УДК 343.34

Р. С. Хамидуллин
начальник кафедры оперативно-розыскной деятельности
органов внутренних дел
Уральского юридического института МВД России,
кандидат юридических наук
Е. В. Берсенев
курсант 304 учебной группы
Уральского юридического института МВД России

ВЕДОМСТВЕННЫЕ КИБЕРПОЛИГОНЫ КАК ПЕРСПЕКТИВА ДЛЯ ПРЕДОТВРАЩЕНИЯ КИБЕРУГРОЗ

Информационная безопасность в Российской Федерации — приоритетная задача для силовых органов, связанная с обеспечением собственной безопасности и с эффективным выполнением задач по обеспечению правоохранительной деятельности и национальной безопасности.

Усложнившаяся инфраструктура современной России представляет широко развитую цифровую среду, требующую особого подхода.

Консолидация ресурсов ведомственных подразделений правоохранительных органов и государственной безопасности является наиболее рациональным средством разработки способов и методов предотвращения киберугроз. Таким образом, ведомственный центр предотвращения киберугроз на базе независимых и автономно функционирующих киберполигонов будет наиболее перспективным инструментом в решении ряда вопросов информационной безопасности и информационных технологий в целом.

Киберполигон представляет собой многофункциональный программно-аппаратный комплекс, мимикрирующий собой цифровую инфраструктуру ведомственного органа (ведомственных органов) или подразделения (подразделений), позволяющий тестировать внедрение структурных аппаратно-программных комплексов, отрабатывать сценарии действий, создавать искусственную контролируемую среду для анализа программных вирусов, «червей» и «троянов», а также дублировать функции основных систем, как резерв цифровой инфраструктуры ведомственного органа или подразделения. Изолированность и подконтрольность как характеристики позволяют реализовать цель генерации киберполигонов в составе ведомственного центра (центров) — реализовывать свои функции без рисков нанесения ущерба основным системам. Опыт симуляции применения искусственных и «случайных» угроз позволит анализировать и находить уязвимости в информационно-

телекоммуникационной инфраструктуре ведомства, не прибегая к деструктивным тестам собственных ресурсов.

Возможности центра предотвращения кибератак напрямую отражают его структуру функциональных генерируемых киберполигонов, которые в перспективе будут подразделяться на учебный (подготовка узкоспециализированных кадров на базе практического обучения борьбе с киберугрозами в искусственной контролируемой среде), тестировочный (создание виртуализированной инфраструктуры, к которой представляется возможным подключение аппаратных и программных модулей, проходящих проверку внедрения в реальные ведомственные системы, а также дальнейшей их эксплуатации в рамках агрессивной среды (провокация атак на данные модули)), дублирующий (система перенаправления адрес-запросов на облачную структуру с модулями и дублирующими серверами для поддержания вышедших из строя в результате кибератак и других сбоев модулей) и фильтрующий (размещение нейронной сети (аналог ручного просмотра алгоритмов входа-выхода IP-подключений) и программ-фильтров, распределяющих входные потоки безопасно к серверам того или иного ведомства). Целью в данном случае является постоянное сокращение поверхности соприкосновения АРМ с внешними сетями и минимизация времени реагирования при обнаружении угроз (сокращение времени реагирования на киберугрозы с 18 часов (по данным исследования McAfee «TheHiddenCostsofCybercrime») (в некоторых случаях со 100 дней) до «максимального времени появления симптомов или выхода из строя модуля киберполигона», т. е. времени, когда киберугроза начнет себя проявлять и критически воздействовать на модули и системы в виртуальном пространстве фильтрующего киберполигона).

Подводя итоги исследования, ссылаясь на уже успешный опыт применения киберполигонов в виде проекта «Национальный киберполигон — безопасное будущее цифровой России», организованного Ростелекомом при поддержке Банка России, «Сириуса» и ДВФУ, а также проекта «Киберучения: RedTeam, BlueTeam, Antiphishing», можно говорить о целесообразности дальнейшей проработки и реализации проекта «Ведомственных центров предотвращения киберугроз: генерации киберполигонов».

Какая бы модель угроз не использовалась, Центр поможет масштабировать ландшафт угроз за счет автоматизации, предоставляя возможность выполнять быстрее и больше симуляций, чем с помощью ручных методов и привлечением пентестеров.