Создание системы защиты информации в составе информационно-технологической инфраструктуры МВД России с учетом ее «облачной архитектуры»

Воробьев
Александр Владимирович,
начальник Управления защиты информации ДИТСиЗИ МВД России, майор внутренней службы

Поваров
Виталий Васильевич,
заместитель начальника Управления — начальник отдела организации управленческой деятельности и оценки эффективности реализации функций в области защиты информации Управления защиты информации ДИТСиЗИ МВД России, полковник внутренней службы

В разрезе государственной политики, проводимой в информационной сфере, приоритетными являются вопросы обеспечения устойчивости и безопасности функционирования государственных информационных систем и гарантированной защищенности обрабатываемых в их составе информационных активов, включая массивы персональных данных.

В контексте рассматриваемого вопроса следует отметить критичность информационной сферы Министерства внутренних дел Российской Федерации[1] относительно реализации требований по защите информации.

МВД России является не только держателем значительных массивов служебной информации, доступ к которой ограничен законодательством и иными правовыми актами, но и выступает крупным оператором, обеспечивающим обработку персональных данных граждан.

В условиях устойчивого усиления угроз информационной безопасности, обусловленного возросшим потенциалом разведслужб других государств и технической оснащенностью преступных сообществ, обеспечение адекватного уровня безопасности информационных активов и поддерживающей инфраструктуры требует тщательно продуманной работы с акцентом на реализацию мер в области технической защиты информации.

В системе МВД России функции головного подразделения в области противодействия техническим разведкам, технической (в том числе криптографической) защиты информации, координации и контроля деятельности по защите персональных данных при их автоматизированной обработке выполняет Департамент информационных технологий, связи и защиты информации Министерства внутренних дел Российской Федерации[2].

Основные мероприятия по защите информации в системе МВД России осуществляются силами подразделений по противодействию техническим разведкам и технической защите информации, созданным во всех территориальных органах МВД России на региональном уровне.

Основным проблемным вопросом, который пришлось решать ДИТСиЗИ МВД России с момента создания в структуре Министерства, стало отсутствие либо неадекватность систем защиты информации в составе большей части ранее созданных информационных систем. Отсутствие корректных механизмов безопасности при предоставлении доступа к ресурсам также создавали неконтролируемые инциденты в области информационной безопасности. Создание в сложившихся условиях так называемых «наложенных» систем защиты информации для разрозненных и реализованных на разных аппаратно-программных платформах информационных систем — решение малоэффективное и экономически нецелесообразное.

Ключевым событием, позволившим решить эту системную проблему и приступить к реализации мер по приведению ведомственной системы защиты информации в соответствие установленным требованиям, послужило решение руководства Министерства о принципиальной модер-

1 Далее МВД России или Министерство

2 Приказ МВД России от 16.06.2011 №681.

низации информационно-коммуникационной платформы органов внутренних дел Российской Федерации.

Основные решения по совершенствованию информационной безопасности были заложены в комплексе задач по созданию на базе единой информационно-телекоммуникационной системы ОВД единой системы информационно-аналитического обеспечения деятельности МВД России, объединяющей в единое информационное пространство (в виде общесистемных и прикладных сервисов обеспечения оперативно-служебной деятельности) аппаратно-программные средства на принципах «облачных технологий».

Вместе с тем необходимо отметить, что найти правильные подходы к решению такой сложной задачи было бы очень сложно без поддержки государственных регуляторов. Поэтому еще на этапе разработки системы защиты информации в составе ИСОД МВД России было организовано конструктивное взаимодействие с ФСБ России и ФСТЭК России.

При такой организации работ удалось в короткие сроки найти оптимальные для Министерства подходы к модернизации ведомственной системы защиты информации и создать необходимые условия для устранения недостатков, отмеченных ранее в рамках государственного контроля.

Принятая МВД России техническая идеология, по нашему мнению, очень перспективна с точки зрения организации защиты информации и позволяет, несмотря на масштабность и технологическую сложность ИСОД МВД России, выделить в ее составе типовые участки и предъявить к ним унифицированные требования по защите информации.

Соответственно, по степени централизации информационных активов в «облачной компоненте» путем их миграции из ранее созданных информационных систем и ввода в эксплуатацию сервисов ИСОД МВД России, не соответствующие требованиям безопасности информационные системы в ближайшие годы будут выводиться из эксплуатации.

