SearchInform

Роль систем информационной безопасности в защите персональных данных

Закон о «Персональных данных»

- Согласно статье 25 закона «О персональных данных», информационные системы персональных данных, созданные до дня вступления в силу настоящего Федерального закона, должны быть приведены в соответствие с требованиями настоящего Федерального закона не позднее 1 января 2010 года.

- По информации Роскомнадзора на сегодня в России более 56000 операторов персональных данных.

- Операторами персональных данных могут являться государственные органы, муниципальные органы, юридические или физические лица, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

К операторам персональных данных можно отнести любую коммерческую, некоммерческую, государственную, частную организацию, работающую с персональными данными (банки, мобильные операторы, поликлиники, учебные заведения, реестр держателей, крупные фирмы и т.д.).

Выдержки из закона

Статья 19. Меры по обеспечению безопасности персональных данных при их обработке

1. Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, **копирования, распространения персональных данных**, а также от иных неправомерных действий.

2. Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только **на таких материальных носителях информации** и с применением такой технологии ее хранения, **которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним**, уничтожения, изменения, блокирования, копирования, распространения.

Статья 24. Ответственность за нарушение требований настоящего Федерального закона

Лица, виновные в нарушении требований настоящего Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

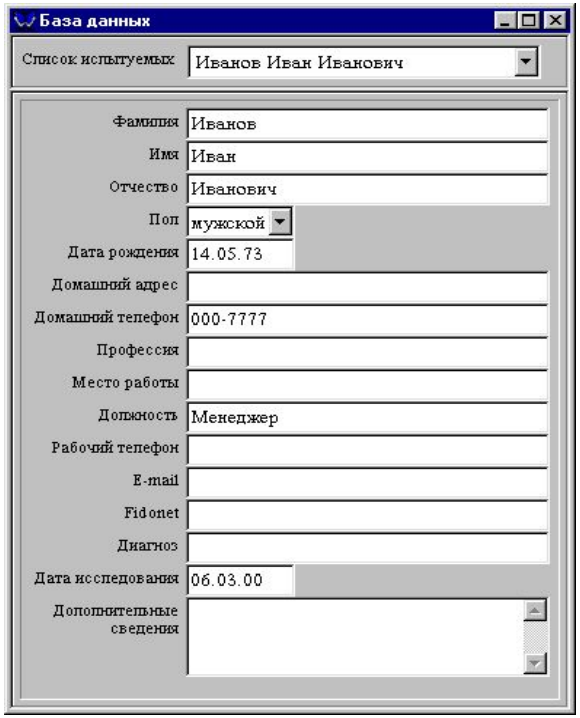
Что такое персональные данные?

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

Как правило, это жестко структурированные данные, которые хранятся в базах данных.

Примеры:

Фамилия, имя, отчество, год, месяц, дата и место рождения, адрес; семейное, социальное, имущественное положение; образование, профессия, доходы, другая информация.



Операторы

Закон о персональных данных имеет важное значение для государства. Персональные данные граждан не должны находиться в свободном доступе. Ситуация, когда на рынках можно купить базы данных с номерами телефонов сотовых операторов, номерами автомобилей и т.д. позволяет незаконно использовать персональные данные в коммерческих целях. Кроме этого эта ситуация играет на руку криминалу. Пока в России нет ответственности за обработку персональных данных эта ситуация не изменится. Именно для решения этой проблемы и был принят «Закон о персональных данных»

