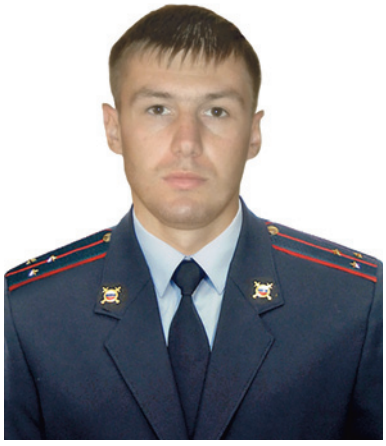
Становление и развитие системы управления доступом к сервисам ИСОД МВД России



Солдатов
Вячеслав Владимирович,
начальник отдела организации противодействия техническим разведкам, технической защиты информации и криптографической защиты информации, не содержащей государственную тайну, Управления защиты информации ДИТСиЗИ МВД России, старший лейтенант внутренней службы

Макаров
Дмитрий Александрович,
старший специалист отдела организации противодействия техническим разведкам, технической защиты информации и криптографической защиты информации, не содержащей государственную тайну, Управления защиты информации ДИТСиЗИ МВД России, старший лейтенант внутренней службы

Развитие Единой системы информационно-аналитического обеспечения деятельности Министерства внутренних дел Российской Федерации (далее ИСОД МВД России) является приоритетной задачей в области информатизации Министерства. Количество сотрудников МВД России, которые используют информационные системы и ресурсы, в перспективе должно достигнуть 500 000 человек. При отсутствии механизмов централизованного автоматизированного управления учетными записями и правами доступа пользователей такой крупной организационной структуры администраторы безопасности сталкиваются с целым рядом проблем, в том числе:

- необходимость отслеживать и выполнять своевременный отзыв прав доступа к информационным системам у уволенных или ушедших в длительный отпуск сотрудников;
- отсутствие инструментов контроля соответствия назначенных прав доступа должностным полномочиям сотрудника;
- отсутствие возможности оперативно получать информацию о фактах доступа сотрудника к закрытым данным.

Данные проблемы увеличивают опасность утечек служебной информации и ущерб от них, не позволяют эффективно расследовать инциденты, связанные с несанкционированным доступом.

Проблемы с управлением большим количеством учетных записей существуют и у службы технической поддержки: рост числа применяемых в организации информационных систем и приложений, увеличение количества пользователей приводят к росту объема работ по созданию, изменению и блокированию учетных записей в каждой информационной системе, что, в свою очередь, влечет за собой необходимость привлечения дополнительного персонала для обслуживания систем.

Ключом к построению эффективной системы управления доступом является реализация механизмов, которые обеспечат централизованный контроль за жизненным циклом идентификационных данных, а также идентификацию и аутентификацию пользователей, протоколирование и предотвращение попыток несанкционированного доступа. Подобные механизмы, в свою очередь, создают прочный базис для реализации функций распределения прав доступа к информации.

Очевидно, что построение подобной системы в теории выглядит проще, чем это оказывается на практике, особенно учитывая, что речь идет об управлении доступом в такой крупной организации, как МВД России, реализующей множество гетерогенных информационных систем.

В данной статье мы рассмотрим проблематику и опыт построения системы управления доступом в рамках ИСОД МВД России — сервиса управления доступом к информационным ресурсам и системам ИСОД МВД России (далее СУДИС), а также перспективы его дальнейшего развития.

Создание сервиса управления доступом

Итак, какие задачи стояли перед нами на начальных этапах создания СУДИС и ИСОД МВД России в целом?

Во-первых, требовалось создать единый пополняемый реестр поль-

зователей ИСОД МВД России. При поиске системы, содержащей наибольшее количество данных о сотрудниках МВД России на начало 2014 года, было принято решение осуществить интеграцию с подсистемой организационно-штатной структуры сервиса электронного документооборота (далее ОШС). В результате в настоящее время при появлении новой записи сотрудника МВД России в ОШС автоматически создается учетная запись в реестре пользователей СУДИС с присвоением индивидуальных логина и пароля, а также прав доступа «по умолчанию» к сервисам ИСОД МВД России. При удалении записи из ОШС учетная запись пользователя автоматически блокируется.

