Каланда
Владимир Александрович,
первый заместитель директора Федеральной службы Российской Федерации по контролю за оборотом наркотиков

Основные направления защиты информации в органах наркоконтроля

Из широкого спектра вопросов, связанных с информационной безопасностью, вопрос защиты информации является наиболее актуальным. Это связано как с большими объемами информации, обрабатываемой в автоматизированных информационных системах органов наркоконтроля, так и с относительно простой возможностью ее добывания средствами разведки и злоумышленниками в случаях невыполнения установленных требований по защите информации.

Обеспечение защиты информации в органах наркоконтроля осуществляется на основе следующих базовых принципов:

- деятельность по обеспечению защиты информации строится в строгом соответствии с действующими нормативными правовыми актами Российской Федерации;
- обеспечение защиты информации достигается за счет комплексного использования всей совокупности организационно-режимных, технических, программных и криптографических методов защиты информации, а также осуществления непрерывного всестороннего контроля эффективности реализованных мер по обеспечению защиты информации;
- принятые меры по обеспечению защиты информации должны обеспечивать эффективную защиту информации на протяжении всего жизненного цикла во всех звеньях и на всех этапах ее обработки, хранения и передачи по каналам связи с минимально возможными ограничениями в эксплуатации, накладываемыми на абонентов и пользователей системы;
- защите подлежит как информация, содержащая сведения, составляющие государственную тайну, так и служебная информация ограниченного распространения, в том числе персональные данные;
- выбор конкретных методов и средств защиты информации осуществляется с учетом разумной достаточности достигаемого при этом уровня защищенности информации в зависимости от степени ее секретности (важности);
- для защиты информации применяются только сертифицированные и стандартизированные средства защиты информации отечественной разработки и производства.

Защита информации в органах наркоконтроля обеспечивается выполнением комплекса следующих мероприятий:

- по предотвращению утечки информации по техническим каналам и несанкционированного доступа к ней;
- по предупреждению преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе обработки, передачи и хранения;
- по противодействию иностранным техническим разведкам.

Основной мерой технической защиты информации является аттестация объектов информатизации на соответствие требованиям по безопасности информации.

Под аттестацией объектов информатизации по требованиям безопасности информации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа – аттестата соответствия требованиям по безопасности информации – подтверждается, что объект информатизации соответствует требованиям стандартов или иных нормативных документов по защите информации, утвержденных ФСТЭК России или другими федеральными исполнительными органами власти в пределах их компетенции.

В связи с развитием информационных технологий, увеличением объема документооборота, ввода в эксплуатацию новых функциональных автоматизированных информационных систем потребность в аттестованных объектах информатизации постоянно растет.

В ФСКН России в 2003 г. на основании полученных во ФСТЭК России аттестата аккредитации органа по аттестации и лицензии на осуществление мероприятий в области защиты государственной тайны в части технической защиты информации создан и функционирует ведомственный орган по аттестации. Аттестационным центром ФСКН России в период с 2003 г. по настоящее время проведено более 1100 аттестационных испытаний объектов информатизации органов наркоконтроля. Основные усилия направлены на защиту ключевых систем информационной инфраструктуры органов наркоконтроля, таких как: оперативно-справочный банк данных, оперативные учеты, централизованные учеты органов наркоконтроля и др.

Укомплектованность подготовленными специалистами и оснащение программными и программно-аппаратными комплексами для проведения аттестационных испытаний позволили в 11 раз увеличить количество объектов информатизации, ежегодно аттестуемых ведомственным органом по аттестации, по сравнению с 2003-2004 гг., доведя их количество до 300 объектов в год.

Вместе с тем рост количества аттестованных объектов информатизации требует увеличения количества подготовленных администраторов безопасности автоматизированных систем, а также повышения уровня

знаний пользователями требований нормативных документов в области защиты информации. Поэтому наряду с организацией мероприятий по технической защите информации в органах наркоконтроля в соответствии с планами служебной подготовки проводятся занятия с сотрудниками по вопросам обеспечения защиты информации, организуется обучение администраторов безопасности автоматизированных систем в специализированных учебных заведениях.

