0.1. *Кулясов Н.* **Влияние наличия информации в системе DNS на активность агентов угроз киберпространства.**

В связи с постоянным расширением киберпространства появилась необходимость отслеживания активности агентов угроз [1]. В данной работе будет рассмотрена активность агентов для новых элементов киберпространства, какими являются созданные интернет-сервисы, службы и компьютерные сети, до и после регистрации элемента на DNS сервере.

Для решения данной задачи был организован модельный стенд по типу darknet [2] нацеленный на сбор информации об активности агентов угроз. Для данного стенда было выделено 253 интернет адресов ранее не фигурировавших в глобальной сети, а также установлен базовый набор интернет сервисов, состоящий из web и ftp серверов. Также для регистрации активности был активирован файрвол. Таким образом, обращение к нашему стенду возможно лишь в результате ошибок конфигурации или нелегитимных действий, например, в целях первичной разведки путем сканирования.

Контрольный период функционирования стенда составил 40 суток, по истечении половины тестового времени была произведена регистрация нечётных адресов из выделенного диапазона на DNS сервере.

Во время функционирования стенд вёл журналы активности web сервисов и файрвола. Таким образом, задача исследования активность агентов угроз свелась к анализу данных из журналов. В связи с большим объёмом данных появилась необходимость в разработке и реализации алгоритмов для обработки лог-файлов и последующей визуализации результатов[3].

В ходе анализа были получены следующие результаты:

1. За весь период функционирования к стенду было произведено 17646072 обращений от 131085 пользователей.
2. За период без записи в DNS было совершено 12261109 обращений, 8 попыток подбора пароля к FTP сервису и 108 попыток обнаружения точек входа в административные ресурсы web-сервиса.
3. За второй период 5384963 обращений и 8 попыток доступа обнаружения точек входа в административные ресурсы web-сервиса.
4. Различий в активности агентов угроз по отношению к адресам с записью DNS и без не выявлено.

На основании полученных результатов можно было бы сделать вывод, что запись на DNS сервере может сократить активность агентов угроз, но если из рассматриваемого периода исключить дни с пиковой активностью, то разница между средним значением активности за сутки составляет 63930 запроса, что на общем фоне незначительно. В связи с этим дальнейшие исследования в данной области по-прежнему актуальны.

Список литературы

[1] Исаев С. В. Кибербезопасность научного учреждения — активы и угрозы // Информатизация и связь. — 2015. — С. 53–57. ISSN: 2078-8320

[2] Марков А. С., Цирлов В. А. Руководящие указания по кибербезопасности в контексте ISO 27032 // Вопросы кибербезопасности. — 2014. — № 1(2), С. 28–35.

[3] Кулясов Н. В. Система распознавания интернет угроз по журналам веб-сервисов // Молодой Учёный. — 2015. — № 11(1), С. 79–83.