Во-вторых, так как ИСОД МВД России объединяет в себе сервисы, функционирующие на базе как лицензируемого, так и разрабатываемого в интересах МВД России программного обеспечения (далее ПО), нужно было определить перечень программных интерфейсов, с помощью которых сервисы могли бы интегрироваться с СУДИС для обеспечения процессов идентификации и аутентификации пользователей. Помимо того, что интерфейсы для интеграции лицензируемого ПО определенно должны были быть основаны на широко известных и стандартизированных протоколах взаимодействия, необходимо было обеспечить поддержку различных форм взаимодействия с пользователем — через «толстые» и «тонкие» клиенты. Таким образом был сформирован следующий перечень интерфейсов:

1. Интерфейс на основе протокола SAML 2.0 для интеграции веб-приложений (так называемых «тонких» клиентов) сервисов ИСОД МВД России (например, ВИСП и СЭД). SAML 2.0 — широко известный протокол проверки подлинности пользователя, который также позволяет реализовать систему однократной аутентификации (о ней мы расскажем ниже).
2. Интерфейс на основе протокола LDAP для интеграции «толстых» клиентов (как, например, клиента сервиса электронной почты). LDAP — это базовый протокол, который поддерживается подавляющим большинством современных систем и обеспечивает проверку подлинности пользователя и предоставление его атрибутов по запросу.
3. Прикладной программный интерфейс СУДИС, который был спроектирован специально для некоторых «толстых» клиентов сервисов ИСОД МВД России с учетом выполняемых ими прикладных функций и особенностей облачной инфраструктуры.

В рамках выполнения этой задачи основной сложностью стало обеспечение соответствия требованиям безопасности в части двухсторонней аутентификации сервисов ИСОД МВД России и СУДИС с использованием отечественных криптографических алгоритмов.

В-третьих, разрабатываемое ПО СУДИС должно было поддерживать различные способы аутентификации (проверки подлинности пользователя):

1. По логину и паролю — наиболее простой способ, реализуемый вышеуказанными интерфейсами «по умолчанию»;
2. С помощью ключа электронной подписи — предпочтительный способ с точки зрения информационной безопасности, но требующий построения полномасштабной инфраструктуры открытых ключей.

Для реализации инфраструктуры открытых ключей в системе МВД России создан и функционирует Удостоверяющий центр МВД России. Удостоверяющий центр успешно прошел процедуру аккредитации Минкомсвязью России и выпускает только квалифицированные сертификаты ключей проверки электронной подписи.

Ключ электронной подписи позволяет не только осуществлять более безопасный вход в систему, чем по логину и паролю, но и подписывать документы и запросы, которыми оперируют сервисы ИСОД МВД России. Главное — не забывать, что его использование накладывает на пользователя такие же обязанности и влечет за собой такой же уровень ответственности, как и реальная подпись. По этой причине электронный идентификатор с ключами электронной подписи, который выдается сотруднику в Удостоверяющем центре МВД России, нужно защищать от компрометации и, в случае утери или подозрений о неправомерном его использовании третьими лицами, сразу же ставить в известность администраторов безопасности своего подразделения.

В-четвертых, уже на начальных этапах создания СУДИС были разработаны требования к сложности и частоте смены паролей для обеспечения необходимого уровня безопасности, что в некотором роде осложнило жизнь пользователям (учитывая низкий процент использования средств электронной подписи на начало 2014 года). В рамках оптимизации процесса аутентификации пользователей по логину и паролю была внедрена система однократной аутентификации для веб-приложений сервисов ИСОД МВД России. Она позволила пользователю вводить учетные данные только один раз при начале работы в одном из сервисов и автоматически (прозрачно для пользователя) проверяла его подлинность при переходе в другие сервисы в рамках одной рабочей сессии.

В дальнейшем эта система получила свое развитие на рабочих местах пользователей и теперь, войдя в операционную систему компьютера с помощью модуля входа СУДИС, пользователь имеет возможность входить в веб-приложения сервисов ИСОД МВД России без необходимости повторного ввода учетных данных.

Однократная аутентификация возможна и для «толстых» клиентов сервисов ИСОД МВД России при условии, что они реализуют в своем ПО дополнительные функции взаимодействия с СУДИС.

Таким образом, на начальном этапе создания ИСОД МВД России сервис управления доступом обеспечил возможности:

1. Ведения единого реестра учетных записей пользователей ИСОД МВД России;
2. Идентификации и аутентификации пользователей в различных типах клиентов сервисов ИСОД МВД России;
3. Входа в сервисы с помощью логина и пароля или ключа электронной подписи;
4. Однократной аутентификации на рабочих местах и в веб-приложениях сервисов ИСОД МВД России.

На следующем этапе появилась необходимость оценить, насколько полно реализуется интеграция сервисов ИСОД МВД России с СУДИС, а также глубину использования этих сервисов сотрудниками

МВД России. Для этого были реализованы механизмы сбора и предоставления статистической отчетности на основании данных об успешных аутентификациях пользователей в сервисах ИСОД МВД России. В настоящий момент СУДИС позволяет получать следующие статистические данные за требуемый период времени:

1. Общее количество успешных аутентификаций в ИСОД МВД России;
2. Общее количество успешных аутентификаций в выбранном сервисе ИСОД МВД России;
3. Количество аутентификаций в сервисе ИСОД МВД России с учетом территориальной привязки пользователей и способов доступа (по логину и паролю, с помощью ключа электронной подписи);
4. Количество уникальных пользователей, которые получили доступ к сервису ИСОД МВД России.

