О некоторых аспектах защиты информации в Единой системе информационно-аналитического обеспечения деятельности МВД России

Фомин
Геннадий Александрович,
заместитель начальника подразделения
ФГКУ «Войсковая часть 43753»,
подполковник

Настоящая материал посвящен ключевым вопросам обеспечения защиты конфиденциальной информации при ее обработке и передаче между компонентами создаваемой Единой системы информационно-аналитического обеспечения деятельности МВД России с учетом архитектуры данной системы, предусматривающей использование технологии «облачных сред».

Ведомственная Единая система информационно-аналитического обеспечения деятельности МВД России (ЕСИАО), создаваемая на основе технологии «облачных сред», является информационной распределенной системой обработки и хранения конфиденциальной информации и объединяет в себе как существующие и эксплуатируемые, так и разрабатываемые для нужд ОВД прикладные распределенные информационные системы (ИС) и банки данных (БД).

Само по себе использование технологии «облачных» вычислений, а также защита информации в «облаке» — относительно новые вопросы, в решении которых, как в мировой практике, так и в России накоплено немного опыта. В этой связи возникают обоснованные трудности даже по поводу решения следующих очевидных вопросов:

- можно ли размещать ИС, обрабатывающие конфиденциальную информацию, в «облаке» с учетом требований регулирующих органов по защите информации;
- какими свойствами должно обладать «облако», чтобы его можно было использовать для построения ИС, обрабатывающих конфиденциальную информацию;
- что необходимо учесть при переносе информационных ресурсов в «облако»;
- какими средствами обеспечить взаимное невлияние ИС, размещенных в «облаке», и возможна ли атака из одной подсистемы на другую внутри «облака».

Действующие законодательство не создает принципиальных препятствий для обработки конфиденциальной информации в «приватном облаке», положенном в основу ЕСИАО. Однако необходимо учитывать особенность ЕСИАО, заключающуюся в объединении существующих ИС и БД, с которыми взаимодействуют данные ИС, к которым предъявляются, возможно, неодинаковые требования по защите информации. И, если в ранее создававшейся ЕИТКС ОВД указанные ИС и БД представлялись в значительной мере изолированными друг от друга, требующими, возможно, разных полномочий персонала по доступу к различным категориям информации, то в условиях «облачной» инфраструктуры данная изолированность и достаточность мер разграничения доступа при переносе ИС и БД в центры обработки данных (ЦОД) требует обоснования.

С учетом существующего в настоящий момент многообразия ИС, разрабатываемых, внедряемых и уже внедренных в ОВД, должны быть локализованы те, которые обрабатывают конфиденциальную информацию, и для таких ИС при переносе в «облако» должна быть проведена оптимизация типов данных, способов их представления и хранения, что позволило бы избежать предъявления чрезмерно строгих требований к составу и функциям средств защиты информации и разграничения доступа к ней в ЦОД и АРМ пользователей. Решение данной задачи особенно актуально для ИС, обрабатывающих информацию, относимую к категории «персональные данные» в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 г. N 152-ФЗ «О персональных данных».

Дополнительная сложность при переносе БД и ИС в ЦОД возникает в связи с особенностями самой технологии «облачных вычислений», предполагающих наличие механизма виртуализации в ЦОД, которые, скорее всего, потребуют доработки средств разграничения доступа внутри прикладных ИС при развертывании серверной их части на средствах ЦОД, а также разработки новых средств разграничения доступа, учитывающих технологию виртуализации. В то же время для клиентской части прикладных ИС необходимо завершить внедрение в подсистемы предусмотренных инструментов зашиты информации, прежде чем начать перенос данных в «облако».

Представляется, что в указанном направлении основные проблемы объединения БД и ИС в «облаке» связаны не столько с технологией «облачных вычислений» как таковой, сколько с общей неопределенностью и незавершенностью работ, унаследованной от создававшейся ранее ЕИТКС ОВД.

При переносе ИС и банков данных в «облако» необходимо выделить три основных элемента, требующих реализации механизмов защиты ([3]):

- совокупность АРМ пользователей на стороне ОВД;
- каналы связи между АРМ и ЦОД;
- совокупность виртуальных машин в ЦОД, на которых функционирует серверное ПО соответствующих прикладных ИС.

К указанным элементам также необходимо добавить еще один, обусловленный особенностью ЕСИАО, элемент — шлюзовые компоненты, обеспечивающие интерфейс с межведомственной системой электронного взаимодействия (МСЭВ) и с подсистемой регистрации и обработки электронных обращений граждан (ЭОГ).

Для устранения угроз информационной безопасности принципиальной является необходимость использования сертифицированных средств защиты в отношении каждого из обозначенных выше элементов.

