Критерии использования криптографических средств при защите персональных данных

Беззубцев Олег Андреевич,
советник генерального директора
ОАО «ЭЛВИС-ПЛЮС»

Москва, 2008 г.

ЭЛВИС+

п. 1 статьи 19 Федерального закона «О персональных данных» специально указал, что «…оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать **шифровальные (криптографические) средства**, для защиты персональных данных …»

Когда (в каких условиях) оператор обработки персональных данных должен применять средства шифрования и Электронно-цифровую подпись в своих автоматизированных информационных системах?

Криптографические средства, какого конкретно уровня защиты он должен при этом использовать?

- Согласно п. 12 Положения, необходимым условием разработки системы защиты персональных данных в АИС оператора является модель угроз безопасности персональных данных

- Согласно п. 16 Положения модель угроз является необходимой для определения класса информационной системы

1) Персональные данные обрабатываются и хранятся в информационной системе с использованием определенных информационных технологий и технических средств, отвечающих, в первую очередь, целям и задачам обработки этих персональных данных. Именно данные технологии м средства порождающих объекты защиты различного уровня, атаки на которые создают прямые или косвенные угрозы защищаемой информации

2) Для обеспечения безопасности персональных данных при их обработке в информационных системах должна быть создана подсистема защиты персональных данных. При этом подсистема защиты не может обеспечить защиту обрабатываемой информации от действий, выполняемых в рамках предоставленных субъекту действий полномочий

3) Нарушитель информационной безопасности может действовать на различных этапах жизненного цикла АИС, подсистемы защиты персональных данных и конкретных, в том числе и криптографических, средств защиты информации. Поэтому при формировании модели угроз необходимо учитывать все возможные возникающие на указанных этапах жизненного цикла АИС и ее компонентов прямые и косвенные угрозы.

4) Для обеспечения безопасности персональных данных должны использоваться СЗИ, в том числе и криптографические, соответствующие требованиям российского законодательства. Средства штатно функционируют совместно с техническими и программными средствами АИС, которые способны повлиять на выполнение предъявляемых к СЗИ требований по безопасности

Формирование модели угроз информационным ресурсам АИС персональных данных

I этап. Анализ АИС:

- субъекты, создающие ПД;
- субъекты, которым ПД предназначены;
- информационные технологии и технические средства используемые в АИС;
- установленные или требуемые правила доступа к ПД;
- характеристики безопасности ПД, которые должны быть обеспечены в процессе обработки этих данных в АИС
- используемые в процессе создания и использования персональных данных объекты АИС
- дополнительная техническая информация, сопутствующая созданию и использованию ПД, которая может служить объектом угроз

Формирование модели угроз информационным ресурсам АИС персональных данных

IIэтап. Модель нарушителя ИБ АИС ПД

- определение типа нарушителя, целей его атаки, имеющихся у него средствах проведения атаки и используемых им для этого возможных каналов доступа к информационным ресурсам АИС;
- определение объекта атаки, а также имеющихся у нарушителя (нарушителей выявленного типа) сведений об объекте атаки – технических и программных средствах АИС

IIэтап. Модель нарушителя ИБ АИС ПД

1. Определение каналов воздействия нарушителя на АИС и подсистему защиты

2. Выделение типа нарушителя из множества H1, H2, .. H6

- хакер
- Корпоративный нарушитель
- Спецслужба зарубежного государства

3. Определение уровня криптографической защиты КС1, КС2, КС3, КВ1, КВ2, КА1

Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации

Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащих сведений, государственную тайну в случае использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных

Спасибо за внимание!

103460, МОСКВА, Зеленоград,

Центральный проспект, 11

тел. 531-4633, факс 531-2403

e-mail: info@elvis.ru

http://www.elvis.ru

http://www.zastava.ru

Олег Беззубцев

e-mail: olegab@elvis.ru