Учитывая, что эффективность системы защиты информации прямым образом определяется пониманием объективных угроз в этой сфере, на начальном этапе проведен анализ степени значимости информации, планируемой к обработке в составе ИСОД МВД России, на основании которого в установленном порядке разработаны и утверждены (03.04.2014) Модели угроз, включая угрозы безопасности персональных данных, и Модели нарушителя безопасности информации, которые актуальны при обработке в ИСОД МВД России.

В целях ограничения доступа к информационным ресурсам ИСОД МВД России определены дифференцированные требования по обеспечению безопасности информации для контура обработки информации, составляющей государственную тайну, и контура обработки информации ограниченного доступа, не составляющей государственную тайну. Также определены требования по обеспечению безопасности информации при доступе к информационным ресурсам ИСОД МВД России с использованием мобильных устройств.

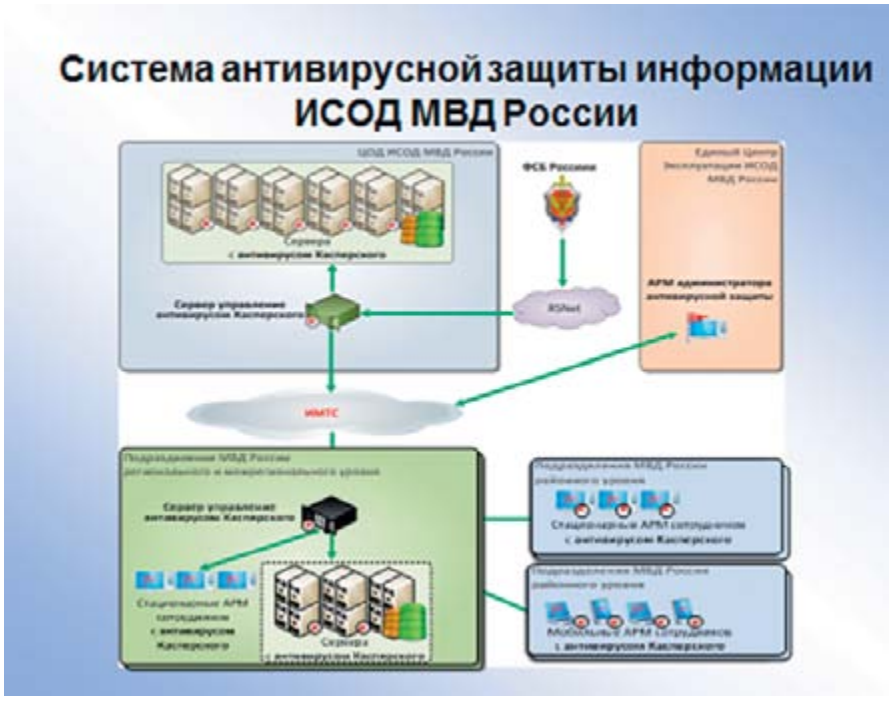
На их основе выработаны организационные и технические меры, составляющие комплексную и взаимоувязанную подсистему обеспечения информационной безопасности ИСОД МВД России, внедряемую в настоящее время на всех уровнях территориальных органов МВД России.

В текущем году реализованы мероприятия по правовому регулированию вопросов обеспечения информационной безопасности ИСОД МВД России в рамках приказа МВД России, регламентирующего вопросы организации эксплуатации единой системы информационно-аналитической деятельности МВД России.

Подсистема обеспечения информационной безопасности ИСОД МВД России является централизованно управляемой и функционирует с учетом строгого протоколирования событий информационной безопасности и систематического аудита информационной безопасности на предмет уязвимостей на всех уровнях информационно-технологической инфраструктуры ИСОД МВД России.

На уровне реализации организационно-технических мероприятий формируется технологическая инфраструктура обеспечения информационной безопасности ИСОД МВД России, включающего применение следующих аппаратных и программных средств защиты информации: криптографической защиты информации, включая средства электронной подписи, антивирусного программного обеспечения, сервиса управления доступом к информационным системам и ресурсам, персональных электронных идентификаторов.