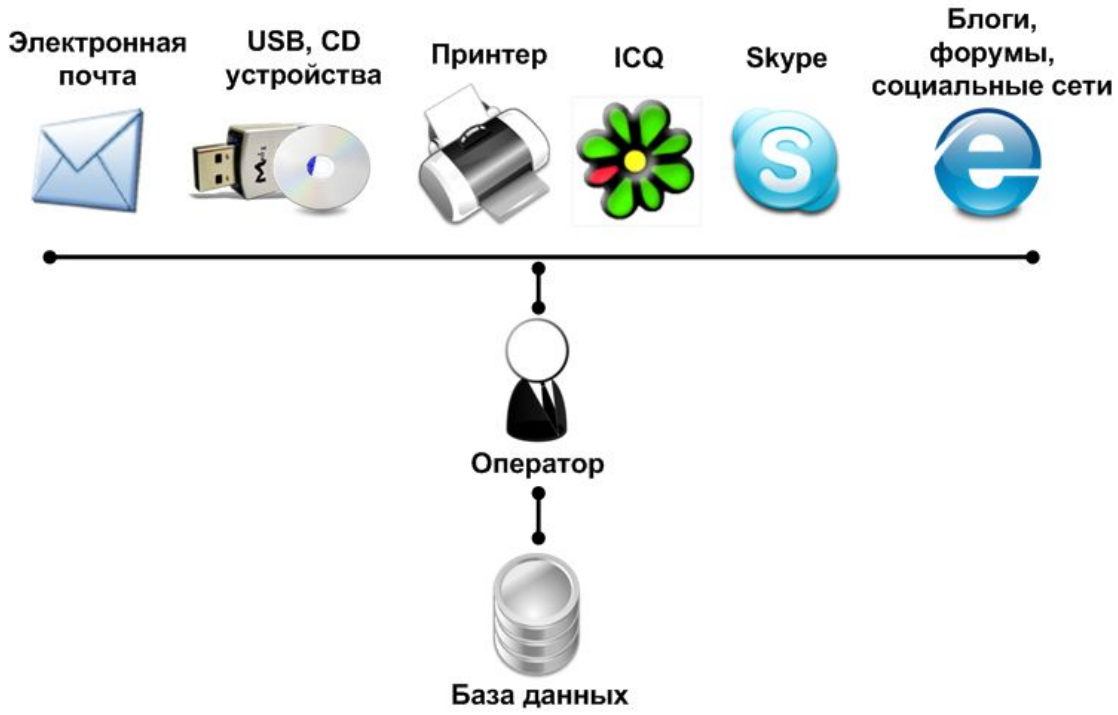
Для осуществления защиты персональных данных оператором должны быть приняты следующие меры:

1. **Шифрование баз данных**. Оно позволит защитить информацию от сотрудников, которые по долгу службы имеют доступ к серверам, на которых хранится информация (например, системный администратор).
2. **Шифрование каналов связи**, по которым ведется работа операторов с базами данных. Это позволит избежать перехвата информации в процессе ее передачи.
3. **Разграничение прав доступа** к базам данных, содержащих персональные данные. Каждый сотрудник должен иметь доступ только к тем данным, которые необходимы ему для выполнения служебных обязанностей.

Перечисленные меры позволяют защититься только от случайного или преднамеренного попадания данных к сотрудникам, не имеющим права с этими данными знакомиться.

- Сотрудники, которые работают с персональными данными по долгу службы, будут всегда иметь доступ к ним в незашифрованном виде.
- Для полноценной защиты данных от утечек необходимо исключить возможность пересылки ими информации, не регламентированной установленными правилами работы.
- Для этого необходимо принятие еще одной обязательной меры для защиты персональных данных от утечек - **организации контроля за всеми информационными потоками**.
- Такой контроль должен позволять оперативно обнаруживать все факты передачи персональных данных по всем возможным каналам утечки.

Каналы, по которым может происходить утечка персональных данных



Контроль за этими каналами предполагает возможность выявлять в больших информационных потоках несанкционированную передачу персональных данных.

Для обнаружения передачи персональных данных существуют несколько методик поиска.

Методика 1. Поиск по ключевым словам и фразам

Этот вариант поиска позволяют осуществлять почти все DLP системы. Так как каждая запись в базе данных является уникальной, этот метод позволяет искать в информационных потоках только присутствие заранее известной информации.

Например, осуществлялась ли пересылка информации о каком-то конкретном клиенте банка.

При необходимости обнаружения факта пересылки произвольной информации из базы данных этот метод не работает.

Вывод: для детектирования передачи персональных данных этот метод не работает.

Методика 2. Цифровые отпечатки в применении к записям БД

Эта методика позволяет осуществлять поиск по своеобразной контрольной сумме каждой записи в базе данных.

