УДК 681.3

А.М. ФАЛЬ, В.Ф. КОЗАК

ПРОБЛЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИСПОЛЬЗОВАНИИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Аннотация. Проведен анализ использования облачных вычислений с точки зрения выполнения требований защиты персональных данных. Рассмотрены рекомендации для поставщиков и потребителей облачных услуг по реализации принципов обработки персональных данных. Сформулированы положения проекта международного стандарта защиты персональных данных в облаках.

Ключевые слова: облачные вычисления, персональные данные, поставщик облачных услуг, потребитель облачных услуг, принципы обработки персональных данных.

ВВЕДЕНИЕ

В последнее время большую популярность приобрели так называемые облачные вычисления. Точного определения этого понятия не существует, а самым авторитетным его источником является документ, изданный Национальным институтом стандартов и технологий (NIST) США [1]. Идея таких вычислений появилась в 60-х годах для систем с разделением времени, впоследствие превратившихся в системы распределенных вычислений, использующие не один процессор, а множество. Реализовать их можно, например, с помощью кластеров и grid-технологий. Отличие облачных вычислений от распределенных состоит в динамичности используемых ресурсов (вычислительных и средств хранения данных). Специально разработанное программное обеспечение (гипервизор) позволяет организовать вычисления и хранение данных, расположенных в географически отдаленных один от другого местах, с помощью так называемых виртуальных машин. Фактически облачные вычисления предоставляют услуги, по характеру аналогичные коммунальным. В связи с этим оперируют такими терминами, как поставщик и потребитель услуг облачных вычислений.

Преимущество облачных вычислений заключается в возможности для малых и средних предприятий отказаться от существенных капитальных вложений в собственную инфраструктуру и направлять операционные затраты на аренду инфраструктуры поставщика облачных услуг. Этим объясняется термин IaaS (Infrastructure as a Service), применяемый в случае, когда обработка данных контролируется как потребителем облачных услуг, так и их поставщиком. Существует также термин PaaS (Platform as a Service) — обработка данных может контролироваться потребителем, а их расположение определяется поставщиком. И, наконец, очень распространен термин SaaS (Software as a Service), когда используется прикладное программное обеспечение, предоставляемое поставщиком облачных услуг. В этом случае контроль над данными осуществляет поставщик с вытекающими отсюда последствиями. Иногда отдельно выделяют услугу по хранению данных (Storage as a Service), также довольно популярную у потребителей, особенно у физических лиц.

По типу развертывания облака (clouds) подразделяют на частные (private), общедоступные (public) и гибридные (hybrid). В частном облаке обрабатывается и/или хранится информация одного потребителя. Оно может быть сконфигурировано в том числе и из собственных средств обработки информации. В общедоступных облаках ресурсы используются одновременно несколькими потребителями и поэтому возникает так называемая проблема изоляции, чтобы не происходила утечка информации между «соседями». Гибридные облака определяются своим названием.

Рассматривая положительные стороны облаков, не следует забывать об обеспечении безопасности данных (security) и защите персональных данных (privacy).

Под обеспечением безопасности принято считать обеспечение конфиденциальности (confidentiality), целостности (integrity) и доступности (availability). Защита персональных данных предполагает следование принципам, определяемым международными соглашениями [2], законодательными актами межгосударственных объединений [3], рекомендациями международных организаций [4] и национальными законодательствами [5].

В данной статье рассмотрены вопросы защиты персональных данных. Актуальность этих вопросов подтверждается событиями, связанными с развертыванием в США программы PRISM по сбору информации о действиях пользователей Интернета, не являющихся гражданами этой страны.

АНАЛИЗ РЕКОМЕНДАЦИЙ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБЛАКАХ

Содержание настоящей статьи основано на материалах нескольких отчетов [6–8], подготовленных коллективами специалистов в области защиты персональных данных.

Состояние технологии облачных вычислений можно охарактеризовать следующим образом [8]:

— не существует общей установившейся терминологии;

— разработка технологии все еще продолжается;

— аккумулируются и концентрируются огромные объемы данных;

— технология является трансграничной;

— обработка информации становится глобализированной;

— отсутствует прозрачность в отношении процессов, процедур и практик со стороны поставщика и возможных субподрядчиков, что усложняет проведение должного оценивания рисков, а также внедрение правил относительно защиты данных;

— поставщики облачных услуг ощущают зависимость от быстрых капитальных инвестиций;

— потребители ощущают зависимость от скорейшего уменьшения затрат;

— для поддержания низких цен поставщики стараются предлагать стандартные условия предоставления услуг.

