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

по предотвращению несанкционированного доступа. Они позволяют нейтрализовать предполагаемую угрозу безопасности при работе с КИС. Для организации процесса обслуживания корпоративных вычислительных сетей вводятся регламенты установки, эксплуатации и обслуживания вычислительной техники. Одним из основных требований регламента является сохранение аппаратной и программной конфигурации эксплуатируемой компьютерной техники.

В докладе обсуждается эффективность применения центра программного обеспечения System Center Configuration Manager [2] в вычислительной сети крупного предприятия. На предприятии запрещено самостоятельно устанавливать программное обеспечение (ПО). Службы системной интеграции ежеквартально проводят аудит ПО, установленного на рабочих станциях с целью контроля и обеспечения функционирования средств вычислительной техники, обнаружения нелицензированного ПО и пр. Центр программного обеспечения позволил не только обеспечить контроль установки и обновления ПО, но и сократить количество обращений в службу технической поддержки на 1/3. Эффективность возросла за счет реализации возможности доступа пользователя к установке разрешенного перечня дополнительного ПО, не повышая вероятности угрозы безопасности данных.

Список литературы

1. Моженкова Е.В., Парамонов А.И. Опыт применения методики определения угроз безопасности информации в корпоративных информационных системах // Тез. докл. XVI Белорусско-российской науч.-техн. конф. «Технические средства защиты информации». Минск, 5 июня 2018 г. С. 65.

2. System Center Configuration Manager Documentation [Электронный ресурс]. URL: https://docs.microsoft.com/en-us/sccm/ (дата обращения: 18.04.2019).

ИССЛЕДОВАНИЕ ПРОЦЕССОВ ПЕРЕНОСА НОСИТЕЛЕЙ ЗАРЯДА В МНОГОСЛОЙНЫХ ПОЛУПРОВОДНИКОВЫХ СТРУКТУРАХ С ИСПОЛЬЗОВАНИЕМ ГРАФЕНА

В.В. Муравьев, В.Н. Мищенко

Рассмотрены вопросы моделирования процессов переноса носителей заряда в многослойной полупроводниковой структуре с использованием одиночного слоя графена. Высокое значение подвижности электронов, высокая теплопроводность и ряд других положительных свойств делают графен перспективным материалом для использования в полупроводниковых приборах и микросхемах. Вместе с тем, для реализации уникальных свойств и характеристик графена, учитывая двухмерный характер этого материала, весьма важен выбор сопутствующих полупроводниковых и диэлектрических материалов, обеспечивающих формирование законченного в технологическом плане полупроводникового прибора. В этом плане большое внимание привлекает внимание использование пленочного нитрида бора – BN, который может иметь гексогональную кристаллическую структуру, которая близка к структуре графена, небольшую величину толщины слоя, и небольшое значение шероховатости поверхности, величина которой заметно ниже, чем у известных аналогов этого материала. На основе известных принципов, которые лежат в основе использования метода статистического моделирования – метода Монте Карло, проведены исследования основных механизмов рассеяния при переносе носителей заряда в слоях структуры полупроводникового прибора, использующего материалы графен и нитрид бора. Для материала BN с гексогональной кристаллической структурой получены зависимости интенсивностей (частот) рассевания от энергии поля при рассеивании на полярных оптических фононах, на примесях, при акустическом рассеянии, при междолинном рассеивании, а также суммарная зависимость по всем механизмам рассеивания. Исследованы закономерности физического процесса переноса носителей заряда в материале BN. Использование многослойных полевых транзисторов, использующих материалы графен и нитрид бора, позволит создать приборы и устройства, которые найдут широкое применение в системах приема, усиления и обработки сигналов в диапазонах СВЧ и КВЧ.