Ермошина В.А.
Научный руководитель – к.т.н., доцент каф. ФПМ Провоторов А.В.
Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»
602264, г. Муром, Владимирская обл., ул. Орловская, 23
valentina_ermoshina@mail.ru

Разработка системы защищенного хранения персональных данных

Персональные данные нуждаются в надежной защите ввиду повсеместно распространившихся краж информации, превратившихся в проблему мирового масштаба. Серьезность и острота проблемы потребовали от органов государственной власти принятия конкретных мер по ее урегулированию, вследствие чего в 2007 году в России вступил в силу Федеральный закон «О персональных данных», направленный на обеспечение всех необходимых мер по защите информации, используемой коммерческими и государственными организациями.

Объект исследования в данной работе – процесс защиты персональных данных, предмет исследования – система защищенного хранения персональных данных.

Целью исследования является изучить способы и средства нарушения конфиденциальности информации, а также методы ее защиты.

Для достижения поставленной цели необходимо выполнить следующие задачи:

1.исследование работы систем хранения персональных данных.

2.исследование способов и средств нарушения конфиденциальности информации.

3.изучение методов защиты информации.

4.разработка системы защиты персональных данных.

Исследование работы систем хранения персональных данных. Информационная система персональных данных представляет собой комплекс автоматизированных рабочих мест и (или) локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа. Необходимость создания информационной системы персональных данных возникает ввиду географической распределенности объектов информатизации.

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

Исследование способов и средств нарушения конфиденциальности информации.

Таблица 1 - Вероятности реализации угроз базе персональных данных

Вероятность реализации угроз ПДн	Вероятность реализации угроз ПДн (описание)	Численное представление вероятности
Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в хранилище носителей).	0
Низкая вероятность	Объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (применяются средства защиты информации).	2
Средняя вероятность	Объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны.	5
Высокая	Объективные предпосылки для реализации угрозы	10

вероятность	существуют, и меры по обеспечению безопасности ПДн не приняты.	

Для нейтрализации и снижения вероятности проявления тех или иных угроз на всех стадиях жизненного цикла узлов необходимо использовать комплекс мер и средств защиты:

- организационных и организационно-технических;
- инженерных и инженерно-технических;

-технических, программных, аппаратных и программно-аппаратных. Кратко рассмотрим каждый из типов лицензирования:

Изучение методов защиты информации. Вся существующая информация представляется в различной форме и на разных физических носителях:

- документальная форма;
- акустическая или речевая форма;
- телекоммуникационная и т.п.

Информация документальная содержится в буквенно-цифровом и графическом виде на бумаге, а также на магнитных носителях. Ее особенностью является содержание сведений, которые подлежат защите, в сжатом виде.

Речевая информация рождается в ходе ведения переговоров в помещениях, а также при работе системы звукоусиления либо звуковоспроизведения.

Носителями этой формы служат акустические колебания, которые являются механическими и распространяются от источника во внешнее пространство.

Циркуляция телекоммуникационной информации происходит в технических средствах хранения и обработки данных в процессе их передачи по каналам связи. Носителем информации в этом случае служит электрический ток, а если она передается по радиоканалу и оптическому каналу, то электромагнитные волны.

1.Управление доступом, включающее следующие функции защиты:

- идентификацию пользователя (присвоение персонального имени, кода, пароля и опознание пользователя по предъявленному идентификатору);
- проверку полномочий, соответствие дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту;
- разрешение и создание условий работы в пределах установленного регламента;
- регистрацию обращений к защищаемым ресурсам;
- реагирование (задержка работ, отказ, отключение, сигнализация) при попытках несанкционированных действий.
- криптографическое шифрование – готовое к передаче сообщение(текст, речь, графика) зашифровывается, т.е. преобразуется в шифрограмму. Когда санкционированный пользователь получает это сообщение, он дешифрует его посредством обратного преобразования криптограммы.

2.Механизм цифровой (электронной) подписи, основывающийся на алгоритмах асимметричного шифрования и включающий две процедуры: формирование подписи отправителя и ее распознавание (верификацию) получателем.

3.Причем для шифрования используется секретный ключ отправителя, а вторая процедура основывается на использовании общедоступного ключа, знания которого достаточно для опознавания отправителя.

4.Механизмы контроля доступа осуществляют проверку полномочий объектов АИТ (программ и пользователей) на доступ к ресурсам сети.

5.Механизмы обеспечения целостности данных (например, отправитель дополняет передаваемый блок данных криптографической суммой, а получатель сравнивает ее с криптографическим значением, соответствующим принятому блоку. Несовпадение свидетельствует об искажении информации в блоке).

6.Механизмы управления маршрутизацией обеспечивает выбор маршрутов движения информации по коммуникационной сети таким образом, чтобы исключить передачу секретных сведений по небезопасным физически ненадежным каналам и др.

Результаты исследования. В результате проведенного исследования было выяснено, что

выбор метода защиты информации напрямую зависит от формы информации, которую необходимо защитить, от количества пользователей обладающих данной информацией, а также от времени, в течение которого программа будет использоваться.

Литература

1. Защита персональных данных [Электронный ресурс] // Studfiles.ru : интернет портал URL: https://studfiles.net/preview/6163104/page:38/ (дата обращения: 5.11.2017).

2. Защита персональных данных [Электронный ресурс] // Википедия : свободная энцикл. URL: https://ru.wikipedia.org/wiki/Защита_персональных_данных (дата обращения: 6.11.2017).

3. Методы и способы защиты персональных данных в информационных системах персональных данных [Электронный ресурс] // itsec2012.ru URL: http://itsec2012.ru/metody-i-sposoby-zashchity-personalnyh-dannyh-v-informacionnyh-sistemah-personalnyh-dannyhaspx (дата обращения: 5.11.2017).