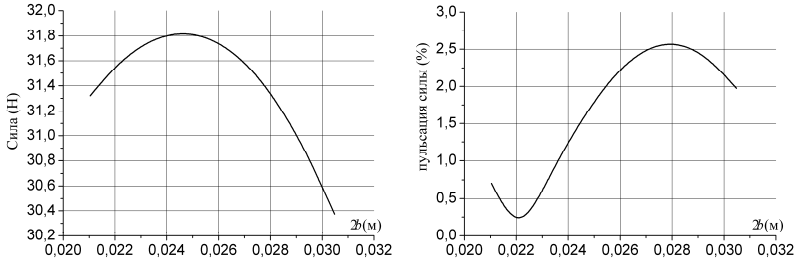

а) *б)*

Рис. 7. График зависимости тягового усилия (*а*) и пульсаций (*б*) от ширины $2b$ полюсного магнита без введения межполюсных магнитов

Дальнейшим шагом является увеличение тягового усилия за счет введения однородно намагниченных постоянных магнитов в межполюсные участки (рис.1). Магнитное поле в этом случае рассчитывалось по формуле (16), учитывающей наличие межполюсных магнитов, а тяговое усилие, как и в предыдущем случае, по формуле (21). Результаты расчётов среднего значения тягового усилия и его пульсации для линейного двигателя с теми же параметрами, что и выше, но при наличии межполюсных участков, представлены на рис.7.

Как показал расчёт, максимальное среднее значение тягового усилия соответствует ширине полюсного магнита $2b \approx 24{,}6$ мм и равно $F_{\text{теор.ср.}} = 31{,}9$ Н, пульсация $\varepsilon = 1{,}59$ %. Таким образом, увеличение тягового усилия по сравнению с магнитной системой, состоящей только из полюсных магнитов с $2b = 27{,}93$ мм, составляет 6 %.

1. *Тозони О. В. Маергойз И. Д.* Расчет трехмерных электромагнитных полей. – К.: Техніка, 1974. – 352 с.

Поступила 1.03.2010р.

УДК 004.056:004.274

Ю.М. Коростиль, А.Н. Давиденко, С.Я. Гильгурт, М.М. Панченко

АНАЛИЗ ВНЕШНИХ АТАК НА ЛОКАЛЬНУЮ СЕТЬ И ВОЗМОЖНОСТЕЙ ЗАЩИТЫ РЕКОНФИГУРИРУЕМЫМИ УСТРОЙСТВАМИ

The utilization of programmable logic for defense of local area network from external attacks is investigated. Specific threats from internet to local computers and possibilities of FPGA-based digital equipment to parry them are discussed.

Проблемы защиты информации становятся все более актуальными с каждым днем. Растет как ущерб, причиняемый компьютерным системам, так и разнообразие форм и способов злонамеренных действий. Тем не менее, можно выделить области, в которых вопросы защиты информационной безопасности возникают намного чаще, а их решение намного актуальнее.

К одной из таких областей относится круг задач, связанных с защитой информации в локальной компьютерной сети. На сегодняшний день отдельно стоящий компьютер все труднее встретить не только в организациях и учреждениях, но и в домашних условиях.

В предыдущей статье авторов [1] на основе анализа известных источников была сформирована классификация существующих и потенциально возможных угроз и опасностей в компьютеризированных системах. Целью создания классификации являлось исследование возможностей применения в качестве средств информационной защиты цифровых реконфигурируемых устройств на базе программируемой логики. Современные программируемые логические интегральные схемы (ПЛИС) позволяют создавать недорогие, но эффективные средства защиты информации в компьютеризированных системах различного уровня [2].

В **настоящей статье** на основе предложенной классификации выбраны и проанализированы наиболее важные и актуальные в смысле частоты реализации угроз и величины причиненного ущерба атаки на локальную компьютерную сеть, инициированные внешними по отношению к ней источниками. При этом главное внимание уделено выявлению таких задач информационной защиты, при решении которых наиболее полно могут быть задействованы возможности цифровых реконфигурируемых устройств.

Анализ последних достижений и публикаций по данной теме свидетельствует о наличии большого количества исследований и практических разработок, связанных с применением программируемой логики для решения проблем информационной безопасности. Однако, в большинстве случаев, область применения данных проектов ограничивается одной конкретной задачей, либо узким классом решаемых задач.

Целью настоящей статьи является исследование и анализ возможностей создания средств информационной безопасности на базе цифровых реконфигурируемых устройств для противодействия широкому классу наиболее актуальных угроз локальной компьютерной сети.

Анализ известных внешних угроз и опасностей, существующих для локальной вычислительной сети, приводит к необходимости рассматривать следующие три класса факторов информационной безопасности [3]:

- вредоносное программное обеспечение (ПО);
- спам;
- глобальные сетевые атаки.

