УДК 681.3.067

П.Б. Хорев

Российский государственный университет, Москва, Россия

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ УЧРЕЖДЕНИЙ СОЦИАЛЬНОЙ СФЕРЫ

В настоящее время весьма актуальной является задача обеспечения безопасности персональных данных граждан в информационных системах учреждений социальной сферы (учреждений общего и высшего профессионального образования, учреждений здравоохранения и т.п.) [1]. Методы и средства защиты персональных данных от несанкционированного доступа и неправомерных действий при обработке такой информации в информационных системах персональных данных (ИСПДн) включают в себя [2]:

- управление доступом к объектам, содержащим персональные данные;
- регистрацию и учет попыток доступа к персональным данным;
- обеспечение целостности объектов с персональными данными;
- контроль отсутствия недекларированных возможностей в программном обеспечении, используемом при обработке персональных данных;
- защиту ИСПДн от вредоносных программ;
- обеспечение безопасного взаимодействия ИСПДн с другими компьютерными сетями (в частности, сетью Интернет);
- анализ защищенности ИСПДн;
- обнаружение вторжений в ИСПДн.

Средства управления доступом, регистрации и учета целесообразно реализовывать на базе программных средств разграничения доступа и аудита операционных систем, систем управления базами данных и прикладных программ. В частности, при создании ИСПДн на платформе 1С: Предприятие 8.1 могут использоваться следующие программные средства защиты [3]:

- идентификация и аутентификация пользователей информационных систем и активизированных ими процессов;
- авторизация субъектов (определение прав доступа субъекта к объекту с персональными данными на основе ролевого разграничения доступа [3]);
- аудит событий, связанных с попытками дос-

тупа к персональным данным.

Подсистему обеспечения целостности объектов с персональными удобно реализовать средствами операционных системам и систем управления базами данных. Средства повышения достоверности и обеспечения целостности передаваемых по сети и сохраняемых данных, имеющиеся в операционных системах и системах управления базами данных, основаны на расчете контрольных сумм (основанных на хешировании кодов аутентификации сообщений, электронной цифровой подписи). Средства обеспечения надежности транзакций базируются на уведомлении о сбое в передаче пакета сообщения, повторе передачи не принятого пакета.

Подсистема контроля отсутствия недекларированных возможностей реализуется в большинстве случаев на базе систем управления базами данных, специальных средств защиты информации, средств защиты информации от вредоносных программ.

Для обеспечения безопасности персональных данных и программно-аппаратных средств ИСПДн, осуществляющих обработку этой информации, необходимо применять специальные средства антивирусной защиты. При выборе средств защиты от вредоносных программ целесообразно учитывать следующие факторы:

- совместимость указанных средств со штатным программным обеспечением ИСПДн;
- степень влияния на эффективность функционирования ИСПДн по их основному назначению;
- возможность централизованного управления функционированием средств антивирусной защиты с рабочего места администратора безопасности информации в ИСПДн;
- возможность своевременного оперативного оповещения администратора безопасности информации в ИСПДн обо всех событиях и фактах проявления вредоносных программ;
- наличие подробной документации по эксплуатации средства антивирусной защиты;
- возможность осуществления периодического тестирования или самотестирования средства антивирусной защиты;
- возможность обновления средств защиты от вредоносных программ без существенных ограничений работоспособности ИСПДн и «конфликта» с другими средствами защиты.

Для разграничения доступа к объектам ИСПДн при взаимодействии с сетью Интернет должны применяться программные и программно-аппаратные межсетевые экраны (МЭ), работающие на сетевом и (или) прикладном уровнях модели OSI. МЭ устанавливается между защищаемой (внутренней) сетью ИСПДн и сетью Интернет (внешней сетью). При этом МЭ должен входить в состав защищаемой сети. С помощью конфигурирования МЭ необходимо отдельно задать правила, ограничивающие доступ из внутренней сети во внешнюю и наоборот.

Подсистема анализа защищенности реализуется на основе использования средств тестирования (анализа защищенности, сканирования уязвимостей) и контроля (аудита) безопасности ИСПДн. Средства анализа защищенности применяются с целью контроля настроек защиты операционных систем на рабочих станциях и серверах и позволяют оценить возможность проведения нарушителями атак на сетевое оборудование. Также анализаторы защищенности позволяют контролировать безопасность (в том числе целостность) системного и прикладного программного обеспечения. Результатом работы средства анализа защищенности является отчет, в котором обобщаются сведения об обнаруженных уязвимостях ИСПДн.

Средства обнаружения уязвимостей могут функционировать на уровне сети, уровне операционной системы и уровне приложения. По результатам сканирования уязвимостей системы сканеры уязвимостей выдают администратору ИСПДн рекомендации и предлагают меры, позволяющие устранить выявленные недостатки в обеспечении безопасности персональных данных.

Для выявления угроз несанкционированного доступа к персональным данным при использовании сети Интернет также должны применяться системы обнаружения вторжений (атак). Такие системы строятся с учетом особенностей реализации атак, этапов их развития и основаны на целом ряде методов обнаружения атак.

К основным проблемам, возникающим при использовании представленных методов и средств защиты в ИСПДн учреждений социальной сферы, можно отнести:

- недостаток финансовых средств, необходимых для приобретения сертифицированных программных и программно-аппаратных средств защиты;
- отсутствие в штатном расписании многих учреждений должностей администраторов безопасности информационных систем;
- недостаточная подготовленность руководителей и сотрудников учреждений в области информационной безопасности;
- неправильная оценка вероятных угроз и рисков, которые могут привести к несанкционированному доступу к персональным данным;
- необходимость использования в ИСПДн учреждений социальной сферы практически тех же методов (например, криптографических алгоритмов) и средств защиты, что и в информационных системах, обрабатывающих информацию, относящуюся к государственной тайне.

Список литературы

1. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

2. Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. [Электронный ресурс]. – Режим доступа к документу: http://www.fstec.ru/ _spravs/ recomend.doc.

3. Хорев П.Б. Программно-аппаратная защита информации. – М.: ФОРУМ, 2009. – 352 с.