Угрозы безопасности и защита информационных систем персональных данных

Анна Савина

Safety threats and protection of information systems of the personal data: *The paper justifies the necessity use of the system approach to safety of personal data in information systems. Author denotes necessity of use of means for information protection in connection with coming into force of the federal law "About the personal data". Mechanism ensuring the isolation of software environment (which based on the differentiating policy of access to protected resources for the subject "process") and mechanism for control of devices connection to system (policy "everything, that is not authorized, it is forbidden") are described.*

Key words: *Information safety, technologies of personal data protection.*

ВЪВЕДЕНИЕ

Развитие локальных и глобальных сетей, каналов спутниковой связи способствует обострению проблемы обеспечения информационной безопасности. С использованием современных технических средств повышается производительность труда, однако возрастает риск уязвимости данных. Одна из наиболее значимых категорий конфиденциальной информации – персональные данные. Следствиями утраты данных могут стать подрыв репутации компании, нанесение ущерба ее торговой марке и снижение конкурентоспособности.

По данным компании Panda Security, в 2008 году более 10 миллионов пользователей пострадали от кражи персональных данных [3]. За тот же период количество вредоносных программ выросло на 200%. Компанией Symantec было зафиксировано 1,6 миллиона новых угроз [1]. Только за вторую половину 2008 года количество компьютеров, зараженных вредоносными программами для кражи персональных данных, увеличилось на 800%. При этом на 35% зараженных компьютеров использовалось обновленное антивирусное программное обеспечение.

Вместе с тем, уложняются организационные и програмнно-аппаратные средства защиты информации. Во многих странах на законодательном уровне закрепляются требования к обработке и защите персональных данных.

В Российской Федерации действует Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» [6]. Выполнение требований этого документа создает определенные трудности в осуществлении деятельности юридических лиц России, попадающих под определение понятия «оператор». Согласно закону, оператор – государственный или муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных. При этом под обработкой персональных данных понимаются действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Закон закрепляет обязанность оператора 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. Также законом устанавливается ряд обязательных процедур по учету, оценке, проверке соответствия СЗИ и согласованию изменению условий их применения.

К 1 января 2010 года все информационные системы (ИС) персональных данных РФ должны быть приведены в соответствие с требованиями закона. Этим определяется актуальность рассмотрения угроз безопасности и механизмов защиты ИС персональных данных.

ИЗЛОЖЕНИЕ

1. Безопасность персональных данных и источники угроз

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к ним, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение данных, а также иных несанкционированных действий. Система защита персональных данных в ИС включает организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в ИС информационные технологии.

Кратко остановимся на источниках угроз. К вредоносной активности, которая может нарушить безопасность компьютерной системы, относят сетевые атаки против уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к важным файлам, а также действия вредоносного программного обеспечения (компьютерных вирусов, троянов и червей). По данным исследования «Инсайдерские угрозы в России 2009», потребители средств защиты связывают потенциальную возможность утечки персональных данных, прежде всего, с мобильными накопителями и электронной почтой (см.рис.1.).

Рис.1. Каналы утечки персональных данных

Широкий спектр источников угроз предполагает комплексный подход к решению проблемы защиты персональных данных.

2. Системный подход к обеспечению безопасности персональных данных

Российское законодательство требует, чтобы безопасность персональных данных при их обработке в информационной системе обеспечивалась оператором или лицом, которому на основании договора оператор поручает обработку персональных данных. Однако, для защиты данных в ИС недостаточно установить программно-аппаратные средства защиты. Приобретению и внедрению технологий, обеспечивающих информационную безопасность (ИБ) предприятий, должны предшествовать: аудит текущего состояния ИТ-инфраструктуры и ИБ компании, анализ угроз, разработка политики ИБ при участии инсайдеров, ознакомление (обучение) сотрудников с проблемами угроз и бизнес-процессами с учетом предлагаемой политики ИБ. Важно не только реализовать адекватные технические решения для обеспечения информационной безопасности, но и сформировать корпоративную культуру, включающую ответственное поведение пользователей и соблюдение ими всех правил и процедур.

Стоит отметить, что в РФ законодательно определен перечень мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах. Эти мероприятия включают:

1) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

2) разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

3) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

4) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

5) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

6) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

7) учет лиц, допущенных к работе с персональными данными в информационной системе;

8) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

9) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

10) описание системы защиты персональных данных [4].

Используемые на предприятии технологии и условия обработки на вычислительных средствах персональных данных влияют на построение защиты от утечек. Важно отметить, что защитить можно только тот объект, который локализован как в части используемых приложений, так и в части подключаемых устройств, так и в части используемых приложений. Это отражено и в действующем нормативном документе РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». Доступ к любому используемому ресурсу должен контролироваться (разграничиваться), иначе система защиты информации несостоятельна.

3. Механизмы локализации объекта защиты

Локализация объекта защиты реализуется, прежде всего, на основе механизма обеспечения замкнутости программной среды и механизма управления подключением к системе устройств. Первый механизм можно реализовать путем указания каталогов, из которых разрешен запуск программ и которые запрещено модифицировать. Таким образом, предотвращается возможность запуска любой деструктивной программы как удаленно, так и локально – инсайдером.

Примером реализации механизма обеспечения замкнутости программной среды для осуществления разграничительной политики доступа к исполняемым файловым объектам могут служить такие системы защиты информации (СЗИ), как КСЗИ «Панцирь-К» и КСЗИ «Панцирь-С». В них реализованы следующие схемы задания разграничительной политики доступа к ресурсам:

1) разграничение прав доступа к объектам процессов вне разграничений пользователей (эксклюзивный режим обработки запросов процессов - доступ к объекту разрешается, если он разрешен процессу);

2) разграничение прав доступа к объектам пользователей, вне разграничений процессов (эксклюзивный режим обработки запросов пользователей - доступ к объекту разрешается, если он разрешен пользователю);

3) комбинированное разграничение прав доступа - разграничение прав доступа к объектам процессов в рамках разграничений пользователей (доступ к объекту разрешается, если он разрешен и пользователю, и процессу).

