей про фізичну особу є*: видані на її ім'я документи; підписані нею документи; відомості, які особа надає про себе" [3]. 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.

Целью данной статьи является анализ законодательных актов в сфере защиты персональных данных стран Евросоюза, США и СНГ, определение основных источников угроз конфиденциальности персональных данных и предложение возможных способов противодействия им. Рассматриваются возможности программно-аппаратных портативных средств обеспечения конфиденциальности информации, на примере устройства "Арморино".

Анализ источников угроз конфиденциальности персональных данных. Необходимость обеспечения безопасности персональных данных в наше время - объективная реальность. 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 или имитируют сайты финансовых учреждений, чтобы заставить пользователя показать свою личную информацию. На самом деле зачастую даже трудно установить источник утечки персональных данных (ПД) вследствие высокой информатизации современного общества, основные средства проникновения и кражи представлены на рис. 1.

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 (скиминг) или имитируют сайты финансовых учреждений, чтобы заставить пользователя предоставить свою личную информацию (фишинг). На практике, когда обнаружены уже последствия утечки информации, бывает очень трудно установить источник этой утечки, вследствие высокой информатизации современного общества.

Под *угрозами безопасности ПД* при их обработке в информационной системе ПД (ИСПД) понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование,

распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных. Классификация угроз безопасности персональных данных представлена на рис. 2 [1–5].

Рис. 1. Основные средства проникновения и кражи персональных данных

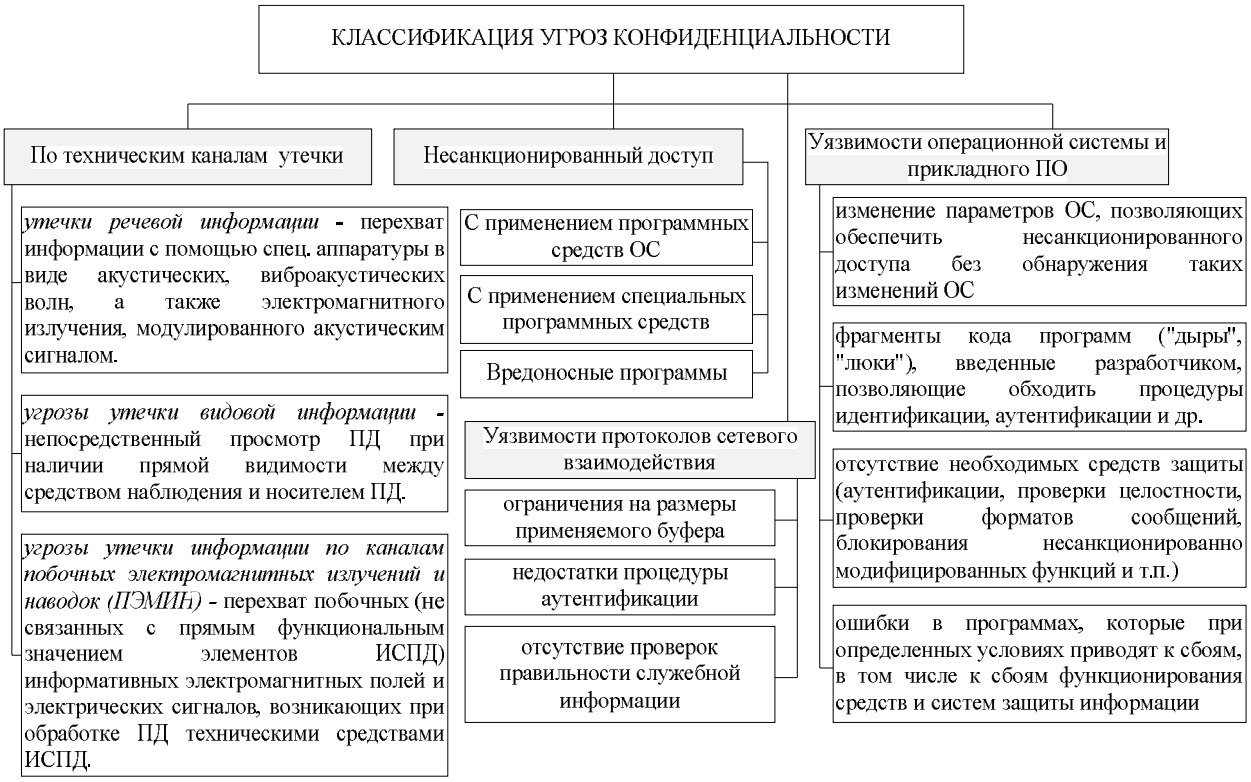

Рис. 2. Классификация угроз безопасности персональных данных

В связи с повсеместным развитием Интернета наиболее часто атаки производятся с использованием уязвимостей протоколов сетевого взаимодействия, основные виды атак представлены на рис. 3.

