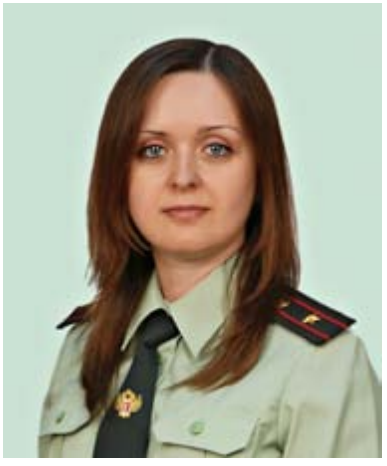
К вопросу об анализе защищенности сетей в ФСКН России



Кузьмина Марина Геннадиевна,
старший инженер Информационно-аналитического управления Организационно-административного департамента Федеральной службы Российской Федерации по контролю за оборотом наркотиков, майор полиции

Рябченко Олег Евгеньевич,
ведущий инспектор Управления делами Организационно-административного департамента Федеральной службы Российской Федерации по контролю за оборотом наркотиков, старший лейтенант полиции

Внедрение и широкое использование информационных технологий во всех сферах человеческой жизни ведет к увеличению роли информации в современном мире. Не материальные ценности, а информация в чистом виде все чаще подлежит хищению.

Постоянно появляются все более новые методы атак на ресурсы информационных систем, и спектр этих атак постоянно расширяется. Способность упреждать эти растущие угрозы носит непрерывный, комплексный и своевременный характер.

Под защитой информации понимается деятельность, направленная на защиту таких свойств информации, как конфиденциальность, целостность и доступность (далее — основные свойства безопасности информации).

Наибольшее внимание в ФСКН России уделяется внешним угрозам, компьютерным атакам, вирусам и другому вредоносному программному обеспечению.

Реализацию защиты информации в указанном аспекте возможно достигнуть путем применения средств защиты информации от утечки по техническим каналам и несанкционированного доступа, средств криптографической защиты, антивирусного программного обеспечения, а также организационных мер. В ФСКН России эти мероприятия проводятся в рамках подготовки к аттестации объектов информатизации на соответствие требованиям по безопасности информации, которая является основной мерой технической защиты информации.

Вместе с тем, в соответствии с приказом ФСТЭК России от 5 февраля 2010 г. №58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных» необходимо выполнять Требования по анализу защищенности информационных систем (далее — ИС), в которых обрабатываются персональные данные. А именно анализ защищенности проводится для распределенных ИС и ИС, подключенных к сетям международного информационного обмена, путем использования в составе ИС программных или программно-аппаратных средств (систем) анализа защищенности. Средства (системы) анализа защищенности должны обеспечивать возможность выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения ИС, которые могут быть использованы нарушителем для реализации атаки на систему.

Обнаружение вторжений проводится для ИС, подключенных к сетям международного информационного обмена, путем использования в составе ИС программных или программно-аппаратных средств (систем) обнаружения вторжений.

Также в соответствии с приказом ФСТЭК России от 6 декабря 2011 г. №638 утверждены вступившие с 15 марта 2012 г. в действие Требования к системам обнаружения вторжений, в которых определено, что под сетевой безопасностью следует понимать защиту информационной инфраструктуры от вторжений злоумышленников извне, а также защиту от случайных ошибок персонала или намеренных действий. Основу стабильности сети составляет надежность ПЭВМ и сетевого оборудования, а также устойчивость каналов связи.

Система обнаружения вторжений уровня сети (объект оценки) представляет собой элемент системы защиты информации ИС, функционирующих на базе вычислительных сетей, и применяется совместно с другими средствами защиты информации от несанкционированного доступа к информации в ИС.

Объект оценки должен обеспечивать обнаружение и (или) блокирование следующих основных угроз безопасности информации, относящихся к вторжениям (атакам):

- преднамеренный несанкционированный доступ или специальные воздействия на информацию (носители информации) со стороны внешних нарушителей, действующих из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена;
- преднамеренный несанкционированный доступ или специальные воздействия на информацию (носители информации) со стороны внутренних нарушителей, обладающих правами и полномочиями на доступ к информации в ИС.

Одновременно с этим при рассмотрении проблем защиты данных сети прежде всего возникает вопрос о классификации сбоев и нарушений прав доступа, которые могут привести к уничтожению или нежелатель-

ной модификации данных. **Среди таких потенциальных угроз можно выделить:**

- сбои оборудования (кабельной системы, электропитания, дисковых систем, систем архивации данных);
- потери информации из-за некорректной работы ПО (потеря или изменение данных при ошибке ПО, сбои работы серверов, рабочих станций, сетевых карт и т.д.);
- потери, связанные с несанкционированным доступом (при заражении системы компьютерными вирусами, несанкционированное копирование, уничтожение или подделка информации);
- потери информации, связанные с неправильным хранением архивных данных;
- ошибки обслуживающего персонала и пользователей (ознакомление с конфиденциальной информацией, составляющей тайну, посторонних лиц, случайное уничтожение или изменение данных).

