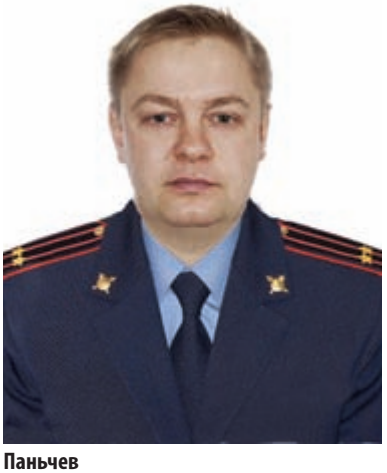
Особенности организации защиты информации в информационных системах МВД России с учётом особенностей «облачной архитектуры»

Чирков Константин Александрович,
начальник Управления защиты информации ДИТСиЗИ МВД России, подполковник внутренней службы



Паньчев Сергей Владимирович,
старший специалист ООТЗИ Управления защиты информации ДИТСиЗИ МВД России, к.т.н., подполковник внутренней службы

В МВД России большое внимание уделяется созданию и развитию автоматизированных информационных систем (АИС) в интересах конкретных подразделений ОВД. В настоящее время в подавляющем большинстве случаев АИС разработаны для реализации функций конкретного подразделения ОВД и доступ к ним осуществляется, как правило, со специализированных АРМ, взаимодействующих только с этой системой.

С целью объединения разнородных информационных ресурсов, обеспечения унифицированного доступа к оперативно-справочным, розыскным и криминалистическим учетам, для решения задач организации документооборота с соблюдением требований безопасности информации и прав доступа пользователей к информации проводились работы в два этапа.

Первый этап — это создание ЕИТКС ОВД, которая является иерархической, территориально-распределенной, многофункциональной, автоматизированной системой, обеспечивающей решение проблем автоматизации процессов информационно-аналитического обеспечения оперативно-служебной и административно-хозяйственной деятельности ОВД и являющейся технологической основой создания единого информационного пространства ОВД.

Второй этап — это создание на базе ЕИТКС единой системы информационно-аналитического обеспечения деятельности органов внутренних дел (ИСОД ОВД) с учетом реализации «облачной архитектуры».

Основа построения ИСОД ОВД в соответствии с поручением Президента Российской Федерации № ПР-2291 от 09 августа 2011 г. по вопросу создания единой системы информационно-аналитического обеспечения деятельности МВД России предусматривает:

- создание центров обработки данных (ЦОД) и перенос в них серверных элементов информационных систем МВД России;
- реализацию «облачной архитектуры» (виртуализации) на базе создаваемых ЦОД.

Проведенный анализ тенденций развития информационных систем МВД России и планов по модернизации показал, что внедрение новых подсистем обработки информации, в том числе использование технологии «облачных» вычислений, влечет за собой ряд изменений в архитектуре информационных систем МВД России. Использование технологии «облачных» вычислений осуществляется на основе виртуализации программных и технических ресурсов, что добавляет новые слои технологий и приводит к возрастанию управленческих затрат на обеспечение безопасности и требует привлечения дополнительных специализированных мер и средств защиты информации. Перемещение и консолидация информационных ресурсов и изменение технологии доступа пользователей к обрабатываемой информации ведет к появлению новых угроз безопасности, а также усугубляет последствия от реализации ранее существовавших угроз.

Данные архитектурные изменения предполагают дополнительные научно-технические задачи в области обеспечения безопасности, которые должны быть решены.

Нормативные документы, учитываемые при разработке требований безопасности:

- Федеральный закон от 27 июля 2006 г. № 49-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Указ Президента Российской Федерации № 351 «О мерах по обеспечению информацион-ной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
- Постановление правительства Российской Федерации № 781 «Об

утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Порядок проведения классификации информационных систем персональных данных. Утверждено приказом ФСТЭК России, ФСБ России, Мининформсвязи России № 55/86/20;
- Руководящий документ ФСТЭК России. Классификация автоматизированных систем и требования к информации;
- Руководящий документ ФСТЭК России. Средства вычислительной техники. Показатели защищенности от несанкционированного доступа к информации;
- Руководящий документ ФСТЭК России. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий;
- «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)»;
- Положение о методах и способах защиты информации в информационных системах персональных данных. Утверждено приказом ФСТЭК России от 5 февраля 2010 г. № 58;
- Нормативные документы ФСТЭК России и ФСБ России по защите персональных данных.