Проведенный анализ показал, что 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, банковских счетах или информации о сбережениях в банках.

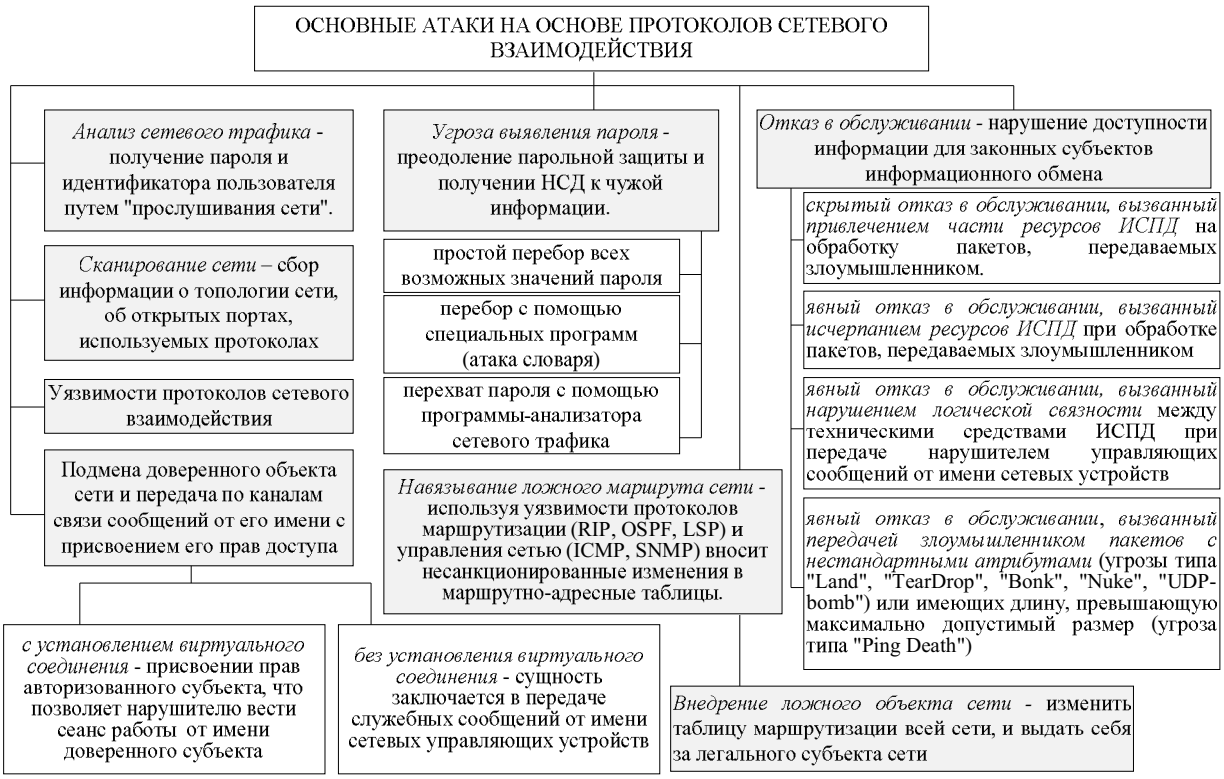

Рис. 3. Основные виды атак с использованием уязвимостей протоколов сетевого взаимодействия