Рассмотрим эти классы подробнее.

1. Вредоносное ПО

Ущерб, причиняемый вредоносными программами, заключается в следующем:

- неавторизованный доступ к информации - ее незаконное уничтожение, изменение, передача (утечка информации);
- ненормальное функционирование программного и аппаратного обеспечения;
- использование вычислительных, дисковых и сетевых ресурсов в чужих интересах в ущерб интересам законных владельцев этих ресурсов.

По принципу действия вредоносное программное обеспечение можно разделить на четыре типа:

- вирусы;
- троянские программы;
- почтовые и сетевые черви;
- пакеты, используемые в хакерских атаках.

Для разработки средств противодействия вредоносному ПО помимо разнообразия его видов необходимо также исследовать среды его возможного обитания и методы проникновения в локальную сеть.

Вредоносное программное обеспечение может функционировать в таких средах, как:

- операционные системы;
- программные пакеты, допускающие запуск сервисных приложений (скриптов, макросов) в целях автоматизации обработки информации или организации различных процессов;
- сетевые приложения, достаточно сложные для того, чтобы располагать функциональными возможностями, необходимыми для размножения вируса или функционирования троянских программ, например, почтовые приложения, браузеры со встроенными скриптовыми языками, сетевые пейджеры, сетевые игры;
- несетевые приложения, которые возможно использовать для распространения вируса, троянской программы или для реализации хакерской атаки, например, вспомогательные утилиты операционных систем, различного рода утилиты, имеющие достаточную сложность и т.п.

Анализ рассмотренных вопросов, а также существующих средств борьбы с вредоносным ПО позволяет выявить следующие проблемы, актуальность которых неуклонно повышается:

- постоянный рост антивирусных баз данных, основанных на хранении сигнатур всех известных вирусов, и, как следствие, неуклонное повышение требований к производительности компьютеров со стороны антивирусных программ такого класса;
- высокая вероятность появления самых различных комбинаций принципов действия, сред обитания и методов проникновения для конкретных реализаций вредоносных программ принципиально исключает

возможность предсказывать заранее их поведение.

Как следствие, для эффективного противодействия вредоносному ПО, от средств защиты требуется качественное повышение как скоростных показателей, так и интеллектуальных возможностей. При этом стоимость таких средств должна обеспечивать доступность, необходимую для массового использования. Технические параметры реконфигурируемых устройств на базе программируемой логики отвечают данным требованиям.

В работе [4] рассмотрен пример возможной организации защиты от вредоносного ПО, а именно, от сетевых червей, с применением реконфигурируемых устройств на базе ПЛИС.

2. Спам

Данный класс атак приводит к таким негативным последствиям, как:

- увеличение нагрузки, вынуждающее увеличивать затраты на поддержку и обслуживание почтовых сервисов;
- риск потери важной информации либо из-за большого количества ненужных данных, либо в результате перегрузки ресурсов (переполнения почтовых ящиков);
- дополнительные непроизводственные расходы временных ресурсов (на фильтрацию спама) и финансовых средств на оплату избыточного трафика (оплату услуг провайдера);
- прочие негативные последствия от опасной и нежелательной информации (фишинг, вовлечение в финансовые аферы и т.п.).

В отличие от вредоносного программного обеспечения, причины появления спама и рост его активности обусловлены в подавляющем большинстве случаев коммерческой мотивацией. Злоумышленники используют его для нелегального маркетинга товаров и услуг. К сожалению, данный факт означает, что актуальность этого класса атак будет только возрастать. По крайней мере, до тех пор, пока не будет найдено принципиальное решение проблемы.

К характерным особенностям борьбы со спамом следует отнести многоплановость предпринимаемых мер. Противодействие осуществляется самыми различными способами, начиная от выявления и оперативного реагирования на появление новых источников распространения спама в глобальной сети, и заканчивая интеллектуальными контекстными фильтрами содержимого почтовых сообщений непосредственно на компьютере пользователя. В этой связи производительность, гибкость и высокие интеллектуальные возможности реконфигурируемых устройств обусловливают перспективность их применения для данных целей.

3. Глобальные сетевые атаки

Разновидности данного класса атак подробно исследованы во многих источниках [5 – 8]. Ущерб от успешно реализованной глобальной интернет-атаки выражается:

- в снижении пропускной способности, либо полном отказе каналов связи интернет-, интранет- или локальной сети;
- в нарушении нормального функционирования программного обеспечения (системного, сетевого, прикладного).

Среди наиболее часто осуществляемых можно выделить следующие реализации сетевых атак.