Обеспечение информационной безопасности в условиях реализации облачной архитектуры (виртуализации) имеет следующие позитивные аспекты:
- **Специализация персонала.** В условиях концентрации вычислительных и программных ресурсов у персонала есть возможность для того, чтобы специализироваться на различных аспектах организации вычислительного процесса, в том числе и на обеспечении безопасности;
- **Мощность платформы.** Однородность программной и аппаратной среды ЦОД облегчает повышение уровня автоматизации выполнения работ по управлению безопасностью таких, как управление конфигурацией, анализ уязвимостей, мониторинг состояния безопасности, устранение недостатков в безопасности компонентов платформы и др.;
- **Доступность ресурса.** Избыточность и возможности аварийного восстановления встроены в вычислительные возможности «облачной архитектуры» и обеспечивают более быстрое восстановление после инцидентов;
- **Концентрация данных.** Цент-ализованное хранение и обработка данных в едином хранилище могут обеспечить меньше риска в распределенной информационной системе, чем размещение данных на локальных и портативных компьютерах или съемных носителях, где возможно хищение данных и потеря устройств.

Однако при реализации «облачной архитектуры» как появляются новые,

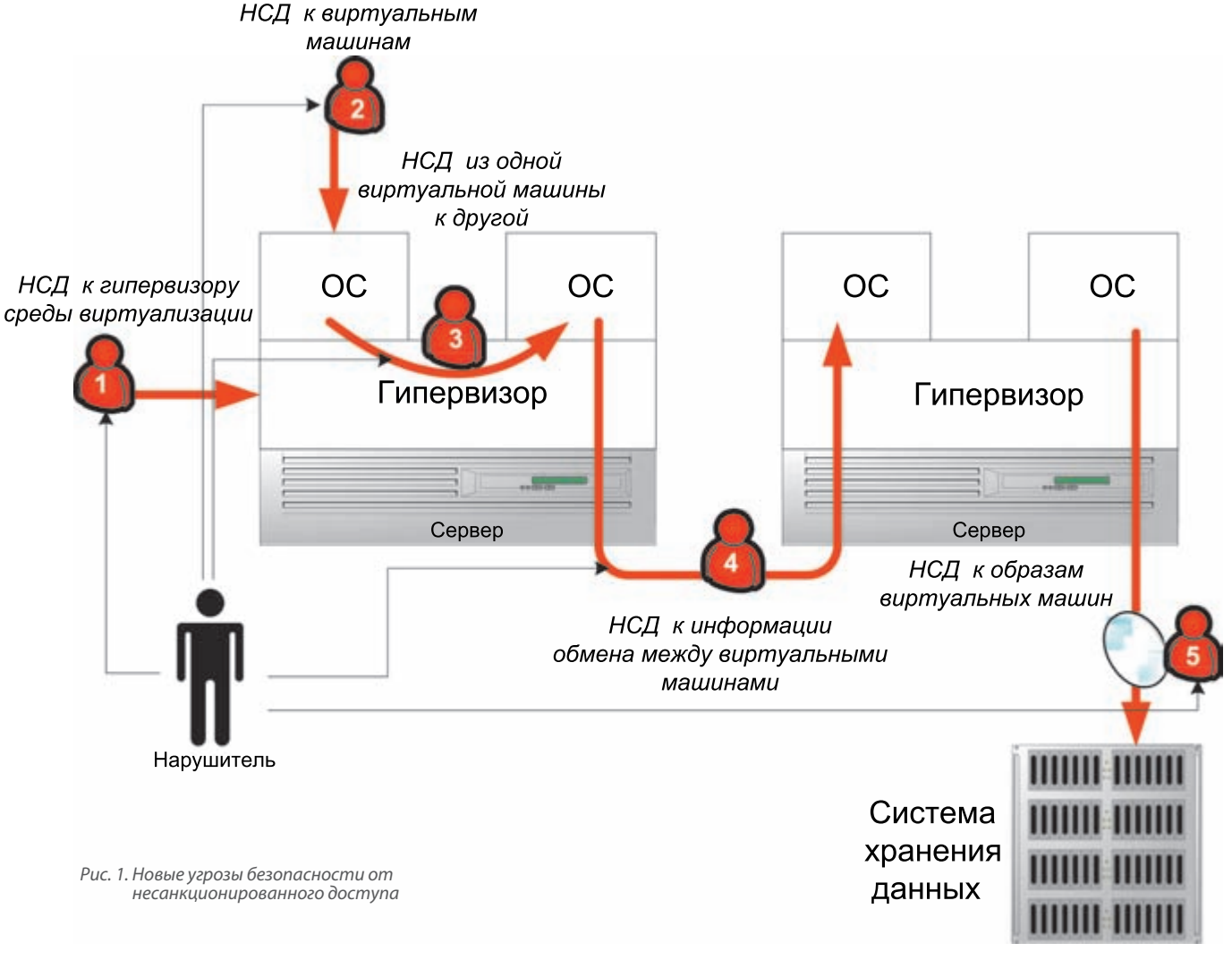


Рис. 1. Новые угрозы безопасности от несанкционированного доступа

так и повышается актуальность традиционных угроз, что обусловлено следующими аспектами:

- **Сложность решения.** Техническая сложность решения по построению «облачной архитектуры» сама по себе является уязвимостью. Безопасность зависит не только от корректности и эффективности многих компонентов, формирующих «облако», но также и от взаимодействия между ними. Сложность, как правило, имеет отношение обратно пропорциональное к безопасности. Монитор гипервизора или виртуальной машины — дополнительный уровень программного обеспечения между операционной системой и аппаратной платформой, которая используется, чтобы управлять виртуальными машинами. По сравнению с традиционной невиртуализированной реализацией добавление гипервизора вызывает увеличение возможностей для атаки.
- **Совместное использование ресурсов.** Совместное использование инфраструктуры различными приложениями и пользователями требует высокого уровня доверия для механизмов безопасности, используемых для логического разделения виртуальной среды. Логическое разделение, само по себе представляющее сложную проблему, усиливается масштабом облачных вычислений. В результате может быть несанкционированно (в том числе вследствие некорректной конфигурации, ошибок и недекларированных возможностей в ПО) получен доступ к приложениям и информационным ресурсам.
- **Расширение возможностей администраторов и обслуживающего персонала по доступу к информационным ресурсам.**

В частности к таким новым угрозам безопасности (рисунок 1) относится несанкционированный доступ:

1) к гипервизору среды виртуализации с целью его модификации, изменения настроек и последующего обхода;
2) к виртуальным машинам с целью ознакомления, модификации (искажения) и (или) уничтожения защищаемой информации;
3) из одной виртуальной машины в другую с целью ознакомления, модификации (искажения) и (или) уничтожения защищаемой информации;
4) к информации обмена между виртуальными машинами с целью ознакомления, модификации (искажения) и (или) уничтожения защищаемой информации;
5) к образам виртуальных машин с целью их уничтожения и создания условий для дезорганизации работы в случае сбоев.

В целях нейтрализации отмеченных угроз безопасности потребуется, в том числе, использование следующих методов и средств обеспечения безопасности информации:

- разработка планов, процедур и организационно-распорядительной документации по обеспечению безопасности при первоначальном внедрении средств виртуализации и поддержания безопасности в процессе эксплуатации;
- обеспечение доступа к функциям управления средств построения виртуализации только уполномоченным лицам;
- подбор персонала, его инструктаж и повышение квалификации в области защиты информации;
- разделение обязанностей системных администраторов, администраторов приложений и администраторов безопасности, организация системы контроля за их действиями;
- обеспечение контроля доступа к оборудованию, позволяющему осуществить локальное (прямое) управление средствами построения виртуализации;
- ограничение и контроль использования внешних портов и интерфейсов виртуальными машинами, отключение (блокирование) всех неиспользуемых портов (интерфейсов);
- контроль целостности файлов виртуальных машин (конфигурационных файлов виртуальной машины, файла образа BIOS виртуальной машины и др.) и средств построения виртуализации;
- своевременное обновление средств построения виртуализации и применяемых средств защиты информации;
- отключение (блокирование, удаление) неиспользуемых функций средств построения виртуализации;
- ограничение (отключение) взаимодействия виртуальных машин через механизмы (интерфейсы) средств построения виртуализации;
- обеспечение защиты данных виртуальных машин (в том числе данных управления и конфигурации виртуальных машин) в процессе их передачи по каналам связи, в том числе с использованием средств криптографической защиты информации;
- использование средств защиты информации, в том числе специального программного обеспечения с функциями защиты информации, прошедших в установленном порядке оценку соответствия (сертификацию).

Вместе с тем архитектурные изменения информационных систем МВД, связанные с созданием ЦОД и централизацией хранения информации и предоставления информационных сервисов создают предпосылки для упрощения решения отдельных вопросов защиты информации:

- основные средства защиты информации концентрируются в ЦОД, минимизируется их количество, упрощается приобретение, внедрение, сопровождение;
- минимизируется количество администраторов безопасности ИСОД ОВД;
- инциденты безопасности в ЦОД могут быть более оперативно выявлены и устранены, минимизируется эффект простоя системы вследствие реализации атак;
- использование терминальных решений минимизирует затраты на защиту распределенных объектов ОВД, а также снижает возможный ущерб от утечки защищаемой информации, поскольку она хранится не на объектах ОВД, а централизованно в ЦОД;
- упрощается модернизация подсистемы информационной безопасности, ускоряется процесс модернизации, поскольку модернизация производится централизованно в ЦОД.

Результаты анализа эффективности решений по защите информации в информационных системах МВД России позволят разработать требования и системные проектные решения по обеспечению комплексной защиты данных информационных систем МВД России в соответствии с требованиями законодательства Российской Федерации и с учетом изменений в архитектуре информационных систем МВД и технологии обработки информации.