Анализ основных законодательных актов в сфере защиты персональных данных стран Евросоюза, США и СНГ. Принятие законов о защите персональных данных обоснованы статистическими данными о краже личной информации. Для примера: в 2010 году в число жертв хищения персональных данных превысило 8,1 млн. человек только в США [5; 6]. Государство на законодательном уровне требует от организаций и физических лиц, обрабатывающих персональные данные, обеспечить их защиту. США была первой страной, принявшей в 1974 закон о защите персональных данных - “Закон о конфиденциальности” (Privacy Act). Закон запрещает разглашение информации из баз персональных данных (БПД) при отсутствии письменного согласия субъекта информации, за исключением случаев являющихся одним из двенадцати уставных исключений. Патриотический Акт США (Patriot Act) – гарант правовой защиты информации, вступил в действие 26 октября 2001 года. Закон о правовой защите информации вносит поправки в 15 положений других законов, включая федеральные законы [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, например, таких как: Ф.И.О., 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, страны Европейского Союза также приступили 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). В 1995

году Европейский Парламент и Совет Европейского Союза, на основании положений Договора об учреждении Европейского Союза приняли Директиву 95/46/ЕС Европейского Парламента 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. 4.

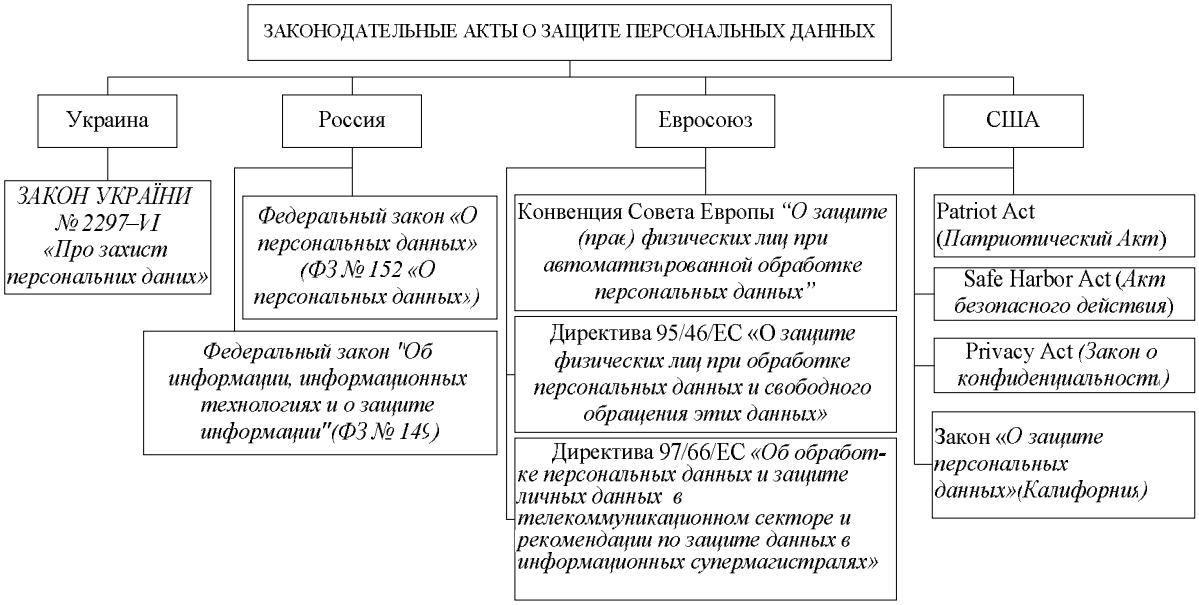

Рис. 4. Законы о защите персональных данных

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.

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.

Украина и Россия приняли законы о защите персональных данных относительно недавно, поэтому законодательная база наших 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”), который был принят 27 июля 2006 года, 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.

Необходимость принятия Закона в Украине давно назрела. 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 несанкционированного доступа к их личным данным.

Закон Украины №2297-VI "О защите персональных данных" был подписан Президентом Украины 1 июня 2010 г. Он регулирует отношения, связанные с защитой персональных данных при их обработке. Закон содержит базовые положения, которые во многих аспектах схожи с Конвенцией Совета Европы.

Таким образом, проведенный анализ законодательных актов о защите персональных данных свидетельствует о высокой значимости и необходимости решения данного вопроса не только для рядовых граждан, но и для государства в целом. Законодательные акты во многом схожи между собой и преследуют единую цель – обеспечить максимальную защиту и юридическую поддержку граждан в решении вопросов защиты их конфиденциальных данных. Особенно это стало актуально в современных условиях резкого возрастания вычислительных возможностей, возникновения и роста кибертерроризма, появления новых угроз на персональные данные пользователей локальных и глобальных сетей. На наш взгляд, наиболее полным и структурированным документом в сфере 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, эта директива была взята в качестве основы 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 несанкционированным путём. 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.