Основные источники угроз для элементов ЕСИАО:

1. Внутренние пользователи ОВД, реализующие атаки на ресурсы, размещенные на объекте ОВД.
2. Внешние злоумышленники, реализующие атаки на ресурсы, размещенные на объекте ОВД.

Угрозы данного типа должны предотвращаться непосредственно на каждом объекте ОВД с использованием сертифицированных средств защиты локальных АРМ, серверов и сетевого окружения.

3. Внешние злоумышленники, атакующие канал связи снаружи с целью перехвата или искажения сетевого трафика;

Эта угроза должна нейтрализовываться использованием сертифицированных средств криптографической защиты сетевого трафика.

4. Персонал ЦОД, обслуживающий серверные компоненты «облака» и связанные с ними телекоммуникационные средства.

Для нейтрализации данной части угроз требуются средства разграничения прав доступа персонала к ресурсам «облачной» платформы, которые могут быть интегрированы в саму платформу ЦОД. Дополнительно, в зависимости от реализованных в ЦОД прикладных ИС, могут использоваться сертифицированные средства защиты, специфичные для данных ИС, которые развертываются на компонентах ЦОД.

5. Внешние злоумышленники, реализующие атаки из-за пределов ЦОД на ресурсы ЦОД и, соответственно, на ресурсы ИС, размещенные в ЦОД.

В данном случае также требуется применение сертифицированных средств криптографической защиты трафика и средств разграничения доступа, которые, в зависимости от реализации, могут являться как частью средств ЦОД, так и частью средств защиты, специфичных для каждой конкретной ИС, развернутой на средствах ЦОД в виде «виртуальной машины».

6. Размещенные в ЦОД ИС, к которым изначально не предъявлялись требования по защите информации или которые имеют доступ к внешним по отношению ЕСИАО информационным системам (ЭОГ, МСЭВ), а также ИС, программные средства которых не проходили исследования на предмет наличия уязвимостей или внедренных средств компьютерных атак, и пользователи которых могут использовать уязвимости ИС и самой платформы ЦОД для атаки из «облачной» среды на другие ИС.

Нейтрализовать данные угрозы могут средства разграничения ресурсов самой «облачной» платформы между прикладными ИС, развернутыми на ее основе. При этом необходимо отметить, что по отношению к ЦОД и развернутым на средствах ЦОД прикладным ИС, компоненты подсистем МСЭВ и ЭОГ должны рассматриваться как внешние нарушители, реализующие атаки на ресурсы ЦОД извне ЕСИАО. Следовательно, с целью снижения затрат на реализуемые в составе ЦОД и АРМ пользователей ЕСИАО средства защиты информации, необходимо обеспечить в компонентах подсистем МСЭВ и ЭОГ, предназначенных для взаимодействия с ЦОД, защиту от действий внутреннего нарушителя, тип которого соответствует типу внешнего для ЦОД нарушителя.

В контексте последнего типа угроз важен аспект, специфичный именно для «облачной» технологии — применение механизма виртуализации. Типичными угрозами для виртуальной среды в ЦОД следует считать ([2]):

- внедрение вредоносного программного обеспечения при работе пользователей с ИС, развернутой на виртуальной платформе;
- несанкционированный сетевой доступ внутри виртуальной инфраструктуры;
- несанкционированное изменение виртуальных машин в выключенном состоянии;
- компрометация образов виртуальных машин.

В связи с этим возникает необходимость проведения исследований средств виртуализации — гипервизора вычислительных ресурсов, системы управления виртуализованной сетью передачи данных, платформы виртуализации системы хранения данных — на соответствие действующим требованиям по защите от несанкционированного доступа к защищаемой информации.

Очевидно, что программно-технические средства ЦОД, реализующие «облачную» технологию ЕСИАО, с учетом наличия разных полномочий пользователей по доступу к разной информации, являются автоматизированной системой, имеющей класс 1Г в соответствии с [1], а при наличии возможности изменения полномочий пользователей — 1 В, и в соответствии с указанными классами должна обеспечиваться защищенность ЦОД и реализованных на их средствах прикладных ИС.

Без предварительной реализации в ЦОД и на АРМ пользователей комплекса мер, позволяющих обеспечить для переносимых ИС невозможность реализации вышеперечисленных угроз, развертывания (встраивания) и ввода в эксплуатацию сертифицированных средств защиты информации и средств разграничения доступа к ресурсам ИС, размещенным на ЦОД, перенос ИС и БД на ресурсы ЦОД без угрозы нарушения конфиденциальности и целостности обрабатываемых данных невозможен.

Литература.

1. РД ФСТЭК России «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации». Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.
2. «Защита ключевых ресурсов в частном облаке». PC Week Review: ИТ-безопасность, май 2012 г.
3. Александр Шибаев. «Из тумана — в облака. Информационная безопасность в облаке». ИКС №07–08 2012 стр. 64.