События успешной и неуспешной аутентификации пользователей, создания и изменения значимых ресурсов ИСОД МВД России и другие события безопасности регистрируются в сервисе протоколирования событий безопасности СУДИС (далее СПСБ). С учетом интеграции СПСБ со специализированными средствами подсистемы обеспечения информационной безопасности ИСОД МВД России можно смело отметить, что СУДИС делает серьезный вклад в решение задачи обнаружения попыток несанкционированного доступа к информационным ресурсам ИСОД МВД России.

Остальные функции СУДИС получили свое развитие относительно недавно и включают следующие механизмы:

1. Механизмы поддержки специализированных типов учетных записей (далее УЗ): помимо управления стандартными УЗ сотрудников МВД России СУДИС позволяет управлять доступом к сервисам ИСОД МВД сотрудников других органов исполнительной власти. При этом на специализированные УЗ распространяются отдельные (более строгие) политики информационной безопасности.
2. Механизмы ограничения доступа пользователей к сервисам ИСОД МВД России по способу входа или типу УЗ: можно, например, разрешить доступ пользователей к конкретному сервису ИСОД МВД России только посредством ключей электронной подписи.
3. Механизмы рассылки уведомлений по электронной почте о событиях, связанных с УЗ пользователей: в настоящее время пользователь ИСОД МВД России, который работает под учетной записью СУДИС, может получать уведомления об истечении срока действия своего пароля или сертификата ключа проверки электронной подписи, а также при изменении полномочий доступа или данных учетной записи администратором безопасности.

Трудности внедрения

Несмотря на то, что СУДИС в настоящее время реализует достаточно широкий перечень функций, остаются факторы, в некоторой степени препятствующие его быстрому внедрению в подразделениях МВД России. В основном это связано с отсутствием или недостаточным развитием отдельных прикладных решений в ИСОД МВД России, которые в классических корпоративных информационных системах реализуются с помощью коммерческого ПО и удовлетворяют следующие потребности пользователей и администраторов систем:

1. Возможность использования сетевых разделяемых ресурсов (общих файлов, папок, принтеров и т. п.);
2. Возможность использования специальных функций программного обеспечения, которое функционирует только в рамках домена Microsoft Active Directory (например, совместная работа с документами в программах пакета Microsoft Office);
3. Централизованное управление парком автоматизированных рабочих мест со стороны системных администраторов.

СУДИС в той или иной степени может накладывать технические ограничения на использование коммерческого ПО. В частности, он полностью блокирует возможность построения доменов Microsoft Windows на базе Microsoft Active Directory.

Со стороны может показаться, что там, где подобные решения уже реализованы и успешно помогают решать конкретные задачи в одном или нескольких структурных подразделениях, необходимо предоставить возможность их дальнейшего использования и не осуществлять переход на использование СУДИС. Но у такого подхода есть серьезные недостатки, в числе которых следующие:

1. Подсистема обеспечения информационной безопасности (далее ПОИБ) ИСОД МВД России состоит из множества элементов, каждый из которых реализует подмножество требований к информационной безопасности в соответствии с Базовой моделью угроз и нарушителя ИСОД МВД России. Средства защиты информации, которые документально не задекларированы в составе ПОИБ ИСОД МВД России и замещают один или несколько его элементов при построении системы защиты, не позволят, тем не менее, пройти аттестацию ИСОД МВД России по требованиям безопасности информации, которая является обязательной для информационных систем такого класса.
2. К средствам защиты, которые не интегрированы с другими элементами ПОИБ, невозможно централизованно применить глобальные политики безопасности и гарантировать полноту реализации системы защиты в отношении информационных ресурсов, которые они защищают.
3. Организационные процессы, связанные с созданием и блокировкой учетных записей, предоставлением и отзывом доступа к информационным ресурсам, оказываются децентрализованными, что приводит к появлению дополнительных угроз безопасности (например, «забытые» учетные записи, предоставление избыточных прав доступа). Фактически при таком подходе отсутствуют гарантии мониторинга состояния информационной безопасности (возможности отслеживания кто обладает доступом к информации и кто, когда и к каким ресурсам действительно получает доступ).

Безусловно, использование различных подходов к построению системы защиты также несет в себе дополнительные материальные затраты.

