МЕТОДИКИ ОЦЕНКИ ЭКСПЛУАТАЦИОННЫХ ХАРАКТЕРИСТИК СИСТЕМ ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ В ИНФОКОММУНИКАЦИОННЫХ СЕТЯХ

Марычев Д.В., Мурашко Е.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Бобов М.Н. – д.т.н., профессор

Описана необходимость существования методик оценки эксплуатационных характеристик программных и программно-аппаратных систем предотвращения вторжений как средств защиты информации в системах инфокоммуникаций.

Разработка современных технических и программных продуктов сопровождается проведением ряда тестовых исследований перед началом серийной реализации. Однако, как показывает практика, если такое тестирование выполняется впервые в процессе разработки, то оно не дает положительных результатов, на основании которых можно принять решение о готовности продукта к выпуску. Тестирование и оценка его результатов должны являться постоянной составляющей процесса формирования продукта, а не только его финальным этапом, т.е. быть частью всего жизненного цикла разработки. Каждый без исключения производитель технических средств или программного обеспечения имеет отдел специалистов по информационной безопасности, которые выполняют необходимые проверки, осуществляют контроль над защищенностью продукта и проверяют подверженность продукта уязвимостям со стороны злоумышленников.

Современные системы предотвращения вторжений являются полноценными средствами защиты информации, обязательные для внедрения в каждую инфокоммуникационную сеть, в которой передаётся и хранится информация, несущая в себе коммерческую и информационную ценность. Получение доступа злоумышленника к конфиденциальной информации может нести за собой как огромные финансовые потери, так и возможную подверженность преступникам отдельных личностей, организаций и даже стран.

Системы предотвращения вторжений (англ. Intrusion Prevention System, или IPS) являются так называемой «Системой 2 в 1», так как являются расширением систем обнаружения вторжений (англ. Intrusion Detection System, или IDS). Задача отслеживания атак у данных систем является одинаковой, однако IPS должна отслеживать активность в реальном времени и быстро реализовывать действия по предотвращению атак. Данный фактор предполагает еще больший уровень требований к системам предотвращения вторжений, так как от них непосредственно зависит безопасность и конфиденциальность различных данных.

Методики оценки эксплуатационных характеристик способствуют своевременному обнаружению проблем, которые могут привести к успешным противозаконным действиям со стороны злоумышленника. Обнаружение уязвимости на этапе тестирования позволяет разработчикам технических и программных продуктов заблокировать все возможные варианты незаконных действий злоумышленника для получения выгоды. Методики оценки позволяют определить, какие типы, виды и количество атак и других типов угроз может предотвратить тестируемая система, что позволяет распределить тестируемые системы предотвращения вторжений, как программные, так и программно-аппаратные, на определенные группы, которые предполагают сценарии их использования. а также их пригодность для использования в сетях различных организаций. Результаты грамотно определенных методик испытаний дают гарантию того, что оцененная система удовлетворяет требованиям и ведет себя в соответствии с ними во всех предусмотренных ситуациях. Также данные результаты помогают определить, какими эксплуатационными параметрами может обладать система, что позволит потенциальному покупателю, увидев заключения экспертов, определить, какое именно решение правильнее и выгоднее всего использовать в организации инфокоммуникационной система.

Для того, чтобы стандартизовать эту деятельность, научное и профессиональное сообщества находятся в постоянном сотрудничестве, направленном на выработку базовой методологии, политик и индустриальных стандартов в области технических мер защиты информации, юридической ответственности, а также стандартов обучения пользователей и администраторов. Эта стандартизация в значительной мере развивается под влиянием широкого спектра законодательных и нормативных актов, которые регулируют способы доступа, обработки, хранения и передачи данных, но подразумевает собой засекречивание методик испытаний, чтобы исключить доступ к этой информации потенциальным злоумышленникам.