DoS-атака (англ. Denial of Service – отказ в обслуживании) – атака на вычислительную систему с целью вывести её из строя, то есть создание таких условий, при которых правомерные пользователи не могут получить доступ к предоставляемым системой ресурсам, либо этот доступ затруднен.

Если атака выполняется одновременно с большого числа компьютеров, которые одновременно активизируются в заданный момент времени, имеет место *DDoS-атака* (англ. Distributed Denial of Service, распределенная атака типа "отказ в обслуживании").

Флуд-атака (англ. flood – наводнение) – массированная спланированная атака с множества зараженных компьютеров многочисленными запросами на прием/передачу файлов или сетевых пакетов, при которой возникает перегрузка каналов передачи данных.

Массированная рассылка вируса с множества зараженных компьютеров - атака, при которой перегрузка каналов является не запланированной акцией, а побочным эффектом неконтролируемого распространения вируса.

Причиной глобальной атаки может стать также *нештатное поведение множества зараженных систем*, при котором они начинают неконтролируемое потребление сетевых ресурсов.

Сложность противодействия удаленным сетевым атакам обусловлена самой их природой. Компоненты глобальной сети, задействованные в этом случае, не контролируются ни провайдерами, ни системными администраторами предприятия, ни домашним пользователями. От таких атак не спасает ни эффективное антивирусное ПО, ни отсутствие уязвимостей в программном обеспечении компьютеров, ни грамотно настроенные средства защиты локальной сети от внешних проникновений.

В этой связи представляет интерес использование возможностей программируемой логики для создания на их базе систем обнаружения атак [9]. Принципы построения таких систем предлагаются в ряде работ, например, в [10]. Однако, наиболее перспективным представляется исследование возможностей создания на базе реконфигурируемых устройств многофункциональных систем, позволяющих решать широкий круг задач информационной защиты локальных компьютерных сетей.

Выводы по результатам настоящей работы могут быть сформулированы следующим образом.

Создание средств противодействия наиболее актуальным угрозам информационной безопасности предъявляет повышенные требования по быстродействию и интеллектуальным возможностям. Производительность и

гибкость реконфигурируемых устройств обусловливают перспективность их применения для данных целей. Способность ПЛИС быстро изменять внутреннюю структуру позволят создавать многофункциональные системы, ориентированные на решение широкого круга задач информационной безопасности локальных компьютерных сетей.

1. *Коростиль Ю.М., Давиденко А.Н, Гильгурт С.Я.* Анализ угроз и опасностей в компьютерных системах на предмет защиты цифровыми реконфигурируемыми устройствами // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ НАН України. – Київ, 2010. – Вип. 54. – С. 9–16.
2. *Гильгурт С.Я.* Обзор современных реконфигурируемых унифицированных вычислителей // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ НАН України. – Вип. 49. – Київ: 2008. – С. 17–24.
3. *Касперский Е.В.* Компьютерное zловредство. – СПб.: Питер, 2007. – 208 с.
4. *Гильгурт С.Я.* Особенности применения реконфигурируемых вычислителей для аппаратной защиты информационных систем // Зб. наук. пр. ІПМЕ НАН України. – Вип. 38. – Київ: 2007. – С. 36–41.
5. *Зима В.М., Молдовян А.А., Молдовян Н.А.* Безопасность глобальных сетевых технологий. – 2-е изд. – СПб.: БХВ-Петербург, 2003. – 368 с.
6. *Конеев И.Р., Беляев А.В.* Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003. – 752 с.
7. *Столингс В.* Основы защиты сетей. Приложения и стандарты: Пер с англ. – М.: Изд. дом "Вильямс", 2002. – 432 с.
8. *Щеглов А.Ю.* Защита компьютерной информации от несанкционированного доступа. – СПб.: Наука и техника, 2004. – 384 с.
9. *Лукацкий А.В.* Обнаружение атак. – СПб.: БХВ-Петербург, 2001. – 624 с.
10. *Baker Z.K., Prasanna V.K.* A Methodology for the Synthesis of Efficient Intrusion Detection Systems on FPGAs // Proceedings of the 12th Annual IEEE Symposium on Field-Programmable Custom Computing Machines. Washington: IEEE Computer Society, 2004. P. 135–144.

Поступила 3.03.2010р.

УДК 519.711

В.О. Артемчук

ОБЧИСЛЕННЯ СТАТИСТИЧНИХ ХАРАКТЕРИСТИК ВИБІРКИ В ІНФОРМАЦІЙНО-АНАЛІТИЧНІЙ СИСТЕМІ ЕКОЛОГО-ЕНЕРГЕТИЧНОГО МОНІТОРИНГУ

Вступ

В статтях [1, 2, 3] обґрунтовано актуальність, поставлено та розв’язано задачу збереження даних еколого-енергетичного моніторингу для їх обробки,