В зависимости от возможных видов нарушений работы сети многочисленные виды защиты информации объединяются в три основных класса:

- средства физической защиты, включающие средства защиты кабельной системы, систем электропитания, средства архивации, дисковые массивы и т.д.;
- программно-аппаратные средства защиты, в том числе: антивирусные программы, системы разграничения полномочий, программные средства контроля доступа и инвентаризации ИС;
- административные меры защиты, включающие контроль доступа в помещения, разработку стратегии безопасности организации, планов действий в чрезвычайных ситуациях и т.д.

Защищенность является одним из важнейших показателей эффективности функционирования АС наряду с такими показателями, как надежность, отказоустойчивость, производительность и т.п.

Под защищенностью АС будем понимать реализованные механизмы защиты информации, существующие в данной среде функционирования, с учетом рисков, связанных с осуществлением угроз безопасности информации. Под угрозами безопасности информации традиционно понимается возможность нарушения основных свойств безопасности информации.

Анализ защищенности является основным элементом таких взаимно пересекающихся видов работ, как аттестация, аудит и обследование безопасности АС.

При построении и анализе моделей защиты в ФСКН России в качестве характеристик используется категорирование объектов: нарушителей (по целям, квалификации и доступным вычислительным ресурсам), информации (по уровням критичности и конфиденциальности), средств защиты (по функциональности и гарантированности реализуемых возможностей) и т. п. Такой подход не позволяет получать точные значения показателей защищенности, однако дает возможность классифицировать АС по уровню защищенности и сравнивать их между собой.

В настоящее время изучается возможность создания Типовой методики исследования системы защиты, включающей использование следующих методов:

- изучение исходных данных по АС;
- оценка рисков, связанных с осуществлением угроз безопасности в отношении ресурсов АС;
- анализ механизмов безопасности организационного уровня, политики безопасности организации и организационно-распорядительной документации по обеспечению режима информационной безопасности и оценка их соответствия требованиям существующих нормативных документов, а также их адекватности существующим рискам;
- анализ конфигурационных файлов маршрутизаторов, МЭ и прокси-серверов, осуществляющих управление межсетевыми взаимодействиями, почтовых и DNS-серверов, а также других критических элементов сетевой инфраструктуры;
- сканирование внешних сетевых адресов ЛВС из внешней сети;
- сканирование ресурсов ЛВС изнутри;
- анализ конфигурации серверов и рабочих станций ЛВС при помощи специализированных программных средств.

Перечисленные методы исследования предполагают использование как активного, так и пассивного тестирования системы защиты. Активное тестирование системы защиты заключается в эмуляции действий потенциального злоумышленника по преодолению механизмов защиты. Пассивное тестирование предполагает анализ конфигурации ОС и приложений по шаблонам с использованием списков проверки. Тестирование может производиться вручную либо с использованием специализированных программных средств.

Таким образом, программные средства анализа защищенности условно можно разделить на два класса. Первый класс, к которому принадлежат сетевые сканеры, иногда называют средствами анализа защищенности сетевого уровня. Второй класс иногда называют средствами анализа защищенности системного уровня.

Сетевые сканеры являются, пожалуй, наиболее доступными и широко используемыми средствами анализа защищенности. Сканер является необходимым инструментом в арсенале любого администратора либо аудитора безопасности АС.

Современный сетевой сканер выполняет пять основных задач:

- идентификация доступных сетевых ресурсов;
- идентификация доступных сетевых сервисов;
- идентификация имеющихся уязвимостей сетевых сервисов;
- выдача рекомендаций по устранению уязвимостей;
- инвентаризация ресурсов.

В ФСКН России с целью анализа защищенности АС предполагается использование программного продукта MaxPatrol компании Positive Technologies. Одним из достоинств продукта является автоматизация процессов анализа и контроля защищенности распределенных компьютерных систем.

Отметим, что в настоящее время работы по обеспечению защищенности АС необходимо проводить на непрерывном уровне. В ходе каждого нового цикла необходимо, выявляя новые уязвимости, предпринимать действия по их устранению, тем самым повышая уровень защищенности АС.

Отработанные методики проведения обследования (аудита) безопасности АС в соответствии с проверенными критериями делают возможным получение исчерпывающей информации о свойствах АС, имеющих отношение к безопасности.