О терминальном доступе к ЕИСЦОД МВД России

Нарцев
Александр Дитольевич,
начальник отдела ЦИТиЗИ НИИСТ ФКУ НПО «Специальная техника и связь» МВД России, полковник внутренней службы

Основными целями создания ЕИСЦОД МВД России являются:

- унификация используемых в МВД России программно-технических решений и приведение архитектуры основных автоматизированных информационных систем МВД России в соответствие современным требованиям доступности данных и надежности функционирования;
- консолидация разнородных данных, содержащихся в различных автоматизированных информационных системах МВД России, и обеспечение единой точки доступа к ним для использования в оперативно-служебной деятельности МВД России;
- уменьшение расходов на создание, поддержку и эксплуатацию автоматизированных информационных систем, используемых в МВД России, а также на развитие и поддержку информационно-технологической инфраструктуры МВД России.

ЕИСЦОД МВД России должен являться территориально-распределенной и катастрофо-устойчивой системой.

ЕИСЦОД МВД России должен состоять из отдельных программно-технических комплексов, обеспечивающих предоставление на рабочие места пользователей соответствующих сервисов (приложений) прикладных программных платформ и работу с ними.

Отдельные ПТК ЕИСЦОД связаны телекоммуникационной системой и должны взаимодействовать между собой для обеспечения:

- взаимного резервирования данных, сервисов и функций ПТК;
- автоматического распределения и балансировки нагрузки между отдельными ПТК для обеспечения оптимальных параметров предоставления сервисов и работы с ними.

В рамках ЕИСЦОД необходимо обеспечивать функционирование следующих прикладных программных платформ:

- платформы предоставления сервисов обеспечения оперативно-служебной деятельности подразделений (ОСД) МВД России;
- платформы предоставления справочно-аналитических сервисов (САС);
- платформы предоставления общесистемных ведомственных сервисов (ОВС).

ЕИСЦОД МВД России предназначен для информационного обеспечения ОСД подразделений МВД России, справочно-аналитического обеспечения деятельности МВД России, предоставления сервисов, напрямую не связанных с оперативно-служебной деятельностью подразделений МВД России и обеспечивающих необходимую среду для взаимодействия между подразделениями и сотрудниками МВД России и обмена неструктурированными служебными информационными материалами, а также управления подсистемами и платформами ЕИСЦОД МВД России.

Существует множество различных видов терминального доступа. От этого зависит тип ПО, архитектура системы и многое другое. Системы дистанционного подключения можно разделить по принципу доступа к интерфейсу и по принципу работы с системой. Так, существуют:

- **«Интернет-клиент»** — система с доступом только с помощью браузера;
- **«Тонкий клиент»** — система, аналогичная «интернет-клиенту», отличающаяся тем, что в браузер встраивается дополнительная надстройка для работы с ключами клиента и установки электронной цифровой подписи (ЭЦП). «Тонкий клиент» в большинстве случаев обладает минимальной аппаратной конфигурацией, вместо жесткого диска для загрузки локальной специализированной ОС используется DOM (DiskOnModule) (модуль с разъёмом IDE, флэш-памятью и микросхемой, реализующей логику обычного жёсткого диска — в BIOS определяется как обычный жёсткий диск, только размер его обычно в 2–3 раза меньше). В некоторых конфигурациях системы «тонкий клиент» загружает операционную систему по сети с сервера, используя протоколы PXE, BOOTP, DHCP, TFTP и Remote Installation Services (RIS);
- **«Толстый клиент»** — система, для работы с которой используется отдельное (от браузера) ПО, запускаемое клиентом при организации доступа. Достоинствами является:

- наличие более широкого функционала в отличие от тонкого;

- режим многопользовательской работы;
- предоставление возможности работы даже при обрывах связи с сервером;
- высокое быстродействие интерфейса.

Однако у него есть и ряд существенных недостатков:
- большой размер дистрибутива;
- многое в работе клиента зависит от того, для какой платформы он разрабатывался;
- при работе с ним возникают проблемы с удаленным доступом к данным;
- довольно сложный процесс установки и настройки;
- сложность обновления и связанная с ней неактуальность данных.

Защита перечисленных систем сводится к использованию идентификатора пользователя и пароля, а также второго фактора аутентификации. Кроме того, существуют каналы оповещения пользователя о событиях в системе.

Большинство систем было разработано на популярных языках программирования, при этом компоненты систем могут быть как веб-приложениями (например, технологии ASP.Net, Java), так и клиентскими приложениями (технология ActiveX) или просто приложениями, написанными на языках семейства Си. В совокупности все эти компоненты обеспечивают функционал для обеспечения удаленного доступа Сотрудника ОВД к ИР. Используя данную базу для создания таких систем, программисты могут совершать ошибки, которые приводят к появлению уязвимостей как на клиентской части, так и на серверной.

Основные уязвимости при разработке толстого клиента, а также серверной части, если это не веб-приложение, появляются в результате ошибок памяти и реализуются через ошибки при управлении переменными в стеке или при неверной работе с указателями, счетчиками или индексами. Класс таких ошибок довольно широк и включает в себя такие известные уязвимости, как:
- переполнение буфера в стеке;
- использование памяти после освобождения;
- целочисленное переполнение.

В худшем случае такие уязвимости приводят к угрозе выполнения произвольного кода на хосте с правами учетной записи, из-под которой запущено атакуемое ПО. В иных случаях это может приводить к отказу в обслуживании, так как атакуемый процесс аварийно завершает свою работу. В случае, если мы говорим о клиентском ПО, наибольшую опасность представляет собой только риск произвольного выполнения кода, так как потенциальный нарушитель сможет выполнить захват рабочей станции. В случае серверного ПО риск отказа в обслуживании также считается критичным, так как может привести к остановке бизнес-процессов. Также существует вероятность, что атаки типа отказа в обслуживании могут использоваться злоумышленником для отвлечения внимания от своих действий, которые могли быть совершены до DoS-атаки.

Выводы

Терминальный доступ упрощает жизнь, если применяется по назначению. Снижение расходов (в том числе экономия на лицензиях), повышение уровня безопасности, уменьшение трудозатрат на обслуживание техники — таковы основные плюсы применения этой технологии. Но терминальный доступ далеко не панацея от всех бед, и делать выбор в его пользу следует только располагая достоверными данными о возможности использования выбранных приложений в терминальной среде — иначе вместо оптимизации рабочих процессов можно нарушить отлаженную работу инфраструктуры и нанести организации финансовый ущерб.

Выбор типа клиента удаленного доступа — непростая задача, которую необходимо решать, учитывая не только удобство разработки, но и технико-экономические аспекты владения всей системой ИСОД МВД России.

Кроме этого, терминальный доступ должен быть единым для всех сервисов ОСД, САС и ОВС.

Правильный выбор терминального клиента позволит обеспечить МВД России:

Высокую производительность даже при низкой пропускной способности сети:
- данные не требуется передавать по сети: они обрабатываются там же, где хранятся — на сервере;
- производительность ПК повышается за счёт производительности сервера, в качестве рабочих мест можно использовать маломощные компьютеры.

Удобство администрирования:
- централизованное администрирование разнородных вычислительных ресурсов;
- быстрое развертывание важных для работы приложений;
- все рабочие места можно быстро настроить с одного компьютера;
- программы устанавливаются централизованно;
- развёртывание нового рабочего места требует минимум времени и усилий;
- безопасная работа по сети;
- сотрудники не зависят от конкретных рабочих мест;
- используется безопасное удалённое подключение. Все передаваемые данные под надёжной защитой;
- оптимизация инвестиций;
- снижение эксплуатационных расходов.