реклама. Расширение поддерживает технологию белых списков, позволяющих создать список исключений (доменов), для которых будет исключаться блокировка процедуры сбора информации о компьютере пользователя. На втором этапе исследования выполнялось тестирование расширения с предустановленными настройками. Необходимо отметить одно из преимуществ расширения – при блокировке процедур отслеживания со стороны интернет ресурса. Расширение демонстрирует, какие из процедур блокируются.

Таким образом, показано, что Ghostery позволяет просматривать и блокировать средства слежения на посещаемых веб-сайтах, позволяя контролировать сбор пользовательских данных. EnhancedAntiTracking (улучшенный антитрекинг) также обезличивает пользовательские данные для дополнительной конфиденциальности. Из недостатков расширения можно указать на более продолжительную загрузку веб-страниц [1, 2].

Список литературы

1. Расширение для браузеров Ghostery: отключение слежки за поведением посетителя. [Электронный ресурс]. URL: https://www.kv.by (дата обращения: 22.04.2019).

2. Ghostery – анонимность в сети Интернет. [Электронный ресурс]. URL: https://sys-team-admin.ru (дата обращения: 22.04.2019).

3. ОбзорприложенияGhostery Storage Server. [Электронный ресурс]. URL: https://geekon.media (дата обращения: 22.04.2019).

ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ КОРПОРАТИВНОЙ СЕТИ С ПОМОЩЬЮ PARROT SECURITY OS

А.Д. Михейчик, О.А. Хацкевич

На сегодняшний день многие организации проводят мониторинг своей корпоративной сети для обнаружения уязвимостей, воспользовавшись которыми злоумышленники могут осуществить нелегитимные действия. Для проведения мониторинга сети могут закупаться специализированные программные или аппаратные средства, наниматься специалисты по информационной безопасности, использоваться online-инструменты и т.п.

В последнее время наибольшую популярность набирает тестирование на проникновение (пентестинг). Задача данной технологии заключается в осуществлении сетевых атак, которые не приводят к существенным последствиям работы сети, но с помощью которых можно обнаружить недостатки в корпоративной сети. К пентестингу можно отнести дистрибутив Linux – Parrot Security OS.

Parrot Security OS – дистрибутив Linux, основанный на операционной системе Debian. Основные задачи данного дистрибутива – проведение пентестинга, осуществление оценки уязвимостей и их устранение, анонимный просмотр веб-стариц.

Главные отличия представленного дистрибутива от известного Kali Linux следующее:

– в состав Parrot Security OS входит больше инструментов, с помощью которых можно осуществлять пентестинг;

– требует меньше ресурсов при установке, чем Kali;

– Parrot Security OS имеет более удобный графический интерфейс;

– направлен на большую анонимность при работе в сети Интернет, в отличие от дистрибутива Kali Linux.

ЦЕНТР ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ КАК СОСТАВЛЯЮЩАЯ СИСТЕМЫ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Е.В. Моженкова, А.И. Парамонов

В состав корпоративной вычислительной сети входят персональные компьютеры пользователей, и являются одним из источников угроз безопасности данных, обрабатываемых корпоративными информационными системами (КИС) [1]. Для снижения уровня угрозы безопасности на предприятиях вводятся ряд организационных и технических мер