Также актуальной и значимой темой в ФСКН России является межведомственное информационное взаимодействие, выполняемое с обязательным соблюдением требований нормативно-правовых актов и действующих федеральных законов Российской Федерации по обеспечению безопасности информации.

Так, в рамках заключенных соглашений об информационном взаимодействии с органами исполнительной власти (МВД России, ФСБ России, ФМС России) дополнительно разрабатывались и согласовывались протоколы по обеспечению безопасности информации.

При подготовке требований по обеспечению безопасности информации, не содержащей сведений, составляющих государственную тайну, в том числе и персональных данных, привлекались организации, имеющие соответствующие лицензии ФСБ России и ФСТЭК России с целью разработки и внедрения системы защиты информации соответствующей категории и класса защищенности. Указанная методика применялась при выполнении работ по обеспечению безопасности информации ведомственных информационных ресурсов, а также при подготовке к выполнению требований Федерального закона от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» в части оказания государственных функций и услуг в электронном виде.

Сотрудники ФСКН России принимают активное участие в изучении использования IT-инноваций при организации обеспечения оперативно-служебной деятельности органов наркоконтроля. В настоящее время рассматриваются варианты использования информационных систем с централизованной системой хранения, управления и обеспечения безопасности информации, таких как DATA-центры.

В основном данный выбор обусловлен высокими показателями при выполнении требований по защищенности и сохранности данных, высокой скоростью их обработки, доступностью и в то же время безопасностью. Так, например, в настоящее время уже большая часть информационной инфраструктуры ФСКН России переведена в создаваемый и периодически модернизируемый DATA-центр.

Использование систем виртуализации при создании информационных систем для обеспечения оперативно-служебной деятельности органов наркоконтроля является приоритетным направлением при планировании и проектировании информационных систем.

Используемые при управлении виртуальной инфраструктурой программные средства VMware в полной мере обеспечивают стабильную работу информационных систем в уже созданных сегментах.

За счет внедрения системы виртуализации в ФСКН России были высвобождены полезные площади серверных помещений и достигнуто повышение энергоэффективности за счет снижения электропотребления.

В ходе перевода информационных ресурсов ФСКН России в виртуальную область была проведена их инвентаризация, что позволило оптимизировать нагрузку штатных администраторов.

С целью обеспечения безопасности информации в DATA-центре планируется использовать сертифицированный ФСТЭК России продукт «vGate 2».

Особое внимание планируется уделить технологиям предотвращения утечек конфиденциальной информации из информационной системы Data Leak Prevention. Это системы, строящиеся на анализе потоков данных, пересекающих периметр защищаемой информационной системы. Ярким примером такой DLP-системы являются программно-аппаратные комплексы InfoWatch Traffic Monitor и InfoWatch Data Control. Изучение этой системы подтвердило ее высокую эффективность в решении задач, связанных с обеспечением безопасности информации, в частности с контролем утечки информации вовне.

Основополагающим звеном в обеспечении безопасности информации является обязательное использование централизованной антивирусной защиты. В настоящее время ведется работа по постановке действующей антивирусной системы на абонентское обслуживание в Антивирусном центре ФСБ России.

Разграничение прав доступа, а также идентификацию и аутентификацию пользователей в системах планируется обеспечивать за счет штатных средств операционных систем, комплексов и приложений при обработке информации, не содержащей сведения, составляющие государственную и иную охраняемую законом тайну.

Повсеместное использование значимого электронного документооборота и требования, предъявляемые к нему, диктуют условия, в которых Удостоверяющий центр является ключевым местом. Так, ведомственными планами в 2012 году предусмотрена разработка технических требований и внедрение Удостоверяющего центра ФСКН России.