Фамилия	Имя	Отчество	Дата рождения	Счет открыт	Пол	Телефон	Адрес	Номер счета	Код	Баланс
Иванов	Иван	Иванович	12.12.1977	01.08.2008	Муж	123456	ул. Новая 54/122	3457832-22	qw12er	27000

Так как записи в базе данных могут постоянно добавляться или изменяться, этот метод будет работать только для тех из них, которые присутствовали в базе данных в момент последней индексации.
Когда, к примеру, в базу данных из миллиона записей каждый час добавляется 100 записей, то контроль за их утечкой будет отсутствовать до момента следующей переиндексации.
Кроме этого, этот метод не в состоянии детектировать передачу отдельных полей из записи.

Баланс	Номер счета	Код	Фамилия	Имя	Отчество	Телефон	Адрес
27000	3457832-22	qw12er	Иванов	Иван	Иванович	123456	ул. Новая 54/122

Например, если из записи о клиенте будет передаваться только фамилия и сумма денег на счету, этот метод не сработает.
Вывод: для детектирования передачи персональных данных этот метод работает частично.

Методика 3. Простые регулярные выражения

Регулярные выражения — система синтаксического разбора текстовых фрагментов по формализованному шаблону, основанная на системе записи образцов для поиска.

Используя простые регулярные выражения, можно отследить передачу данных, совпадающих по структуре с записями в базе данных.

Фамилия	Имя	Телефон	Адрес	Пол

Этот метод позволяет также описать и всевозможные комбинации сочетаний полей базы данных.

Фамилия	Имя	Телефон	Адрес	Пол
Имя	Фамилия	Адрес	Телефон	
Телефон	Адрес	Имя	Фамилия	
Адрес	Телефон	Фамилия		

Количество возможных комбинаций зависит от количества полей в записях базы данных.

Методика 3. Простые регулярные выражения

Плюсы:

- Не требуется переиндексации базы данных, так как поиск ведется по структуре а не по содержанию.
- Исключает ложные срабатывания

Минусы:

- для использования регулярных выражений необходимо определить все возможные комбинации полей базы данных. Это трудоемкий процесс, который не позволяет получить 100% определения комбинаций для баз данных с большим количеством полей.

Если, как и в предыдущем примере, из различных полей будет сделана выборка, то для использования регулярных выражений необходимо будет определять все возможные комбинации полей базы данных. Это трудоемкий процесс и он сильно усложняет работу по поиску информации.

Вывод: для детектирования передачи персональных данных этот метод требует сложной настройки.

Методика 4. Сложные регулярные выражения

Главное отличие сложных регулярных выражений от простых заключается в отсутствии необходимости описания всех возможных комбинаций полей базы данных.

Для организации поиска информации из базы данных в информационных потоках достаточно будет описать свойства всех полей.

При использовании этого метода будет обеспечен качественный поиск информации из базы данных в независимости от порядка следования полей, их сочетания и количества.

Вывод: для детектирования передачи персональных данных этот метод является оптимальным.

Для защиты персональных данных от утечек необходимо обеспечение шифрования баз данных и каналов связи, наличие разграничение прав доступа к базам данных.

Так же необходим контроль за всеми возможными каналами утечки информации с возможностью 100% детектирования передачи по ним персональных данных

Такую возможность может обеспечить только поисковая система, использующая методику поиска при помощи сложных регулярных выражений.

Единственным программным продуктом, позволяющим решить проблему защиты персональных данных, является «**Контур информационной безопасности SearchInform**»

SearchInform

Контру информационной безопасности

«Контур информационной безопасности SearchInform» позволяет отслеживать утечки конфиденциальной информации через e-mail, ICQ, Skype, внешние устройства (USB/CD), документы отправляемые на печать и выявлять её появление на компьютерах пользователей.

Итоги

Программные продукты «SearchInform» успешно решают поставленные задачи в банках и финансовых компаниях, государственных структурах и в крупных промышленных, сырьевых, телекоммуникационных и IT-компаниях России и стран СНГ.

SearchInform

Спасибо за внимание