УТВЕРЖДЕНО
приказом председателя
НП "Южкузбасстуриндустрия"
№ 20 от 01.11.2011

П О Л О Ж Е Н И Е
по обеспечению безопасности и защите персональных данных при их обработке в информационных системах

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с "Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденным Постановлением Правительства Российской Федерации от 17 ноября 2007 г. N 781.

1.2. Настоящее Положение устанавливает методы и способы защиты информации, применяемые для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных.

1.3. К методам и способам защиты информации в информационных системах относятся: методы и способы защиты информации, обрабатываемой техническими средствами информационной системы, от 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 (далее - методы и способы защиты информации от несанкционированного доступа);

1.4. Выбор и реализация методов и способов защиты информации в информационной системе осуществляются на основе определяемых угроз безопасности персональных данных (модели угроз) и в зависимости от класса информационной системы.

1.5. Выбранные и реализованные методы и способы защиты информации в информационной системе должны обеспечивать нейтрализацию предполагаемых угроз безопасности персональных данных при их обработке в информационных системах

1.6. Персональные компьютеры (ПК) обладают всеми свойствами ЭВМ других классов.

1.7. Целями защиты информации в информационной системе является обеспечение физической и логической целостности, предупреждение несанкционированного получения информации, несанкционированной модификации и несанкционированного копирования Физическая целостность информации в информационной системе (ПК) зависит от целостности самого ПК, целостности дисков и дискет, целостности информации на дисках, дискетах и полях оперативной памяти. Предупреждение несанкционированной модификации является защита от действия вредоносных программ (компьютерных вирусов), разрушающих или уничтожающих программы или массивы данных.

II. Методы и способы защиты информации от несанкционированного доступа

2.1. Основными методами защиты персональных данных в информационных системах являются физическая защита ПК и носителей информации, аутентификация (распознавание) пользователей и используемых компонентов обработки информации, разграничение доступа к элементам защищаемой информации, регистрация всех обращений к защищаемой информации.

2.2. Физическими методами и способами защиты информации в информационной системе являются учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение; ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации; размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории; хранение ПК в нерабочее время в сейфах.

2.3. Аутентификация пользователей и используемых компонентов данных заключается в определении законности обращения к информационным ресурсам (реализация разрешительной системы допуска пользователей к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам) с использованием простых персональных паролей.

2.4. Разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации по специальным спискам;

2.5. Регистрация обращений к защищаемой информации в ПК включает в себя контроль использование защищаемой информации, выявление попыток несанкционированного доступа к защищаемой информации, накопление статистических данных о функционировании систем защиты.

2.6. Другими мерами обеспечения безопасности персональных данных в информационной системе являются резервирование технических средств, дублирование массивов и носителей информации; использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия; использование защищенных каналов связи; предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок; блокирование клавиатуры, мыши и экрана по истечение заданного времени бездействия пользователя.

2.7. В информационных системах, имеющих подключение к информационно-телекоммуникационным сетям международного информационного обмена (сетям связи общего пользования), или при функционировании которых предусмотрено использование съемных носителей информации, используются средства антивирусной защиты.

2.8. Для информационных систем 3 класса при однопользовательском режиме обработки персональных данных применяются следующие основные методы и способы защиты информации:

а) управление доступом:

идентификация и проверка подлинности пользователя при входе в систему информационной системы по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

б) регистрация и учет:

регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы;

учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета;

в) обеспечение целостности:

обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом

целостность программных средств проверяется при загрузке системы по наличию имен (идентификаторов) компонентов системы защиты персональных данных, целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ;

физическая охрана информационной системы (технических средств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации;

периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа;

наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.

2.9. Анализ защищенности проводится для распределенных информационных систем и информационных систем, подключенных к сетям международного информационного обмена, путем использования в составе информационной системы программных или программно-аппаратных средств (систем) анализа защищенности.

Средства (системы) анализа защищенности должны обеспечивать возможность выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационной системы, которые могут быть использованы нарушителем для реализации атаки на систему.

2.10. Обнаружение вторжений проводится для информационных систем, подключенных к сетям международного информационного обмена, путем использования в составе информационной системы программных или программно-аппаратных средств (систем) обнаружения вторжений.