Еще одним фактором, влияющим на скорость внедрения СУДИС, является отсутствие в ИСОД МВД России полного и коррект-

ного (с точки зрения качества информации) источника данных о сотрудниках МВД России и структуре МВД России. Сервисы кадрового учета (Сервис обеспечения кадровой деятельности и Сервис организационно-штатных подразделений) находятся в стадии разработки и пока не предоставляют программных интерфейсов, необходимых для обеспечения доступности кадровых данных. При этом процесс наполнения ОШС МВД новыми записями хоть и отличается высокими темпами, но отсутствие в подсистеме механизмов проверки на дублирование и корректность вводимых данных, а также своевременного обновления справочников подразделений, приводит к следующим проблемам:

1. Появление дублей учетных записей и необходимости их выявления и удаления на стороне СУДИС в рамках задачи по обеспечению защиты от несанкционированного доступа;
2. Трудности при сопоставлении учетной записи пользователя и сотрудника, которому она назначена (установление однозначного соответствия может занимать продолжительное время);
3. Ограничения на дальнейшее развитие функций СУДИС, которые требуют использования полноценных справочников подразделений и установления их региональной принадлежности (как, например, реализация веб-приложения СУДИС для администраторов доступа подразделений МВД России);
4. Вероятность неправильного распространения полномочий доступа к информации (в том числе содержащейся в СУДИС) как результат некорректной структуры и состава данных справочников сотрудников и подразделений.

Дальнейшее развитие

Так как первоочередной задачей УЗИ ДИТСиЗИ МВД России является обеспечение полноценной защиты ресурсов ИСОД МВД России от несанкционированного доступа, в ближайшей перспективе планируется разработка и внедрение следующих решений:

1. Программное обеспечение для идентификации и аутентификации пользователей автоматизированных рабочих мест, функционирующих на базе Linux-подобных операционных систем (Ubuntu, Debian, CentOS и т. п.), которое должно быть реализовано в объеме, аналогичном ПО СУДИС для операционной системы Windows, включая:
   - сетевой вход в операционную систему под УЗ СУДИС с помощью логина и пароля или ключа электронной подписи;
   - прозрачную аутентификацию в веб-приложениях сервисов ИСОД МВД России при наличии действующей сессии пользователя в ОС Windows;
   - регистрацию событий безопасности в СПСБ СУДИС;
   - блокировку сеанса работы в ОС при извлечении индивидуального электронного идентификатора;
   - автоматическое обновление компонентов СУДИС на автоматизированном рабочем месте пользователя.

   Эта задача рассматривается нами как принципиально важная в свете государственной политики импортозамещения в отношении лицензируемого программного обеспечения.
2. Программное обеспечение для идентификации и аутентификации пользователей устройств на базе ОС Android, как уже используемых в МВД России, так и перспективных.
3. Средства защиты информации от несанкционированного доступа к ресурсам автоматизированного рабочего места пользователя, включая:
   - средства централизованного управления политиками безопасности автоматизированного рабочего места;
   - управление доступом к локальным и сетевым ресурсам.

   Функциональные требования к разрабатываемому программному обеспечению СЗИ от НСД сформированы на основе требований приказа № 17 ФСТЭК России «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и руководящего документа Гостехкомиссии России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (по 5-му классу защищенности средства вычислительной техники). СЗИ от НСД разрабатывается как программное решение, которое может функционировать независимо от СУДИС и планируется к передаче на сертификацию в конце 2-го квартала 2017 года.

В приоритетном порядке рассматриваются вопросы ускорения обработки заявок на получение учетных записей и предоставления доступа к сервисам ИСОД МВД России, в том числе и полный переход на автоматизацию создания учетных записей при интеграции СУДИС с сервисами кадрового учета.

Поддержка в СУДИС дополнительных возможностей для интеграции с различным прикладным ПО (в том числе упоминаемом в предыдущем параграфе) — это вопрос своевременного и правильного формирования функциональных требований к подсистеме обеспечения информационной безопасности. На каждом этапе развития СУДИС требования к интеграции будут анализироваться, дополняться и передаваться на реализацию — для того чтобы сделать информационные ресурсы ИСОД МВД России максимально доступными и удобными в использовании.

Заключение

В настоящее время в МВД России реализуется централизованный подход к управлению доступом в отношении сервисов ИСОД МВД России. В СУДИС уже зарегистрировано порядка 350 000 учетных записей пользователей и около 40 прикладных сервисов, что само по себе говорит о высокой востребованности системы. В то же время СУДИС продолжает свое развитие в рамках решения задач повышения эффективности системы управления доступом, закрытия пробелов в инфраструктуре ИСОД МВД России и решения ряда смежных вопросов.