Для обеспечения информационной безопасности ИСОД МВД России используются исключительно программно-аппаратные комплексы и программные средства защиты информации российского производства, сертифицированные ФСБ России и ФСТЭК России. Вместе с тем в рамках государственного оборонного заказа также выполнены работы по созданию собственного специального программного обеспечения, в том числе реализующего функционал защиты информации, на основе свободного программного обеспечения.



В рамках организации доступа сотрудников МВД России к сервисам ИСОД МВД России внедряется **Программное обеспечение сервиса управления доступом к информационным системам и ресурсам** (далее СУДИС), реализующее функции защиты от несанкционированного доступа к информации в части идентификации и строгой аутентификации пользователей в рамках делегированных прав доступа.

При этом доступ к ресурсам ИСОД МВД России осуществляется на основе единственно возможной учетной записи со сложным паролем, с использованием **персонального электронного идентификатора ruToken**.

Программно-аппаратное СКЗИ КриптоПроCSP усиливает механизм аутентификации пользователя за счет сверки предъявленной учетной записи с данными сертификата-ключа проверки электронной подписи, записанного в защищенной области памяти персонального электронного идентификатора ruToken.

Для создания защищенной транспортной среды передачи данных на всех уровнях технологической инфраструктуры ИСОД МВД России формируется сеть конфиденциальной связи МВД России с использованием **программных средств криптографической защиты конфиденциальной информации** (далее СКЗИ) (ViPNet Administrator, ViPNet StateWatcher, ViPNet Client), а также **программно-аппаратных СКЗИ** (ViPNet Coordinator HW 1000 и ПАК ViPNet Coordinator HW 2000).

Результаты ведомственного контроля показали, что наиболее актуальной угрозой информационной безопасности для МВД России является проникновение в информационные системы вредоносного кода. В целях минимизации этой категории угроз в рамках подсистемы обеспечения информационной безопасности ИСОД МВД России сформирована технологическая **инфраструктура антивирусной защиты на базе программного обеспечения Kaspersky**. В составе инфраструктуры антивирусной защиты в «облачных компонентах» ИСОД МВД России (в том числе в 96 территориальных органах МВД России на региональном уровне) развернута иерархическая система серверов антивирусной защиты, управляемая головным компонентом системы — сервером управления, мониторинга и обновления вирусных баз клиентского ПО Kaspersky (далее управляющий сервер), размещенным на технологической площадке ЦОД.

Во всех подразделениях центрального аппарата и территориальных органах МВД России организовано автоматическое получение обновлений средств антивирусной защиты и баз вирусных сигнатур с управляющего сервера, получающего в автоматическом режиме доверенным способом обновления баз вирусных сигнатур с антивирусного портала ФСБ России.

В настоящее время к централизованной системе управления, мониторинга и обновления антивирусных баз подключено порядка 90 000 пользовательских АРМ. Благодаря принятым техническим мерам и своевременному реагированию на эти инциденты в текущем году общее количество вирусных заражений АРМ, имеющим подключение к ИСОД МВД России, снизилось с показателя 10% и в настоящее время не превышает 1,5%.

Учитывая возрастающие угрозы информационной безопасности, обусловленные компьютерными атаками, реализована первая очередь ведомственного сегмента государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на критически важных объектах ИСОД МВД России, на которых обрабатывается значительное количество трафика и хранится значительный объем данных.

Приведенные выше конкретные типы технических средств определены на принципах научно-обоснованного подхода применительно к аппаратно-программной и программной реализации информационно-технологической инфраструктуры ИСОД МВД России.

К числу очередных мероприятий, реализация которых актуальна для МВД России в рассматриваемой области деятельности, относятся:

- проведение сертификации разработанного для нужд МВД России программного обеспечения сервисов ИСОД МВД России, в том числе реализующего функции защиты информации;
- организация и реализация работ по аттестации ИСОД МВД России с учетом облачной архитектуры.

В завершении статьи считаем необходимым остановиться на крайне важном аспекте. Как хорошо известно, надежность любых принимаемых технических мер обеспечения безопасности информации в конечном итоге зависит от человеческого фактора. Поэтому делаем акцент на неукоснительном соблюдении культуры обеспечения информационной безопасности на этапе эксплуатации ИСОД МВД России, сущностью которой является не только личная ответственность руководителей всех уровней за организацию защиты информационных ресурсов, но также и строгое выполнение установленных правил обеспечения безопасности информации каждым отдельным сотрудником.