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

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);
- отсутствие привязки к природе персональных данных, технологиям обработки, адекватности затрат.

В актах стран Евросоюза / США:

- учитывается природа ПД, возможности нарушителя, технологии обработки, адекватность стоимости системы защиты наносимому ущербу;
- гибкий подход к созданию системы защиты баз персональных 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.

Сравнительная характеристика законодательных актов разных стран Таблица 1

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 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	+	+	+/-	+/-

Для обеспечения защиты персональных данных, выделяются три основных типа мер по обеспечению безопасности: организационные, технические и правовые. Их классификация представлена на рис. 5.

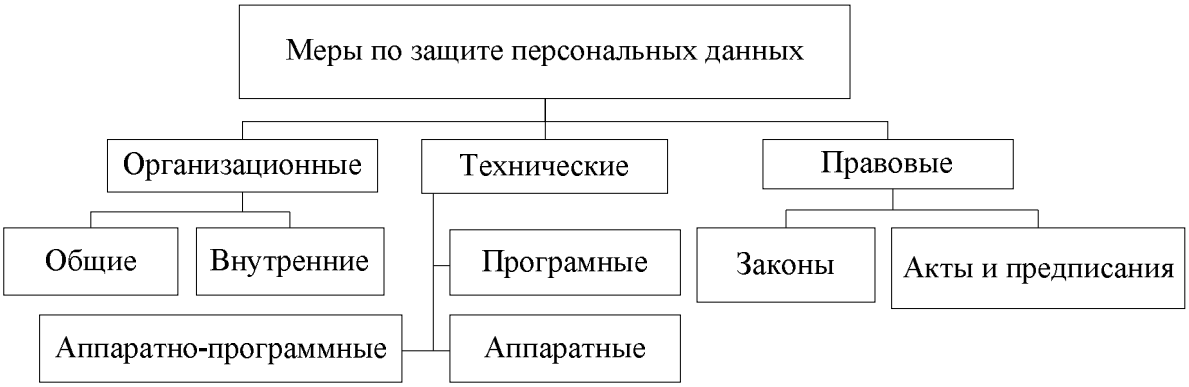

Рис. 5. Основные типы мер по защите персональных данных

Важной составляющей при защите персональных данных являются *технические средства защиты ПД*. Условно, их можно разделить на три основных вида (по способу реализации): аппаратные, программные и программно-аппаратные. При этом, в силу стремительного развития микропроцессорной техники, исключительно аппаратные средства защиты сегодня встречаются очень редко.

К *аппаратным средствам* относят комплексы электронных 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 различного производства (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. Сравнительная характеристика представлена в табл. 2 [8; 9].

Примерами реализации аппаратно-программных средств, криптографической защит ПБД являются Armorino (Украина) и InfoWatch CryptoStorage (Россия). Сравнительная характеристика Armorino и InfoWatch Crypto-Storage представлена в табл. 3.

Решения представлены в виде флеш-накопителей с интегрированным программным обеспечением и предназначены для защищённого хранения и обработки конфиденциальных данных. Данные устройства – наиболее универсальны в обеспечении защиты персональных данных, в случаях, использования и распространения БПД на разных компьютерах.

Накопитель "Арморино" позволяет эффективно противодействовать угрозам безопасности, возникающим в корпоративном секторе, и обеспечивает безопасное хранение, обработку и обмен конфиденциальной информации между разными рабочими станциями на платформе Windows. Для обеспечения конфиденциальности информации, устройство применяет высоконадежный блочный симметричный шифр AES-256 и аутентификацию авторизованных пользователей с помощью паролей, количество неудачных попыток аутентификации ограниченно. "Прозрачное" шифрование и проверка паролей реализованы непосредственно в аппаратном обеспечении, позволяя достигнуть высокого уровня защиты без потери быстродействия [7–9].