Описанные обстоятельства могут привести к следующим повышенным рискам:

— нарушение безопасности информации, т.е. конфиденциальности, целостности или доступности (персональных) данных, не замеченное потребителем;

— передача данных в страны, не обеспечивающие должной защиты персональных данных;

— принятие потребителем условий, которые сформулированы поставщиком облачных услуг так, что позволяют поставщику облачных вычислений обрабатывать персональные данные с нарушением инструкций потребителя;

— возможное использование поставщиками облачных услуг или их подрядчиками персональных данных, предоставленных потребителем, для собственных целей без ведома или разрешения потребителя;

— неконтролируемость потребителем персональных данных и обработки данных;

— невозможность проведения потребителем или его доверенной третьей стороной (например, аудитором) должного мониторинга поставщика облачных услуг.

В сферу облачных вычислений вовлечены несколько сторон. Поэтому необходимо уяснить права и обязательства каждой из них.

Потребитель облачных услуг определяет конечную цель обработки персональных данных и принимает решение о делегировании внешней организации всех функций по обработке персональных данных или их части. Потребитель облачных услуг действует как контроллер (владелец) персональных данных. Он несет ответственность за соблюдение норм законодательства, касающихся защиты этих данных. Потребитель облачных услуг может поставить задачу поставщику облачных услуг о выборе технических и организационных мер для выполнения указанных норм.

Поставщик облачных услуг рассматривается как процессор (распорядитель) персональных данных. В некоторых ситуациях процессор может стать также контроллером персональных данных. Отметим, что даже в сложной среде обработки данных, в которой задействованы различные контроллеры, должна четко распределяться ответственность за соблюдение или нарушение правил защиты данных. Это помогает избегать появления «дыр», когда некоторые обязательства не выполняются ни одной из сторон.

На практике поставщики облачных услуг сами формулируют условия их предоставления и у пользователя ограничены возможности отражения своих требований в заключаемых контрактах. Тем не менее это не избавляет пользователя от соблюдения принципов защиты персональных данных. Поставщик облачных услуг, который намерен заключить контракты с контроллерами персональных данных, должен быть готов к включению в контракт требований к надлежащей обработке таких данных. Еще один способ привлечения клиентов — это проведение сертификации услуг поставщика независимой аудиторской компанией.

Процессоры персональных данных часто нанимают субподрядчиков, которые становятся дополнительными процессорами данных и получают доступ к данным потребителя. Тогда процессоры должны получать разрешение от потребителя с указанием типа предоставляемой субподрядчиком услуги и гарантией выполнения требований защиты персональных данных. Поставщик облачных услуг и его субподрядчик должны заключить контракт, отражающий требования, содержащиеся в контракте между поставщиком облачных услуг и их потребителем.

Законность обработки персональных данных в облаках зависит от выполнения основных законодательных принципов защиты персональных данных, а именно гарантии прозрачности для субъекта персональных данных, соответствия принципа спецификации цели и ограничений, уничтожение персональных данных в связи с ненужностью их дальнейшего хранения. Необходимо реализовать надлежащие технические и организационные меры для обеспечения адекватного уровня защиты и безопасности данных.

Прозрачность в облаках означает, что потребитель осведомлен о всех субподрядчиках, вовлеченных в оказание облачных услуг, о расположении всех дата-центров, в которых могут обрабатываться персональные данные.

Согласно принципу спецификации целей и ограничений персональные данные должны собираться для определенных и легитимных целей и в дальнейшем не обрабатываться способом, не совместимым с этими целями. Необходимо исключить возможность нелегальной обработки персональных данных поставщиком облачных услуг и его субподрядчиками.

Гарантированное уничтожение персональных данных предполагает разрушение носителя информации или их удаление путем неоднократной перезаписи одних данных поверх других. В обеспечении защиты персональных данных особенно важно содержание контрактов или соглашений, заключаемых между поставщиком и потребителем облачных услуг, а также между поставщиком и его субподрядчиками. Приведем рекомендации по составлению таких соглашений [7, 8], в которых должны содержаться следующие положения:

— потребитель предварительно получает полный список информации о физическом расположении мест хранения или обработки данных поставщиком услуг, включая резервирование, на протяжении действия соглашения;

— поставщик облачных услуг не может использовать данные потребителя для собственных целей;

