ДЕСЯТАЯ МЕЖДУНАРОДНАЯ НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

НОВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ

Повышение эффективности обучения и управления образовательными учреждениями с использованием технологий «1С»

Обеспечение безопасности персональных данных в информационных системах образовательных учреждений

2-3 февраля 2010 г.

Хорев П.Б., РГСУ

Терминология

- **Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.**
- **Оператор персональных данных – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.**

Нормативно-правовая база

- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»
- Постановление Правительства РФ от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»
- Постановление Правительства РФ от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»
- Постановление Правительства РФ от 29 декабря 2007 г. № 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами»

Нормативно-правовая база

- **Документы ФСТЭК России**
  - **РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ**
  - **ОСНОВНЫЕ МЕРОПРИЯТИЯ ПО ОРГАНИЗАЦИИ И ТЕХНИЧЕСКОМУ ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ**
  - **МЕТОДИКА ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ**
  - **БАЗОВАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ**
- **Документы доступны на сайте ФСТЭК http://www.fstec.ru/_spravs**

Нормативно-правовая база

- **Документы ФСБ России**
  - **Приказ от 9 февраля 2005г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)**
  - **Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, № 149/54-144, 2008 г.**
  - **Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, № 149/6/6-622, 2008 г.**
- **Для получения документов можно обращаться в 8 Центр ФСБ России и территориальные органы ФСБ России (http://www.fsb.ru/fsb/science.htm)**

Требования федерального закона

- 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.
- Контроль и надзор за выполнением требований, установленных Правительством Российской Федерации в соответствии с частью 2 настоящей статьи, осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

Мероприятия по защите ПДн при их обработке в ИСПДн

- управление доступом;
- регистрация и учет;
- обеспечение целостности;
- контроль отсутствия недекларированных возможностей;
- антивирусная защита;
- обеспечение безопасного межсетевого взаимодействия ИСПДн;
- анализ защищенности;
- обнаружение вторжений.

Реализация средств защиты

- Подсистему управления доступом, регистрации и учета рекомендуется реализовывать на базе программных средств блокирования несанкционированных действий, сигнализации и регистрации операционных систем, электронных баз ПДн и прикладных программ.
- Подсистема обеспечения целостности реализуется преимущественно операционными системами и системами управления базами данных.
- Подсистема контроля отсутствия недекларированных возможностей реализуется в большинстве случаев на базе систем управления базами данных, специальных средств защиты информации, антивирусных средств защиты информации.

Факторы выбора средств антивирусной защиты

- совместимость указанных средств со штатным программным обеспечением ИСПДн;
- степень снижения производительности функционирования ИСПДн по их основному назначению;
- наличие средств централизованного управления функционированием средств антивирусной защиты с рабочего места администратора безопасности информации в ИСПДн;
- возможность оперативного оповещения администратора безопасности информации в ИСПДн обо всех событиях и фактах проявления вредоносных программ;

Факторы выбора средств антивирусной защиты

- наличие подробной документации по эксплуатации средства антивирусной защиты;
- возможность осуществления периодического тестирования или самотестирования средства антивирусной защиты;
- возможность наращивания состава средств защиты от вредоносных программ новыми дополнительными средствами без существенных ограничений работоспособности ИСПДн и «конфликта» с другими типами средств защиты.

Реализация средств защиты

- Для осуществления разграничения доступа к ресурсам ИСПДн при взаимодействии с Интернетом применяется межсетевое экранирование, которое реализуется программными и программно-аппаратными межсетевыми экранами (МЭ).
- Подсистема анализа защищенности реализуется на основе использования средств тестирования (анализа защищенности, сканирования уязвимостей) и контроля (аудита) безопасности информации. Средства обнаружения уязвимостей могут функционировать на уровне сети, уровне операционной системы и уровне приложения.
- Для выявления угроз несанкционированного доступа к ПДн за счет использования сети Интернет применяются системы обнаружения вторжений (атак).

Защита ПДн от утечки по техническим каналам

- Применяются организационные и технические мероприятия, направленные на исключение утечки речевой и визуальной информации, утечки информации за счет побочных электромагнитных излучений и наводок (ПЭМИН). Например, увеличение звукоизоляции дверей достигается применением уплотняющих прокладок, обивкой полотен дверей специальными материалами.

Спасибо за внимание!