преодоления», «Обучение личности безопасному поведению с учетом психофизических характеристик».

Изучаемые в рамках семинарских занятий методики тестирования и оценки различных аспектов социально-психологического поведения позволят специалистам в области информационной безопасности получить практические навыки и умения по оценке особенностей нервной системы, восприятия, памяти, внимания и мышления человека, достаточно важные при обеспечении информационной безопасности.

Литература

1. *Кузнецов М.В., Симдянов И.В.* Социальная инженерия и социальные хакеры. Санкт-Петербург, 2007.

2. *Емельянов С.М.* Практикум по конфликтологии. Санкт-Петербург, 2009.

СОВЕРШЕНСТВОВАНИЕ ПРЕПОДАВАНИЯ КУРСА «ЦИФРОВЫЕ УСТРОЙСТВА»

А.А. Будько

Булева алгебра и классический синтез цифровых логических устройств составляют основу любого курса по цифровой технике. Изложение этого материала в русскоязычной, а также англоязычной литературе не меняется в течение довольно длительного периода времени и, к сожалению, имеет ряд недостатков.

Обычно при синтезе комбинационных устройств составляется таблица истинности, извлекается функция алгебры логики в совершенной дизъюнктивной нормальной форме, затем эта функция минимизируется и строится логическая схема, используя элементы И, ИЛИ, или только И-НЕ элементы. Такой подход является успешным, но не более чем в 50%. В докладе анализируется эта ситуация и показывается, что для успешного синтеза комбинационных устройств необходимо извлекать из таблицы истинности и минимизировать не только саму функцию алгебры логики, но и обратную функцию. И не только в дизъюнктивной, но и в конъюнктивной нормально форме, и только после этого выбирать и строить логическую схему.

Второе, что предлагается в докладе, это включить в классический синтез комбинационных устройств упрощение (минимизацию) функций алгебры логики в базисе функций ИСКЛЮЧАЮЩЕЕ ИЛИ, ИСКЛЮЧАЮЩЕЕ ИЛИ-НЕ. Эти функции широко используются в синтезе комбинационных схем и широко представлены в интегральном исполнении. Логический синтез в базисе функций ИСКЛЮЧАЮЩЕЕ ИЛИ впервые был рассмотрен в работе «Ring Map Minimizes Logic Circuit» автора Fronek, Donald K. Предложенная модернизация карт Карно оказалась не очень удачной, и этот метод не нашёл практического применения. Однако в книге «Modern Digital Electronics» автором R.P.Jain предложено использовать обычные карты Карно. И в отличие от поиска логически соседних минтермов или макстермов, которые на карте Карно геометрически находятся по горизонтали и вертикали, при синтезе комбинационных устройств в базисе функций ИСКЛЮЧАЮЩЕЕ ИЛИ, ИСКЛЮЧАЮЩЕЕ ИЛИ-НЕ рассматривается диагональное соседство (diagonal), D-соседство и отдаленное(offset) соседство или О-соседство.

БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ ПОПУЛЯРНЫХ CMS В УЧРЕЖДЕНИЯХ ОБРАЗОВАНИЯ

А.С. Цалко

В настоящие момент ни одно учреждение образование образования не обходится без веб-сайта. Как правило, сайты университетов или прочих крупных образовательных или научных организацией самостоятельно разрабатываются командой профессионалов. Однако, у любого такого института существуют подразделения, которым не хватает функционала главного сайта. В таких случаях им на помощь приходят бесплатные популярные CMS (системы управления содержимым).

Сайты образовательных и научных учреждений пользуются у поисковых систем высоким авторитетом. Материалы, размещенные на таких сайтах, быстрее занимают лидирующие позиции в выдаче поисковых систем. Это автоматически делает такие ресурсы объектом внимания злоумышленников, неправомерно использующих сайты для получения выгоды.

Была проведена начальная работа по разработке комплекса мер и набора методик для защиты сайтов на примере образовательных веб-ресурсов БГУИР. Необходимо было составить список популярных CMS, безопасность которых будет проанализирована в первую очередь. В качестве исследуемой совокупности были выбраны 260 млн сайтов, размещенных на более чем 50 популярных доменных зонах. С помощью распределенных вычислений на комплексе серверов проведен анализ наличия признаков более чем 600 CMS. Наиболее популярными оказались WordPress (более 14 млн. сайтов), Joomla (3 млн сайтов) и Drupal (700 тыс. сайтов).

Далее для 10 самых популярных CMS был проведен первичный количественный анализ наличия уязвимостей к данным системам и их компонентам. Были исследованы открытые базы данных, на подобии OSVDB и CVE. В результате можно сделать вывод о корреляции количества использования CMS в сети «Интернет» и количества уязвимостей к ним.

В структуре веб-узлов подразделений БГУИР, как и любого другого образовательного учреждения, работает немалое количество сайтов, использующих описанные системы. Их популярность уже создает сильнейшую угрозу информационной безопасности данных организаций. Проведенная работа подтверждает актуальность выбранного мной направления исследования информационной безопасности веб-узлов.

ОПТИМИЗАЦИЯ СОСТОЯНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЧЕРЕЗ ОБУЧЕНИЕ СОТРУДНИКОВ

Д.В. Новоселецкий, Г.А. Пухир

Существующие на сегодняшний день программно-технические средства способны успешно противостоять угрозам информационной безопасности, но при этом с каждым годом растёт процент утечек, произошедших по вине персонала. По данным Infowatch, в 2014 г., по сравнению с 2013 г. возросла доля случайных утечек (49,7% против 39,4%), а в 55% случаев причиной утечек стали настоящие или бывшие сотрудники [1].

Осведомлённость персонала позволит не только снизить процент утечек, но и значительно сократить число жалоб на трудновыполнимые правила политики информационной безопасности.

Процесс обучения ни в коем случае не должен ограничиваться автографом после ознакомления с политикой безопасности. Необходима постоянная активная работа специалистов службы безопасности или руководства компании в отношении сотрудников: лекции, инструктажи, тренировочные мероприятия, имитирующие атаки. Должен быть разработан свод простых четких и понятных правил, которые рекомендуется располагать в хорошо заметных местах: на канцелярских принадлежностях, на дверях, на кулерах с водой, кофе-машинах и чайниках. Оценить успешность процесса обучения помогут заранее установленные критерии, например: количество открытых ссылок в письмах, имитирующих фишинг-атаку; количество подключенных к ПК накопителей, оставленных на столе в отсутствии сотрудника; количество не уничтоженных бумаг в мусоре. Любой процесс обучения должен сопровождаться поощрениями и наказаниями, здесь важно не забывать о том, что не столь эффективно само наказание, как осознание его неотвратимости. Знания сотрудников — это сила в защите компании.

Литература

1. Исследование утечек конфиденциальной информации в 2014 г. [Электронный ресурс]. – Режим доступа: http://www.infowatch.ru/report2014