— потребитель имеет право контролировать все аспекты действия поставщика облачных услуг и его подрядчиков касательно того, что персональные данные обрабатываются в соответствии с инструкциями потребителя и легальным способом;

— потребитель имеет право на привлечение третьей доверенной стороны (например, аудиторской фирмы) для проведения мониторинга;

— до использования облачных вычислений потребитель должен совершить оценивание рисков, связанных с обработкой персональных данных поставщиком облачных услуг;

— потребитель должен иметь возможность полностью выполнять свои обязательства по отношению к субъекту данных и уполномоченному органу по защите данных в случае компрометации данных, а поставщик облачных услуг обязан своевременно и полно извещать уполномоченный орган по защите данных о свершившейся компрометации данных;

— поставщик облачных услуг должен обеспечить право субъекта данных получать доступ к своим данным, исправлять ошибки, а также удалять или блокировать свои данные.

Поставщики облачных услуг в Украине сталкиваются с проблемой защиты персональных данных при предоставлении услуг потребителям из стран Европейского Союза. Контракт с потребителем услуг облачных вычислений должен отражать приведенные выше рекомендации и основываться на стандартных контрактных положениях для процессоров персональных данных в третьих странах, утвержденных Европейской Комиссией 5 февраля 2010 года [9].

Потребители облачных услуг сталкиваются с проблемой защиты персональных данных при использовании облачных вычислений, предоставляемых компаниями из стран, не присоединившихся к Конвенции о защите частных лиц в отношении автоматизированной обработки личных данных, в частности компаниями США. Контракт с поставщиком облачных вычислений должен отражать требования Дополнительного протокола к Конвенции о защите частных лиц в отношении автоматизированной обработки данных личного характера от 8 ноября 2001 года [10] и Закона Украины «О защите персональных данных». Типовые контрактные положения разработаны Американской торговой палатой в Украине и согласованы уполномоченным органом Украины по вопросам защиты персональных данных [11].

ОТРАЖЕНИЕ ВОПРОСОВ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ПРИНЯТЫХ И РАЗРАБАТЫВАЕМЫХ СТАНДАРТАХ

Вопросами стандартизации методов защиты персональных данных занимаются в Международной организации по стандартизации (ISO) в рамках 5-й Рабочей группы 27-го Подкомитета 1-го Объединенного технического комитета «Информационные технологии». Подробнее о разрабатываемых стандартах можно ознакомиться на сайте подкомитета www.jtc1sc27.din.de. В настоящей статье рассмотрены лишь положения проекта стандарта ISO/IEC 27018, посвященного проблеме защиты персональных данных в облаках.

В сфере менеджмента безопасности информации фундаментальными являются стандарты ISO/IEC 27001 [12] и ISO/IEC 27002 [13]. В первом из них сформулированы требования к системам менеджмента безопасности информации, а во втором — перечислены меры по обеспечению безопасности информации и изложены рекомендации по их реализации. Рассмотренный далее проект стандарта ISO/IEC 27018 имеет структуру, подобную ISO/IEC 27002. Все положения стандарта ISO/IEC 27002 повторены в ISO/IEC 27018. Они дополнены новыми положениями, отражающими специфику облачных вычислений.

Далее приведены формулировки стандарта ISO/IEC 27002, дополненные новыми рекомендациями. В проекте имеется также дополнение A, содержащее положения, отражающие принципы обработки персональных данных. Отметим, что употребление в стандартах ISO термина PII (Personally Identifiable Information) эквивалентно термину «персональные данные», а также то, что в данном стандарте поставщик облачных услуг является процессором персональных данных, а потребитель этих услуг — их контроллером.

Как указывалось выше, в проекте стандарта ISO/IEC 27018 сохранены нумерация и названия разделов стандарта ISO/IEC 27002. Рассмотрим содержание лишь тех разделов (а также сохраним их нумерацию), в которых приведены рекомендации относительно защиты персональных данных. Разделы приложения A стандарта ISO/IEC 27018 изложены в соответствии с принципами защиты персональных данных, сформулированными в стандарте ISO/IEC 29100.

5.1.1. Политики обеспечения безопасности информации. Политики должны содержать положение, касающееся поддержки и обязательства обеспечивать соответствие с применяемым законодательством о защите персональных данных и с условиями контракта, заключенного между поставщиком облачных услуг и его клиентами (потребителями облачных услуг).