Интерес представляет первая схема (субъект доступа – процесс), так как если задавать разграничения для процессов, то они будут действовать на всех пользователей, в том числе и системных.

При реализации политики разграничения прав доступа к объектам процессов права доступа назначаются не объектам (в качестве атрибутов), а субъектам (в качестве их прав доступа). Настраиваются всего три типа доступа: чтение, запись, выполнение. Остальные типы доступа (удаление, переименование, создание и т.д.) КСЗИ устанавливаются по умолчанию. Для настраиваемых типов доступа может быть задана разрешительная (Ресурсы, разрешенные для…) или запретительная (Ресурсы, запрещенные для…) политика. Субъект «Процесс» задается своим полнопутевым именем. Могут использоваться маски и регулярные выражения. Для каждого субъекта устанавливаются его права доступа (разрешения или запреты по трем типам доступа) к объектам, указываемым своими полнопутевыми именами, масками, либо регулярными выражениями [5].

По сравнению с существующими решениями, основанными на эвристическом и сигнатурном анализах, способ защиты от вторжений, основанный на реализации разграничительной политики доступа к защищаемым ресурсам для субъекта «процесс», расширяет возможности средства защиты от вторжений. Так как он позволяет не только обнаруживать вторжения, но и предотвращать возможность эксплуатации злоумышленником осуществленного вторжения вне зависимости от возможности выявления.

Второй механизм направлен на указание жестко заданного набора устройств, подключение которых разрешается к системе. Оптимальна разрешительная политика управления подключением устройств «все, что не разрешено, то запрещено». Для реализации механизма администратору необходимо сначала выбрать контролируемые классы устройств (например, через «Управление подключением устройств» в ОС Windows) и соответствующую (разрешительную или запретительную) политику для каждого класса. Затем для каждого устройства указать запрет или разрешение на его подключение. Причем настраивать доступ к устройствам необходимо с учетом серийных номеров производителей, если такие номера имеются (см.рис.2). Следует учесть, что некоторые устройства могут иметь родительские и/или дочерние устройства.

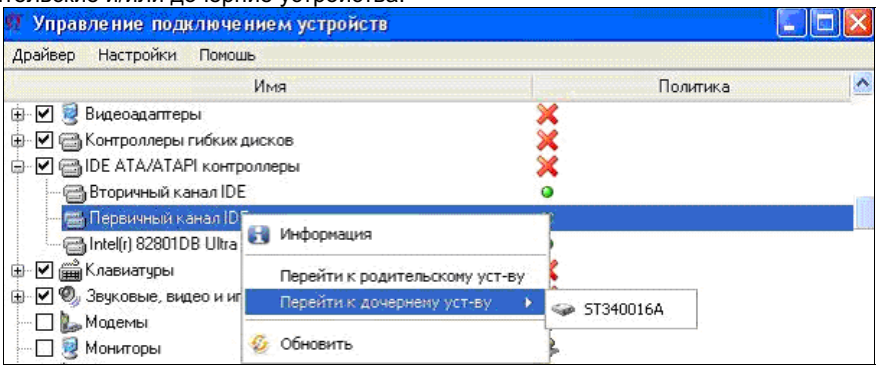

Рис.2. Настройка политики доступа к устройствам

Реализация второго механизма обеспечивает предотвращение несанкционированного подключения к системе иных устройств, кроме тех, которые определяются областью практического использования системы.

ЗАКЛЮЧЕНИЕ

В последние годы потребность в технологиях, программных и аппаратных средствах защиты информации значительно возрасла. Необходимость использования СЗИ при обработке персональных данных операторами, к которым относят почти все юридические и некоторые физические лица, в России теперь закреплена законодательно. Угрозам безопасности персональных данных могут противостоять разработка и внедрение политики ИБ, использование эффективных технических решений, реализация комплекса мероприятий по обеспечению ИБ. Решением задачи локализации объектов защиты является использование механизма обеспечения замкнутости программной среды (например, на основе разграничительной политики доступа к защищаемым ресурсам для субъекта «процесс») и механизма управления подключением к системе устройств.

ЛИТЕРАТУРА

[1] EMEA Internet Security Threat Report от Symantec [Электронный ресурс]. – Режим доступа: ww.itsec.ru (14.04.2009).

[2] Инсайдерские угрозы в России 2009 [Электронный ресурс]. – Режим доступа: www.securitylab.ru (12.02.2009).

[3] Отчет Panda Security. Сайт «Информационная безопасность» [Электронный ресурс]. – Режим доступа: ww.itsec.ru (13.03.2009).

[4] Постановление Правительства РФ от 17 ноября 2007 г. N 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

[5] Технология защиты от утечек конфиденциальной информации и персональных данных ЗАО «НПП «Информационные технологии в бизнесе» [Электронный ресурс]. – Режим доступа: http://www.npp-itb.spb.ru/files/Tech-def-loss.doc (05.09.2009).

[6] Федеральный закон Российской Федерации от 27 июля 2006 г. N 152-ФЗ «О персональных данных».

За контакти:

Ассистент, кандидат экономических наук Анна Юрьевна Савина, Кафедра “Прикладная информатика в экономике”, Поволжский государственный университет сервиса (Россия), тел.: +7-8482-229108, e-mail: annatlt@mail.ru

Докладът е рецензиран.