Сравнительная характеристика программных средств Таблица 2

	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
Запрет доступа к конфиденциальным файлам на PC для заданных приложений	Нет	-	Нет	Есть	Есть	Нет
Очистка диска PC от конфиденциальных данных (перемещение в карантин)	Нет	-	в разработке	Есть	Есть	Нет
Контроль источников хранимых данных	Хранение документов на рабочих местах, сетевых папках, в базах данных	-	в разработке	Хранение документов на PC, сетевых папках, в БД	Хранение документов на PC, сетевых папках, в БД	Хранение документов на PC, сетевых папках, в биб. MS SharePoint
Интеграция с решениями сторонних производителей						
Интеграция с любыми утилитами посредством 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)

Дополнительно, этот накопитель может применяться для безопасного хранения некоторого критического программного обеспечения, которое может быть запущено непосредственно с накопителя на любой рабочей станции Windows (портативное программное обеспечение), что позволяет в некоторых случаях повысить степень защиты от вредоносного программного обеспечения.

Сравнительная характеристика Armorino и InfoWatch Crypto-Storage Таблица 3

Характеристики	Armorino	InfoWatch Crypto-Storage
Несколько разделов, с различным типом доступа.	+	-
Аппаратное шифрование данных стойкими алгоритмами.	+	+
Устойчивость к ошибкам в процессе шифрования	+	+
Поддержка нескольких учетных записей пользователей и возможность управления ними	+	-
Наличие различных ролей доступа таких как “Пользователь”, “Администратор”	+	-
Поддержка работы со всеми типами и версиями ОС	+/-	+
Удобство и простота в использовании	+	+
Безвозвратное удаление	-	+
Удалённое восстановление данных	-	+

Накопитель “Арморино” вводит гибкую систему управления полномочиями и поддерживает несколько ролей пользователей с разными правами доступа. Для авторизации в рамках любой роли, имеющей привилегированный доступ («Пользователь» или «Администратор»), необходимо ввести пароль. Реализованная система позволяет создать единую корпоративную политику безопасности, и одновременно решить возможные проблемы, связанные с утратой (забыванием) паролей пользователями и, как следствие, потерей критической информации. Устройство “Арморино” может применяться для надежной аутентификации пользователей Windows. Для этого на хост-систему устанавливается провайдер аутентификации (Windows Logon), позволяющий выполнять вход в систему, подключив устройство и выполнив аутентификацию на пароле «Пользователя» или «Администратора» устройства. Таким образом, пользователю достаточно запомнить лишь пароль доступа к устройству и иметь само устройство.

Устройство “Арморино” поддерживает возможность корпоративной настрйки и дальнейшего менеджмента устройства на Корпоративной консоли администрирования.

Корпоративная консоль позволяет выполнять следующие функции администрирования устройства:

- начальную инициализацию устройства, включая установку пароля «Администратора», политики безопасности паролей и возможность дистанционного восстановления устройства;
- изменение конфигурации устройства (тип дистанционного восстановления и политика паролей);
- восстановление устройства без потери защищенных данных (при непосредственном подключении);
- вычисление “одноразового пароля” для дистанционного восстановления устройства без потери защищенных данных;
- “сбрасывание” ключа защиты CD-ROM раздела;

- сервисные функции.

Дополнительно, устройство позволяет создавать на его “скрытом” разделе “скрытые защищенные хранилища”. Каждое такое хранилище ассоциируется с некоторым сертифицированным приложением, которое создает и использует такое хранилище для хранения собственных секретных данных (в большинстве случаев, ключевой информации).

Создавать и использовать “скрытые защищенные хранилища” может лишь приложение сертифицированное компанией-разработчиком. Доступ к данным скрытого хранилища возможен лишь после аутентификации «Администратора» или «Пользователя». Права доступа «Пользователя» к хранилищу приложения могут быть ограничены и определяются во время его создания. Накопители семейства “Арморино” позволяют изменить концепцию обеспечения конфиденциальности от *“защиты отдельных файлов”* до *“портативного защищенного офиса в кармане рубашки”*.

Проведенный анализ технических средств 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, дополняют и ужесточают требования, выдвигаемые к законодательной базе в сфере защиты персональных данных. С ростом вычислительных возможностей, развитием телекоммуникационных и IT-технологий ужесточаются требования к программным и программно-аппаратным средствам защиты как конфиденциальных, так персональных данных, особое внимание при этом уделяется их криптостойкости и портативности. На сегодняшний день 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.

ЛИТЕРАТУРА

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-i-evropejskogo-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

Надійшла: 26.01.2012

Рецензент: д.т.н., проф. Дудикевич В.Б.