Могут существовать изменяющиеся или разделяемые функции, распределенные между потребителем облачных услуг и их поставщиком. В результате, потребители облачных услуг обязаны определять и выполнять свои собственные политики и процедуры обеспечения безопасности информации и защиты персональных данных. Например, потребители облачных услуг, чьи сотрудники производят и эксплуатируют собственные приложения в облаках, могут проводить собственное оценивание рисков и реализовывать собственные мероприятия по их модификации.

Существуют юрисдикции, в которых облачный процессор персональных данных напрямую обязан выполнять нормы законодательства о защите PII. Это должно отражаться в контракте между потребителем облачных услуг и их поставщиком.

7.2.2. Осведомленность об обеспечении безопасности информации, обучение и тренинг. Необходимо проведение мероприятий для осведомления соответствующего персонала о возможных последствиях (физических, материальных, эмоциональных) для субъекта PII, связанных с нарушением правил и процедур обеспечения защиты PII и их безопасности.

12.3.1. Резервирование информации. Облачный процессор PII (он же поставщик облачных услуг) должен иметь политику, которая касается требований к резервированию информации, условий контракта, а также правовых требований к уничтожению PII, которые могут содержаться в резервных копиях.

12.4.1. Регистрация событий. Необходимо обеспечение мер для доступа офицера безопасности к проверке журнала событий, где задокументирована определенная периодичность, для выявления нерегулярности и указания действий по ее устранению.

По возможности и в журнале событий должны содержаться записи об изменениях в PII (добавление, модификация или удаление) в результате происшедшего события с указанием ответственного лица.

Облачный процессор PII должен определять процедуры доступа к информации в журнале и ее использования потребителем облачных услуг.

13.2.1. Политики и процедуры передачи информации. Должна существовать система регистрации поступающих и «покидающих» организацию физических накопителей, содержащих PII, включая тип и количество физических накопителей, дату и время, типы PII, содержащихся в них.

16.1. Менеджмент инцидентов безопасности информации и улучшения

16.1.1. Обязанности и процедуры. Инцидент, связанный с нарушением безопасности информации, должен инициировать анализ со стороны облачного процессора PII, как часть управления инцидентами безопасности информации, с целью определения, было ли нарушение PII, включающее его потерю, раскрытие или изменение. В случае нарушения должны поддерживаться записи с описанием инцидента и его последствия, временной отрезок, имя докладывающего об инциденте и адресата, шаги, предпринятые для разрешения инцидента (включая ответственное лицо), и факт, что результатом инцидента были потеря, раскрытие, изменение PII. Запись должна включать описание скомпрометированных данных (если это известно) и шаги, сделанные для извещения потребителя услуг и/или регулирующих органов.

18.2.1. Независимый анализ безопасности информации. В случаях, когда индивидуальные аудиты потребителями облачных услуг являются непрактичными или могут увеличить риски нарушения безопасности, облачный процессор PII должен до составления контракта сделать доступным для потенциальных потребителей облачных услуг независимое доказательство того, что обеспечение безопасности

информации осуществляется в соответствии с политиками и процедурами облачного процессора PII. Подходящим методом есть проведение независимого аудита.

A.1.1. Обязательство сотрудничать касательно прав субъекта PII. Облачный процессор PII должен выполнять обязательства контроллера PII, способствовать реализации прав субъекта PII на доступ, исправление и/или уничтожение касающейся его PII.

A.2.2. Коммерческое использование PII облачным процессором. Необходимо установление меры по обеспечению защиты PII, обрабатываемых в соответствии с контрактом, от несанкционированного использования для маркетинга и рекламы.

Предоставление таких санкций не должно являться условием получения услуги.

A.4.2. Безопасное уничтожение временных файлов. Должны быть осуществлены меры по уничтожению через задокументированный период временных файлов и документов.

A.5.1. Извещение о раскрытии PII. В контракте между облачным процессором PII и потребителем облачных услуг должно предусматриваться обязательное извещение облачным процессором PII потребителя облачных услуг о любом легальном запросе на раскрытие PII со стороны правоохранительных органов.

A.5.2. Регистрация раскрытий PII. Информация о регистрации раскрытия PII должна содержать сведения о том, какие PII были раскрыты, кому и в какое время.

A.7.1. Раскрытие обработки PII субподрядчиками. В контракте должны содержаться положения об использовании субподрядчиков для обработки PII, а именно, что субподрядчики могут быть задействованы лишь с согласия потребителя облачных услуг, предоставленного в начале получения услуги. Облачный процессор PII должен своевременно извещать потребителя о намечаемом изменении привлеченных субподрядчиков. В контракте необходимо указывать имена субподрядчиков и страны, в которых они действуют.

