М. А. Зубров, Р. А. Чебан
Научный руководитель — кандидат технических наук, доцент А. А. Гордич
БГЭУ (Минск)

КИБЕРАТАКИ И КИБЕРРАЗВЕДКА

В современную эпоху, когда цифровые технологии становятся неотъемлемой частью нашей повседневной жизни, кибератаки представляют собой не только виртуальные угрозы, но и реальные вызовы для нашего общества. От промышленных предприятий до малого бизнеса, от государственных институтов до индивидуальных пользователей — все подвержены риску кибератак, которые могут привести к различным последствиям, начиная от финансовых потерь, утечки конфиденциальной информации и заканчивая реальными угрозами для жизни и здоровья людей.

Кибератаки — это совокупность преднамеренных действий злоумышленника, направленных на нарушение одного из трех свойств информации: доступности, целостности и конфиденциальности.

Выделяют следующие типы кибератак: фишинг, загрузка вредоносных программ, DoS- и DDoS-атаки, спам-атаки, BEC-атаки, брутфорс-атаки, SQL-инъекции, MITM, эксплойт нулевого дня, XSS (англ. Cross-Site Scripting — «межсайтовый скриптинг»). В связи с этим ключевой проблемой является необходимость обеспечения надежной защиты от кибератак.

Борьба с кибератаками предлагает множество вариантов решений. Например, использование эффективных технических средств защиты, недопущение использования простых паролей, контроль безопасности систем, использование актуальных версий веб-серверов и систем управления базами данных.

Но прежде всего стоит отметить кибербразведку. Кибербразведка — это один из наиболее сложных и в то же время важных элементов информационной безопасности (ИБ). Она помогает выстроить надежную систему защиты с опорой на информацию о хакерских группировках, атаки которых направлены против компаний в конкретном регионе или определенной сфере деятельности. С помощью кибербразведки можно идентифицировать угрозы, проанализировать слабые места, понять тактику злоумышленников, что позволяет выстроить надежную систему защиты. Как и любой другой элемент ИБ-системы, кибербразведка использует свои инструменты и сервисы. Кто же осуществляет кибербразведку в целях обеспечения информационной безопасности? Национальные правительства активно занимаются кибербразведкой для обеспечения безопасности своих граждан и критической инфраструктуры.

Для решения задач кибербразведки используются различные программы. Программа Threat Intelligence Platform является одной из наиболее известных. Threat Intelligence Platform — программное обеспечение, которое использует миллионы источников данных для объединения, анализа, сопоставления и визуального

представления информации об угрозах кибербезопасности, кибератаках и уязвимостях, чтобы специалисты ИБ были осведомлены о потенциальных рисках.

Важно подчеркнуть, что кибератаки становятся все более сложными и разрушительными. В настоящее время самым опасным видом киберугроз являются целевые атаки, самым эффективным способом борьбы с которыми являются сетевые песочницы. Песочницы помогают защититься от неизвестных ранее угроз, содержащих в себе макросы или коды, отсутствующие в базе данных сигнатур. Метод действия сетевых песочниц состоит в создании имитации реального компьютера. На рынке присутствует достаточно решений, как аппаратных, так и облачных, которые могут справиться с поставленной задачей.

В целом эффективная киберразведка и использование сетевых песочниц играют решающую роль в обеспечении безопасности информационных систем и сетей, и их важность в борьбе с кибератаками нельзя недооценивать.

А. А. Киселёва, А. А. Кажуро
Научный руководитель — кандидат технических наук М. Н. Садовская
БГЭУ (Минск)

ГРАФИЧЕСКАЯ ВИЗУАЛИЗАЦИЯ ДАННЫХ ДЛЯ АНАЛИЗА ПОКАЗАТЕЛЕЙ ДЕЯТЕЛЬНОСТИ

В деятельности любой организации необходимо анализировать множество взаимосвязанных показателей различных видов ее деятельности. Поэтому данная работа посвящена использованию технологий визуализации, которые позволят упростить анализ информации, сделав ее наглядной. Это и обусловливает актуальность выбранной темы работы.

Основной целью данного исследования является применение инструментов графической визуализации табличных данных для анализа показателей деятельности организации. Пример практической реализации выполнен на основе данных о деятельности Белорусского государственного экономического университета (БГЭУ).

Учреждение образования отличается разносторонностью видов деятельности, поэтому для анализа его деятельности необходим инструмент, позволяющий одновременно представить несколько показателей. Для достижения поставленной цели был выбран функционал Excel как одного из самых распространенных программных продуктов для работы с табличными данными, а именно — возможности построения дашборда.

Дашборд — это информационная панель, отображающая данные нескольких показателей с интерактивным управлением. Дашборды нужны для того, чтобы принимать решения оперативно по наглядным данным вместо изучения объ-