A.10.1. Соглашения о конфиденциальности или неразглашении. Контракт между облачным процессором PII и его сотрудниками должен содержать раздел о конфиденциальности, согласно которому сотрудники не могут раскрывать PII для нужд, не согласующихся с инструкциями потребителя облачных услуг.

A.10.2. Ограничение на создание твердых копий. Необходимо установление мер по ограничению создания твердых копий, содержащих PII.

A.10.3. Контроль и регистрация восстановления данных. Должна существовать процедура восстановления данных и ее регистрация.

A.10.4. Защита данных, хранящихся на переносных носителях информации. Должна существовать процедура, обеспечивающая для PII на переносных носителях информации авторизацию и защиту доступа тем, у кого нет на это полномочий (например, с помощью шифрования).

A.10.5. Использование носителей с незашифрованными данными. Должны быть установлены меры для обеспечения блокирования физических носителей и переносных устройств, в которых не существует возможности шифрования. Если невозможно избежать использования таких средств, это должно быть задокументировано.

A.10.6. Шифрование PII, передаваемой по открытым сетям. Должна быть установлена процедура по шифрованию PII, передаваемой через открытые сети.

A.10.7. Гарантированное уничтожение твердых копий. Должны использоваться механизмы для гарантированного уничтожения твердых копий.

A.10.8. Уникальное использование идентификаторов. Если к хранимой PII имеют доступ несколько лиц, должны быть установлены меры для обеспечения каждому лицу индивидуального идентификатора для нужд идентификации, аутентификации и предоставления полномочий.

A.10.9. Регистрация уполномоченных пользователей. Необходимо ведение актуальных записей пользователей или профилей пользователей, которые имеют доступ к информационной системе.

A.10.10. Управление идентификаторами. Должны быть установлены меры блокирования идентификаторов, срок действия которых истек, для других лиц.

Важно учитывать положения стандарта ISO/IEC 29100 [14] в части максимально возможного выполнения псевдономизации персональных данных перед их передачей поставщику облачных услуг.

ЗАКЛЮЧЕНИЕ

Проблема защиты персональных данных приобретает все большую актуальность особенно в связи с многочисленными публикациями, раскрывающими факты незаконного использования таких данных. В Украине вопросам защиты персональных данных посвящены различные научно-технические мероприятия, на которых отмечается недостаток методических материалов, посвященных защите персональных данных. Тем более это справедливо для ситуации с использованием облачных вычислений. Рассмотренные в данной статье рекомендации могут в некоторой степени восполнить этот пробел.

СПИСОК ЛИТЕРАТУРЫ

1. National Institute of Standards and Technology (NIST), Special Publication 800-145, The NIST Definition of Cloud Computing, September 2011.
2. Council of Europe. Convention on protection of individuals with regard to automatic processing of personal data. Strasbourg, 28 Jan. 1981. — http://conventions.coe.int/Treaty/rus/Treaties/Html/108.htm.
3. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data. — http://zakon3.rada.gov.ua/laws/show/994_242.
4. Organization for Economic Cooperation and Development. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. — http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.
5. Закон України «Про захист персональних даних». — http://zakon4.rada.gov.ua/laws/show/2297-17.
6. ENISA, Report on Cloud Computing: Benefits, risks and recommendations for information security, November 2009.
7. European Union, 29 Article Working Party, Opinion 05/2012 on Cloud Computing, July 2012.
8. International Working Group on Data Protection in Telecommunications, Working Paper on Cloud Computing — Privacy and data protection issues — “Sopot Memorandum”, April 2012.
9. European Commission. Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council. — http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm#h2-5.
10. Council of Europe. Additional Protocol to the Convention on protection of individuals with regard to automatic processing of personal data regarding supervisory authorities and transborder data flows. Strasbourg, 8 Nov. 2001. — http://zakon2.rada.gov.ua/laws/show/994_363.
11. American Chamber of Commerce in Ukraine. Corporate Code of Conduct on the Transborder Transfer of Personal Data. — http://www.chamber.ua/files/documents/updoc/32/Agreement_PD_transfer_cont_proc_Chamber_logo.pdf.
12. ISO/IEC 27001:2005, Information technology — Security techniques — Information security management systems — Requirements.
13. ISO/IEC 27002:2005, Information technology — Security techniques — Code of practice for information security management.
14. ISO/IEC 29100:2011, Information technology — Security techniques — Privacy framework.

Поступила 20.01.2014